

KTest

高品質 より良いサービス



練習問題

<https://www.ktest.jp>

1年間無料アップデート

Exam : HPE7-A06

Title : Aruba Certified Campus
Access Switching Expert
Written Exam

Version : DEMO

1. An IT administrator uses AOS-CX switches to send TCP 22 traffic from the switch port to a remote server for analysis. The administrator now wants to save it locally to be downloaded and used later in case the admin changes their mind about the approach to take.

```
class ip Class_Mirror22
 10 match tcp any any eq 22
policy Policy_Mirror22
 10 class ip Class_Mirror22 action mirror 2

mirror session 2
 source interface 1/1/20 both
 destination tunnel 10.1.100.100 source 10.2.10.1 desc 10 vrf default
```

- A. destination file tshark-pcap
- B. destination tunnel file tshark-pcap
- C. destination cpu
- D. destination flash:./my-mirror.pcap policy Policy Minor22

Answer: A

Explanation:

The question involves an AOS-CX switch administrator using a packet capture (e.g., tshark) to monitor TCP port 22 traffic and wanting to save it locally for later download, instead of sending it to a remote server.

Analysis of Options:

Why Option A is Correct: In AOS-CX, packet captures can be configured using the monitor command (e.g., monitor session 1 source interface 1/1/1 destination file tshark-pcap). The destination file tshark-pcap option saves the captured packets (e.g., TCP port 22 traffic) to a local file on the switch's flash storage, which can be downloaded later via SCP, SFTP, or the Web UI. This meets the administrator's requirement to store the capture locally for future analysis, aligning with AOS-CX's packet capture capabilities.

Relevance to Certification Objectives:

References:

HPE Aruba Networking AOS-CX Configuration Guide: Packet Capture and Monitoring, detailing file-based captures.

HPE7-A06 Study Guide: Covers troubleshooting with packet analysis tools.

HPE Aruba Networking Technical Documentation: AOS-CX Packet Capture Best Practices.

2. DRAG DROP

Match the customer requirement with the relevant commands.

Establish redundant links between the aggregation and core layers.	interface vxlan 1 no shutdown source ip 10.1.0.4	
Identify individual layer 2 segments in an overlay.	router ospf 1 maximum-paths 2	
Aggregate links across multiple switches.	vni 11 vtep-peer 10.1.0.5 vlan 11	
Extend layer 2 across multiple sites.	vsx role primary inter-switch-link lag 256 keepalive peer 192.168.0.1 source 192.168.0.0 vrf KA	

Answer:

Establish redundant links between the aggregation and core layers.	interface vxlan 1 no shutdown source ip 10.1.0.4	Extend layer 2 across multiple sites.
Identify individual layer 2 segments in an overlay.	router ospf 1 maximum-paths 2	Establish redundant links between the aggregation and core layers.
Aggregate links across multiple switches.	vni 11 vtep-peer 10.1.0.5 vlan 11	Identify individual layer 2 segments in an overlay.
Extend layer 2 across multiple sites.	vsx role primary inter-switch-link lag 256 keepalive peer 192.168.0.1 source 192.168.0.0 vrf KA	Aggregate links across multiple switches.

Explanation:

Aggregate links across multiple switches -->

vsx role primary inter-switch-link lag 256

keepalive peer 192.168.0.1 source 192.168.0.0 vrf KA (Snippet 4)

Establish redundant links between the aggregation and core layers -->

router ospf 1

maximum-paths 2

(Snippet 2)

Extend layer 2 across multiple sites -->

interface vxlan 1

no shutdown source ip 10.1.0.4

(Snippet 1)

Identify individual layer 2 segments in an overlay -->

vni 11

vtep-peer 10.1.0.5

vlan 11

(Snippet 3)

Comprehensive Detailed Explanation along with All References available from related to the HPE Campus Access Switching Expert certification objectives at end of each question below:

⇒ Aggregate links across multiple switches: This requirement describes Multi-Chassis Link Aggregation (MC-LAG), where a device forms a LAG to two separate upstream switches that act as a logical pair. In AOS-CX, VSX (Virtual Switching

Extension) enables this functionality. Snippet 4 shows commands related to setting up VSX (vsx, role primary, inter-switch-link, keepalive), which is the foundation for MC-LAG.

References: AOS-CX VSX Guide. Relates to "Network Resiliency and virtualization" (8%), "Switching" (19%).

Establish redundant links between the aggregation and core layers: This often involves Layer 3 routing protocols utilizing multiple paths. Snippet 2 (router ospf 1, maximum-paths 2) configures OSPF to use up to two Equal Cost Multi-Paths (ECMP). If redundant links between aggregation and core result in equal OSPF costs, this command enables load sharing and redundancy at Layer 3.

References: AOS-CX IP Routing Guide (OSPF, ECMP). Relates to "Routing" (16%), "Network Resiliency and virtualization" (8%).

Extend layer 2 across multiple sites: VXLAN (Virtual Extensible LAN) is the standard overlay technology for extending Layer 2 segments over an underlying Layer 3 network, enabling L2 adjacency across different physical locations (sites, racks, pods). Snippet 1 shows the basic configuration of a VXLAN tunnel interface (interface vxlan 1, source ip), which is the core component for VXLAN tunneling.

References: AOS-CX VXLAN Guide. Relates to "Switching" (19%), "Connectivity" (9%).

