Accelerate Your Certification with HPE7-A06 Practice Questions

Last chance to prepare smart! Get your hands on free HPE Campus Access Switching Expert Written Exam PDF questions. Study real HPE7-A06 dumps with verified answers and fast-track your certification success with PrepBolt HPE7-A06 exam pdf questions and answers.

Thank you for Downloading HPE7-A06 exam PDF Demo

https://prepbolt.com/HPE7-A06.html

QUESTIONS & ANSWERS

DEMO VERSION

(LIMITED CONTENT)

Question 1

Question Type: MultipleChoice

A plying the command "ip Igmp snooping blocked VLAN 6. 6* on a port ...

Options:

A- won't prune multicast on that port on VLAN 5 and 6
B- won't accept multicast Igmp joins on that port or VLAN 5 and 6.
C- won't allow multicast traffic between VLAN 5 and 6.
D- won't allow multicast on that port in VLAN 5 and 6 and disables the port.

Answer:

B

Explanation:

The question asks for the effect of applying the command ip igmp snooping blocked vlan 5,6 on a switch port.

ip igmp snooping blocked vlan <vlan-list>: This interface configuration command instructs the IGMP snooping process on the switch to block (ignore/drop) any inbound IGMP control packets (specifically Membership Reports, i.e., 'joins', and Leave messages) received on this port for the specified VLANs (5 and 6 in this case).

Effect: By blocking IGMP join messages from hosts connected to this port, the switch will not learn about any multicast group memberships requested by those hosts in VLANs 5 and 6. Consequently, the switch will not forward multicast traffic for those groups out of this port for those VLANs (unless the port is designated as a multicast router port). It effectively prevents hosts on this port from receiving multicast streams in the specified VLANs via standard IGMP mechanisms.

Analysis of Options:

A: It results in traffic effectively being pruned because memberships aren't learned, but the command itself blocks the IGMP control packets (joins).

B: Correct. It stops the switch from accepting IGMP join messages on this port for VLANs 5 and 6.

C: Incorrect. It doesn't control inter-VLAN traffic.

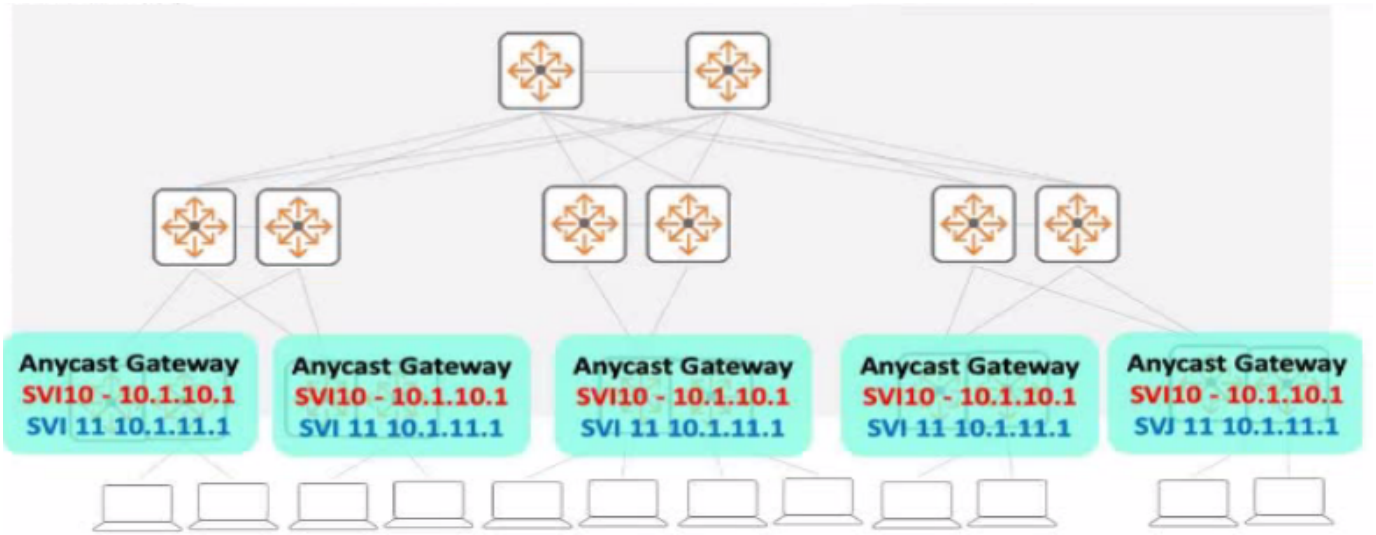
D: Incorrect. It doesn't disable the entire port.

