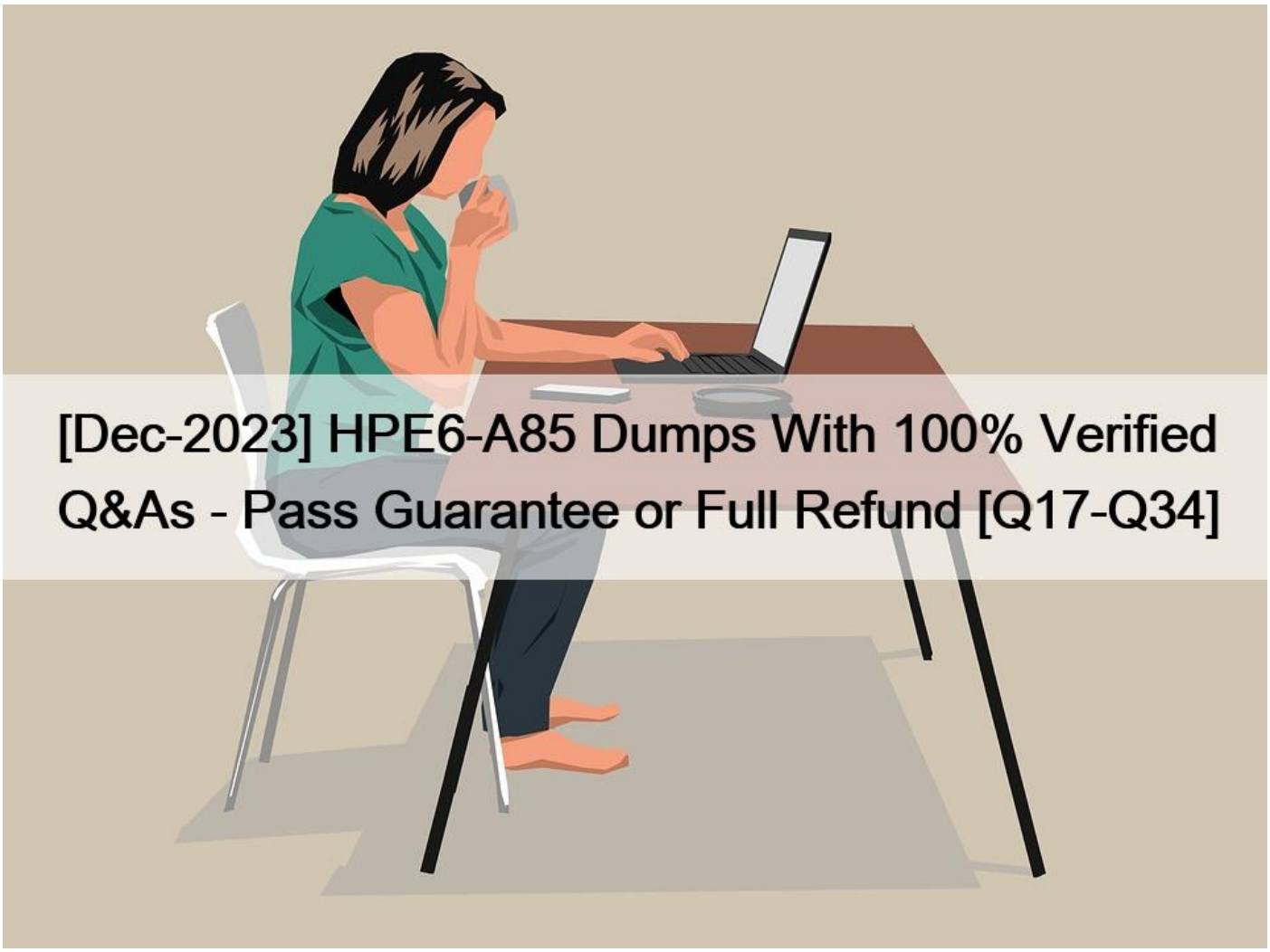
[Dec-2023 HPE6-A85 Dumps With 100% Verified Q&As - Pass Guarantee or Full Refund [Q17-Q34



[Dec-2023] HPE6-A85 Dumps With 100% Verified Q&As - Pass Guarantee or Full Refund
Pass HP HPE6-A85 Exam With Practice Test Questions Dumps Bundle

HP HPE6-A85 (Aruba Campus Access Associate) Exam is a certification exam designed for IT professionals who want to prove their skills and knowledge in designing, implementing, and managing Aruba wireless networks in a campus environment. This industry-recognized certification is offered by Hewlett Packard Enterprise (HPE), one of the leading providers of IT products and solutions worldwide.

HPE6-A85 exam covers a range of topics, including ArubaOS switches, access points, and basic network security. Candidates will be tested on their ability to configure and troubleshoot Aruba networks, as well as their understanding of network design principles and best practices.

QUESTION 17

What is a weakness introduced into the WLAN environment when WPA2-Personal is used for security?
* It uses X 509 certificates generated by a Certification Authority
* The Pairwise Temporal Key (PTK) is specific to each session
* The Pairwise Master Key (PMK) is shared by ail users
* It does not use the WPA 4-Way Handshake
Explanation

The weakness introduced into WLAN environment when WPA2-Personal is used for security is that PMK Pairwise Master Key (PMK) is a key that is derived from PSK Pre-shared Key (PSK) is a key that is shared between two parties before communication begins , which are both fixed. This means that all users who know PSK can generate PMK without any authentication process. This also means that if PSK or PMK are compromised by an attacker, they can be used to decrypt all traffic encrypted with PTK Pairwise Temporal Key (PTK) is a key that is derived from PMK, ANonce AuthenticatorNonce (ANonce) is a random number generated by an authenticator (a device that controls access to network resources, such as an AP), SNonce Supplicant Nonce (SNonce) is a random number generated by supplicant (a device that wants to access network resources, such as an STA), AA Authenticator Address (AA) is MAC address of authenticator, SA Supplicant Address (SA) is MAC address of supplicant using Pseudo-Random Function (PRF). PTK consists of four subkeys: KCK Key Confirmation Key (KCK) is used for message integrity check, KEK Key Encryption Key (KEK) is used for encryption key distribution, TK Temporal Key (TK) is used for data encryption, MIC Message Integrity Code (MIC) key. .

The other options are not weaknesses because:

It uses X 509 certificates generated by a Certification Authority: This option is false because WPA2-Personal does not use X 509 certificates or Certification Authority for authentication. X 509 certificates and Certification Authority are used in WPA2-Enterprise mode, which uses 802.1X and EAP Extensible Authentication Protocol (EAP) is an authentication framework that provides support for multiple authentication methods, such as passwords, certificates, tokens, or biometrics. EAP is used in wireless networks and point-to-point connections to provide secure authentication between a supplicant (a device that wants to access the network) and an authentication server (a device that verifies the credentials of the supplicant). for user authentication with a RADIUS server Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service .

The Pairwise Temporal Key (PTK) is specific to each session: This option is false because PTK being specific to each session is not a weakness but a strength of WPA2-Personal. PTK being specific to each session means that it changes periodically during communication based on time or number of packets transmitted. This prevents replay attacks and increases security of data encryption.

It does not use the WPA 4-Way Handshake: This option is false because WPA2-Personal does use the WPA 4-Way Handshake for key negotiation. The WPA 4-Way Handshake is a process that allows the station and the access point to exchange ANonce and SNonce and derive PTK from PMK. The WPA

4-Way Handshake also allows the station and the access point to verify each other’s PMK and confirm the installation of PTK.

References: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA_key_hierarchy_and_management

https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf

QUESTION 18

When measuring signal strength, dBm is commonly used and 0 dBm corresponds to 1 mW power.

