

HP.HPE7-A01.v2026-10-28.q69

Exam Code:	HPE7-A01
Exam Name:	Aruba Certified Campus Access Professional Exam
Certification Provider:	HP
Free Question Number:	69
Version:	v2026-10-28
# of views:	199
# of Questions views:	690
https://www.freepdfdumps.com/HP.HPE7-A01.v2026-10-28.q69.html	

NEW QUESTION: 1

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

Answer: C (LEAVE A REPLY)

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/>

NEW QUESTION: 2

You are configuring an SVI on an Aruba CX switch that needs to have the following characteristics:

- * VLANID = 25
- . IPv4 address 10.105.43.1 with mask 255.255.255.0
- * IPv6 address fd00:5708::f02d:4df6 with a 64 bit prefix length
- * member of VRF eng
- * VRF eng and VLAN 25 have not yet been created

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

A.

```
vrf eng
vlan 25
interface vlan 25
ip address 10.105.43.1 255.255.255.0
ipv6 address fd00:5708::f02d:4df6/64
vrf attach eng
```

B.

```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
```

C.

```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
```

D.

```
vrf eng
vlan 25
interface vlan 25
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
vrf attach eng
```

Answer: C ([LEAVE A REPLY](#))

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

Option C uses the following commands:

- * vrf eng: This command creates a VRF named eng and enters the VRF configuration mode1.
- * vlan 25: This command creates a VLAN with ID 25 and enters the VLAN configuration mode2.
- * interface vlan 25: This command creates an SVI on VLAN 25 and enters the interface configuration mode3.
- * ip address 10.105.43.1/24 ipv6 address fd00:5780::102d:4df6/64 vrf attach eng: This command assigns an IPv4 address of 10.105.43.1 with a subnet mask of 255.255.255.0 and an IPv6 address of fd00:5780::102d:4df6 with a prefix length of 64 to the SVI, and attaches it to the VRF eng.

NEW QUESTION: 3

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

- A. DMO is configured individually for each SSID in use in the network.
- B. The AP uses OOS to provide equal air time for multicast traffic,
- C. DMO is configured globally for each SSID in use in the network.
- D. The controller converts multicast streams into unicast streams.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 4

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

Client Insights

Cloud Auth

The Fabric Wizard

Policy Manager

Answer Area

Built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network blind spots

Defines user and device groups and creates the associated access enforcement rules for the physical network

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

Simplifies the creation of the overlays using an intuitive, graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways

Answer:

Client Insights

Cloud Auth

The Fabric Wizard

Policy Manager

Answer Area

Client Insights

Policy Manager

Cloud Auth

The Fabric Wizard

Built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network blind spots

Defines user and device groups and creates the associated access enforcement rules for the physical network

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

Simplifies the creation of the overlays using an intuitive, graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways

Explanation:

Answer Area

Client Insights

Policy Manager

Cloud Auth

The Fabric Wizard

Answer Area

Built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network blind spots

Defines user and device groups and creates the associated access enforcement rules for the physical network

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

Simplifies the creation of the overlays using an intuitive, graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways

NEW QUESTION: 5

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: ([SHOW ANSWER](#))

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: 6

Which feature supported by SNMPv3 provides an advantage over SNMPv2c?

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

Answer: D ([LEAVE A REPLY](#))

Encryption is a feature supported by SNMPv3 that provides an advantage over SNMPv2c. Encryption protects the confidentiality and integrity of SNMP messages by encrypting them with a secret key. SNMPv2c does not support encryption and relies on community strings for authentication and authorization, which are transmitted in clear text and can be easily intercepted or spoofed. Transport mapping, community strings, and GetBulk are features that are common to both SNMPv2c and SNMPv3. References:

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmp.htm

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmpv3.htm

NEW QUESTION: 7

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 the APs 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?

