DUMPSARENA

# HPE Aruba Networking Certified ProfessionalSwitching

## HP HPE7-A08

**Version Demo**

**Total Demo Questions: 16**

**Total Premium Questions: 164**

**Buy Premium PDF**

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Network Stack | 5 |
| Topic 2, Network Infrastructure | 49 |
| Topic 3, Network Services | 27 |
| Topic 4, Network Security | 26 |
| Topic 5, Network Management | 43 |
| Topic 6, Troubleshooting | 14 |
| Total | 164 |

QUESTION NO: 1

Which two configuration tasks must be performed when creating a device profile for an AP? (Select two.)

**A.** Associate a role

**B.** Associate a QoS policy

**C.** Associate an LLDP group

**D.** Associate a VLAN

**E.** Associate an ACL

**ANSWER: A C**

**Explanation:**

A device profile on an AOS-CX switch connects device-identification criteria with the policy that the switch must apply when it recognizes that device. Therefore, **Associate a role** is required: the role supplies the port configuration and enforcement parameters that are to be dynamically applied to the interface after the AP is identified. A role can contain the relevant access-control and network-service settings, allowing the profile to apply a consistent policy to AP-facing ports.

**Associate an LLDP group** is also required because the LLDP group provides the identification match for the connected AP. The switch uses LLDP information advertised by the endpoint to evaluate the group criteria. When an AP matches the LLDP group, the device-profile association selects the configured role and applies it to that port. This creates the required detection-to-policy workflow without relying on a RADIUS-driven dynamic-role assignment.

In short, a functional AP device profile needs both an LLDP-based classification association and a role association: one identifies the endpoint and the other defines the treatment it receives. Aruba documents device-profile configuration and its LLDP group/role associations in the AOS-CX Security Guide: Device Profiles and related command details in the Device Profile Commands reference.

**QUESTION NO: 2**

You need to configure BGP on an HPE Aruba Networking switch using AS 65010. What is required when establishing peering with neighboring devices using eBGP that are not directly connected?

**A.** Use of next-hop-self

**B.** Use of ebgp-multihop

**C.** Use of route-reflector

**D.** Use of address-family ipv4 external

**ANSWER: B**

**Explanation:**

Use of ebgp-multihop is required when an eBGP peer is reached through one or more intervening Layer 3 hops. By default, an eBGP session uses an IP time-to-live value of 1, which limits the BGP packets to directly connected peers. Configuring eBGP multihop raises the permitted TTL so that the TCP session for BGP, which uses port 179, can reach a peer beyond the directly connected subnet. On ArubaOS-CX, this is configured under the relevant BGP neighbor with the `ebgp-multihop` command and an appropriate maximum-hop value. The value should be selected to cover the actual routed path while remaining as restrictive as practical. This setting is commonly used for eBGP peering to loopback addresses, across a routed transit network, or to an external peer that is multiple hops away. The local AS number 65010 identifies the switch's BGP autonomous system, while eBGP multihop addresses the separate reachability constraint imposed by the default one-hop eBGP TTL behavior. Aruba's BGP configuration guidance documents the neighbor-level eBGP multihop setting: ArubaOS-CX ebgp-multihop command reference. General BGP protocol behavior is specified in RFC 4271.

## QUESTION NO: 3

A pair of CX switches is configured as VSX and provides the default gateway for a VLAN. Servers are dual-homed through VSX LAGs, and the customer requires both VSX members to forward traffic sent to the default gateway while hosts retain one default-gateway IP address. Which feature should be configured?

**A.** Configure Active Gateway.

**B.** Configure VRRP.

**C.** Configure a VSX LAG.

**D.** Configure a VRF.

## ANSWER: A

**Explanation:**

**Active Gateway** is designed for this VSX gateway requirement. Both VSX members share the same virtual gateway IP and virtual MAC address, allowing either member to route traffic received from connected hosts. This enables active-active default-gateway forwarding while clients use a single, consistent gateway address.

