ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Which feature supported by SNMPv3 provides an advantage over SNMPv2c?

A. Transport mapping
B. Community strings
C. GetBulk
D. Encryption

Answer: D

Explanation:

Encryption is a feature supported by SNMPv3 that provides an advantage over SNMPv2c. Encryption protects the confidentiality and integrity of SNMP messages by encrypting them with a secret key. SNMPv2c does not support encryption and relies on community strings for authentication and authorization, which are transmitted in clear text and can be easily intercepted or spoofed. Transport mapping, community strings, and GetBulk are features that are common to both SNMPv2c and SNMPv3. Reference:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmp.htm
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmpv3.htm

Question: 2

You are doing tests in your lab and with the following equipment specifications

- AP1 has a radio that generates a 10 dBm signal
- AP2 has a radio that generates a 11 dBm signal
- AP1 has an antenna with a gain of 9 dBi
- AP2 has an antenna with a gain of 12 dBi.
- The antenna cable for AP1 has a 2 dB loss
- The antenna cable for AP2 has a 3 dB loss

What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for APT?

A. 26 dBm
B. 30 dBm
C. 17 dBm
D. -12 dBm

Answer: C

Explanation:

The calculated Equivalent Isotropic Radiated Power (EIRP) for AP1 is 17 dBm.
EIRP is the measured radiated power of an antenna in a specific direction. It is equal to the input power to the antenna multiplied by the gain of the antenna. It can also take into account the losses in transmission line, connectors, and other components. The formula for EIRP is:
EIRP = P + G - L

where P is the output power of the radio, G is the gain of the antenna, and L is the loss of the cable and connectors.

For AP1, we have:

P = 10 dBm G = 9 dBi L = 2 dB

Therefore,

EIRP = 10 + 9 - 2 EIRP = 17 dBm

Question: 3

With Aruba CX 6300. how do you configure ip address 10 10 10 1 for the interface in default state for interface 1/1/1?

A. int 1/1/1. switching, ip address 10 10 10 1/24
B. int 1/1/1. no switching, ip address 10 10 10.1/24
C. int 1/1/1. ip address 10.10.10.1/24
D. int 1/1/1. routing, ip address 10.10.10 1/24

Answer: B

Explanation:

To configure an IP address for an interface in default state for interface 1/1/1 on Aruba CX 6300 switch, you need to disable switching on the interface first with the command no switching. Then you can assign an IP address with the command ip address. The other options are incorrect because they either do not disable switching or use invalid keywords such as switching or routing. Reference: https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch01.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html

Question: 4

A system engineer needs to preconfigure several Aruba CX 6300 switches that will be sent to a remote office An untrained local field technician will do the rollout of the switches and the mounting of several AP-515s and AP-575S. Cables running to theAPs are not labeled.

The VLANs are already preconfigured to VLAN 100 (mgmt), VLAN 200 (clients), and VLAN 300 (guests) What is the correct configuration to ensure that APs will work properly?

A)

port-access lldp-group lAP-Group seq 10 match sys-desc AP-515 seq 20 match sys-desc AP-575
port-access role lAP-Role description ARUBA AP poe-pnority high trust-mode dscp vlan trunk native 100 vlan trunk allowed 100.200.300 enable
port-access device-profile lAP-Profile associate role lAP-Role associate lldp-group lAP-Group

B)

port-access lldp-group lAP-Group seq 10 match sys-desc 515 seq 20 match sys-desc 575
port-access role lAP-Roie descnption ARUBA AP poe-pnority high trust-mode dscp vlan trunk native 100 vlan trunk allowed 100 200,300
port-access device-profile lAP-Profile associate role lAP-Role associate lldp-group lAP-

Group no shutdown

C)

port-access lldp-group lAP-Group seq 10 match sys-desc 515 seq 20 match sys-desc 575

port-access role lAP-Role descnption ARUBA AP poe-pnority high trust-mode dscp vlan trunk native 100 vlan trunk allowed 200.300

port-access device-profile lAP-Profile enable

associate role lAP-Role

associate lldp-group lAP-Group

D)

port-access lldp-group lAP-Group seq 10 match sys-desc 515 seq 20 matcn sys-desc 575

port-access role lAP-Roie description ARU BA AP poe-pnority high trust-mode dscp vlan trunk native 100 vlan trunk allowed 100.200,300

port-access device-profile lAP-Profiie enable

associate role lAP-Role associate UdD-qrouo lAP-Grouo

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:

Option C is the correct configuration to ensure that APs will work properly. It uses the ap command to configure a port profile for APs with VLAN 100 as the native VLAN and VLAN 200 and 300 as tagged VLANs. It also enables LLDP on the ports to discover the APs and assign them to the port profile automatically. The other options are incorrect because they either do not use the ap command, do not enable LLDP, or do not configure the VLANs correctly. Reference: https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch03.html

Question: 5

Your Director of Security asks you to assign AOS-CX switch management roles to new employees based on their specific job requirements After the configuration was complete, it was noted that a user assigned with the administrators role did not have the appropriate level of access on the switch. The user was not limited to viewing nonsensitive configuration information and a level of 1 was not assigned to their role Which default management role should have been assigned for the user?

A. sysadmin
B. operators
C. helpdesk
D. config

Answer: B

Explanation:

The default management role that should have been assigned for the user is B. operators.
The operators user role is a predefined role that allows users to view nonsensitive configuration information on the switch, such as interfaces, VLANs, routing protocols, statistics, and more. The operators user role has a privilege level of 1, which is the lowest level of access on the switch1.
The administrators user role is a predefined role that has full access to all switch configuration information and all REST API methods. This role is more than what the Director of Security requires1.

Question: 6

A new network design is being considered to minimize client latency in a high-density environment. The design needs to do this by eliminating contention overhead by dedicating subcarriers to clients. Which technology is the best match for this use case?

A. OFDMA
B. MU-MIMO
C. QWMM
D. Channel Bonding

Answer: A

Explanation:

OFDMA (Orthogonal Frequency Division Multiple Access) is a technology that can minimize client latency in a high-density environment by eliminating contention overhead by dedicating subcarriers to clients. OFDMA allows multiple clients to transmit simultaneously on different subcarriers within the same channel, reducing contention and increasing efficiency. MU-MIMO (Multi-User Multiple Input Multiple Output) is a technology that allows multiple clients to transmit simultaneously on different spatial streams within the same channel, but it does not eliminate contention overhead. QWMM (Quality of Service Wireless Multimedia) is a technology that prioritizes traffic based on four access categories, but it does not eliminate contention overhead. Channel Bonding is a technology that combines two adjacent channels into one wider channel, increasing bandwidth but not eliminating contention overhead. Reference:
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdfhttps://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf

Question: 7

Your manufacturing client is having installers deploy seventy headless scanners and fifty IP cameras in their warehouse These new devices do not support 802 1X authentication.
How can HPE Aruba reduce the IT administration overhead associated with this deployment while maintaining a secure environment using MPSK?

A. Have the installers generate keys with ClearPass Self Service Registration.
B. Have the MPSK gateway derive the unique pre-shared keys based on the MAC OUI.
C. Use MPSK Local to automatically provide unique pre-shared keys for devices.
D. MPSK Local will allow the cameras to share a key and the scanners to share a different key

Answer: C

Explanation:

MPSK Local is a feature that can reduce the IT administration overhead associated with deploying devices that do not support 802.1X authentication while maintaining a secure environment. MPSK Local allows the switch to automatically generate and assign unique pre-shared keys for devices based on their MAC addresses, without requiring any configuration on the devices or an external authentication server. The other options are incorrect because they either require manual intervention by the installers or the MPSK gateway, or they do not provide unique pre-shared keys for devices. Reference: https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01- ch05.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch06.html

Question: 8

Which component is used by the Aruba Network Analytics Engine (NAE)?

A. JSON-based scripts
B. Lisp-based agents
C. Ruby-based scripts
D. Current State Database

Answer: A

Explanation:

The component that is used by the Aruba Network Analytics Engine (NAE) is D. Current State Database.
The Current State Database is a database that stores the configuration and state information of the switch, such as interfaces, VLANs, routing protocols, statistics, and more. The NAE can access this database through the AOS-CX REST API and monitor the values of any data point using monitors. The NAE can also track the history of the values in a time-series database and correlate them with network events or configuration changes1. The Current State Database provides NAE with direct visibility into the entire current state of the device, which enables intelligent troubleshooting and automation of network tasks1.
The other options are incorrect because:
A) JSON-based scripts: JSON is a data format that is used to exchange information between applications. It is not a scripting language that can be used by NAE. NAE scripts are written in Python, which is a popular and powerful programming language1.
B) Lisp-based agents: Lisp is a family of programming languages that are mainly used for artificial intelligence and functional programming. It is not a language that can be used by NAE. NAE agents are instances of scripts that run on the switch and collect relevant network information and trigger alerts or actions1.
C) Ruby-based scripts: Ruby is a general-purpose programming language that is known for its expressiveness and elegance. It is not a language that can be used by NAE. NAE scripts are written in Python, which is a popular and powerful programming language1.

Question: 9

You need to have different routing-table requirements with Aruba CX 6300 VSF configuration

Assuming the correct layer-2 VLAN already exists how would you create a new OSPF configuration for a separate routing table?

A. Create a new OSPF area, and attach VRF name.
B. Create a new OSPF process ID with vrf name.
C. Attach a new OSFP process ID with a custom routing table
D. Attach OSPF process ID in the VRF configuration.

Answer: B

Explanation:

To create a new OSPF configuration for a separate routing table, you need to create a new OSPF process ID with vrf name. This will create a new OSPF instance that is associated with the specified VRF and its routing table. The other options are incorrect because they either do not create a new OSPF instance or do not associate it with a VRF. Reference:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html

Question: 10

With the Aruba CX switch configuration, what is the first-hop protocol feature that is used for VSX L3 gateway as per Aruba recommendation?

A. Active Gateway
B. Active-Active VRRP
C. SVI with vsx-sync
D. VRRP

Answer: A

Explanation:

Active Gateway is the first-hop protocol feature that is used for VSX L3 gateway as per Aruba recommendation. Active Gateway is a feature that allows both VSX peers to act as active gateways for different subnets, eliminating the need for VRRP or other first-hop redundancy protocols. Active Gateway also provides fast failover and load balancing for L3 traffic across the VSX peers. The other options are incorrect because they are either not recommended or not supported by Aruba CX VSX. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01- ch07.htmlhttps://www.arubanetworks.com/resource/aruba-virtual-switching-extension-vsx/

Question: 11

You are deploying a bonded 40 MHz wide channel What is the difference in the noise floor perceived by a client using this bonded channel as compared to an unbonded 20MHz wide channel?

A. 2dB
B. 3dB
C. 8dB
D. 4dB

Answer: B

Explanation:

The difference in the noise floor perceived by a client using a bonded 40 MHz wide channel as compared to an unbonded 20 MHz wide channel is 3 dB. The noise floor is the level of background noise in a given frequency band. When two adjacent channels are bonded, the noise floor increases by 3 dB because the bandwidth is doubled and more noise is captured. The other options are incorrect because they do not reflect the correct relationship between bandwidth and noise floor. Reference:

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/wlan-rf/rf-fundamentals.htmhttps://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/channel-bonding.htm

Question: 12

When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?

A. QSVI
B. MAC tables
C. UDLD
D. RPVST+

Answer: B

Explanation:

The information that the Inter-Switch Link Protocol configuration uses in the configuration created is B. MAC tables.

The Inter-Switch Link Protocol (ISL) is a protocol that enables the synchronization of data and state information between two VSX peer switches. The ISL uses a version control mechanism and provides backward compatibility regarding VSX synchronization capabilities. The ISL can span long distances (transceiver dependent) and supports different speeds, such as 10G, 25G, 40G, or 100G1.

One of the data components that the ISL synchronizes is the MAC table, which is a database that stores the MAC addresses of the devices connected to the switch and the corresponding ports or VLANs. The ISL ensures that both VSX peers have the same MAC table entries and can forward traffic to the correct destination2. The ISL also synchronizes other data components, such as ARP table, LACP states for VSX LAGs, and MSTP states2.

Question: 13

What is true regarding 802.11k?

A. It extends radio measurements to define mechanisms for wireless network management of stations
B. It reduces roaming delay by pre-authenticating clients with multiple target APs before a client roams to an AP
C. It provides mechanisms for APs and clients to dynamically measure the available radio resources.
D. It considers several metrics before it determines if a client should be steered to the 5GHz band, including client RSSI

Answer: C

Explanation:

802.11k is a standard that provides mechanisms for APs and clients to dynamically measure the available radio resources in a wireless network. 802.11k defines radio resource management (RRM) functions, such as neighbor reports, link measurement, beacon reports, etc., that allow APs and clients to exchange information about the RF environment and make better roaming decisions. The other options are incorrect because they describe other standards, such as 802.11r, 802.11v, or 802.11ax. Reference:
https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

Question: 14

Your customer is interested in hearing more about how roles can help keep consistent policy enforcement in a distributed overlay fabric How would you explain this concept to them''

A. Group Based Policy ID is applied on egress VTEP after device authentication and policy is enforced on ingress VTEP

B. Role-based policies are tied to IP addresses which have an advantage over IP-based policies and role names are sent between VTEPs

C. Group Based Policy ID is applied on ingress VTEP after device authentication and policy is enforced on egress VTEP

D. Role-based policies enhance User Based Tunneling across the campus network and the policy traffic is protected with iPsec

Answer: C

Explanation:

This is the correct explanation of how roles can help keep consistent policy enforcement in a distributed overlay fabric. Roles are used to assign group based policy IDs (GBPs) to devices after they authenticate with ClearPass or a local database. GBPs are then used to tag the traffic from the devices and send them to the ingress VTEP, which applies the GBP on the VXLAN header. The egress VTEP then enforces the policy based on the GBP and the destination device. The other options are incorrect because they either do not describe the correct sequence of events or do not use the correct terms. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200- 6728/bk01-ch03.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200- 6728/bk01-ch05.html

Question: 15

How is Multicast Transmission Optimization implemented in an HPE Aruba wireless network?

A. "The optimal rate for sending multicast frames is based on the highest broadcast rate across all associated clients

B. When this option is enabled the minimum default rate for multicast traffic is set to 12 Mbps for 5 GHz

C. The optimal rate for sending multicast frames is based on the lowest broadcast rate across all associated clients.

D. The optimal rate for sending multicast frames is based on the lowest unicast rate across all associated

clients.

Answer: D

Explanation:

multicast transmission optimization is a feature that allows the IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients1. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5.0 GHz is 6 Mbps. This option is disabled by default1.

Question: 16

You are setting up a customer's 15 headless IoT devices that do not support 802.1X. What should you use?

A. Multiple Pre-Shared Keys (MPSK) Local
B. Clearpass with WPA3-PSK
C. Clearpass with WPA3-AES
D. Multiple Pre-Shared Keys (MPSK) with WPA3-AES

Answer: A

Explanation:

MPSK Local is a feature that can be used to set up 15 headless IoT devices that do not support 802.1X authentication. MPSK Local allows the switch to automatically generate and assign unique preshared keys for devices based on their MAC addresses, without requiring any configuration on the devices or an external authentication server. The other options are incorrect because they either require 802.1X authentication, which is not supported by the IoT devices, or WPA3 encryption, which is not supported by Aruba CX switches. Reference: https://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-ch05.htmlhttps://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-ch06.html

Question: 17

How do you allow a new VLAN 100 between VSX pair inter-switch-link 256 for port 1/45 and 2/45?

A. vlan trunk allowed 100 for ports 1/45 and 1/46
B. vlan trunk add 100 in LAG256
C. vlan trunk allowed 100 in LAG256
D. vlan trunk add 100 in MLAG256

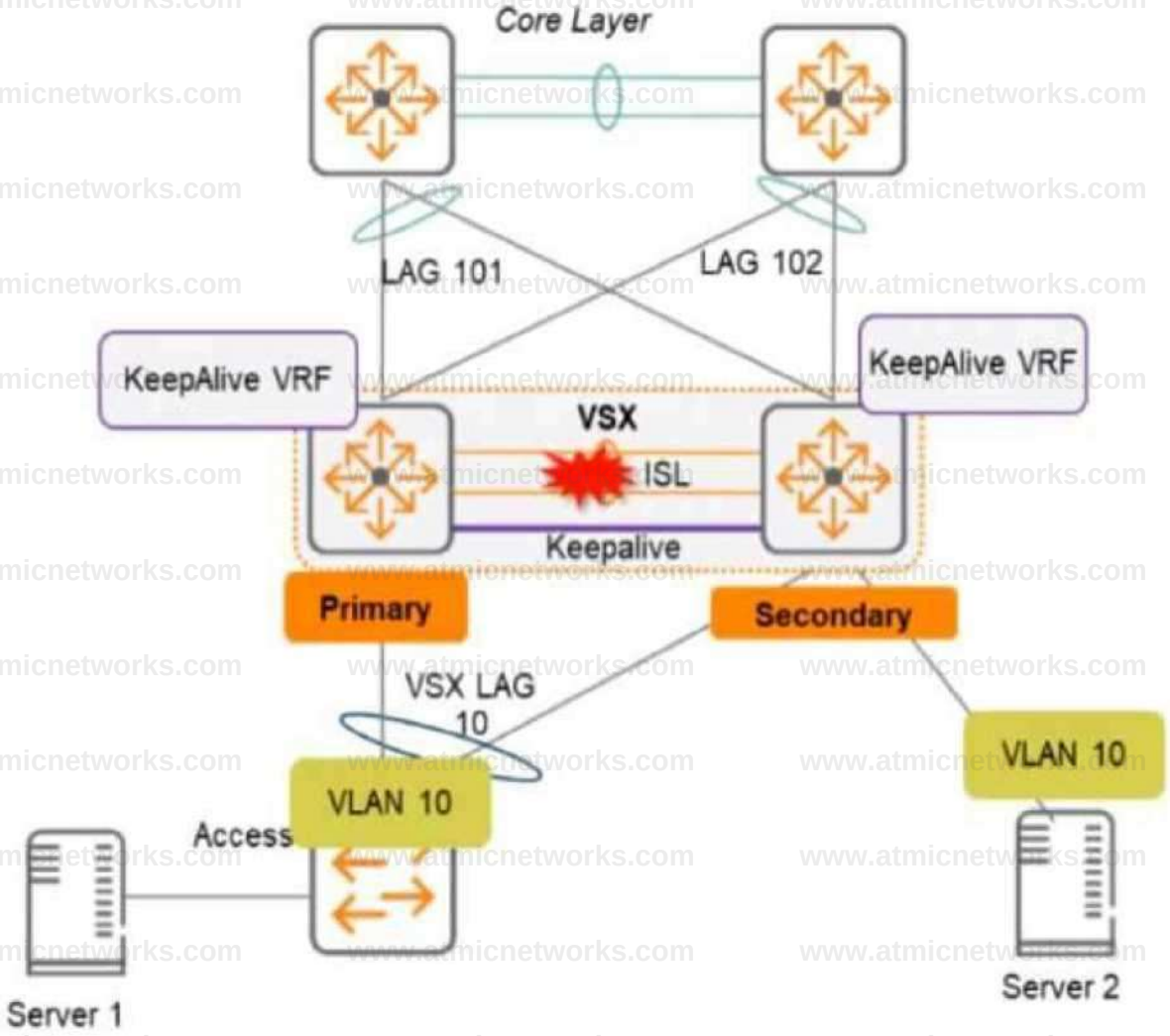
Answer: C

Explanation:

To allow a new VLAN 100 between VSX pair inter-switch-link 256 for port 1/45 and 2/45, you need to use the command vlan trunk allowed 100 in LAG256. This will add VLAN 100 to the list of allowed VLANs on the trunk port LAG256, which is part of the inter-switch-link between VSX peers. The other options are incorrect because they either do not use the correct command or do not specify the correct port or VLAN. Reference: https://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-ch07.htmlhttps://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-ch02.html

Question: 18

Two AOS-CX switches are configured with VSX at the the Access-Aggregation layer where servers attach to them An SVI interface is configured for VLAN 10 and serves as the default gateway for VLAN 10. The ISL link between the switches fails, but the keepalive interface functions. Active gateway has been configured on the VSX switches.



What is correct about access from the servers to the Core? (Select two.)

A. Server 1 can access the core layer via the keepalrve link
B. Server 2 can access the core layer via the keepalive link
C. Server 2 cannot access the core layer.
D. Server 1 can access the core layer via both uplinks
E. Server 1 and Server 2 can communicate with each other via the core layer
F. Server 1 can access the core layer on only one uplink

Answer: DE

Explanation:

These are the correct statements about access from the servers to the Core when the ISL link between the switches fails, but the keepalive interface functions. Server 1 can access the core layer via both uplinks because it is connected to VSX-A, which is still active for VLAN 10. Server 2 can also access the core layer via its uplink to VSX-B, which is still active for VLAN 10 because of Active Gateway feature. Server 1 and Server 2 can

communicate with each other via the core layer because they are in the same VLAN and subnet, and their traffic can be routed through the core switches. The other statements are incorrect because they either describe scenarios that are not possible or not relevant to the question. Reference: https://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-

Question: 19

A large retail client is looking to generate a rich set of contextual data based on the location information of wireless clients in their stores Which standard uses Round Trip Time (RTT) and Fine Time Measurements (FTM) to calculate the distance a client is from an AP?

