PassQueen
a.k.a dumpsqueen.com

HPE Network Switching Associate Exam

HP HPE6-A86

Version Demo

Total Demo Questions: 12

Total Premium Questions: 122

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Network Stack	19
Topic 2, Switching	46
Topic 3, Routing	9
Topic 4, Network Services	7
Topic 5, Security	12
Topic 6, Management	29
Total	122

QUESTION NO: 1

A DHCP server is located in VLAN 50, while newly deployed clients are connected to VLAN 120 on an HPE Aruba Networking CX 6300 switch.

Which statements describe how DHCP relay enables the clients to receive addresses? Choose two.

A. The relay function forwards client DHCP broadcasts as unicast packets to the DHCP server.

B. The relay function is configured on the VLAN 120 Layer 3 interface.

C. The DHCP server must be connected by a Layer 2 trunk to VLAN 120.

D. The relay function is configured only on the VLAN 50 Layer 3 interface.

E. Each client access port must be converted to a routed interface.

ANSWER: A B

Explanation:

DHCP relay is required because client DHCPDISCOVER messages are broadcasts and routers do not forward broadcasts between VLANs. The relay function is configured on the Layer 3 interface for the client VLAN, VLAN 120 in this scenario. It forwards the client request as a unicast message to the DHCP server and includes relay information that lets the server identify the client subnet from which it should allocate an address.

Configuring the helper function only on VLAN 50 would not process broadcasts received from VLAN 120. The DHCP server does not need a Layer 2 trunk directly to every client VLAN, and converting the client port into a routed port would not provide DHCP relay service.

QUESTION NO: 2

At which layer of the OSI model does HTTP operate?

A. Session Layer

B. Network Layer

C. Application Layer

D. Data Link Layer

ANSWER: C

Explanation:

HTTP operates at the **Application Layer**, which is Layer 7 of the OSI model. This layer provides network services directly to end-user applications and defines the protocols that applications use to exchange information over a network. HTTP is the web's request-response protocol: a browser or other client sends an HTTP request for a resource, and a web server returns an HTTP response containing content or status information. Its methods, headers, message formatting, and status codes are all application-level functions.

Although HTTP normally relies on lower-layer protocols to deliver its messages—typically TCP at the transport layer and IP at the network layer—those protocols provide the communication path rather than the web communication semantics defined by HTTP. In modern environments, HTTPS is HTTP protected with TLS; TLS adds encryption, but the HTTP protocol remains an application-layer protocol. Aruba networking platforms commonly identify and classify HTTP traffic as Layer 7 application traffic for policy and visibility purposes. The HTTP specification is maintained by the IETF and describes HTTP as an application-layer protocol for distributed, collaborative information systems. See RFC 9110: HTTP Semantics and Aruba's Application Monitoring documentation.

QUESTION NO: 3

Which commands can ensure the current configuration persists after a reboot? Choose two.

A. commit confirm

B. write memory

C. save force

D. copy startup-config running-config

E. copy running-config startup-config

ANSWER: B E

Explanation:

On an HPE Aruba Networking AOS-CX switch, configuration changes take effect in the running configuration, which is the active configuration held for the current operating session. To retain those changes across a reload or power cycle, the switch must save that running configuration as the startup configuration. The command `copy running-config startup-config` performs precisely this operation: it copies the active configuration to the startup configuration file that AOS-CX loads during its next boot. The command `write memory` is the equivalent shortcut command and saves the running configuration for subsequent reboots as well. Either command therefore ensures that the current switch settings, including interface, VLAN, routing, and management configuration changes, remain available after restart. Aruba's AOS-CX Fundamentals Guide documents saving configuration with `write memory`, while the Command-Line Interface Guide documents the running-to-startup copy operation and its use in preserving configuration changes. See the AOS-CX Fundamentals Guide and the AOS-CX CLI Guide.

QUESTION NO: 4

When explaining the HPE Aruba Networking Virtual Switching features, which statement about VSF is true?

