HP

Exam Questions HPE6-A85

Aruba Certified Campus Access Associate Exam

NEW QUESTION 1
What does the status of "ALFOE" mean when checking LACP with "show lacp interfaces"'?

A. The interface on the local switch is configured as static-LAG
B. LACP is not configured on the peer side
C. LACP is in a synchronizing process
D. LACP is working fine with no problems

Answer: D

Explanation:
The status of ??ALFOE?? means that LACP Link Aggregation Control Protocol (LACP) is a network protocol that provides dynamic negotiation of link aggregation between two devices. LACP allows multiple physical links to be combined into a single logical link for increased bandwidth, redundancy, and load balancing. LACP is defined in IEEE 802.3ad standard. is working fine with no problems when checking LACP with ??show lacp interfaces??. The status of ??ALFOE?? is an acronym that stands for:
? A: Active - The interface is actively sending LACP packets to negotiate link
aggregation with the peer device.
? L: Link Up - The interface has physical connectivity with the peer device.
? F: Aggregatable - The interface can be aggregated with other interfaces into a single logical link.
? O: Synchronized - The interface has successfully negotiated link aggregation parameters with the peer device and can transmit or receive traffic on the logical link.
? E: Collecting/Distributing - The interface is collecting incoming traffic from the peer
device and distributing outgoing traffic to the peer device on the logical link. The other options are not correct because:
? The interface on the local switch is configured as static-LAG: This option is false because static-LAG does not use LACP to negotiate link aggregation. Static-LAG requires manual configuration of link aggregation parameters on both devices and does not have any status indicators.
? LACP is not configured on the peer side: This option is false because if LACP is
not configured on the peer side, the status of the interface would be ??ALF–?? instead of ??ALFOE??. This means that the interface would not be synchronized or collecting/distributing with the peer device.
? LACP is in a synchronizing process: This option is false because if LACP is in a
synchronizing process, the status of the interface would be ??ALF-O?? instead of ??ALFOE??. This means that the interface would not be collecting/distributing with the peer device.
References: https://www.arubanetworks.com/techdocs/AOS- CX_10_08/NOSCG/Content/cx-noscg/lag/lag-overview.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx- noscg/lag/lag-lacp.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/lag/lag-lacp-status.htm

NEW QUESTION 2
DRAG DROP
Match the appropriate QoS concept with its definition.

QoS concept		Definition
Best Effort Service		A method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Class of Service		A method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes
Differentiated Services		A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard
WMM		A method where traffic is treated equally in a first-come, first-served manner

A. Mastered
B. Not Mastered

Answer: A

Explanation:
QoS Quality of Service (QoS) is a set of techniques that manage network resources and provide different levels of service to different types of traffic based on their requirements. QoS can improve network performance, reduce latency, increase throughput, and prevent congestion. concept and its definition. Here is my Answer:
QoS Concept:
? Best Effort Service
? Class of Service
? Differentiated Services
? WMM ========== Definition:
d) A method where traffic is treated equally in a first-come, first-served manner a) A method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes b) A method for classifying network traffic at Layer 3 by
marking packets with one of 64 different service classes c) A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard
Short But Comprehensive Explanation of Correct Answer Only: The correct match between QoS concept and its definition is as follows:
? Best Effort Service: This is a method where traffic is treated equally in a first-come,
first-served manner without any prioritization or differentiation. This is the default service level for most networks and applications that do not have specific QoS requirements or guarantees. Best Effort Service does not provide any assurance of bandwidth, delay, jitter, or packet loss.
? Class of Service: This is a method for classifying network traffic at Layer 2 by
marking 802.1Q VLAN Ethernet frames with one of eight service classes (0 to 7). These service classes are also known as IEEE 802.1p priority values or PCP Priority Code Point (PCP) is a 3-bit field in the 802.1Q VLAN tag that indicates the priority level of an Ethernet frame . Class of Service allows network devices to identify and handle different types of traffic based on their priority levels. Class of Service is typically used in LAN Local Area Network (LAN) is a network that

connects devices within a limited geographic area, such as a home, office, or building environments where Layer 2 switching is predominant.
? Differentiated Services: This is a method for classifying network traffic at Layer 3
by marking packets with one of 64 different service classes (0 to 63). These service classes are also known as DiffServ Code Points (DSCP) DiffServ Code Point (DSCP) is a 6-bit field in the IP header that indicates the service class of a packet . Differentiated Services allows network devices to identify and handle different types of traffic based on their service classes. Differentiated Services is typically used in WAN Wide Area Network (WAN) is a network that connects devices across a large geographic area, such as a country or continent environments where Layer 3 routing is predominant.
? WMM: This is a method for classifying network traffic using access categories
based on the IEEE 802.11e QoS standard. WMM stands for Wi-Fi Multimedia and it is a certification program developed by the Wi-Fi Alliance to enhance QoS for wireless networks. WMM defines four access categories (AC): Voice, Video, Best Effort, and Background. These access categories correspond to different priority levels and contention parameters for wireless traffic. WMM allows wireless devices to identify and handle different types of traffic based on their access categories.
References: https://en.wikipedia.org/wiki/Quality_of_service https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_dfsrv/configuration/xe-16/qos-dfsrv-xe-16-book/qos-dfsrv-overview.htmlhttps://www.cisco.com/c/en/us/support/docs/quality-of- service-qos/qos-packet-marking/10103-dscpvalues.html https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/81831-qos- wlan.html https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm

NEW QUESTION 3
You need to troubleshoot an Aruba CX 6200 4-node VSF stack switch that fails to boot correctly Select the option that allows you to access the switch and see the boot options available for OS images and ServiceOS.

