ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

A network technician is using Aruba Central to troubleshoot network issues Which dashboard can be used to view and acknowledge issues when beginning the troubleshooting process?

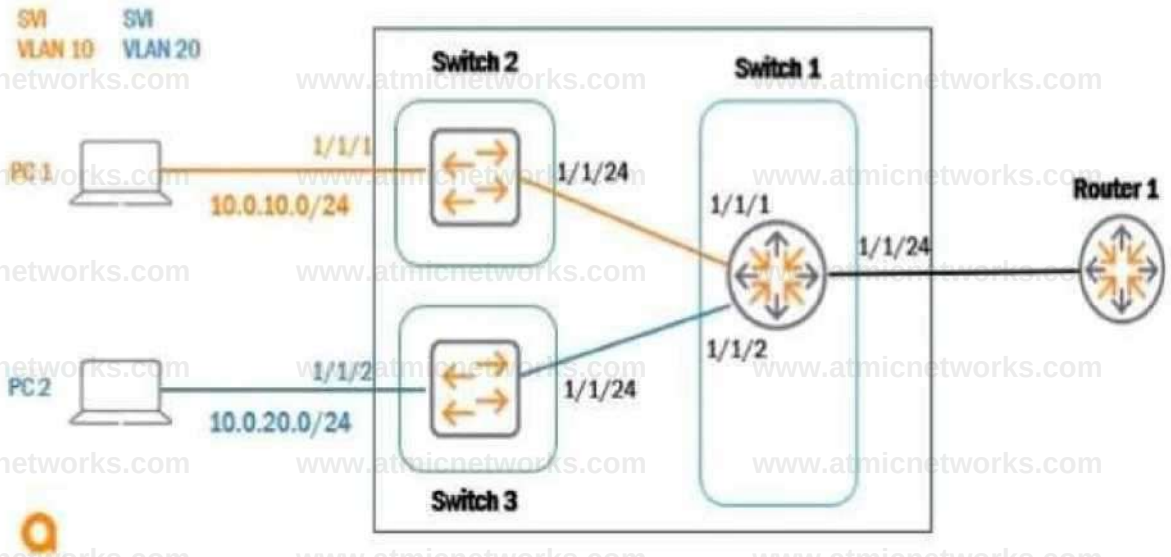
A. the Alerts and Events dashboard
B. the Audit Trail dashboard
C. the Reports dashboard
D. the Tools dashboard

Answer: A

Explanation:

The Alerts and Events dashboard displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. You can use the Config icon to configure alerts and notifications for different alert categories and severities1. You can also view the alerts and events in the List view and Summary view2. Reference: 1 https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/configuri ng-alerts.htm 2 https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/viewing- alerts.htm

Question: 2



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: A

Explanation:

On Aruba switches, the Link Layer Discovery Protocol (LLDP) is enabled by default on all ports. This protocol is an industry-standard network discovery protocol that is used for network devices to advertise their identity, capabilities, and neighbors on a locally managed network, typical in an IEEE 802 network. This is beneficial for network mapping and troubleshooting purposes. Since LLDP is enabled by default, there is no need for any additional configuration on Switch 1 port 1/1/24 to receive LLDP messages from Router 1, as long as LLDP is not disabled on the port.

Question: 3

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: B

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

Question: 4

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. Reference:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/osfp/osfp.htm

Question: 5

DRAG DROP
Match the phase of message processing with the Open Systems interconnection (OSI) layer.

Layer	Phase of Message Processing
Physical Layer	Organizes the data into segments
Network Layer	Organizes the data into packets
Transport Laver	Organizes the data into frames
Data Link Layer	Organizes the data into bits

Answer:

Layer: 1) Physical layer Phase of Message Processing: d) Organize the data into bits
Layer: 2) Data Link layer Phase of Message Processing: c) Organize the data into frames Layer: 3) Network layer Phase of Message Processing: b) Organize the data into packets Layer: 4) Transport layer Phase of Message Processing: a) Organize the data into segments The OSI model divides the networking process into seven layers, each representing a different step of the transmission chain. Each layer has its own function and is responsible for well-defined tasks. User data passes sequentially from the highest layer down through the lower layers until the device transmits it externally. The lowest layer, the physical layer, converts the data into bits that can be sent over a physical medium. The second layer, the data link layer, organizes the bits into frames that can be transmitted over a link between two nodes. The third layer, the network layer, organizes the frames into packets that can be routed across a network of nodes. The fourth layer, the transport layer, organizes the packets into segments that can provide reliable and error-free communication between two end points12. Reference: 1 https://www.linode.com/docs/guides/introduction-to-osi- networking-model/ 2 https://en.wikipedia.org/wiki/OSI_model

Question: 6

What happens when the signal from an AP weakens by being absorbed as it moves through an object?