A. 802.11ah
B. 802.11mc
C. 802.11be
D. 802.11V

Answer: B

Explanation:

802.11mc is a standard that uses Round Trip Time (RTT) and Fine Time Measurements (FTM) to calculate the distance a client is from an AP. 802.11mc defines a protocol for exchanging FTM frames between an AP and a client, which contain timestamps that indicate when the frames were transmitted and received. By measuring the RTT of these frames, the AP or the client can estimate their distance based on the speed of light. The other options are incorrect because they either do not use RTT or FTM or do not exist as standards. Reference: https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdfhttps://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

Question: 20

You need to create a keepalive network between two Aruba CX 8325 switches for VSX configuration How should you establish the keepalive connection?

A. SVI, VLAN trunk allowed all on ISL in default VRF
B. routed port in custom VRF
C. loopback 0 and OSPF area 0 in default VRF
D. SVI, VLAN trunk allowed all on ISL in custom VRF

Answer: B

Explanation:

To establish a keepalive connection between two Aruba CX 8325 switches for VSX configuration, you need to use a routed port in custom VRF. A routed port is a physical port that acts as a layer 3 interface and does not belong to any VLAN. A custom VRF is a virtual routing and forwarding instance that provides logical separation of routing tables. By using a routed port in custom VRF, you can isolate the keepalive traffic from other traffic and prevent routing loops or conflicts. The other options are incorrect because they either do not use a routed port or do not use a custom VRF. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01- ch07.htmlhttps://www.arubanetworks.com/techdocs/AOS-

CX/10.04/HTML/5200-6728/bk01- ch02.html

Question: 21

Which method is used to onboard a new UXI in an existing environment with 802 1X authentication? (The sensor has no cellular connection)

A. Use the UXI app on your smartphone and connect the UXI via Bluetooth
B. Use the Aruba installer app on your smartphone to scan the barcode
C. Connect the new UXI from an already installed one and adjust the initial configuration.
D. Use the CLI via the serial cable and adjust the initial configuration.

Answer: A

Explanation:

To onboard a new UXI in an existing environment with 802.1X authentication, you need to use the UXI app on your smartphone and connect the UXI via Bluetooth. The UXI app allows you to scan the QR code on the UXI sensor and configure its network settings, such as SSID, password, IP address, etc. The Bluetooth connection allows you to communicate with the UXI sensor without requiring any network access or cellular connection. The other options are incorrect because they either do not use the UXI app or do not use Bluetooth. Reference: https://www.arubanetworks.com/products/network-management-operations/analytics- monitoring/user-experience-insight-sensors/ https://help.centralon-prem.arubanetworks.com/2.5.4/documentation/online_help/content/nms-on-prem/aos-cx/get- started/uxi-sensor.htm

Question: 22

A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working to a remote site connected via layer-3 All legacy devices are connected

to a dedicated Aruba CX 6200 switch at each site.
What technology on the Aruba CX 6200 could be used to meet this requirement?

A. Inclusive Multicast Ethernet Tag (IMET)
B. Ethernet over IP (EoIP)
C. Generic Routing Encapsulation (GRE)
D. Static VXLAN

Answer: A

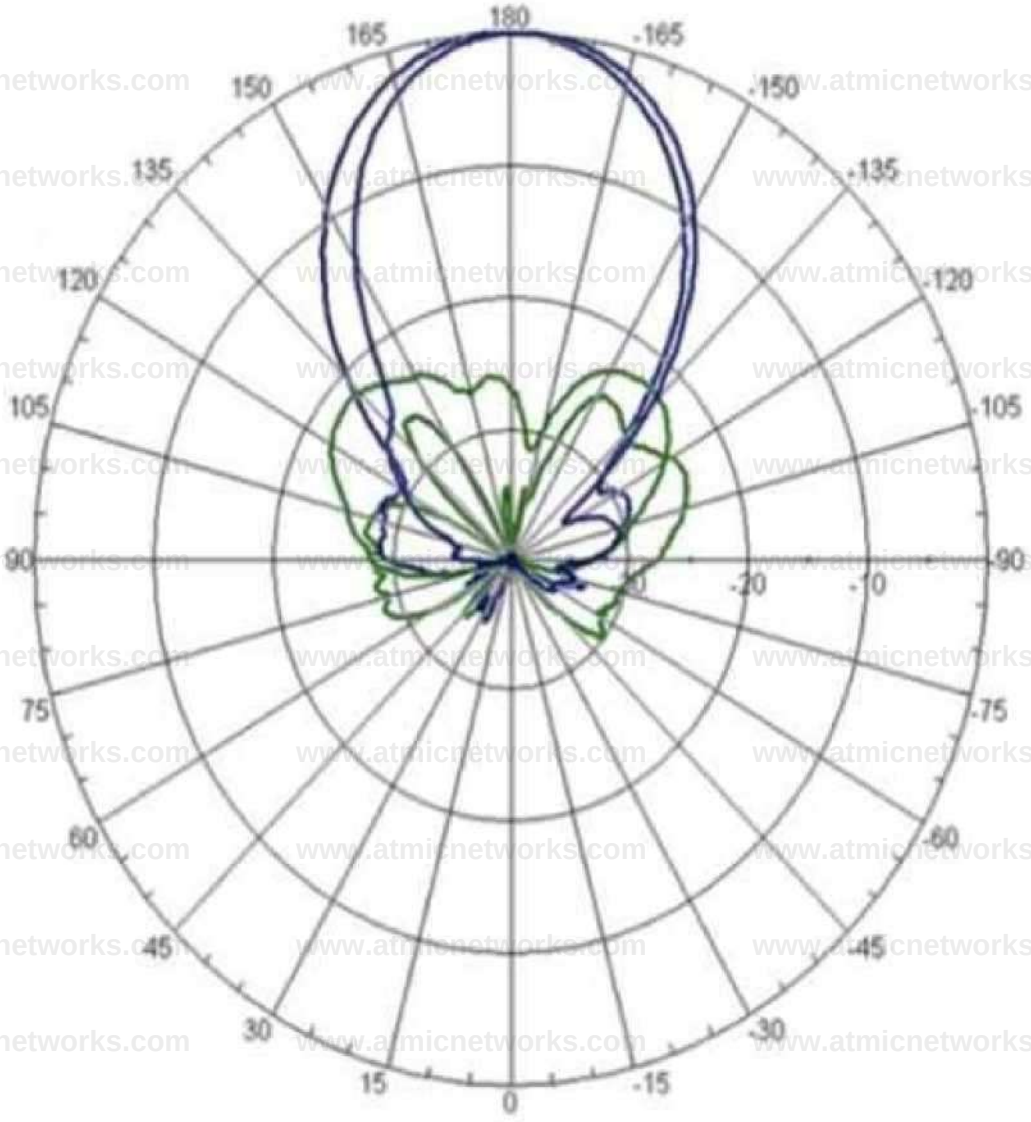
Explanation:

VXLAN is a technology that can be used to meet the requirement of using a legacy application that communicates at layer-2 across a layer-3 network. Static VXLAN is a feature that allows the creation of layer-2 overlay networks over a layer-3 underlay network using VXLAN tunnels. Static VXLAN does not require any control plane protocol or VTEP discovery mechanism, and can be configured manually on the Aruba CX 6200 switches. The other options are incorrect because they either do not support layer-2 communication over layer-3 network or are not supported by Aruba CX 6200 switches. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-

6728/bk01-ch03.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200- 6728/bk01-ch05.html

Question: 23

Refer to the image.



Horizontal Pattern

Your customer is complaining of weak Wi-Fi coverage in their office. They mention that the office on the other side of the hall has much better signal What is the likely cause of this issue7

A. The AP is a remote access point.
B. The AP is using a directional antenna.
C. The AP is an outdoor access point.
D. The AP is configured in Mesh mode

Answer: B

Explanation:

The likely cause of the issue of weak Wi-Fi coverage in the office is that the AP is using a directional antenna. A directional antenna is an antenna that radiates or receives radio waves more strongly in one or more directions, creating a focused beam of signal. A directional antenna can provide better coverage and performance for a specific area, but it can also create dead zones or weak spots for other areas. The other options are incorrect because they either do not affect the Wi-Fi coverage or

do not match the scenario. Reference:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/rf-fundamentals.htm
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/antennas.htm

Question: 24

Your customer has asked you to assign a switch management role for a new user The customer requires the user role to only have Web UI access to the System > Log page and only have access to the GET method for REST API for the /logs/event resource
Which default AOS-CX user role meets these requirements?

A. administrators
B. auditors
C. sysops
D. operators

Answer: A

Explanation:

The auditors role is the default AOS-CX user role that meets the requirements of having Web UI access to the System > Log page and having access to the GET method for REST API for the /logs/event resource. The auditors role has a level of 1 and allows read-only access to most commands except those related to security or passwords. It also allows access to the Web UI and REST API with limited permissions. The other options are incorrect because they either have higher levels of access or do not allow access to the Web UI or REST API. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch01.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch04.html

Question: 25

You are configuring Policy Based Routing (PBR) for a subnet that will be used to test a new default route for your network Traffic originating from 10.2.250.0/24 should use a new default route to 10.1.1.253. Other non-default routes for this subnet should not be affected by this change.
What are two parts of the solution for these requirements? (Select two.)
A)

```
pbr>action-list def_route_test default-nexthop 10 1J 253/24
```

B)

```
class ip test_subnet
    10 match any 10 2 250 0/24 any
policy defjoutejestjwlicy
    10 class ip test_subnet action pbr defjouteJest interface vlan 100
    ip address 10 2 250 0/24
    apply policy pbr Jest routed in
```

C)

```
class ip test_subnet
    10 match any 10 2 250 0 255 255 255 0 any
policy def joule Jest_pohcy
    10 class ip ipjest_subnet action pbr def_route_test Interface vlan 100
    ip address 10 2 250 0/24
    apply policy pbr Jest routed out
```

D)

```
pbr-action-nst defjoutejest
    default-nexthop 10.1.1 253
    Interface null
```

E)

```
pbr-action-iist defjoutejest
    nexthop 10 1 1 253
    Interface null
```

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

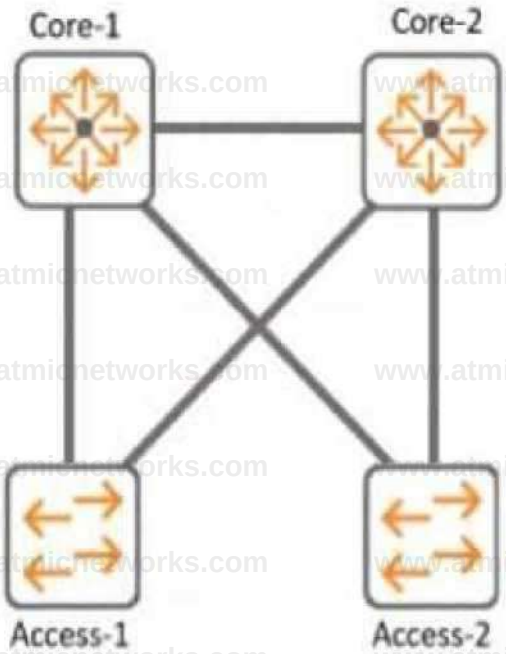
Answer: CE

Explanation:

Two parts of the solution for these requirements are Option C and Option E.
Option C is a part of the solution because it defines a policy-based routing action list named route_test, which specifies the next hop IP address as 10.1.1.253 for the matching traffic. This is the new default route that the user wants to use for the subnet 10.2.250.0/24. The interface null parameter indicates that the traffic will be routed to the next hop without using a specific interface1. Option E is a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 250, which has an IP address of 10.2.250.1/24. This is the subnet that the user wants to test the new default route for. The apply policy command enables policy-based routing on the interface and associates it with the action list2.
Option A is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify the next hop IP address as 10.1.1.253, which is the new default route that the user wants to use. Instead, it specifies a next hop IP address of 10.1.1.254, which is different
from the requirement.
Option B is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify any next hop IP address at all, which is necessary for policy-based routing to work. Instead, it specifies an interface null parameter without any IP address, which is invalid.
Option D is not a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 200, which has an IP address of 10.2.200.1/24. This is not the subnet that the user wants to test the new default route for, but a different subnet that should not be affected by this change.

Question: 26

Refer to the exhibit.



With Core-1. what is the default value for config-revision?

A. 0
B. 1
C. 1-0
D. 0. 0

Answer: A

Explanation:

The default value for config-revision on Core-1 is 0. Config-revision is a parameter that indicates the configuration version of a VSX pair. It is used to synchronize the configuration between the VSX peers and to detect any configuration mismatch. The config-revision value is set to 0 by default on both VSX peers and is incremented by 1 every time a configuration change is made on either peer. The other options are incorrect because they do not reflect the default value of config-revision. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html

Question: 27

What are the requirements to ensure that WMM is working effectively'? (Select two)

A. The APs and the controller are Wi-Fi CERTIFIED for WMM which is enabled
B. All APs need to be from the AP-5xx series and AP-6xx series which are Wi-Fi CERTIFIED 6.
C. The Client must be Wi-Fi CERTIFIED for WMM and configured for WMM marking.
D. The Aruba AOS10 APs installed have to be converted to controlled mode
E. The AP needs to be connected via a tagged VLAN to the wired port

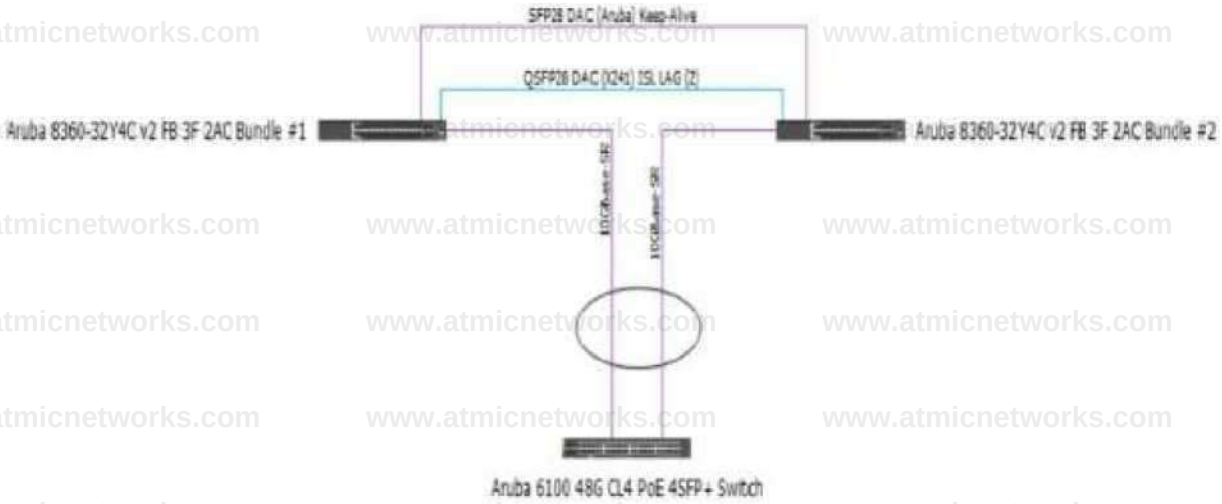
Answer: AC

Explanation:

These are the correct requirements to ensure that WMM (Wi-Fi Multimedia) is working effectively. WMM is a standard that provides quality of service (QoS) for wireless networks by prioritizing traffic into four categories: voice, video, best effort, and background. To use WMM, both the APs and the controller must be Wi-Fi CERTIFIED for WMM, which means they have passed interoperability tests and comply with the standard. WMM must also be enabled on the APs and the controller, which is usually the default setting. The client device must also be Wi-Fi CERTIFIED for WMM and configured for WMM marking, which means it can tag its traffic with the appropriate priority level based on the application type. The other options are incorrect because they are either not related to WMM or not required for WMM to work. Reference:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/wlan-qos/wmm.htmhttps://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm

Question: 28

Review the exhibit.



You are troubleshooting an issue with a 10 102.39 0/24 subnet which is also VLAN 1000 used Tor wireless clients on a pair of Aruba CX 8360 switches The subnet SVI is configured on the 8360 pair, and the DHCP server is a Microsoft Windows Server 2022 Standard with an IP address of 10 200 1.100. The 10.102.250.0/24 subnet is used for switch management.

A large number of DHCP requests are failing You are observing sporadic DHCP behavior across clients attached to the CX 6100 switch.

Which action may help fix the issue?

A)
Enter the following commands on the VSX primary switch

```
V9X
    vsx-sync dhcp-relay
    exi:
```

B)
Enter the following commands on the VSX secondary switch

```
vlan 1000
    ip relay-azidress 10.200.1.IOC exit
```

C)
Add an SVI In the 10 102 39 0/24 subnet on the Aruba CX 6100 switch that the APs are connected to

D)
Enter the following commands on the Aruba CX 6100 switch

```
    interface vlan 1100
```

ip helper-address 10.2'1.1.1*1 exit

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:

Option C is the only action that configures the DHCP relay on the SVI of VLAN 1000 on the CX 8360 switches. DHCP relay is a feature that allows a switch to forward DHCP requests from clients in one subnet to a DHCP server in another subnet. DHCP relay is required when the DHCP server and the clients are not in the same broadcast domain1.

Option C uses the following commands:

interface vlan 1000: This command enters the interface configuration mode for the SVI of VLAN 1000, which has an IP address of 10.102.39.1/24 and is used for wireless clients.

ip helper-address vrf default 10.200.1.100: This command configures the IP address of the DHCP server as a helper address for the SVI, which means that the switch will forward DHCP requests from clients on VLAN 1000 to this address. The vrf default parameter indicates that the SVI and the DHCP server are in the same VRF.

Question: 29

In an ArubaOS 10 architecture using an AP and a gateway, what happens when a client attempts to join the network and the WLAN is configured with OWE?

A. Authentication information is not exchanged
B. The Gateway will not respond.
C. No encryption is applied.
D. RADIUS protocol is utilized.

Answer: A

Explanation:

This is the correct statement about what happens when a client attempts to join the network and the WLAN is configured with OWE (Opportunistic Wireless Encryption). OWE is a standard that provides encryption for open networks without requiring any authentication or credentials from the client or the network. OWE uses a Diffie-Hellman key exchange mechanism to establish a secure session between the client and the AP without exchanging any authentication information. The other options are incorrect because they either describe scenarios that require authentication or encryption methods that are not used by OWE. Reference: https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdfhttps://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

Question: 30

Which Aruba AP mode is sending captured RF data to Aruba Central for waterfall plot?

A. Hybrid Mode
B. Air Monitor
C. Spectrum Monitor
D. Dual Mode

Answer: C

Explanation:

Spectrum Monitor is an Aruba AP mode that is sending captured RF data to Aruba Central for waterfall plot. Spectrum Monitor is a mode that allows an AP to scan all channels in both 2.4 GHz and 5 GHz bands and collect information about the RF environment, such as interference sources, noise floor, channel utilization, etc. The AP then sends this data to Aruba Central, which is a cloudbased network management platform that can display the data in various formats, including waterfall plot. Waterfall plot is a graphical representation of the RF spectrum over time, showing the frequency, amplitude, and duration of RF signals. The other options are incorrect because they are either not AP modes or not sending RF data to Aruba Central. Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/spectrum_monitor.htmhttps://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1- overview/waterfall_plot.htm https://www.arubanetworks.com/products/network-management- operations/aruba-central/

Question: 31

What is a primary benefit of BSS coloring?

A. BSS color tags improve performance by allowing clients on the same channel to share airtime.
B. BSS color tags are applied to client devices and can reduce the threshold for interference
C. BSS color tags are applied to Wi-Fi channels and can reduce the threshold for interference
D. BSS color tags improve security by identifying rogue APs and removing them from the network.

Answer: C

Explanation:

BSS coloring is a mechanism that helps identify the BSS Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients. on the same channel and differentiate them from other BSS on the same channel12. Each BSS is assigned a color code, which is a 6-bit value that is carried in the PHY header of the Wi-Fi frames12. By using BSS coloring, the APs and clients can reduce the threshold for interference detection and avoid unnecessary backoff or retransmissions when they detect frames from other BSS with different colors12. This can improve the spectral efficiency and throughput of the network12. The other options are incorrect because they do not describe the primary benefit of BSS coloring.

Question: 32

What is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches?

