Number: HPE6-A85
Passing Score: 800
Time Limit: 120
File Version: 5.0

**Exam Code: HPE6-A85**

**Exam Name: Aruba Certified Campus Access Associate**

**Exam A**

**QUESTION 1**
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

**Correct Answer: C**
**Section:**
**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 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 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.

**QUESTION 2**
Which statement is correct when comparing 5 GHz and 6 GHz channels with identical channel widths?

A. 5 GHz channels travel the same distances and provide different throughputs to clients compared to 6 GHz channels
B. 5 GHz channels travel different distances and provide different throughputs to clients compared to 6 GHz channels
C. 5 GHz channels travel the same distances and provide the same throughputs to clients compared to 6 GHz channels
D. 5 GHz channels travel different distances and provide the same throughputs to clients compared to 6 GHz channels

**Correct Answer: B**
**Section:**
**Explanation:**
The correct statement when comparing 5 GHz and 6 GHz channels with identical channel widths is that 5 GHz channels travel different distances and provide different throughputs to clients compared to 6 GHz channels. This statement reflects the fact that higher frequency signals tend to have higher attenuation Attenuation is a general term that refers to any reduction in signal strength during transmission over distance

or through an object or medium . Higher attenuation means that higher frequency signals have shorter range and lower throughput than lower frequency signals. Some facts about this statement are:
5 GHz channels have lower frequency than 6 GHz channels, which means they have lower attenuation than 6 GHz channels.
Lower attenuation means that 5 GHz channels can travel longer distances and provide higher throughputs to clients than 6 GHz channels with identical channel widths.
However, the difference in distance and throughput between 5 GHz and 6 GHz channels may not be significant in indoor environments where there are many obstacles and reflections that affect signal propagation.
The advantage of using 6 GHz channels over 5 GHz channels is that they offer more spectrum availability, less interference, and more non-overlapping channels than 5 GHz channels.
The other options are not correct because:
5 GHz channels travel the same distances and provide different throughputs to clients compared to 6 GHz channels: This option is false because 5 GHz channels do not travel the same distances as 6 GHz channels due to higher attenuation of higher frequency signals.
5 GHz channels travel the same distances and provide the same throughputs to clients compared to 6 GHz channels: This option is false because 5 GHz channels do not travel the same distances or provide the same throughputs as 6 GHz channels due to higher attenuation of higher frequency signals.
5 GHz channels travel different distances and provide the same throughputs to clients compared to 6 GHz channels: This option is false because 5 GHz channels do not provide the same throughputs as 6 GHz channels due to higher attenuation of higher frequency signals.

**QUESTION 3**
DRAG DROP
Match the appropriate QoS concept with its definition.

**Select and Place:**

| 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 |



**Correct Answer:**

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

**Section:**
**Explanation:**

**QUESTION 4**
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

**Correct Answer: B**
**Section:**
**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.

**QUESTION 5**
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

**Correct Answer: B**
**Section:**
**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.
Reference: https://help.central.arubanetworks.com/latest/documentation/online_help/content/devices/switches/provisioning/manual-provisioning.htm

**QUESTION 6**
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

**Correct Answer: A**
**Section:**
**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.
Reference: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/wlan-roaming/client-roaming.htm

**QUESTION 7**
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

**Correct Answer: B**
**Section:**
**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.
Reference: https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content/CPPM_UserGuide/EAP-TLS/EAP-TLS.htm

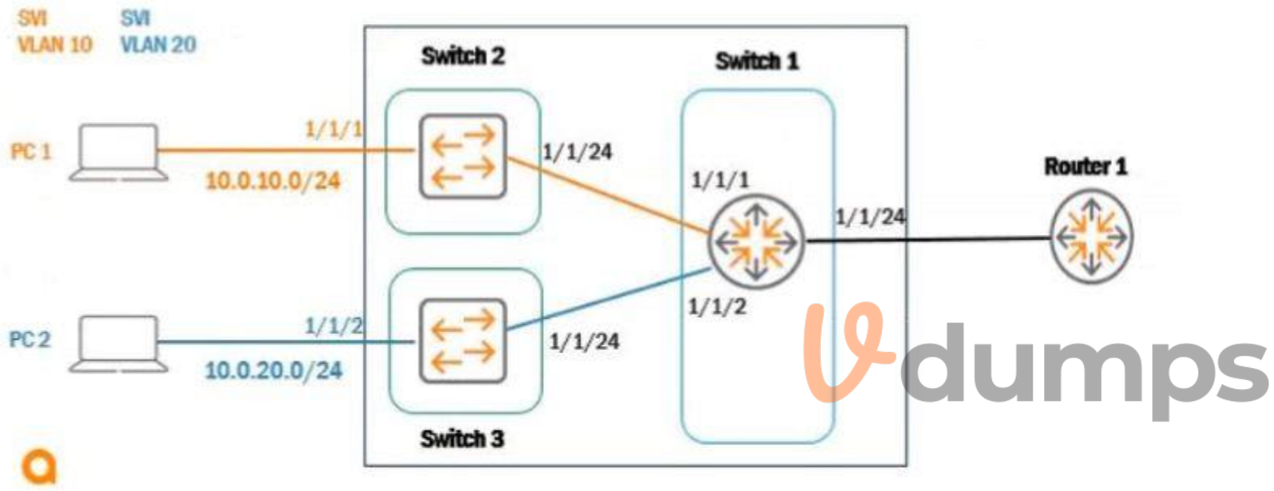
**QUESTION 8**
A network technician is using Aruba Central to troubleshoot network issues Which dashboard can be used to view and acknowledge issues when beginning the troubleshooting process?

