



# HPE7-A01<sup>Q&As</sup>

Aruba Certified Campus Access Professional

## Pass HP HPE7-A01 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/hpe7-a01.html>

100% Passing Guarantee  
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

In AOS 10, which session-based ACL below will only allow ping from any wired station to wireless clients but will not allow ping from wireless clients to wired stations"? The wired host ingress traffic arrives on a trusted port.

- A. ip access-list session pingFromWired any user any permit
- B. ip access-list session pingFromWired user any svc-icmp deny any any svc-icmp permit
- C. ip access-list session pingFromWired any any svc-icmp permit user any svc-icmp deny
- D. ip access-list session pingFromWired any any svc-icmp deny any user svc-icmp permit

Correct Answer: D

Explanation: A session-based ACL is applied to traffic entering or leaving a port or VLAN based on the direction of the session initiation. To allow ping from any wired station to wireless clients but not vice versa, a session-based ACL should be used to deny icmp echo traffic from any source to any destination, and then permit icmp echo-reply traffic from any source to user destination. The user role represents wireless clients in AOS 10. References: [https://techhub.hpe.com/eginfolib/Aruba/OS-CX\\_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html](https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html) <https://techhub.hpe.com/eginfolib/networking/docs/arubaos-switch/security/GUID-EA0A5B3C-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html>

### QUESTION 2

Match the appropriate QoS concept with its definition. (Options may be used more than once or not at all.)

Select and Place:

Best Effort Service	Class of Service
Differentiated Services	WMM

#### Answer Area

	A method for classifying network traffic at layer-2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
	A method for classifying network traffic at layer-3 by marking packets with one of 64 different service classes
	A method where traffic is treated equally in a first-come, first-served manner
	A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard

Correct Answer:




**Answer Area**

Best Effort Service	A method for classifying network traffic at layer-2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Differentiated Services	A method for classifying network traffic at layer-3 by marking packets with one of 64 different service classes
Class of Service	A method where traffic is treated equally in a first-come, first-served manner
WMM	A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard

**QUESTION 3**

Which statements are true about VSX LAG? (Select two.)

- A. The total number of configured links may not exceed 8 for the pair or 4 per switch
- B. Outgoing traffic is switched to a port based on a hashing algorithm which may be either switch in the pair
- C. LAG traffic is passed over VSX ISL links only while upgrading firmware on the switch pair
- D. Outgoing traffic is preferentially switched to local members of the LAG.
- E. Up to 255 VSX lags can be configured on all 83xx and 84xx model switches.

Correct Answer: AD

Explanation: The correct answers are A and D. According to the web search results, VSX LAG is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices<sup>1</sup>. VSX LAGs span both aggregation switches and appear as one device to partner downstream or upstream devices or both when forming a LAG with the VSX pair<sup>2</sup>. One of the statements that is true about VSX LAG is that the total number of configured links may not exceed 8 for the pair or 4 per switch<sup>1</sup>. This means that a VSX LAG across a downstream switch can have at most a total of eight member links, and a switch can have a maximum of four member links. When creating a VSX LAG, it is recommended to select an equal number of member links in each segment for load balancing<sup>1</sup>. Another statement that is true about VSX LAG is that outgoing traffic is preferentially switched to local members of the LAG<sup>2</sup>. This means that when active forwarding and active gateway are enabled, north-south and south-north traffic bypasses the ISL link and uses the local ports on the switch. This optimizes the traffic path and reduces the load on the ISL link<sup>2</sup>. The other statements are false or not relevant for VSX LAG. Outgoing traffic is not switched to a port based on a hashing algorithm, which may be either switch in the pair. This is a characteristic of MLAG (Multi-Chassis Link Aggregation), which is a different feature from VSX LAG. LAG traffic is not passed over VSX ISL links only while upgrading firmware on the switch pair. This is a scenario that may occur when performing hitless upgrades, which is a feature that allows software updates without impacting network availability. The number of VSX lags that can be configured on all 83xx and 84xx model switches is not 255, but depends on the switch model and firmware version. For example, the AOS-CX 10.04 supports up to 64 VSX lags for 8320 switches and up to 128 VSX lags for 8325 and 8400 switches.

**QUESTION 4**

Select the Aruba stacking technology matching each option (Options may be used more than once or not at all.)