A. The switch member ID does not change on either of the members.

B. The switch control plane is shared.

C. The configuration is limited to two members.

D. The management plane operates independently.

ANSWER: B

Explanation:

The switch control plane is shared. Aruba Virtual Switching Framework (VSF) virtualizes multiple physical switches into one logical switching system. The stack is administered as a single device, and its members use a shared control plane, allowing the system to present unified configuration, management, and network operation. A VSF stack has a conductor that performs the active control-plane role, with another member able to serve as standby to maintain resiliency. This architecture lets connected devices and the broader network treat the stack as one virtual switch rather than as separately managed switches. VSF uses standard Ethernet interfaces for stack links, which supports flexible physical deployment while retaining the operational simplicity of a unified logical device. The exact number of supported members depends on the applicable Aruba switch family and AOS-CX release, but that does not change the fundamental VSF model of a single shared control plane. Aruba's VSF documentation describes the technology as combining physical switches into a single virtual device and identifies the conductor and standby roles used for control-plane operation. See the Aruba AOS-CX VSF Guide and the VSF overview.

QUESTION NO: 5 - (SIMULATION)

Match the definitions for Power over Ethernet.

ANSWER: See the explanation for the answer

Explanation:

Match the PoE standards to their maximum power supplied by the Power Sourcing Equipment (PSE):

Therefore, in the answer area from top to bottom: `802.3at`, `802.3bt (Type 4)`, `802.3bt (Type 3)`, and `802.3af`.

QUESTION NO: 6

Which protocols can be used to control administrative access to HPE Aruba Networking AOS-CX switches? Choose two.

A. RADIUS

B. LDAP

C. Diameter

D. SAML

E. TACACS+

ANSWER: A E

Explanation:

RADIUS and TACACS+ are supported AAA protocols for centrally controlling administrative access to AOS-CX switches. Rather than defining and maintaining every administrator account solely in the switch's local user database, an administrator can configure the switch to send login authentication requests to a centralized AAA server. This supports consistent account management, credential validation, and auditing across a switching environment. With RADIUS, AOS-CX can authenticate management users and use returned authorization attributes, including role information where configured, to determine the level of access granted after login. TACACS+ is also designed for device-administration workflows and provides centralized authentication, authorization, and accounting. In particular, TACACS+ can apply authorization decisions to administrative activity, making it well suited to controlling privileged access to network infrastructure. AOS-CX documentation describes configuring both RADIUS and TACACS+ server groups, selecting them for AAA authentication and authorization methods, and defining fallback behavior when remote servers are unavailable. These capabilities make RADIUS and TACACS+ the appropriate protocols for the administrative-access use case described. See the AOS-CX RADIUS documentation and TACACS+ documentation.

QUESTION NO: 7

Which statement describes static routing?

A. Unpredictable routing behavior

B. Suitable for basic Layer 3 networks

C. Scalable to any size

D. Supports automatic failure throughout the entire network

ANSWER: B

Explanation:

Static routing is suitable for basic Layer 3 networks because routes are explicitly configured by an administrator rather than learned and maintained through a routing protocol. A static route identifies the destination prefix and the next-hop address or outgoing interface that the switch must use. This direct, administrator-controlled approach is especially appropriate where the topology is small, stable, and has a limited number of paths to manage, such as a branch site, a small routed VLAN deployment, or a connection toward an upstream router. It also provides a simple way to configure a gateway of last resort by adding a static default route.

On AOS-CX switches, static routes are configured in the routing table and remain in use until they are changed, removed, or their associated next-hop/interface becomes unavailable. Because route selection is intentionally defined in configuration, static routing offers predictable forwarding for a basic Layer 3 design without requiring the overhead of a dynamic routing protocol. Aruba's AOS-CX IP Routing guide documents the configuration and operation of static routes, including default routes and next-hop/interface specifications: AOS-CX Static Routing documentation. HPE Aruba Networking's routing overview also provides context for Layer 3 routing features: About IP routing in AOS-CX.

QUESTION NO: 8

A network management system must poll HPE Aruba Networking CX switches without exposing management information or credentials in clear text.

Which protections are provided when SNMPv3 is configured with the authPriv security level? Choose two.