A. Member 2 RJ-45 console port
B. Member 2 switch mgmt port
C. Conductor USB-C console port
D. Conductor mgmt port using SSH

Answer: C

Explanation:
The option that allows you to access the switch and see the boot options available for OS images and ServiceOS is Conductor USB-C console port. This option provides direct access to ServiceOS, which is an operating system that runs on Aruba CX switches independently of AOS-CX Aruba Operating System CX (AOS-CX) is an operating system that runs on Aruba CX switches . ServiceOS provides low-level functions such as booting, firmware upgrades, password recovery, hardware diagnostics, switch stacking, and system recovery. ServiceOS can be accessed through one of two methods:
? Conductor USB-C console port: This method allows you to connect your PC or
laptop to the USB-C console port on any member switch in a VSF stack using a USB-C cable. This method provides direct access to ServiceOS without requiring any configuration or authentication on AOS-CX.
? AOS-CX CLI: This method allows you to access ServiceOS through AOS-CX CLI
using SSH or Telnet protocols. This method requires you to configure an IP address on AOS-CX and authenticate with your username and password.
To see the boot options available for OS images and ServiceOS, you need to access ServiceOS through Conductor USB-C console port and enter boot menu command at ServiceOS prompt.
The other options do not allow you to access the switch and see the boot options available for OS images and ServiceOS because:
? Member 2 RJ-45 console port: This option allows you to connect your PC or laptop
to the RJ-45 console port on any member switch in a VSF stack using an RJ-45 cable. This option provides direct access to AOS-CX CLI, not ServiceOS.
? Member 2 switch mgmt port: This option allows you to connect your PC or laptop
to the switch mgmt port on any member switch in a VSF stack using an Ethernet cable. This option provides indirect access to AOS-CX CLI through SSH or Telnet protocols, not ServiceOS.
? Conductor mgmt port using SSH: This option allows you to connect your PC or
laptop to the mgmt port on any member switch in a VSF stack using an Ethernet cable. This option provides indirect access to AOS-CX CLI through SSH protocol, not ServiceOS.
References: https://www.arubanetworks.com/techdocs/AOS- CX_10_08/NOSCG/Content/cx-noscg/serviceos/serviceos-overview.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx- noscg/serviceos/access-serviceos.htm https://www.arubanetworks.com/techdocs/AOS- CX_10_08/NOSCG/Content/cx-noscg/serviceos/boot-menu.htm

NEW QUESTION 4
DRAG DROP
Match each AAA service with its correct definition (Matches may be used more than once or not at all)

Definition	AAA Service
A list of rules that specifies which entities are permitted or denied access	Accounting
Control users access on the network	Authentication
Tracking user activity on the network	Authorization
Who can access the network based on credentials/certificates	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
AAA Authentication, Authorization, and Accounting (AAA) Authentication, Authorization, and Accounting (AAA) is a framework that provides security services for network access control . AAA consists of three components:
? Authentication: The process of verifying the identity of a user or device that wants
to access the network based on credentials such as username and password , certificates , tokens , etc . Authentication can use different protocols such as PAP , CHAP , EAP , RADIUS , TACACS+ , etc .
? Authorization: The process of granting or denying access to network resources
based on the identity and privileges of a user or device . Authorization can use different methods such as ACLs , RBAC , MAC , DAC , etc .

? Accounting: The process of recording and reporting the activities and usage of
network resources by users or devices . Accounting can use different formats such as syslog , SNMP , NetFlow , etc .service. Here is my Answer:
The correct match for each AAA service with its definition is:
? Accounting: C. Tracking user activity on the network
? Authentication: D. Who can access the network based on credentials/certificates
? Authorization: B. Control users access on the network The other options are not correct matches because:
? A list of rules that specifies which entities are permitted or denied access: This option is a definition of an access control list (ACL) Access Control List (ACL) Access Control List (ACL) is a list of rules that specifies which entities are
permitted or denied access to a network resource such as a router , switch , firewall , server , etc . ACLs can be based on different criteria such as source and destination IP addresses , port numbers , protocol types , time of day , etc . ACLs can be applied to different interfaces or directions such as inbound or outbound . ACLs can be verified by using commands such as show access-lists , show ip access-lists , debug ip packet , etc . , not an AAA service.
? Who can access the network based on credentials/certificates: This option is a
definition of authentication, not authorization. Authorization is the process of granting or denying access to network resources based on the identity and privileges of a user or device, not based on credentials/certificates.
References: https://en.wikipedia.org/wiki/AAA_(computer_security) https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

NEW QUESTION 5
When performing live firmware upgrades on Aruba APs. which technology partitions all the APs based on RF neighborhood data minimizing the impact on clients?

A. Aruba ClientMatch
B. Aruba Ai insights
C. Aruba AirMatch
D. Aruba ESP

Answer: C

Explanation:
Aruba AirMatch is a feature that optimizes RF Radio Frequency. RF is any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. performance and user experience by using machine learning algorithms and historical data to dynamically adjust AP power levels, channel assignments, and channel width. AirMatch performs live firmware upgrades on Aruba APs by partitioning all the APs based on RFneighborhood data and minimizing the impact on clients. AirMatch uses a rolling upgrade process that upgrades one partition at a time while ensuring that adjacent partitions are not upgraded simultaneously. References: https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdfhttps://www.arubanetworks.co m/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/arm/AirMatch.htm

NEW QUESTION 6
Based on the "snow ip route" output on an AruDaCX 8400. what type of route is "10.1 20
0/24, vrf default via 10.1.12.2. [1/0]"?

A. local
B. static
C. OSPF
D. connected

Answer: B

Explanation:
A static route is a route that is manually configured on a router or switch and does not change unless it is modified by an administrator. Static routes are used to specify how traffic should reach specific destinations that are not directly connected to the device or that are not reachable by dynamic routing protocols. In Aruba CX switches, static routes can be configured using the ip route command in global configuration mode. Based on the ??show ip route?? output on an Aruba CX 8400 switch, the route ??10.1 20 0/24, vrf default via 10.1.12.2, [1/0]?? is a static route because it has an administrative distance of 1 and a metric of 0, which are typical values for static routes. References: https://en.wikipedia.org/wiki/Static_routing https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static- routes.htmhttps://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx- noscg/ip-routing/show-ip-route.htm

NEW QUESTION 7
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

NEW QUESTION 8
Which device configuration group types can a user define in Aruba Central during group creation? (Select two.)

A. Security group
B. Template group
C. Default group
D. Ul group
E. ESP group

Answer: BC

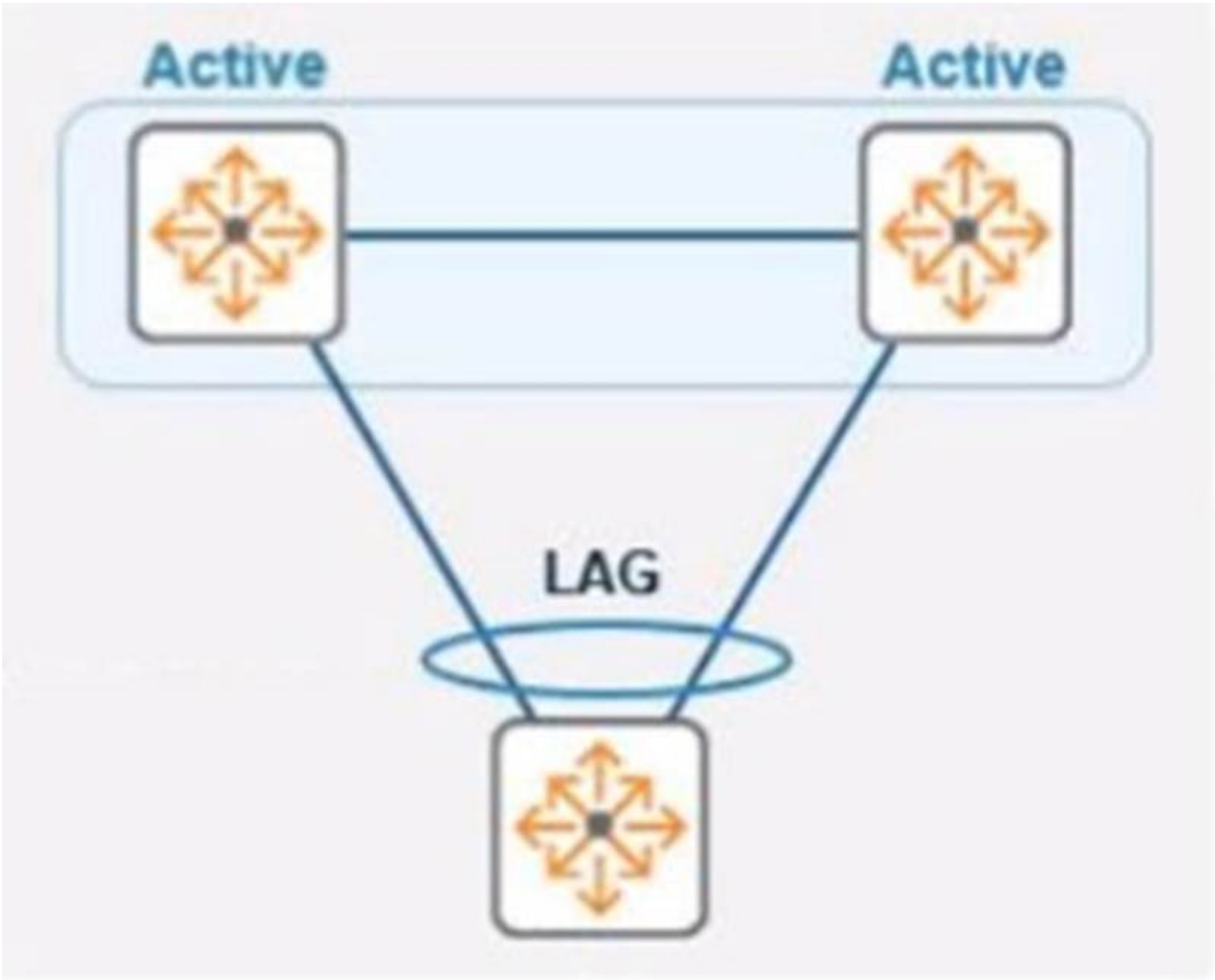
Explanation:
Aruba Central allows you to create device configuration groups that define common settings for devices within each group. You can create different types of groupsdepending on your network requirements and management preferences. Two types
of groups that you can define in Aruba Central during group creation are:
? Template group: A template group allows you to create configuration templates using variables and expressions that can be applied to multiple devices or device groups. Template groups provide flexibility and scalability for managing large-scale deployments with similar configurations.
? Default group: A default group is automatically created when you add devices to Aruba Central for the first time. The default group contains basic configuration settings that are applied to all devices that are not assigned to any other group. You can modify or delete the default group as needed.
References: https://www.arubanetworks.com/techdocs/Central/latest/content/nms/device- groups.htm
https://www.arubanetworks.com/techdocs/Central/latest/content/nms/template- groups.htm
https://www.arubanetworks.com/techdocs/Central/latest/content/nms/default- group.htm

NEW QUESTION 9
Describe the purpose of the administrative distance

A. Routes teamed via external BGP have a higher administrative distance than routes learned via OSPF
B. The administrative distance is used as a trust rating tor route entries
C. The administrative distance for a static route is 10
D. The higher administrative distance is preferred

Answer: B

NEW QUESTION 10
Refer to the exhibit.



In the given topology, a pair of Aruba CX 8325 switches are in a VSX stack using the active gateway What is the nature and behavior of the Virtual IP for the VSX pair if clients are connected to the access switch using VSX as the default gateway?

A. Virtual IP is active on the primary VSX switch Virtual floating IP will failover in case of a failure
B. Virtual IP is active on both CX switches
C. Virtual IP uses SVI IP address synced with VSX

Answer: A

Explanation:
Virtual Switching Extension (VSX) is a feature that allows two Aruba CX switches to operate as a single logical device with a single control plane and data plane. VSX provides high availability, scalability, and simplified management for campus and data center networks3. In VSX, one switch is designated as the primary switch and the other as the secondary switch. The primary switch owns and responds to ARP Address Resolution Protocol. ARP is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite. requests for the virtual IP address of the VSX pair4. The virtual IP address is used as the default gateway for clients connected to the access switch. If the primary switch fails, the secondary switch takes over the virtual IP address and continues to forward traffic for the clients5. References: 3 https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-overview.htm 4 https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-ip- addressing.htm 5 https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-failover.htm

NEW QUESTION 10
Which part of the WPA Key Hierarchy is used to encrypt and/or decrypt data"

A. Pairwise Temporal Key (PTK)
B. Pairwise Master Key (PMK)
C. Key Confirmation Key (KCK)
D. number used once (nonce)

Answer: A

Explanation:
The part of WPA Key Hierarchy that is used to encrypt and/or decrypt data is Pairwise Temporal Key (PTK). PTK is a key that is derived from PMK Pairwise Master Key (PMK) is a key that is derived from PSK Pre-shared Key (PSK) is a key that is shared between two parties before communication begins , ANonce Authenticator Nonce (ANonce) is a random number generated by an authenticator (a device that controls access to network resources, such as an AP) , SNonce Supplicant Nonce (SNonce) is a randomnumber generated by supplicant (a device that wants to access network resources, such as an STA) , AA Authenticator Address (AA) is MAC address of authenticator , SA Supplicant Address (SA) is MAC address of supplicant using Pseudo-Random Function (PRF). PTK consists of four subkeys:
? KCK Key Confirmation Key (KCK) is used for message integrity check
? KEK Key Encryption Key (KEK) is used for encryption key distribution
? TK Temporal Key (TK) is used for data encryption

? MIC Message Integrity Code (MIC) key
The subkey that is specifically used for data encryption is TK Temporal Key (TK). TK is also known as Pairwise Transient Key (PTK). TK changes periodically during communication based on time or number of packets transmitted.
The other options are not part of WPA Key Hierarchy because:
? PMK: PMK is not part of WPA Key Hierarchy, but rather an input for deriving PTK.
? KCK: KCK is part of WPA Key Hierarchy, but it is not used for data encryption, but rather for message integrity check.
? Nonce: Nonce is not part of WPA Key Hierarchy, but rather an input for deriving PTK.
References: https://en.wikipedia.org/wiki/Wi- Fi_Protected_Access#WPA_key_hierarchy_and_management https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf

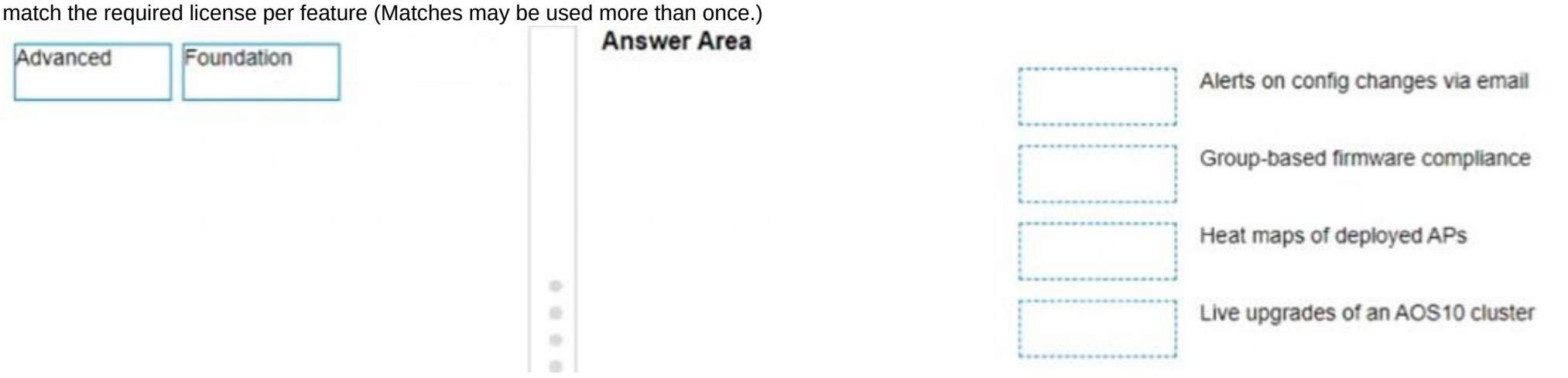
NEW QUESTION 13
What does a slow amber-flashing Stack-LED indicate?

A. One switch has a stacking failure.
B. A port has a stacking failure Stacking mode Is not selected
C. Stacking mode selected
D. Stacking is synchronizing Please wait

Answer: C

Explanation:
A slow amber-flashing Stack-LED indicates that stacking mode is selected on the switch. This means that the switch is ready to join a stack or form a new stack if no other switches are present. References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/1-overview/stacking-leds.htm

NEW QUESTION 17
DRAG DROP
A network administrator with existing IAP-315 access points is interested in Aruba Central and needs to know which license is required for specific features Please match the required license per feature (Matches may be used more than once.)



A. Mastered
B. Not Mastered

Answer: A

Explanation:
a) Alerts on config changes via email - Foundation b) Group-based firmware compliance - Foundation c) Heat maps of deployed APs - Advanced d) Live upgrades of an AOS10 cluster - Advanced
According to the Aruba Central Licensing Guide1, the Foundation License provides basic device management features such as configuration, monitoring, alerts, reports, firmware management, etc. The Advanced License provides additional features such as AI insights, WLAN services, NetConductor Fabric, heat maps, live upgrades, etc. https://www.arubanetworks.com/techdocs/central/2.5.3/content/pdfs/licensing-guide.pdf

NEW QUESTION 18
Which statement about manual switch provisioning with Aruba Central is correct?

A. Manual provisioning does not require DHCP and requires DNS
B. Manual provisioning does not require DHCP and does not require DNS
C. Manual provisioning requires DHCP and does not require DNS
D. Manual provisioning requires DHCP and requires DNS

Answer: B

Explanation:
Manual provisioning is a method to add switches to Aruba Central without using DHCP or DNS. It requires the user to enter the switch serial number, MAC address, and activation code in Aruba Central, and then configure the switch with the same activation code and Aruba Central??s IP address.
References:https://help.central.arubanetworks.com/latest/documentation/online_help/conte nt/devices/switches/provisioning/manual-provisioning.htm

NEW QUESTION 20
A customer has just implemented user and device certificates via a company-wide Group Based Policy (GPO) Which EAP method requires client certificates when authenticating to the network?

A. EAP-TTLS
B. EAP-TLS
C. EAP-TEAP
D. PEAP

Answer: B

Explanation:
EAP-TLS is an authentication method that requires client certificates when authenticating to the network. It provides mutual authentication between the client and the server using public key cryptography and digital certificates. References:https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content/CPPM _UserGuide/EAP-TLS/EAP-TLS.htm

NEW QUESTION 21
When using the OSPF dynamic routing protocol on an Aruba CX switch, what must match on the neighboring devices to exchange routes?

A. Hello timers
B. DR configuration
C. ECMP method
D. BDR configuration

Answer: A

Explanation:
OSPF Open Shortest Path First. OSPF is a link-state routing protocol that uses a hierarchical structure to create a routing topology for IP networks. OSPF routers exchange routing information with their neighbors using Hello packets, which are sent periodically on each interface. To establish an adjacency Adjacency is a relationship formed between selected neighboring routers for the purpose of exchanging routing information., OSPF routers must agree on several parameters, including Hello timers, which specify how often Hello packets are sent on an interface. If the Hello timers do not match between neighboring routers, they will not form an adjacency and will not exchange routes. References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/osfp/osfp.htm

NEW QUESTION 24
DRAG DROP
Match the phase of message processing with the Open Systems interconnection (OSl) layer.

Layer		Phase of Message Processing
Physical Layer		Organizes the data into segments
Network Layer		Organizes the data into packets
Transport Layer		Organizes the data into frames
Data Link Layer		Organizes the data into bits

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The OSI model divides the networking process into seven layers, each representing a different step of the transmission chain. Each layer has its own function and is responsible for well-defined tasks. User data passes sequentially from the highest layer down through the lower layers until the device transmits it externally. The lowest layer, the physical layer, converts the data into bits that can be sent over a physical medium. The second layer, the data link layer, organizes the bits into frames that can be transmitted over a link between two nodes. The third layer, the network layer, organizes the frames into packets that can be routed across a network of nodes. The fourth layer, the transport layer, organizes the packets into segments that can provide reliable and error-free communication between two end points12. References: 1 https://www.linode.com/docs/guides/introduction-to-osi- networking-model/ 2 https://en.wikipedia.org/wiki/OSI_model

NEW QUESTION 27
What is the ideal Aruba access switch for a cost-effective connection to 200-380 clients, printers and APs per distribution rack?

A. Aruba CX 6400
B. Aruba CX 6200
C. Aruba CX 6300
D. Aruba CX 6000

Answer: B

Explanation:
The ideal Aruba access switch for a cost-effective connection to 200-380 clients, printers and APs per distribution rack is the Aruba CX 6200. This switch series is a cloud- manageable, stackable access switch series that is ideal for enterprise branch offices and campus networks, as well as SMBs. The CX 6200 series offers the following benefits:
? Enterprise-class connectivity: The CX 6200 series supports ACLs, robust QoS,
and common protocols such as static and Access OSPF routing.
? Power and speed for users and IoT: The CX 6200 series provides built-in 1/10GbE uplinks and 30W to 60W of Class 4 to Class 6 PoE for powering devices such as APs and cameras.
? Scalable growth made simple: The CX 6200 series supports Aruba Virtual Switching Framework (VSF) that allows you to quickly grow your network to eight members in a single stack using high-performance built-in 10G SFP ports.
? Management flexibility: The CX 6200 series supports a choice of management, including cloud-based and on-prem Central, CLI, switch Web GUI and programmability with AOS-CX operating system, and REST APIs.

The other options are not ideal because:
? Aruba CX 6400: This switch series is a high-availability modular switch series that is ideal for versatile edge access to data center deployments. It offers more performance, scalability, and modularity than the CX 6200 series, but it is also more expensive and complex to deploy and manage. It may not be cost-effective for connecting 200-380 clients per distribution rack.
? Aruba CX 6300: This switch series is a layer 3 stackable access and aggregation switch series that offers Smart Rate and High Power PoE. It offers more features and performance than the CX 6200 series, but it is also more expensive and may not be necessary for connecting 200-380 clients per distribution rack.
? Aruba CX 6000: This switch series is a layer 2 access switch series that offers PoE. It offers less features and performance than the CX 6200 series, and it does not support VSF stacking or routing protocols. It may not be sufficient for connecting 200-380 clients per distribution rack.
References: https://www.arubanetworks.com/products/switches/access/ https://www.arubanetworks.com/products/switches/access/6200-series/ https://www.arubanetworks.com/products/switches/access/6400-series/ https://www.arubanetworks.com/products/switches/access/6300-series/ https://www.arubanetworks.com/products/switches/access/6000-series/

NEW QUESTION 30
What are two advantages of a UXI? (Select two.)

A. A UXI can be used without any internet connection
B. A UXI helps to calculate the best WiFi channels in a remote location
C. A UXI behaves like a client/user
D. A UXI measures the Wi-Fi coverage of all APs in the given location.
E. A UXI can check different applications, such as HTTP VOIP or Office 365.

Answer: CE

Explanation:
A UXI (User Experience Insight) is a device that simulates user behavior and tests network performance from the user perspective. It can check different applications, such as HTTP, VOIP, or Office 365, and measure metrics such as latency, jitter, packet loss, and throughput.
References:https://www.arubanetworks.com/products/networking/user-experience-insight/

NEW QUESTION 32
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.
References:https://www.arubanetworks.com/techdocs/AOS- CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm

NEW QUESTION 33
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?

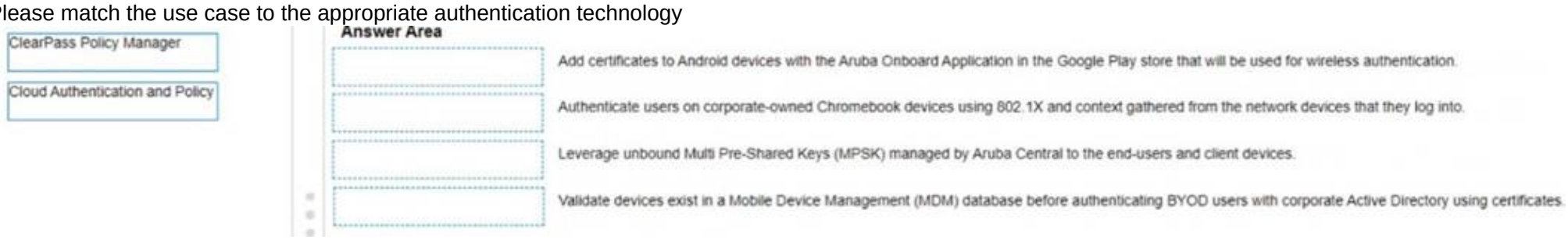
A. Session-specific information (MACs and nonces)
B. Opportunistic Wireless Encryption (OWE)
C. Simultaneous Authentication of Equals (SAE)
D. Key Encryption Key (KEK)

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.
References: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e https://www.wi-fi.org/file/wi- fi-alliance-unlicensed-spectrum-in-the-us https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access- points/wpa3-dep-guide-og.html https://info.support.huawei.com/info-finder/encyclopedia/en/WPA3.html https://rp.os3.nl/2019-2020/p99/presentation.pdf

NEW QUESTION 34
DRAG DROP
Please match the use case to the appropriate authentication technology



A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Add certificates to Android devices with the Aruba Onboard Application in the Google Play store that will be used for wireless authentication A) ClearPass Policy Manager
? Authenticate users on corporate-owned Chromebook devices using 802.1X and context gathered from the network devices that they log into B) Cloud Authentication and Policy
? Leverage unbound Mum Pre-Shared Keys (MPSK) managed by Aruoa Central to the end-users and client devices B) Cloud Authentication and Policy
? Validate devices exist in a Mobile Device Management (MDM) database before authenticating BYOD users with corporate Active Directory using certificates A) ClearPass Policy Manager https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPPM_ UserGuide/About%20ClearPass/About_ClearPass.htm https://www.arubanetworks.com/products/security/network-access-control/

NEW QUESTION 37
When using an Aruba standalone AP you select "Native VLAN" for the Client VLAN Assignment In which subnet will the client IPs reside?

A. The same subnet as the mobility controller
B. The same subnet as the Aruba ESP gateway
C. The same subnet as the mobility conductor
D. The same subnet as the access point

Answer: D

Explanation:
When using an Aruba standalone AP, selecting ??Native VLAN?? for the Client VLAN Assignment means that the clients will get their IP addresses from the same subnet as the access point??s IP address. This is because the access point acts as a DHCP server for the clients in this mode.
References:https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instan t-ug/iap-dhcp/iap-dhcp.htm

NEW QUESTION 41
Where are wireless client roaming decisions made?

A. Client device
B. Virtual Controller
C. Joint decision made by the origination and destination APs
D. Aruba Central

Answer: A

Explanation:
Wireless client roaming decisions are made by the client device based on its own criteria, such as signal strength, noise level, data rate, etc. The network can influence the client??s roaming decision by providing information such as neighbor reports, load
balancing, band steering, etc., but the final decision is up to the client. References:https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instan t-ug/wlan-roaming/client-roaming.htm

NEW QUESTION 46
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.
References: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/ap-led- behavior.htm
https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/troubleshooting/ap-monitor-mode.htm
https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/troubleshooting/ap-spectrum-analysis.htm

NEW QUESTION 51
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. References:https://ieeexplore.ieee.org/document/9288995

NEW QUESTION 55
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 severities1. You can also view the alerts and events in the List view and Summary view2. References: 1
https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/configuring- alerts.htm 2
https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/viewing- alerts.htm

NEW QUESTION 56
After having configured the edge switch uplink as requested your colleague says that they have failed to ping the core You ask your colleague to verify the connection is plugged in and the switch is powered on They confirm that both are correct You attempt to ping the core switch and confirm that the ping is failing. Knowing the nature of this deployment, what commands might you use to troubleshoot this issued

A. Ping 10.11 1 - ping the core to attempt to verify connectivity Show trunk - to verify if the LAG interface was correctly added to the switch Show spanning tree - to check for spanning-tree blocked states Show port-access clients interface all - to view any port- access blocking states or failed authentication attempts on all interfaces Show run interface vlan20 - to double check the layer 3 svi configuration is correct for l_3 connectivity Show lldp neighors - to verify whether you are able to see the Core as an L2 neighbor to verify if the correct links are plugged in to the correct ports
B. diagnostic diag cable-diag 1/1/51 diag cable-diag 1/1/52 - to view diagnostic information for the physical link to get a status on any interruptions to Layer 1 connectivity, show ip route - to verify that the default gateway is present in the routing table show ip ospf - to check whether there is a layer 3 routing protocol enabled show ip dns - to view whether there is a valid dns source
C. Ping 10.1.1.1 - ping the core to attempt to verify connectivity show lacp agg - to verify which link aggregations are currently configured using which physical ports show lacp int - to verify the LACP status and whether any links are blocking in your topology show lldp neighors - to verify whether you are able to see the Core as an L2 neighbor to verify if the correct links are plugged in to the correct ports show run interface 1/1/51.1/1/52-to ensure the physical interfaces are no-shut and members of the lag show run interface lag 1 - to ensure the correct vlan trunking configuration is applied to the logical interface show run int vlan 20 - to ensure you have the L3 SVI no shut and configured in the correct subnet
D. Show run - to view the running configuration of the switch Show run | begin 20 "vlan 20"- to ensure VLAN 20 was correctly added to the database show run | begin 20 'interface vlan 20' - to view the L3 SVI configuration Show run interface 1/1/51.1/1/52 - to ensure the physical interfaces are no shut and were added as

members of LAG 1 Show run int lag 1 - to verify LACP mode active was configured to eliminate LACP blocking states

Answer: C

Explanation:
These commands might help troubleshoot this issue as they check various aspects of the connectivity between the edge switch and the core switch, such as Layer 3 reachability, Layer 2 adjacency, LACP configuration and status, VLAN trunking configuration, and interface status.
References:https://www.arubanetworks.com/techdocs/AOS-CX_10_04/CLI/GUID- 8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html

NEW QUESTION 61
What is a weakness introduced into the WLAN environment when WPA2-Personal is used for security?

A. It uses X 509 certificates generated by a Certification Authority
B. The Pairwise Temporal Key (PTK) is specific to each session
C. The Pairwise Master Key (PMK) is shared by ail users
D. It does not use the WPA 4-Way Handshake

Answer: C

Explanation:
The weakness introduced into WLAN environment when WPA2-Personal is used for security is that PMK Pairwise Master Key (PMK) is a key that is derived from PSK Pre-shared Key (PSK) is a key that is shared between two parties before communication begins , which are both fixed. This means that all users who know PSK can generate PMK without any authentication process. This also means that if PSK or PMK are compromised by an attacker, they can be used to decrypt all traffic encrypted with PTK Pairwise Temporal Key (PTK) is a key that is derived from PMK, ANonce AuthenticatorNonce (ANonce) is a random number generated by an authenticator (a device that controls access to network resources, such as an AP), SNonce Supplicant Nonce (SNonce) is a random number generated by supplicant (a device that wants to access network resources, such as an STA), AA Authenticator Address (AA) is MAC address of authenticator, SA Supplicant Address (SA) is MAC address of supplicant using Pseudo-Random Function (PRF). PTK consists of four subkeys: KCK Key Confirmation Key (KCK) is used for message integrity check, KEK Key Encryption Key (KEK) is used for encryption key distribution, TK Temporal Key (TK) is used for data encryption, MIC Message Integrity Code (MIC) key. .
The other options are not weaknesses because:
? It uses X 509 certificates generated by a Certification Authority: This option is false because WPA2-Personal does not use X 509 certificates or Certification Authority for authentication. X 509 certificates and Certification Authority are used in WPA2- Enterprise mode, which uses 802.1X and EAP Extensible Authentication Protocol (EAP) is an authentication framework that provides support for multiple authentication methods, such as passwords, certificates, tokens, or biometrics. EAP is used in wireless networks and point-to-point connections to provide secure authentication between a supplicant (a device that wants to access the network) and an authentication server (a device that verifies the credentials of the supplicant). for user authentication with a RADIUS server Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service .
? The Pairwise Temporal Key (PTK) is specific to each session: This option is false because PTK being specific to each session is not a weakness but a strength of WPA2-Personal. PTK being specific to each session means that it changes periodically during communication based on time or number of packets transmitted. This prevents replay attacks and increases security of data encryption.
? It does not use the WPA 4-Way Handshake: This option is false because WPA2- Personal does use the WPA 4-Way Handshake for key negotiation. The WPA 4- Way Handshake is a process that allows the station and the access point to exchange ANonce and SNonce and derive PTK from PMK. The WPA 4-Way Handshake also allows the station and the access point to verify each other??s PMK and confirm the installation of PTK.
References: https://en.wikipedia.org/wiki/Wi- Fi_Protected_Access#WPA_key_hierarchy_and_management https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf

NEW QUESTION 65
You are configuring a network with a stacked pair of 6300M switches used for distribution and layer 3 services. You create a new VLAN for users that will be used on multiple access stacks of CX6200 switches connected downstream of the distribution stack You will be creating multiple VLANs/subnets similar to this will be utilized in multiple access stacks
What is the correct way to configure the routable interface for the subnet to be associated with this VLAN?

A. Create a physically routed interface in the subnet on the 6300M stack for each downstream switch.
B. Create an SVl in the subnet on each downstream switch
C. Create an SVI in the subnet on the 6300M stack, and assign the management address of each downstream switch stack to a different IP address in the same subnet
D. Create an SVI in the subnet on the 6300M stack.

Answer: D

Explanation:
The correct way to configure the routable interface for the subnet to be associated with this VLAN is to create an SVI Switched Virtual Interface (SVI) Switched Virtual Interface (SVI) is a virtual interface on a switch that represents a VLAN and provides Layer 3 routing functions for that VLAN . SVIs are used to enable inter-VLAN routing , provide gateway addresses for hosts in VLANs , apply ACLs or QoS policies to VLANs , etc. SVIs have some advantages over physical routed interfaces such as saving interface ports , reducing cable costs , simplifying network design , etc . SVIs are usually numbered according to their VLAN IDs (e.g., vlan 10) and assigned IP addresses within the subnet of their VLANs . SVIs can be created and configured by using commands such as interface vlan , ip address , no shutdown , etc . SVIs can be verified by using commands such as show ip interface brief , show vlan , show ip route , etc . in the subnet on the 6300M stack.
An SVI is a virtual interface on a switch that represents a VLAN and provides Layer 3 routing functions for that VLAN. Creating an SVI in the subnet on the 6300M stack allows the switch to act as a gateway for the users in that VLAN and enable inter-VLAN routing between different subnets. Creating an SVI in the subnet on the 6300M stack also simplifies network design and management by reducing the number of physical interfaces and cables required for routing.
The other options are not correct ways to configure the routable interface for the subnet to be associated with this VLAN because:
? Create a physically routed interface in the subnet on the 6300M stack for each
downstream switch: This option is incorrect because creating a physically routedinterface in the subnet on the 6300M stack for each downstream switch would require using one physical port and cable per downstream switch, which would consume interface resources and increase cable costs. Creating a physically routed interface in the subnet on the 6300M stack for each downstream switch would also complicate network design and management by requiring separate routing configurations and policies for each interface.
? Create an SVI in the subnet on each downstream switch: This option is incorrect
because creating an SVI in the subnet on each downstream switch would not enable inter-VLAN routing between different subnets, as each downstream switch would act as a gateway for its own VLAN only. Creating an SVI in the subnet on each downstream switch would also create duplicate IP addresses in the same subnet, which would cause IP conflicts and routing errors.
? Create an SVI in the subnet on the 6300M stack, and assign the management

address of each downstream switch stack to a different IP address in the same subnet: This option is incorrect because creating an SVI in the subnet on the 6300M stack, and assigning the management address of each downstream switch stack to a different IP address in the same subnet would not enable inter-VLAN routing between different subnets, as each downstream switch would still act as a gateway for its own VLAN only. Creating an SVI in the subnet on the 6300M stack, and assigning the management address of each downstream switch stack to a different IP address in the same subnet would also create unnecessary IP addresses in the same subnet, which would waste IP space and complicate network management.
References: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200- 7295/index.html https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-overview.htm https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-config.htm

NEW QUESTION 69
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

HPE6-A85 Practice Exam Features:

* HPE6-A85 Questions and Answers Updated Frequently

* HPE6-A85 Practice Questions Verified by Expert Senior Certified Staff

* HPE6-A85 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* HPE6-A85 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year