

HP HPE4-A31

Aruba Certified Switching Expert Practical

**Thank You for Downloading HPE4-A31 Updated Exam
Questions**

<https://certs4sale.com/hp/hpe4-a31-pdf-exam-dumps>

Question: 1

You are given access to two Aruba switches. Your task is to configure a Link Aggregation Group (LAG) using ports 1/1/1 and 1/1/2 on both switches. How would you verify that the LAG is functioning correctly?

Answer: See the Solution below.

Solution:

1. Use the show lacp interfaces command to check if the interfaces are bundled in the LAG.
2. Ensure that both interfaces show an "Active" state and "Up" status.
3. Check for any error messages or discrepancies related to LAG in the switch logs.
4. Test connectivity by pinging between devices connected across the LAG link.

Question: 2

You are tasked with setting up a dynamic LACP link aggregation between Switch A and Switch B. Use interfaces 1/2/1 and 1/2/2. How would you ensure successful LACP negotiation?

Answer: See the Solution below.

Solution:

1. Use the show lacp status command to check if both interfaces are negotiating LACP correctly.
2. Ensure the interfaces show "Active" and "Negotiated" status.
3. Check LACP counters for any errors or timeouts.
4. Test connectivity between switches to validate LACP functionality.

Question: 3

You are required to configure a trunk interface to allow VLANs 10, 20, and 30 across two switches using a static LAG. How would you verify that the trunk is forwarding traffic for all specified VLANs?

Answer: See the Solution below.

Solution:

1. Run the show vlan command to ensure that VLANs 10, 20, and 30 are tagged on the trunk ports.
2. Use the show interfaces trunk command to verify the VLANs are properly forwarded.
3. Test connectivity by pinging devices in each VLAN to ensure traffic is passing through.
4. Check for any trunking errors or inconsistencies in the switch logs.

Question: 4

Your task is to remove an existing dynamic LACP link aggregation and create a new one using static mode. How would you validate that the static LAG is operational?

Answer: See the Solution below.

Solution:

1. After removing the LACP configuration, set up the static LAG using the appropriate commands.
2. Use the show interfaces status command to verify that the interfaces are "Up" and bundled in the LAG.
3. Confirm that both interfaces are forwarding traffic by testing connectivity across the LAG.
4. Check for any error messages or log entries related to the new LAG configuration.

Question: 5

You need to create a link aggregation group between two switches with redundant connections for failover. Use interfaces 1/3/1, 1/3/2, and 1/3/3 on both switches. How would you verify redundancy and failover functionality?

Answer: See the Solution below.

Solution:

1. Configure the LAG with the specified interfaces and verify using show lacp that all interfaces are active.
2. Run a continuous ping test between two devices on either side of the LAG.
3. Disconnect one of the interfaces in the LAG and observe that traffic seamlessly continues through the other interfaces.
4. Use show lacp again to confirm that the disconnected interface is down while the others remain operational.

Question: 6

You are given access to two Aruba switches with pre-configured LAGs. Your task is to add a new VLAN, VLAN 50, and allow it through the LAG trunk. How would you ensure that VLAN 50 is added successfully?

Answer: See the Solution below.

Solution:

1. Add VLAN 50 to the LAG trunk configuration using the appropriate command.
2. Use the show running-config command to verify that VLAN 50 is part of the trunk configuration.
3. Test connectivity by pinging devices in VLAN 50 to ensure traffic is being passed.
4. Check the switch logs for any trunking errors related to VLAN 50.

Question: 7

You need to secure a VLAN by implementing access control lists (ACLs) to restrict access to certain IP ranges. How would you verify that the ACLs are applied and functioning as intended?

Answer: See the Solution below.

Solution:

1. Configure the ACLs on the relevant VLAN interfaces.
2. Use the show access-list hitcount command to verify that the ACL is being triggered by matching traffic.
3. Test access from IP addresses within the restricted ranges to ensure they are blocked.
4. Check the switch logs for any errors or anomalies related to the ACLs.

Question: 8

You are tasked with creating a VLAN for guest users and isolating it from the corporate VLANs. How would you validate that the guest VLAN is properly isolated?

Answer: See the Solution below.

Solution:

1. Create the guest VLAN and ensure it is applied to the necessary ports.

2. Use the show vlan command to verify that the VLAN is correctly configured and assigned.
3. Perform a ping test between devices in the guest VLAN and corporate VLANs to ensure isolation.
4. Check the switch routing table to confirm no routes exist between the guest VLAN and corporate VLANs.

Question: 9

You need to configure a switch for inter-VLAN routing between VLANs 100 and 200. How would you validate that the routing configuration is correct?

Answer: See the Solution below.

Solution:

1. Configure the inter-VLAN routing on the switch by assigning the necessary interfaces.
2. Use the show ip route command to verify that routes for VLANs 100 and 200 are present in the routing table.
3. Perform a ping test between devices in VLAN 100 and VLAN 200 to confirm routing is working.
4. Check the switch logs for any routing errors or inconsistencies.

Question: 10

Your task is to implement loop protection across all edge ports in VLAN 300 using Aruba's Loop Guard feature. How would you confirm that Loop Guard is active and functioning?

Answer: See the Solution below.

Solution:

1. Enable Loop Guard on all edge ports in VLAN 300 using the appropriate command.
2. Use the show spanning-tree detail command to verify that Loop Guard is enabled on the necessary ports.
3. Simulate a loop by connecting two edge ports and check that Loop Guard blocks the affected ports.
4. Review the switch logs to confirm that Loop Guard events are recorded.

Question: 11

You need to configure BPDU Guard on all access ports to protect against BPDU attacks. How would you

Answer: See the Solution below.

Solution:

1. Enable BPDU Guard on all access ports using the appropriate command.
2. Use the show spanning-tree interface command to verify BPDU Guard is active on the correct ports.
3. Simulate a BPDU attack by sending BPDUs into an access port and check that the port is automatically disabled.
4. Review the switch logs to confirm BPDU Guard actions are logged.

Question: 12

Your task is to configure a root guard on a specific switch to maintain its position as the root bridge. How would you validate that the root guard configuration is correct?

Answer: See the Solution below.

Solution:

1. Enable root guard on the necessary ports using the appropriate command.
2. Use the show spanning-tree detail command to confirm that root guard is active on the designated ports.
3. Simulate a root bridge election by sending a higher priority BPDU and check that root guard prevents the port from accepting the change.
4. Review the switch logs to verify that root guard actions are logged.

Question: 13

You are asked to configure a basic VSX deployment between two Aruba switches. How would you verify the VSX configuration is active and synchronized?

Answer: See the Solution below.

Solution:

1. After configuring VSX, use the show vsx status command to check if both switches are in the "Active-Active" state.
2. Run the show vsx config-sync command to ensure that the configuration is synchronized across both switches.

3. Validate that the VSX inter-switch link (ISL) is operational by checking for any errors or packet loss.
4. Test failover functionality by simulating a failure and verifying the other switch takes over.

Question: 14

You are required to configure VRRP for gateway redundancy between two Aruba switches. How would you validate that VRRP failover occurs correctly?

Answer: See the Solution below.

Solution:

1. Configure VRRP on both switches and verify with the show vrrp command that the master and backup roles are properly assigned.
2. Simulate a failure on the master switch and ensure that the backup switch takes over as the master without any downtime.
3. Check the show vrrp output on the backup switch after failover to confirm its new role as master.
4. Review the switch logs for any VRRP-related errors or failover events.

Question: 15

You need to configure Multi-Chassis Link Aggregation (MC-LAG) using VSX. How would you ensure that the MC-LAG is correctly established and operational?

Answer: See the Solution below.

Solution:

1. Configure MC-LAG on both VSX switches using the appropriate LACP settings.
2. Use the show lacp command to verify that the MC-LAG interfaces are active and operating correctly.
3. Check that the LACP status on both switches shows that the ports are synchronized and part of the LAG.
4. Perform a load balancing test by sending traffic across the MC-LAG to confirm proper load distribution between the interfaces.
5. Verify there are no error messages in the logs related to MC-LAG configuration.

Question: 16

You are required to configure Gateway Redundancy (GTR) on two Aruba switches and ensure that traffic

switch is the root bridge. How would you validate that the configured switch is the root bridge?

Answer: See the Solution below.

Solution:

1. Set the switch priority to a lower value (e.g., 4096) to ensure it becomes the root bridge.
2. Use the show spanning-tree command to verify the switch is elected as the root bridge in the network.
3. Check the role of each port in the spanning tree topology and ensure that root ports and designated ports are correctly assigned.
4. Test STP by introducing a network change, such as disconnecting a link, and verify that the network topology reconverges with the switch as the root.
5. Check the switch logs for any STP-related errors or changes.

Question: 17

You need to harden a switch by disabling unused interfaces and applying a default security policy. How would you validate that the security policy is effectively applied?

Answer: See the Solution below.

Solution:

1. Disable all unused interfaces by manually shutting them down using the interface disable command.
2. Apply the security policy by configuring access control and other security features as needed.
3. Use the show interface status command to verify that all unused interfaces are administratively down.
4. Check the policy logs and security counters to ensure the security policy is being enforced.
5. Perform tests to simulate unauthorized access attempts and confirm that the security measures block them.

Question: 18

You are tasked with configuring a private VLAN for enhanced security. How would you confirm that the private VLAN is effectively isolating devices?

Answer: See the Solution below.

Solution:

1. Configure the private VLAN by setting up primary, isolated, and promiscuous ports.
2. Use the show vlan private-vlan command to verify that the private VLAN is configured correctly.
3. Perform ping tests between devices in isolated ports and promiscuous ports to ensure that communication is allowed only through the promiscuous port.
4. Test communication between isolated ports to confirm they cannot communicate directly.
5. Review the logs for any VLAN-related errors or misconfigurations.

Question: 19

You are asked to implement VLAN-based load balancing between two switches. How would you verify that the load balancing is working as intended?

Answer: See the Solution below.

Solution:

1. Configure VLAN-based load balancing by assigning different VLANs to multiple trunk links between the switches.
2. Use the show vlan statistics command to monitor traffic distribution across the trunks for each VLAN.
3. Test the configuration by generating traffic for each VLAN and verifying that the load is balanced across the available links.
4. Perform a failover test by disconnecting one trunk link and ensuring that traffic is redistributed correctly without any loss.
5. Check the switch logs for any errors or issues related to load balancing.

Question: 20

You need to configure Loop Protection using Aruba's loop protection feature across multiple switches. How would you validate that Loop Protection is functioning?

Answer: See the Solution below.

Solution:

1. Enable Loop Protection on the necessary ports using the appropriate command.
2. Use the show loop-protect command to confirm that the feature is active on the correct ports.
3. Simulate a loop by physically creating a network loop and verifying that the switch blocks the affected

ports to prevent the loop.

4. Check the logs for any loop protection events and ensure the feature is successfully preventing loops.
5. Reconnect the network and verify that the ports are automatically re-enabled after the loop condition is resolved.

THANK YOU FOR DOWNLOADING HPE4-A31 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our HPE4-A31 Exam Product

Visit Our Site to Purchase the Full Set of Actual HPE4-A31 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/hp/hpe4-a31-pdf-exam-dumps>