A. It encrypts SNMP management payloads in transit.

B. It authenticates the configured SNMP user and protects message integrity.

C. It uses only an SNMPv2c community string for access control.

D. It automatically transports all SNMP messages using TLS.

E. It eliminates the need to configure SNMP users on the switch.

ANSWER: A B

Explanation:

SNMPv3 authPriv provides both authentication and privacy. Authentication validates the SNMP user and protects message integrity, while privacy encrypts the SNMP payload exchanged between the management system and the switch. This is the appropriate security level when the monitoring design requires encrypted polling and notifications.

SNMPv2c community strings are not encrypted, and SNMPv3 does not automatically use TLS simply because it is enabled. SNMPv3 also requires configured user credentials; it does not remove the need to identify and authorize the management system.

QUESTION NO: 9

A customer is planning a VSF stack using HPE Aruba Networking CX switches. The design must preserve ports for user and uplink traffic and must use a supported stacking design.

Which planning statements are correct? Choose two.

A. Select member switches that are supported together by the applicable VSF platform requirements.

B. Reserve interfaces used as VSF links because they are unavailable for normal user traffic.

C. Configure each member as an independently managed switch after the stack forms.

D. Configure the VSF links as ordinary user VLAN trunks.

E. Assign the same VSF member ID to every switch in the stack.

ANSWER: A B

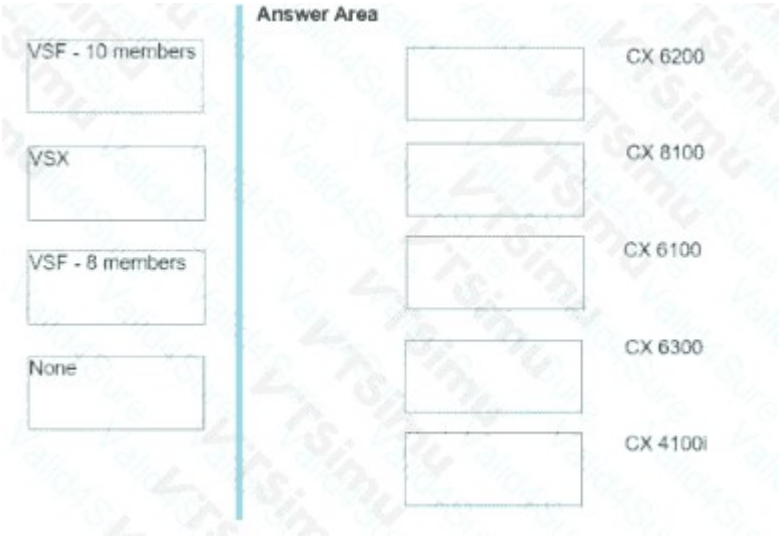
Explanation:

VSF members must be selected according to the applicable platform support rules, including supported switch-family and software compatibility requirements. Interfaces assigned as VSF links are dedicated to the stack fabric and are removed from normal data-plane use, so those ports cannot also be allocated for endpoint, uplink, or ordinary VLAN-trunk connectivity.

A VSF stack is managed as one logical switch, rather than by independently configuring each member as a separate device. VSF links are not configured as ordinary user VLAN trunks, and each member requires a unique member ID within the stack.

QUESTION NO: 10 - (HOTSPOT)

Match the device stacking or clustering feature to the correct HPE Aruba Networking CX switch series when selecting a switch family for a use case where device failure needs to be protected by using HPE Aruba Networking OS capabilities. Matches may be used more than once.



ANSWER:

Answer:

Explanation:

CX Switch Series	Answer
CX 6200	C. VSF - 8 members
CX 8100	B. VSX
CX 6100	D. None
CX 6300	A. VSF - 10 members
CX 4100i	D. None

The correct matches are based on the high-availability technologies supported by each CX switch family in the answer list. HPE Aruba Networking AOS-CX VSF documentation states that VSF supports up to 8-member stacks for CX 6200F devices and up to 10-member stacks for CX 6300 devices. That makes CX 6200 match â€œVSF - 8 membersâ€□ and CX 6300 match â€œVSF - 10 members.â€□ HPE Aruba Networking documentation for VSX support lists the CX 8100 as a VSX-supported switch series, so CX 8100 matches â€œVSX.â€□ The CX 6100 and CX 4100i do not match the listed VSF 8-member, VSF 10-member, or VSX choices. Although AOS-CX VSF documentation lists other VSF limits for some platforms, the choices provided only include VSF-8, VSF-10, VSX, and None; therefore, CX 6100 and CX 4100i map to â€œNoneâ€□ in this drag-and-drop question.