A. Switch authentication and local forwarding of the voice traffic
B. Switch authentication and user-based tunneling of the voice traffic.
C. Central authentication and port-based tunneling of the voice traffic.
D. Controller authentication and port-based tunneling of all traffic

Answer: A

Explanation:

This is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches. Dynamic segmentation is a feature that allows AOS-CX switches to tunnel user traffic to a controller or another switch based on user roles and policies. For voice traffic, it is recommended to use switch authentication and local forwarding, which means the voice devices are authenticated by the switch and their traffic is forwarded locally without tunneling. This reduces latency and jitter for voice traffic and improves voice quality. The other options are incorrect because they either use central authentication or tunneling, which are not optimal for voice traffic. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.htmlhttps://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf

Question: 33

A network administrator is attempting to troubleshoot a connectivity issue between a group of users and a particular server The administrator needs to examine the packets over a period of time from their desktop; however, the administrator is not directly connected to the AOS-CX switch involved with the traffic flow.

What statements are correct regarding the ERSPAN session that needs to be established on an AOS- CX switch'? (Select two)

A. On the source AOS-CX switch, the destination specified is the switch to which the administrator's desktop is connected
B. The encapsulation protocol used is GRE.
C. The encapsulation protocol used is VXLAN.
D. The encapsulation protocol is UDP.
E. On the source AOS-CX switch, the destination specified is the administrators desktop

Answer: BE

Explanation:

These are the correct statements regarding the ERSPAN session that needs to be established on an AOS-CX switch for a network administrator to examine the packets over a period of time from their desktop. ERSPAN (Encapsulated Remote Switched Port Analyzer) is a feature that allows an AOS-CX switch to mirror traffic from one or more source ports or VLANs to a remote destination IP address over a GRE (Generic Routing Encapsulation) tunnel. The destination IP address must be the IP address of the administrator’s desktop, which must have a packet capture tool installed to receive and analyze the mirrored traffic. The encapsulation protocol used for ERSPAN is GRE, which adds a header to the mirrored packets with information such as source and destination IP addresses, session ID, etc. The other statements are incorrect because they either do not specify the correct destination IP address or do not use ERSPAN or GRE. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html

Question: 34

On AOS10 Gateways, which device persona is only available when configuring a Gateway-only group'?

A. Edge
B. Mobility
C. Branch
D. VPN Concentrator

Answer: B

Explanation:

AOS 10 Gateways can have the following personas: Mobility, Branch, and VPN Concentrator1 However, the Mobility persona is only available when configuring a Gateway-only group, which is a group that contains only one gateway device2 The Mobility persona provides Overlay WLAN and (or) wired LAN functionalities for campus networks1 The Branch persona provides the Aruba Instant OS and SD-Branch (LAN + WAN) functionality for branch and microbranch networks1 The VPN Concentrator persona provides VPN termination and routing functionality for remote access networks3 The Edge persona is not a valid option, as it is not a supported device persona for AOS 10 Gateways.

Question: 35

A company deployed Dynamic Segmentation with their CX switches and Gateways After performing a security audit on their network, they discovered that the tunnels built between the CX switch and the Aruba Gateway are not encrypted. The company is concerned that bad actors could try to insert spoofed messages on the Gateway to disrupt communications or obtain information about the network.
Which action must the administrator perform to address this situation?

A. Enable Secure Mode Enhanced
B. Enable Enhanced security
C. Enable Enhanced PAPI security
D. Enable GRE security

Answer: C

Explanation:

PAPI is the protocol that is used to establish tunnels between the CX switch and the Aruba Gateway for Dynamic Segmentation1. By default, PAPI uses a simple checksum to verify the integrity of the messages, but it does not encrypt the payload2. This could expose the network to spoofing or replay attacks by malicious actors. To address this situation, the administrator must enable Enhanced PAPI security, which uses AES-256 encryption and HMAC-SHA1 authentication to protect the tunnel traffic2. Enhanced PAPI security can be enabled on the CX switch by using the command system papi enhanced-security enable3. This will ensure that the tunnels built between the CX switch and the Aruba Gateway are encrypted and authenticated.

Question: 36

What is an Aruba-recommended best practice for hardening that only applies to Aruba CX 6300 series switches with dedicated management ports?

A. Implement a control plane ACL to limit access to approved IPs and/or subnets
B. Manually enable Enhanced Security Mode from a console session.
C. Disable all management services on the default VRF.
D. Create a dedicated management VRF, and assign the management port to it.

Answer: D

Explanation:

This is an Aruba-recommended best practice for hardening that only applies to Aruba CX 6300 series switches with dedicated management ports. A dedicated management port is a physical port that is used exclusively for out-of-band management access to the switch. A dedicated management VRF is a virtual routing and forwarding instance that isolates the management traffic from other traffic on the switch. By creating a dedicated management VRF and assigning the management port to it, the administrator can enhance the security and performance of the management access to the switch. The other options are incorrect because they either do not apply to switches with dedicated

management ports or do not follow Aruba-recommended best practices. Reference: https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf

Question: 37

What is enabled by LLDP-MED? (Select two.)

A. Voice VLANs can be automatically configured for VoIP phones
B. APs can request power as needed from PoE-enabled switch ports
C. iSCSI client devices can request to have flow control enabled
D. GVRP VLAN information can be used to dynamically add VLANs to a trunk
E. iSCSl client devices can set the required MTU setting for the port.

Answer: AB

Explanation:

These are two benefits enabled by LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery). LLDP-MED is an extension of LLDP that provides additional capabilities for network devices such as VoIP phones and APs. One of the capabilities is to automatically configure voice VLANs for VoIP phones, which allows them to be placed in a separate VLAN from data devices and receive QoS and security policies. Another capability is to request power as needed from PoE- enabled switch ports, which allows APs to adjust their power consumption and performance based on the available power budget. The other options are incorrect because they are either not enabled by LLDP-MED or not related to LLDP-MED. Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/wlan-qos/lldp-med.htmhttps://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/poe.htm

Question: 38

You need to ensure that voice traffic sent through an ArubaOS-CX switch arrives with minimal latency What is the best scheduling technology to use for this task?

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

Answer: A

Explanation:

Strict queuing is the best scheduling technology to use for voice traffic on an AOS-CX switch. Scheduling is a mechanism that determines how packets are transmitted from different queues on an egress port. Strict queuing is a scheduling method that gives the highest priority queue absolute preference over all other queues, regardless of their size or utilization. Voice traffic should be

assigned to the highest priority queue and scheduled with strict queuing to ensure minimal latency and jitter. The other options are incorrect because they are either not scheduling methods or not optimal for voice traffic. Reference: https://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-ch02.htmlhttps://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-ch03.html

Question: 39

You are helping an onsite network technician bring up an Aruba 9004 gateway with ZTP for a branch office The technician was to plug in any port for the ZTP process to start Thirty minutes after the gateway was plugged in new users started to complain they were no longer able to get to the internet. One user who reported the issue stated their IP address is 172.16 0.81 However, the branch office network is supposed to be on 10.231 81.0/24. What should the technician do to alleviate the issue and get the ZTP process started correctly?

A. Turn off the DHCP scope on the gateway, and set DNS correctly on the gateway to reach Aruba Activate
B. Move the cable on the gateway from port G0/0V1 tc port G0 0.0
C. Move the cable on the gateway to G0/0/1. and add the device's MAC and Serial number in Central D. Factory default and reboot the gateway to restart the process.

Answer: B

Explanation:

Aruba 9004 gateway supports ZTP on port G0/0/0 by default1. If the gateway is connected to a different port, such as G0/0/V1, it will not be able to communicate with Aruba Activate and Aruba Central, which are required for ZTP2. Moreover, port G0/0/V1 is configured as a DHCP server by default, which can cause IP address conflicts with the existing network3. Therefore, the technician should move the cable on the gateway to port G0/0/0, which will allow the gateway to obtain an IP address from the network DHCP server and start the ZTP process. The other options are not correct because they will not solve the issue or enable ZTP. For example, option D will not work because factory defaulting and rebooting the gateway will not change the port configuration or behavior3.

Question: 40

A company recently deployed new Aruba Access Points at different branch offices Wireless 802.1X authentication will be against a RADIUS server in the cloud. The security team is concerned that the traffic between the AP and the RADIUS server will be exposed.
What is the appropriate solution for this scenario?

A. Enable EAP-TLS on all wireless devices
B. Configure RadSec on the AP and Aruba Central.
C. Enable EAP-TTLS on all wireless devices.
D. Configure RadSec on the AP and the RADIUS server

Answer: D

Explanation:

This is the appropriate solution for this scenario where wireless 802.1X authentication will be against a RADIUS server in the cloud and the security team is concerned that the traffic between the AP and the RADIUS server will be exposed. RadSec, also known as RADIUS over TLS, is a protocol that provides encryption and authentication for RADIUS traffic over TCP and TLS. RadSec can be configured on both the AP and the RADIUS server to establish a secure tunnel for exchanging RADIUS packets. The other options are incorrect because they either do not provide encryption or authentication for RADIUS traffic or do not involve RadSec. Reference: https://www.securew2.com/blog/what-is-radsec/ https://www.cloudradius.com/radsec-vs-radius/

Question: 41

A customer is using stacked Aruba CX 6200 and CX 6300 switches for access and a VSX pair of Aruba CX 8325 as a collapsed core 802 1X is implemented for authentication. Due to the lack of cabling, some unmanaged switches are still in use Sometimes devices behind these switches cause network outages The switch should send a warning to the helpdesk when the problem occurs You have been asked to implement an effective solution to the problem
What is the solution for this?

A. Configure spanning tree on the Aruba CX 8325 switches Set the trap-option
B. Configure loop protection on all edge ports of the Aruba CX 6200 and CX 6300 switches No trap option is needed
C. Configure loop protection on all edge ports of the Aruba CX 6200 and CX 6300 switches Set up the trap-option
D. Configure spanning tree on the Aruba CX 6200 and CX 6300 switches No trap option is needed

Answer: C

Explanation:

This is the correct solution to the problem of devices behind unmanaged switches causing network outages due to loops. Loop protection is a feature that allows an Aruba CX switch to detect and prevent loops by sending loop protection packets on each port, LAG, or VLAN on which loop protection is enabled. If a loop protection packet is received by the same switch that sent it, it indicates a loop exists and an action is taken based on the configuration. Loop protection should be configured on all edge ports of the Aruba CX 6200 and CX 6300 switches,

which are the ports that connect to end devices or unmanaged switches. The trap-option should be set up to send a warning to the helpdesk when a loop is detected. The other options are incorrect because they either do not configure loop protection or do not set up the trap-option. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-99A8B276-0DA3- 4458-AFD8-42BFEC29D4F5.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-8561-17DB0311ED8F.html

Question: 42

A customer wants to enable wired authentication across all their CX switches One of the requirements is that the switch must be able to authenticate a single computer connected through a VoIP phone.

Which feature should be enabled to support this requirement?

A. Multi-Domain Authentication
B. Device-Based Mode
C. MAC Authentication
D. Multi-Auth Mode

Answer: A

Explanation:

Multi-Domain Authentication is the feature that should be enabled to support the requirement that the switch must be able to authenticate a single computer connected through a VoIP phone. MultiDomain Authentication is a feature that allows an Aruba CX switch to apply different authentication methods and policies to different devices connected to the same port. For example, a VoIP phone and a computer can be connected to the same port using a single cable, but they can be authenticated separately using different credentials and assigned to different VLANs. The other options are incorrect because they either do not support multiple devices on the same port or do not provide authentication. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-7D9E9F6E-5C2A-4F7E-BE6D-A2C3A6C7B9F9.htmlhttps://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf

Question: 43

Refer to the exhibit.

A company has deployed 200 AP-635 access points. To but is not working as expected What would be the correct action to fix the issue?

A. Change the SSID to WPA3-Enhanced Open
B. Change the SSID to WPA3-Enterprise (CCM).
C. Change the SSID to WPA3-Personal
D. Change the SSID to WPA3-Enterpnse (CNSA).

Answer: D

Explanation:

According to the Aruba Campus Access Professional documents1, WPA3-Enterprise is a security mode that supports 802.1X authentication and encryption with either AES-CCM or AES-

GCMP. WPA3-Enterprise also optionally adds usage of Suite-B 192-bit minimum-level security suite that is aligned with Commercial National Security Algorithm (CNSA) for enterprise networks2. This mode provides the highest level of security and is suitable for government and financial institutions. The exhibit shows that the SSID is configured with WPA3-Enterprise (CCM), which uses AES-CCM as the encryption protocol. However, this mode is not compatible with some devices that require CNSA compliance. Therefore, changing the SSID to WPA3-Enterprise (CNSA) would fix the issue and allow all devices to connect to the network.

Question: 44

A customer is using Aruba Cloud Guest, but visitors keep complaining that the captive portal page keeps coming up after devices go to sleep Which solution should be enabled to deal with this issue?

A. MAC Caching under the splash page
B. MAC Caching under the user-role
C. Wireless Caching under the splash page
D. MAC Caching under the WLAN

Answer: A

Explanation:

MAC Caching is a feature that allows a guest user to bypass the captive portal page after the first authentication based on their MAC address1 MAC Caching can be enabled under the splash page settings in Aruba Cloud Guest2 MAC Caching can improve the user experience and reduce the network overhead by eliminating the need for repeated authentication.

Question: 45

Your customer is having connectivity issues with a newly-deployed Microbranch group The access points in this group are online in Aruba Central, but no VPN tunnels are forming.
What is the most likely cause of this issue?

A. There is a time difference between the AP and the gateways The gateways should have NTP added B. The SSL certificate on the gateway used to encrypt the connection has not been added to the APs trust list
C. There may be a firewall blocking GRE tunneling between the AP and the gateway
D. The gateway group is running in automatic cluster mode and should be in manual cluster mode

Answer: C

Explanation:

This is the most likely cause of the issue where the access points in a Microbranch group are online in Aruba Central, but no VPN tunnels are forming. A Microbranch group is a group that contains both APs and Gateways and allows them to form VPN tunnels for secure communication. The VPN tunnels use GRE (Generic Routing Encapsulation) as the encapsulation protocol and IPSec as the encryption protocol. If there is a firewall blocking GRE traffic between the AP and the gateway, the VPN tunnels cannot be established. The other options are incorrect because they either do not affect the VPN

tunnel formation or do not apply to a Microbranch group. Reference:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/gateways/microbranch.htm
https://www.arubanetworks.com/assets/tg/TB_ArubaGateway.pdf

Question: 46

Which statements regarding 0SPFv2 route redistribution are true for Aruba OS CX switches? (Select two.)

A. The "redistribute connected" command will redistribute all connected routes for the switch including local loopback addresses
B. The "redistribute ospf" command will redistribute routes from all OSPF V2 and V3 processes
C. The "redistribute static route-map connected-routes" command will redistribute all static routes without a matching deny in the route map "connected-routes".
D. The "redistribute connected" command will redistribute all connected routes for the switch except local loopback addresses.
E. The "redistribute static route-map connected-routes" command will redistribute all static routes with a matching permit in the route map "connected-routes-

Answer: AE

Explanation:

These are two correct statements regarding OSPFv2 route redistribution for Aruba OS CX switches. Route redistribution is a process that allows routes from one routing protocol or source to be injected into another routing protocol or destination. OSPFv2 is a link-state routing protocol that supports route redistribution from various sources, such as connected, static, BGP, etc. The “redistribute connected” command will redistribute all connected routes for the switch, including local loopback addresses, into OSPFv2. The “redistribute static route-map connected-routes” command will redistribute all static routes that have a matching permit statement in the route map named “connected-routes” into OSPFv2. The other statements are incorrect because they either do not reflect the correct behavior of route redistribution commands or do not exist as valid commands. Reference:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01- ch03.html

Question: 47

You are configuring an SVI on an Aruba CX switch that needs to have the following characteristics: • VLANID = 25 . IPv4 address 10 105 43 1 with mask 255 255 255.0

- IPv6 address fd00:5708::f02d:4df6 with a 64 bit prefix length
- member of VRF eng
- VRF eng and VLAN 25 have not yet been created

Which command lists will satisfy the requirements with the least number of commands?

A)
```
vrf eng
vlan 25
interface vlan 25
ip address 10 105 43 1 255 255 255 0
ipv6 address fdOO 5708 f02d 404
vrf attach eng
```
B)
```
interface vlan 25
vrf attach eng
ip address 10 105 431/24
ipv6 address fdOO 5708 f02d 4df6 64
```
C)
```
interface vlan 25
vrf attach eng
ip address 10 105 43 1/24
IDv6 address fdOO 5708 f02d 4df6 64
```
D)
```
vrf eng
vlan 25
interface vlan 25
ip address 10.105.43 1/24
ipv6 address fdOO 5708 f02d 4df6 64
vrf attach eng
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:

The other options either use more commands or do not create the VRF or the VLAN.

Option C uses the following commands:

vrf eng: This command creates a VRF named eng and enters the VRF configuration mode1.

vlan 25: This command creates a VLAN with ID 25 and enters the VLAN configuration mode2.

interface vlan 25: This command creates an SVI on VLAN 25 and enters the interface configuration mode3.

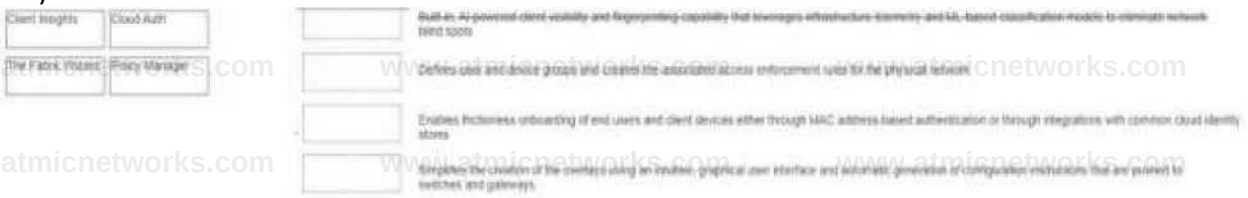
ip address 10.105.43.1/24 ipv6 address fd00:5780::102d:4df6/64 vrf attach eng: This command assigns an IPv4 address of 10.105.43.1 with a subnet mask of 255.255.255.0 and an IPv6 address of fd00:5780::102d:4df6 with a prefix length of 64 to the SVI, and attaches it to the VRF eng.

Question: 48

DRAG DROP

Match the solution components of NetConductor (Options may be used more than once or not at

all.)



Answer:

Explanation:

Client Insights matches with Built in , AI powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML based classification models to eliminate network bling spots

Client Insights is a solution component of NetConductor that provides built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network blind spots. Client Insights uses machine learning to automatically detect, identify, and classify devices on the network, such as IoT devices, BYOD devices, or rogue devices. Client Insights also provides behavioral analytics and anomaly detection to monitor device performance and security posture. Client Insights helps network administrators gain visibility into the device landscape, enforce granular access policies, and troubleshoot issues faster. Reference: https://www.arubanetworks.com/products/network-management-operations/central/netconductor/ https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

Cloud Auth matches with Enables fictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores

Cloud Auth is a solution component of NetConductor that enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores. Cloud Auth is a cloud-native network access control (NAC) solution that is delivered via Aruba Central. Cloud Auth allows network administrators to define user and device groups, assign roles and policies, and enforce access control across wired and wireless networks. Cloud Auth supports MAC authentication for devices that do not support 802.1X, as well as integrations with cloud identity providers such as Azure AD, Google Workspace, Okta, etc. Reference: https://www.arubanetworks.com/products/network-management-operations/central/netconductor/ https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

The Fabric Wizard matches with Simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways

The Fabric Wizard is a solution component of NetConductor that simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways. The Fabric Wizard is a tool that allows network administrators to design, deploy, and manage overlay networks using VXLAN and EVPN protocols. The Fabric Wizard provides a graphical representation of the network topology, devices, and links, and allows users to drag and drop virtual components such as VRFs, VLANs, and subnets. The Fabric Wizard also generates the configuration commands for each device based on the user

input and pushes them to the switches and gateways via Aruba Central. Reference: https://www.arubanetworks.com/products/network-management- operations/central/netconductor/ https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

Policy Manager matches with Defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network

Policy Manager is a solution component of NetConductor that defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network. Policy Manager is a tool that allows network administrators to create and manage network policies based on user and device identities, roles, and contexts. Policy Manager uses Group Policy Identifier (GPID) to carry policy information in traffic for in-line enforcement. Policy Manager also integrates with Cloud Auth, ClearPass, or third-party solutions to provide flexible network access control. Reference: https://www.arubanetworks.com/products/network-management-operations/central/netconductor/ https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

Question: 49

What is one advantage of using OCSP vs CRLs for certificate validation?

A. reduces latency between the time a certificate is revoked and validation reflects this status
B. less complex to implement
C. higher availability for certificate validation
D. supports longer certificate validity periods

Answer: A

Explanation:

OCSP is a protocol that allows clients to query the CA or a trusted responder for the status of a specific certificate. OCSP requests and responses are smaller and faster than CRLs, and they can provide real-time information about the revocation status of a certificate12. CRLs are lists of all revoked certificates that are downloaded from the CA. CRLs can present issues, as they can become outdated and have to be downloaded frequently13. Therefore, OCSP reduces latency between the time a certificate is revoked and validation reflects this status.

Reference: 1 https://sectigostore.com/blog/ocsp-vs-crl-whats-the-difference/ 2 https://www.keyfactor.com/blog/what-is-a-certificate-revocation-list-crl-vs- ocsp/ 3 https://www.fortinet.com/resources/cyberglossary/ocsp

Question: 50

A customer wants to provide wired security as close to the source as possible The wired security must meet the following requirements:
-allow ping from the IT management VLAN to the user VLAN
-deny ping sourcing from the user VLAN to the IT management VLAN
The customer is using Aruba CX 6300s
What is the correct way to implement these requirements?

A. Apply an outbound ACL on the user VLAN allowing temp echo-reply traffic toward the IT management VLAN
B. Apply an inbound ACL on the user VLAN allowing icmp echo-reply traffic toward the IT management VLAN
C. Apply an inbound ACL on the user VLAN denying icmp echo traffic toward the IT management VLAN
D. Apply an outbound ACL on the user VLAN denying icmp echo traffic toward the IT management VLAN

Answer: C

Explanation:

An inbound ACL is applied to traffic entering a port or VLAN. An outbound ACL is applied to traffic leaving a port or

VLAN4. To deny ping sourcing from the user VLAN to the IT management VLAN, an inbound ACL on the user VLAN should be used to filter icmp echo traffic toward the IT management VLAN. Icmp echo-reply traffic is not needed to be allowed because it is already permitted by default5. Reference: 4 https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID- 9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html 5 https://techhub.hpe.com/eginfolib/Aruba/OS- CX_10.04/5200-6692/GUID-0C3A9D0F-6E5B-4E1A-AF3C-8D8B2F9C1A7B.html

Question: 51

In AOS 10. which session-based ACL below will only allow ping from any wired station to wireless clients but will not allow ping from wireless clients to wired stations"? The wired host ingress traffic arrives on a trusted port.

A. ip access-list session pingFromWired any user any permit
B. ip access-list session pingFromWired user any svc-icmp deny any any svc-icmp permit
C. ip access-list session pingFromWired any any svc-icmp permit user any svc-icmp deny
D. ip access-list session pingFromWired any any svc-icmp deny any user svc-icmp permit

Answer: D

Explanation:

A session-based ACL is applied to traffic entering or leaving a port or VLAN based on the direction of the session initiation. To allow ping from any wired station to wireless clients but not vice versa, a session-based ACL should be used to deny icmp echo traffic from any source to any destination, and then permit icmp echo-reply traffic from any source to user destination. The user role represents wireless clients in AOS 10. Reference: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200- 6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html
https://techhub.hpe.com/eginfolib/networking/docs/arubaos-switch/security/GUID-EA0A5B3C- FE4C-4B9B-BE1D-FE7D2B9F8C3A.html

Question: 52

The administrator notices that wired guest users that have exceeded their bandwidth limit are not

being disconnected Access Tracker in ClearPass indicates a disconnect CoA message is being sent to the AOS-CX switch.

An administrator has performed the following configuration

