HP

Exam Questions HPE6-A85

Aruba Certified Campus Access Associate Exam

NEW QUESTION 1
A network technician has successfully connected to the employee SSID via 802 1X Which RADIUS message should you look for to ensure a successful connection?

A. Authorized
B. Access-Accept
C. Success
D. Authenticated

Answer: B

Explanation:
The RADIUS message that you should look for to ensure a successful connection via 802.1X is Access-Accept. This message indicates that the RADIUS server has authenticated and authorized the supplicant (the device that wants to access thenetwork) and has granted it access to the network resources. The Access-Accept message may also contain additional attributes such as VLAN ID, session timeout, or filter ID that specify how the authenticator (the device that controls access to the network, such as a switch) should treat the supplicant??s traffic.
The other options are not RADIUS messages because:
? Authorized: This is not a RADIUS message, but a state that indicates that a port on an authenticator is allowed to pass traffic from a supplicant after successful authentication and authorization.
? Success: This is not a RADIUS message, but a status that indicates that an 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). exchange has completed successfully between a supplicant and an authentication server.
? Authenticated: This is not a RADIUS message, but a state that indicates that a port on an authenticator has received an EAP-Success message from an authentication server after successful authentication of a supplicant.
References: https://en.wikipedia.org/wiki/RADIUS#Access-Accept https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html https://en.wikipedia.org/wiki/IEEE_802.1X#Port- based_network_access_control
https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_exchange

NEW QUESTION 2
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

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

NEW QUESTION 3
Two independent ArubaOS-CX 6300 switches with Spanning Tree (STP) settings are interconnected with two cables between ports 1/1/1 and 1/1/2 All four ports have "no
shutdown" and "no routing" commands
How will STP forward or discard traffic on these ports?

A. The switch with the lower MAC address will forward on both ports, while the switch with the higher MAC address will forward on both ports
B. The switch with the lower MAC address will forward on both ports, while the switch with the higher MAC address will discard on one port
C. The switch with the lower MAC address will discard on one port, while the switch with the higher MAC address will forward on both ports
D. The switch with the lower MAC address will discard on one port, while the switch with the higher MAC address will discard on one port

Answer: D

Explanation:

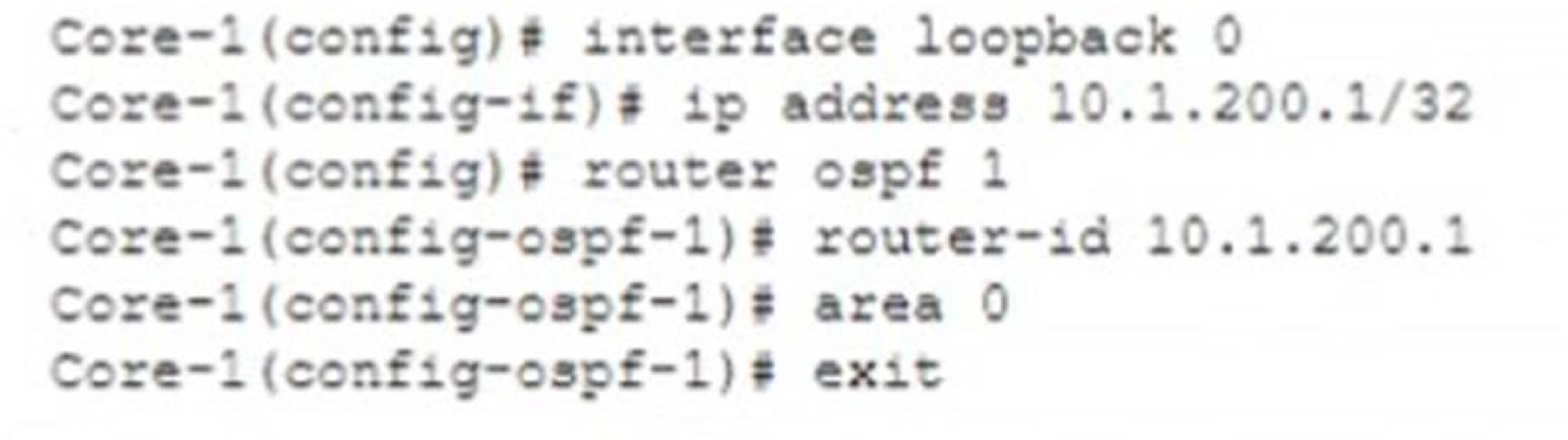
The way that STP Spanning Tree Protocol. STP is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network by preventing redundant paths between switches or bridges from creating loops that cause broadcast storms, multiple frame transmission, and MAC table instability. STP creates a logical tree structure that spans all of the switches in an extended network and blocks any redundant links that are not part of the tree from forwarding data packets3. will forward or discard traffic on these ports is as follows:
? STP will elect a root bridge among the two switches based on their bridge IDs,
which are composed of a priority value and a MAC address. The switch with the lower bridge ID will become the root bridge and will forward traffic on all its ports.
? STP will assign a role and a state to each port on both switches based on their
port IDs, which are composed of a priority value and a port number. The port with the lower port ID will become the designated port and will forward traffic, while the port with the higher port ID will become the alternate port and will discard traffic.
? In this scenario, since both switches have two cables connected between ports 1/1/1 and 1/1/2, there will be two possible paths between them, creating a loop. To prevent this loop, STP will block one of these paths by discarding traffic on one of the ports on each switch.
? Assuming that both switches have the same priority value (default is 32768), the switch with the lower MAC address will have the lower bridge ID and will become the root bridge. The root bridge will forward traffic on both ports 1/1/1 and 1/1/2.
? Assuming that both ports have the same priority value (default is 128), port 1/1/1
will have a lower port ID than port 1/1/2 on both switches because it has a lower port number. Port 1/1/1 will become the designated port and will forward traffic, while port 1/1/2 will become the alternate port and will discard traffic.
? Therefore, the switch with the lower MAC address will discard traffic on one port
(port 1/1/2), while the switch with the higher MAC address will also discard traffic on one port (port 1/1/2).
References: 3 https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