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

A. associate lldp-group IAP-Group

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

B. no shutdown

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

C. associate lldp-group IAP-Group

```

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

```

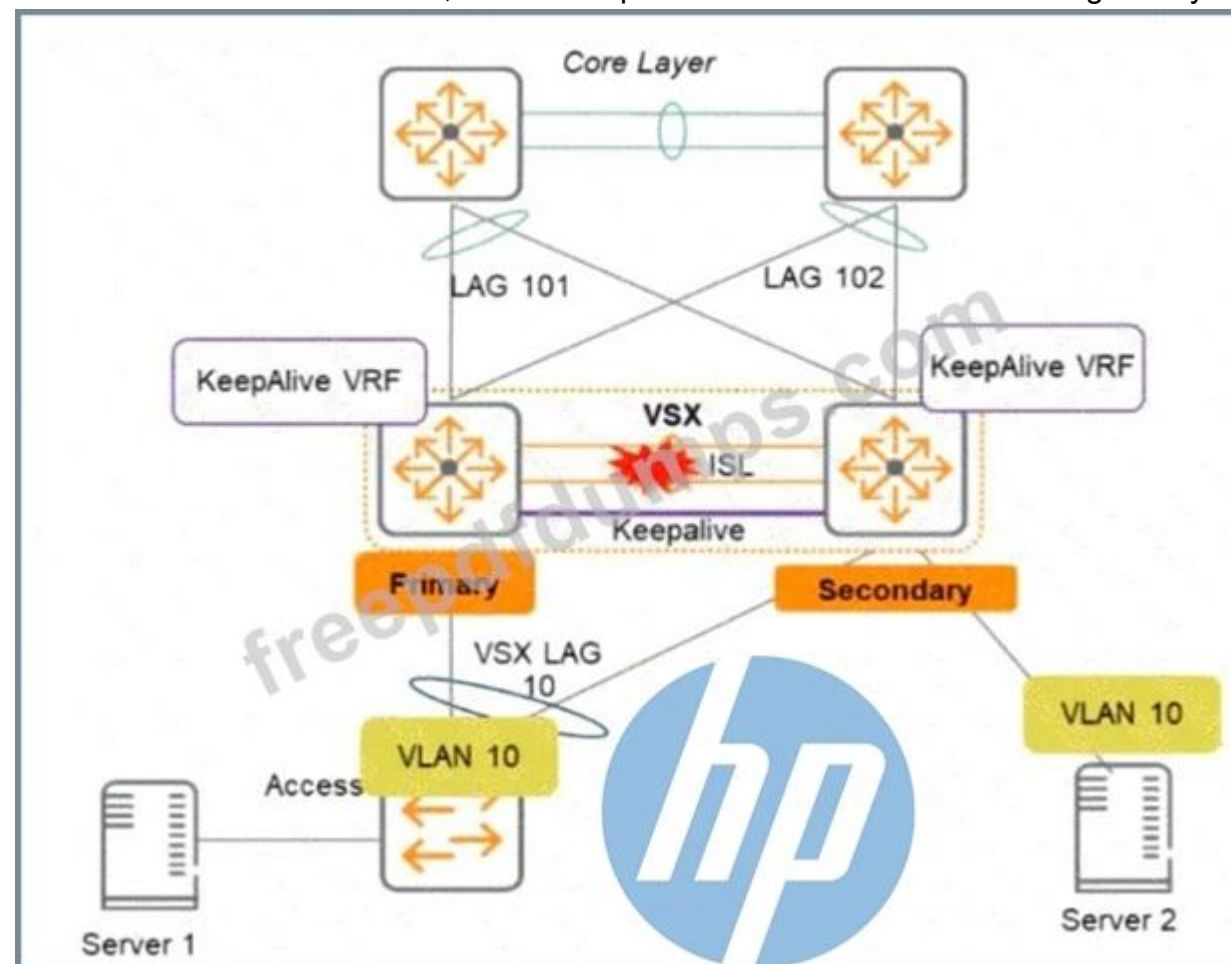
D.

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 8

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: ([SHOW ANSWER](#))

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: 9

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 10

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 OSPF process ID with a custom routing table.
- D. Attach OSPF process ID in the VRF configuration.

Answer: B ([LEAVE A REPLY](#))

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>

NEW QUESTION: 11

You are building a configuration in Central that will be used for a standardized network design for small sites for your company. You want to use GUI configuration for gateways and APs, while template configuration for switches. You need to align with Aruba best practices.

Which set of actions will satisfy these requirements?