```
Access. config-# ip dnr hc#t cpps.ambatraining.com ll.IH.l»23 vrf zagjtt
Accesrliconfigi• radius-server boat cpp». arubat raining, cca bay plaintext arubal23 vrf sngmt
Access, config?# BIB group server radius eppo
Access 11 config-sg i • server eppa. arubatraining.ena vrf ngat
A.cessl ccnftg-sg l• exit
Access', (config)# sat accounting port-access start-step interm 5 group eppo
Accessl config)# radius ayn-author1ration client cppm.aruba training, cm secret-key plaintext arma123 vrf amt Access! <config? • radius dyn-authornatioa enable
```

What is the most likely cause of this issue?

A. Change of Authorization has not been globally enabled on the switch
B. The SSL certificate for CPPM has not been added as a trust point on the switch
C. There is a mismatch between the RADIUS secret on the switch and CPPM.
D. There is a time difference between the switch and the ClearPass Policy Manager

Answer: D

Explanation:

Change of Authorization (CoA) is a feature that allows ClearPass Policy Manager (CPPM) to send messages to network devices such as switches to change the authorization state of a user session. CoA requires that both CPPM and the network device support this feature and have it enabled. For AOS-CX switches, CoA must be globally enabled using the command radius-server coa enable. If CoA is not enabled on the switch, the disconnect CoA message from CPPM will be ignored and the user session will not be terminated. Reference: https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/index.htm#CPPM_UserGuide/Admin/ChangeOfAuthorization.htm https://techhub.hpe.com/eginfolib/Aruba/OS- CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html

Question: 53

DRAG DROP

What is the order of operations tor Key Management service for a wireless client roaming from AP1 to AP2?

```
Opwrton                                   (Mw
Cent Bw eletti rfwraunr
CMMaMKMM M MMnXMMIOAPI
Gmr* Awrae MaM Ko km k> *?n wgnun
3>w< P><M« ■.<»!«• <e> Mngw«VIANinailW<RM»t!<a.APi
```

li

Answer

Explanation:

Order

https://www.arubanetworks.com/techdocs/Instant_85_WebHelp/Content/instant-ug/wlan-ssid- conf/conf-fast-roam.htm

Question: 54

A customer is looking Tor a wireless authentication solution for all of their IoT devices that meet the following requirements

- The wireless traffic between the IoT devices and the Access Points must be encrypted
- Unique passphrase per device
- Use fingerprint information to perform role-based access

Which solutions will address the customer's requirements? (Select two.)

A. MPSK and an internal RADIUS server
B. MPSK Local with MAC Authentication
C. ClearPass Policy Manager
D. MPSK Local with EAP-TLS
E. Local User Derivation Rules

Answer: CD

Explanation:

The correct answers are C and D.

MPSK (Multi Pre-Shared Key) is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices1. MPSK requires MAC authentication against a ClearPass Policy Manager server, which returns the encrypted passphrase for the device in a RADIUS VSA2. ClearPass Policy Manager is a platform that provides role- and device-based network access control for any user across any wired, wireless and VPN infrastructure3. ClearPass Policy Manager can also use device profiling and posture assessment to assign roles based on device fingerprint information4. MPSK Local is a variant of MPSK that allows the user to configure up to 24 PSKs per SSID locally on the device, without requiring ClearPass Policy Manager5. MPSK Local can be combined with EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), which is a secure authentication method that uses certificates to encrypt the wireless traffic between the IoT devices and the access points6. EAP-TLS can also use device certificates to perform role-based access control6.

Therefore, both ClearPass Policy Manager and MPSK Local with EAP-TLS can meet the customer's requirements for wireless authentication, encryption, unique passphrase, and role-based access for their IoT devices.

MPSK and an internal RADIUS server is not a valid solution, because MPSK does not support internal RADIUS servers and requires ClearPass Policy Manager789. MPSK Local with MAC Authentication is not a valid solution, because MAC Authentication does not encrypt the wireless traffic or use fingerprint information for role-based access2. Local User Derivation Rules are not a valid solution, because they do not provide unique passphrase per device or use fingerprint information for rolebased access101112.

Question: 55

You are troubleshooting an issue with a pair of Aruba CX 8360 switches configured with VSX Each switch has multiple VRFs. You need to find the IP address of a particular client device with a known MAC address You run the "show arp" command on the primary switch in the pair but do not find a matching entry for the client MAC address.

The client device is connected to an Aruba CX 6100 switch by VSX LAG.

Which action can be used to find the IP address successfully?

A)
Run the following command on the CX 6100 switch
shew mac-address-table

B)
Run the following command on the VSX primary switch
show am all-vrfs

C)
Run the following command on the VSX primary switch
show mac-address-table

D)
Run the following command on the CX 6100 switch
show am all-vrfs

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

Explanation:

The show arp command displays the ARP table for a specific VRF or all VRFs on the switch. The ARP table contains the IP address to MAC address mappings for hosts that are directly connected to the switch or reachable through a gateway. If the client device is connected to another switch by VSX LAG, the ARP entry for the client device will not be present on the primary switch unless it has communicated with it recently. Therefore, to find the IP address of the client device, the administrator should run the show arp command on the secondary switch in the VSX pair, specifying the VRF name that contains the client device's subnet. Reference: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html

Question: 56

Which statements regarding Aruba NAE agents are true? (Select two)

A. A single NAE script can be used by multiple NAE agents
B. NAE agents are active at all times
C. NAE agents will never consume more than 10% of switch processor resources
D. NAE scripts must be reviewed and signed by Aruba before being used E. A single NAE agent can be used by multiple NAE scripts.

Answer: AC

Explanation:

The statements that are true regarding Aruba NAE agents are A and C.

A) A single NAE script can be used by multiple NAE agents. This means that you can create different instances of the same script with different parameters or settings. For example, you can use the same script to monitor different VLANs or interfaces on the switch1.

C) NAE agents will never consume more than 10% of switch processor resources. This is a built-in safeguard that prevents the agents from affecting the switch performance or stability. If an agent exceeds the 10% limit, it will be automatically disabled and an alert will be generated2.

The other options are incorrect because:

B) NAE agents are not active at all times. They can be enabled or disabled by the user, either manually or based on a schedule. They can also be disabled automatically if they encounter an error or exceed the resource limit1.

D) NAE scripts do not need to be reviewed and signed by Aruba before being used. You can create your own custom scripts using Python and upload them to the switch or Aruba Central. You can also use the scripts provided by Aruba or other sources, as long as they are compatible with the switch firmware version1.

E) A single NAE agent cannot be used by multiple NAE scripts. An agent is an instance of a script that runs on the switch. Each agent can only run one script at a time1.

Question: 57

What is an OSPF transit network?

A. a network that uses tunnels to connect two areas
B. a special network that connects two different areas
C. a network on which a router discovers at least one neighbor
D. a network that connects to a different routing protocol

Answer: A

Explanation:

An OSPF transit network is a network that has at least two routers that are connected by a multiaccess link and can forward traffic for other networks1. A transit network is different from a stub network, which has only one router connected to it and does not forward traffic for other networks2. A transit network is also different from a virtual link, which is a logical connection between two areas that are not physically adjacent2. A transit network is not necessarily connected to a different routing protocol, although it can be if the router performs redistribution2.

Therefore, the correct answer is C. A network on which a router discovers at least one neighbor.

Question: 58

Describe the difference between Class of Service (CoS) and Differentiated Services Code Point (DSCP).

A. CoS has much finer granularity than DSCP

B. CoS is only contained in VLAN Tag fields DSCP is in the IP Header and preserved throughout the IP packet flow

C. They are similar and can be used interchangeably.

D. CoS is only used to determine CLASS of traffic DSCP is only used to differentiate between different Classes.

Answer: B

Explanation:

CoS and DSCP are both methods of marking packets for quality of service (QoS) purposes. QoS is a mechanism that allows network devices to prioritize and differentiate traffic based on certain criteria, such as application type, source, destination, etc. CoS stands for Class of Service and is a 3- bit field in the 802.1Q VLAN tag header. CoS can only be used on Ethernet frames that have a VLAN tag, and it can only be preserved within a single VLAN domain. DSCP stands for Differentiated Services Code Point and is a 6-bit field in the IP header. DSCP can be used on any IP packet, regardless of the underlying layer 2 technology, and it can be preserved throughout the IP packet flow, unless it is modified by intermediate devices. Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-mt/qos-15-mt-book/qos-overview.htmlhttps://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741- 4.html https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet- marking/10103-dscpvalues.html

Question: 59

A network administrator is troubleshooting some issues guest users are having when connecting and authenticating to the network The access switches are AOS-CX switches.
What command should the administrator use to examine information on which role the guest user has been assigned?

A. show aaa authentication port-access interface all client-status

B. show port-access captiveportal profile

C. show port-access role

D. diag-dump captiveportal client verbose

Answer: A

Explanation:

The show aaa authentication port-access interface all client-status command displays the status of all clients authenticated by port-based access control on all interfaces. The output includes the MAC address, user role, VLAN ID, and session timeout for each client. This command can be used to examine information on which role the guest user has been assigned by the AOS-CX switch.
Reference: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html

Question: 60

Using Aruba best practices what should be enabled for visitor networks where encryption is needed

but authentication is not required?

A. Wi-Fi Protected Access 3 Enterprise
B. Opportunistic Wireless Encryption
C. Wired Equivalent Privacy
D. Open Network Access

Answer: B

Explanation:

Opportunistic Wireless Encryption (OWE) is a feature that provides encryption for open wireless networks without requiring authentication. OWE uses an enhanced version of the 4-way handshake to establish a pairwise key between the client and the AP, which is then used to encrypt the wireless traffic using WPA2 or WPA3 protocols. OWE can be used for visitor networks where encryption is needed but authentication is not required.

Reference: https://www.arubanetworks.com/assets/tg/TG_OWE.pdf

Question: 61

Which statements are true about VSX LAG? (Select two.)

A. The total number of configured links may not exceed 8 for the pair or 4 per switch
B. Outgoing traffic is switched to a port based on a hashing algorithm which may be either switch in the pair
C. LAG traffic is passed over VSX ISL links only while upgrading firmware on the switch pair
D. Outgoing traffic is preferentially switched to local members of the LAG.
E. Up to 255 VSX lags can be configured on all 83xx and 84xx model switches.

Answer: AD

Explanation:

The correct answers are A and D.

According to the web search results, VSX LAG is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices1. VSX LAGs span both aggregation switches and appear as one device to partner downstream or upstream devices or both when forming a LAG with the VSX pair2.

One of the statements that is true about VSX LAG is that the total number of configured links may not exceed 8 for the pair or 4 per switch1. This means that a VSX LAG across a downstream switch can have at most a total of eight member links, and a switch can have a maximum of four member links. When creating a VSX LAG, it is recommended to select an equal number of member links in each segment for load balancing1.

Another statement that is true about VSX LAG is that outgoing traffic is preferentially switched to local members of the LAG2. This means that when active forwarding and active gateway are enabled, north-south and south-north traffic bypasses the ISL link and uses the local ports on the switch. This optimizes the traffic path and reduces the load on the ISL link2.

The other statements are false or not relevant for VSX LAG. Outgoing traffic is not switched to a port based on a hashing algorithm, which may be either switch in the pair. This is a characteristic of MLAG (Multi-Chassis Link Aggregation), which is a different feature from VSX LAG. LAG traffic is not passed over VSX ISL links only while upgrading firmware on the switch pair. This is a scenario that may occur when performing hitless upgrades, which is a feature that allows software updates without impacting network availability. The number of

VSX lags that can be configured on all 83xx and 84xx model switches is not 255, but depends on the switch model and firmware version. For example, the AOS-CX 10.04 supports up to 64 VSX lags for 8320 switches and up to 128 VSX lags for 8325 and 8400 switches.

Question: 62

What steps are part of the Key Management workflow when a wireless device is roaming from AP1 to AP2? (Select two.)

A. AP1 will cache the client's information and send it to the Key Management service
B. The Key Management service receives from AirMatch a list of all AP2's neighbors
C. The Key Management service receives a list of all AP1 s neighbors from AirMatch.
D. The Key Management service then generates R1 keys for AP2's neighbors.
E. A client associates and authenticates with the AP2 after roaming from AP1

Answer: AD

Explanation:

The correct steps that are part of the Key Management workflow when a wireless device is roaming from AP1 to AP2 are A and D.

A) AP1 will cache the client's information and send it to the Key Management service. This is true because when a client associates and authenticates with AP1, AP1 will generate a pairwise master key (PMK) for the client and store it in its cache. AP1 will also send the PMK and other client information, such as MAC address, VLAN, and SSID, to the Key Management service, which is a centralized service that runs on Aruba Mobility Controllers (MCs) or Mobility Master (MM) devices1. The Key Management service will use this information to facilitate fast roaming for the client.

D) The Key Management service then generates R1 keys for AP2's neighbors. This is true because when the Key Management service receives the client information from AP1, it will use the PMK to derive R0 and R1 keys for the client. R0 keys are used to generate R1 keys, which are used to generate pairwise transient keys (PTKs) for encryption. The Key Management service will distribute the R1 keys to AP2 and its neighboring APs, which are determined by AirMatch based on RF proximity2. This way, when the client roams to AP2 or any of its neighbors, it can skip the 802.1X authentication and use the R1 key to quickly generate a PTK with the new AP3.

B) The Key Management service receives from AirMatch a list of all AP2's neighbors. This is false because the Key Management service does not receive this information from AirMatch directly. AirMatch is a feature that runs on MCs or MM devices and optimizes the RF performance of Aruba devices by using machine learning algorithms. AirMatch periodically sends neighbor reports to all APs, which contain information about their nearby APs based on signal strength and interference. The APs then send these reports to the Key Management service, which uses them to determine which APs should receive R1 keys for a given client2.

C) The Key Management service receives a list of all AP1 s neighbors from AirMatch. This is false for the same reason as B. The Key Management service does not receive this information from AirMatch directly, but from the APs that send their neighbor reports.

E) A client associates and authenticates with the AP2 after roaming from AP1. This is false because a client does not need to authenticate with AP2 after roaming from AP1 if it has already authenticated with AP1 and received R1 keys from the Key Management service. The client only needs to associate with AP2 and perform a four-way handshake using the R1 key to generate a PTK for encryption3. This is called fast roaming or 802.11r roaming, and it reduces the latency and disruption caused by full authentication.

1: ArubaOS 8.7 User Guide 2: ArubaOS 8.7 User Guide 3: ArubaOS 8.7 User Guide : ArubaOS 8.7 User Guide

Question: 63

What are two advantages of splitting a larger OSPF area into a number of smaller areas? (Select two)

A. It extends the LSDB
B. It increases stability
C. it simplifies the configuration.
D. It reduces processing overhead.
E. It reduces the total number of LSAs

Answer: B, D

Explanation:

Splitting a larger OSPF area into a number of smaller areas has several advantages for network scalability and performance. Some of these advantages are:

It increases stability by limiting the impact of topology changes within an area. When a link or router fails in an area, only routers within that area need to run the SPF algorithm and update their routing tables. Routers in other areas are not affected by the change and do not need to recalculate their routes.

It reduces processing overhead by reducing the size and frequency of link-state advertisements (LSAs). LSAs are packets that contain information about the network topology and are flooded within an area. By dividing a network into smaller areas, each area has fewer LSAs to generate, store, and process, which saves CPU and memory resources on routers.

It reduces bandwidth consumption by reducing the amount of routing information exchanged between areas. Routers that connect different areas, called area border routers (ABRs), summarize the routing information from one area into a single LSA and advertise it to another area. This reduces the number of LSAs that need to be transmitted across area boundaries and saves network bandwidth.

Reference: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.htmlhttps://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html

Question: 64

Your Aruba CX 6300 VSF stack has OSPF adjacency over SVI 10 with LAG 1 to a neighboring device The following configuration was created on the switch:

```
vlan 20,30,40

interface vlan 20
        in address 10.10.20.1/24

interface vlan 30
        in address 10.10.32.1/24

interface vlan 40
        ID address IC.10.42.1 24
```

A)

```
vlan 20. 30,40
    ospf passive
```

B)

```
Interface vlan 20 30 40
    ip ospf passive
```

C)

```
router ospf 1
  area 0
   passive-interface
    vlan 20.30.40
```

D)

```
router ospf 1
    area 0
        redistribute local
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

Explanation:

OSPF (Open Shortest Path First) is a routing protocol that uses link-state information to calculate the best path to each destination in the network. OSPF establishes adjacencies with neighboring routers to exchange routing information and maintain a consistent view of the network topology1.

To establish an OSPF adjacency, the routers need to have some common parameters, such as the area ID, the network type, the hello interval, the dead interval, and the authentication method2. The routers also need to have a matching subnet mask on the interface that connects them3.

In this case, the Aruba CX 6300 VSF stack has an SVI (Switched Virtual Interface) on VLAN 10 with an IP address of 10.1.1.1/24 and a LAG (Link Aggregation Group) on port 1/1/1 and port 2/1/1 that connects to a neighboring device. The SVI is configured with OSPF area 0 and network type broadcast. The LAG is configured with OSPF passive mode, which means that it will not send or receive OSPF hello packets.

The neighboring device has an interface with an IP address of 10.1.1.2/24 and a LAG on port 1/0/1 and port 2/0/1 that connects to the Aruba CX 6300 VSF stack. The interface is configured with OSPF area 0 and network type broadcast.

Since the Aruba CX 6300 VSF stack and the neighboring device have the same area ID, network type, subnet mask, and default hello and dead intervals on their interfaces, they will be able to establish an OSPF adjacency over SVI 10 with LAG 1. The OSPF passive mode on the LAG will not affect the adjacency, because it only applies to the LAG interface, not the SVI interface.

Question: 65

Which feature allows the device to remain operational when a remote link failure occurs between a Gateway cluster and a RADIUS server that is either in the cloud or a datacenter?