NEW QUESTION 4
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

Answer: B

NEW 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 preventsloops
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.

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

NEW QUESTION 6
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)

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:
1 https://blogs.arubanetworks.com/solutions/simplify-iot-authentication-with-multiple-pre-shared-keys/ 2
https://www.arubanetworks.com/techdocs/ClearPass/6.8/Guest/Content/AdministrationTasks1/Configuring-MPSK.htm

NEW QUESTION 7
What does a slow amber-flashing Stack-LED indicate?

A. One switch has a stacking failure.
B. A port has a stacking failure Stacking mode Is not selected
C. Stacking mode selected
D. Stacking is synchronizing Please wait

Answer: C

Explanation:
A slow amber-flashing Stack-LED indicates that stacking mode is selected on the switch. This means that the switch is ready to join a stack or form a new stack if no other switches are present. References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/1-overview/stacking-leds.htm

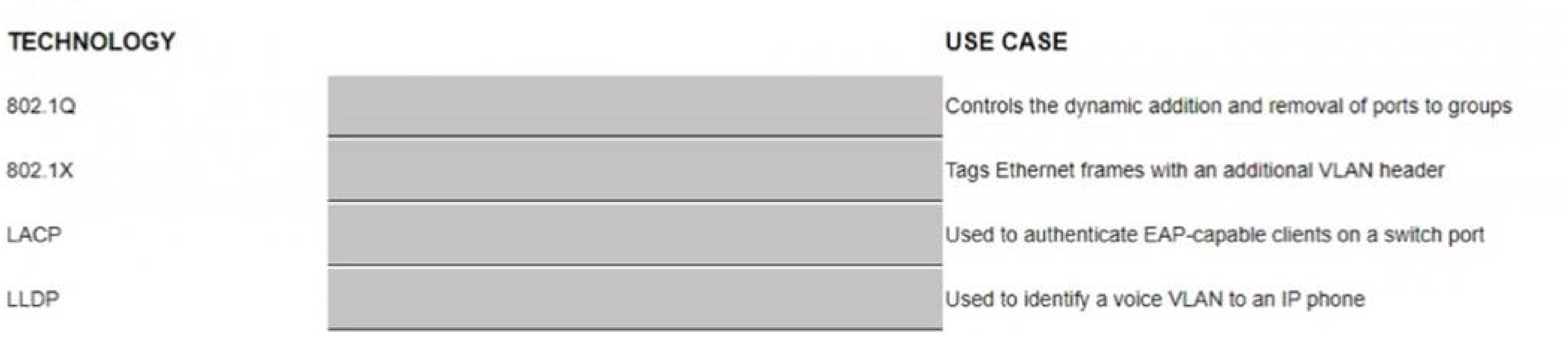
NEW QUESTION 8
When using the OSPF dynamic routing protocol on an Aruba CX switch, what must match on the neighboring devices to exchange routes?

