HPE7-A01^{Q&As}

Aruba Certified Campus Access Professional

Pass HP HPE7-A01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/hpe7-a01.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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?
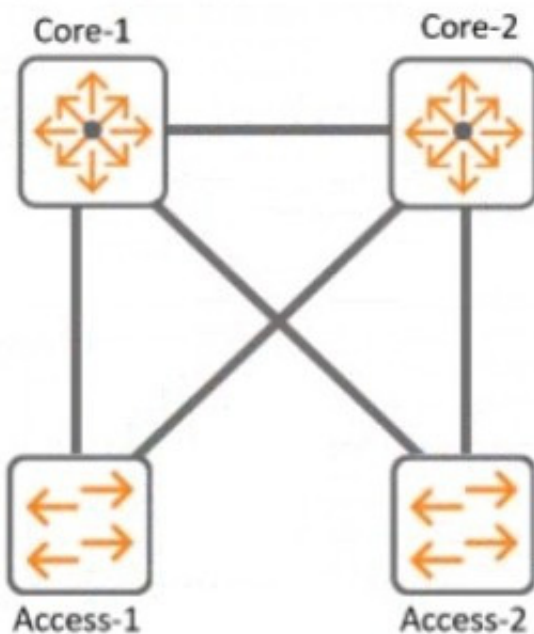
A. Create a new OSPF area, and attach VRF name.

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.

Correct 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. 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

---

QUESTION 2

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

Correct 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

---

QUESTION 3

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 4

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 1 1/1/50
    link 2 1/1/49
vsf renumber-to 3

B. On the new switch issue:

vsf member 3
    type jl726a

C. On the existing VSF issue:

vsf member 3
    stack join
    type jl726a

D. On the new switch issue:

vsf member 1
    type jl726a
    link 1 3/1/50
    link 2 3/1/49

A. Option A

B. Option B

C. Option C

D. Option D

Correct 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 5

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.

Correct 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. References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-mt/qos-15-mt- book/qos-overview.html
https://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

[HPE7-A01 VCE Dumps](#)   [HPE7-A01 Study Guide](#)   [HPE7-A01 Braindumps](#)