A. the Alerts and Events dashboard
B. the Audit Trail dashboard

C. the Reports dashboard
D. the Tools dashboard

**Correct Answer: A**
**Section:**
**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.
Reference:1https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/configuring-alerts.htm2https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/viewing-alerts.htm

**QUESTION 9**
Refer to exihibit




Based on the given topology, what is the requirement on an Aruba switch to enable LLDP messages to be received by Switch 1 port 1/1/24. when Router 1 is enabled with LLDP?

A. LLDP is enabled by default
B. global configuration lldp enable
C. int 1/1/24, lldp receive
D. int 1/1/24, no cdp

**Correct Answer: C**
**Section:**
**Explanation:**
LLDP Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network. is enabled by default on Aruba switches, but it can be disabled on a per-port basis using the no lldp command. To enable LLDP messages to be received by Switch 1 port 1/1/24, you need to enter the interface configuration mode for that port and use the lldp receive command.
Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/lldp/lldp.htm

**QUESTION 10**
You are in a meeting with a customer where you are asked to explain the network redundancy feature Multiple Spanning Tree (MSTP). What is the correct statement for this feature?

A. MSTP configuration ID revision by default as current MSTP root priority
B. MSTP configuration ID name by default using switch IMC address
C. MSTP configuration ID name by default using switch serial number
D. MSTP configuration ID revision by default as switch serial number

**Correct Answer: B**
**Section:**
**Explanation:**
MSTP Multiple Spanning Tree Protocol. MSTP is an IEEE standard protocol for preventing loops in a network with multiple VLANs. MSTP allows multiple VLANs to be mapped to a reduced number of spanning-tree instances. configuration ID consists of two parameters: name and revision. The name is a 32-byte ASCII string that identifies the MSTP region, which is a group of switches that share the same configuration ID and VLAN-to-instance mapping. The revision is a 16-bit number that indicates the version of the configuration ID. By default, the MSTP configuration ID name is set to the switch IMC address, which is a unique identifier derived from the MAC address Media Access Control address. MAC address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. of the switch.
Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/mstp/mstp.htm

**QUESTION 11**
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

**Correct Answer: A**
**Section:**
**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.
Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/osfp/osfp.htm

**QUESTION 12**
DRAG DROP
Match the phase of message processing with the Open Systems interconnection (OSl) layer.

**Select and Place:**

| 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 |

**Correct Answer:**

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



**Section:**
**Explanation:**

**QUESTION 13**
What happens when the signal from an AP weakens by being absorbed as it moves through an object?

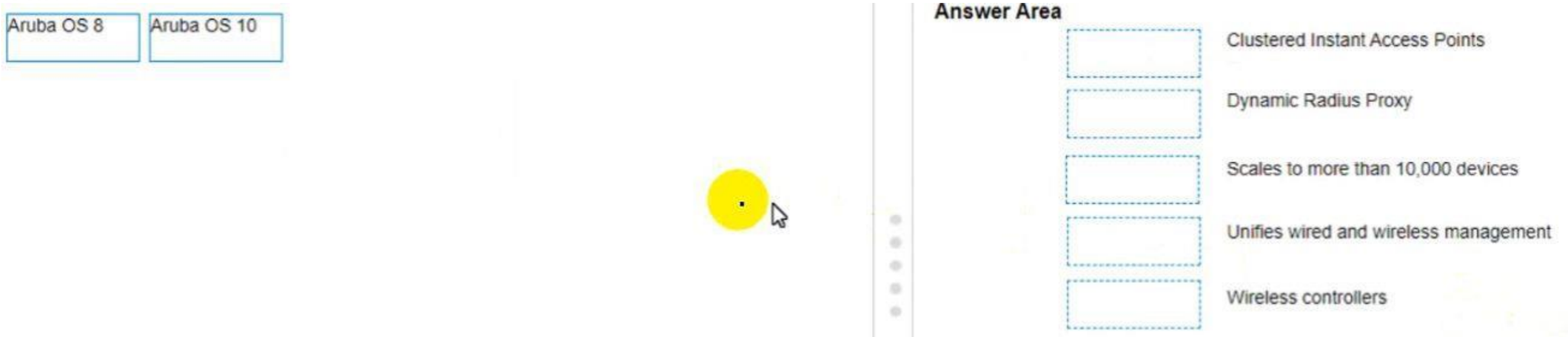
A. APs will use bonded channels to decrease latency to clients
B. Signal to Noise Ratio (SNR) increases
C. Signal to Noise Ratio (SNR) decreases
D. Aruba Central dynamically moves clients to neighboring APs

**Correct Answer: C**
**Section:**
**Explanation:**
Signal to noise ratio (SNR) is a measure that compares the level of a desired signal to the level of background noise. SNR is defined as the ratio of signal power to the noise power, often expressed in decibels (dB).A high SNR means that the signal is clear and easy to detect or interpret, while a low SNR means that the signal is corrupted or obscured by noise and may be difficult to distinguish or recover1. When the signal from an AP Access Point. AP is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. weakens by being absorbed as it moves through an object, such as a wall or a furniture, the signal power decreases. This reduces the SNR and affects the quality of the wireless connection.The noise power may also increase due to interference from other sources, such as other APs or devices operating in the same frequency band2.Therefore, the correct answer is that SNR decreases when the signal from an AP weakens by being absorbed as it moves through an object.