A. Hello timers
B. DR configuration
C. ECMP method
D. BDR configuration

Answer: A

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/ar ubaos-solutions/osfp/osfp.htm

NEW QUESTION 9
DRAG DROP
Match the switching technology with the appropriate use case.



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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
USE CASE: a) Controls the dynamic addition and removal of ports to groups
Technology: 3) LACP
USE CASE: b) Tags Ethernet frames with an additional VLAN header Technology: 1) 802.1Q
USE CASE: c) Used to authenticate EAP-Capable client on a switch port Technology: 2) 802.1X
USE CASE: d) Used to identify a voice VLAN to an IP phone Technology: 4) LLDP The following table summarizes the switching technologies and their use cases:
Technology
Use case
1) 802.1Q
* 802.1Q is a standard that defines how to create and manage virtual LANs (VLANs) on a network. VLANs allow network administrators to logically segment a network into different broadcast domains, improving security, performance, and manageability. 802.1Q tags Ethernet frames with an additional VLAN header that contains a VLAN identifier (VID), which indicates which VLAN the frame belongs to1.
2) 802.1X
* 802.1X is a standard that defines how to provide port-based network access control (PNAC) on a network. PNAC allows network administrators to authenticate and authorize devices before granting them access to network resources. 802.1X uses the Extensible Authentication Protocol (EAP) to exchange authentication messages between a supplicant (a device that wants to access the network), an authenticator (a device that controls access to the network, such as a switch), and an authentication server (a device that verifies the credentials of the supplicant, such as a RADIUS server)2.
3) LACP
LACP stands for Link Aggregation Control Protocol, which is part of the IEEE 802.3ad standard that defines how to bundle multiple physical links into a single logical link, also known as a link aggregation group (LAG) or an EtherChannel. LAGs provide increased bandwidth, load balancing, and redundancy for network connections. LACP controls the dynamic addition and removal of ports to groups, ensuring that only ports with compatible configurations can form a LAG3.
4) LLDP
LLDP stands for Link Layer Discovery Protocol, which is part of the IEEE 802.1AB standard that defines how to discover and advertise information about neighboring devices on a network. LLDP operates at Layer 2 of the OSI model and uses TLVs (type-length-value) to exchange information such as device name, port number, VLAN ID, capabilities, and power requirements. LLDP can be used to identify a voice VLAN to an IP phone by sending a TLV that contains the voice VLAN ID and priority.
References: 1 https://en.wikipedia.org/wiki/IEEE_802.1Q2 https://en.wikipedia.org/wiki/IEEE_802.1X3 https://en.wikipedia.org/wiki/Link_aggregation https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

NEW QUESTION 10
What are the main characteristics of the 6 GHz band?

A. Less RF signal is absorb by objects in a 6 GHz WLAN.
B. In North America, the 6 GHz band offers more 80 MHz channels than there are 40 MHz channels in the 5 GHz band.
C. The 6 GHz band is fully backward compatible with the existing bands.
D. Low Power Devices are allowed for indoor and outdoor usage.

