# HP

## HPE7-A02 Exam

**Aruba Certified Network Security Professional Exam**

**Questions & Answers**
**Demo**

# Version: 5.1

## Question: 1

You have configured an AOS-CX switch to implement 802.1X on edge ports. Assume ports operate in the default auth-mode. VoIP phones are assigned to the
"voice" role and need to send traffic that is tagged for VLAN 12.

Where should you configure VLAN 12?

A. As the trunk native VLAN on edge ports and the trunk native VLAN on the "voice" role

B. As a trunk allowed VLAN on edge ports and the trunk native VLAN in the "voice" role

C. As the trunk native VLAN in the "voice" role (and not in the edge port settings)

D. As the allowed trunk VLAN in the "voice" role (and not in the edge port settings)

**Answer: D**

Explanation:

When configuring 802.1X authentication on edge ports of an AOS-CX switch and assigning VoIP phones to a "voice" role, the correct approach is to configure VLAN 12 as the allowed trunk VLAN in the "voice" role. This setup ensures that traffic tagged for VLAN 12 is appropriately managed by the role applied to the VoIP phones. In AOS-CX switches, the role-based VLAN configuration allows for more granular control and ensures that the VoIP phones' traffic is handled correctly without altering the edge port settings, which typically operate with default settings for authentication.
Reference: Detailed configuration and role assignment practices for AOS-CX switches can be found in Aruba's configuration guides and documentation related to AOS-CX switch deployments.

## Question: 2

You need to set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to provide certificate-based authentication of 802.1X supplicants.

How should you upload the root CA certificate for the supplicants' certificates?

A. As a ClearPass Server certificate with the RADIUS/EAP usage

B. As a Trusted CA with the AD/LDAP usage

C. As a Trusted CA with the EAP usage

D. As a ClearPass Server certificate with the Database usage

**Answer: C**

Explanation:

To set up HPE Aruba Networking ClearPass Policy Manager (CPPM) for certificate-based authentication of 802.1X supplicants, you need to upload the root CA certificate as a Trusted CA with the EAP usage. This configuration allows the ClearPass server to validate the certificates presented by the supplicants during the 802.1X authentication process. By marking the certificate for EAP usage, ClearPass can properly authenticate the supplicant devices using the trusted certificate authority (CA) that issued their certificates.
Reference: Configuration guidelines and best practices for ClearPass Policy Manager are available in Aruba's ClearPass documentation, specifically detailing the steps for uploading and configuring root CA certificates for EAP-based authentication.

## Question: 3

A company has AOS-CX switches. The company wants to make it simpler and faster for admins to detect denial of service (DoS) attacks, such as ping or ARP
floods, launched against the switches.

What can you do to support this use case?

A. Deploy an NAE agent on the switches to monitor control plane policing (CoPP).

B. Implement ARP inspection on all VLANs that support end-user devices.

C. Configure the switches to implement RADIUS accounting to HPE Aruba Networking ClearPass and enable HPE Aruba Networking ClearPass Insight.

D. Enabling debugging of security functions on the switches.

**Answer: A**

Explanation:

To support the detection of denial of service (DoS) attacks on AOS-CX switches, deploying an NAE (Network Analytics Engine) agent to monitor control plane policing (CoPP) is the best approach. NAE agents provide real-time analytics and monitoring capabilities, allowing administrators to detect anomalies and potential DoS attacks, such as ping or ARP floods, more quickly and efficiently. Control plane policing helps protect the switch's CPU from unnecessary or malicious traffic, and the NAE agent can alert administrators when thresholds are exceeded, providing a proactive measure to detect and mitigate DoS attacks.

Reference: Aruba's documentation on AOS-CX and NAE agents provides detailed information on configuring and deploying NAE for network monitoring and security purposes.

## Question: 4

You have run an Active Endpoint Security Report on HPE Aruba Networking ClearPass. The report indicates that hundreds of endpoints have MAC addresses but
no known IP addresses.

What is one step for addressing this issue?

A. Set up network devices to implement RADIUS accounting to CPPM.

B. Add CPPM's IP address to the IP helper list on routing switches.

C. Set up switches to implement ARP inspection on client VLANs.

D. Configure CPPM as a Syslog destination on network devices.

**Answer: B**

Explanation:

When the Active Endpoint Security Report on HPE Aruba Networking ClearPass indicates that endpoints have MAC addresses but no known IP addresses, one effective step to address this issue is to add CPPM's (ClearPass Policy Manager) IP address to the IP helper list on routing switches. This configuration ensures that DHCP requests are forwarded to the ClearPass server, allowing it to track and report the IP addresses assigned to the endpoints. This helps ClearPass maintain an accurate mapping of MAC addresses to IP addresses, improving endpoint visibility and security management. Reference: ClearPass configuration guides and best practices documentation outline the importance of integrating ClearPass with network infrastructure using IP helper addresses to ensure comprehensive endpoint visibility and management.

## Question: 5

An admin has configured an AOS-CX switch with these settings:
port-access role employees
vlan access name employees

This switch is also configured with CPPM as its RADIUS server.

Which enforcement profile should you configure on CPPM to work with this configuration?

A. RADIUS Enforcement type with HPE-User-Role VSA set to "employees"

B. HPE Aruba Networking Downloadable Role Enforcement type with role name set to "employees"

C. HPE Aruba Networking Downloadable Role Enforcement type with gateway role name set to "employees"

D. RADIUS Enforcement type with Aruba-User-Role VSA set to "employees"

| | |
|---|---|
| | **Answer: D** |

Explanation:

To ensure that the AOS-CX switch properly assigns the "employees" role when using CPPM (ClearPass Policy Manager) as the RADIUS server, you should configure a RADIUS Enforcement profile on CPPM with the Aruba-User-Role VSA (Vendor-Specific Attribute) set to "employees". This configuration ensures that when an endpoint authenticates, CPPM sends the appropriate role assignment to the AOS-CX switch, which then applies the corresponding policies and VLAN settings defined for the "employees" role.
Reference: Aruba's ClearPass documentation and AOS-CX configuration guides detail the integration and configuration of RADIUS enforcement profiles using Aruba-User-Role VSAs for role-based access control.