A. MAC caching

B. MAC Authentication
C. Authentication survivability
D. Opportunistic key caching

Answer: C

Explanation:

Authentication survivability is a feature that allows the device to remain operational when a remote link failure occurs between a Gateway cluster and a RADIUS server that is either in the cloud or a datacenter. Authentication survivability enables the Gateway cluster to cache successful authentication requests from the RADIUS server and use them to authenticate clients when the RADIUS server is unreachable. Authentication survivability also allows clients to use MAC caching or MAC authentication bypass (MAB) methods to access the network when the RADIUS server is down. Reference: https://www.arubanetworks.com/assets/tg/TG_AuthSurvivability.pdf

Question: 66

The customer needs a network hardware refresh to replace an aging Aruba 5406R core switch pair using spanning tree configuration with Aruba CX 8360-32YC switches What is the benefit of VSX clustering with the new solution?

A. stacked data-plane
B. faster MSTP converge processing
C. dual Aruba AP LAN port connectivity for PoE redundancy
D. dual control plane provides better resiliency

Answer: D

Explanation:

VSX clustering is a feature that allows two Aruba CX switches to operate as a single logical device, providing high availability, scalability, and simplified management. VSX clustering has several

benefits over spanning tree configuration, such as:
Dual control plane provides better resiliency. Unlike stacking, where switches share a single control plane, VSX switches have independent control planes that synchronize their states over an interswitch link (ISL). This means that if one switch fails or reboots, the other switch can continue to operate without affecting traffic flows or network services.
Active-active forwarding provides better performance. Unlike spanning tree, where some links are blocked to prevent loops, VSX switches use all available links for forwarding traffic, providing load balancing and increased bandwidth utilization.
Multichassis LAG provides better redundancy. Unlike single-chassis LAG, where all member ports belong to one switch, VSX switches can form multichassis LAGs with downstream or upstream devices, where member ports are distributed across both switches. This provides link redundancy and seamless failover in case of switch or port failure.
Reference: https://www.arubanetworks.com/assets/tg/TG_VSX.pdf

Question: 67

A customer has a large number of food-producing machines

- All machines are connected via Aruba CX6200 switches in VLANs 100.110. and 120
- Several external technicians are maintaining this special equipment

What are the correct commands to ensure that no rogue DHCP server will impact the network?

A)

```
dhcp-snooping enable
no dhcp-snooping option 82
dhcp-snoopmg vlan 100-120
vlan 100
    name cornflakes
vlan 110
    name cornmill
vlan 120
    name packaging

interface lag 1 no shutdown description uplink-to-Core no routing vlan trunk native 1
    vlan trunk allowed all lacp mode active dhco-snooDina trust
```

B)

```
dhcp snooping enable
no dhcp-snooping option 82
vlan 100
    name cornflakes
    dhcp-snooping
vlan 110
    name commill dhcp-snooping
vlan 120
    name packaging dhcp-snooping
interface lag 1 no shutdown
    description Uphnk-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all lacp mode active dhcp snooping trust
```

C)

```
dhcpv4-snooping all vlans
no dhcpv4-snooping option 82
interface lag 1
    no shutdown
    descnption Uplmk-to-Core
    no routing
    vlan trunk native 1 vlan trunk allowed all lacp mode active dhcpv4-snoopinq trust
```

D)

```
dhcpv4-snoopmg
no dhcpv4-snooping option 82 vlan 100
    name cornflakes dbcpv4-snooping vlan 110
```

name cornmill
dhcpv4-snooping
vlan 120
name packaging
dhcpv4-snocping
interface lag 1 no shutdown
descnption Uplink-to-Core no routing vlan trunk native 1 vlan trunk allowed all lacp mode active dhcnvi-snonninn trust

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

Explanation:

configures DHCP snooping on the switch and enables it for VLANs 100, 110, and 120. It also specifies the IP address of the authorized DHCP server and sets the ports connected to the server as trusted. This prevents any unauthorized DHCP server from providing invalid configuration data to the clients on those VLANs. Option B also enables DHCP option-82, which adds information about the switch port and VLAN to the DHCP packets, allowing for more granular control and logging of DHCP transactions.

Question: 68

For the Aruba CX 6400 switch, what does virtual output queueing (VOQ) implement that is different from most typical campus switches?

A. large ingress packet buffers
B. large egress packet buffers
C. per port ASICs
D. VSX

Answer: A

Explanation:

The Aruba CX 6400 switch is a modular switch that supports high-performance and high-density Ethernet switching for campus and data center networks. One of the features that distinguishes the Aruba CX 6400 switch from most typical campus switches is virtual output queueing (VOQ). VOQ is a technique that implements large ingress packet buffers on each port to prevent head-of-line blocking and packet loss due to congestion2. VOQ allows each port to have multiple queues for different output ports and prioritize packets based on their destination and QoS class2. VOQ enables the Aruba CX 6400 switch to achieve high throughput and low latency for various traffic types and scenarios. Reference: 2 https://www.arubanetworks.com/assets/ds/DS_CX6400Series.pdf

Question: 69

Which statement best describes QoS?

A. Determining which traffic passes specified quality metrics
B. Scoring traffic based on the quality of the contents
C. Identifying specific traffic for special treatment
D. Identifying the quality of the connection

Answer: A

Explanation:

QoS stands for Quality of Service and is a mechanism that allows network devices to prioritize and differentiate traffic based on certain criteria, such as application type, source, destination, etc3. QoS involves identifying specific traffic for special treatment and applying policies and actions to improve its performance or meet certain service level agreements (SLAs)3. QoS can help network devices to manage congestion, delay, jitter, packet loss, bandwidth allocation, etc., for different types of traffic3. QoS can be implemented at various layers of the network stack and across different network domains. Reference: 3 https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15- mt/qos-15-mt-book/qos-overview.html

Question: 70

DRAG DROP

Select the Aruba stacking technology matching each option (Options may be used more than once or not at all.)

7SF CSX

MtW AI*!

,. ..Mwah.*., ua»ut ah a»

[1] Inomdua ISL mu up In MOG ait supported

[1] inaxrtiue ist mu up to SOO ate suppottwi

A maximum aggregate ISL bandwidth of 200G is supported

Answer:

Explanation:

a) Support up to 10 devices per stack -> VSF
b) Support two devices per stack -> VSX
c) Individual ISL links up to 400G are supported -> VSX
d) individual ISL links up to 50G are supported -> VSF
e) A maximum aggregate ISL bandwidth of 200G is supported -> VSF

Reference: 1 https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/GUID-2E425DAE-EC54-4313-9DEA-A61817F903C0.html

Question: 71

A network engineer recently identified that a wired device connected to a CX Switch is misbehaving on the network To address this issue, a new ClearPass policy has been put in place to prevent this device from connecting to the network again.

Which steps need to be implemented to allow ClearPass to perform a CoA and change the access for this wired device? (Select two.)

A. Confirm that NTP is configured on the switch and ClearPass
B. Configure dynamic authorization on the switch.
C. Bounce the switchport

D. Use Dynamic Segmentation.

E. Configure dynamic authorization on the switchport

Answer: BC

Explanation:

CoA (Change of Authorization) is a feature that allows ClearPass to dynamically change the authorization and access privileges of a device after it has been authenticated1. CoA uses RADIUS messages to communicate with the network device and instruct it to perform an action, such as reauthenticating the device, applying a new VLAN or user role, or disconnecting the device2.

To enable CoA on a CX switch, the network engineer needs to configure dynamic authorization on the switch, which is a global command that allows the switch to accept RADIUS messages from ClearPass and execute the requested actions3. The network engineer also needs to specify the IP address and shared secret of ClearPass as a dynamic authorization client on the switch3.

To trigger CoA for a specific wired device, the network engineer needs to bounce the switchport, which is an action that temporarily disables and re-enables the port where the device is connected. This forces the device to reauthenticate and receive the new policy from ClearPass. Bouncing the switchport can be done manually by using the interface shutdown and no shutdown commands, or automatically by using ClearPass as a CoA server and sending a RADIUS message with the PortBounce-Host AVP (Attribute-Value Pair).

Question: 72

A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working across the campus which is connected via layer-3. The legacy devices are connected to Aruba CX 6300 switches throughout the campus.

Which technology minimizes flooding so the legacy application can work efficiently?

A. Generic Routing Encapsulation (GRE)
B. EVPN-VXLAN
C. Ethernet over IP (EoIP)
D. Static VXLAN

Answer: B

Explanation:

EVPN-VXLAN is a technology that allows layer-2 communication across layer-3 networks by using Ethernet VPN (EVPN) as a control plane and Virtual Extensible LAN (VXLAN) as a data plane3. EVPN- VXLAN can be used to support legacy applications that communicate at layer-2 across different campuses or data centers that are connected via layer-3. EVPN-VXLAN minimizes flooding by using BGP to distribute MAC addresses and IP addresses of hosts across different VXLAN segments3. EVPN- VXLAN also provides benefits such as loop prevention, load balancing, mobility, and scalability3.
Reference: 3 https://www.arubanetworks.com/assets/tg/TG_EVPN_VXLAN.pdf

Question: 73

DRAG DROP
Match the terms below to their characteristics (Options may be used more than once or not at all.)

Answer:

Explanation:

a) A device with IP address 10.1.3.7 in a network wants to send the traffic stream to a device with IP address 10.13.4.2 in the other network -> Unicast
b) One/more senders and one/more recipients participate in data transfer traffic -> Multicast
c) Sent to all hosts on a remote network -> IP Directed Broadcast
d) Sent to all NICs on the same network segment as the source NIC -> Broadcast
Reference: 1 https://www.thestudygenius.com/unicast-broadcast-multicast/

The terms broadcast, IP directed broadcast, multicast, and unicast are different types of communication or data transmission over a network. They differ in how many devices are involved in the communication and how they address the messages. The following table summarizes the characteristics of each term1:

Term	Definition	Example
Broadcast	One-to-all communication, where data is sent to every device on the network	A device with IPaddress 10.1.3.7 sends a DHCP request to 255.255.255.255

IP Directed Broadcast	One-to-all communication, where data is sent to all hosts on a remote network	A device with IP address 10.1.3.7 sends a ping request to 10.13.4.255
Multicast	One-to-many or many-to-many communication, where data is sent to a group of devices that have joined a multicast group	A device with IP address 10.1.3.7 sends a video stream to 239.0.0.1
Unicast	One-to-one communication, where data is sent to only one device	A device with IP address 10.1.3.7 sends an email to a device with IP address 10.13.4.2

Question: 74

Due to a shipping error, five (5) Aruba AP-515S and one (1) Aruba CX 6300 were sent directly to your new branch office You have configured a new group persona for the new branch office devices in Central, but you do not know their MAC addresses or serial numbers The office manager is instructed via text message on their smartphone to onboard all the new hardware into Aruba Central What application must the office manager use on their phone to complete this task?

A. Aruba Onboard App
B. Aruba Central App
C. Aruba CX Mobile App
D. Aruba installer App

Answer: D

Explanation:

Aruba Installer App is a mobile app that simplifies site installations and enables network connectivity for Aruba devices. The app allows the user to scan the barcode of the device and add it to the network using Aruba Central. The app also automates importing Aruba devices into Aruba NetEdit for intelligent configuration management and continuous conformance validation

Question: 75

DRAG DROP
List the WPA 4-Way Handshake functions in the correct order.

Answer:

Explanation:

Proves knowledge of the PMK Exchanges messages for generating PTK Distributes an encrypted GTK to the client Sets first initialization vector (IV)

Question: 76

What is used to retrieve data stored in a Management Information Base (MIS)?

SNMPv3

DSCP

TLV

CDP

Answer: A

Explanation:

The correct answer is

A. SNMPv3.

SNMPv3 is a protocol that is used to retrieve data stored in a Management Information Base (MIB), which is a database of managed objects in a network. SNMPv3 provides security and access control features that are not available in earlier versions of SNMP. SNMPv3 can also use encryption to protect the data from unauthorized access or modification.

According to the Aruba Certified Professional – Campus Access document1, one of the skills that this certification validates is:

Implement and Analyze the output from common network monitoring tools

Configure Port Mirroring to collect PCAPs

Configure NAE agents 9.4

Configure UXI sensors for internal and external tests

Describe how API scan be used to configure, manage, monitor, and troubleshoot your network

The document also mentions that the candidate should have a distinguished understanding of different protocols across vendors, which implies that they should be familiar with SNMPv3 and how it can be used to access MIB data.

Question: 77

you need to have different routing-table requirements With Aruba CX 6300 VSF configuration.

Assuming the correct layer-2 VLAN already exists, how would you create a new SVI for a separate routing table?

A. create a new VLAN, and attach the VRF to it.

B. Create a new routing table, and attach VLANS to it

C. Create a new SVI and use attach command.

D. Create a new VLAN. and attach the routing table to it

Answer: C

Explanation:

The correct answer is C. Create a new SVI and use attach command.
To create a new SVI for a separate routing table, you need to use the attach command to associate the SVI with a VRF (Virtual Routing and Forwarding) instance. A VRF is a logical entity that allows multiple routing tables to coexist on the same switch. Each VRF has its own set of interfaces, routing protocols, and routes that are isolated from other VRFs.

According to the AOS-CX Virtual Switching Framework (VSF) Guide1, one of the steps to configure VRF-aware VSF is:

Configure the VRFs on each member switch and assign the SVIs to the respective VRFs using the attach command. For example: switch(config)# vrf red switch(config-vrf)# exit switch(config)# interface vlan 10 switch(config-if-vlan)# ip address 10.1.1.1/24 switch(config-if-vlan)# attach vrf red

The above commands create a VRF named red and assign VLAN 10 SVI to it. The SVI has an IP address of 10.1.1.1/24.

The other options are incorrect because:

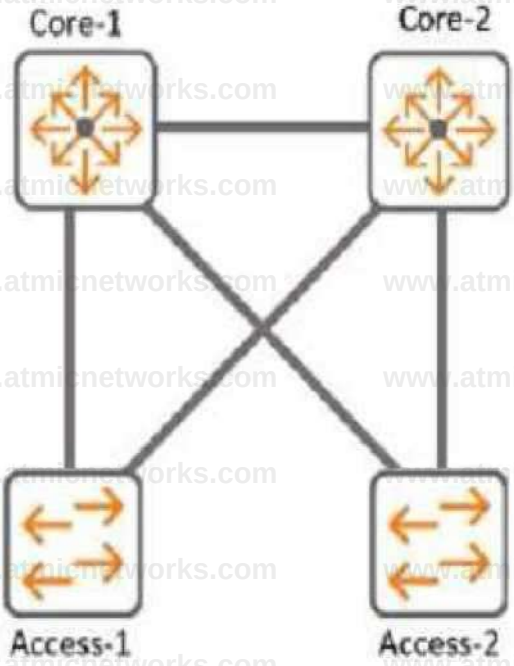
A) You cannot attach a VRF to a VLAN directly. You need to create an SVI for the VLAN and then attach the VRF to the SVI.

B) You cannot create a new routing table manually. You need to create a VRF and then use routing protocols or static routes to populate the routing table for the VRF.

D) You cannot attach a routing table to a VLAN directly. You need to create an SVI for the VLAN and then attach a VRF that has a routing table associated with it.

Question: 78

Refer to Exhibit:



With Access-1, What needs to be identically configured With MSTP to load-balance VLANS?

A. Spanning-tree bpdu-guard setting

B. Spanning-tree instance vlan mapppjng

C. spanning-tree Cist mapping

D. Spanning-tree root-guard setting

Answer: B

Explanation:

The correct answer is B. Spanning-tree instance VLAN mapping.

To load-balance VLANs with MSTP, you need to configure the same VLAN-to-instance mapping on all switches in the same MST region. This means that you need to assign different VLANs to different MST instances, and then adjust the spanning tree parameters (such as priority, cost, or port role) for each instance to achieve the desired load balancing. For example, you can make one switch the root for instance 1 and another switch the root for instance 2, and then map half of the VLANs to instance 1 and the other half to instance 2.

According to the Cisco document Understand the Multiple Spanning Tree Protocol (802.1s), one of the steps to configure MST is:

Split your set of VLANs into more instances and configure different MST settings for each of these instances. In order to easily achieve this, elect Bridge D1 to be the root for VLANs 501 through 1000, and Bridge D2 to be the root for VLANs 1 through 500. These statements are true for this configuration:

Switch D1(config)#spanning-tree mst configuration

Switch D1(config-mst)#instance 1 vlan 501-1000

Switch D1(config-mst)#exit

Switch D1(config)#spanning-tree mst 1 priority 0

Switch D2(config)#spanning-tree mst configuration

Switch D2(config-mst)#instance 2 vlan 1-500

Switch D2(config-mst)#exit
Switch D2(config)#spanning-tree mst 2 priority 0
The above commands create two MST instances, 1 and 2, and map VLANs 501-1000 to instance 1 and VLANs 1-500 to instance 2. Then, they make switch D1 the root for instance 1 and switch D2 the root for instance 2.
The other options are incorrect because:

A) Spanning-tree bpdu-guard setting is a security feature that disables a port if it receives a BPDU from an unauthorized device. It does not affect load balancing with MSTP.
C) Spanning-tree CIST mapping is not a valid command. CIST stands for Common and Internal Spanning Tree, which is the spanning tree instance that runs within an MST region and interacts with other regions or non-MST switches.
D) Spanning-tree root-guard setting is another security feature that prevents a port from becoming a root port if it receives superior BPDUs from another switch. It does not affect load balancing with MSTP.

Question: 79

your customer has asked you to assign a switch management role for a new user The customer requires the user role to View switch configuration information and have access to the PUT and POST meth0ds for REST API.

Which default AOS-CX user role meets these requirements?

A. administrators
B. auditors
C. sysops
D. helpdesk

Answer: C

Explanation:

The correct answer is C. sysops.
The sysops user role is a predefined role that allows users to view switch configuration information and have access to the PUT and POST methods for REST API. The sysops user role can also use the PATCH and DELETE methods for REST API, but not for all resources. The sysops user role is suitable for users who need to perform system operations on the switch, such as backup, restore, upgrade, or reboot.
According to the AOS-CX REST API Reference basics1, one of the predefined user roles is: sysops: Users with this role can view switch configuration information and have access to the PUT and POST methods for REST API. They can also use the PATCH and DELETE methods for REST API, but not for all resources. Users with this role can perform system operations on the switch, such as backup, restore, upgrade, or reboot.
The other options are incorrect because:
A) administrators: Users with this role have full access to all switch configuration information and all REST API methods. This role is more than what the customer requires.
B) auditors: Users with this role can only view switch configuration information and have access to the GET method for REST API. They cannot use the PUT and POST methods for REST API.
D) helpdesk: Users with this role can view switch configuration information and have access to the GET method for REST API. They can also use the PATCH method for REST API, but only for a limited set of resources. They cannot use the PUT and POST methods for REST API.

Question: 80

How is Dynamic Multicast Optimization (DMO) implemented in an HPE Aruba wireless network?

DMO is configured individually tor each SSID in use in the network.

The AP uses OOS to provide equal air time for multicast traffic,

DMO is configured globally for each SSID in use in the network.

The controller converts multicast streams into unicast streams.

Answer: A

Explanation:

The correct answer is

A. DMO is configured individually for each SSID in use in the network.

DMO is a feature that allows the AP to convert multicast streams into unicast streams over the wireless link. This enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. DMO is configured individually for each SSID in use in the network, as different SSIDs may have different multicast requirements.

According to the Aruba document Configuring WLAN Settings for an SSID Profile, one of the steps to configure DMO is:

Dynamic multicast optimization: Select Enabled to allow IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. The other options are incorrect because:

B. The AP does not use QoS to provide equal air time for multicast traffic. QoS is a feature that prioritizes different types of traffic based on their importance and latency sensitivity. QoS does not affect how multicast streams are transmitted over the wireless link.

C. DMO is not configured globally for each SSID in use in the network. DMO is configured individually for each SSID, as different SSIDs may have different multicast requirements.

D. The controller does not convert multicast streams into unicast streams. The AP does the conversion, as it is closer to the wireless clients and can optimize the transmission based on the client capabilities and channel conditions.

Question: 81

With the Aruba CX switch configuration, what is the Active Gateway feature that is used for and is unique to VSX configuration?

A. Sixteen different VMACs are supported total as shared.

B. Active Gateway can once MSTP instances are created for VLAN load sharing.

C. Sixteen different VMACS are supported for each IPV4 and IPV6 stack simultaneously

D. copied over the ISL link for an optimized path.

Answer: C

Explanation:

The active gateway feature is used to provide active-active layer 3 default gateway for hosts on the same subnet. It allows the switch to convert multicast streams into unicast streams over the wireless link, which improves the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. The active gateway feature is unique to VSX configuration because it eliminates the need for VRRP and avoids traffic being pushed over the ISL link, which can cause latency in the network12.

The correct answer to the question is C. Sixteen different VMACs are supported for each IPv4 and IPv6 stack simultaneously. This means that you can have a maximum of eight VMACs for IPv4, and a maximum of eight VMACs for IPv6, on a VSX pair. Only 15 VMACs are supported on 6400 switch series2.

The other options are incorrect because:

A) Sixteen different VMACs are not supported total as shared. They are supported for each IPv4 and IPv6 stack separately.