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

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

Answer: C ([LEAVE A REPLY](#))

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

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

NEW QUESTION: 12

AppRF 2.0 allows you to:

- A.** monitor applications and radio frequencies
- B.** customize application signatures
- C.** classify web content based on reputation
- D.** configure ACL and bandwidth control for applications

Answer: (SHOW ANSWER)

NEW QUESTION: 13

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

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

Answer: A ([LEAVE A REPLY](#))

OCSP is a protocol that allows clients to query the CA or a trusted responder for the status of a specific certificate. OCSP requests and responses are smaller and faster than CRLs, and they can provide real-time information about the revocation status of a certificate¹². CRLs are lists of all revoked certificates that are downloaded from the CA. CRLs can present issues, as they can become outdated and have to be downloaded frequently¹³. Therefore, OCSP reduces latency between the time a certificate is revoked and validation reflects this status. References: 1 <https://sectigostore.com/blog/ocsp-vs-crl-whats-the-difference/> 2

<https://www.keyfactor.com/blog/what-is-a-certificate-revocation-list-crl-vs-ocsp/> 3 <https://www.fortinet.com/resources/cyberglossary/ocsp>

NEW QUESTION: 14

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

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

Answer: (SHOW ANSWER)

MPSK Local is a feature that can be used to set up 15 headless IoT devices that do not support 802.1X authentication. MPSK Local allows the switch to automatically generate and assign unique 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 802.1X authentication, which is not supported by the IoT devices, or WPA3 encryption, which is not supported by Aruba CX switches. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html>

<https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch06.html>

NEW QUESTION: 15

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

- A. SNMPv3
- B. DSCP
- C. TLV
- D. CDP

Answer: (SHOW ANSWER)

The correct answer is A. SNMPv3.

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

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

- * Implement and Analyze the output from common network monitoring tools
- * Configure Port Mirroring to collect PCAPs
- * Configure NAE agents 9.4
- * Configure UXI sensors for internal and external tests
- * Describe how API scan be used to configure, manage, monitor, and troubleshoot your network The document also mentions that the candidate should have a distinguished understanding of different protocols across vendors, which implies that they should be familiar with SNMPv3 and how it can be used to access MIB data.

NEW QUESTION: 16

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

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

Answer: A (LEAVE A REPLY)

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

Valid HPE7-A01 Dumps shared by Actual4test.com for Helping Passing HPE7-A01 Exam! Actual4test.com now offer the **newest HPE7-A01 exam dumps**, the Actual4test.com HPE7-A01 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com HPE7-A01 dumps with Test Engine here: https://www.actual4test.com/HPE7-A01_examcollection.html (**164** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 17

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

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

- A. Spanning-tree configuration is synced by default with VSX.
- B. Enable vsx-sync stp-global in vsx mode to sync the configuration.
- C. Use vsx-sync in the MSTP region configuration to get synced.
- D. Enable vsx-peer stp-global in vsx mode to sync the configuration.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 18

A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working to a remote site connected via layer-3 All legacy devices are connected to a dedicated Aruba CX 6200 switch at each site.

What technology on the Aruba CX 6200 could be used to meet this requirement?

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

Answer: (SHOW ANSWER)

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

<https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html>

<https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html>

NEW QUESTION: 19

Refer to the output from a CX 6100 switch:



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

- A. The dBm values for Tx are too high and affect Rx signals.
- B. The dBm values for Rx are within acceptable values, and the link is up.

- C. The dbm values for T are too far away from 0, and the link is down.
- D. The dBm values for Rx are too low, indicating that the link is down.

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 20

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

What is the appropriate solution for this scenario?

- A. Enable EAP-TLS on all wireless devices. Enable EAP-TTLS on all wireless devices.
- B. Configure RedSec on the AP and the RADIUS server.
- C. Enable IPSec under Data Handling in HPE Aruba Networking Central

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 21

You are configuring Policy Based Routing (PBR) for a subnet that will be used to test a new default route for your network Traffic originating from 10.2.250.0/24 should use a new default route to 10.1.1.253. Other non-default routes for this subnet should not be affected by this change.

What are two parts of the solution for these requirements? (Select two.)