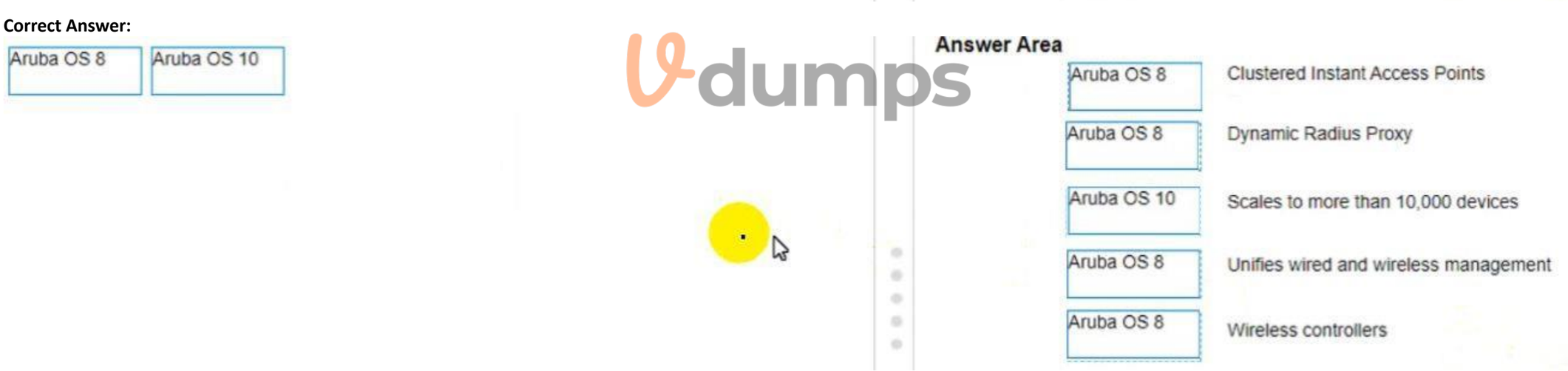
Reference:1https://en.wikipedia.org/wiki/Signal-to-noise_ratio2https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_%28SNR%29_and_Wireless_Signal_Strength

**QUESTION 14**
DRAG DROP
Match the feature to the Aruba OS version (Matches may be used more than once.)

**Select and Place:**




**Correct Answer:**



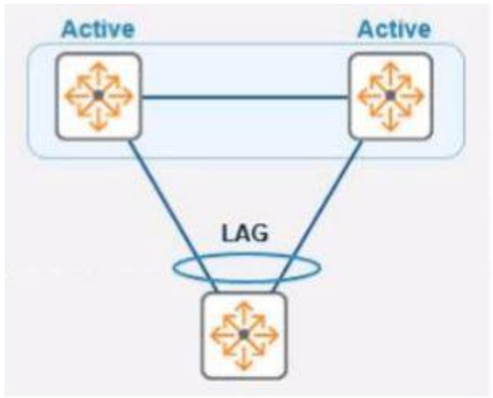

**Section:**
**Explanation:**

**QUESTION 15**
Which Aruba technology will allow for device-specific passphrases to securely add headless devices to the WLAN?

A. Wired Equivalent Privacy (WEP)
B. Multiple Pre-Shared Key (MPSK)
C. Opportunistic Wireless Encryption (OWE)
D. Temporal Key Integrity Protocol (TKIP)

**Correct Answer: B**
**Section:**
**Explanation:**
Multiple Pre-Shared Key (MPSK) is a feature that allows device-specific or group-specific passphrases to securely add headless devices to the WLAN Wireless Local Area Network. WLAN is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building. . MPSK enhances the WPA2 PSK Wi-Fi Protected Access 2 Pre-Shared Key. WPA2 PSK is a method of securing your network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users without an enterprise authentication server. mode by allowing different PSKs for different devices on the same SSID Service Set Identifier. SSID is a case-sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a wireless local-area network (WLAN). The SSID acts as a password when a mobile device tries to connect to the basic service set (BSS) --- a component of the IEEE 802.11 WLAN architecture. .MPSK passwords can be generated or user-created and are managed by ClearPass Policy Manager12.
Reference:1https://blogs.arubanetworks.com/solutions/simplify-iot-authentication-with-multiple-pre-shared-keys/2https://www.arubanetworks.com/techdocs/ClearPass/6.8/Guest/Content/AdministrationTasks1/Configuring-MPSK.htm

**QUESTION 16**
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

**Correct Answer: A**
**Section:**
**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.
Reference:3https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-overview.htm4https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-ip-addressing.htm5https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-failover.htm

**QUESTION 17**
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

**Correct Answer: C**
**Section:**
**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 RF neighborhood 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.
Reference: https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdf https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/arm/AirMatch.htm

**QUESTION 18**
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

**Correct Answer: B**
**Section:**
**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.
Reference: https://en.wikipedia.org/wiki/Static_routing https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/show-ip-route.htm

**QUESTION 19**
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

**Correct Answer: B, C**
**Section:**
**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 groups depending 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.