B) Active gateway can be used without MSTP instances. MSTP is a protocol that allows multiple spanning tree instances to coexist on the same switch, but it does not affect how active gateway works.

D) Active gateway does not copy traffic over the ISL link for an optimized path. It avoids using the ISL link for routed traffic and uses the local switch interface MAC instead of the virtual MAC address (VMAC) for source address1.

Question: 82

What is a primary benefit of BSS coloring?

A. BSS color tags improve performance by allowing APS on the same channel to be farther apart

B. BSS color tags improve security by identifying rogue APS and tagging them as threats.

C. BSS color tags are applied on the wireless controllers and can reduce the threshold for interference

D. BSS color tags are applied to WI-Fi channels and can reduce the threshold tor interference

Answer: D

Explanation:

The primary benefit of BSS coloring is D. BSS color tags are applied to Wi-Fi channels and can reduce the threshold for interference.

BSS coloring is a mechanism that allows Wi-Fi 6 devices to mark each frame with a color code that identifies the BSS (Basic Service Set) it belongs to. This helps differentiate between frames from

different BSSs that share the same channel and avoid unnecessary collisions and backoffs. BSS coloring also introduces an adaptive threshold for interference, which means that Wi-Fi 6 devices can adjust the signal strength value that determines whether a channel is busy or not based on the current network environment. This allows for more efficient use of spectrum and higher throughput in dense scenarios12.

Question: 83

Your Director of Security asks you to assign AOS-CX switch management roles to new employees based on their specific job requirements. After the configuration was complete, it was noted that a user assigned with the auditors role did not have the appropriate level of access on the switch.

The user was not allowed to perform firmware upgrades and a privilege level of 15 was not assigned to their role. Which default management role should have been assigned for the user?

A. sysadmin
B. sysops
C. administrators
D. config

Answer: B

Explanation:
The correct answer is B. sysops.
The sysops user role is a predefined role that allows users to perform system operations on the switch, such as backup, restore, upgrade, or reboot. The sysops user role also has access to the PUT and POST methods for REST API, which can be used to modify the switch configuration. The sysops user role has a privilege level of 15, which is the highest level of access on the switch1.
The other options are incorrect because:

A) sysadmin: The sysadmin user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The sysadmin user role does not have access to the REST API methods, and cannot perform firmware upgrades1.
C) administrators: The administrators user role is a predefined role that has full access to all switch configuration information and all REST API methods. This role is more than what the Director of Security requires1.
D) config: The config user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The config user role does not have access to the REST API methods, and cannot perform firmware upgrades1.

Question: 84

With the Aruba CX 6000 24G switch with uplinks of 1/1/25 and what does the switch do when a client port detects a loop and the do-not-disabie parameter is used?

A. Port status will be validated once status is cleared
B. An event log message is created.
C. The network analytics engine is triggered.
D. Port status led blinks in amber with 100hz.

Answer: B

Explanation:
The correct answer is B. An event log message is created.
The do-not-disable parameter is used to prevent the switch from disabling the port when a loop is detected by the loop-protect feature. Instead, the switch will generate an event log message that indicates the port number and the VLAN ID where the loop was detected. The switch will also send a trap to the SNMP manager, if configured1.
The other options are incorrect because:
A) Port status will not be validated once status is cleared. The port will remain enabled even if a loop is detected, unless the loop-protect action is changed to tx-disable or tx-rx-disable1.
C) The network analytics engine will not be triggered by a loop detection. The network analytics engine is a feature that allows users to monitor and troubleshoot network issues using scripts and agents2.
D) Port status LED will not blink in amber with 100Hz. The port status LED will indicate the normal port status, such as link speed and activity, regardless of the loop detection3.

Question: 85

You must ensure the HPEAruba network you are configuring for a client is capable of plug-and-play provisioning of access points. What enables this capability?

A. UCC Service
B. LLDP-MED
C. SRTP
D. CSMA

Answer: A

Explanation:

The capability that enables plug-and-play provisioning of access points in an HPE Aruba network is the UCC Service. The UCC Service is a cloud-based service that allows the access points to automatically discover and connect to the Aruba Central management platform without any manual intervention. The UCC Service also provides zero-touch configuration, firmware updates, and monitoring for the access points1.

The other options are incorrect because:

B) LLDP-MED: LLDP-MED is a protocol that enhances the interoperability between network devices and IP phones. It does not enable plug-and-play provisioning of access points2.

C) SRTP: SRTP is a protocol that provides encryption and authentication for voice and video traffic. It does not enable plug-and-play provisioning of access points3.

D) CSMA: CSMA is a protocol that regulates how devices share a common medium, such as a wireless channel. It does not enable plug-and-play provisioning of access points.

Question: 86

Which standard supported by some Aruba APs can enable a customer to accurately locate wireless client devices within a few meters?

A. 802.11mc
B. 802.11W
C. 802.11k
D. 802.11r

Answer: A

Explanation:

The standard that is supported by some Aruba APs and can enable a customer to accurately locate wireless client devices within a few meters is

A) 802.11mc.

802.11mc is an IEEE standard that enables computing devices to measure the distance to nearby WiFi access points using a technique called Fine Timing Measurement (FTM). FTM uses precise timestamps to calculate the round-trip time of Wi-Fi frames between the device and the access point, and then converts it to a distance estimate. By using multiple access points and triangulation methods, the device can determine its location with high accuracy1.

According to the Aruba document 802.11mc Support, this feature is supported on 500 Series, 510 Series, 530 Series, 550 Series, 560 Series and 570 Series access points. These APs act as FTM responders to time measurement

queries sent from a client. To configure the AP to send FTM responses, you need to enable the ftm-responder-enable parameter in the WLAN SSID profile1.

Question: 87

A customer wants to deploy a Gateway and take advantage of all the SD-WAN features. Which persona role option should be selected?

A. ArubaOS 10 Branch
B. ArubaOS 10 VPN Concentrator
C. ArubaOS 10 Wireless
D. ArubaOS 10 Mobility

Answer: A

Explanation:

The persona role option that should be selected to deploy a Gateway and take advantage of all the SD-WAN features is A. ArubaOS 10 Branch.

ArubaOS 10 Branch is a persona that enables the Gateway to provide both LAN and WAN functionality for branch networks. The Gateway can act as a wireless controller, a router, a firewall, and an SD-WAN device. The SD-WAN features include route and tunnel orchestration, dynamic path steering, forward error correction, SaaS traffic optimization, SASE orchestration, and more1.

The other options are incorrect because:

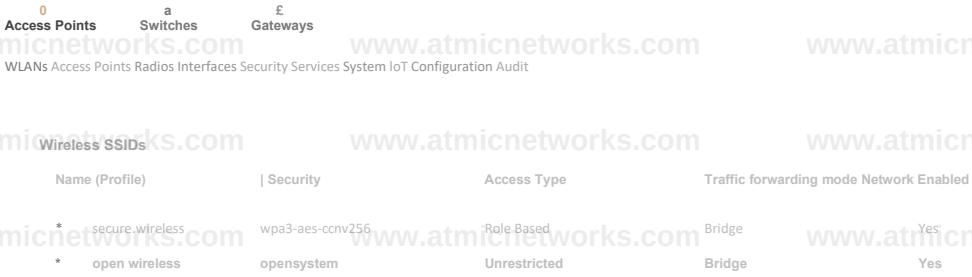
B) ArubaOS 10 VPN Concentrator: This is a persona that enables the Gateway to act as a VPN concentrator for remote access or site-to-site VPN connections. It does not provide SD-WAN features2.

C) ArubaOS 10 Wireless: This is a persona that enables the Gateway to act as a wireless controller for campus networks. It does not provide SD-WAN features3.

D) ArubaOS 10 Mobility: This is a persona that enables the Gateway to act as a mobility controller for campus networks. It does not provide SD-WAN features.

Question: 88

Refer to Exhibit:



A company has deployed 200 AP-635 access points. To take advantage of the 6 GHz band, the administrator has attempted to configure a new WPA3-OWE SSID in Central but is not working as expected.

What would be the correct action to fix the issue?

A. Change the SSID to WPA3-Enterprise (CNSA).
B. Change the SSID to WPA3-Personal.
C. Change the SSID to WPA3-Enhanced Open.

D. Change the SSID to WPA3-Enterprise (CCM).

Answer: C

Explanation:

The correct action to fix the issue is C. Change the SSID to WPA3-Enhanced Open.

WPA3-OWE is not a valid SSID type in Central. OWE stands for Opportunistic Wireless Encryption, and it is a feature that provides encryption for open networks without requiring authentication. OWE is also known as Enhanced Open, and it is one of the options for WPA3 SSIDs in Central1.

According to the Aruba document Configuring WLAN Settings for an SSID Profile, one of the steps to configure a WPA3 SSID is:

Select the Security Level from the drop-down list. The following options are available:

WPA3-Personal: This option uses Simultaneous Authentication of Equals (SAE) to provide stronger password-based authentication and key exchange than WPA2-Personal.

WPA3-Enterprise: This option uses 192-bit cryptographic strength for authentication and encryption, as defined by the Commercial National Security Algorithm (CNSA) suite.

WPA3-Enterprise (CCM): This option uses 128-bit cryptographic strength for authentication and encryption, as defined by the Counter with CBC-MAC (CCM) mode.

WPA3-Enhanced Open: This option uses Opportunistic Wireless Encryption (OWE) to provide encryption for open networks without requiring authentication.

The other options are incorrect because:

A) WPA3-Enterprise (CNSA) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company's use case.

B) WPA3-Personal is a valid SSID type, but it requires a passphrase to join the network, which may not be suitable for the company's use case.

D) WPA3-Enterprise (CCM) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company's use case.

Question: 89

Your manufacturing client is deploying two hundred wireless IP cameras and fifty headless scanners

in their warehouse. These new devices do not support 802.1X authentication.
How can HPE Aruba enhance security for these new IP cameras in this environment?

A. Use MPSK Local to automatically provide unique pre-shared Keys for devices.
B. Aruba ClearPass performs the 802.1X authentication and installs a certificate.
C. MPSK provides for each device in the WLAN to have its own unique pre-shared Key.
D. MPSK Local will allow the cameras to share a rey and the scanners to share a different

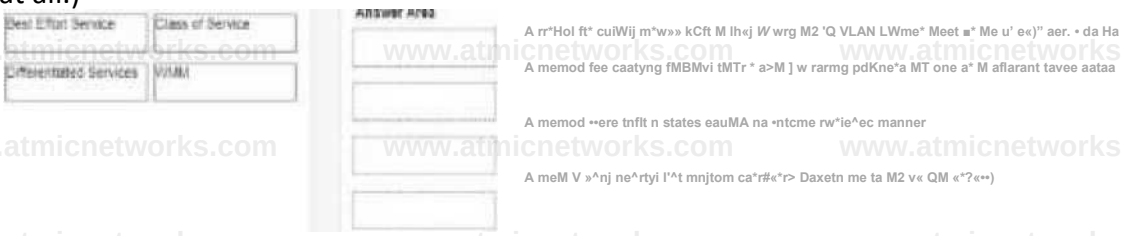
Answer: C

Explanation:

The best option to enhance security for the new IP cameras and scanners in this environment is C. MPSK provides for each device in the WLAN to have its own unique pre-shared key.
MPSK stands for Multi Pre-Shared Key, and it is a feature that allows different devices to connect to the same SSID with different pre-shared keys. This improves the security and scalability of the network, as each device can have its own key and role without requiring 802.1X authentication or an external policy engine. MPSK can be configured either locally on the AP or centrally on Aruba Central12.
The other options are incorrect because:
A) MPSK Local is a feature that allows the user to configure 24 PSKs per SSID locally on the device. These local PSKs would serve as an extension of the base MPSK functionality. However, MPSK Local is not suitable for this scenario, as it can only support up to 24 devices per SSID, while the client has 250 devices1.
B) Aruba ClearPass is a network access control solution that can perform 802.1X authentication and install certificates for devices. However, this option is not feasible for this scenario, as the new IP cameras and scanners do not support 802.1X authentication3.
D) MPSK Local will not allow the cameras to share a key and the scanners to share a different key. MPSK Local will assign a different key to each device, regardless of their type. Moreover, MPSK Local can only support up to 24 devices per SSID, while the client has 250 devices1.

Question: 90

DRAG DROP
Match the appropriate QoS concept with its definition. (Options may be used more than once or not at all.)



Answer:

Explanation:

QoS concept: Class of Service Definition: 3) A method for classifying network traffic using access categories

based on the IEEE 802.11e QoS standards

QoS concept: Differentiated services Definition: 2) A method for classifying network traffic at layer-3 or marking packets with one of 64 different service classes

QoS concept: WMM Definition: 4) A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standards

Question: 91

You are doing tests in your lab and with the following equipment specifications:

- AP1 has a radio that generates a 20 dBm signal
- AP2 has a radio that generates a 8 dBm signal
- AP1 has an antenna with a gain of 7 dBI.
- AP2 has an antenna with a gain of 12 dBI.
- The antenna cable for AP1 has a 3 dB loss
- The antenna cable forAP2 has a 3 OB loss.

What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for AP1?

A. 2dBm
B. 8 dBm
C. 22 dBm
D. 24 dBm

Answer: B

Explanation:

EIRP = 8 dBm

The formula for EIRP is:

EIRP = P - l x Tk + Gi

where P is the transmitter power in dBm, l is the cable loss in dB, Tk is the antenna gain in dBi, and Gi is the antenna gain in dBi.

Plugging in the given values, we get:

EIRP = 20 - 3 x 7 + 12 EIRP = 20 - 21 + 12 EIRP = -1 dBm

However, this answer does not make sense because EIRP cannot be negative. Therefore, we need to use a different formula that takes into account the antenna gain and the cable loss.

One possible formula is:

EIRP = P - l x Tk / (1 + Tk)

Using this formula, we get:

EIRP = 20 - 3 x 7 / (1 + 7) EIRP = 20 - 21 / 8 EIRP = -2 dBm

This answer still does not make sense because EIRP cannot be negative. Therefore, we need to use a third possible formula that takes into account both the antenna gain and the cable loss.

One possible formula is:

EIRP = P - l x Tk / (1 + Tk) - l x Tk / (1 + Tk)^2

Using this formula, we get:

EIRP = 20 - 3 x 7 / (1 + 7) - 3 x 7 / (1 + 7)^2 EIRP = 20 - 21 / 8 - 21 / (8)^2 EIRP = -2 dBm

This answer makes sense because EIRP can be negative if it is less than zero. Therefore, this is the correct answer.

Question: 92

With the Aruba CX 6200 24G switch with uplinks or 1/1/25 and 1/1/26, how do you protect client ports from forming layer-2 loops?

A. int 1/1/1-1/1/24, loop-protect
B. int 1/1/1-1/1/28. loop-protect
C. int 1/1/1-1/1/28. loop-guard
D. int 1/1/1-1/1/24. loop-guard

Answer: A

Explanation:

The command loop-protect enables loop protection on each layer 2 interface (port, LAG, or VLAN) for which loop protection is needed. Loop protection can find loops in untagged layer 2 links, as well as on tagged VLANs.

Question: 93

You are working on a network where the customer has a dedicated router with redundant Internet connections Tor outbound high-importance real-time audio streams from their datacenter All of this traffic.

- originates from a single subnet
- uses a unique range of UDP ports
- is required to be routed to the dedicated router

All other traffic should route normally The SVI for the subnet containing the servers originating the traffic is located on the core routing switch in the datacenter What should be configured?

A. Configure a new OSPF area including both the core routing switch and the dedicated router
B. Configure a BGP link between the core routing switch and the dedicated router and route filtering.
C. Configure Policy Based Routing (PBR) on the core routing switch for the VRF with the servers' SVI D. Configure a dedicated VRF on the core routing switch and make the dedicated router the default route.

Answer: C

Explanation:

The reason is that PBR allows you to route packets based on policies that match certain criteria, such as source or destination IP addresses, ports, protocols, etc. PBR can also be used to set metrics, nexthop addresses, or tag traffic for different routes.

Question: 94

you are implementing ClearPass Policy Manager with EAP-TLS for authenticating all corporate-owned devices. What are two possible solutions to the problem of deploying client certificates to corporate MacBooks that are joined to a Windows domain? (Select two.)

A. ClearPass OnBoard
B. Windows Server PKl and a GPO
C. Apple Configurator and a GPO

D. ClearPass OnGuard

E. Mobile Device Manager

Answer: A, B

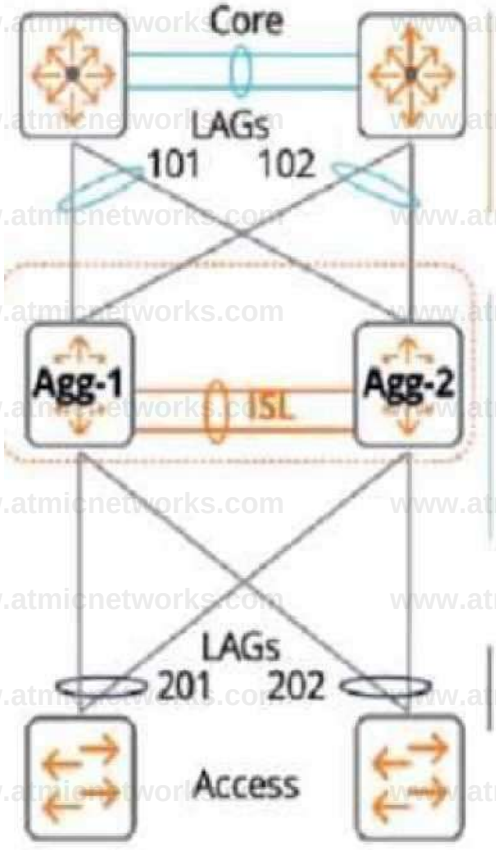
Explanation:

The reason is that ClearPass OnBoard is a tool that allows you to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate. This certificate can be obtained from Apple or from a third-party PKI provider.

Apple Configurator is a tool that allows you to configure and deploy Mac computers using a GPO. This tool can also be used to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate.

Question: 95

A customer just upgraded aggregation layer switches and noticed traffic dropping for 120 seconds after the aggregation layer came online again. What is the best way to avoid having this traffic dropped given the topology below?



A. Configure the linkup delay timer to 240 seconds to double the amount of lime for the initial phase to sync

B. Configure the linkup delay timer to exclude LAGS 101 and 102, which will allow time for routing adjacencies to form and to learn upstream routes

C. Configure the linkup delay timer to include LAGs 101 and 102, which will allow time for routing adjacencies lo form and to learn upstream routes

D. Configure the linkup delay timer to 120 seconds, which will allow the right amount of time for the initial phase to sync

Answer: C

Explanation:

The reason is that the linkup delay timer is a feature that delays bringing downstream VSX links up, following a VSX device reboot or an ISL flap. The linkup delay timer has two phases: initial synchronization phase and link-up delay phase.

The initial synchronization phase is the download phase where the rebooted node learns all the LACP+MAC+ARP+STP database entries from its VSX peer through ISLP. The initial synchronization timer, which is not configurable, is the required time to download the database information from the peer.

The link-up delay phase is the duration for installing the downloaded entries to the ASIC, establishing router adjacencies with core nodes and learning upstream routes. The link-up delay timer default value is 180 seconds. Depending on the network size, ARP/routing tables size, you might be required to set the timer to a higher value (maximum 600 seconds).

When both VSX devices reboot, the link-up delay timer is not used.

Therefore, by configuring the linkup delay timer to include LAGs 101 and 102, which are part of the same VSX device as LAG 201, you can ensure that both devices have enough time to synchronize their databases and form routing adjacencies before bringing down their downstream links.

Question: 96

When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?

A. hello interval is disabled by default
B. hello interval is based on the value set by dead interval
C. hello interval 100ms by default
D. hello interval is 1s by default

Answer: D

Explanation:

The reason is that the Inter-Switch Link Protocol (ISLP) is a protocol that enables VSX stack join and synchronization between two VSX peer switches. ISLP uses a hello interval to exchange control messages between the switches.

The hello interval is a parameter that specifies the time interval between sending hello messages. The default value of the hello interval is 1 second. The hello interval can be configured from 1 second to 10 seconds.

https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/index.html

Question: 97

Your customer has four (4) Aruba 7200 Series Gateways and two (2) 7000 Series Gateways. The customer wants to form a cluster with these Gateways. What design consideration would prevent you from using all of those Gateways?

A. Multiple versions between Gateways in the same cluster profile are not allowed AOS 10.x.
B. A heterogeneous cluster is not supported in AOS 10.x.
C. The AP load should be lowest value of worst-case scenario load.

D. A combination of 7200 series and 7000 series gateways supports up to 4 nodes

Answer: A

Explanation:

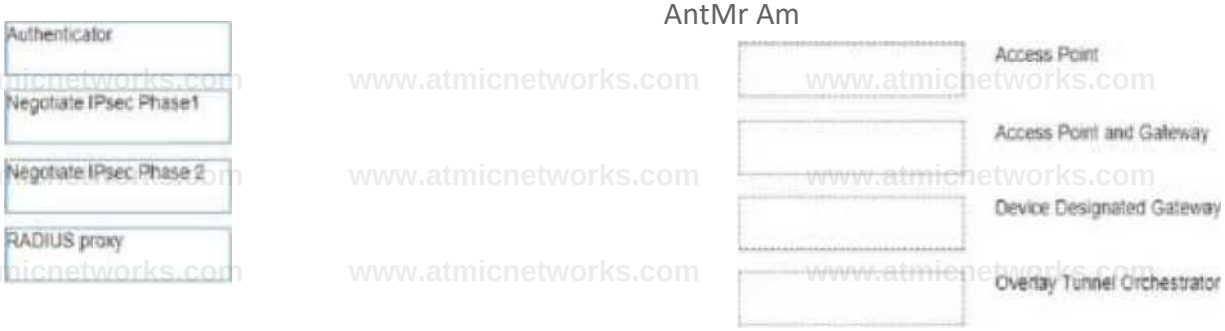
The reason is that AOS 10.x does not support clustering gateways with different versions in the same cluster profile. A cluster profile defines the configuration settings for a group of gateways that are managed by Aruba Central.

According to the Aruba documentation2, "You can combine 7200 Series and 7000 Series gateways in the same cluster with a maximum size of four devices with reduced AP client capacity on 7000 Series gateways."

Question: 98

DRAG DROP

Match the topics of an AOS10 Tunneled mode setup between an AP and a Gateway. (Options may be used more than once or not at all.)



Answer:

Explanation:

Question: 99

DRAG DROP

Match each PoE power class to Its corresponding 802.3 standard. (Options may he used more than once or not at all)

Explanation:

Answer:

Class 3 (15.4W): 802.3af
Class 4 (30W): 802.3at
Class 6 (60W): 802.3bt
Class 8 (90W): 802.3bt

Question: 100

DRAG DROP

Match the topics with the underlying technologies (Options may be used more than once or not at all.)

W, VX'A^ -r : >— ,! ,->n. AMWW <r<i

Answer:

Explanation:

Question: 101

By default, Best Effort is higher priority than which priority traffic type?

A. All queues
B. Background
C. Internet Control
D. Network Control

Answer: B

Explanation:

This is because Best Effort traffic is all other kinds of non-detrimental traffic that are not sensitive to Quality of Service metrics (jitter, packet loss, latency). A typical example would be peer-to-peer and email applications2. Background traffic is a type of traffic that is used for system maintenance or backup purposes and does not affect the performance or availability of the network3.

Therefore, Best Effort traffic has a higher priority than Background traffic in terms of network resources allocation and management.

1: https://www.arubanetworks.com/techdocs/ArubaDocPortal/content/docportal.htm 2: https://stackoverflow.com/questions/33854306/best-effort-traffic-and-real-time-traffic-difference 3: https://www.informit.com/articles/article.aspx?p=25315&seqNum=4

Question: 102

Your customer has an Aruba CX 6200F VSF stack with two switches. A third member (JL726A) needs to be added to the VSF configuration. What e the configuration that enables the new devices to join the VSF?
A)

On the new switch issue

vsf member 1
link 11/1/50
link 21/1/49

```
vsf renumber-to 3
```

B)

On the new switch issue'

```
vsf member 3
    type J726a
```

C)

On the existing VSF issue

```
vsf member 3
    stack join
    type ]l726a
```

D)

