HP.HPE6-A85.v2023-07-31.q28

Exam Code:	HPE6-A85
Exam Name:	Aruba Campus Access Associate Exam
Certification Provider:	HP
Free Question Number:	28
Version:	v2023-07-31
# of views:	548
# of Questions views:	280
https://www.freepdfdumps.com/HP.HPE6-A85.v2023-07-31.q28.html	

NEW QUESTION: 1
Which feature can network administrators use to centralized RF planning and optimization service when using an Aruba mobility master architecture?
A. Airwave
B. Client Match
C. AirMatch
D. Client Wave
Answer: C (LEAVE A REPLY)
Explanation
AirMatch is a feature that provides centralized RF planning and optimization service for Aruba wireless networks. It uses cloud-based algorithms and machine learning to optimize the RF performance and user experience. References:https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdf

NEW QUESTION: 2
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 (LEAVE A REPLY)
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/ 2 https://www.arubanetworks.com/techdocs/ClearPass/6.8/Guest/Content/AdministrationTasks1/Configuring-MPS

NEW QUESTION: 3
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 (LEAVE A REPLY)
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/arubaos-solutions/1-ove

NEW QUESTION: 4
Match the switching technology with the appropriate use case.

Answer:
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)
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_802.1Q 2 https://en.wikipedia.org/wiki/IEEE_802.1X 3 https://en.wikipedia.org/wiki/Link_aggregation
https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

NEW QUESTION: 5
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
Answer: (SHOW ANSWER)
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

NEW QUESTION: 6
What is the ideal Aruba access switch for a cost-effective connection to 200-380 clients, printers and APs per distribution rack?
A. Aruba CX 6400
B. Aruba CX 6200
C. Aruba CX 6300
D. Aruba CX 6000
Answer: B (LEAVE A REPLY)
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/

NEW QUESTION: 7
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 (LEAVE A REPLY)
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/13838-1
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: 8
You put in a few show commands on switches EDGE1 and CORE1 to attempt to gather information to troubleshoot the issue Use the show command output images to determine the reason for the EDGE1 uplink being down
A. The physical interfaces are not members of the correct LAG.
B. Spanning-Tree block state is preventing the Core uplink from having connectivity to the edge
C. The Core is connected to the incorrect physical interlaces

D. LACP is not configured on the Core uplink

Answer: D (LEAVE A REPLY)

Explanation

LACP is a protocol that allows multiple physical links to be aggregated into a single logical link for increased bandwidth and redundancy. LACP must be configured on both ends of the link for it to work properly. In this case, EDGE1 has LACP configured on its uplink port-channel 1, but CORE1 does not have LACP configured on its corresponding port-channel 1. This causes a mismatch and prevents the link from coming up.

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

NEW QUESTION: 9

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

A. Rate limiting

B. DWRR queuing

C. QoS shaping

D. Strict queuing

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 10
Which flew in a Layer 3 IPv4 packet header is used to mitigate Layer 3 route loops?
A. Checksum
B. Time To Live
C. Protocol
D. Destination IP
Answer: B (LEAVE A REPLY)
Explanation
The field in a Layer 3 IPv4 packet header that is used to mitigate Layer 3 route loops is Time To Live (TTL). TTL is an 8-bit field that indicates the maximum number of hops that a packet can traverse before being discarded. TTL is set by the source device and decremented by one by each router that forwards the packet. If TTL reaches zero, the packet is dropped and an ICMP Internet Control Message Protocol (ICMP) Internet Control Message Protocol (ICMP) is a network protocol that provides error reporting and diagnostic functions for IP networks. ICMP is used to send messages such as echo requests and replies (ping), destination unreachable, time exceeded, parameter problem, source quench, redirect, etc. ICMP messages are encapsulated in IP datagrams and have a specific format that contains fields such as type, code, checksum, identifier, sequence number, data, etc. ICMP messages can be verified by using commands such as ping , traceroute , debug ip icmp , etc . message is sent back to the source device. TTL is used to mitigate Layer 3 route loops because it prevents packets from circulating indefinitely in a looped network topology. TTL also helps to conserve network resources and avoid congestion caused by looped packets.
The other options are not fields in a Layer 3 IPv4 packet header because:
Checksum: Checksum is a 16-bit field that is used to verify the integrity of the IP header. Checksum is calculated by the source device and verified by the destination device based on the values of all fields in the IP header. Checksum does not mitigate Layer 3 route loops because it does not limit the number of hops that a packet can traverse.
Protocol: Protocol is an 8-bit field that indicates the type of payload carried by the IP datagram. Protocol identifies the upper-layer protocol that uses IP for data transmission, such as TCP Transmission Control Protocol (TCP) Transmission Control Protocol (TCP) is a connection-oriented transport layer protocol that provides reliable, ordered, and error-checked delivery of data between applications on different devices . TCP uses a three-way handshake to establish a connection between two endpoints , and uses sequence numbers , acknowledgments , and windowing to ensure data delivery and flow control . TCP also uses mechanisms such as retransmission , congestion avoidance , and fast recovery to handle packet loss and congestion . TCP segments data into smaller units called segments , which are encapsulated in IP datagrams and have a specific