Select and Place:

	Answer Area
<input type="text" value="VSF"/>	<input type="text" value="Supports up to 10 devices per stack"/>
<input type="text" value="VSX"/>	<input type="text" value="Supports two devices per stack"/>
<input type="text" value="VSF"/>	<input type="text" value="Individual ISL links up to 400G are supported"/>
<input type="text" value="VSX"/>	<input type="text" value="Individual ISL links up to 50G are supported"/>
<input type="text" value="VSF"/>	<input type="text" value="A maximum aggregate ISL bandwidth of 200G is supported"/>

Correct Answer:

	Answer Area
<input type="text" value="VSF"/>	<input type="text" value="Supports up to 10 devices per stack"/>
<input type="text" value="VSX"/>	<input type="text" value="Supports two devices per stack"/>
<input type="text" value="VSX"/>	<input type="text" value="Individual ISL links up to 400G are supported"/>
<input type="text" value="VSF"/>	<input type="text" value="Individual ISL links up to 50G are supported"/>
<input type="text" value="VSF"/>	<input type="text" value="A maximum aggregate ISL bandwidth of 200G is supported"/>

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>

**QUESTION 5**

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



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

Correct Answer: B

Explanation: CoS and DSCP are both methods of marking packets for quality of service (QoS) purposes. QoS is a mechanism that allows network devices to prioritize and differentiate traffic based on certain criteria, such as application type,

source, destination, etc. CoS stands for Class of Service and is a 3-bit field in the 802.1Q VLAN tag header. CoS can only be used on Ethernet frames that have a VLAN tag, and it can only be preserved within a single VLAN domain. DSCP

stands for Differentiated Services Code Point and is a 6-bit field in the IP header. DSCP can be used on any IP packet, regardless of the underlying layer 2 technology, and it can be preserved throughout the IP packet flow, unless it is

modified by intermediate devices. References:

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

<https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html>

[https://www.cisco.com/c/en/us/support/docs/](https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html)

[quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html](https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html)

---

## QUESTION 6

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.

Correct Answer: A

The correct answer is A. DMO is configured individually for each SSID in use in the network.

DMO is a feature that allows the AP to convert multicast streams into unicast streams over the wireless link. This enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. DMO is

configured individually for each SSID in use in the network, as different SSIDs may have different multicast requirements.

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



Dynamic multicast optimization: Select Enabled to allow IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients.

The other options are incorrect because:

B. The AP does not use QoS to provide equal air time for multicast traffic. QoS is a feature that prioritizes different types of traffic based on their importance and latency sensitivity. QoS does not affect how multicast streams are transmitted over the wireless link.

C. DMO is not configured globally for each SSID in use in the network. DMO is configured individually for each SSID, as different SSIDs may have different multicast requirements.

D. The controller does not convert multicast streams into unicast streams. The AP does the conversion, as it is closer to the wireless clients and can optimize the transmission based on the client capabilities and channel conditions.

---

### QUESTION 7

Which Aruba AP mode is sending captured RF data to Aruba Central for waterfall plot?

- A. Hybrid Mode
- B. Air Monitor
- C. Spectrum Monitor
- D. Dual Mode

Correct Answer: C

Explanation: Spectrum Monitor is an Aruba AP mode that is sending captured RF data to Aruba Central for waterfall plot. Spectrum Monitor is a mode that allows an AP to scan all channels in both 2.4 GHz and 5 GHz bands and collect information about the RF environment, such as interference sources, noise floor, channel utilization, etc. The AP then sends this data to Aruba Central, which is a cloud-based network management platform that can display the data in various formats, including waterfall plot. Waterfall plot is a graphical representation of the RF spectrum over time, showing the frequency, amplitude, and duration of RF signals. The other options are incorrect because they are either not AP modes or not sending RF data to Aruba Central. References:

[https://www.arubanetworks.com/techdocs/ArubaOS\\_86\\_Web\\_Help/Content/arubaos-solutions/1-overview/spectrum\\_monitor.htm](https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/spectrum_monitor.htm)

[https://www.arubanetworks.com/techdocs/ArubaOS\\_86\\_Web\\_Help/Content/arubaos-solutions/1-overview/waterfall\\_plot.htm](https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/waterfall_plot.htm) <https://www.arubanetworks.com/products/network-management-operations/aruba-central/>

---

### QUESTION 8

Match the topics of an AOS10 Tunneled mode setup between an AP and a Gateway. (Options may be used more than once or not at all.)

