Vendor:HP

Exam Code:HPE7-A01

Exam Name: Aruba Certified Campus Access Professional

Version: Demo

QUESTION 1

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+

Correct 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 2

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

Correct 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 3

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.

Correct Answer: B

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 4

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

Correct Answer: C

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 5

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

Correct 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. References: 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/channel-bonding.htm

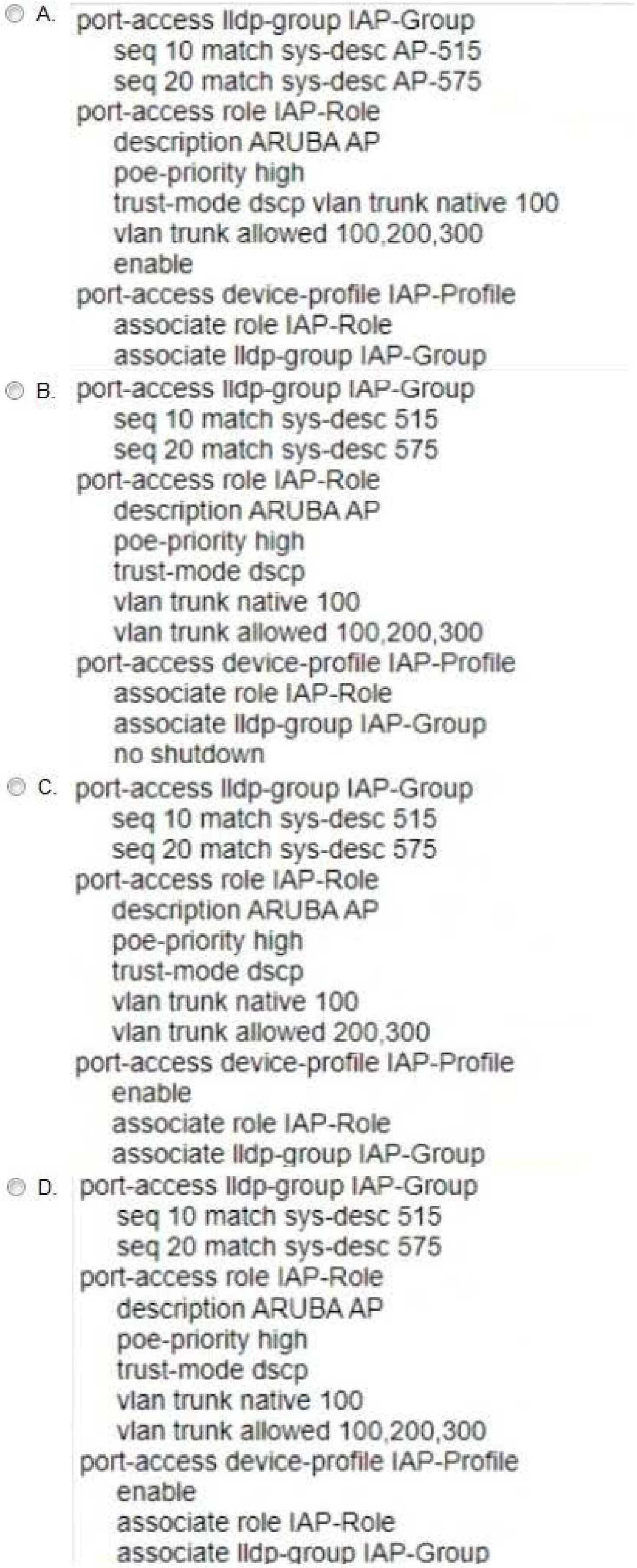
---

QUESTION 6

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 IAP-Group
    seq 10 match sys-desc AP-515
    seq 20 match sys-desc AP-575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp vlan trunk native 100
    vlan trunk allowed 100,200,300
    enable
port-access device-profile IAP-Profile
    associate role IAP-Role
    associate lldp-group IAP-Group
```

○ B.

```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
    associate role IAP-Role
    associate lldp-group IAP-Group
    no shutdown
```

○ C.

```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
    associate lldp-group IAP-Group
```

○ D.

```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
    associate lldp-group IAP-Group
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct 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.

References:

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch03.html

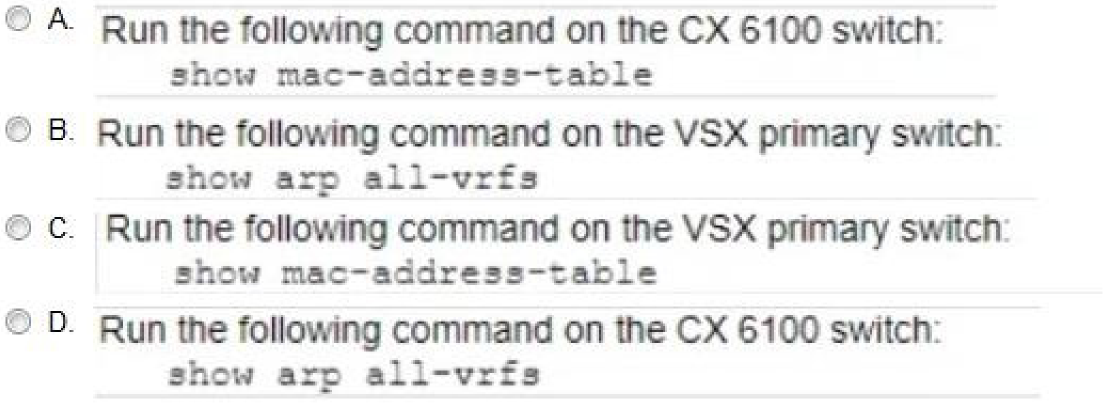
---

QUESTION 7

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:

```
show mac-address-table
```

○ B. Run the following command on the VSX primary switch:

```
show arp 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 arp all-vrfs
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct 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. References: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A- 4F0D-AE7B-9D8E6C5B6A7F.html

---

QUESTION 8

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

Correct 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. References: 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 9

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

Correct 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. References:
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf
https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf

QUESTION 10

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

Correct 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. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID- 99A8B276-0DA3-4458-AFD8-42BFEC29D4F5.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID- D8613BDE-CD21-4B83-8561-17DB0311ED8F.html

---

QUESTION 11

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

Correct 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 12

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

Correct 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. Multi-Domain 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. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-7D9E9F6E-5C2A-4F7E-BE6D-A2C3A6C7B9F9.html
https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf