

HP

Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam



NEW QUESTION 1

You need to drop excessive broadcast traffic on an ingress port on 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

NEW QUESTION 2

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. References: 3
https://www.arubanetworks.com/assets/tg/TG_EVPN_VXLAN.pdf

NEW QUESTION 3

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

NEW QUESTION 4

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 Wi-Fi 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>

NEW QUESTION 5

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.

NEW QUESTION 6

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. References: 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

NEW QUESTION 7

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>

NEW QUESTION 8

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.

NEW QUESTION 9

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 for AP2 has a 3 dB 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:

$$EIRP = P - l \times Tk + Gi$$

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:

$$EIRP = 20 - 3 \times 7 + 12 \quad EIRP = 20 - 21 + 12 \quad EIRP = -1 \text{ dBm}$$

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.

$$\text{One possible formula is: } EIRP = P - l \times Tk / (1 + Tk)$$

Using this formula, we get:

$$EIRP = 20 - 3 \times 7 / (1 + 7) \quad EIRP = 20 - 21 / 8 \quad EIRP = -2 \text{ dBm}$$

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:

$$EIRP = P - l \times Tk / (1 + Tk) - l \times Tk / (1 + Tk)^2 \quad \text{Using this formula, we get:}$$

$$EIRP = 20 - 3 \times 7 / (1 + 7) - 3 \times 7 / (1 + 7)^2 \quad EIRP = 20 - 21 / 8 - 21 / (8)^2 \quad EIRP = -2 \text{ dBm}$$

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

NEW QUESTION 10

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.

NEW QUESTION 10

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>

NEW QUESTION 11

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

- AP1 has a radio that generates a 16 dBm signal.
- AP2 has a radio that generates a 13 dBm signal.
- AP1 has an antenna with a gain of 8 dBi.
- AP2 has 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:

$EIRP = P_{TL} + G_a$ where P_T is the output power of the transmitter in dBm, L_c is the cable and connector loss in dB, and G_a is the antenna gain in dBi.

For AP1, the EIRP can be calculated as: $EIRP = 164 + 8 = 20$ dBm

Therefore, the answer B is correct.

References: 1: Aruba Campus Access documents and learning resources 2: EIRP Calculator - Effective Isotropic Radiated Power

NEW QUESTION 15

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 G0/0/V1 to 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.

NEW QUESTION 18

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. 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>

NEW QUESTION 23

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. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html>

<https://www.arubanetworks.com/resource/aruba-virtual-switching-extension-vsx/>

NEW QUESTION 26

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:

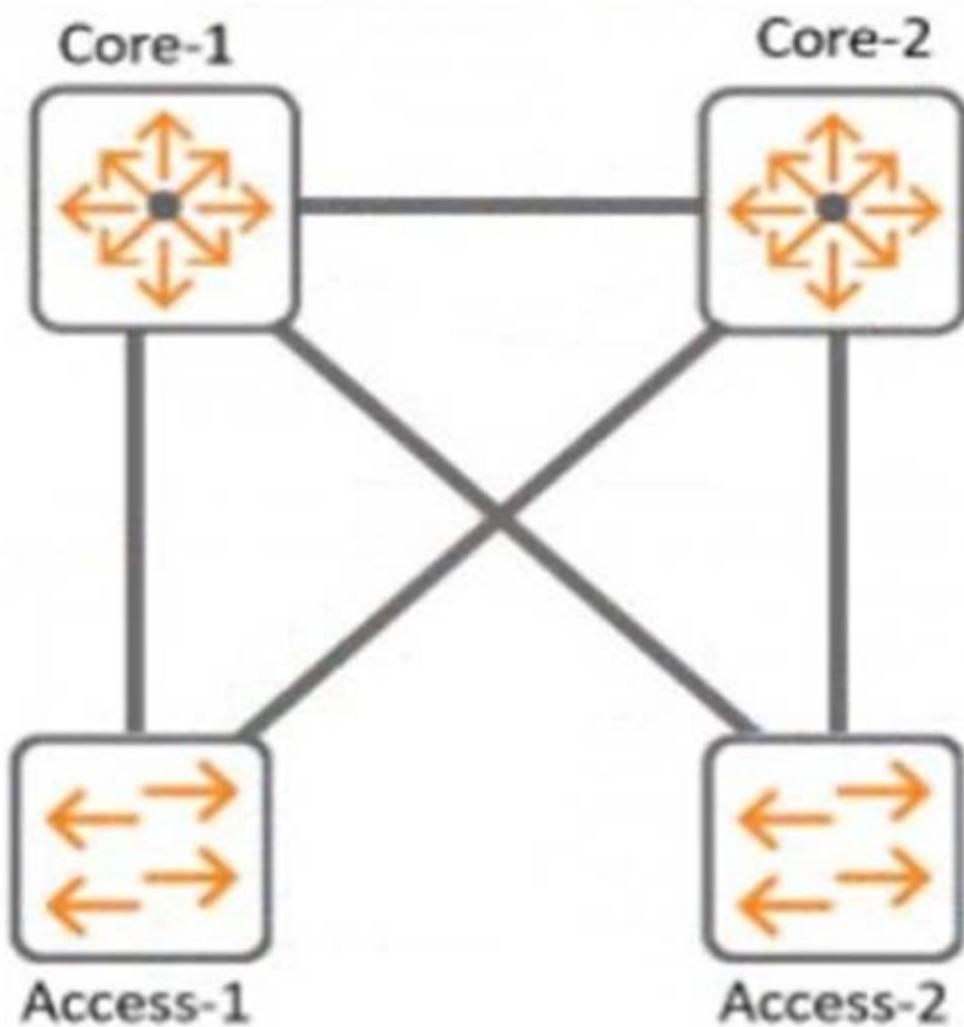
? A. sysadmin: The sysadmin user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The sysadmin user role does not have access to the REST API methods, and cannot perform firmware upgrades1.

? 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.

NEW QUESTION 30

Refer to the exhibit.



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

- A. 1
- B. 1-0
- C. 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. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html>

NEW QUESTION 34

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. References: https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf

NEW QUESTION 36

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

NEW QUESTION 40

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.)

Authenticator			Access Point
Negotiate IPsec Phase1			Access Point and Gateway
Negotiate IPsec Phase 2			Device Designated Gateway
RADIUS proxy			Overlay Tunnel Orchestrator

- A. Mastered
- B. Not Mastered

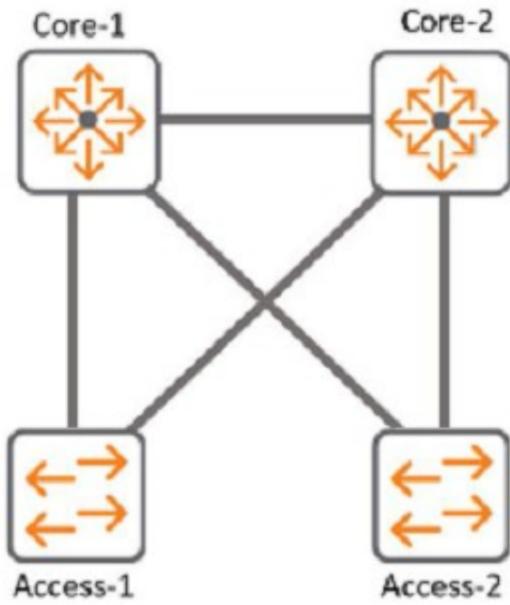
Answer: A

Explanation:

Authenticator		Negotiate IPsec Phase1	Access Point
Negotiate IPsec Phase1		Negotiate IPsec Phase 2	Access Point and Gateway
Negotiate IPsec Phase 2		Authenticator	Device Designated Gateway
RADIUS proxy		RADIUS proxy	Overlay Tunnel Orchestrator

NEW QUESTION 42

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 mappjng
- 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:

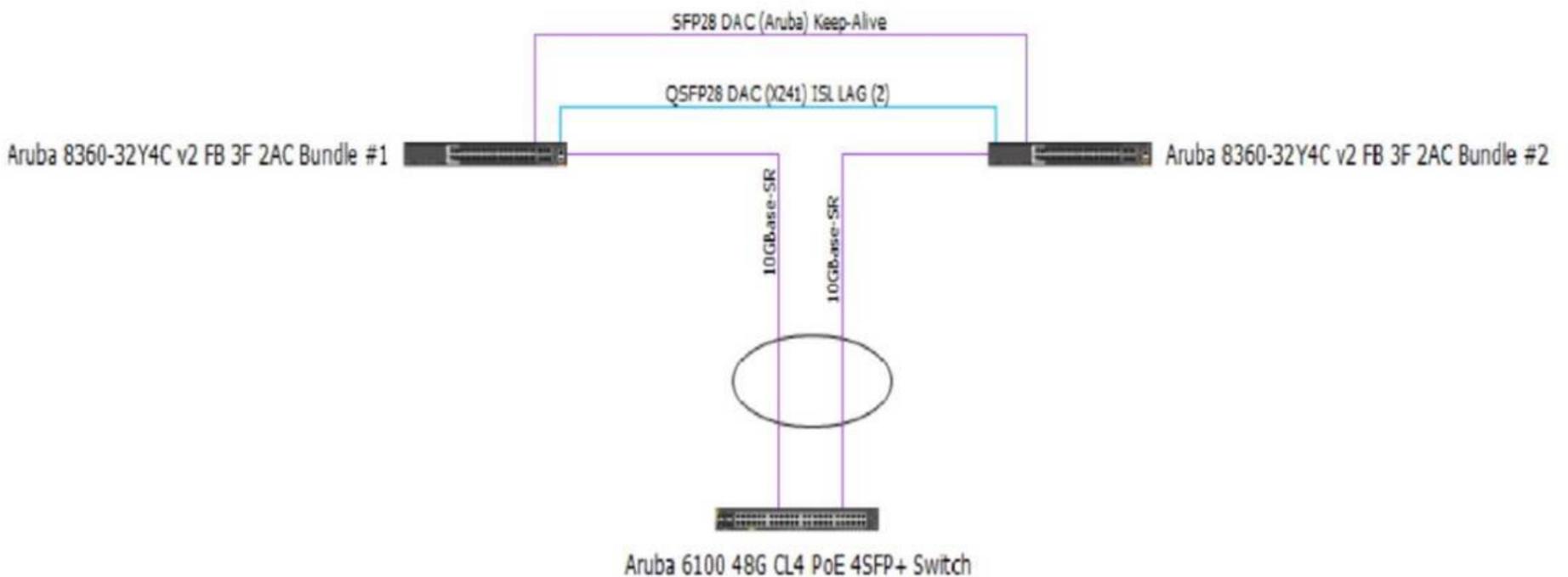
? A. Spanning-tree bpdu-guard setting is a security feature that disables a port if it receives a BPDU from an unauthorized device. It does not affect load balancing with MSTP.

? 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.

NEW QUESTION 46

Review the exhibit.



You are troubleshooting an issue with a 10.102.39.0/24 subnet which is also VLAN 1000 used for 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:

```
vsx
vsx-sync dhcp-relay
exit
```

B)

Enter the following commands on the VSX secondary switch:

```
vlan 1000
ip relay-address 10.200.1.100
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 1000
ip helper-address 10.200.1.100
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 domain.

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.

NEW QUESTION 47

You are working on a network where the customer has a dedicated router with redundant Internet connections for 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.

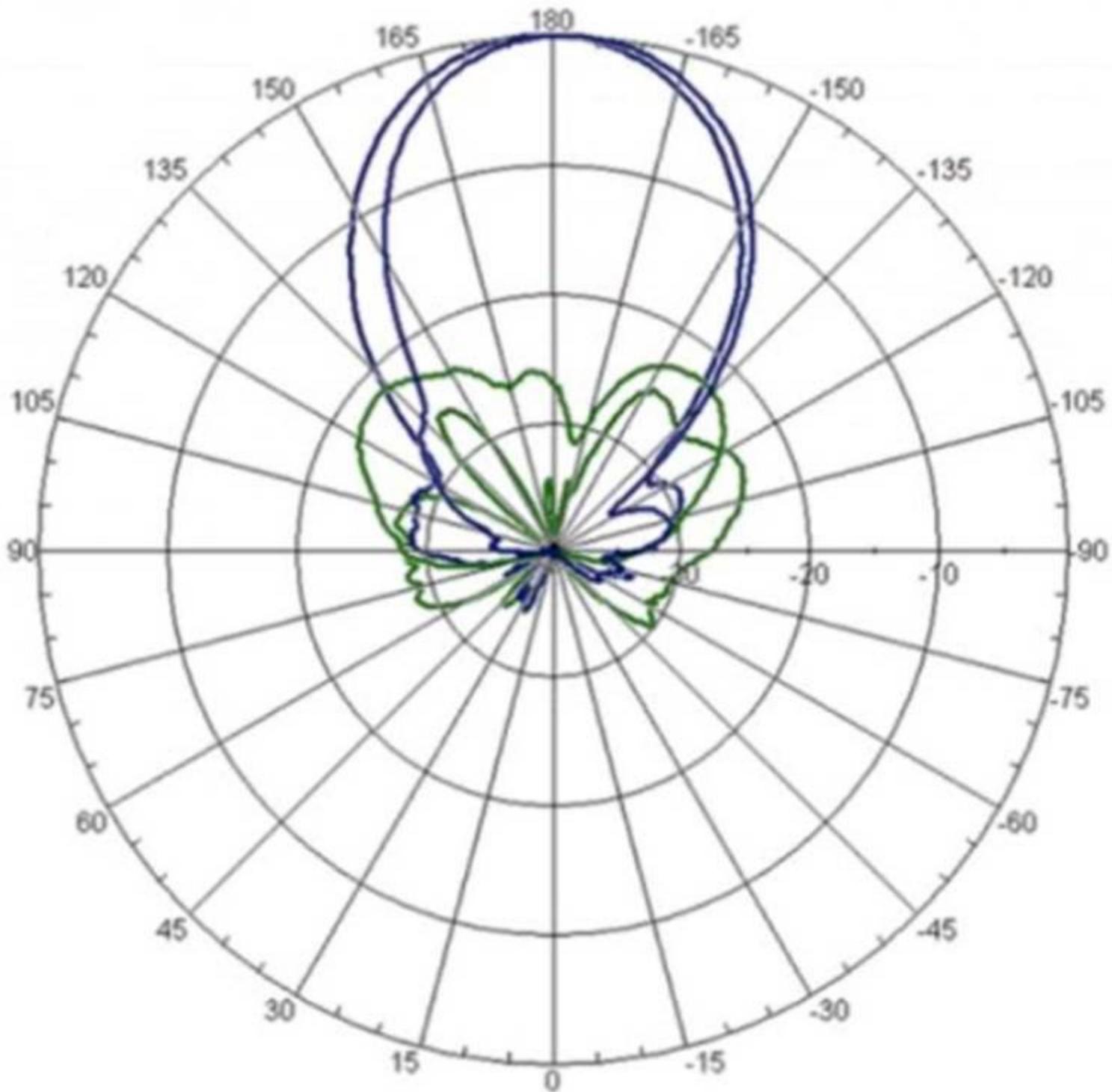
Answer: C

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, next-hop addresses, or tag traffic for different routes.

NEW QUESTION 49

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 issue?

- 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. 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/antennas.htm

NEW QUESTION 51

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-disable 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.

NEW QUESTION 54

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. References: https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch05.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch06.html

NEW QUESTION 57

Which statements regarding OSPFv2 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. References: <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>

NEW QUESTION 59

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

NEW QUESTION 60

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: BD

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.

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

NEW QUESTION 63

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 role VoIP device-traffic-class voice What set of commands best fits this requirement?

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

NEW QUESTION 65

DRAG DROP

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

Term	Characteristic
Broadcast	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
IP Directed Broadcast	One/more senders and one/more recipients participate in data transfer traffic
Multicast	Sent to all hosts on a remote network
Unicast	Sent to all NICs on the same network segment as the source NIC

- A. Mastered
- B. Not Mastered

Answer: A

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

References: 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 IP address 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

NEW QUESTION 66

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. 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

NEW QUESTION 67

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.

NEW QUESTION 71

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?

EVPN-VXLAN User Based Tunneling (UBT)

Answer Area

- Centralized Overlay
- Distributed Overlay
- Encapsulated in UDP
- Generic Routing Encapsulation (GRE)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

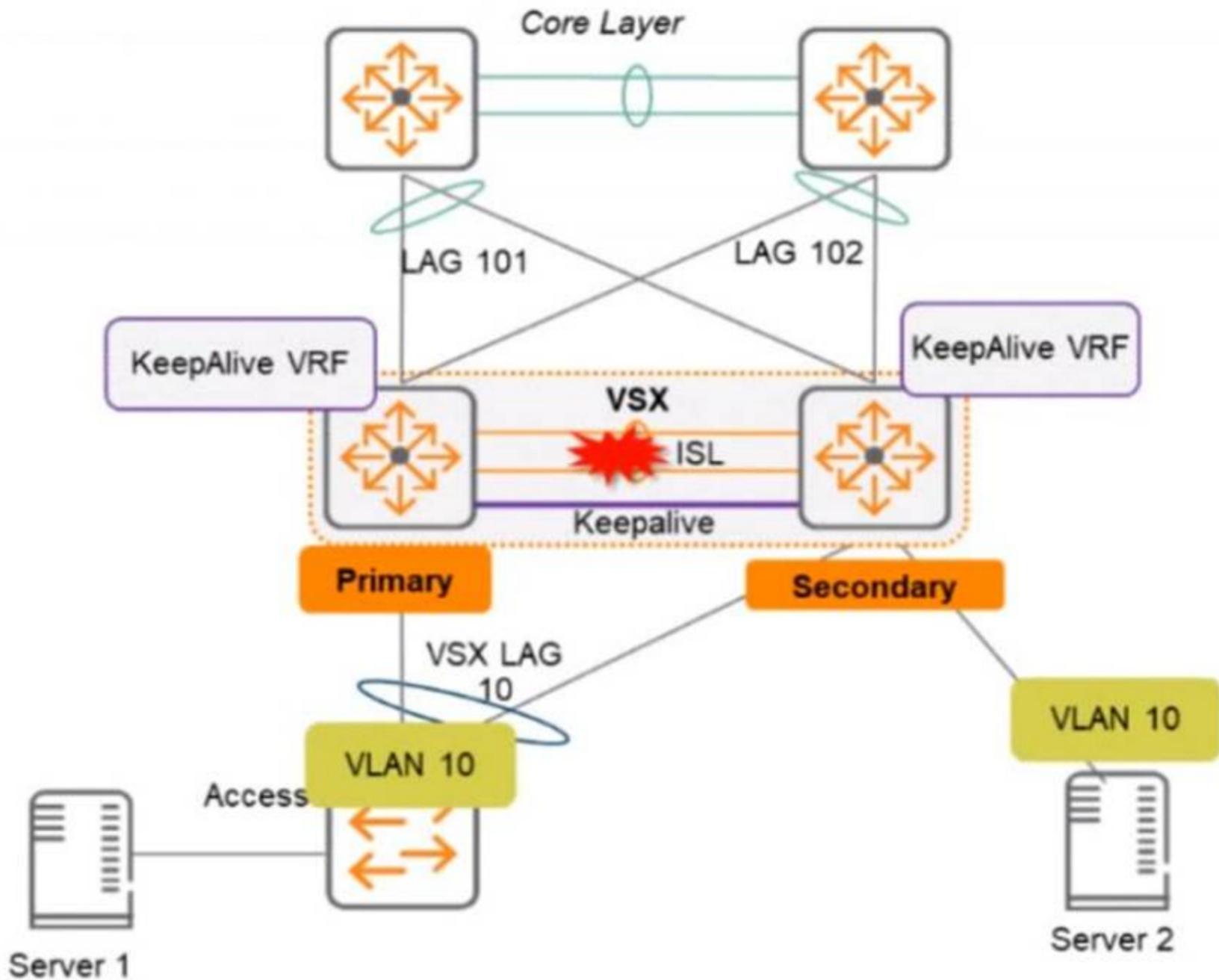
EVPN-VXLAN User Based Tunneling (UBT)

Answer Area

- EVPN-VXLAN Centralized Overlay
- EVPN-VXLAN Distributed Overlay
- EVPN-VXLAN Encapsulated in UDP
- User Based Tunneling (UBT) Generic Routing Encapsulation (GRE)

NEW QUESTION 85

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 keepalive 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. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01->

NEW QUESTION 86

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. 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

NEW QUESTION 89

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 methods 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.

NEW QUESTION 90

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

NEW QUESTION 91

DRAG DROP

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

Best Effort Service	Class of Service	Answer Area <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	A method for classifying network traffic at layer-2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Differentiated Services	WMM		A method for classifying network traffic at layer-3 by marking packets with one of 64 different service classes
			A method where traffic is treated equally in a first-come, first-served manner
			A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 94

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. References: https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch01.html
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html

NEW QUESTION 98

A customer is looking for 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 role-based access¹⁰¹¹¹².

NEW QUESTION 102

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 multi-access 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.

NEW QUESTION 103

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

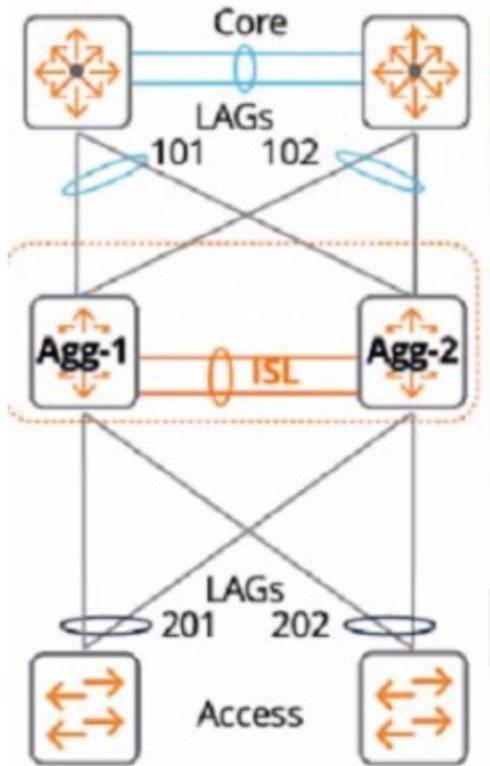
This is because option A shows how to identify the speed of an Ethernet port based on its name and the standard it supports. A port that supports 2.5GBASE-T or 5GBASE-T is a multi-gigabit port that can operate at speeds of up to 2.5 Gbit/s or 5 Gbit/s over twisted pair cables²³.