What does -20 dBm correspond to?
* .-1 mW
* .01 mw
* 10 mW
* 1mW
Explanation

dBm is a unit of power that measures the ratio of a given power level to 1 mW. The formula to convert dBm to mW is: P(mW) = 1mW * 10(P(dBm)/10). Therefore, -20 dBm corresponds to 0.01 mW, as follows: P(mW) =

1mW * 10(-20/10) = 0.01 mW References:https://www.rapidtables.com/convert/power/dBm_to_mW.html

QUESTION 19

You need to drop excessive broadcast traffic on ingress to an ArubaOS-CX switch What is the best technology to use for this task?
* Rate limiting
* DWRR queuing
* QoS shaping
* Strict queuing
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 20

When using the OSPF dynamic routing protocol on an Aruba CX switch, what must match on the neighboring devices to exchange routes?
* Hello timers
* DR configuration
* ECMP method
* BDR configuration

Explanation

OSPF Open Shortest Path First. OSPF is a link-state routing protocol that uses a hierarchical structure to create a routing topology for IP networks. OSPF routers exchange routing information with their neighbors using Hello packets, which are sent periodically on each interface. To establish an adjacency Adjacency is a relationship formed between selected neighboring routers for the purpose of exchanging routing information., OSPF routers must agree on several parameters, including Hello timers, which specify how often Hello packets are sent on an interface. If the Hello timers do not match between neighboring routers, they will not form an adjacency and will not exchange routes.

References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/osfp/o

QUESTION 21

A customer has just implemented user and device certificates via a company-wide Group Based Policy (GPO) Which EAP method requires client certificates when authenticating to the network?
* EAP-TTLS
* EAP-TLS
* EAP-TEAP
* PEAP

Explanation

EAP-TLS is an authentication method that requires client certificates when authenticating to the network. It provides mutual authentication between the client and the server using public key cryptography and digital certificates.

References:https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content/CPPM_UserGuide/EAP-TLS

QUESTION 22

What can be done to dynamically set the PoE Priority on a switch port when deploying IP cameras APs. and other PoE devices?
* Enable Quick PoE on the switch modules
* Enable profiling for device provisioning
* Configure PoE power management to Class-based Mode

* Configure PoE power management to Dynamic Mode
Explanation

Profiling is a feature that allows Aruba switches to automatically identify and classify devices connected to them based on various attributes such as MAC address, DHCP options, LLDP information, etc. Profiling can be used to dynamically set the PoE priority on a switch port based on the device type and power requirements.

For example, an IP camera may have a higher PoE priority than a printer or a PC. Profiling can also be used to apply other configuration settings such as VLANs, ACLs, QoS, etc. based on the device profile.

References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-ove

QUESTION 23

What is the ideal Aruba access switch for a cost-effective connection to 200-380 clients, printers and APs per distribution rack?
* Aruba CX 6400
* Aruba CX 6200
* Aruba CX 6300
* Aruba CX 6000
Explanation

The ideal Aruba access switch for a cost-effective connection to 200-380 clients, printers and APs per distribution rack is the Aruba CX 6200. This switch series is a cloud-manageable, stackable access switch series that is ideal for enterprise branch offices and campus networks, as well as SMBs. The CX 6200 series offers the following benefits:

Enterprise-class connectivity: The CX 6200 series supports ACLs, robust QoS, and common protocols such as static and Access OSPF routing.

Power and speed for users and IoT: The CX 6200 series provides built-in 1/10GbE uplinks and 30W to

60W of Class 4 to Class 6 PoE for powering devices such as APs and cameras.

Scalable growth made simple: The CX 6200 series supports Aruba Virtual Switching Framework (VSF) that allows you to quickly grow your network to eight members in a single stack using high-performance built-in 10G SFP ports.

Management flexibility: The CX 6200 series supports a choice of management, including cloud-based and on-prem Central, CLI, switch Web GUI and programmability with AOS-CX operating system, and REST APIs.

The other options are not ideal because:

Aruba CX 6400: This switch series is a high-availability modular switch series that is ideal for versatile edge access to data center deployments. It offers more performance, scalability, and modularity than the CX 6200 series, but it is also more expensive and complex to deploy and manage. It may not be cost-effective for connecting 200-380 clients per distribution rack.

