# HPE6-A85$^{\text{Q\&As}}$

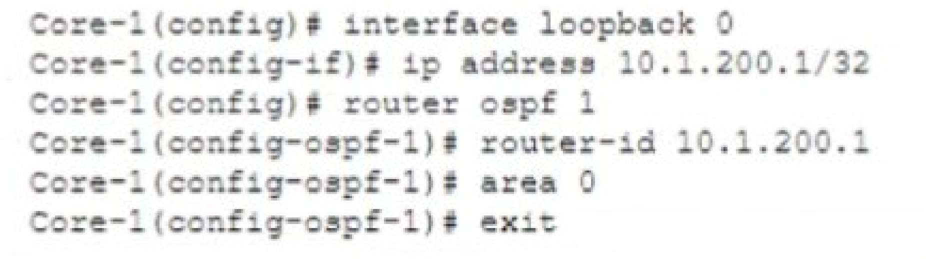
Aruba Certified Campus Access Associate

## Pass HP HPE6-A85 Exam with 100% Guarantee

Following Questions and Answers are all new published by HP Official Exam Center

**QUESTION 1**

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 2**

After having configured the edge switch uplink as requested your colleague says that they have failed to ping the core You ask your colleague to verify the connection is plugged in and the switch is powered on They confirm that both are correct You attempt to ping the core switch and confirm that the ping is failing. Knowing the nature of this deployment, what commands might you use to troubleshoot this issued

A. Ping 10.11 1 - ping the core to attempt to verify connectivity Show trunk - to verify if the LAG interface was correctly added to the switch Show spanning tree - to check for spanning-tree blocked states Show port-access clients interface all

- to view any port- access blocking states or failed authentication attempts on all interfaces Show run interface vlan20 - to double check the layer 3 svi configuration is correct for l_3 connectivity Show lldp neighors - to verify whether you are able to see the Core as an L2 neighbor to verify if the correct links are plugged in to the correct ports

B. diagnostic diag cable-diag 1/1/51 diag cable-diag 1/1/52 - to view diagnostic information for the physical link to get a status on any interruptions to Layer 1 connectivity, show ip route - to verify that the default gateway is present in the routing table show ip ospf - to check whether there is a layer 3 routing protocol enabled show ip dns - to view whether there is a valid dns source

C. Ping 10.1.1.1 - ping the core to attempt to verify connectivity show lacp agg - to verify which link aggregations are currently configured using which physical ports show lacp int - to verify the LACP status and whether any links are blocking in your topology show lldp neighors - to verify whether you are able to see the Core as an L2 neighbor to verify if the correct links are plugged in to the correct ports show run interface 1/1/51.1/1/52-to ensure the physical interfaces are no-shut and members of the lag show run interface lag 1 - to ensure the correct vlan trunking configuration is applied to the logical interface show run int vlan 20 - to ensure you have the L3 SVI no shut and configured in the correct subnet

D. Show run - to view the running configuration of the switch Show run | begin 20 "vlan 20"

- to ensure VLAN 20 was correctly added to the database show run | begin 20 \\'interface vlan 20\\' - to view the L3 SVI configuration Show run interface 1/1/51.1/1/52 - to ensure the physical interfaces are no shut and were added as

members of LAG 1 Show run int lag 1 - to verify LACP mode active was configured to eliminate LACP blocking states

Correct Answer: C

Explanation: These commands might help troubleshoot this issue as they check various aspects of the connectivity between the edge switch and the core switch, such as Layer 3 reachability, Layer 2 adjacency, LACP configuration and status, VLAN trunking configuration, and interface status. References:https://www.arubanetworks.com/techdocs/AOS-CX_10_04/CLI/GUID- 8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html

**QUESTION 3**

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 4**

Which Aruba technology will allow for device-specific passphrases to securely add headless devices to the WLAN?

A. Wired Equivalent Privacy (WEP)

B. Multiple Pre-Shared Key (MPSK)

C. Opportunistic Wireless Encryption (OWE)

D. Temporal Key Integrity Protocol (TKIP)

Correct Answer: B

Explanation: Multiple Pre-Shared Key (MPSK) is a feature that allows device-specific or group-specific passphrases to securely add headless devices to the WLAN Wireless Local Area Network. WLAN is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building. . MPSK enhances the WPA2 PSK Wi-Fi Protected Access 2 Pre-Shared Key. WPA2 PSK is a method of securing your network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users without an enterprise authentication server. mode by allowing different PSKs for different devices on the same SSID Service Set Identifier. SSID is a case-sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a wireless local-area network (WLAN). The SSID acts as a password when a mobile device tries to connect to the basic service set (BSS) -- a component of the IEEE 802.11 WLAN architecture. . MPSK passwords can be generated or user-created and are managed by ClearPass Policy Manager12.

References:

https://blogs.arubanetworks.com/solutions/simplify-iot-authentication-with-multiple-pre- shared-keys/
https://www.arubanetworks.com/techdocs/ClearPass/6.8/Guest/Content/AdministrationTas ks1/Configuring-MPSK.htm

**QUESTION 5**

Describe the purpose of the administrative distance

A. Routes teamed via external BGP have a higher administrative distance than routes learned via OSPF

B. The administrative distance is used as a trust rating tor route entries

C. The administrative distance for a static route is 10

D. The higher administrative distance is preferred

Correct Answer: B