A. APs will use bonded channels to decrease latency to clients
B. Signal to Noise Ratio (SNR) increases
C. Signal to Noise Ratio (SNR) decreases
D. Aruba Central dynamically moves clients to neighboring APs

Answer: C

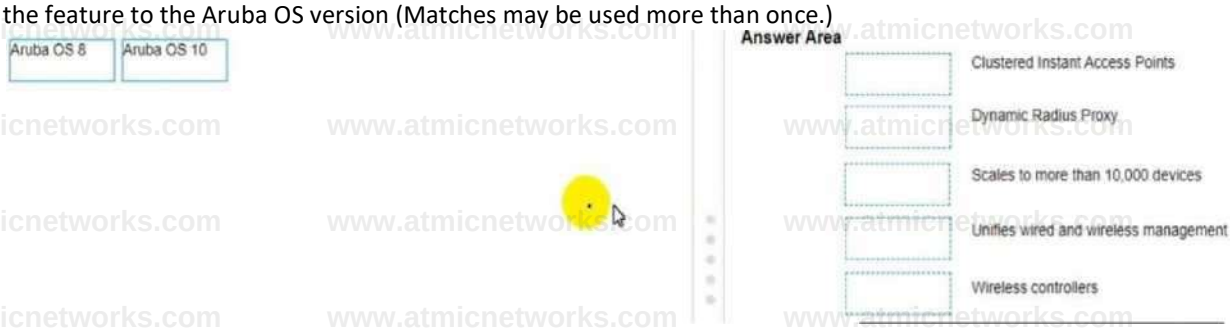
Explanation:

Signal to noise ratio (SNR) is a measure that compares the level of a desired signal to the level of background noise. SNR is defined as the ratio of signal power to the noise power, often expressed in decibels (dB). A high SNR means that the signal is clear and easy to detect or interpret, while a low SNR means that the signal is corrupted or obscured by noise and may be difficult to distinguish or recover1. When the signal from an AP Access Point. AP is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. weakens by being absorbed as it moves through an object, such as a wall or a furniture, the signal power decreases. This reduces the SNR and affects the quality of the wireless connection. The noise power may also increase due to interference from other sources, such as other APs or devices operating in the same frequency band2. Therefore, the correct answer is that SNR decreases when the signal from an AP weakens by being absorbed as it moves through an object. Reference: 1 https://en.wikipedia.org/wiki/Signal-to- noise_ratio 2 https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to- Noise_Ratio_%28SNR%29_and_Wireless_Signal_Strength

Question: 7

DRAG DROP

Match the feature to the Aruba OS version (Matches may be used more than once.)



Answer:

Explanation:

Features: 1) Clustered Instant Access Points Aruba OS version: a) Aruba OS 8

Features: 2) Dynamic Radius Proxy Aruba OS version: a) Aruba OS 8

Features: 3) Scales to more than 10,000 devices Aruba OS version: b) Aruba OS 10

Features: 4) Unifies wired and wireless management Aruba OS version: a) Aruba OS 8

Features: 5) Wireless controllers Aruba OS version: a) Aruba OS 8

ArubaOS is the operating system for all Aruba Mobility Controllers (MCs) and controller-managed wireless access points (APs). ArubaOS 8 delivers unified wired and wireless access, seamless roaming, enterprise grade security, and a highly available network with the required reliability to support high density environments1. Some of the features of ArubaOS 8 are:

Clustered Instant Access Points: This feature allows multiple Instant APs to form a cluster and share configuration and state information. This enables seamless roaming, load balancing, and fast failover for clients2.