Aruba CX 6300: This switch series is a layer 3 stackable access and aggregation switch series that offers Smart Rate and High Power PoE. It offers more features and performance than the CX 6200 series, but it is also more expensive and may not be necessary for connecting 200-380 clients per distribution rack.

Aruba CX 6000: This switch series is a layer 2 access switch series that offers PoE. It offers less features and performance than the CX 6200 series, and it does not support VSF stacking or routing protocols. It may not be sufficient for connecting 200-380 clients

per distribution rack.

References: https://www.arubanetworks.com/products/switches/access/

https://www.arubanetworks.com/products/switches/access/6200-series/

https://www.arubanetworks.com/products/switches/access/6400-series/

https://www.arubanetworks.com/products/switches/access/6300-series/

https://www.arubanetworks.com/products/switches/access/6000-series/

QUESTION 24

What are the main characteristics of the 6 GHz band?
* Less RF signal is absorb by objects in a 6 GHz WLAN.
* In North America, the 6 GHz band offers more 80 MHz channels than there are 40 MHz channels in the

5 GHz band.
* The 6 GHz band is fully backward compatible with the existing bands.
* Low Power Devices are allowed for indoor and outdoor usage.

Explanation

The main characteristic of the 6 GHz band that is true among the given options is that in North America, the 6 GHz band offers more 80 MHz channels than there are 40 MHz channels in the 5 GHz band. This characteristic provides more spectrum availability, less interference, and higher throughput for wireless devices that support Wi-Fi 6E Wi-Fi Enhanced (Wi-Fi 6E) is an extension of Wi-Fi 6 (802.11ax) standard that operates in the newly available unlicensed frequency spectrum around 6 GHz in addition to existing bands below it. Some facts about this characteristic are:

In North America, there are up to seven non-overlapping channels available in each of three channel widths (20 MHz, 40 MHz, and 80 MHz) in the entire unlicensed portion of the new spectrum (5925-7125 MHz). This means there are up to 21 non-overlapping channels available for Wi-Fi devices in total.

In comparison, in North America, there are only nine non-overlapping channels available in each of two channel widths (20 MHz and 40 MHz) in the entire unlicensed portion of the existing spectrum below it (2400-2483 MHz and 5150-5825 MHz). This means there are only up to nine non-overlapping channels available for Wi-Fi devices in total.

Therefore, in North America, there are more than twice as many non-overlapping channels available in each channel width in the new spectrum than in the existing spectrum below it.

Specifically, there are more than twice as many non-overlapping channels available at 80 MHz width (seven) than at 40 MHz width (three) in the existing spectrum below it.

The other options are not true because:

Less RF signal is absorbed by objects in a 6 GHz WLAN: This option is false because higher frequency signals tend to be more absorbed by objects than lower frequency signals due to higher attenuation Attenuation is a general term that refers to any reduction in signal strength during transmission over distance or through an object or medium . Therefore, RF signals in a 6 GHz WLAN would be more absorbed by objects than RF signals in a lower frequency WLAN.

The 6 GHz band is fully backward compatible with existing bands: This option is false because Wi-Fi devices need to support Wi-Fi 6E standard to operate in the new spectrum around 6 GHz . Existing Wi-Fi devices that do not support Wi-Fi 6Estandard cannot use this spectrum and can only operate in existing bands below it.

Low Power Devices are allowed for indoor and outdoor usage: This option is false because Low Power Indoor Devices (LPI) are only allowed for indoor usage under certain power limits and registration requirements . Outdoor usage of LPI devices is prohibited by regulatory authorities such as FCC Federal Communications Commission (FCC) is an independent agency of United States government that regulates communications by radio, television, wire, satellite, and cable across United States . However, outdoor usage of Very Low Power Devices (VLP) may be allowed under certain power limits and without registration requirements.

