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.geekcert.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

What is indicated by a solid amber radio status LED on an Aruba AP?

A. Not enough PoE is provided from the switch to power both radios of the AP

B. The radio is working in mesh mode

C. The radio is working the 5 GHz band only.

D. The radio is enabled in monitor or spectrum analysis mode

Correct Answer: D

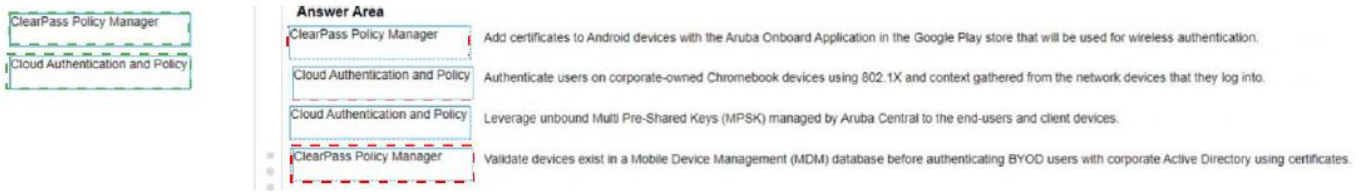
Explanation: The solid amber radio status LED on an Aruba AP Access Point (AP) Access Point (AP) is a device that connects wireless devices to a wired network using Wi-Fi or other wireless standards . APs act as transmitters and receivers of wireless signals and provide wireless coverage for a specific area . APs can operate in different modes such as root , repeater , bridge , mesh , etc . APs can also support different features such as security , QoS , roaming , load balancing , etc . APs can be standalone devices or managed by controllers or cloud services . APs can be verified by using commands such as show ap active , show ap database , show ap bss-table , etc . indicates that the radio is enabled in monitor or spectrum analysis mode. Monitor mode is a mode that allows the AP to scan all channels and collect information about wireless traffic, interference, rogue devices, etc. Spectrum analysis mode is a mode that allows the AP to scan all channels and collect information about RF Radio Frequency (RF) Radio Frequency (RF) is a term that refers to electromagnetic waves that have frequencies between 3 kHz and 300 GHz . RF waves are used for various purposes such as communication , broadcasting , radar , navigation , remote control , etc . RF waves can be modulated by changing their amplitude , frequency , or phase to encode information . RF waves can also be affected by various factors such as attenuation , reflection , refraction , diffraction , scattering , interference , noise , etc . RF waves can be measured by using devices such as spectrum analyzers , power meters , antennas , etc . environment, noise sources, channel utilization, etc. Both modes are useful for troubleshooting and optimizing wireless performance, but they disable normal data transmission and reception on the radio. The other options are not indicated by a solid amber radio status LED on an Aruba AP because: Not enough PoE is provided from the switch to power both radios of the AP: This option is false because not enough PoE Power over Ethernet (PoE) Power over Ethernet (PoE) is a technology that allows network devices to receive power and data over the same Ethernet cable . PoE eliminates the need for separate power sources and cables for devices such as IP phones , cameras , access points , etc . PoE is defined in IEEE 802.3af and IEEE 802.3at standards and supports different power classes and modes . PoE can be provided by switches or injectors that act as power sourcing equipment (PSE) and received by devices that act as powered devices (PD) . PoE can be verified by using commands suchas show power inline , show power-over-ethernet , debug ip device tracking , etc . is indicated by a blinking amber power status LED on an Aruba AP, not by a solid amber radio status LED. A blinking amber power status LED means that the AP is receiving insufficient power from the switch or injector and cannot operate normally. A solid green power status LED means that the AP is receiving sufficient power from the switch or injector and can operate normally. The radio is working in mesh mode: This option is false because the radio working in mesh mode is indicated by a solid green radio status LED on an Aruba AP, not by a solid amber radio status LED. A solid green radio status LED means that the radio is working in normal mode or mesh mode and can transmit or receive data on the assigned channel. Mesh mode is a mode that allows the AP to connect wirelessly to other APs and form a mesh network without requiring wired connections. The radio is working the 5 GHz band only: This option is false because the radio working in the 5 GHz band only is indicated by a solid blue radio status LED on an Aruba AP, not by a solid amber radio status LED. A solid blue radio status LED means that the radio is working in dual-band mode and can transmit or receive data on both 2.4 GHz and 5 GHz bands. References: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/ap-led- behavior.htm https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant- ug/troubleshooting/ap-monitor-mode.htm https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant- ug/troubleshooting/ap-spectrum-analysis.htm

QUESTION 2

Please match the use case to the appropriate authentication technology.

Select and Place:

Correct Answer:



QUESTION 3

Match the switching technology with the appropriate use case.

Select and Place:

Correct Answer:

TECHNOLOGY	USE CASE
LACP	Controls the dynamic addition and removal of ports to groups
802.1Q	Tags Ethernet frames with an additional VLAN header
802.1X	Used to authenticate EAP-capable clients on a switch port
LLDP	Used to identify a voice VLAN to an IP phone

QUESTION 4

Which commands are used to set a default route to 10.4.5.1 on an Aruba CX switch when ln-band management using an SVl is being used?

A. iP default-gateway 10.4.5.1

B. ip route 0 0 0.070 10.4 5.1 vrf mgmt

C. ip route 0.0 0 0/0 10.4.5.1

D. default-gateway 10.4.5.1

Correct Answer: C

Explanation: The command that is used to set a default route to 10.4.5.1 on an Aruba CX switch when in-band management using an SVI is being used is ip route 0.0 0 0/0 10.4.5.1 . This command specifies the destination network address

(0.0 0 0) and prefix length (/0) and the next-hop address (10.4.5.1) for reaching any network that is not directly connected to the switch. The default route applies to the default VRF Virtual Routing and Forwarding. VRF is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. VRFs are typically used to segment network traffic for security, privacy, or administrative purposes. , which is used for in-band management traffic that goes through an SVI Switch Virtual Interface. SVI is a virtual interface on a switch that allows the switch to route packets between different VLANs on the same switch or different switches that are connected by a trunk link. An SVI is associated with a VLAN and has an IP address and subnet mask assigned to it12.

References: https://www.arubanetworks.com/techdocs/AOS-CX/10_08/HTML/ip_route_4100i-6000-6100-6200/Content/Chp_StatRoute/def-rou.htm https://www.arubanetworks.com/techdocs/AOS-CX/10_08/HTML/ip_route_4100i-6000- 6100-6200/Content/Chp_VRF/vrf-overview.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