VRRP provides gateway redundancy, but it normally uses an active/standby forwarding model. A VSX LAG provides resilient Layer 2 attachment for the servers, but it does not itself provide the shared Layer 3 gateway function. A VRF provides routing separation rather than gateway redundancy.

## QUESTION NO: 4

You have recently configured WMM to DSCP mapping on your HPE Aruba Networking APs and want to make sure that only the correct traffic is prioritized on the wired network. What should you configure to achieve this? (Choose two.)

**A.** DSCP trust on the AP user-role

**B.** DSCP trust on ports connected to APs

**C.** LLDP based on QoS policy

**D.** Colorless ports

**E.** DSCP trust globally

## ANSWER: A B

**Explanation:**

DSCP trust on the AP user-role and DSCP trust on ports connected to APs provide the required ingress trust boundary for traffic leaving an AP and entering the wired network. WMM-to-DSCP mapping marks packets according to their wireless access category before the AP forwards them to Ethernet. The wired QoS policy must therefore preserve and classify packets from that trusted AP source by using the DSCP value that the AP has applied.

Configuring DSCP trust on the physical switch interfaces used by APs makes the policy explicit at the wired ingress point. This allows the switch QoS classifier and queues to use the received DSCP values for forwarding treatment. Configuring DSCP trust in the AP user-role applies the same trust behavior through the role-based policy assigned to the AP. This is useful where role-based access is used, because the AP's authorized identity and its QoS handling remain associated even when the AP connection is dynamically assigned.

Using both controls ensures that DSCP markings are honored only for authenticated, policy-approved AP traffic, preserving the intended end-to-end voice, video, and best-effort treatment. Aruba's QoS documentation describes DSCP trust as an ingress classification mechanism, while Aruba wireless documentation covers WMM and DSCP marking behavior. See the AOS-CX QoS Guide and ArubaOS WMM-to-DSCP mapping documentation.

## QUESTION NO: 5


Refer to the exhibit for an HPE Aruba Networking CX 6300M VSF:

What VSF configuration is required for the stack configuration to work and avoid split-brain?

**A.** vsf start-auto-stacking

**B.** vsf secondary-member 2

**C.** vsf conductor-member 2

**D.** vsl split-detect mgrep

**E.** vsf split-detect mgmt

## ANSWER: E

**Explanation:**

`vsf split-detect mgmt` is the required ArubaOS-CX VSF configuration when the members have management interfaces connected through an independent management network, as depicted for this type of VSF design. It enables the VSF split-detection mechanism to use management-network reachability as an additional path to determine whether a VSF link failure is an actual member isolation event. This is essential for preventing two separated stack fragments from both continuing to operate as active control planes, which is the split-brain condition.

When the VSF links between members fail, split detection lets the stack determine whether the peer is still reachable through the out-of-band management path. The resulting role and forwarding behavior protects network consistency while the VSF topology is partitioned. The management connectivity used for this purpose must remain independent of the VSF links so that it is still available during a VSF-link failure. Aruba documents management-based split detection for VSF in the ArubaOS-CX VSF Guide and the associated CLI command reference: ArubaOS-CX VSF Guide and vsf split-detect mgmt command reference.

## QUESTION NO: 6

A network-management platform must receive sampled traffic-flow information from CX switches by using sFlow. Which two configuration tasks are required to export sFlow samples to the collector? (Choose two.)

**A.** Configure the sFlow collector address.

**B.** Enable packet sampling on the interfaces to be monitored.

**C.** Configure a local mirror destination interface.

**D.** Configure an SNMP trap receiver as the sFlow destination.

**E.** Enable DHCP snooping on the monitored VLANs.

**ANSWER: A B**

**Explanation:**

The switch must be configured with the sFlow collector destination so that sampled datagrams have a remote management endpoint. Sampling must also be enabled on the interfaces that should contribute traffic samples; interface sampling settings determine where the switch observes packets.

A mirror destination port creates full packet copies for local analysis rather than sampled flow telemetry. An SNMP trap receiver does not act as an sFlow collector.

## QUESTION NO: 7

Your customer ' s CX switches are managed in HPE Aruba Networking Central. If a VSX primary switch is accidentally powered off, which alert will be triggered?