Answer: B

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_paper0900aecd807395a9.html
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

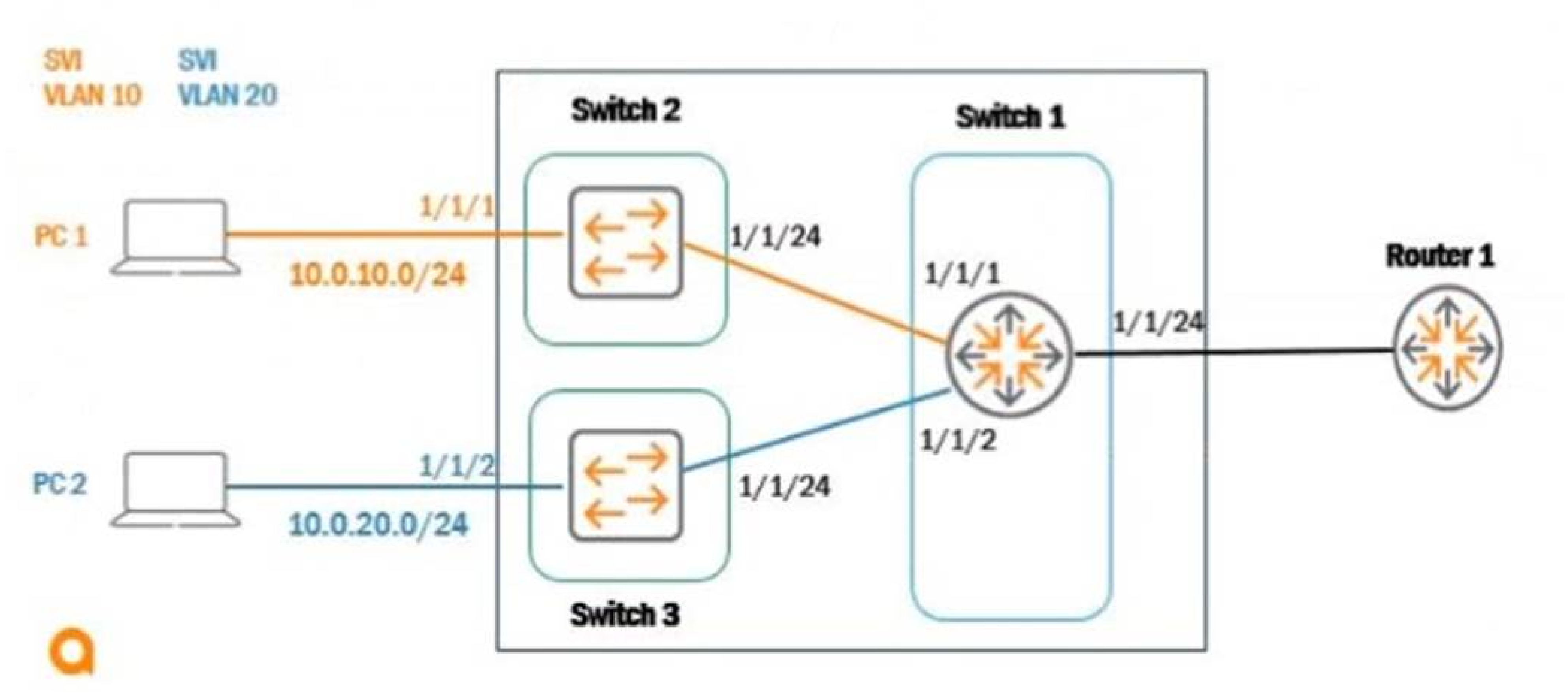
NEW QUESTION 10
When measuring signal strength, dBm is commonly used and 0 dBm corresponds to 1 mW power.
What does -20 dBm correspond to?

A. .-1 mW
B. .01 mw
C. 10 mW
D. 1mW

Answer: B

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

NEW QUESTION 11
Based on the given topology, what is the requirement on an Aruba switch to enable LLDP messages to be received by Switch 1 port 1/1/24. when Router 1 is enabled with LLDP?



A. LLDP is enabled by default
B. global configuration lldp enable
C. int 1/1/24, lldp receive

D. int 1/1/24, no cdp

Answer: C

Explanation:
LLDP Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network. is enabled by default on Aruba switches, but it can be disabled on a per-port basis using the no lldp command. To enable LLDP messages to be received by Switch 1 port 1/1/24, you need to enter the interface configuration mode for that port and use the lldp receive command.
References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/lldp/lldp.htm

NEW QUESTION 14
When would you bond multiple 20MHz wide 802.11 channels?

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

Answer: B

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

NEW QUESTION 17
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

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

NEW QUESTION 22
......