- A.

```
pbr-action-list def_route_test
default-nexthop 10.1.1.253/24
```

- B.

```
class ip test_subnet
 10 match any 10.2.250.0/24 any
policy def_route_test_policy
 10 class ip test_subnet action pbr def_route_test
interface vlan 100
 ip address 10.2.250.0/24
 apply policy pbr_test routed in
```

- C.

```
class ip test_subnet
 10 match any 10.2.250.0 255.255.255.0 any
policy def_route_test_policy
 10 class ip ip_test_subnet action pbr def_route_test
interface vlan 100
 ip address 10.2.250.0/24
 apply policy pbr_test routed out
```

- D.

```
pbr-action-list def_route_test
default-nexthop 10.1.1.253
interface null
```

- E.

```
pbr-action-list def_route_test
nexthop 10.1.1.253
interface null
```

Answer: [\(SHOW ANSWER\)](#)

Two parts of the solution for these requirements are Option C and Option E.

Option C is a part of the solution because it defines a policy-based routing action list named route_test, which specifies the next hop IP address as 10.1.1.253 for the matching traffic. This is the new default route that the user wants to use for the subnet 10.2.250.0/24. The interface null parameter indicates that the traffic will be routed to the next hop without using a specific interface1.

Option E is a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 250, which has an IP address of 10.2.250.1/24. This is the subnet that the user wants to test the new default route for. The apply policy command enables policy-based routing on the interface and associates it with the action list2.

Option A is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify the next hop IP address as 10.1.1.253, which is the new default route that the user wants to use. Instead, it specifies a next hop IP address of 10.1.1.254, which is different from the requirement.

Option B is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify any next hop IP address at all, which is necessary for policy-based routing to work. Instead, it specifies an interface null parameter without any IP address, which is invalid.

Option D is not a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 200, which has an IP address of 10.2.200.1/24. This is not the subnet that the user wants to test the new default route for, but a different subnet that should not be affected by this change.

NEW QUESTION: 22

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

The user was not limited to viewing nonsensitive configuration information and a level of 1 was not assigned to their role Which default management role should have been assigned for the user?

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

Answer: B (LEAVE A REPLY)

The default management role that should have been assigned for the user is B. operators.

The operators user role is a predefined role that allows users to view nonsensitive configuration information on the switch, such as interfaces, VLANs, routing protocols, statistics, and more. The operators user role has a privilege level of 1, which is the lowest level of access on the switch1.

The administrators user role is a predefined role that has full access to all switch configuration information and all REST API methods. This role is more than what the Director of Security requires1.

NEW QUESTION: 23

Refer to the exhibit.

Access Points				
Switches				
Gateways				
WLANs	Access Points	Radios	Interfaces	Security
Services	System	IoT	Configuration Audit	
Wireless SSIDs				
Name (Profile)	Security	Access type	Traffic forwarding mode	Network Enabled
secure_wireless	wpa3-enterprise	Role Based	Bridge	Yes
open_wireless	opensystem	Unrestricted	Bridge	Yes

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

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

Answer: D ([LEAVE A REPLY](#))

According to the Aruba Campus Access Professional documents¹, WPA3-Enterprise is a security mode that supports 802.1X authentication and encryption with either AES-CCM or AES-GCMP. WPA3-Enterprise also optionally adds usage of Suite-B 192-bit minimum-level security suite that is aligned with Commercial National Security Algorithm (CNSA) for enterprise networks². This mode provides the highest level of security and is suitable for government and financial institutions.

The exhibit shows that the SSID is configured with WPA3-Enterprise (CCM), which uses AES-CCM as the encryption protocol. However, this mode is not compatible with some devices that require CNSA compliance. Therefore, changing the SSID to WPA3-Enterprise (CNSA) would fix the issue and allow all devices to connect to the network.

NEW QUESTION: 24

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

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

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 25

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

- A. Multiple Pre-Shared Keys (MPSK) with WPA3-AES
- B. Multiple Pre-Shared Keys (MPSK) Local
- C. HPE Aruba Networking ClearPass profiling with WPA-PSK
- D. HPE Aruba Networking ClearPass profiling with MAC-AUTH

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 26

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 ([LEAVE A REPLY](#))

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: 27

The administrator notices that wired guest users that have exceeded their bandwidth limit are not being disconnected. Access Tracker in ClearPass indicates a disconnect CoA message is being sent to the AOS-CX switch.