Identify individual layer 2 segments in an overlay: Within a VXLAN overlay, each separate Layer 2 broadcast domain (typically corresponding to a VLAN) is identified by a unique VXLAN Network Identifier (VNI). This VNI tags the encapsulated traffic. Snippet 3 shows the configuration associating VNI 11 with the local VLAN 11 (vni 11, vlan 11). The vtep-peer command is relevant when using EVPN as the control plane. This configuration directly maps an L2 segment (VLAN 11) to its identifier (VNI 11) within the overlay. References: AOS-CX EVPN Guide, AOS-CX VXLAN Guide. Relates to "Switching" (19%), "Connectivity" (9%).

3.DRAG DROP

Match the BGP connection states to the conditions that could have caused that state.

Answer Area

active	The last keepalive is less than 3 times the negotiated holddown timer.	
connect	The router has not received a response. The neighbor might be unreachable.	
established	The router is waiting for an initial response from the neighbor.	
idle	The router starts listening for a connection.	

Answer:

Answer Area

active	The last keepalive is less than 3 times the negotiated holddown timer.	established
connect	The router has not received a response. The neighbor might be unreachable.	active
established	The router is waiting for an initial response from the neighbor.	connect
idle	The router starts listening for a connection.	idle

Explanation:

The last keepalive is less than 3 times the negotiated hold down timer. -->established

The router has not received a response. The neighbor might be unreachable. -->active

The router is waiting for an initial response from the neighbor. -->connect

The router starts listening for a connection. -->idle

This question requires matching specific BGP connection states from the BGP Finite State Machine (FSM) to descriptions of the router's activity or condition in those states.

Idle: This is the starting state. The BGP process is administratively up but is not actively trying to connect. It refuses all incoming BGP connection attempts but listens for a start event (like configuration or operator initiation) or potentially listens for incoming connections if configured for passive peering.

Connect: In this state, BGP is actively trying to establish a TCP connection with the peer. It has initiated the TCP three-way handshake and is waiting for it to complete, or it is waiting for a remote peer to initiate the TCP connection.

Active: If the TCP connection attempt in the Connect state fails (e.g., timeout), the router transitions to the Active state. In this state, it will periodically retry establishing the TCP connection while also listening for an incoming connection from the peer. This state indicates repeated failures to establish TCP connectivity.

Established: This is the final, operational state where the TCP connection is up, BGP session parameters have been successfully negotiated via OPEN messages, and KEEPALIVE messages are being exchanged. Routing information (UPDATES) can be exchanged. The condition described implies the session is healthy and timers are being maintained.

References: RFC 4271 (BGP4 Specification - Section 8, Finite State Machine), BGP configuration and troubleshooting guides for AOS-CX. This relates to the "Routing" (16%) and "Troubleshooting" (10%) objectives.

4.Which minimal configurations must be completed for MSTP to work correctly? (Select two.)

- A. MSTP region
- B. bridge priority number
- C. revision number
- D. MSTP enabled interfaces
- E. creating MSTP instances

Answer: A, C

Explanation:

The question asks for the minimal configurations required for Multiple Spanning Tree Protocol (MSTP) to

work correctly on AOS-CX switches.

Analysis of Options:

Why A and C are Correct: MSTP requires a consistent region configuration across all switches to function correctly.

The minimal configuration includes:

These settings ensure switches form a single MSTP region, allowing VLAN-to-instance mappings (default instance 0 if not specified) and loop prevention. Other settings, like bridge priority or explicit instance creation, are optional and not strictly required for basic MSTP operation.

Relevance to Certification Objectives:

References:

HPE Aruba Networking AOS-CX Configuration Guide: MSTP Configuration, detailing region and revision requirements.

HPE7-A06Study Guide: Covers MSTP setup and best practices.

HPE Aruba Networking Technical Documentation: Spanning Tree Protocols for AOS-CX.

5.Which issue may be causing the new door locks on the APs to network?

- A. AT power to the AP is too much.
- B. BT power to the AP is too much.
- C. AF power to the AP is not enough.
- D. AT power to the AP is not enough.

Answer: C

Explanation:

New PoE-powered door locks, connected via the PoE passthrough port on Aruba APs, are not working. We need to find the likely cause related to PoE power.

PoE Passthrough: An AP feature where the AP, powered by PoE from a switch, provides PoE power out to another device connected to one of its Ethernet ports.

Power Budget: The AP must receive enough power from the switch via its PoE input (e.g., 802.3af, 802.3at, 802.3bt) to power itself and meet the power demand of the downstream device (the door lock).

PoE Standards Power (Approx.

Available to Device):

Analysis: Modern APs (especially Wi-Fi 6/6E) can consume significant power themselves (>15W or >25W under load). Standard 802.3af PoE (supplying only

~13W) is often insufficient to power both a modern AP and a downstream PoE device like a door lock.

The AP will power up, but won't enable PoE output if its input power budget is insufficient.

Analysis of Options:

Conclusion: Insufficient input power to the AP is the most common reason for PoE passthrough failure. 802.3af (PoE) power is often inadequate.

References: IEEE 802.3 PoE standards (af/at/bt), Aruba Access Point datasheets (PoE requirements, passthrough capabilities/budgets). This relates to "WLAN" (9%) and "Connectivity" (9%) objectives.