**QUESTION 20**
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

**Correct Answer: A**
**Section:**
**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.
Reference: https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm

**QUESTION 21**
You need to configure wireless access for several classes of loT devices, some of which operate only with 802 11b. Each class must have a unique PSK and will require a different security policy applied as a role
There will be 15-20 different classes of devices and performance should be optimized
Which option fulfills these requirements''

A. Single SSID with MPSK for each loT class using 5 GHz and 6 GHz bands
B. Single SSID with MPSK for each loT class using 2.4GHz and 5 GHz bands
C. Individual SSIDs with unique PSK for each loT class, using 5GHz and 6 GHz bands
D. Individual SSIDs with unique PSK for each loT class, using 2.4GHZ and 5GHz band

**Correct Answer: D**
**Section:**
**Explanation:**
The option that fulfills the requirements is to create individual SSIDs with unique PSK for each loT class, using 2.4 GHz and 5 GHz band. This option provides the following benefits:
Each loT class has a unique PSK that can be used to apply a different security policy as a role. This enhances the security and flexibility of the WLAN network.
Individual SSIDs allow for better isolation and management of different loT classes. This improves the performance and scalability of the WLAN network.
Using both 2.4 GHz and 5 GHz bands allows for backward compatibility with loT devices that operate only with 802.11b, which uses the 2.4 GHz band1.It also allows for higher throughput and less interference for loT devices that support 802.11a, 802.11g, 802.11n, or 802.11ac, which use the 5 GHz band2.
The other options do not fulfill the requirements because:
Single SSID with MPSK for each loT class using 5 GHz and 6 GHz bands: This option does not support loT devices that operate only with 802.11b, which uses the 2.4 GHz band1. It also does not optimize the performance of the WLAN network, as a single SSID may cause co-channel interference and congestion among different loT classes.
Single SSID with MPSK for each loT class using 2.4 GHz and 5 GHz bands: This option does not optimize the performance of the WLAN network, as a single SSID may cause co-channel interference and congestion among different loT classes.
Individual SSIDs with unique PSK for each loT class, using 5 GHz and 6 GHz bands: This option does not support loT devices that operate only with 802.11b, which uses the 2.4 GHz band1.

**QUESTION 22**
The noise floor measures 000000001 milliwatts, and the receiver's signal strength is -65dBm. What is the Signal to Noise Ratio?

A. 35 dBm
B. 15 dBm
C. 45 dBm
D. 25 dBm

**Correct Answer: D**
**Section:**
**Explanation:**
The signal to noise ratio (SNR) is a measure that compares the level of a desired signal to the level of background noise. SNR is defined as the ratio of signal power to the noise power, often expressed in decibels (dB).A high SNR means that the signal is clear and easy to detect or interpret, while a low SNR means that the signal is corrupted or obscured by noise and may be difficult to distinguish or recover3. To calculate the SNR in dB, we can use the following formula:
SNR (dB) = Signal power (dBm) - Noise power (dBm)
In this question, we are given that the noise floor measures -90 dBm (0.000000001 milliwatts) and the receiver's signal strength is -65 dBm (0.000316 milliwatts). Therefore, we can plug these values into the formula and get:
SNR (dB) = -65 dBm - (-90 dBm) SNR (dB) = -65 dBm + 90 dBm SNR (dB) = 25 dBm
Therefore, the correct answer is that the SNR is 25 dBm.

**QUESTION 23**
DRAG DROP
Match the switching technology with the appropriate use case.

**Select and Place:**

| TECHNOLOGY | | USE CASE |
|---|---|---|
| 802.1Q | | Controls the dynamic addition and removal of ports to groups |
| 802.1X | | Tags Ethernet frames with an additional VLAN header |
| LACP | | Used to authenticate EAP-capable clients on a switch port |
| LLDP | | Used to identify a voice VLAN to an IP phone |

**Correct Answer:**

| TECHNOLOGY | | USE CASE |
|---|---|---|
| LACP | | Controls the dynamic addition and removal of ports to groups |
| 802.1Q | | Tags Ethernet frames with an additional VLAN header |
| 802.1X | | Used to authenticate EAP-capable clients on a switch port |
| LLDP | | Used to identify a voice VLAN to an IP phone |

**Section:**
**Explanation:**

**QUESTION 24**
Which commands are used to set a default route to 10.4.5.1 on an Aruba CX switch when In-band management using an SVI is being used?

A. iP default-gateway 10.4.5.1
B. ip route 0 0 0.070 10.4 5.1 vrf mgmt
C. ip route 0.0 0 0/0 10.4.5.1
D. default-gateway 10.4.5.1

**Correct Answer: C**
**Section:**
**Explanation:**
The command that is used to set a default route to 10.4.5.1 on an Aruba CX switch when in-band management using an SVI is being used is ip route 0.0 0 0/0 10.4.5.1 . This command specifies the destination network address (0.0 0 0) and prefix length (/0) and the next-hop address (10.4.5.1) for reaching any network that is not directly connected to the switch. The default route applies to the default VRF Virtual Routing and Forwarding. VRF is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. VRFs are typically used to segment network traffic for security, privacy, or administrative purposes. , which is used for in-band management traffic that goes through an SVI Switch Virtual Interface. SVI is a virtual interface on a switch that allows the switch to route packets between different VLANs on the same switch or different switches that are connected by a trunk link.An SVI is associated with a VLAN and has an IP address and subnet mask assigned to it12.
Reference:1https://www.arubanetworks.com/techdocs/AOS-CX/10_08/HTML/ip_route_4100i-6000-6100-6200/Content/Chp_StatRoute/def-rou.htm2https://www.arubanetworks.com/techdocs/AOS-CX/10_08/HTML/ip_route_4100i-6000-6100-6200/Content/Chp_VRF/vrf-overview.htm

**QUESTION 25**
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

**Correct Answer: D**
**Section:**

**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 26**
What are the main characteristics of the 6 GHz band?

A. Less RF signal is absorb by objects in a 6 GHz WLAN.
B. In North America, the 6 GHz band offers more 80 MHz channels than there are 40 MHz channels in the 5 GHz band.
C. The 6 GHz band is fully backward compatible with the existing bands.
D. Low Power Devices are allowed for indoor and outdoor usage.