Conclusion: The command specifically blocks the reception and processing of IGMP join messages on the configured port for the listed VLANs.

Question 2

Question Type: MultipleChoice

Exhibit.



After Implementing a distributed overlay with distributed anycast gateways, you noticed that too many ARP packets are being replicated to every access (leaf) switch Which command can you use to optimize the network?

Options:

A- vlan 10 arp-suppression vlan 11 arp-suppression
B- evpn arp-suppression
C- evpn ip proxy-arp
D- interface vlan 10 ip proxy-arp interface vlan 11 ip proxy-arp

Answer:

B

Explanation:

In an EVPN VXLAN distributed overlay network, excessive ARP packet replication (flooding) to all leaf switches is observed. We need the command to optimize this.

EVPN ARP Optimization: EVPN uses its control plane (BGP) to distribute MAC and IP address reachability information. Leaf switches (VTEPs) learn these mappings. To reduce ARP flooding across the VXLAN fabric:

ARP Suppression: VTEPs intercept ARP requests. If the VTEP already knows the MAC address for the

requested IP (learned via EVPN), it can suppress the ARP request, preventing it from being flooded over VXLAN.

Proxy ARP: VTEPs intercept ARP requests. If the VTEP knows the MAC for the requested IP, it can generate an ARP reply on behalf of the remote host.

AOS-CX Commands: These features are configured within the EVPN context.

evpn arp-suppression (B): Enables the ARP suppression feature for EVPN.

evpn ip proxy-arp (C): Enables the proxy ARP feature for EVPN.

Options A and D use standard interface/VLAN level arp-suppression or proxy-arp commands, which are not specific to optimizing flooding within the EVPN VXLAN fabric itself.

Conclusion: To optimize by reducing the replication/flooding of ARP packets across the EVPN VXLAN overlay, enabling evpn arp-suppression (Option B) is the direct command. This leverages the EVPN control plane knowledge to stop unnecessary ARP flooding.

Question 3

Question Type: MultipleChoice

An HPE Aruba Networking CX switch administrator wants to monitor all inter-switch connections and change their descriptions dynamically with Python script and NAE engine. The administrator has written the script template and uploaded it to the switch GUI. After the upload, not all data is stored as planned.

Which things should be checked first? (Select three.]

Options:

A- flash memory usage
B- Agent usage
C- script usage
D- processor usage
E- monitor usage
E- memory usage

Answer:

B, C, E, E

Explanation:

An NAE (Network Analytics Engine) Python script designed to monitor links and update descriptions isn't storing data as planned. We need the first things to check (select three).

NAE Components & Troubleshooting: NAE involves Agents running Scripts, often triggered by Monitors observing system state (like interface status or LLDP changes). Failures can occur in any component or due to resource issues.

Initial Checks:

Script (script usage - C): Check the script itself for syntax errors, logic flaws, status, and logs (show nae script <name> [status|log]). Ensure it's uploaded correctly and enabled.

Agent (Agent usage - B): Check the agent configured to run the script. Is it running? Are its parameters correct? Are there errors associated with the agent? (show nae agent [status|detail]). Check agent resource limits.

Monitor (monitor usage - E): If the script relies on a monitor to trigger or gather data, check the monitor's status, configuration, and associated conditions (show nae monitor [status|detail]). Is the monitor detecting the intended events?

Resources (Processor/Memory/Flash - D, F, A): General switch health is important. High CPU (D) or memory (F) usage could prevent the script/agent from running correctly. If the script is supposed to store data persistently (e.g., write to a file or NAE database), check flash memory usage (A) or NAE database limits.