Dynamic Radius Proxy: This feature allows an MC to act as a proxy for RADIUS authentication requests from clients or APs. This simplifies the configuration and management of RADIUS servers
and reduces the network traffic between MCs and RADIUS servers3.
Wireless controllers: Aruba wireless controllers are devices that centrally manage and control the wireless network. They provide functions such as AP provisioning, configuration, security, policy enforcement, and network optimization.
ArubaOS 10 is the next-generation operating system that works with Aruba Central, a cloud-based network management platform. ArubaOS 10 delivers greater scalability, security, and AI-powered optimization across large campuses, branches, and remote work environments. Some of the features of ArubaOS 10 are:
Scales to more than 10,000 devices: ArubaOS 10 can support up to 10,000 devices per cluster, which is ten times more than ArubaOS 8. This enables customers to scale their networks without compromising performance or reliability.
Unifies wired and wireless management: ArubaOS 10 provides a single platform for managing both wired and wireless devices across the network. Customers can use Aruba Central to configure, monitor, troubleshoot, and update their devices from anywhere.
Both ArubaOS 8 and ArubaOS 10 share some common features, such as:
Unifies wired and wireless management: Both operating systems provide unified wired and wireless access for customers who use Aruba switches and APs. Customers can use a single interface to manage their entire network infrastructure1 .
Reference: 1 https://www.arubanetworks.com/resource/arubaos-8-fundamental-guide/ 2 https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/iap- maintenance/cluster.htm 3 https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/dynamic-radius-proxy.htm
https://www.arubanetworks.com/products/networking/controllers/
https://www.arubanetworks.com/products/network-management-operations/arubaos/
https://blogs.arubanetworks.com/solutions/making-the-switch/
https://www.arubanetworks.com/products/network-management-operations/aruba-central/

Question: 8

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

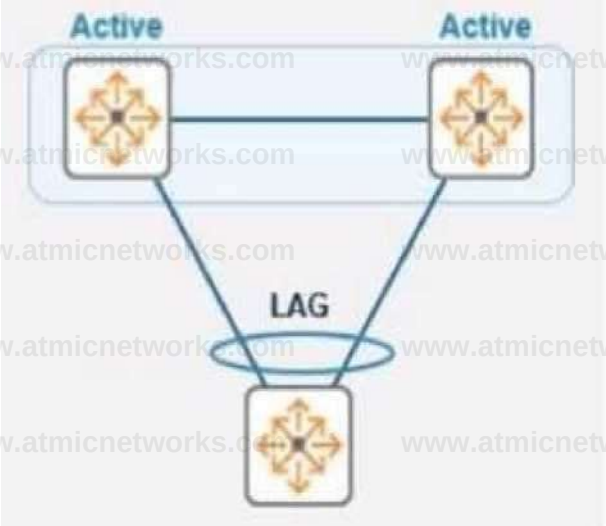
Explanation:

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. Reference: 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/AdministrationTas ks1/Configuring-MPSK.htm

Question: 9

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
B. Virtual floating IP will failover in case of a failure
C. Virtual IP is active on both CX switches
D. Virtual IP uses SVI IP address synced with VSX

Answer: B

Explanation:

In a Virtual Switching Extension (VSX) stack, the Virtual IP (VIP) provides a single default gateway IP address for clients connected to the access switch. This VIP is a floating IP that is active on the primary VSX switch. In the event of a failure of the primary switch, the VIP will failover to the secondary switch, ensuring that client traffic can continue to be routed without disruption.

Question: 10

When performing live firmware upgrades on Aruba APs. which technology partitions all the APs based on RF neighborhood data minimizing the impact on clients?

A. Aruba ClientMatch
B. Aruba Ai insights
C. Aruba AirMatch
D. Aruba ESP

Answer: C

Explanation:

Aruba AirMatch is a feature that optimizes RF Radio Frequency. RF is any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. performance and user experience by using machine learning algorithms and historical data to dynamically adjust AP power levels, channel assignments, and channel width. AirMatch performs live firmware upgrades on Aruba APs by partitioning all the APs based on RF neighborhood data and minimizing the impact on clients. AirMatch uses a rolling upgrade process that upgrades one partition at a time while ensuring that adjacent partitions are not upgraded simultaneously. Reference: https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdfhttps://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/arm/AirMatch.htm

Question: 11

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: B

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. Reference: https://en.wikipedia.org/wiki/Static_routing https://www.arubanetworks.com/techdocs/AOS- CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip- routing/show-ip-route.htm

Question: 12

Which device configuration group types can a user define in Aruba Central during group creation? (Select two.)