An administrator has performed the following configuration:

```
Access1(config)# ip dns host cppm.arubatraining.com 10.254.1.23 vrf mgmt
Access1(config)# radius-server host cppm.arubatraining.com key plaintext aruba123 vrf mgmt
Access1(config)# aaa group server radius cppm
Access1(config-sg)# server cppm.arubatraining.com vrf mgmt
Access1(config-sg)# exit
Access1(config)# aaa accounting port-access start-stop interim 5 group cppm
Access1(config)# radius dyn-authorization client cppm.arubatraining.com secret-key plaintext aruba123 vrf mgmt
Access1(config)# radius dyn-authorization enable
```

What is the most likely cause of this issue?

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

Answer: D (LEAVE A REPLY)

Change of Authorization (CoA) is a feature that allows ClearPass Policy Manager (CPPM) to send messages to network devices such as switches to change the authorization state of a user session. CoA requires that both CPPM and the network device support this feature and have it enabled. For AOS-CX switches, CoA must be globally enabled using the command `radius-server coa enable`. If CoA is not enabled on the switch, the disconnect CoA message from CPPM will be ignored and the user session will not be terminated. References:

https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/index.htm#CPPM_UserGuide/Admin/ChangeOfAuthorization.htm https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html

NEW QUESTION: 28

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

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

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 29

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

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

Answer:

802.3at	802.3bt	802.3af
---------	---------	---------

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

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

NEW QUESTION: 30

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: A,E (LEAVE A REPLY)

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: 31

you are implementing ClearPass Policy Manager with EAP-TLS for authenticating all corporate-owned devices.

What are two possible solutions to the problem of deploying client certificates to corporate MacBooks that are joined to a Windows domain? (Select two.)

- A. ClearPass OnBoard
- B. Windows Server PKI and a GPO
- C. Apple Configurator and a GPO
- D. ClearPass OnGuard
- E. Mobile Device Manager

Answer: (SHOW ANSWER)

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

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

Valid HPE7-A01 Dumps shared by Actual4test.com for Helping Passing HPE7-A01 Exam! Actual4test.com now offer the **newest HPE7-A01 exam dumps**, the Actual4test.com HPE7-A01 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com HPE7-A01 dumps with Test Engine here: https://www.actual4test.com/HPE7-A01_examcollection.html (**164** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 32

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

- A. Sixteen different VMACs are supported total as shared.
- B. Active Gateway can once MSTP instances are created for VLAN load sharing.
- C. Sixteen different VMACS are supported for each IPV4 and IPV6 stack simultaneously
- D. copied over the ISL link for an optimized path.

Answer: (SHOW ANSWER)

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

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

The other options are incorrect because:

- A) Sixteen different VMACs are not supported total as shared. They are supported for each IPv4 and IPv6 stack separately.
- B) Active gateway can be used without MSTP instances. MSTP is a protocol that allows multiple spanning tree instances to coexist on the same switch, but it does not affect how active gateway works.
- D) Active gateway does not copy traffic over the ISL link for an optimized path. It avoids using the ISL link for routed traffic and uses the local switch interface MAC instead of the virtual MAC address (VMAC) for source address1.

NEW QUESTION: 33

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

- A. Authenticated Diffie-Hellman is not utilized
- B. The gateway will not respond.
- C. No encryption is applied.
- D. RADIUS protocol is utilized.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 34

List the firewall role derivation flow in the correct order

Firewall Role

Authentication default role

Initial role assigned

Server derived role

User derived role

Order

Answer:

Firewall Role

Authentication default role

Initial role assigned

Server derived role

User derived role

Order

Server derived role

User derived role

Authentication default role

Initial role assigned

Explanation:

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

* Server derived role

- * User derived role
- * Authentication default role
- * Initiation role assigned

NEW QUESTION: 35

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

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

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

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

Answer: C ([LEAVE A REPLY](#))

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: 36

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

Client Insights

Cloud Auth

The Fabric Wizard

Policy Manager

Answer Area

Built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network blind spots

Defines user and device groups and creates the associated access enforcement rules for the physical network

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

Simplifies the creation of the overlays using an intuitive, graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways

Answer:



Answer Area

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

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

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

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

Explanation:



Answer Area

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

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

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

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

NEW QUESTION: 37

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

What is the appropriate solution for this scenario?

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

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 38

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

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

Answer: A (LEAVE A REPLY)

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

Option A: Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway This is because option A shows how to implement an IPSec tunnel between two devices using the interface command and the ipsec command. An IPSec tunnel can provide encryption and authentication for PAPI traffic between two devices, such as an AOS-CX switch and a gateway².

