HPE6-A85 Q&As

Aruba Certified Campus Access Associate

Pass HP HPE6-A85 Exam with 100% Guarantee

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

https://www.certbus.com/hpe6-a85.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

Match each AAA service with its correct definition (Matches may be used more than once or not at all)

Select and Place:

Correct Answer:

QUESTION 2

What is the correct command to add a static route to a class-c-network 10.2.10.0 via a gateway of 172.16.1.1?

A. ip-route 10.2.10.0/24 172.16.1.1

B. ip route 10.2.10.0.255.255.255.0 172.16.1.1 description aruba

C. ip route 10.2.10.0/24.172.16.11

D. ip route-static 10.2 10.0.255.255.255.0 172.16.1.1

Correct Answer: A

Explanation: The correct command to add a static route to a class-c-network 10.2.10.0 via a gateway of 172.16.1.1 is ip-route 10.2.10.0/24 172.16.1.1 . This command specifies the destination network address (10.2.10.0) and prefix length (/24) and the next-hop address (172.16.1 .1) for reaching that network from the switch. The other commands are either incorrect syntax or incorrect parameters for adding a static route.

References: https://www.arubanetworks.com/techdocs/AOS- CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm

QUESTION 3

What does WPA3-Personal use as the source to generate a different Pairwise Master Key (PMK) each time a station connects to the wireless network?

A. Session-specific information (MACs and nonces)

B. Opportunistic Wireless Encryption (OWE)

C. Simultaneous Authentication of Equals (SAE)

D. Key Encryption Key (KEK)

Correct Answer: A

Explanation: The source that WPA3-Personal uses to generate a different Pairwise Master Key (PMK) each time a station connects to the wireless network is session-specific information (MACs and nonces). WPA3-Personal uses

Simultaneous Authentication of Equals (SAE) to replace PSK authentication in WPA2-Personal. SAE is a secure key establishment protocol that uses a Diffie-Hellman key exchange to derive a shared secret between two parties without

revealing it to an eavesdropper. SAE involves the following steps:

The station and the access point exchange Commit messages that contain their MAC addresses and random numbers called nonces.

The station and the access point use their own passwords and the received MAC addresses and nonces to calculate a shared secret called SAE Password Element (PE).

The station and the access point use their own PE and the received MAC addresses and nonces to calculate a shared secret called SAE Key Seed (KS). The station and the access point use their own KS and the received MAC addresses

and nonces to calculate a shared secret called SAE Key Confirmation Key (KCK).

The station and the access point use their own KCK and the received MAC addresses and nonces to calculate a confirmation value called SAE Confirm. The station and the access point exchange Confirm messages that contain their SAE

Confirm values.

The station and the access point verify that the received SAE Confirm values match their own calculated values. If they match, the authentication is successful and the station and the access point have established a shared secret called SAE

PMK.

The SAE PMK is different for each session because it depends on the MAC addresses and nonces that are exchanged in each authentication process. The SAE PMK is used as an input for the 4-way handshake that generates the Pairwise

Temporal Key (PTK) for encrypting data frames.

The other options are not sources that WPA3-Personal uses to generate a different PMK each time a station connects to the wireless network because:

Opportunistic Wireless Encryption (OWE): OWE is a feature that provides encryption for open networks without requiring authentication or passwords. OWE uses a similar key establishment protocol as SAE, but it does not generate a PMK.

Instead, it generates a Pairwise Secret (PS) that is used as an input for the 4-way handshake that generates the PTK.

Simultaneous Authentication of Equals (SAE): SAE is not a source, but a protocol that uses session-specific information as a source to generate a different PMK each time a station connects to the wireless network. Key Encryption Key (KEK): KEK is not a source, but an output of the 4-way handshake that generates the PTK. KEK is used to encrypt group keys that are distributed by the access point.

References: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e https://www.wi-fi.org/file/wi- fi-alliance-unlicensed-spectrum-in-the-us https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access- points/wpa3-dep-guide-og.html https://info.support.huawei.com/info- finder/encyclopedia/en/WPA3.html https://rp.os3.nl/2019-2020/p99/presentation.pdf

QUESTION 4

When using an Aruba standalone AP you select "Native VLAN" for the Client VLAN Assignment In which subnet will the client IPs reside?

A. The same subnet as the mobility controller

B. The same subnet as the Aruba ESP gateway

C. The same subnet as the mobility conductor

D. The same subnet as the access point

Correct Answer: D

Explanation: When using an Aruba standalone AP, selecting "Native VLAN" for the Client VLAN Assignment means that the clients will get their IP addresses from the same subnet as the access point\\'s IP address. This is because the access point acts as a DHCP server for the clients in this mode.

References:https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instan t-ug/iap-dhcp/iap-dhcp.htm

QUESTION 5

Review the configuration below.

```
Core-1(config)# interface loopback 0
Core-1(config-if)# ip address 10.1.200.1/32
Core-1(config)# router ospf 1
Core-1(config-ospf-1)# router-id 10.1.200.1
Core-1(config-ospf-1)# area 0
Core-1(config-ospf-1)# exit
```

Why would you configure OSPF to use the IP address 10.1.200.1 as the router ID?

A. The IP address associated with the loopback interface is non-routable and prevents loops

B. The loopback interface state is dependent on the management interface state and reduces routing updates.

C. The IP address associated with the loopback interface is routable and prevents loops

D. The loopback interface state Is independent of any physical interface and reduces routing updates.

Correct Answer: D

Explanation: The reason why you would configure OSPF Open Shortest Path First (OSPF) is a link-state routing protocol that dynamically calculates the best routes for data transmission within an IP network. OSPF uses a hierarchical structure that divides a network into areas and assigns each router an identifier called router ID (RID). OSPF uses hello packets to discover neighbors and exchange routing information. OSPF uses Dijkstra\\'s algorithm to compute the shortest path tree (SPT) based on link costs and build a routing table based on SPT. OSPF supports multiple equal-cost paths, load balancing, authentication, and various network types such as broadcast, point-to-point, point-to- multipoint, non-broadcast multi-access (NBMA), etc. OSPF is defined in RFC 2328 for IPv4 and RFC 5340 for IPv6. to use the IP address IP address Internet Protocol (IP) address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing. There are two versions of IP addresses: IPv4 and IPv6. IPv4 addresses are 32 bits long and written in dotted-decimal notation, such as 192.168.1.1. IPv6 addresses are 128 bits long and written in hexadecimal notation, such as 2001:db8::1. IP addresses can be either static (fixed) or dynamic (assigned by a DHCP server). 10.1.200.1 as the router ID Router ID (RID) Router ID (RID) is a unique identifier assigned to each router in a routing domain or protocol. RIDs are used by routing protocols such as OSPF, IS-IS, EIGRP, BGP, etc., to identify neighbors, exchange routing information, elect designated routers (DRs), etc. RIDs are usually derived from one of the IP addresses configured on the router\\'s interfaces or loopbacks, or manually specified by network administrators. RIDs must be unique within a routing domain or protocol instance. is that the loopback interface state Loopback interface Loopback interface is a virtual interface on a router that does not correspond to any physical port or connection. Loopback interfaces are used for various purposes such as testing network connectivity, providing stable router IDs for routing protocols, providing management access to routers, etc. Loopback interfaces have some advantages over physical interfaces such as being always up unless administratively shut down, being independent of any hardware failures or link failures, being able to assign any IP address regardless of subnetting constraints, etc. Loopback interfaces are usually numbered from zero (e.g., loopback0) upwards on routers. Loopback interfaces can also be created on PCs or servers for testing or configuration purposes using special IP addresses reserved for loopback testing (e.g., 127.x.x.x for IPv4 or ::1 for IPv6). Loopback interfaces are also known as virtual interfaces or dummy interfaces . Loopback interface state Loopback interface state refers to whether a loopback interface is up or down on a router . A loopback interface state can be either administratively controlled (by using commands such as no shutdown or shutdown) or automatically determined by routing protocols (by using commands such as passive-interface or ip ospf network point-to-point). A loopback interface state affects how routing protocols use the IP address assigned to the loopback interface for neighbor discovery , router ID selection , route advertisement , etc . A loopback interface state can also affect how other devices can access or ping the loopback interface . A loopback interface state can be checked by using commands such as show ip interfacebrief or show ip ospf neighbor . is independent of any physical interface and reduces routing updates. The loopback interface state is independent of any physical interface because it does not depend on any hardware or link status. This means that the loopback interface state will always be up unless it is manually shut down by an administrator. This also means that the loopback interface state will not change due to any physical failures or link failures that may affect other interfaces on the router. The loopback interface state reduces routing updates because it provides a stable router ID for OSPF that does not change due to any physical failures or link failures that may affect other interfaces on the router. This means that OSPF will not have to re-elect DRs Designated Routers (DRs) Designated Routers (DRs) are routers that are elected by OSPF routers in a broadcast or non-broadcast multi-access (NBMA) network to act as leaders and coordinators of OSPF operations in that network. DRs are responsible for generating link-state advertisements (LSAs) for the entire network segment, maintaining adjacencies with all other routers in the segment, and exchanging routing information with other DRs in different segments through backup designated routers (BDRs). DRs are elected based on their router priority values and router IDs . The highest priority router becomes the DR and the second highest priority router becomes the BDR . If there is a tie in priority values , then the highest router ID wins . DRs can be manually configured by setting the router priority value to 0 (which means ineligible) or 255 (which means always eligible) on specific interfaces . DRs can also be influenced by using commands such as ip ospf priority , ip ospf dr-delay , ip ospf network point-to-multipoint , etc . DRs can be verified by using commands such as show ip ospf neighbor , show ip ospf interface , show ip ospf database , etc . , recalculate SPT Shortest Path Tree (SPT) Shortest Path Tree (SPT) is a data structure that represents the shortest paths from a source node to all other nodes in a graph or network . SPT is used by link-state routing protocols such as OSPF and IS-IS to compute optimal routes based on link costs . SPT is built using Dijkstra\\'s algorithm , which starts

from the source node and iteratively adds nodes with the lowest cost paths to the tree until all nodes are included . SPT can be represented by a set of pointers from each node to its parent node in the tree , or by a set of next-hop addresses from each node to its destination node in the network . SPT can be updated by adding or removing nodes or links , or by changing link costs . SPT can be verified by using commands such as show ip route , show ip ospf database , show clns route , show clns database , etc . , or send LSAs Link- State Advertisements (LSAs) Link-State Advertisements (LSAs) are packets that contain information about the state and cost of links in a network segment . LSAs are generated and flooded by link-state routing protocols such as OSPF and IS-IS to exchange routing information with other routers in the same area or level . LSAs are used to build link-state databases (LSDBs) on each router , which store the complete topology of the network segment . LSAs are also used to compute shortest path trees (SPTs) on each router , which determine the optimal routes to all destinations in the network . LSAs have different types depending on their origin and scope , such as router LSAs , network LSAs , summary LSAs , external LSAs , etc . LSAs have different formats depending ontheir type and protocol version , but they usually contain fields such as LSA header , LSA type , LSA length , LSA age , LSA sequence number , LSA checksum , LSA body , etc . LSAs can be verified by using commands such as show ip ospf database , show clns database , debug ip ospf hello , debug clns hello , etc . due to changes in router IDs. The other options are not reasons because: The IP address associated with the loopback interface is non-routable and prevents loops: This option is false because the IP address associated with the loopback interface is routable and does not prevent loops. The IP address associated with the loopback interface can be any valid IP address that belongs to an existing subnet or a new subnet created specifically for loopbacks. The IP address associated with the loopback interface does not prevent loops because loops are caused by misconfigurations or failures in routing protocols or devices, not by IP addresses. The loopback interface state is dependent on the management interface state and reduces routing updates: This option is false because the loopback interface state is independent of any physical interface state, including the management interface state Management interface Management interface is an interface on a device that provides access to management functions such as configuration, monitoring, troubleshooting, etc . Management interfaces can be physical ports such as console ports, Ethernet ports, USB ports, etc., or virtual ports such as Telnet sessions, SSH sessions, web sessions, etc . Management interfaces can use different protocols such as CLI Command-Line Interface (CLI) Command-Line Interface (CLI) is an interactive text- based user interface that allows users to communicate with devices using commands typed on a keyboard . CLI is one of the methods for accessing management functions on devices such as routers, switches, firewalls, servers, etc . CLI can use different protocols such as console port serial communication protocol Serial communication protocol Serial communication protocol is a method of transmitting data between devices using serial ports and cables . Serial communication protocol uses binary signals that represent bits (0s and 1s) and sends them one after another over a single wire . Serial communication protocol has advantages such as simplicity, low cost, long

QUESTION 6

You need to drop excessive broadcast traffic on ingress to an ArubaOS-CX switch What is the best technology to use for this task?

A. Rate limiting

B. DWRR queuing

C. QoS shaping

D. Strict queuing

Correct Answer: A

Explanation: The best technology to use for dropping excessive broadcast traffic on ingress to an ArubaOS-CX switch is rate limiting. Rate limiting is a feature that allows network administrators to control the amount of traffic that enters or leaves a port or a VLAN on a switch by setting bandwidth thresholds or limits. Rate limiting can be used to prevent network congestion, improve network performance, enforce service level agreements(SLAs), or mitigate denial-of-service (DoS) attacks. Rate limiting can be applied to broadcast traffic on ingress to an ArubaOS-CX switch by using the storm-control command in interface configuration mode. This command allows network administrators to specify the percentage of bandwidth or packets per second that can be used by broadcast traffic on an ingress port. If the

broadcast traffic exceeds the specified threshold, the switch will drop the excess packets. The other options are not technologies for dropping excessive broadcast traffic on ingress because: DWRR queuing: DWRR stands for Deficit Weighted Round Robin, which is a queuing algorithm that assigns different weights or priorities to different traffic classes or queues on an egress port. DWRR ensures that each queue gets its fair share of bandwidth based on its weight while avoiding starvation of lower priority queues. DWRR does not drop excessive broadcast traffic on ingress, but rather schedules outgoing traffic on egress. QoS shaping: QoS stands for Quality of Service, which is a set of techniques that manage network resources and provide different levels of service to different types of traffic based on their requirements. QoS shaping is a technique that delays or buffers outgoing traffic on an egress port to match the available bandwidth or rate limit. QoS shaping does not drop excessive broadcast traffic on ingress, but rather smooths outgoing traffic on egress. Strict queuing: Strict queuing is another queuing algorithm that assigns different priorities to different traffic classes or queues on an egress port. Strict queuing ensures that higher priority queues are always served before lower priority queues regardless of their bandwidth requirements or weights. Strict queuing does not drop excessive broadcast traffic on ingress, but rather schedules outgoing traffic on egress.

References: https://en.wikipedia.org/wiki/Rate_limiting https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx- noscg/qos/storm-control.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/dwrr.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx- noscg/qos/shaping.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/strict.htm

QUESTION 7

Which flew in a Layer 3 IPv4 packet header is used to mitigate Layer 3 route loops?

A. Checksum

B. Time To Live

C. Protocol

D. Destination IP

Correct Answer: B

Explanation: The field in a Layer 3 IPv4 packet header that is used to mitigate Layer 3 route loops is Time To Live (TTL). TTL is an 8-bit field that indicates the maximum number of hops that a packet can traverse before being discarded. TTL is set by the source device and decremented by one by each router that forwards the packet. If TTL reaches zero, the packet is dropped and an ICMP Internet Control Message Protocol (ICMP) Internet Control Message Protocol (ICMP) is a network protocol that provides error reporting and diagnostic functions for IP networks. ICMP is used to send messages such as echo requests and replies (ping), destination unreachable, time exceeded, parameter problem, source quench, redirect, etc. ICMP messages are encapsulated in IP datagrams and have a specific format that contains fields such as type, code, checksum, identifier, sequence number, data, etc. ICMP messages can be verified by using commands such as ping , traceroute , debug ip icmp , etc . message is sent back to the source device. TTL is used to mitigate Layer 3 route loops because it prevents packets from circulating indefinitely in a looped network topology. TTL also helps to conserve network resources and avoid congestion caused by looped packets. The other options are not fields in a Layer 3 IPv4 packet header because: Checksum: Checksum is a 16-bit field that is used to verify the integrity of the IP header. Checksum is calculated by the source device and verified by the destination device based on the values of all fields in the IP header. Checksum does not mitigate Layer 3 route loops because it does not limit the number of hops that a packet can traverse. Protocol: Protocol is an 8-bit field that indicates the type of payload carried by the IP datagram. Protocol identifies the upper-layer protocol that uses IP for data transmission, such as TCP Transmission Control Protocol (TCP) Transmission Control Protocol (TCP) is a connection-oriented transport layer protocol that provides reliable, ordered, and error-checked delivery of data between applications on different devices . TCP uses a three-way handshake to establish a connection between two endpoints , and uses sequence numbers , acknowledgments , and windowing to ensure data delivery and flow control . TCP also uses mechanisms such as retransmission , congestion avoidance , and fast recovery to handle packet loss and congestion . TCP segments data

into smaller units called segments , which are encapsulated in IP datagrams and have a specific format that contains fields such as source port , destination port , sequence number , acknowledgment number , header length , flags , window size , checksum , urgent pointer , options , data , etc . TCP segments can be verified by using commands such as telnet , ftp , ssh , debug ip tcp transactions , etc . , UDP User Datagram Protocol (UDP) User Datagram Protocol (UDP) is a connectionless transport layer protocol that provides

QUESTION 8

What is an advantage of using Layer 2 MAC authentication?

A. it matches user names to MAC address

B. No setup is required on the client

C. MAC allow lists are easily maintained over time

D. MAC identifiers are hard to spoof

Correct Answer: B

Explanation: Layer 2 MAC authentication is a method of authenticating devices based on their MAC addresses without requiring any client-side configuration or credentials. The switch sends the MAC address of the device to an authentication server such as ClearPass or RADIUS, which checks if the MAC address is authorized to access the network. If yes, the switch grants access to the device based on the assigned role and policies. If no, the switch denies access or redirects the device to a captive portal for further authentication.

References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/1-overview/mac-authentication.htm

QUESTION 9

What does the status of "ALFOE" mean when checking LACP with "show lacp interfaces\\'"?

A. The interface on the local switch is configured as static-LAG

B. LACP is not configured on the peer side

C. LACP is in a synchronizing process

D. LACP is working fine with no problems

Correct Answer: D

Explanation: The status of "ALFOE" means that LACP Link Aggregation Control Protocol (LACP) is a network protocol that provides dynamic negotiation of link aggregation between two devices. LACP allows multiple physical links to be combined into a single logical link for increased bandwidth, redundancy, and load balancing. LACP is defined in IEEE 802.3ad standard. is working fine with no problems when checking LACP with "show lacp interfaces". The status of "ALFOE" is an acronym that stands for:

A: Active - The interface is actively sending LACP packets to negotiate link aggregation with the peer device.

L: Link Up - The interface has physical connectivity with the peer device.

F: Aggregatable - The interface can be aggregated with other interfaces into a single logical link.

O: Synchronized - The interface has successfully negotiated link aggregation parameters with the peer device and can transmit or receive traffic on the logical link.

E: Collecting/Distributing - The interface is collecting incoming traffic from the peer device and distributing outgoing traffic to the peer device on the logical link.

The other options are not correct because:

The interface on the local switch is configured as static-LAG: This option is false because static-LAG does not use LACP to negotiate link aggregation. Static-LAG requires manual configuration of link aggregation parameters on both devices

and does not have any status indicators.

LACP is not configured on the peer side: This option is false because if LACP is not configured on the peer side, the status of the interface would be "ALF? instead of "ALFOE". This means that the interface would not be synchronized or

collecting/distributing with the peer device.

LACP is in a synchronizing process: This option is false because if LACP is in a synchronizing process, the status of the interface would be "ALF-O" instead of "ALFOE". This means that the interface would not be collecting/distributing with

the peer device.

References: https://www.arubanetworks.com/techdocs/AOS- CX_10_08/NOSCG/Content/cx-noscg/lag/lag-overview.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx- noscg/lag/lag-lacp.htm https:// www.arubanetworks.com/techdocs/AOS- CX_10_08/NOSCG/Content/cx-noscg/lag/lag-lacp-status.htm

QUESTION 10

A network technician is troubleshooting one new AP at a branch office that will not receive Its configuration from Aruba Central The other APs at the branch are working as expected The output of the \\'show ap debug cloud-server command\\' shows that the "cloud conflg received" Is FALSE.

After confirming the new AP has internet access, what would you check next?

A. Disable and enable activate to trigger provisioning refresh

B. Verify the AP can ping the device on arubanetworks.com

C. Verify the AP has a license assigned

D. Disable and enable Aruba Central to trigger configuration refresh

Correct Answer: C

If the AP has internet access but does not receive its configuration from Aruba Central, one possible reason is that the AP does not have a license assigned in Aruba Central. A license is required for each AP to be managed by Aruba Central.

References:https://www.arubanetworks.com/techdocs/Central/2.5.2-GA/HTML_frameset.htm#GUID-8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html

Latest HPE6-A85 Dumps HPE6-A85 Practice Test HPE6-A85 Study Guide