A. Security group
B. Template group
C. Default group
D. UI group
E. ESP group

Answer: BC

Explanation:

In Aruba Central, during the creation of a device configuration group, users can define various types of groups to manage and

apply configurations to devices centrally. Among the options, "Template group" and "Default group" are valid types. A "Template group" allows the definition of configuration settings in a template format, which can be applied to multiple devices or device groups, ensuring consistency and efficiency in configurations across the network. A "Default group" is typically a predefined group in Aruba Central that applies a basic or initial set of configurations to devices that are not assigned to any other specific group. This helps in initial provisioning and management of devices. The other options, such as "Security group," "UI group," and "ESP group," are not standard group types defined in Aruba Central for device configuration purposes.

Question: 13

What is the correct command to add a static route to a class-c-network 10.2.10.0 via a gateway of 172.16.1.1?

A. ip-route 10.2.10.0/24 172.16.1.1
B. ip route 10.2.10.0.255.255.255.0 172.16.1.1 description aruba
C. ip route 10.2.10.0/24.172.16.11
D. ip route-static 10.2 10.0.255.255.255.0 172.16.1.1

Answer: A

Explanation:

The correct command to add a static route to a class-c-network 10.2.10.0 via a gateway of 172.16.1.1 is ip-route 10.2.10.0/24 172.16.1.1 . This command specifies the destination network address (10.2.10.0) and prefix length (/24) and the next-hop address (172.16.1 .1) for reaching that network from the switch. The other commands are either incorrect syntax or incorrect parameters for adding a static route. Reference: https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm

To add a static route in network devices, including Aruba switches, the correct command format generally includes the destination network, subnet mask (or CIDR notation for the mask), and the next-hop IP address. The command "ip route 10.2.10.0/24 172.16.1.1" correctly specifies the destination network "10.2.10.0" with a class C subnet mask indicated by "/24", and "172.16.1.1" as the next-hop IP address. This command is succinct and follows the standard syntax for adding a static route in many network operating systems, including ArubaOS-CX. The other options either have incorrect syntax or include additional unnecessary parameters that are not typically part of the standard command to add a static route.

Question: 14

You need to configure wireless access for several classes of loT devices, some of which operate only with 802 11b. Each class must have a unique PSK and will require a different security policy applied as a role There will be 15-20 different classes of devices and performance should be optimized Which option fulfills these requirements''

A. Single SSID with MPSK for each loT class using 5 GHz and 6 GHz bands
B. Single SSID with MPSK for each loT class using 2.4GHz and 5 GHz bands
C. Individual SSIDs with unique PSK for each loT class, using 5GHz and 6 GHz bands
D. Individual SSIDs with unique PSK for each loT class, using 2.4GHZ and 5GHz band

Answer: B

Explanation:

For configuring wireless access for multiple classes of IoT devices with varying security requirements, using a single SSID with Multiple Pre-Shared Keys (MPSK) is an efficient solution. MPSK allows different devices or groups of devices to connect to the same SSID but with unique PSKs, facilitating unique security policies for each class. Given that some IoT devices only support 802.11b, which operates in the 2.4GHz band, it is essential to include the 2.4GHz band in the configuration. The 5GHz band should also be included to support devices capable of operating in that band and to optimize network performance. The 6GHz band (option A) is not suitable since 802.11b devices are not compatible with it. Individual SSIDs for each IoT class (options C and D) would unnecessarily complicate network management and SSID overhead.

Question: 15

The noise floor measures 000000001 milliwatts, and the receiver's signal strength is -65dBm. What is the Signal to Noise Ratio?