Select and Place:





Authenticator

Negotiate IPsec Phase1

Negotiate IPsec Phase 2

RADIUS proxy

#### Answer Area

Access Point

Access Point and Gateway

Device Designated Gateway

Overlay Tunnel Orchestrator

Correct Answer:

#### Answer Area

Negotiate IPsec Phase1

Access Point

Negotiate IPsec Phase 2

Access Point and Gateway

Authenticator

Device Designated Gateway

RADIUS proxy

Overlay Tunnel Orchestrator

### QUESTION 9

Match the terms below to their characteristics (Options may be used more than once or not at all.)

Select and Place:

Term	Characteristic
Broadcast	A device with IP address 10.1.3.7 in a network wants to send the traffic stream to a device with IP address 10.13.4.2 in the other network
IP Directed Broadcast	One/more senders and one/more recipients participate in data transfer traffic
Multicast	Sent to all hosts on a remote network
Unicast	Sent to all NICs on the same network segment as the source NIC

Correct Answer:

**Term****Characteristic**

Unicast	A device with IP address 10.1.3.7 in a network wants to send the traffic stream to a device with IP address 10.13.4.2 in the other network
Multicast	One/more senders and one/more recipients participate in data transfer traffic
IP Directed Broadcast	Sent to all hosts on a remote network
Broadcast	Sent to all NICs on the same network segment as the source NIC

---

**QUESTION 10**

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

Correct Answer: B

Explanation: The correct answer is B. sysops.

The sysops user role is a predefined role that allows users to perform system operations on the switch, such as backup, restore, upgrade, or reboot. The sysops user role also has access to the PUT and POST methods for REST API, which can be used to modify the switch configuration. The sysops user role has a privilege level of 15, which is the highest level of access on the switch<sup>1</sup>.

The other options are incorrect because:

A. sysadmin: The sysadmin user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The sysadmin user role does not have access to the REST API methods, and cannot perform firmware upgrades<sup>1</sup>.

C. administrators: 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 requires<sup>1</sup>. D. config: The config user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The config user role does not have access to the REST API methods, and cannot perform firmware upgrades<sup>1</sup>.

---

**QUESTION 11**





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.

Correct Answer: C

Explanation: 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 network<sup>12</sup>.

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 series<sup>2</sup>.

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 address<sup>1</sup>.

---

## QUESTION 12

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

Select and Place:



Client Insights	Cloud Auth
The Fabric Wizard	Policy Manager

	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

Correct Answer:


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

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

Client Insights is a solution component of NetConductor that provides built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and MLbased classification models to eliminate network blind spots.

Client Insights uses machine learning to automatically detect, identify, and classify devices on the network, such as IoT devices, BYOD devices, or rogue devices. Client Insights also provides behavioral analytics and anomaly detection to

monitor device performance and security posture. Client Insights helps network administrators gain visibility into the device landscape, enforce granular access policies, and troubleshoot issues faster.

References:

<https://www.arubanetworks.com/products/network-managementoperations/central/netconductor/>

[https://www.arubanetworks.com/assets/wp/WP\\_NetConductor.pdf](https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf)

## QUESTION 13



Which feature supported by SNMPv3 provides an advantage over SNMPv2c?

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

Correct Answer: D

Explanation: 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/snmp.htm)

[https://www.arubanetworks.com/techdocs/ArubaOS\\_86\\_Web\\_Help/Content/arubaos- solutions/snmp/snmpv3.htm](https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/snmp/snmpv3.htm)

---

#### QUESTION 14

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.

Correct Answer: C

Explanation: 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.

---

#### QUESTION 15

Your customer is interested in hearing more about how roles can help keep consistent policy enforcement in a distributed overlay fabric.

How would you explain this concept to them?



- A. Group Based Policy ID is applied on egress VTEP after device authentication and policy is enforced on ingress VTEP
- B. Role-based policies are tied to IP addresses which have an advantage over IP-based policies and role names are sent between VTEPs
- C. Group Based Policy ID is applied on ingress VTEP after device authentication and policy is enforced on egress VTEP
- D. Role-based policies enhance User Based Tunneling across the campus network and the policy traffic is protected with iPsec

Correct Answer: C

Explanation: This is the correct explanation of how roles can help keep consistent policy enforcement in a distributed overlay fabric. Roles are used to assign group based policy IDs (GBPs) to devices after they authenticate with ClearPass or a local database. GBPs are then used to tag the traffic from the devices and send them to the ingress VTEP, which applies the GBP on the VXLAN header. The egress VTEP then enforces the policy based on the GBP and the destination device. The other options are incorrect because they either do not describe the correct sequence of events or do not use the correct terms. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01ch03.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html>

[HPE7-A01 Practice Test](#)

[HPE7-A01 Exam Questions](#)

[HPE7-A01 Braindumps](#)