Conclusion: When troubleshooting NAE, the core components to check first are the Script itself (C), the Agent running it (B), and any Monitors it depends on (E). These cover the specific NAE elements involved. General system resources (D, F, A) are secondary checks if the core components appear configured correctly but still fail.

Question 4

Question Type: MultipleChoice

A customer wants to deploy IoT security devices that are PoE-powered. Due to its criticality. it is required that those devices remain active even during a switch software upgrade. What is a valid solution to meet customer requirements?

Options:

A- a VSX pair of switches for redundancy
B- power-over-ether net quick-poe
C- power-over-ethernet always-on

D- power-over-ethernel priority

Answer:

C

Explanation:

The question involves a customer deploying PoE-powered IoT security devices (e.g., door locks) that must remain active during an AOS-CX switch software upgrade. The task is to identify a valid solution.

Analysis of Options:

Option A: Incorrect. A VSX pair provides redundancy but does not guarantee PoE continuity during a single switch's upgrade.

Option B: Incorrect. quick-poe reduces PoE startup time but does not ensure power during upgrades.

Option C: Correct. power-over-ethernet always-on ensures PoE remains active during software upgrades, meeting the requirement.

Option D: Incorrect. PoE priority adjusts power allocation but does not guarantee continuity during upgrades.

Why Option C is Correct: The power-over-ethernet always-on feature on AOS-CX switches ensures that PoE power delivery continues uninterrupted during software upgrades or reboots, critical for devices like IoT security door locks that require constant power. This feature prevents power cycling on PoE ports, maintaining device operation. For example, enabling it on relevant ports (e.g., interface 1/1/1 power-over-ethernet always-on) ensures compliance with the customer's requirement, as per HPE Aruba Networking's PoE high-availability guidelines.

Relevance to Certification Objectives:

Connectivity (9%): Configuring PoE for critical device deployment.

Network Resiliency and Virtualization (8%): Ensuring device uptime during maintenance.

Troubleshooting (10%): Resolving PoE continuity issues.

HPE Aruba Networking AOS-CX Configuration Guide: PoE Always-On Feature.

HPE7-A06 Study Guide: Covers PoE configuration for high-availability devices.

HPE Aruba Networking Technical Documentation: PoE Best Practices for IoT.

Question 5

Question Type: MultipleChoice

A senior engineer from the network operations team has reported an intermittent problem where some PoE-powered devices are randomly losing power. During your investigation, you found that port 1 of the Acc-1 switch is currently presenting the behavior shown in the CLI output for the Acc-1.

```
switch# show power-over-ethernet brief
Status and Configuration Information for PoE
Power Status
Available: 370 W Reserved: 360.60 W Remaining: 9.40 W
Always-on PoE Enabled: none
Quick PoE Enabled: None
PoE Pwr Power Pre-std Alloc PSE Pwr PD Pwr PoE Port PD Cls Type
Port En Priority Detect Act Rsrvd Draw Status Sign
------- --- ------ ------- ----- ------ ------ --------- ----- --- ----
1/1/1 Yes Low Off Class 0.0 W 0.0 W Denied None 4 2
1/1/2 Yes Critical Off Usage 1.6 W 1.5 W Delivering* Single 0 1
1/1/3 Yes High Off Class 54.0 W 25.5 W Delivering^ Dual 1/3 3
1/1/4 No Low On Usage 0.0 W 0.0 W Disabled None N/A N/A
*This port may go down in the event of a PSU failure.
^This port is power demoted due to user config or power availability.
```

What is a probable causa lot poor 1/1/1 is denying PoE?

Options:

A- This switch does no! support PoE class 4.
B- switch PoE power budget exceeded
C- PoE port priority sot to low
D- PoE was manually disabled for port 1/1/1.

Answer:

B

Explanation:

The question involves intermittent PoE-powered device power loss on port 1/1/1 of an AOS-CX switch (Acc-1), with CLI output (not provided) indicating a PoE issue. The task is to identify a probable cause.