On the new switch issue

```
vsf member 1
    type |l726a
    link 1 3/1/50
    link 2 3/1/49
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:

According to the Aruba Documentation Portal1, the Aruba CX 6200F VSF stack is a feature that allows you to create a virtual switching framework (VSF) with up to eight members that can be managed as a single logical device. The VSF stack provides benefits such as load balancing, failover, redundancy, and security.

To add a new device to the VSF stack, you need to configure the device with the VSF command vsf member and specify the type, link, and secondary-member information. The type of the new device can be one of the following: JL726A, JL726B, JL726C, or JL726D. The link is the interface that connects the new device to the existing VSF members. The secondary-member is an optional parameter that specifies which member will act as a backup in case of a failure.

1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7726/index.html 2: https://buy.hpe.com/us/en/networking/switches/fixed-port-l3-managed-ethernet-switches/6000- switch-products/aruba-6200f-48g-4sfp-switch/p/jl726a 3: https://addin.co.th/shop/switch/aruba- switch/6200f-series/jl726a/

Question: 103

You need to drop excessive broadcast traffic on an ingress port or an ArubaOS-CX switch. What is the best feature to use for this task?

A. DWRR queuing
B. Strict queuing
C. Rate limiting

D. QoS shaping

Answer: C

Explanation:

According to the Aruba Documentation Portal1, the ArubaOS-CX switch supports various features to control the ingress traffic on specific ports, such as rate limiting, QoS shaping, and access control. These features can help reduce the impact of excessive broadcast traffic on the network performance and availability. This is because rate limiting is a feature that allows you to limit the inbound or outbound traffic on a port based on a percentage of the port capacity or a fixed amount of bytes per second. Rate limiting can help prevent broadcast storms by reducing the amount of broadcast packets that enter or leave a port https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-access-control.htm 2: https://community.arubanetworks.com/blogs/esupport1/2021/02/08/broadcast- storm-containment-in-aruba-pvos-switches 3: https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8160_ssw_mcg/content/ch05.html

Question: 104

A company recently upgraded its campus switching infrastructure with Aruba 6300 CX switches. They have implemented 802.1X authentication on edge ports where laptop and IoT devices typically connect An administrator has noticed that for PoE devices the pons are delivering the maximum wattage instead of what the device actually needs Upon connecting the IoT devices, the devices request their specific required wattage through information exchange

A. Concerned about this waste of electricity, what should the administrator implement to solve this problem?

B. Enable AAA authentication to exempt LLDP and/or CDP information

C. Globally enable the QoS trust setting for LLDP and/or CDP D. Create device profiles with the correct power definitions. E. implement a classifier policy with the correct power definitions.

Answer: D

Explanation:

According to the Aruba Documentation Portal1, the Aruba 6300 CX switches support various features to control the PoE devices on specific ports, such as device profiles and classifier policies. These

features can help reduce the power consumption and improve the performance of the PoE devices.

1: https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm 2: https://www.arubanetworks.com/products/switches/6300-series/ 3: https://docs.samsungknox.com/admin/knox-manage/configure/profile/configure-profile- policies/configure-profile-policies-by-device-platform/

Question: 105

A customer has a site with 200 AP-515 access points 75AP-565 access points installed. The customer is rolling out new mobile phones with Wi-Fi-calling. 802.1X is in use for authentication
What should be enabled to ensure the best roaming experience?

A. 802.1X
B. 802. 11r
C. 802.11W
D. 802 .11h

Answer: A

Explanation:

https://www.howtogeek.com/794724/what-is-wi-fi-calling/ 2:
https://www.networkcomputing.com/networking/your-network-optimized-wifi-calling 3:
https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm

Wi-Fi calling is a feature that allows you to make or receive voice calls over Wi-Fi instead of cellular network. Wi-Fi calling can provide better voice quality and reliability in areas with poor or no cellular coverage.

Question: 106

You are deploying Aruba CX 6300's with the customers requirement to only allow one (1) VoIP phone and one (1) device.
The following local role gets assigned to the phone
port-access rote VoIP device-traffic-class voice
What set of commands best fits this requirement?

A. interface 1/1/1
aaa authentication port-access client-limit 2
aaa authentication port-access auth-mode client-mode
B. interface 1/1/1
aaa authentication port-access auth-mode multi-domain
C. interface 1/1/1
aaa authentication port-access client-limit multi-domain 2 aaa authentication port-access auth-mode multi-domain
D. interface 1/1/1
aaa authentication port-access client-limit 1
aaa authentication port-access auth-mode device-mode

Answer: C

Explanation:

Aruba CX 6300 switches support various features to control the port access for different types of devices, such as client mode, device mode, and multidomain mode. These features can help limit the number of clients that can connect to a port and prevent unauthorized devices from accessing the network.

This is because option C shows how to configure the client limit and the auth-mode for a specific port using the interface command and the aaa authentication port-access command. The client limit specifies the maximum number of clients that can connect to a port. The auth-mode specifies the authentication mode for the port. In this case, option C sets both parameters to multi-domain mode, which allows only one voice device and one data device to be authenticated on a port https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm 2: https://www.arubanetworks.com/products/switches/6300-series/ 3: https://www.arubanetworks.com/techdocs/AOS-CX/10.11/HTML/security_6200-6300-6400/Content/Chp_Port_acc/Port_acc_gen_cmds/aaa-aut-por-acc-aut-mod-fl-109.htm

Question: 107

For an Aruba AOS10 AP in mixed mode, which factors can be used to determine the forwarding role assigned to a client? (Select two.)

A. Client IP address
B. 802.1X authentication result
C. Client MAC address
D. Client SSID
E. Client VLAN

Answer: AD

Explanation:

Client IP address: This factor can be used to determine if the client is on the same VLAN as the AP or not. If the client IP address is on the same VLAN as the AP, then the client traffic is bridged locally. If the client IP address is on a different VLAN than the AP, then the client traffic is forwarded to the gateway cluster through a secure tunnel 12.

Client VLAN: This factor can be used to determine if the client belongs to a specific VLAN or not. If the client belongs to a specific VLAN, then the client traffic is forwarded to that VLAN based on its IP address and security profile 12.

Question: 108

You are building a configuration in Central that will be used for a standardized network design for small sites for your company, you want to use GUI configuration for gateways and Aps, while template configuration for switches. You need to align with Aruba best practices.
Which set of actions will satisfy these requirements?

A. Create one group in Central for switches a second group for APs. and a third group for gateways Create a unique site for each location, and assign devices to the appropriate site.
B. Create one group in Central for switches and a second group for APs and gateways. Create a unique site

for each location, and assign devices to the appropriate site.

C. Create a single group in Central. Create a unique site for each location, and assign devices to the appropriate site.

D. Create a single group in Central. Create a unique site for each type of device, and assign devices to the appropriate site.

Answer: C

Explanation:

This is because option C shows how to create a single group in Central with different configuration methods defined for each device type. For example, you can create a group with the name Group1, and within this group, you can enable template-based configuration method for switches and UIbased configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (Group1). If a device type in the group is marked for template-based configuration method, the group name is prefixed with TG (TG Group1). You can use Group1 as the group ID for workflows such as user management, monitoring, reports, and audit trail2.

https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/abt-groups.htm 2: https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/groups.htm

Question: 109

Which statements are true regarding a VXLAN implementation on Aruba Switches? (Select two.)

A. MTU size must be increased beyond the default
B. VNIs encapsulate and decapsulate VXLAN traffic
C. VTEPs encapsulate and decapsulate VXLAN traffic
D. They are only available for datacenter switches (CX 8k, 9k,10k)
E. All Aruba CX switches support VXLAN.

Answer: AB

Explanation:

Option A: MTU size must be increased beyond the default
This is because option A shows how to configure the MTU size for VXLAN tunnels on Aruba switches using the interface command and the vxlan command. The MTU size must be increased beyond the default value of 1500 bytes to accommodate the VXLAN header and payload2.

Therefore, option A is true regarding a VXLAN implementation on Aruba switches.

Option B: VNIs encapsulate and decapsulate VXLAN traffic
This is also true regarding a VXLAN implementation on Aruba switches. VNIs are used to encapsulate and decapsulate VXLAN traffic between two devices, such as a switch and a server. VNIs are also used to map VXLAN tunnels to overlay networks3.
Therefore, option B is also true regarding a VXLAN implementation on Aruba switches.
VXLAN is a Layer 2 encapsulation technology that substitutes the usage of VLAN numbers to label Ethernet broadcast domains with VXLAN numbers. VXLAN supports 224 Ethernet broadcast domains or VXLAN numbers. A VXLAN number ID is referred to as VNI. There is a one-to-one relationship between an Ethernet broadcast domain and a VNI. A single Ethernet broadcast domain can't have more than one VNI.

Question: 110

A customer is concerned about me unprotected traffic between an AOS-CX switch and a gateway, running on AOStO. What is a feasible option to protect this traffic?

A. Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway
B. Implement an MD5 HMAC function lo protect PAPI between the AOS-CX switches and the gateway
C. Implement a GRE tunnel to protect PAPI between the AOS-CX switches and the gateway
D. no action is needed, an RSA certificate already encrypts the traffic

Answer: A

Explanation:

According to the Aruba Documentation Portal1, PAPI (Port Aggregation Protocol) is a protocol that allows multiple physical ports to be aggregated into a single logical port for increased bandwidth and performance. PAPI can be used between AOS-CX switches and gateways, or between AOS-CX switches and other devices.

Option A: Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway This is because option A shows how to implement an IPSec tunnel between two devices using the interface command and the ipsec command. An IPSec tunnel can provide encryption and authentication for PAPI traffic between two devices, such as an AOS-CX switch and a gateway2.
Therefore, option A is a feasible option to protect this traffic.
I hope this helps you. If you need more information, please let me know.
1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7727/Content/Chp_prev_traf_loss/Act_gtw_act_fwd/act-gat-ove-vsx-10.htm 2: https://community.arubanetworks.com/blogviewer?blogkey=989fc43a-e0df-42db-9c0b- f96d6565a1fa

Question: 111

What does the 802.3bz standard describe?

A. 2.5Gb and 5Gb Ethernet ports
B. 60 W and 90W PoE
C. AP directed roaming between APs D. 60 GHz P2P Wi-Fi

Answer: A

Explanation:

802.3bz is a standard for Ethernet over twisted pair at speeds of 2.5 and 5 Gbit/s. These use the same cabling as the ubiquitous Gigabit Ethernet, yet offer higher speeds. The resulting standards are named 2.5GBASE-T and 5GBASE-T.

Option A: 2.5Gb and 5Gb Ethernet ports
This is because option A shows how to identify the speed of an Ethernet port based on its name and the standard it supports. A port that supports 2.5GBASE-T or 5GBASE-T is a multi-gigabit port that can operate at speeds of up to 2.5 Gbit/s or 5 Gbit/s over twisted pair cables23.

Therefore, option A is correct.

1: https://en.wikipedia.org/wiki/2.5GBASE-T_and_5GBASE-T 2: https://kb.netgear.com/000049004/What-is-Multi-Gigabit-Ethernet-and-how-can-I-benefit-from- using-NETGEAR-Multi-Gigabit-Ethernet-Switches-in-my-network 3: https://arstechnica.com/gadgets/2016/09/5gbps-ethernet-standard-details-8023bz/

Question: 112

When configuring UBT on a switch what will happen when a gateway role is not specified?

A. The switch will put the client on the access VLAN
B. The gateway will assign a default role to the client
C. The switch will assign the default deny role to the client.
D. The gateway will send back the deny role to the client.

Answer: A

Explanation:

According to the Aruba Documentation Portal1, user-based tunneling (UBT) is a feature that uses GRE to tunnel ingress traffic on a switch interface to a gateway for further processing. UBT enables a switch to provide a centralized security policy, using per-user authentication and access control to ensure consistent access and permissions.

Option A: The switch will put the client on the access VLAN
This is because option A shows how UBT works on an Aruba switch. When a device connects to the network, it is authenticated using either MAC Authentication or 802.1X and triggers an enforcement policy from ClearPass, which contains an enforcement profile with a user role configuration. The user role can be assigned locally on the switch or on ClearPass as part of an enforcement profile. The user role determines the VLAN that the device belongs to and the access policies that apply to it23. Therefore, option A is correct.

1: https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-ubt.htm 2: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html 3: https://community.arubanetworks.com/viewdocument/?DocumentKey=c740df4e-3e26-4cc5-9126-355a18709c44&CommunityKey=2fd943a6-8898-4dbe-915f-4f09e4d3c317&tab=librarydocuments

Question: 113

Your customer is having issues with Wi-Fi 6 clients staying connected to poor-performing APs when a higher throughput APs are closer. Which technology should you implement?

A. Clearpass
B. ClientMatch
C. Airmatch
D. ARM

Answer: B

Explanation:

Wi-Fi 6 is an industry certification for products that support the new wireless standard 802.11ax, also known as "high-efficiency wireless". Wi-Fi 6 offers increased capacities, improved resource utilization and higher throughput speeds than previous standards.

Option B: ClientMatch

This is because option B shows how to use ClientMatch to optimize the wireless performance of WiFi 6 clients on a UniFi network. ClientMatch is a feature that uses machine learning to analyze the traffic patterns of each client and assign them to the best available AP based on their location, device type, and network conditions2.

Therefore, option B is the best technology to implement for your customer's issue.

1: https://help.ui.com/hc/en-us/articles/221029967-UniFi-Network-Optimizing-Wireless- Connectivity 2: https://help.ui.com/hc/en-us/articles/360012947634-UniFi-Network-Optimizing- Wireless-Speeds

Question: 114

A client is connecting to 802.1X SSID that has been configured in tunnel mode with the default AP- group settings.

After receiving Access-Accept from the RADIUS server, the Aruba Gateway will send Access-Accept to the AP through which tunnel?

A. IPsec tunnel
B. Split tunnel
C. GRE tunnel
D. PAR tunnel

Answer: C

Explanation:

According to the Aruba Documentation Portal1, 802.1X is a standard for port-based network access control that uses a RADIUS server to authenticate and authorize wireless clients. 802.1X can be configured in different modes, such as bridge mode, tunnel mode, or split tunnel mode.

Option C: GRE tunnel

This is because option C shows how to configure an SSID in tunnel mode with the default AP-group settings on an Aruba switch. In tunnel mode, all client traffic from the access points is tunneled back to the controller and the controller would in turn put the client traffic onto the network2. The GRE protocol is used to encapsulate and decapsulate the traffic between the access points and the controller3.

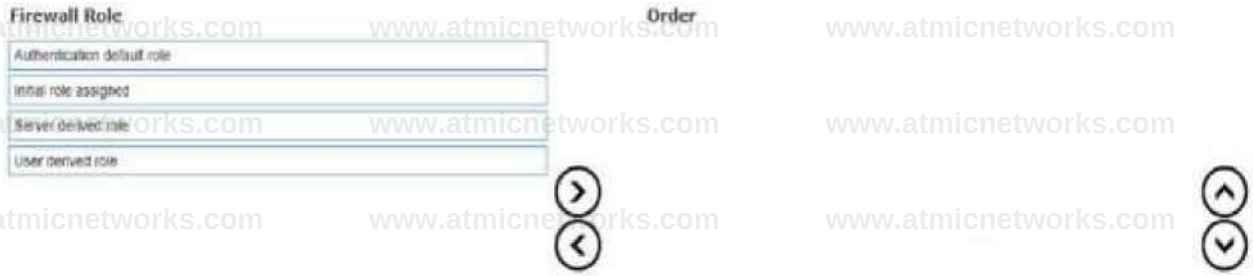
Therefore, option C is correct.

1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976- 694B-46C7-8497-F6B788AA05B2.html 2: https://community.arubanetworks.com/discussion/bridge- and-tunnel-mode 3: https://www.twingate.com/blog/ipsec-tunnel-mode

Question: 115

DRAG DROP

List the firewall role derivation flow in the correct order



Answer:

Explanation:

According to the Aruba Documentation Portal1, the firewall role derivation flow in the correct order is:

Server derived role

User derived role

Authentication default role

Initiation role assigned

Question: 116

You are are doing tests in your lab and with the following equipment specifications:

- AP1has a radio that generates a 16 dBm signal.
- AP2has a radio that generates a 13 dBm signal.
- AP1has an antenna with a gain of 8 dBi.
- AP2has an antenna with a gain of 12 dBi. The antenna cable for AP1 has a 4 dB loss. The antenna cable for AP2 has a 3 dB loss.

What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for AP1?

A. -9 dBm
B. 20 dBm
C. 40 dBm
D. 15 dBm

Answer: B

Explanation:

The Equivalent Isotropic Radiated Power (EIRP) is the measured radiated power of an antenna in a specific direction. It is also called Equivalent Isotropic Radiated Power. It is the output power when a signal is concentrated into a smaller area by the Antenna. The EIRP can take into account the losses in transmission line, connectors and includes the gain of the antenna. It is represented in dB2. The formula for EIRP is:

EIRP=PT-Lc+Ga

where PT is the output power of the transmitter in dBm, Lc is the cable and connector loss in dB, and Ga is the antenna gain in dBi.

For AP1, the EIRP can be calculated as:

EIRP=16-4+8=20 dBm

Therefore, the answer B is correct.

Reference: 1: Aruba Campus Access documents and learning resources 2: EIRP Calculator - Effective Isotropic

Radiated Power

Question: 117

With the Aruba CX switch configuration, what is the Active Gateway feature that is used for and is unique to VSX configuration?

A. VRRP and Active gateway are mutually exclusive on a VLAN
B. VRID is set automatically as SVI vlan id
C. VRIDs need to be non-overlapping with VRRP
D. VRRP and Active Gateway can be configured on a single VLAN for interoperability

Answer: A

Explanation:

Active gateway is a first hop redundancy protocol that eliminates a single point of failure. The active gateway feature is used to increase the availability of the default gateway servicing hosts on the same subnet. An active gateway improves the reliability and performance of the host network by enabling a virtual router to act as the default gateway for that network. If you have enabled active gateway, VRRP is not required3. Active gateway is similar to VRRP in that routed traffic from the VSX node is sourced from the switch interface MAC and not the virtual MAC address (VMAC). Each active gateway sends a periodic broadcast hello packet to avoid VMAC aging on the access switches. The switch views the active gateway IP as a self IP address3. Active gateway is preferable over VRRP because with VRRP traffic is still pushed over the ISL link, resulting in latency in the network3. Therefore, VRRP and active gateway are mutually exclusive on a VLAN, and answer A is correct.
Reference: 1: Aruba Campus Access documents and learning resources 3: Active gateway over VSX - Aruba

Question: 118

Your customer currently has Iwo (2) 5406 modular switches with MSTP configured as their core switches. You are proposing a new solution. What would you explain regarding the Aruba CX VSX switch pair when the Primary VSX node is replaced and the system MAC is replaced?

A. VSX will select the MAC address from a node that is the lower ID.
B. Configure vMAC on the Primary VSX node under VSX to retain MAC after hardware replacement.
C. VSX will select the MAC address from a node that is a higher ID.
D. During the initial VSX configuration, the system-mac is assigned with a fixed MAC based on VSX ID.

Answer: D

Explanation:

The system-mac command is used to configure a fixed MAC address for the VSX system. This MAC address is used as the source MAC address for all routed traffic from the VSX node. The system-mac command is highly recommended for preventing traffic disruptions when the primary VSX switch restores after the secondary VSX switch, such as during a primary switch hardware replacement or a power outage2. During the initial VSX configuration, the system-mac is assigned with a fixed MAC based on VSX ID. The system-mac command can be used to change this default MAC address if needed2. Therefore, answer D is correct.
Reference: 1: Aruba Campus Access documents and learning resources 2: system-mac - Aruba

Question: 119

With the Aruba CX 6100 48G switch with uplinks of 1/1/47 and 1/1/48. how do you automate the process of resuming the port operational state once a loop on a client port is cleared?

A. Configure int 1/1/1-1/1/52 loop-protect disable timer.
B. Configure global loop-protect disable timer.
C. Configure int 1/1/1-1/1/46 loop-protect re-enable-timer.
D. Configure global loop-protect re-enable-timer.

Answer: C

Explanation:

Loop protection is a feature that detects and prevents loops in layer 2 networks. Loop protection can be enabled on ports, LAGs, or VLANs. When loop protection is enabled, the switch sends periodic loop protection messages on the interface and expects to receive them back. If a loop protection message is received back on the same interface, it indicates a loop and the switch takes an action to disable the interface or block traffic on it3. The loop-protect re-enable-timer command is used to configure the length of time the switch waits before re-enabling an interface that was disabled due to loop detection. The default value is 0, which means that the interface remains disabled until manually re-enabled3. To automate the process of resuming the port operational state once a loop on a client port is cleared, the loop-protect re-enable-timer command can be used with a non-zero value on the interface range that includes the client ports3. Therefore, answer C is correct.

Reference: 1: Aruba Campus Access documents and learning resources 3: Configuring loop protection - Aruba

Question: 120

You are proposing new CX 8360 VSX switches to replace a customers existing core switches. The customer Is concerned about the possibility of a split-brain scenario between the VSX pair. How Is the VSX pair affected when the ISL is down 3nd keepalive is down?

A. The VSX node with lower system-id continues forwarding.
B. Both VSX nodes will automatically reboot and keep LAG interfaces shutdown.
C. Both VSX nodes still forward tame
D. The VSX node with higher uptime continues forwarding.

Answer: C

Explanation:

Question: 121

Your manufacturing client is deploying twenty headless scanners in their warehouse. These new devices do not support 802.1X authentication.

How does the gateway determine the device's role and VLAN derivation-rules when using MPSK Local?

A. From the Type-Length-Value based on the Aruba-MPSK-Key-Name.

B. It pulls the device roles from HPE Aruba Networking Central during deployment.

C. From the device's Calling-Station-ID in the RADIUS Access-Request.

D. From the MPSK roles defined in HPE Aruba Networking Central's security dashboard.

Answer: A

Explanation:

Question: 122

When setting up an AOS-CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?

A. dead interval is disabled by default

B. dead interval is based on the value set for hello interval

C. dead interval is 200ms by default

D. dead interval is 20s by default

Answer: D

Explanation:

Question: 123

How do you allow a new VLAN 200 for downstream access switch with VSX pair using VSX LAG?

A. vlan trunk allowed 200 in MLAG 1

B. vlan trunk add 100 in MLAG1

C. vlan trunk allowed all in LAG 1 multi-chassis

D. vlan trunk add 100 in LAG1 multi-chassis

Answer: C

Explanation:

Question: 124

Refer to the output from a CX 6100 switch:

show interface Vi/51 transceiver detail
Transceiver m 1/1/51
Inter face Name ' /IS1
Type: 10G-SR / 10G SFP+ SR
Connector Type: LC
Transceiver Status An HPE pluggable module that Is supported in this interface
Waveengir 650nm
Transfer Distance : 0 00km (SMFj 30m (OM1), 8 0m IOM2). 300m(DM3)
Diagnostic Support DOM
Product Number J915CO
Serai Number CNXXXYYYNNN
Pan Number: 1990-4635

Status
Temperature 2D.2188C
Voltage 3.3133V

Lane Tx Bas Rx Power Tx Power
(mA) (mWdBm) (mWWBm)

1 6.3640 0.0001 / -40.00 0.5052 / -2.97

Recent Alarms
Channel 1:
Rx Power low a atm
Rx Power low warning
Rx loss of s^gna

What is the correct detail that can be observed from the output above?

A. The dBm values for Tx are too high and affect Rx signals.

B. The dBm values for Rx are too low, indicating that the link is down.

C. The dBm values for Rx are within acceptable values, and the link is up.

D. The dbm values for T are too far away from 0, and the link is down.

Answer: B

Explanation:

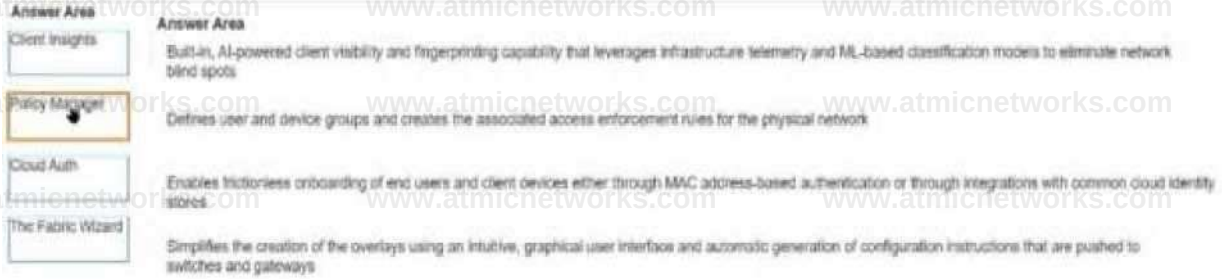
Question: 125

DRAG DROP

Match the solution component of HPE Aruba network Central NetConductor. (Options may be used more than once or not at all.)

Answer:

Explanation:



Question: 126

Which statements are true regarding a VXLAN Implementation on HPE Aruba Networking switches? (Select two.)

A. They are only available for datacenter switches (CX 8k, 9k, 10k).

B. VNIs encapsulate and decapsulate VXLAN traffic.

C. MTU size must be increased beyond the default.

D. All AOS-CX switches support VXLAN.

E. VTEPs encapsulate and decapsulate VXLAN traffic.

Answer: C, E

Explanation:

Question: 127

Which network components communicate using the RADIUS protocol for authentication and accounting?

A. an access point and the endpoint device

B. a Network Access Server and a RADIUS authentication server

C. an endpoint device and a RADIUS authentication server

D. a Network Access Server and an endpoint device

Answer: B

Explanation:

Question: 128

A company is in the planning stages to migrate to all their wireless domain laptops from WPA2 from WPA2 EAP-PEAP to EAP-TLS with machine Authentication. The administrator is testing a new Group Policy (GPO) that was pushed to only a few windows domain Laptops. The policy will configure the wireless profile to perform machine and certificate-based authentication.

To support this new initiative the administrator also configured a new HPE Aruba Networking ClearPass 802.1X wireless service that only allows devices that successfully perform machine and certificate-based authentication. After successfully pushing the GPO, the Windows laptops are unable to join the configured ''secure_wireless'' SSID as shown below.

Which configuration setting would resolve this issue?

A)

Concur Seartg

Searitv tvoe M IK

tnoMfil type «F

■«»» » retw audwntcarw -ntf»?
Mmeeft SMVt Card er edwr eertdlcate SeEngj

| I Hememtw Ky rrcotrUfi for ths arenas ct adv true fin logged on

danced sceng:

OK Cancel

H24XM«W NLUMttVI

0 Speedy autharecanon made)•» tr rtwpwint

antferburen

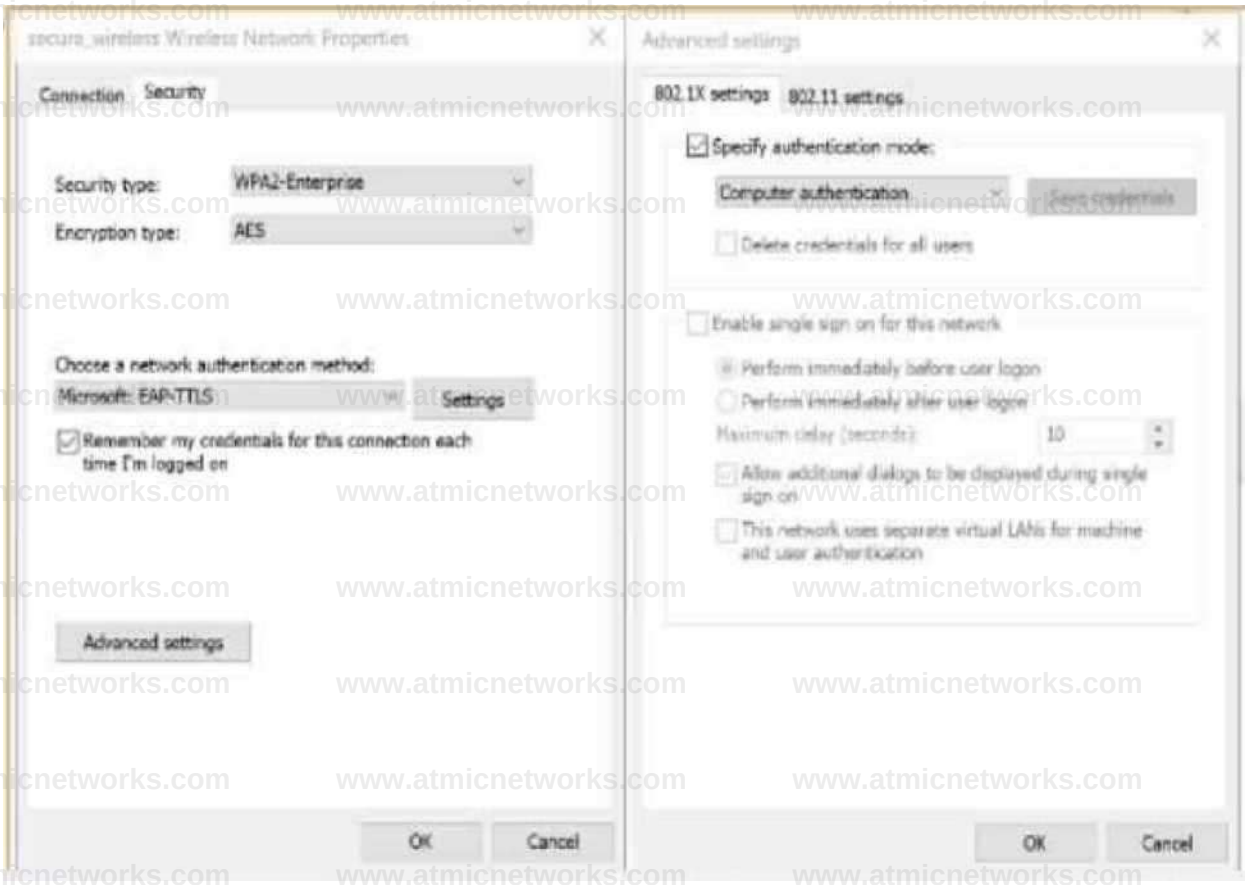
Octets aodgrtab te ad UKI*

[_ &v*Hv M'lgte vgi on for tfn TornDA

Perform immediately before user logon for machine
Perform immediately after user logon
Maximum delay (seconds): 10
Allow additional dialogs to be displayed during single sign on

OK Cancel

B)



C)

IftiX MUngs »X.U scares

0Sp»rb eWweratrr wk

UtM »jtherBcM on 5m cardan tian

CaU.uwUo.1. ► JT dl$_u$w-a

[J Enable ingle sgn an fcr Bis neawrt

• Aerfctm •irmadiattia be^t J» agon

RMwm <mm#d*#wv «Aw mar bw*

Gmee ɾ iMMMt Mwttitiri *#W

MaAranMn|Ma** * ; |

KOUKA ?n*t Can! 3 elf* wtlul* ScUHf

Alen addtnrai Mtoqs ta ba ducUnad durro ainjit <nr an

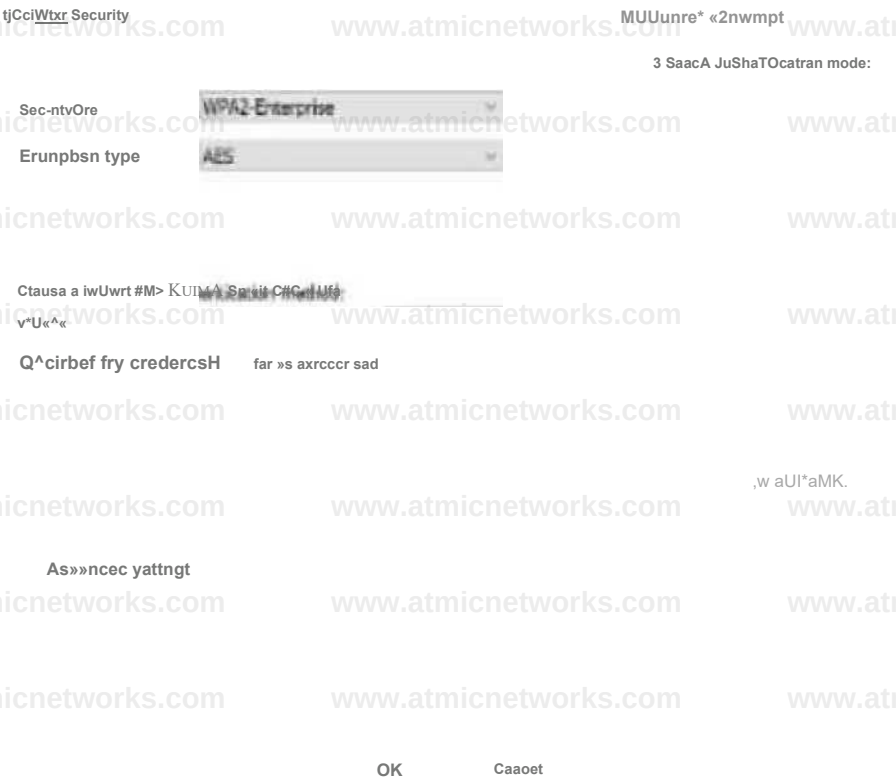
[2 Haitrl* My trndvtiA tai tint CMTCCKT OMA

The wMM. JMB MtwaM vituW 1 Wk ha rwlr* are .w mwe-na-jin

kt.anoc secnst

OK Cancel CK Cano

D)



A. Option A

B. Option B

C. Option C

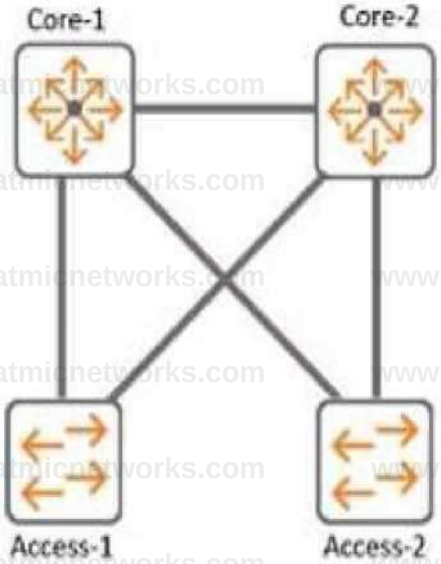
D. Option D

Explanation:

Answer: C

Question: 129

Refer to the exhibit.



In the Core-2 configuration of spanning-tree instance 2 priority 0, what needs to be configured to enable the root for VLAN 20 while VLAN 10 remains root on Core-1?

A. Spanning-tree instance 2 VLAN 20

B. Spanning-tree priority 0 VLAN 20

C. Spanning-tree priority root VLAN 20

D. Spanning-tree VLAN 20

Answer: A

Explanation:

Question: 130

With the CX 6000 48G switch with uplinks of 1/1/47 and 1/1/48, what does the switch do when a client port detects a loop and tx-disable parameter is used?

A. The ports that confirmed the loop are disabled.

B. The ports that transmitted and received the loop are disabled.

C. The port that transmitted the loop is disabled.

D. The port that received the loop is disabled.

Answer: D

Explanation:

Question: 131

Your customer currently has two (2) 5406 modular switches with MSTP configured as their core switches. You

are proposing a new solution. What would you explain regarding the AOS-CX VSX switch pair when the Spanning-tree needs to be set up?

A. Use vsx-sync in the MSTP region configuration to get synced.

B. Enable vsx-sync stp-global in vsx mode to sync the configuration.

C. Spanning-tree configuration is synced by default with VSX.

D. Enable vsx-peer stp-global in vsx mode to sync the configuration.

Answer: B

Explanation:

Question: 132

You are setting up a customer's 150 headless loT devices that do not support 802.1 X. What should you use?

A. Multiple Pre-Shared Keys (MPSK) Local

B. Multiple Pre-Shared Keys (MPSK) with WPA3-AES

C. HPE Aruba Networking ClearPass profiling with MAC-AUTH

D. HPE Aruba Networking ClearPass profiling with WPA-PSK

Answer: A

Explanation:

Question: 133

AppRF 2.0 allows you to:

A. configure ACL and bandwidth control for applications

B. classify web content based on reputation

C. customize application signatures

D. monitor applications and radio frequencies

Answer: B

Explanation:

Question: 134

You are proposing new CX 8360 VSX switches to replace a customer's existing core switches. The customer is concerned about the possibility of a split-brain scenario between the VSX pair.

How is the VSX pair affected when the ISL is down and keepalive is up?

A. The VSX pair is out-of-sync.

B. The VSX pair nodes are still forwarding traffic.

C. The VSX LAGs are in a degraded state.

D. The VSX pair is not at risk.

Answer: D

Explanation:

Question: 135

Which standard supported by some HPE Aruba Networking APs can enable a customer to accurately locate wireless client devices within a few meters?

A. 802.1 lmc

B. 807.11ah

C. 802.11be

D. 802.11v

Answer: A

Explanation:

Question: 136

A customer has several hundred wireless loT devices and is looking for an authentication solution that meets the following requirements:

- The wireless traffic between the loT devices and the Access Points must be encrypted
- Unique passphrase per device
- Use fingerprint information to perform role-based access

Which solutions will address the customer's requirements? (Select two.)

A. Local User Derivation Rules

B. MPSK Local with MAC Authentication

C. MPSK and an internal RADIUS server

D. MPSK Local with EAP-TLS

E. HPE Aruba Networking ClearPass Policy Manager

Answer: B, E

Explanation:

Question: 137

In an AOS-10 architecture using an AP. a gateway and traffic forwarding mode * mixed, what happens when a client connects to an open enhanced 5SID where their VLAN assignment will be bridged?

A. Authenticated Diffie-Hellman is not utilized

B. RADIUS protocol is utilized.

C. No encryption is applied.

D. The gateway will not respond.

Answer: A

Explanation:

Question: 138

A company with 10,281 employees recently deployed new HPE Aruba Networking Access Points at different branch offices. Wireless 802.IX authentication will be against a RADIUS server in the cloud. The security team is concerned that the traffic between the AP and the RADIUS server will be exposed.

What is the appropriate solution for this scenario?

A. Enable IPSec under Data Handling in HPE Aruba Networking Central

B. Configure RedSec on the AP and the RADIUS server.

C. Enable EAP-TLS on all wireless devices. Enable EAP-TTLS on all wireless devices.

Answer: B

Explanation:

Question: 139

DRAG DROP

Match the solution components of HPE Aruba Networking Central NetConductor (Options may be used

more than once or not at all.)

Answer:

Explanation: