HPE6-A85 Practice Questions

Shared by Pratt on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You put in a few show commands on switches EDGE1 and CORE1 to attempt to gather information to troubleshoot the issue Use the show command output images to determine the reason for the EDGE1 uplink being down

EDGE1# TROUBLESHOOTING - SHOW COMMANDS OUTPUT

```
EDGE1# show span vlan 20
Port          Role          State
    TCN-Tx     TCN-Rx
------------ -------------- ----------
--- ---------- ----------
lag1          Disabled      Blocking
    2          2
EDGE1# show run int 1/1/51
interface 1/1/51
    no shutdown
    description Uplink_To_Core1
    lag 1
    exit
EDGE1# show run int 1/1/52
interface 1/1/52
    no shutdown
    description Uplink_To_Core1
    lag 1
    exit
EDGE1# show run int lag1
interface lag 1
    no shutdown
    no routing
    vlan trunk native 20
    vlan trunk allowed all
    lacp mode active
    exit
EDGE1# show lacp int
Actor details of all interfaces:
-------------------------------------------------------------------------------
Intf      Aggr      Port  Port  State   System-ID         System Aggr Forwarding
          Name      Id    Pri                             Pri    Key  State
-------------------------------------------------------------------------------
1/1/51    lag1      52    1     ALFOE   b8:d4:e7:b5:22:80 65534  1    lacp-block
1/1/52    lag1      53    1     ALFOE   b8:d4:e7:b5:22:80 65534  1    lacp-block
```

CORE1# TROUBLESHOOTING - SHOW COMMANDS OUTPUT

```
CORE1# show span vlan 20
Port          Role          State
Rx    TCN-Tx     TCN-Rx
------------ -------------- ----------
----- ---------- ----------
lag1          Designated    Forwarding
    2          2
CORE1# show run int 1/1/51
interface 1/1/51
    no shutdown
    lag 1
    exit
CORE1# show run int 1/1/52
interface 1/1/52
    no shutdown
    lag 1
    exit
CORE1# show run int lag 1
interface lag 1
    no shutdown
    no routing
    vlan trunk native 20
    vlan trunk allowed all
    exit
CORE1# show lacp int
Actor details of all interfaces:
CORE1# show lacp int
Actor details of all interfaces:
-------------------------------------------------------------------------------
Intf      Aggr      Port  Port  State   System-ID         System Aggr Forwarding
          Name      Id    Pri                             Pri    Key  State
-------------------------------------------------------------------------------
1/1/51    lag1                                                      up
1/1/52    lag1                                                      up
```

Options:

A- The physical interfaces are not members of the correct LAG.
B- Spanning-Tree block state is preventing the Core uplink from having connectivity to the edge
C- The Core is connected to the incorrect physical interlaces
D- LACP is not configured on the Core uplink

Answer:

D

Explanation:

LACP is a protocol that allows multiple physical links to be aggregated into a single logical link for increased bandwidth and redundancy. LACP must be configured on both ends of the link for it to work properly. In this case, EDGE1 has LACP configured on its uplink port-channel 1, but CORE1 does not have LACP configured on its corresponding port-channel 1. This causes a mismatch and prevents the link from coming up. Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/lacp.htm

Question 2

Question Type: OrderList

What is the correct order of the TCP 3-Way Handshake sequence?

Answer:

The initiating host sends a packet with no data to the target host with a SEQ=1 and sets the SYN flag to 1.The target host responds with a packet with ACK=2, SEQ=8, and the SYN and ACK flags set to 1.The initiating host sends a packet with SEQ=2, ACK=9, and the ACK flag set to 1.A normal-controlled connection is established.

Question 3

Question Type: MultipleChoice

What change does a client make when it roams from one access point to another in a WLAN?

Options:

A- It changes the destination MAC address on its 802.11 frames.
B- It changes the SSID to match the SSID on the new access point.
C- It changes its default gateway to the IP of the new access point.
D- It changes its association with the new wireless controller's SSID.

Answer:

A

Explanation:

When a client roams from one access point to another, it must change the destination MAC address on its 802.11 frames to match the new access point to which it is associated. The SSID does not change since it is typically consistent across an entire WLAN, and the default gateway remains the same as long as the client stays within the same IP subnet. The association to a new access point involves updating the destination MAC address in the frames that the client sends.

Question 4

Question Type: MultipleChoice

What is a common use of LLDP for wireless access points?

Options:

A- testing the quality of the physical link between the access point and the switch
B- discovery of rogue access points
C- exchange of RF channel information with nearby access points
D- negotiation of PoE power level to be provided to the access point

Answer:

D

Explanation:

LLDP (Link Layer Discovery Protocol) is commonly used by network devices, including wireless access points, to negotiate PoE (Power over Ethernet) power levels with the switch they are connected to. This allows the access point to communicate its power requirements to ensure it receives the necessary power for optimal operation.

Question 5

Question Type: MultipleChoice

When would you bond multiple 20MHz wide 802.11 channels?

Options:

A- To decrease the Signal to Noise Ratio (SNR)
B- To increase throughput between the client and AP
C- To provision highly available AP groups
D- To utilize high gain omni-directional antennas

Answer:

B

Explanation:

Bonding multiple 20MHz wide 802.11 channels is a technique to create a wider bandwidth channel that supports higher data rate transmissions. It can increase the throughput between the client and AP by using more spectrum resources and reducing interference. Reference: https://ieeexplore.ieee.org/document/9288995

Bonding multiple 20MHz wide 802.11 channels is a technique used to increase the throughput between the client device and the Access Point (AP). By combining two or more 20MHz channels into a wider channel (e.g., 40MHz, 80MHz, or even 160MHz), the data carrying capacity and, consequently, the overall throughput of the wireless connection are increased. This method is particularly useful in high-bandwidth applications or environments where higher data rates are required.

Question 6

Question Type: MultipleChoice

Which statement is true for a device with a MAC address of B8-31-B5-80-41-4F?

Options:

A- The device OUI is B8-31-B5 and the device NIC serial number is 80-41-4F
B- The device OUI is B8-31 and the device NIC serial number is B5-80-41-4F
C- The device OUI is 80-41-4F and the device NIC serial number is B8-31-B5
D- The device OUI is B8-31-B5 and the device serial number is MD5 hash is 80-41-4F

Answer:

A

Explanation:

A MAC address is divided into two parts: the Organizationally Unique Identifier (OUI) and the Network Interface Controller (NIC) serial number. The OUI is the first three octets of the MAC address and is unique to the manufacturer. The NIC serial number is the last three octets and is unique to the device itself. Therefore, for the MAC address B8-31-B5-80-41-4F, the OUI is B8-31-B5, and the NIC serial number is 80-41-4F.

Question 7

Question Type: MultipleChoice

When does the 802.1x authentication process begin when connecting to a secured enterprise mode WLAN?

Options:

A- After the firewall policies are applied to the session
B- After the client completes 802.11 association
C- After the captive portal authentication completes
D- After the WPA 4-Way Handshake is completed

Answer:

B

Explanation:

The 802.1x authentication process begins after the client device completes the 802.11 association with the access point but before the WPA 4-Way Handshake. This is part of the EAP (Extensible Authentication Protocol) process, which authenticates the device before allowing full network access.

Question 8

Question Type: MultipleChoice

You need to ensure that voice traffic sent through an ArubaOS-CX switch arrives with minimal latency. What is the best scheduling technology to use for this task?

Options:

A- QoS shaping
B- Rate limiting
C- Strict queuing
D- DWRR queuing

Answer:

C

Explanation:

Strict queuing is the best scheduling technology for ensuring that voice traffic, which is sensitive to latency, is prioritized above other types of traffic. This method ensures that voice traffic is sent first before other queued traffic, effectively reducing the possibility of delay.

Question 9

Question Type: MultipleChoice

Which authentication does Aruba's Captive Portal use?

Options:

A- Layer 3 authentication
B- MAC authentication
C- 802.1x authentication
D- Layer 2 authentication

Answer:

A

Explanation:

Aruba's Captive Portal uses Layer 3 authentication, which means that it intercepts the client's HTTP requests and redirects them to a web page where the client can enter their credentials. The credentials are then verified by a RADIUS server or a local database before granting network access. Reference: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/captive-portal/captive-portal-auth.htm

Aruba's Captive Portal primarily uses Layer 3 authentication, which operates at the network layer. When a user connects to a network with a Captive Portal, they are redirected to a web page for authentication. This process involves the user entering credentials or accepting terms and conditions through a web interface before gaining full access to the network. The Captive Portal intercepts the user's web traffic at Layer 3, requiring them to authenticate before proceeding, which is why it's considered a form of Layer 3 authentication.

Question 10

Question Type: MultipleChoice

Which three channels can be used simultaneously in a 2.4GHz WLAN environment while avoiding any co-channel interference?

Options:

A- 1,6, 11
B- 1,5, 10
C- 3,6, 9
D- 2,7, 11

Answer:

A

Explanation:

In a 2.4GHz WLAN environment, channels 1, 6, and 11 are recommended for use simultaneously to avoid co-channel interference because these channels do not overlap with each other. Each of these channels is separated by enough frequency space to ensure that the signals do not interfere, which is not the case with other channel combinations.