**Correct Answer: B**
**Section:**
**Explanation:**
The main characteristic of the 6 GHz band that is true among the given options is that in North America, the 6 GHz band offers more 80 MHz channels than there are 40 MHz channels in the 5 GHz band. This characteristic provides more spectrum availability, less interference, and higher throughput for wireless devices that support Wi-Fi 6E Wi-Fi Enhanced (Wi-Fi 6E) is an extension of Wi-Fi 6 (802.11ax) standard that operates in the newly available unlicensed frequency spectrum around 6 GHz in addition to existing bands below it. Some facts about this characteristic are:
In North America, there are up to seven non-overlapping channels available in each of three channel widths (20 MHz, 40 MHz, and 80 MHz) in the entire unlicensed portion of the new spectrum (5925--7125 MHz). This means there are up to 21 non-overlapping channels available for Wi-Fi devices in total.
In comparison, in North America, there are only nine non-overlapping channels available in each of two channel widths (20 MHz and 40 MHz) in the entire unlicensed portion of the existing spectrum below it (2400--2483 MHz and 5150--5825 MHz). This means there are only up to nine non-overlapping channels available for Wi-Fi devices in total.
Therefore, in North America, there are more than twice as many non-overlapping channels available in each channel width in the new spectrum than in the existing spectrum below it.
Specifically, there are more than twice as many non-overlapping channels available at 80 MHz width (seven) than at 40 MHz width (three) in the existing spectrum below it.
The other options are not true because:
Less RF signal is absorbed by objects in a 6 GHz WLAN: This option is false because higher frequency signals tend to be more absorbed by objects than lower frequency signals due to higher attenuation Attenuation is a general term that refers to any reduction in signal strength during transmission over distance or through an object or medium . Therefore, RF signals in a 6 GHz WLAN would be more absorbed by objects than RF signals in a lower frequency WLAN.
The 6 GHz band is fully backward compatible with existing bands: This option is false because Wi-Fi devices need to support Wi-Fi 6E standard to operate in the new spectrum around 6 GHz . Existing Wi-Fi devices that do not support Wi-Fi 6E standard cannot use this spectrum and can only operate in existing bands below it.
Low Power Devices are allowed for indoor and outdoor usage: This option is false because Low Power Indoor Devices (LPI) are only allowed for indoor usage under certain power limits and registration requirements . Outdoor usage of LPI devices is prohibited by regulatory authorities such as FCC Federal Communications Commission (FCC) is an independent agency of United States government that regulates communications by radio, television, wire, satellite, and cable across United States . However, outdoor usage of Very Low Power Devices (VLP) may be allowed under certain power limits and without registration requirements.

**QUESTION 27**

A hospital uses a lot of mobile equipment for the diagnosis and documentation of patient data What Is the ideal access switch for this large hospital with distribution racks of over 400 ports in a single VSF stack?

A. CX 6300
B. OCX 6400
C. OCX 6200
D. OCX 6100

**Correct Answer: A**
**Section:**
**Explanation:**
The ideal access switch for a large hospital with distribution racks of over 400 ports in a single VSF stack is the CX 6300. This switch provides the following benefits:
The CX 6300 supports up to 48 ports per switch and up to 10 switches per VSF stack, allowing for a total of 480 ports in a single stack. This meets the requirement of having over 400 ports in a single VSF stack.
The CX 6300 supports high-performance switching with up to 960 Gbps of switching capacity and up to 714 Mpps of forwarding rate. This meets the requirement of having high throughput and low latency for mobile equipment and patient data.
The CX 6300 supports advanced features such as dynamic segmentation, policy-based routing, and role-based access control. These features enhance the security and flexibility of the network by applying different policies and roles to different types of devices and users.
The CX 6300 supports Aruba NetEdit, a network configuration and orchestration tool that simplifies the management and automation of the network. This reduces the complexity and human errors involved in network configuration and maintenance.
The other options are not ideal because:
OCX 6400: This switch is designed for data center applications and does not support VSF stacking. It also does not support dynamic segmentation or policy-based routing, which are useful for network security and flexibility.
OCX 6200: This switch is designed for small to medium-sized businesses and does not support VSF stacking. It also has lower switching capacity and forwarding rate than the CX 6300, which may affect the performance of the network.
OCX 6100: This switch is designed for edge applications and does not support VSF stacking. It also has lower switching capacity and forwarding rate than the CX 6300, which may affect the performance of the network.



**QUESTION 28**
A network technician has successfully connected to the employee SSID via 802 1X Which RADIUS message should you look for to ensure a successful connection?