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

NEW QUESTION: 11
What is indicated by a solid amber radio status LED on an Aruba AP?
A. Not enough PoE is provided from the switch to power both radios of the AP
B. The radio is working in mesh mode
C. The radio is working the 5 GHz band only.
D. The radio is enabled in monitor or spectrum analysis mode
Answer: (SHOW ANSWER)
Explanation
The solid amber radio status LED on an Aruba AP Access Point (AP) Access Point (AP) is a device that connects wireless devices to a wired network using Wi-Fi or other wireless standards . APs act as transmitters and receivers of wireless signals and provide wireless coverage for a specific area . APs can operate in different modes such as root , repeater , bridge , mesh , etc . APs can also support different features such as security , QoS , roaming , load balancing , etc . APs can be standalone devices or managed by controllers or cloud services . APs can be verified by using commands such as show ap active , show ap database , show ap bss-table , etc . indicates that the radio is enabled in monitor or spectrum analysis mode. Monitor mode is a mode that allows the AP to scan all channels and collect information about wireless traffic, interference, rogue devices, etc. Spectrum analysis mode is a mode that allows the AP to scan all channels and collect information about RF Radio Frequency (RF) Radio Frequency (RF) is a term that refers to electromagnetic waves that have frequencies between 3 kHz and 300 GHz . RF waves are used for various purposes such as communication , broadcasting , radar , navigation , remote control , etc . RF waves can be modulated by changing their amplitude , frequency , or phase to encode information . RF waves can also be affected by various factors such as attenuation , reflection , refraction , diffraction , scattering , interference , noise , etc . RF waves can be measured by using devices such as spectrum analyzers , power meters , antennas , etc . environment, noise sources, channel utilization, etc. Both modes are useful for troubleshooting and optimizing wireless performance, but they disable normal data transmission and reception on the radio.
The other options are not indicated by a solid amber radio status LED on an Aruba AP because:
Not enough PoE is provided from the switch to power both radios of the AP: This option is false because not enough PoE Power over Ethernet (PoE) Power over Ethernet (PoE) is a technology that allows network devices to receive power and data over the same Ethernet cable . PoE eliminates the need for separate power sources and cables for devices such as IP phones , cameras , access points , etc .
PoE is defined in IEEE 802.3af and IEEE 802.3at standards and supports different power classes and modes . PoE can be provided by switches or injectors that act as power sourcing equipment (PSE) and received by devices that act as powered devices (PD) . PoE can be verified by using commands suchas show power inline , show power-over-ethernet , debug ip device tracking , etc . is indicated by a blinking amber power status LED on an Aruba AP, not by a solid amber radio status LED. A blinking amber power status LED means that the AP

is receiving insufficient power from the switch or injector and cannot operate normally. A solid green power status LED means that the AP is receiving sufficient power from the switch or injector and can operate normally.
The radio is working in mesh mode: This option is false because the radio working in mesh mode is indicated by a solid green radio status LED on an Aruba AP, not by a solid amber radio status LED. A solid green radio status LED means that the radio is working in normal mode or mesh mode and can transmit or receive data on the assigned channel. Mesh mode is a mode that allows the AP to connect wirelessly to other APs and form a mesh network without requiring wired connections.
The radio is working the 5 GHz band only: This option is false because the radio working in the 5 GHz band only is indicated by a solid blue radio status LED on an Aruba AP, not by a solid amber radio status LED. A solid blue radio status LED means that the radio is working in dual-band mode and can transmit or receive data on both 2.4 GHz and 5 GHz bands.
References:
https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/ap-led-behavior.htm
https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/troubleshooting/ap-monitor-m
https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/troubleshooting/ap-spectrum