A. 35 dBm
B. 15 dBm
C. 45 dBm
D. 25 dBm

Answer: D

Explanation:

The signal to noise ratio (SNR) is a measure that compares the level of a desired signal to the level of background noise. SNR is defined as the ratio of signal power to the noise power, often expressed in decibels (dB). A high SNR means that the signal is clear and easy to detect or interpret, while a low SNR means that the signal is corrupted or obscured by noise and may be difficult to distinguish or recover3. To calculate the SNR in dB, we can use the following formula:

SNR (dB) = Signal power (dBm) - Noise power (dBm)

In this question, we are given that the noise floor measures -90 dBm (0.000000001 milliwatts) and the receiver's signal strength is -65 dBm (0.000316 milliwatts). Therefore, we can plug these values into the formula and get:

SNR (dB) = -65 dBm - (-90 dBm) SNR (dB) = -65 dBm + 90 dBm SNR (dB) = 25 dBm

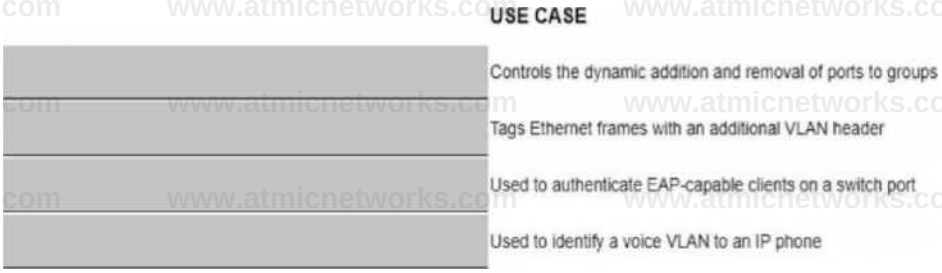
Therefore, the correct answer is that the SNR is 25 dBm.

Reference: 3 https://en.wikipedia.org/wiki/Signal-to-noise_ratio

Question: 16

DRAG DROP

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

802.1 Q 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, improvi security, performance, and manageability. 802.1Q tags Ethernet frames with an additional VLAN heade 1) 802.1Q contains a VLAN identifier (VID), which indicates which VLAN the frame belongs to1.

802.2 X is a standard that defines how to provide port-based network access control (PNAC) on a netwo PNAC allows network administrators to authenticate and authorize devices before granting them acces network resources. 802.1X uses the Extensible Authentication Protocol (EAP) to exchange authenticati messages between a supplicant (a device that wants to access the network), an authenticator (a device controls access to the network, such as a switch), and an authentication server (a device that verifies th

2) 802.1X credentials of the supplicant, such as a RADIUS server)2.

LACP stands for Link Aggregation Control Protocol, which is part of the IEEE 802.3ad standard that defin how to bundle multiple physical links into a single logical link, also known as a link aggregation group (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 po

3) LACP with compatible configurations can form a LAG3.

LLDP stands for Link Layer Discovery Protocol, which is part of the IEEE 802.1AB standard that defines h discover and advertise information about neighboring devices on a network. LLDP operates at Layer 2 o OSI model and uses TLVs (type-length-value) to exchange information such as device name, port numb VLAN ID, capabilities, and power requirements. LLDP can be used to identify a voice VLAN to an IP pho

4) LLDP sending a TLV that contains the voice VLAN ID and priority.

Reference: 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

Question: 17

Which commands are used to set a default route to 10.4.5.1 on an Aruba CX switch when In-band management using an SVI

is being used?

A. iP default-gateway 10.4.5.1
B. ip route 0 0 0.070 10.4 5.1 vrf mgmt
C. ip route 0.0 0 0/0 10.4.5.1
D. default-gateway 10.4.5.1

Answer: C

Explanation:

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

Reference: 1 https://www.arubanetworks.com/techdocs/AOS-CX/10_08/HTML/ip_route_4100i- 6000-6100-6200/Content/Chp_StatRoute/def-rou.htm 2 https://www.arubanetworks.com/techdocs/AOS-CX/10_08/HTML/ip_route_4100i-6000-6100-6200/Content/Chp_VRF/vrf-overview.htm

Question: 18

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).

Reference: 3 https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

Question: 19

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 nonoverlapping 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 WiFi devices that do not support Wi-Fi 6E standard 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.

Reference: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6ehttps://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.htmlhttps://www.wi-fi.org/file/wi-fi-alliance-unlicensed-spectrum-in-the-us

Question: 20

A hospital uses a lot of mobile equipment for the diagnosis and documentation of patient data What Is the ideal access switch for this large hospital with distribution racks of over 400 ports in a single VSF stack?