**A.** Switch Reboot

**B.** Switch Stack Conductor Change

**C.** Switch Disconnected

**D.** Switch STP Root Change

**ANSWER: C**

**Explanation:**

**Switch Disconnected** is the expected HPE Aruba Networking Central alert when the VSX primary is powered off. A power loss immediately stops the switch's management-plane communication with Central, including its secure connection and periodic status updates. After Central's connectivity monitoring determines that the device is no longer reachable, it generates a disconnected-device alert for that switch. This alert enables administrators to identify the affected switch quickly and investigate a physical power issue, upstream connectivity failure, or an unexpected device outage. The switch's role as the VSX primary does not prevent Central from monitoring it as an individual managed device; Central still reports the loss of that device's connection. In a VSX deployment, the peer may continue forwarding traffic according to the configured VSX and network resiliency design, but the powered-off primary itself remains unavailable to Central until it is restored and reconnects. Aruba Central documentation describes alert monitoring and device connectivity events in its alerts documentation, while the AOS-CX VSX guide provides the relevant high-availability context: HPE Aruba Networking Central Alerts and AOS-CX VSX Guide.

## QUESTION NO: 8

A customer has asked if their new CX switches will support their legacy management system. Which of these would this include? (Choose two.)

**A.** CLI

**B.** REST API

**C.** NAE

**D.** HTTPS

**E.** SNMP

**ANSWER: A E**

**Explanation:**

CLI and SNMP are the appropriate compatibility interfaces for a legacy network-management environment. AOS-CX provides a command-line interface for direct administrative access and for established operational workflows that use scripts or terminal-based automation to retrieve status and apply configuration. This preserves a familiar management path for teams moving from conventional switch operating systems to Aruba CX.

SNMP is also a core interoperability interface because established network-management systems commonly poll devices for inventory, interface counters, operational state, fault information, and other monitored values through standard SNMP MIB objects. AOS-CX supports SNMP operation, allowing an existing monitoring platform to continue collecting switch telemetry and receiving relevant management information without requiring an immediate migration to a new management architecture. Aruba's AOS-CX documentation identifies both the CLI and SNMP among the supported switch management and monitoring capabilities. See the AOS-CX management interfaces documentation and the AOS-CX SNMP documentation.

## QUESTION NO: 9

You are helping another engineer troubleshoot a new downloadable user role configuration between your CX switches and ClearPass. Which configuration on the switch should you verify?

**A.** HTTPS client certificate

**B.** REST API credentials

**C.** SNMP community string

**D.** User-role configuration

## ANSWER: A

**Explanation:**

**HTTPS client certificate** is the switch configuration to verify because a downloadable user role is retrieved by the AOS-CX switch from ClearPass through a secured HTTPS connection. After successful network access authentication, ClearPass can return the role information that instructs the switch to obtain the downloadable role definition. The switch therefore operates as an HTTPS client while contacting the ClearPass service that provides the role. The TLS settings must be valid for that transaction to succeed.

In practice, verify that the switch has the required client certificate configured when ClearPass is configured for mutual TLS, that the corresponding private key is available and usable, and that the ClearPass certificate chain is trusted by the switch. Also confirm certificate validity dates, the identity expected by ClearPass, and connectivity to the ClearPass HTTPS service in the applicable VRF. A certificate or trust failure can prevent the secure role retrieval even though the initial RADIUS exchange is otherwise successful. Aruba documents downloadable roles as part of its ClearPass and dynamic-segmentation access-control workflow; see Aruba ClearPass Downloadable User Roles documentation and the AOS-CX Security Guide.

## QUESTION NO: 10 - (SIMULATION)

Company A has an existing HPE Aruba Networking CX 8325 VSX. It has acquired Company B and must merge its networks onto the same VSX switch configuration as Company A. Both Company A and Company B share the same 10.100.100.1/21 subnet.

What is the correct order for creating a configuration allowing overlapping networks in the setup?