References: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e

https://www.wi-fi.org/file/wi-fi-alliance-spectrum-needs-study

https://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert-wi-fi/prod_white_paper0900aecd80

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-power-levels.html

https://www.wi-fi.org/file/wi-fi-alliance-unlicensed-spectrum-in-the-us

QUESTION 25

The customer has a requirement to create authorization policies for their users with Windows 10 clients, with a requirement Tor authorizing both device and user credentials within one Radius session.

What would be the correct solution for the requirement?
* ClearPass 6.9 with EAP-TTLS
* ClearPass 6.9 with EAP-TLS
* ClearPass 6.9 with PEAP
* ClearPass 6.9 with EAP-TEAP

Explanation

EAP-TEAP is a tunnel-based authentication method that supports both device and user authentication within a single RADIUS session. ClearPass 6.9 supports EAP-TEAP as anauthentication method for Windows 10 clients. References:

https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content/CPPM_UserGuide/EAP-TEAP/EAP-TE

QUESTION 26

Please match the use case to the appropriate authentication technology

Explanation

Add certificates to Android devices with the Aruba Onboard Application in the Google Play store that will be used for wireless authentication A) ClearPass Policy Manager Authenticate users on corporate-owned Chromebook devices using 802.1X and context gathered from the network devices that they log into B) Cloud Authentication and Policy Leverage unbound Mum Pre-Shared Keys (MPSK) managed by Aruoa Central to the end-users and client devices B) Cloud Authentication and Policy Validate devices exist in a Mobile Device Management (MDM) database before authenticating BYOD users with corporate Active Directory using certificates A) ClearPass Policy Manager

https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPPM_UserGuide/About%20

https://www.arubanetworks.com/products/security/network-access-control/

QUESTION 27

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
* 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
* 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
* 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
* 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

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-AE7

QUESTION 28

When would you bond multiple 20MHz wide 802.11 channels?
* To decrease the Signal to Noise Ratio (SNR)
* To increase throughput between the client and AP
* To provision highly available AP groups
* To utilize high gain omni-directional antennas

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.
References:https://ieeexplore.ieee.org/document/9288995

QUESTION 29

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?
* Disable and enable activate to trigger provisioning refresh
* Verify the AP can ping the device on arubanetworks.com
* Verify the AP has a license assigned
* Disable and enable Aruba Central to trigger configuration refresh

Explanation

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

QUESTION 30

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?
* The IP address associated with the loopback interface is non-routable and prevents loops
* The loopback interface state is dependent on the management interface state and reduces routing updates.
* The IP address associated with the loopback interface is routable and prevents loops
* The loopback interface state Is independent of any physical interface and reduces routing updates.

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 31

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

* The same subnet as the mobility controller
* The same subnet as the Aruba ESP gateway
* The same subnet as the mobility conductor

* The same subnet as the access point

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/instant-ug/iap-dhcp/iap-dhc

QUESTION 32

What is the recommended VSF topology? (Select two.)

* Star
* Daisy chain plus MAD
* Full mesh
* Full mesh plus MAD
* Ring

Explanation

Only: Daisy chain plus MAD and ring are the recommended VSF topologies for Aruba switches. They provide high availability and redundancy for the VSF stack. MAD (Multiple Active Detection) is a mechanism to detect and resolve split-brain scenarios in a VSF stack.

References:https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790/GUID-D6EF042E-EEE

QUESTION 33

You are in a meeting with a customer where you are asked to explain the network redundancy feature Multiple Spanning Tree (MSTP). What is the correct statement for this feature?

* MSTP configuration ID revision by default as current MSTP root priority
* MSTP configuration ID name by default using switch IMC address
* MSTP configuration ID name by default using switch serial number
* MSTP configuration ID revision by default as switch serial number

Explanation

MSTP Multiple Spanning Tree Protocol. MSTP is an IEEE standard protocol for preventing loops in a network with multiple VLANs. MSTP allows multiple VLANs to be mapped to a reduced number of spanning-tree instances. configuration ID consists of two parameters: name and revision. The name is a

32-byte ASCII string that identifies the MSTP region, which is a group of switches that share the same configuration ID and VLAN-to-instance mapping. The revision is a 16-bit number that indicates the version of the configuration ID. By default, the MSTP configuration ID name is set to the switch IMC address, which is a unique identifier derived from the MAC address Media Access Control address. MAC address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. of the switch.

References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/mstp/

QUESTION 34

You are configuring a network with a stacked pair of 6300M switches used for distribution and layer 3 services. You create a new

VLAN for users that will be used on multiple access stacks of CX6200 switches connected downstream of the distribution stack You will be creating multiple VLANs/subnets similar to this will be utilized in multiple access stacks What is the correct way to configure the routable interface for the subnet to be associated with this VLAN?

* Create a physically routed interface in the subnet on the 6300M stack for each downstream switch.
* Create an SVl in the subnet on each downstream switch
* Create an SVl in the subnet on the 6300M stack, and assign the management address of each downstream switch stack to a different IP address in the same subnet
* Create an SVl in the subnet on the 6300M stack.

Explanation

The correct way to configure the routable interface for the subnet to be associated with this VLAN is to create an SVI Switched Virtual Interface (SVI) Switched Virtual Interface (SVI) is a virtual interface on a switch that represents a VLAN and provides Layer 3 routing functions for that VLAN . SVIs are used to enable inter-VLAN routing , provide gateway addresses for hosts in VLANs , apply ACLs or QoS policies to VLANs

, etc . SVIs have some advantages over physical routed interfaces such as saving interface ports , reducing cable costs , simplifying network design , etc . SVIs are usually numbered according to their VLAN IDs (e.g., vlan 10) and assigned IP addresses within the subnet of their VLANs . SVIs can be created and configured by using commands such as interface vlan , ip address , no shutdown , etc . SVIs can be verified by using commands such as show ip interface brief , show vlan , show ip route , etc . in the subnet on the 6300M stack.

An SVI is a virtual interface on a switch that represents a VLAN and provides Layer 3 routing functions for that VLAN. Creating an SVI in the subnet on the 6300M stack allows the switch to act as a gateway for the users in that VLAN and enable inter-VLAN routing between different subnets. Creating an SVI in the subnet on the 6300M stack also simplifies network design and management by reducing the number of physical interfaces and cables required for routing.

The other options are not correct ways to configure the routable interface for the subnet to be associated with this VLAN because:

Create a physically routed interface in the subnet on the 6300M stack for each downstream switch: This option is incorrect because creating a physically routedinterface in the subnet on the 6300M stack for each downstream switch would require using one physical port and cable per downstream switch, which would consume interface resources and increase cable costs. Creating a physically routed interface in the subnet on the 6300M stack for each downstream switch would also complicate network design and management by requiring separate routing configurations and policies for each interface.

Create an SVl in the subnet on each downstream switch: This option is incorrect because creating an SVI in the subnet on each downstream switch would not enable inter-VLAN routing between different subnets, as each downstream switch would act as a gateway for its own VLAN only. Creating an SVI in the subnet on each downstream switch would also create duplicate IP addresses in the same subnet, which would cause IP conflicts and routing errors.

Create an SVl in the subnet on the 6300M stack, and assign the management address of each downstream switch stack to a different IP address in the same subnet: This option is incorrect because creating an SVI in the subnet on the 6300M stack, and assigning the management address of each downstream switch stack to a different IP address in the same subnet would not enable inter-VLAN routing between different subnets, as each downstream switch would still act as a gateway for its own VLAN only. Creating an SVI in the subnet on the 6300M stack, and assigning the management address of each downstream switch stack to a different IP address in the same subnet would also create unnecessary IP addresses in the same subnet, which would waste IP space and complicate network management.

References: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/index.html

https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-ove

https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-con

2023 Valid HPE6-A85 test answers & HP Exam PDF: https://www.validexam.com/HPE6-A85-latest-dumps.html]