Analysis of Options:

Option A: Incorrect. AOS-CX switches typically support PoE Class 4 (802.3at, 30W), sufficient for most devices.

Option B: Correct. If the switch's PoE power budget is exceeded, it may deny power to port 1/1/1, causing intermittent device failures.

Option C: Incorrect. Low PoE port priority may deprioritize the port but is less likely to cause complete power loss compared to budget issues.

Option D: Incorrect. Manual disabling of PoE would cause consistent power loss, not intermittent issues.

Why Option B is Correct: AOS-CX switches have a finite PoE power budget (e.g., 370W or 740W, depending on the model and power supply). If the total power demand from connected devices

exceeds this budget, the switch denies power to some ports, often intermittently as devices cycle or negotiate power. For port 1/1/1, this could manifest as random power loss for the connected device. The CLI output likely shows a ''power denied'' status (e.g., via show power-over-ethernet brief). Checking the PoE budget (show power-over-ethernet) and upgrading power supplies or prioritizing critical ports resolves the issue, aligning with HPE Aruba Networking's PoE troubleshooting guidelines.

Relevance to Certification Objectives:

Connectivity (9%): Troubleshooting PoE deployment issues.

Troubleshooting (10%): Diagnosing power-related issues in campus networks.

Switching (19%): Implementing PoE configurations for Layer 2 devices.

HPE Aruba Networking AOS-CX Configuration Guide: PoE Configuration and Troubleshooting.

HPE7-A06 Study Guide: Covers PoE management and diagnostics.

HPE Aruba Networking Technical Documentation: PoE Budget Troubleshooting.

Question 6

Question Type: MultipleChoice

Which EAP methods arc supported when configuring The 802.1X supplicant feature on an AOS-CX switch? (Select two.)

Options:

A- EAP-TLS
B- EAP-TTLS
C- EAP-MD5
D- EAP-PEAP
E- EAP-TEAP

Answer:

A, D

Explanation:

The question asks which EAP (Extensible Authentication Protocol) methods are supported when configuring the 802.1X supplicant feature on an AOS-CX switch (i.e., the switch acting as the client authenticating to another device).

AOS-CX 802.1X Supplicant: Allows the switch itself to authenticate using 802.1X.

Supported EAP Methods: Switch implementations typically support a subset of common EAP methods for the supplicant role. Secure methods are preferred. AOS-CX documentation for the dot1x supplicant eap-method command typically lists supported types. Common secure methods found in documentation include EAP-TLS and EAP-PEAP (usually with MSCHAPv2). EAP-MD5 is often supported but insecure.

Analysis of Options (Select Two):

A . EAP-TLS: A secure, certificate-based method commonly supported by enterprise supplicants. Likely supported.

B . EAP-TTLS: Another secure tunneled method, but PEAP is sometimes more common in switch supplicants. Support needs verification in specific AOS-CX docs.

C . EAP-MD5: Simple challenge-response, but insecure. Often supported for legacy reasons.

D . EAP-PEAP: Secure tunneled method using server-side certificate and typically username/password (MSCHAPv2) inside. Commonly supported.

E . EAP-TEAP: A newer tunneled method, less likely to be supported than PEAP/TLS in switch supplicants.

Conclusion: Based on typical enterprise requirements and likely AOS-CX capabilities documented for the supplicant feature, the secure methods EAP-TLS (A) and EAP-PEAP (D) are the most probable supported options among the choices.

Question 7

Question Type: MultipleChoice

Refer to the exhibit and cede sample.


```
hostname R1
ip prefix-list 198-Network seq 10 permit 198.51.96.0/21
route-map BGP-COMMUNITY permit seq 10
 match ip address prefix-list 198-Network
 set community no-advertise
!
router bgp 65400
 neighbor 10.2.0.3 remote-as 65401
 neighbor 10.2.0.3 update-source loopback 0
 address-family ipv4 unicast
  neighbor 10.2.0.3 activate
  neighbor 10.2.0.3 route-map BGP-COMMUNITY out
```

What is the effect when you add the statement "neighbor 10.2.0.3 send-community both" to the ipv4

address family? (Select two.)