Therefore, option A is a feasible option to protect this traffic.

I hope this helps you. If you need more information, please let me know. #

1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7727/Content/Chp_prev_traf_loss/Act_gtw_act_fwd/act-gat-ove-vsx-10.htm

2: <https://community.arubanetworks.com/blogviewer?blogkey=989fc43a-e0df-42db-9c0b-f96d6565a1fa>

NEW QUESTION: 39

Which statement best describes QoS?

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

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 40

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

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

Answer: D (LEAVE A REPLY)

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

* Dual control plane provides better resiliency. Unlike stacking, where switches share a single control plane, VSX switches have independent control planes that synchronize their states over an inter-switch link (ISL).

This means that if oneswitch fails or reboots, the other switch can continue to operate without affecting traffic flows or network services.

* Active-active forwarding provides better performance. Unlike spanning tree, where some links are blocked to prevent loops, VSX switches use all available links for forwarding traffic, providing load balancing and increased bandwidth utilization.

* Multichassis LAG provides better redundancy. Unlike single-chassis LAG, where all member ports belong to one switch, VSX switches can form multichassis LAGs with downstream or upstream devices, where member ports are distributed across both switches. This provides link redundancy and seamless failover in case of switch or port failure.

References: https://www.arubanetworks.com/assets/tg/TG_VSX.pdf

NEW QUESTION: 41

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

- A. CoS has much finer granularity than DSCP
- B. CoS is only contained in VLAN Tag fields DSCP is in the IP Header and preserved throughout the IP packet flow
- C. They are similar and can be used interchangeably.
- D. CoS is only used to determine CLASS of traffic DSCP is only used to differentiate between different Classes.

Answer: (SHOW ANSWER)

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>

NEW QUESTION: 42

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: C (LEAVE A REPLY)

https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7885/Content/Chp_Mng_Use/bui-in- use-gro-the-pri-10.htm

NEW QUESTION: 43

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

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

Answer: (SHOW ANSWER)

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

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

NEW QUESTION: 44

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

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

- A. Confirm that NTP is configured on the switch and ClearPass
- B. Configure dynamic authorization on the switch.
- C. Bounce the switchport
- D. Use Dynamic Segmentation.
- E. Configure dynamic authorization on the switchport

Answer: (SHOW ANSWER)

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

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

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

NEW QUESTION: 45

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 icmp 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 (LEAVE A REPLY)

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: 46

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

- A. 807.11ah
- B. 802.11be
- C. 802.11mc
- D. 802.11v

Answer: (SHOW ANSWER)

Valid HPE7-A01 Dumps shared by Actual4test.com for Helping Passing HPE7-A01 Exam! Actual4test.com now offer the **newest HPE7-A01 exam dumps**, the Actual4test.com HPE7-A01 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com HPE7-A01 dumps with Test Engine here: https://www.actual4test.com/HPE7-A01_examcollection.html (164 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 47

Refer to Exhibit:

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

What would be the correct action to fix the issue?

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

Answer: C (LEAVE A REPLY)

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

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

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

- * Select the Security Level from the drop-down list. The following options are available:
- * WPA3-Personal: This option uses Simultaneous Authentication of Equals (SAE) to provide stronger password-based authentication and key exchange than WPA2-Personal.
- * WPA3-Enterprise: This option uses 192-bit cryptographic strength for authentication and encryption, as defined by the Commercial National Security Algorithm (CNSA) suite.
- * WPA3-Enterprise (CCM): This option uses 128-bit cryptographic strength for authentication and encryption, as defined by the Counter with CBC-MAC (CCM) mode.
- * WPA3-Enhanced Open: This option uses Opportunistic Wireless Encryption (OWE) to provide encryption for open networks without requiring authentication.

The other options are incorrect because:

- * A. WPA3-Enterprise (CNSA) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company's use case.
- * B. WPA3-Personal is a valid SSID type, but it requires a passphrase to join the network, which may not be suitable for the company's use case.
- * D. WPA3-Enterprise (CCM) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company's use case.

NEW QUESTION: 48

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?

```
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
```

A.

```
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
```

B.

```
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
```

C.

```
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
```

D.

Answer: B ([LEAVE A REPLY](#))

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: 49

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: (SHOW ANSWER)

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: 50

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 ([LEAVE A REPLY](#))

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 dBm. 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:

$$EIRP = 16 + 8 = 24 \text{ dBm}$$

Therefore, the answer B is correct.