A. CX 6300
B. OCX 6400
C. OCX 6200
D. OCX 6100

Answer: A

Explanation:

The ideal access switch for a large hospital with distribution racks of over 400 ports in a single VSF stack is the CX 6300. This switch provides the following benefits:

The CX 6300 supports up to 48 ports per switch and up to 10 switches per VSF stack, allowing for a total of 480 ports in a single stack. This meets the requirement of having over 400 ports in a single VSF stack.

The CX 6300 supports high-performance switching with up to 960 Gbps of switching capacity and up to 714 Mpps of forwarding rate. This meets the requirement of having high throughput and low latency for mobile equipment and patient data.

The CX 6300 supports advanced features such as dynamic segmentation, policy-based routing, and role-based access control. These features enhance the security and flexibility of the network by applying different policies and roles to different types of devices and users.

The CX 6300 supports Aruba NetEdit, a network configuration and orchestration tool that simplifies the management and automation of the network. This reduces the complexity and human errors involved in network configuration and

maintenance.

The other options are not ideal because:

OCX 6400: This switch is designed for data center applications and does not support VSF stacking. It also does not support dynamic segmentation or policy-based routing, which are useful for network security and flexibility.

OCX 6200: This switch is designed for small to medium-sized businesses and does not support VSF stacking. It also has lower switching capacity and forwarding rate than the CX 6300, which may affect the performance of the network.

OCX 6100: This switch is designed for edge applications and does not support VSF stacking. It also has lower switching capacity and forwarding rate than the CX 6300, which may affect the performance of the network.

Reference: https://www.arubanetworks.com/assets/ds/DS_CX6300Series.pdf

https://www.arubanetworks.com/assets/ds/DS_OC6400Series.pdf

https://www.arubanetworks.com/assets/ds/DS_OC6200Series.pdf

https://www.arubanetworks.com/assets/ds/DS_OC6100Series.pdf

Question: 21

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 the network) 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.

Reference: 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

Question: 22

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

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.

Reference: https://en.wikipedia.org/wiki/Rate_limiting
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/storm-control.htmhttps://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: 23

What does WPA3-Personal use as the source to generate a different Pairwise Master Key (PMK) each time a station connects to the wireless network?

A. Session-specific information (MACs and nonces)

B. Opportunistic Wireless Encryption (OWE)
C. Simultaneous Authentication of Equals (SAE)
D. Key Encryption Key (KEK)

Answer: C

Explanation:

WPA3-Personal enhances the security of wireless networks by using Simultaneous Authentication of Equals (SAE), which is a more secure replacement for the Pre-Shared Key (PSK) method used in WPA2. SAE strengthens the initial key exchange, providing better protection against offline dictionary attacks and ensuring that each session has a unique Pairwise Master Key (PMK), derived from the interaction between the client and the access point, including session-specific information like MAC addresses and nonces.

Question: 24

You need to troubleshoot an Aruba CX 6200 4-node VSF stack switch that fails to boot correctly Select the option that allows you to access the switch and see the boot options available for OS images and ServiceOS.

A. Member 2 RJ-45 console port
B. Member 2 switch mgmt port
C. Conductor USB-C console port
D. Conductor mgmt port using SSH

Answer: A

Explanation:

To troubleshoot an Aruba CX 6200 switch that is failing to boot correctly, accessing the switch via the RJ-45 console port on any of its member switches provides direct access to the switch's console for troubleshooting. This method allows a network technician to interact with the boot process, view boot messages, and access boot options, including the selection of different OS images or ServiceOS for recovery purposes.

Question: 25

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

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 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 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.
Reference: 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: 26

What is a weakness introduced into the WLAN environment when WPA2-Personal is used for security?

A. It uses X 509 certificates generated by a Certification Authority
B. The Pairwise Temporal Key (PTK) is specific to each session
C. The Pairwise Master Key (PMK) is shared by ail users
D. It does not use the WPA 4-Way Handshake

Answer: C

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

Reference: 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: 27

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: D

Explanation:

While both 5 GHz and 6 GHz channels can provide similar throughputs, the higher frequency of the 6 GHz band means its signals have a shorter range and are more attenuated by obstacles compared to 5 GHz signals. This results in 5 GHz channels generally being able to travel longer distances than 6 GHz channels under similar conditions, although both can support high data rates for connected clients.

Question: 28

DRAG DROP

Match the appropriate QoS concept with its definition.

QoS concept	Definition
Best Effort Service	A method for classifying network traffic at Layer 2 by marking 802 1Q VLAN Ethernet frames with one of eight service classes
Class of Service	A method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes
Differentiated Services	A method for classifying network traffic using access categories based on the IEEE 802.11 e QoS standard
	A method where traffic is treated equally tn a first-come, first-served manner

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.

Reference: 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-dfsrv-overview.htmlhttps://www.cisco.com/c/en/us/support/docs/quality-of-service- qos/qos-packet-marking/10103-dscpvalues.html
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/81831-qos- wlan.htmlhttps://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm

Question: 29

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: C

Explanation:

The Aruba CX 6300 Series is an ideal access switch for medium to high-density client environments, offering a range of models that can accommodate various port densities and types. For a distribution rack supporting 200-380 clients, printers, and APs, the CX 6300 provides the necessary port density and performance capabilities, including high-speed uplinks, support for Class 4 PoE (PoE+), and stacking capabilities. This series is cost-effective and designed for enterprises requiring reliable connectivity and consistent performance. The other options, such as the CX 6400, CX 6200, and CX 6000, may either be over-specified and more expensive (CX 6400), not offer the necessary port density (CX 6200), or not exist in the product line (CX 6000).

Question: 30

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: B

Explanation:

When checking the status of LACP (Link Aggregation Control Protocol) with the command "show lacp interfaces," various flags indicate the state of the LACP negotiation. "ALFOE" indicates different states for each letter: A (Activity), L (Link), F (Aggregation), O (Synchronization), and E (Collecting). In this context, the O flag is particularly of interest. If the O flag is not set (meaning the synchronization is not achieved), it typically suggests that LACP is not configured or not functioning correctly on the peer side, hence the link is not operational as part of an LACP channel.

Question: 31

Review the configuration below.

```
Core-1(config)# interface loopback 0
Core-1(config-if)# ip address 10.1.200.1/32
Core-1(config)# router ospf 1
Core-1(config-ospf-1)# router-id 10.1.200.1
Core-1(config-ospf-1)# area 0
Core-1(config-ospf-1)# exit
```

Why would you configure OSPF to use the IP address 10.1.200.1 as the router ID?

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

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 interface brief 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 multiaccess (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 on their 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: 32

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

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

Question: 33

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: A

Explanation:

A solid amber radio status LED on an Aruba Access Point (AP) typically indicates a power issue, specifically that not enough Power over Ethernet (PoE) is being provided from the switch to fully power all functionalities of the AP, including both of its radios. In environments where APs are powered via PoE, it is crucial to ensure that the switch supplying the power is capable of delivering sufficient power for the AP's requirements. If the AP does not receive enough power, it may disable certain features or radios to conserve energy, which is indicated by the solid amber LED. This situation is common in scenarios where the switch provides only 802.3af PoE rather than the more powerful 802.3at PoE+ needed by some high-performance APs to operate all features, including dual radios, at full capacity.

Question: 34

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?

A. ClearPass 6.9 with EAP-TTLS
B. ClearPass 6.9 with EAP-TLS
C. ClearPass 6.9 with PEAP
D. ClearPass 6.9 with EAP-TEAP

Answer: D

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 an authentication method for Windows 10 clients. Reference:
https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content/CPPM_UserGuide/EAP-TEAP/EAP-TEAP.htm

For the requirement to authorize both device and user credentials within one Radius session, the correct solution would be ClearPass 6.9 with EAP-TEAP (EAP-Tunneled Extensible Authentication Protocol). EAP-TEAP is a tunneling protocol that creates a secure communication channel between the client and the server, allowing for the transmission of multiple authentication transactions within a single session. This capability is particularly useful in scenarios where both user and device credentials need to be verified before granting access to network resources, providing an additional layer of security and ensuring that both the user and the device are authorized to access the network.