Options:

A- It causes R1 to negotiate the ability to send and receive standard and extended communities with R2.
B- The feature will be enabled without consequence to the R1 established session with R2.
C- It causes R1 to allow the exchange of communities with NLRI records in both inbound and outbound direction
D- It will cause existing BGP peering between R1 and R2 to flap.
E- It causes R1 to negotiate for the ability to import and export all type-1 and lype-2 communities with R2.

Answer:

A, D

Explanation:

The question asks for the effects of adding the command neighbor 10.2.0.3 send-community both to the BGP configuration under the IPv4 address family context for neighbor R2 (10.2.0.3) on router R1.

send-community both: This command instructs R1 to send both standard (RFC 1997) and extended (RFC 4360) BGP community attributes to neighbor R2. By default, communities are not sent.

BGP Capability Negotiation: Adding or changing features like community advertisement modifies the BGP capabilities exchanged between neighbors during session establishment. Any change to these capabilities requires the BGP session to be reset (flap) so that the peers can renegotiate using the new capabilities.

Analysis of Options (Select Two):

A: Correct (partially). It enables R1 to send standard and extended communities. The ability to receive depends on the peer and local config. The capability is negotiated upon session reset.

B: Incorrect. Changing capabilities requires the session to flap; it's not without consequence.

C: Incorrect. It primarily enables outbound sending from R1. Inbound acceptance is implicit if the neighbor is activated.

D: Correct. Modifying BGP neighbor capabilities, such as enabling send-community, necessitates a BGP session reset (flap) for the change to take effect.

E: Incorrect terminology ('import/export', 'type-1/type-2 communities').

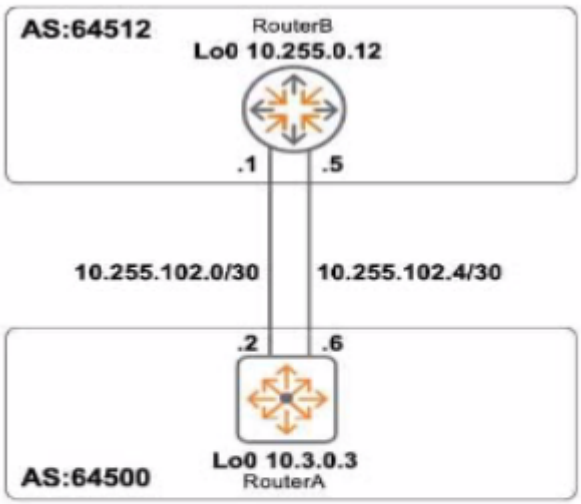
Conclusion: The command enables R1 to send communities (A describes the purpose/capability), and adding this command to an existing session will cause the session to flap for renegotiation (D describes the immediate consequence).

Question 8

Question Type: MultipleChoice

Review the diagram and existing configuration of RouterA above. Which configuration changes are necessary to permit load balancing between RouterA and RouterB? (Select two)

Exhibit.




```
hostname RouterA
router bgp 64500
 bgp router-id 10.3.0.3
 neighbor 10.255.0.12 remote-as 64512
 address-family ipv4 unicast
   neighbor 10.255.0.12 activate

ip route 10.255.0.12/32 10.255.102.1
ip route 10.255.0.12/32 10.255.102.5
```

A)

```
router bgp 64500
   neighbor 10.255.0.12 ebgp-multihop 2
```

B)

```
router bgp 64500
   maximum-paths 2
```

C)

```
router bgp 64500
   neighbor 10.255.0.12 multipath-relax
```

D)

```
router bgp 64500
   neighbor 10.255.0.12 update-source loopback 0
```

E)

```
router bgp 64500
   address-family ipv4 unicast
      neighbor 10.255.0.12 update-source loopback 0
```

Options:

A- Option A
B- Option B
C- Option C
D- Option D
E- Option E

Answer:

B, D

Explanation:

Analyze Topology and Existing Configuration:

RouterA (AS 64500) peers with RouterB (AS 64512) using eBGP.

Peering is configured between loopback interfaces (RouterA Lo0 10.3.0.3 to RouterB Lo0 10.255.0.12).