## ANSWER: See the explanation for the answer

**Explanation:**

**Correct order:** create the separate VRFs first, create separate VLAN/SVI interfaces for each company, attach each SVI to its VRF, and only then configure the overlapping IP subnet on the SVIs.

1. Create a VRF for Company A and a different VRF for Company B.
2. Create distinct VLANs for the two companies (for example, VLAN 100 for A and VLAN 200 for B).

3. Create/configure each VLAN interface (SVI).
4. On each SVI, use `vrf attach <vrf-name>` **before** assigning its IP address.
5. Configure `10.100.100.1/21` on both SVIs. This is valid because each SVI is now in a different VRF.
6. Apply the equivalent required configuration on both VSX peers (or use the applicable VSX synchronization process), so both switches have matching VLAN/VRF gateway connectivity.

```
vrf COMPANY_A
vrf COMPANY_B

vlan 100
vlan 200

interface vlan 100
   vrf attach COMPANY_A
   ip address 10.100.100.1/21

interface vlan 200
   vrf attach COMPANY_B
   ip address 10.100.100.1/21
```

The key simulation point is that the `vrf attach` operation must occur **before** the duplicate IP subnet is configured. An IP prefix cannot overlap within the same routing table, but it can be reused in separate VRFs.

## QUESTION NO: 11

A merger connects a partner network through an eBGP peer. The customer must accept only the partner prefixes that have been approved, and must advertise only the customer aggregate to that peer. Which two policy actions should be configured? (Choose two.)

**A.** Apply an inbound prefix-list-based route policy to the eBGP peer.

**B.** Apply an outbound prefix-list-based route policy to the eBGP peer.

**C.** Increase local preference for all routes received from the peer.

**D.** Prepend the local AS to all routes received from the peer.

**E.** Set the OSPF cost of the peer-facing interface to zero.

## ANSWER: A B

**Explanation:**

An inbound route policy using a prefix list can filter received routes so that only approved partner prefixes enter the local BGP table. An outbound route policy using a prefix list can restrict advertisements toward the partner to the intended customer aggregate.

Changing local preference affects the preferred outbound exit within the local AS, but does not prevent unwanted prefixes from being accepted or advertised. AS-path prepending influences how remote networks select an inbound path, not which routes are exchanged.

## QUESTION NO: 12 - (SIMULATION)

**Match each REST API method to the correct description.**

## ANSWER: See the explanation for the answer

**Explanation:**

**Correct REST API method matches:**

`POST` — Create a new object instance.
`PUT` — Modify a group of object properties (a complete object update/replacement).
`PATCH` — Modify object instance properties (a partial/incremental update).
`DELETE` — Remove an object instance.
`GET` — Retrieve object instance properties.

In short: `POST` creates, `GET` reads, `PUT` performs a full update, `PATCH` performs a partial update, and `DELETE` removes the resource.

## QUESTION NO: 13

Refer to the exhibit:


How can you implement route summarization for the routes originating from Area 2?

**A.** router ospf 1area 0 range 10.1.0.0/16 type inter-area

**B.** router ospf 1area 2 range 10.1.0.0/16 summary-only

**C.** router ospf 1area 2 range 10.1.0.0/16 type inter-area

**D.** router ospf 1area 0 range 10.1.0.0/16 summary-only

## ANSWER: C

**Explanation:**

`router ospf 1`
`area 2 range 10.1.0.0/16 type inter-area` is the appropriate AOS-CX configuration because inter-area OSPF route summarization is performed by an Area Border Router for routes learned within a connected nonbackbone area. The summarized networks shown originate in Area 2 and occupy the 10.1.x.x address space. The `10.1.0.0/16` range therefore aggregates the individual Area 2 prefixes into one route advertisement.

The range is configured under the source area, Area 2, on the ABR. With `type inter-area`, the ABR originates an inter-area summary advertisement for that aggregate toward the other OSPF areas, including the backbone. This reduces the number of individual intra-area prefixes that need to be advertised beyond Area 2 while preserving reachability through the ABR. Aruba AOS-CX documents the `area <AREA-ID> range <IP-ADDR/MASK> type inter-area` command specifically for configuring OSPF inter-area route summarization. See the AOS-CX OSPF area range command reference and Aruba's OSPF configuration documentation.

## QUESTION NO: 14

A customer is deploying an Any-Source Multicast application between several routed VLANs. The multicast sources and receivers are connected to different CX switch interfaces. Which two configuration elements are required for a PIM-SM design? (Choose two.)

**A.** Enable PIM on the routed interfaces carrying multicast traffic.

**B.** Configure a rendezvous point for the multicast groups.

**C.** Enable IGMP snooping globally as the multicast routing protocol.

**D.** Configure BFD on all receiver access ports.

**E.** Configure a static ARP entry for each multicast source.

**ANSWER: A B**

**Explanation:**

PIM must be enabled on the Layer 3 interfaces that participate in multicast forwarding so that the switches can form PIM neighbor relationships and build multicast distribution trees. An Any-Source Multicast PIM-SM deployment also requires a rendezvous point, which provides the shared-tree meeting point used while sources and receivers are discovered.

IGMP snooping is useful within receiver VLANs, but it is a Layer 2 optimization and does not provide routed multicast forwarding. BFD can accelerate failure detection, but it is not a PIM-SM requirement.

## QUESTION NO: 15

You are troubleshooting a complex routing issue after a recent change. Your customer has just called and reported that the issue now impacts all users. What should you do next?

**A.** Restore the last-known working configuration.

**B.** Ask the customer to send logs from each user.

**C.** Explain to the customer what the issue is.

**D.** Collect a show tech and log a case with TAC.

**ANSWER: A**

**Explanation:**

Restore the last-known working configuration is the appropriate next action because the incident has escalated from a complex routing problem to a service outage affecting every user, immediately following a change. The operational priority at this stage is service restoration and impact reduction, not continued diagnosis. Rolling back the recent change to the last verified working configuration removes the most likely source of the disruption and returns the network to a known stable state as quickly as possible. This follows standard change-management and incident-response practice: changes should have a documented backout plan, and that plan should be executed when a change causes unacceptable business impact. Once connectivity is restored, the team can preserve relevant evidence, review routing state and logs, determine the precise failure mechanism, and plan a controlled correction with appropriate validation and rollback procedures. Aruba AOS-CX configuration-management documentation describes retaining and restoring configurations, which supports recovery to a known configuration state. Aruba's support guidance also emphasizes collecting diagnostic information for further investigation after the immediate service-restoration need is addressed. See AOS-CX Configuration Management documentation and Aruba Support Center.

## QUESTION NO: 16

Your customer's CX switches are managed in HPE Aruba Networking Central. They have recently deployed new cabling to some desks and want to be notified of any physical cabling issues. Which alerts should you enable? (Choose two.)

**A.** Switch Port Input Errors

**B.** Switch Port Rx Rate

**C.** Switch Hardware Failure

**D.** Switch Uplink Port Usage

**E.** Switch Port Duplex Mode

**ANSWER: A E**

**Explanation:**

**Switch Port Input Errors** is appropriate because input-error counters provide a direct operational indication that frames are arriving at a switch port with problems. Newly installed or damaged copper cabling, poor terminations, interference, or connector faults can result in corrupted frames and error-counter increases. Configuring this alert in HPE Aruba Networking Central enables proactive notification when a port's error behavior crosses the configured threshold, allowing the administrator to investigate the cable path, patch leads, wall jack, and endpoint connection before users report a service issue.

**Switch Port Duplex Mode** should also be enabled because the negotiated duplex state is relevant when validating a newly connected endpoint and its physical Ethernet connection. A duplex-state change can identify an unexpected link negotiation outcome and prompt timely investigation of the connected device, NIC settings, and cabling installation. Monitoring port duplex information alongside input errors gives operations staff both an error symptom and a link-parameter signal for diagnosing access-port connectivity after cabling work. Aruba Central supports switch alerting and event monitoring so administrators can receive notifications and investigate affected devices and ports from the management interface. See the HPE Aruba Networking Central alerts documentation and the AOS-CX port statistics documentation.