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

NEW QUESTION: 51

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

- A. dead interval is 200ms by default
- B. dead interval is 20s by default
- C. dead interval is based on the value set for hello interval
- D. dead interval is disabled by default

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 52

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

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

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

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

Answer: ([SHOW ANSWER](#))

The calculated Equivalent Isotropic Radiated Power (EIRP) for AP1 is 17 dBm.

EIRP is the measured radiated power of an antenna in a specific direction. It is equal to the input power to the antenna multiplied by the gain of the antenna. It can also take into account the losses in transmission line, connectors, and other components. The formula for EIRP is:

$$\text{EIRP} = P + G - L$$

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

For AP1, we have:

$$P = 10 \text{ dBm} \quad G = 9 \text{ dBi} \quad L = 2 \text{ dB}$$

Therefore,

$$\text{EIRP} = 10 + 9 - 2 \quad \text{EIRP} = 17 \text{ dBm}$$

NEW QUESTION: 53

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: ([SHOW ANSWER](#))

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: 54

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: ([SHOW ANSWER](#))

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: 55

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

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

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 56

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

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

Answer: **B,D** ([LEAVE A REPLY](#))

NEW QUESTION: 57

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

- A.** MAC caching
- B.** MAC Authentication
- C.** Authentication survivability
- D.** Opportunistic key caching

Answer: **C** ([LEAVE A REPLY](#))

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

NEW QUESTION: 58

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: ([SHOW ANSWER](#))

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: 59

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

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

Answer: C ([LEAVE A REPLY](#))

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.](https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-access-control.htm)

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: 60

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

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

Answer: A,D ([LEAVE A REPLY](#)**)**

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

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

NEW QUESTION: 61

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 ([LEAVE A REPLY](#)**)**

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/>

Valid HPE7-A01 Dumps shared by Actual4test.com for Helping Passing HPE7-A01 Exam! Actual4test.com now offer the **newest HPE7-A01 exam dumps**, the Actual4test.com HPE7-A01 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com HPE7-A01 dumps with Test Engine here: https://www.actual4test.com/HPE7-A01_examcollection.html (**164** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 62

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

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

Answer: A ([LEAVE A REPLY](#)**)**

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

Option A: The switch will put the client on the access VLAN

This is because option A shows how UBT works on an Aruba switch. When a device connects to the network, it is authenticated using either MAC Authentication or 802.1X and triggers an enforcement policy from ClearPass, which contains an enforcement profile with a user role configuration. The user role can be assigned locally on the switch or on ClearPass as part of an enforcement profile. The user role determines the VLAN that the device belongs to and the access policies that apply to it³.

Therefore, option A is correct.

1: <https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-ubt.htm>

2: <https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html>

3: <https://community.arubanetworks.com/viewdocument/?DocumentKey=c740df4e-3e26-4cc5-9126-355a18709c44&CommunityKey=2fd943a6-8898-4dbe-915f-4f09e4d3c317&tab=librarydocuments>

NEW QUESTION: 63

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

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

Answer: A,C ([LEAVE A REPLY](#))

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

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

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

The other options are incorrect because:

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

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

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

NEW QUESTION: 64

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 ([LEAVE A REPLY](#))

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: 65

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 66

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

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

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

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 67

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

Answer:



Answer Area

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

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: 68

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

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

Answer: C ([LEAVE A REPLY](#))

To allow a new VLAN 100 between VSX pair inter-switch-link 256 for port 1/45 and 2/45, you need to use the command `vlan trunk allowed 100` in LAG256. This will add VLAN 100 to the list of allowed VLANs on the trunk port LAG256, which is part of the inter-switch-link between VSX peers. The other options are incorrect because they either do not use the correct command or do not specify the correct port or VLAN.

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: 69

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

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

Answer: ([SHOW ANSWER](#))

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

Valid HPE7-A01 Dumps shared by Actual4test.com for Helping Passing HPE7-A01 Exam! Actual4test.com now offer the **newest HPE7-A01 exam dumps**, the Actual4test.com HPE7-A01 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com HPE7-A01 dumps with Test Engine here: https://www.actual4test.com/HPE7-A01_examcollection.html (**164** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)