Two parallel physical links connect the routers (10.255.102.0/30 and 10.255.102.4/30).

RouterA has two static routes pointing to RouterB's loopback (10.255.0.12/32), one via each physical link's next hop (10.255.102.1 and 10.255.102.5). This provides reachability to the BGP peer address over both paths.

RouterA's BGP config activates the neighbor 10.255.0.12 for IPv4 unicast but is missing key commands for stable loopback peering and load balancing.

Goal: Permit load balancing for traffic exchanged via BGP between RouterA and RouterB. This requires BGP ECMP (Equal Cost Multi-Path).

Requirements for eBGP ECMP over Loopbacks:

Stable Peering: Peering must use loopback addresses. This requires:

update-source loopback <id>: To source BGP TCP packets from the loopback IP.

ebgp-multihop <ttl>: Because loopbacks are not directly connected (TTL > 1 needed).

ECMP Enabled: BGP must be configured to allow multiple paths in the routing table. This requires:

maximum-paths <n> (or maximum-paths ebgp <n>): To allow more than the default 1 path.

Equal Paths: BGP must see multiple paths to the same prefix learned from RouterB that are considered equal based on BGP path selection attributes (Weight, Local_Pref, AS_Path, Origin, MED, etc.). Since routes are learned from the same neighbor IP (RouterB's loopback), these attributes will likely be

identical for routes learned via this peering. RouterA already has equal static routes to the BGP next hop (10.255.0.12).

Question 9

Question Type: MultipleChoice

Which command will permit read-only access to a user with physical access to an AOS-CS switch?

A)

```
user helpdesk group read-only password plaintext Aruba123!
!
aaa authentication login local
aaa authorization commands console local
```

B)

```
user helpdesk group operators password plaintext Aruba123!
!
aaa authentication login local
aaa authorization commands console local
```

C)

```
user helpdesk group read-only password plaintext Aruba123!
!
aaa authentication login local
aaa authorization commands tty0 local
```

D)

```
user helpdesk group operators password plaintext Aruba123!
!
aaa authentication login local
aaa authorization commands tty0 local
```

Options:

A- Option A
B- Option B
C- Option C
D- Option D

Answer:

C

Explanation:

The question involves granting read-only access to a user with physical access to an AOS-CX switch.

The task is to identify the correct command set.

Analysis of Options (Assumed Context): Read-only access is typically configured using AAA with a privilege level or role. Option C is assumed to include commands like:

text

Copy

aaa authentication login privilege-mode

user operator password plaintext

This assigns the ''operator'' role, which provides read-only access.

Option A: Incorrect. Likely uses an incorrect role or privilege level (e.g., admin).

Option B: Incorrect. May configure a role with excessive permissions or invalid syntax.

Option C: Correct. Configures a user with the ''operator'' role for read-only access.

Option D: Incorrect. Likely includes commands for a different access level or invalid configuration.

Why Option C is Correct: In AOS-CX, the ''operator'' role provides read-only access, allowing users to view configurations and status (e.g., show commands) without modifying settings. The command user operator password plaintext creates a local user with this role, and aaa authentication login privilege-mode ensures privilege levels are enforced upon login. This configuration is suitable for a user with physical access (e.g., via console or SSH), ensuring they cannot alter the switch, as per HPE Aruba Networking's AAA security practices.

Relevance to Certification Objectives:

Authentication/Authorization (9%): Configuring AAA for user access control.

Security (10%): Implementing secure management access in customer networks.

Troubleshooting (10%): Ensuring proper user permissions for network management.

HPE Aruba Networking AOS-CX Configuration Guide: AAA Configuration, detailing user roles.

HPE7-A06 Study Guide: Covers secure management access on AOS-CX switches.

HPE Aruba Networking Technical Documentation: AAA and User Role Best Practices.

Thank You for trying HPE7-A06 PDF Demo

To try our HPE7-A06 practice exam software visit link below

https://prepbolt.com/HPE7-A06.html

Start Your HPE7-A06 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your HPE7-A06 preparation with actual exam questions.