NEW QUESTION: 12
Which statement is correct when comparing 5 GHz and 6 GHz channels with identical channel widths?
A. 5 GHz channels travel the same distances and provide different throughputs to clients compared to 6 GHz channels
B. 5 GHz channels travel different distances and provide different throughputs to clients compared to 6 GHz channels
C. 5 GHz channels travel the same distances and provide the same throughputs to clients compared to 6 GHz channels
D. 5 GHz channels travel different distances and provide the same throughputs to clients compared to 6 GHz channels
Answer: (SHOW ANSWER)
Explanation
The correct statement when comparing 5 GHz and 6 GHz channels with identical channel widths is that 5 GHz channels travel different distances and provide different throughputs to clients compared to 6 GHz channels. This statement reflects the fact that higher frequency signals tend to have 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 . Higher attenuation means that higher frequency signals have shorter range and lower throughput than lower frequency signals. Some facts about this statement are:
5 GHz channels have lower frequency than 6 GHz channels, which means they have lower attenuation than 6 GHz channels.
Lower attenuation means that 5 GHz channels can travel longer distances and provide higher throughputs to clients than 6 GHz channels with identical channel widths.
However, the difference in distance and throughput between 5 GHz and 6 GHz channels may not be significant in indoor environments where there are many obstacles and reflections that affect signal propagation.

The advantage of using 6 GHz channels over 5 GHz channels is that they offer more spectrum availability, less interference, and more non-overlapping channels than 5 GHz channels.
The other options are not correct because:
5 GHz channels travel the same distances and provide different throughputs to clients compared to 6 GHz channels: This option is false because 5 GHz channels do not travel the same distances as 6 GHz channels due to higher attenuation of higher frequency signals.
5 GHz channels travel the same distances and provide the same throughputs to clients compared to 6 GHz channels: This option is false because 5 GHz channels do not travel the same distances or provide the same throughputs as 6 GHz channels due to higher attenuation of higher frequency signals.
5 GHz channels travel different distances and provide the same throughputs to clients compared to 6 GHz channels: This option is false because 5 GHz channels do not provide the same throughputs as
6 GHz channels due to higher attenuation of higher frequency signals.
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/support/docs/wireless-mobility/wireless-lan-wlan/82068-power-levels.html
https://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert-wi-fi/prod_white_paper0900aecd80

NEW QUESTION: 13
Match the appropriate QoS concept with its definition.
Answer:
Explanation
QoS Quality of Service (QoS) 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 can improve network performance, reduce latency, increase throughput, and prevent congestion. concept and its definition. Here is my answer:
QoS Concept:
Best Effort Service
Class of Service
Differentiated Services
WMM ========== Definition:
d) A method where traffic is treated equally in a first-come, first-served manner a) A method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes b) A method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes c) A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard Short But Comprehensive Explanation of Correct Answer Only: The correct match between QoS concept and its definition is as follows:
Best Effort Service: This is a method where traffic is treated equally in a first-come, first-served manner without any prioritization or differentiation. This is the default service level for most networks and applications that do not have specific QoS requirements or guarantees. Best Effort Service does not provide any assurance of bandwidth, delay, jitter, or packet loss.
Class of Service: This is a method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes (0 to 7). These service classes are also known as IEEE

802.1p priority values or PCP Priority Code Point (PCP) is a 3-bit field in the 802.1Q VLAN tag that indicates the priority level of an Ethernet frame . Class of Service allows network devices to identify and handle different types of traffic based on their priority levels. Class of Service is typically used in LAN Local Area Network (LAN) is a network that connects devices within a limited geographic area, such as a home, office, or building environments where Layer 2 switching is predominant.
Differentiated Services: This is a method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes (0 to 63). These service classes are also known as DiffServ Code Points (DSCP) DiffServ Code Point (DSCP) is a 6-bit field in the IP header that indicates the service class of a packet . Differentiated Services allows network devices to identify and handle different types of traffic based on their service classes. Differentiated Services is typically used in WAN Wide Area Network (WAN) is a network that connects devices across a large geographic area, such as a country or continent environments where Layer 3 routing is predominant.
WMM: This is a method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard. WMM stands for Wi-Fi Multimedia and it is a certification program developed by the Wi-Fi Alliance to enhance QoS for wireless networks. WMM defines four access categories (AC): Voice, Video, Best Effort, and Background. These access categories correspond to different priority levels and contention parameters for wireless traffic. WMM allows wireless devices to identify and handle different types of traffic based on their access categories.
References: https://en.wikipedia.org/wiki/Quality_of_service
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_dfsrv/configuration/xe-16/qos-dfsrv-xe-16-book/qos-dfsr
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/81831-qos-wlan.html
https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm

NEW QUESTION: 14
A network administrator with existing IAP-315 access points is interested in Aruba Central and needs to know which license is required for specific features Please match the required license per feature (Matches may be used more than once.)
Answer:
Explanation
a) Alerts on config changes via email - Foundation b) Group-based firmware compliance - Foundation c) Heat maps of deployed APs - Advanced d) Live upgrades of an AOS10 cluster - Advanced According to the Aruba Central Licensing Guide1, the Foundation License provides basic device management features such as configuration, monitoring, alerts, reports, firmware management, etc. The Advanced License provides additional features such as AI insights, WLAN services, NetConductor Fabric, heat maps, live upgrades, etc.
https://www.arubanetworks.com/techdocs/central/2.5.3/content/pdfs/licensing-guide.pdf

NEW QUESTION: 15
When using Aruba Central what can identify recommended steps to resolve network health issues and allows you to share detailed information with support personnel?
A. Overview Dashboard
B. OAIOps

C. Alerts and Events
D. Audit Trail
Answer: B (LEAVE A REPLY)
Explanation
OAIOps is a feature of Aruba Central that uses artificial intelligence and machine learning to identify recommended steps to resolve network health issues and allows you to share detailed information with support personnel. OAIOps provides insights into network performance, root cause analysis, anomaly detection, proactive alerts, and automated remediation actions.OAIOps also integrates with Aruba User Experience Insight (UXI) sensors to measure and improve user experience across wired and wireless networks.
References:https://www.arubanetworks.com/assets/ds/DS_ArubaCentral.pdf

NEW QUESTION: 16
Which part of the WPA Key Hierarchy is used to encrypt and/or decrypt data"
A. Pairwise Temporal Key (PTK)
B. Pairwise Master Key (PMK)
C. Key Confirmation Key (KCK)
D. number used once (nonce)
Answer: A (LEAVE A REPLY)
Explanation
The part of WPA Key Hierarchy that is used to encrypt and/or decrypt data is Pairwise Temporal Key (PTK). PTK is a key that is derived from 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 , ANonce Authenticator Nonce (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 randomnumber 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 subkey that is specifically used for data encryption is TK Temporal Key (TK). TK is also known as Pairwise Transient Key (PTK). TK changes periodically during communication based on time or number of packets transmitted.
The other options are not part of WPA Key Hierarchy because:
PMK: PMK is not part of WPA Key Hierarchy, but rather an input for deriving PTK.
KCK: KCK is part of WPA Key Hierarchy, but it is not used for data encryption, but rather for message integrity check.
Nonce: Nonce is not part of WPA Key Hierarchy, but rather an input for deriving 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

NEW QUESTION: 17
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?
A. MSTP configuration ID revision by default as current MSTP root priority
B. MSTP configuration ID name by default using switch IMC address
C. MSTP configuration ID name by default using switch serial number
D. MSTP configuration ID revision by default as switch serial number
Answer: (SHOW ANSWER)
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/

NEW QUESTION: 18
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?
A. Create a physically routed interface in the subnet on the 6300M stack for each downstream switch.
B. Create an SVI in the subnet on each downstream switch
C. Create an SVI 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
D. Create an SVI in the subnet on the 6300M stack.

Answer: D (LEAVE A REPLY)

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 SVI 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 SVI 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

NEW QUESTION: 19
What can be done to dynamically set the PoE Priority on a switch port when deploying IP cameras APs. and other PoE devices?
A. Configure PoE power management to Dynamic Mode
B. Configure PoE power management to Class-based Mode
C. Enable Quick PoE on the switch modules
D. Enable profiling for device provisioning
Answer: D (LEAVE A REPLY)
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

NEW QUESTION: 20
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. 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
B. 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
C. 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
D. 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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 21

Which statement about manual switch provisioning with Aruba Central is correct?

A. Manual provisioning does not require DHCP and requires DNS

B. Manual provisioning does not require DHCP and does not require DNS

C. Manual provisioning requires DHCP and does not require DNS

D. Manual provisioning requires DHCP and requires DNS

Answer: B (LEAVE A REPLY)

Explanation

Manual provisioning is a method to add switches to Aruba Central without using DHCP or DNS. It requires the user to enter the switch serial number, MAC address, and activation code in Aruba Central, and then configure the switch with the same activation code and Aruba Central's IP address.

References:https://help.central.arubanetworks.com/latest/documentation/online_help/content/devices/switches/pr

NEW QUESTION: 22

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: (SHOW ANSWER)

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/arubaos-solutions/lldp/l

NEW QUESTION: 23

What can be done to dynamically set the PoE Priority on a switch port when deploying IP cameras APs. and other PoE devices?

A. Enable Quick PoE on the switch modules
B. Enable profiling for device provisioning
C. Configure PoE power management to Class-based Mode
D. Configure PoE power management to Dynamic Mode
Answer: B (LEAVE A REPLY)
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

NEW QUESTION: 24
Refer to the exhibit.
In the given topology, a pair of Aruba CX 8325 switches are in a VSX stack using the active gateway What is the nature and behavior of the Virtual IP for the VSX pair if clients are connected to the access switch using VSX as the default gateway?
A. Virtual IP is active on the primary VSX switch
Virtual floating IP will failover in case of a failure
B. Virtual IP is active on both CX switches
C. Virtual IP uses SVI IP address synced with VSX
Answer: A (LEAVE A REPLY)
Explanation
Virtual Switching Extension (VSX) is a feature that allows two Aruba CX switches to operate as a single logical device with a single control plane and data plane. VSX provides high availability, scalability, and simplified management for campus and data center networks3. In VSX, one switch is designated as the primary switch and the other as the secondary switch. The primary switch owns and responds to ARP Address Resolution Protocol. ARP is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite. requests for the virtual IP address of the VSX pair4. The virtual IP address is used as the default gateway for clients connected to the access switch. If the primary switch fails, the secondary switch takes over the virtual IP address and continues to forward traffic for the clients5.
References: 3
https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-overview.htm 4
https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-ip-addressing.htm 5
https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-failover.htm

NEW QUESTION: 25
Based on the "snow ip route" output on an AruDaCX 8400. what type of route is "10.1 20 0/24, vrf default via

10.1.12.2. [1/0]"?
A. local
B. static
C. OSPF
D. connected
Answer: (SHOW ANSWER)
Explanation
A static route is a route that is manually configured on a router or switch and does not change unless it is modified by an administrator. Static routes are used to specify how traffic should reach specific destinations that are not directly connected to the device or that are not reachable by dynamic routing protocols. In Aruba CX switches, static routes can be configured using the ip route command in global configuration mode. Based on the "show ip route" output on an Aruba CX 8400 switch, the route "10.1 20 0/24, vrf default via 10.1.12.2, [1/0]" is a static route because it has an administrative distance of 1 and a metric of 0, which are typical values for static routes. References: https://en.wikipedia.org/wiki/Static_routing https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.h

NEW QUESTION: 26
Which Protocol Data Unit (PDU) represents the data link layer PDU?
A. PDU1 - Signal
B. PDU2 - Frame
C. PDU3 - Packet
D. PDU4 - Segment
Answer: B (LEAVE A REPLY)
Explanation
A frame is the data link layer PDU that encapsulates the network layer PDU (packet) with a header and a trailer that contain information such as source and destination MAC addresses, frame type, error detection, etc.
A frame is transmitted over a physical medium such asEthernet, Wi-Fi, etc.
References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-ove

NEW QUESTION: 27
A network technician is troubleshooting one new AP at a branch office that will not receive Its configuration from Aruba Central The other APs at the branch are working as expected The output of the 'show ap debug cloud-server command' shows that the "cloud conflg received" Is FALSE.
After confirming the new AP has internet access, what would you check next?
A. Disable and enable activate to trigger provisioning refresh
B. Verify the AP can ping the device on arubanetworks.com
C. Verify the AP has a license assigned
D. Disable and enable Aruba Central to trigger configuration refresh
Answer: C (LEAVE A REPLY)
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

NEW QUESTION: 28
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 (LEAVE A REPLY)
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