Explanation:

The correct mapping identifies the AOS-CX resiliency capability that is available on each listed switch family. CX 6200 uses Virtual Switching Framework, or VSF, with support for an eight-member stack. VSF combines the physical members into a single logical switch for simplified administration and provides continuity when a member or link fails, subject to the configured topology and redundancy design. HPE's VSF documentation describes the CX 6200 family's eight-member capability: AOS-CX VSF overview.

CX 6300 also supports VSF, but its applicable scale in this match is ten members. This makes it the appropriate family for the ten-member VSF designation. The selected CX 8100 match is VSX. VSX is the AOS-CX high-availability virtualization technology that forms a resilient pair of independent switches while preserving separate control planes. It is designed for redundant access, aggregation, and distribution designs, including dual-attached downstream devices. Aruba's VSX documentation explains the paired-switch architecture and its synchronization mechanisms: AOS-CX VSX guide.

For the feature set represented by the labels in this question, CX 6100 and CX 4100i are assigned "None." The point of this selection is to distinguish the families that support the stated eight-member VSF, ten-member VSF, or VSX protection technologies from families that do not provide one of those particular choices. Thus, the complete correct result is CX 6200 with VSF - 8 members, CX 8100 with VSX, CX 6100 with None, CX 6300 with VSF - 10 members, and CX 4100i with None.

QUESTION NO: 11

A customer has a skilled internal DevOps team with extensive Python programming knowledge.

Which HPE Aruba Networking CX switch would you recommend for the customer to support self-made or HPE Aruba Networking-provided scripts for onboard analytics?

A. CX 6100

B. CX 6200

C. CX 4100i

D. CX 6000

ANSWER: B

Explanation:

CX 6200 is the appropriate recommendation because it supports the AOS-CX Network Analytics Engine (NAE), Aruba Networking's onboard, programmable analytics framework. NAE uses Python-based scripts, called agents, to monitor switch resources and telemetry, evaluate conditions, and optionally initiate actions when specified conditions occur. This gives a DevOps team the flexibility to develop and deploy its own Python analytics logic while also using Aruba Networking-provided agents for common operational monitoring use cases.

The CX 6200 is included in the NAE documentation's supported switch platforms and supports a defined number of concurrently installed NAE scripts and agents. Its support for this capability directly meets the requirement for onboard analytics driven by either custom-developed or vendor-provided Python scripts. NAE is particularly valuable for proactively detecting network conditions locally on the switch and collecting relevant state information at the time an event is detected, helping teams automate operational visibility and response.

See the AOS-CX Network Analytics Engine Guide and the NAE supported maximums documentation for platform support and capacity details.

QUESTION NO: 12

You have access to the CLI of an HPE Aruba Networking CX switch.

How can you output the switch make, model, and serial number displayed on the session?

A. Issue command:show support-information

B. Issue command:diag dump basic

C. Issue command:show configuration

D. Issue command:show system

ANSWER: D

Explanation:

Issue the `show system` command. In the AOS-CX CLI, this command displays general system and chassis identity information directly in the active terminal session. Its output includes fields such as the vendor, product name, and chassis serial number, which collectively identify the switch manufacturer, hardware model, and unique serial number. This makes it the appropriate concise operational command when the requirement is simply to view the device identity without gathering an extensive diagnostic bundle or inspecting configuration details. The command is useful during inventory verification, hardware replacement workflows, support cases, and initial device validation because the requested information is presented in a standard, readable summary. Aruba's AOS-CX command documentation describes `show system` as displaying system status information and provides output containing the relevant product and chassis identification fields. For command syntax and sample output, see the AOS-CX show system command reference. Aruba also maintains its complete AOS-CX documentation library at the AOS-CX Help Center, where the reference can be selected for the switch software version in use.