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/>

NEW QUESTION 107

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 time 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 to 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.

NEW QUESTION 108

DRAG DROP

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

VSF VSX

Answer Area

- Supports up to 10 devices per stack
- Supports two devices per stack
- Individual ISL links up to 400G are supported
- Individual ISL links up to 50G are supported
- A maximum aggregate ISL bandwidth of 200G is supported

- A. Mastered
- B. Not Mastered

Answer: A

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

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

NEW QUESTION 109

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 cloud-based 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. References:

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/spectrum_monitor.htm
https://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/>

NEW QUESTION 113

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-snooping 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
    dhcp-snooping trust
```

B)

```

dhcp snooping enable
no dhcp-snooping option 82
vlan 100
  name cornflakes
  dhcp-snooping
vlan 110
  name cornmill
  dhcp-snooping
vlan 120
  name packaging
  dhcp-snooping
interface lag 1
  no shutdown
  description Uplink-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
  description Uplink-to-Core
  no routing
  vlan trunk native 1
  vlan trunk allowed all
  lacp mode active
  dhcpv4-snooping trust

```

D)

```

dhcpv4-snooping
no dhcpv4-snooping option 82
vlan 100
  name cornflakes
  dhcpv4-snooping
vlan 110
  name cornmill
  dhcpv4-snooping
vlan 120
  name packaging
  dhcpv4-snooping
interface lag 1
  no shutdown
  description Uplink-to-Core
  no routing
  vlan trunk native 1
  vlan trunk allowed all
  lacp mode active
  dhcpv4-snooping 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.

NEW QUESTION 118

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

HPE7-A01 Practice Exam Features:

- * HPE7-A01 Questions and Answers Updated Frequently
- * HPE7-A01 Practice Questions Verified by Expert Senior Certified Staff
- * HPE7-A01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * HPE7-A01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The HPE7-A01 Practice Test Here](#)