A. Authorized
B. Access-Accept
C. Success
D. Authenticated

**Correct Answer: B**
**Section:**
**Explanation:**
The RADIUS message that you should look for to ensure a successful connection via 802.1X is Access-Accept. This message indicates that the RADIUS server has authenticated and authorized the supplicant (the device that wants to access the network) and has granted it access to the network resources. The Access-Accept message may also contain additional attributes such as VLAN ID, session timeout, or filter ID that specify how the authenticator (the device that controls access to the network, such as a switch) should treat the supplicant's traffic.
The other options are not RADIUS messages because:
Authorized: This is not a RADIUS message, but a state that indicates that a port on an authenticator is allowed to pass traffic from a supplicant after successful authentication and authorization.
Success: This is not a RADIUS message, but a status that indicates that an 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). exchange has completed successfully between a supplicant and an authentication server.
Authenticated: This is not a RADIUS message, but a state that indicates that a port on an authenticator has received an EAP-Success message from an authentication server after successful authentication of a supplicant.

**QUESTION 29**
You need to drop excessive broadcast traffic on ingress to an ArubaOS-CX switch What is the best technology to use for this task?

A. Rate limiting
B. DWRR queuing
C. QoS shaping
D. Strict queuing

**Correct Answer: A**
**Section:**
**Explanation:**
The best technology to use for dropping excessive broadcast traffic on ingress to an ArubaOS-CX switch is rate limiting. Rate limiting is a feature that allows network administrators to control the amount of traffic that enters or leaves a port or a VLAN on a switch by setting bandwidth thresholds or limits. Rate limiting can be used to prevent network congestion, improve network performance, enforce service level agreements (SLAs), or mitigate denial-of-service (DoS) attacks. Rate limiting can be applied to broadcast traffic on ingress to an ArubaOS-CX switch by using the storm-control command in interface configuration mode. This command allows network administrators to specify the percentage of bandwidth or packets per second that can be used by broadcast traffic on an ingress port. If the broadcast traffic exceeds the specified threshold, the switch will drop the excess packets.
The other options are not technologies for dropping excessive broadcast traffic on ingress because:
DWRR queuing: DWRR stands for Deficit Weighted Round Robin, which is a queuing algorithm that assigns different weights or priorities to different traffic classes or queues on an egress port. DWRR ensures that each queue gets its fair share of bandwidth based on its weight while avoiding starvation of lower priority queues. DWRR does not drop excessive broadcast traffic on ingress, but rather schedules outgoing traffic on egress.
QoS shaping: QoS stands for Quality of Service, which 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 shaping is a technique that delays or buffers outgoing traffic on an egress port to match the available bandwidth or rate limit. QoS shaping does not drop excessive broadcast traffic on ingress, but rather smooths outgoing traffic on egress.
Strict queuing: Strict queuing is another queuing algorithm that assigns different priorities to different traffic classes or queues on an egress port. Strict queuing ensures that higher priority queues are always served before lower priority queues regardless of their bandwidth requirements or weights. Strict queuing does not drop excessive broadcast traffic on ingress, but rather schedules outgoing traffic on egress.

**QUESTION 30**
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)

**Correct Answer: A**
**Section:**
**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 31**
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

**Correct Answer: C**
**Section:**
**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.

**QUESTION 32**
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

**Correct Answer: D**
**Section:**

**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.

**QUESTION 33**
Review the configuration below.

```
Core-1(config)# interface loopback 0
Core-1(config-if)# ip address 10.1.200.1/32
Core-1(config)# router ospf 1
Core-1(config-ospf-1)# router-id 10.1.200.1
Core-1(config-ospf-1)# area 0
Core-1(config-ospf-1)# exit
```

Why would you configure OSPF to use the IP address 10.1.200.1 as the router ID?

A. The IP address associated with the loopback interface is non-routable and prevents loops
B. The loopback interface state is dependent on the management interface state and reduces routing updates.
C. The IP address associated with the loopback interface is routable and prevents loops
D. The loopback interface state Is independent of any physical interface and reduces routing updates.

**Correct Answer: D**
**Section:**
**Explanation:**
The reason why you would configure OSPF Open Shortest Path First (OSPF) is a link-state routing protocol that dynamically calculates the best routes for data transmission within an IP network. OSPF uses a hierarchical structure that divides a network into areas and assigns each router an identifier called router ID (RID). OSPF uses hello packets to discover neighbors and exchange routing information. OSPF uses Dijkstra's algorithm to compute the shortest path tree (SPT) based on link costs and build a routing table based on SPT. OSPF supports multiple equal-cost paths, load balancing, authentication, and various network types such as broadcast, point-to-point, point-to-multipoint, non-broadcast multi-access (NBMA), etc. OSPF is defined in RFC 2328 for IPv4 and RFC 5340 for IPv6. to use the IP address IP address Internet Protocol (IP) address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing. There are two versions of IP addresses: IPv4 and IPv6. IPv4 addresses are 32 bits long and written in dotted-decimal notation, such as 192.168.1.1. IPv6 addresses are 128 bits long and written in hexadecimal notation, such as 2001:db8::1. IP addresses can be either static (fixed) or dynamic (assigned by a DHCP server). 10.1.200.1 as the router ID Router ID (RID) Router ID (RID) is a unique identifier assigned to each router in a routing domain or protocol. RIDs are used by routing protocols such as OSPF, IS-IS, EIGRP, BGP, etc., to identify neighbors, exchange routing information, elect designated routers (DRs), etc. RIDs are usually derived from one of the IP addresses configured on the router's interfaces or loopbacks, or manually specified by network administrators. RIDs must be unique within a routing domain or protocol instance. is that the loopback interface state Loopback interface Loopback interface is a virtual interface on a router that does not correspond to any physical port or connection. Loopback interfaces are used for various purposes such as testing network connectivity, providing stable router IDs for routing protocols, providing management access to routers, etc. Loopback interfaces have some advantages over physical interfaces such as being always up unless administratively shut down, being independent of any hardware failures or link failures, being able to assign any IP address regardless of

subnetting constraints, etc. Loopback interfaces are usually numbered from zero (e.g., loopback0) upwards on routers. Loopback interfaces can also be created on PCs or servers for testing or configuration purposes using special IP addresses reserved for loopback testing (e.g., 127.x.x.x for IPv4 or ::1 for IPv6). Loopback interfaces are also known as virtual interfaces or dummy interfaces . Loopback interface state Loopback interface state refers to whether a loopback interface is up or down on a router . A loopback interface state can be either administratively controlled (by using commands such as no shutdown or shutdown ) or automatically determined by routing protocols (by using commands such as passive-interface or ip ospf network point-to-point ). A loopback interface state affects how routing protocols use the IP address assigned to the loopback interface for neighbor discovery , router ID selection , route advertisement , etc . A loopback interface state can also affect how other devices can access or ping the loopback interface . A loopback interface state can be checked by using commands such as show ip interface brief or show ip ospf neighbor . is independent of any physical interface and reduces routing updates.
The loopback interface state is independent of any physical interface because it does not depend on any hardware or link status. This means that the loopback interface state will always be up unless it is manually shut down by an administrator. This also means that the loopback interface state will not change due to any physical failures or link failures that may affect other interfaces on the router.
The loopback interface state reduces routing updates because it provides a stable router ID for OSPF that does not change due to any physical failures or link failures that may affect other interfaces on the router. This means that OSPF will not have to re-elect DRs Designated Routers (DRs) Designated Routers (DRs) are routers that are elected by OSPF routers in a broadcast or non-broadcast multi-access (NBMA) network to act as leaders and coordinators of OSPF operations in that network. DRs are responsible for generating link-state advertisements (LSAs) for the entire network segment, maintaining adjacencies with all other routers in the segment, and exchanging routing information with other DRs in different segments through backup designated routers (BDRs). DRs are elected based on their router priority values and router IDs . The highest priority router becomes the DR and the second highest priority router becomes the BDR . If there is a tie in priority values , then the highest router ID wins . DRs can be manually configured by setting the router priority value to 0 (which means ineligible) or 255 (which means always eligible) on specific interfaces . DRs can also be influenced by using commands such as ip ospf priority , ip ospf dr-delay , ip ospf network point-to-multipoint , etc . DRs can be verified by using commands such as show ip ospf neighbor , show ip ospf interface , show ip ospf database , etc . , recalculate SPT Shortest Path Tree (SPT) Shortest Path Tree (SPT) is a data structure that represents the shortest paths from a source node to all other nodes in a graph or network . SPT is used by link-state routing protocols such as OSPF and IS-IS to compute optimal routes based on link costs . SPT is built using Dijkstra's algorithm , which starts from the source node and iteratively adds nodes with the lowest cost paths to the tree until all nodes are included . SPT can be represented by a set of pointers from each node to its parent node in the tree , or by a set of next-hop addresses from each node to its destination node in the network . SPT can be updated by adding or removing nodes or links , or by changing link costs . SPT can be verified by using commands such as show ip route , show ip ospf database , show clns route , show clns database , etc . , or send LSAs Link-State Advertisements (LSAs) Link-State Advertisements (LSAs) are packets that contain information about the state and cost of links in a network segment . LSAs are generated and flooded by link-state routing protocols such as OSPF and IS-IS to exchange routing information with other routers in the same area or level . LSAs are used to build link-state databases (LSDBs) on each router , which store the complete topology of the network segment . LSAs are also used to compute shortest path trees (SPTs) on each router , which determine the optimal routes to all destinations in the network . LSAs have different types depending on their origin and scope , such as router LSAs , network LSAs , summary LSAs , external LSAs , etc . LSAs have different formats depending on their type and protocol version , but they usually contain fields such as LSA header , LSA type , LSA length , LSA age , LSA sequence number , LSA checksum , LSA body , etc . LSAs can be verified by using commands such as show ip ospf database , show clns database , debug ip ospf hello , debug clns hello , etc . due to changes in router IDs.
The other options are not reasons because:
The IP address associated with the loopback interface is non-routable and prevents loops: This option is false because the IP address associated with the loopback interface is routable and does not prevent loops. The IP address associated with the loopback interface can be any valid IP address that belongs to an existing subnet or a new subnet created specifically for loopbacks. The IP address associated with the loopback interface does not prevent loops because loops are caused by misconfigurations or failures in routing protocols or devices, not by IP addresses.
The loopback interface state is dependent on the management interface state and reduces routing updates: This option is false because the loopback interface state is independent of any physical interface state, including the management interface state Management interface Management interface is an interface on a device that provides access to management functions such as configuration, monitoring, troubleshooting, etc . Management interfaces can be physical ports such as console ports, Ethernet ports, USB ports, etc., or virtual ports such as Telnet sessions, SSH sessions, web sessions, etc . Management interfaces can use different protocols such as CLI Command-Line Interface (CLI) Command-Line Interface (CLI) is an interactive text-based user interface that allows users to communicate with devices using commands typed on a keyboard . CLI is one of the methods for accessing management functions on devices such as routers, switches, firewalls, servers, etc . CLI can use different protocols such as console port serial communication protocol Serial communication protocol Serial communication protocol is a method of transmitting data between devices using serial ports and cables . Serial communication protocol uses binary signals that represent bits (0s and 1s) and sends them one after another over a single wire . Serial communication protocol has advantages such as simplicity, low cost, long

**QUESTION 34**
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

**Correct Answer: B**
**Section:**
**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

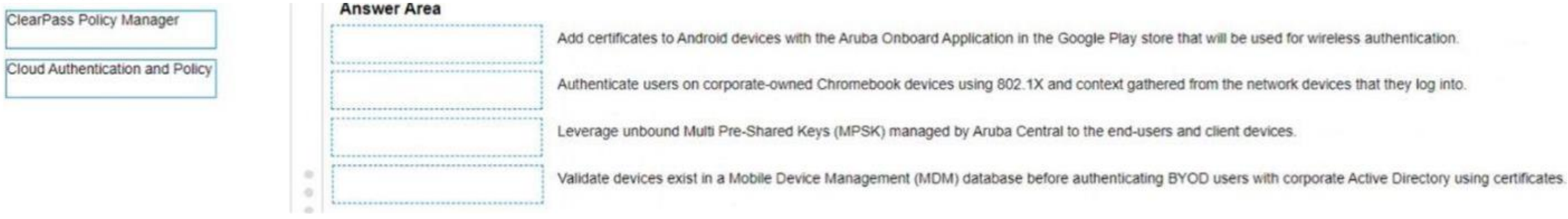
**QUESTION 35**
Describe the purpose of the administrative distance

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

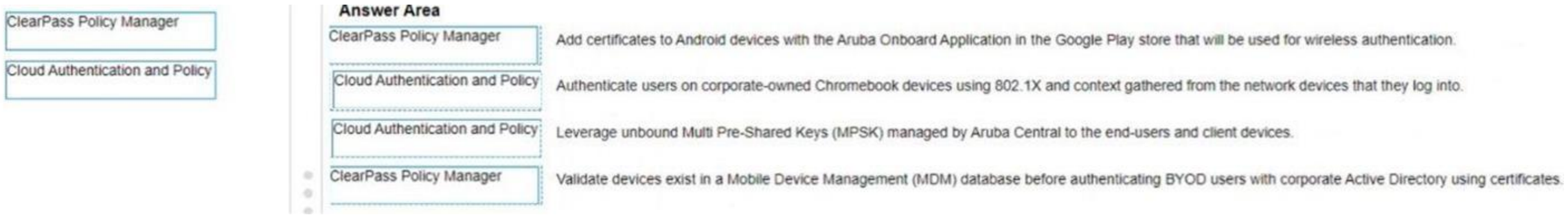
**Correct Answer: B**
**Section:**

**QUESTION 36**
DRAG DROP
Please match the use case to the appropriate authentication technology

**Select and Place:**




**Correct Answer:**




**Section:**
**Explanation:**

**QUESTION 37**
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 SVl 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 SVl in the subnet on the 6300M stack.

**Correct Answer: D**
**Section:**
**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 routed interface 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 SVl 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 SVl 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.

**QUESTION 38**
You have been asked to onboard a new Aruba 6300M in a customer deployment You are working remotely rather than on-site You have a colleague installing the switch The colleague has provided you with a remote console session to configure the edge switch You have been asked to configure a link aggregation going back to the cores using interfaces 1/1/51 and 1/1/52 The Senior Engineer of the project has asked

you to configure the switch and 1Q uplink with these guidelines
1. Add VLAN 20 to the local VLAN database with name Mgmt
2. Add L3 SVl on VLAN 20 for Management using address 10 in the 10.1.1 0/24 subnet 3. Add LAG 1 using LACP mode active for the uplink
4 use vlan 20 as the native vlan on the LAG 5. Make sure the interfaces are all ON.
Which configuration script will achieve the task?

A. Edge1# conf t vlan 20 name Mgmt interface vlan 20 ip address 10.1.1.10/24 no shut interface lag 1 shut vlan access 20 lacp mode active Int 1/1/51.1/1/52 shut no routing lag 1 interface lag 1 no shut
B. Edgel# conf t vlan 20 name Mgmt interface vlan 20 ip address 10 1.1 10/24 no shut interface 1/1/51.1/1/52 shut vlan trunk native 20 vlan trunk allowed all lag 1 lacp mode active interface 1/1/51.1/1/52 no shut
C. Edgel# conf t vlan 20 name Mgmt interface vlan 20 ip address 10 1 1 10/24 no shut interface lag 1 shut vlan trunk native 20 vlan trunk allowed all lacp mode active Int 1/1/51.1/1/52 shut no routing lag 1 interface lag 1 no shut interface 1/1/51.1/1/52 no shut
D. conf t vlan 20 name Mgmt ip address 10 1 1.10/24 no shut interface lag 1 shut vlan trunk native 1 vlan trunk allowed all lacp mode active int 1/1/51.1/1/52 shut no routing interface lag 1 no shut interface 1/1/51.1/1/52 no shut

**Correct Answer: C**
**Section:**
**Explanation:**
This configuration script will achieve the task as it follows the guidelines given by the Senior Engineer. It creates VLAN 20 with name Mgmt, adds L3 SVI on VLAN 20 with IP address 10.1.1.10/24, creates LAG 1 with LACP mode active for the uplink, uses VLAN 20 as the native VLAN on the LAG, and ensures that the interfaces are all ON.
Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790/GUID-8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html

**QUESTION 39**
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

**Correct Answer: C**
**Section:**
**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.
Reference: https://www.arubanetworks.com/techdocs/AOS-CX_10_04/CLI/GUID-8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html