Question: 35

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: D

Explanation:

When using an Aruba standalone AP, selecting “Native VLAN” for the Client VLAN Assignment means

that the clients will get their IP addresses from the same subnet as the access point’s IP address. This is because the access point acts as a DHCP server for the clients in this mode. Reference:
https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/iap-dhcp/iap-dhcp.htm

Question: 36

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.
Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/stacking-leds.htm

Question: 37

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: A

Explanation:

When an Aruba AP is not receiving its configuration from Aruba Central, and other APs at the location are functioning normally, a common troubleshooting step is to disable and then re-enable the activation process on the AP. This action can trigger a provisioning refresh, prompting the AP to attempt to retrieve its configuration from Aruba Central again. This step is often effective in resolving communication or provisioning issues between the AP and the management platform.

Question: 38

What are two advantages of a UXl? (Select two.)

A. A UXl can be used without any internet connection
B. A UXl helps to calculate the best WiFi channels in a remote location
C. A UXl behaves like a client/user
D. A UXl measures the Wi-Fi coverage of all APs in the given location.
E. A UXl can check different applications, such as HTTP VOIP or Office 365.

Answer: CE

Explanation:

A UXI (User Experience Insight) is a device that simulates user behavior and tests network performance from the user perspective. It can check different applications, such as HTTP, VOIP, or Office 365, and measure metrics such as latency, jitter, packet loss, and throughput. Reference: https://www.arubanetworks.com/products/networking/user-experience-insight/

A User Experience Insight (UXI) sensor, such as those used in Aruba networks, is designed to mimic client behavior and test the performance of various network services and applications from the user's perspective. It can simulate user activities and measure the quality of experience for different applications, including HTTP, VOIP, and cloud services like Office 365, providing valuable insights into network performance and user experience.

Question: 39

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 For route entries
C. The administrative distance for a static route is 10
D. The higher administrative distance is preferred

Answer: B

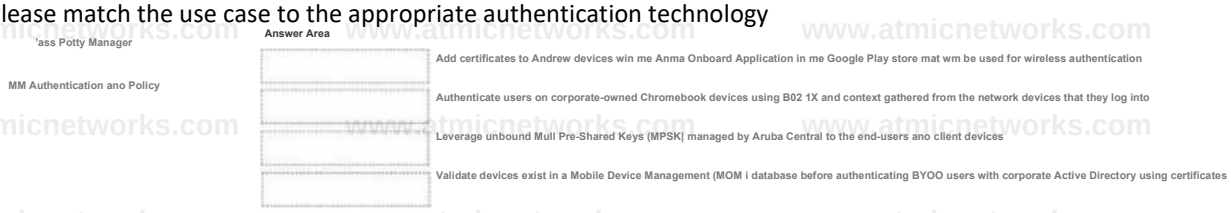
Explanation:

The administrative distance is used as a trust rating for route entries (B). It is a metric used by routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. The lower the administrative distance value, the more trustworthy the source of the route. For example, a directly connected network has an administrative distance of 0 because it is the most trusted source of routing information. In contrast, routes learned from different routing protocols have higher administrative distances, reflecting their relative trustworthiness.

Question: 40

DRAG DROP

Please match the use case to the appropriate authentication technology



Answer:

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%20ClearPass/About_ClearPass.htm

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

Question: 41

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

A. Star
B. Daisy chain plus MAD
C. Full mesh
D. Full mesh plus MAD
E. Ring

Answer: BE

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. Reference:

https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790/GUID-D6EF042E-EEEF-49F7-B67E-4CAC41CCB24D.html

Question: 42

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

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.
Reference:
https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdf
In Aruba networks, the recommended Virtual Switching Framework (VSF) topologies include the daisy chain plus Multi-Active Detection (MAD) and the ring topology. The daisy chain topology with MAD provides a straightforward and effective way to connect multiple switches in a series while ensuring there is a mechanism in place (MAD) to detect and handle situations where more than one switch in the VSF might become active simultaneously. The ring topology offers redundancy by creating a looped connection pattern among the VSF members, enhancing network resilience and reliability.

Question: 43

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: C

Explanation:

Manual switch provisioning in Aruba Central can be done without relying on DNS services, but it does require DHCP to assign IP addresses to the switches. DHCP is essential for the switches to obtain an IP address, which is necessary for them to communicate within the network and with Aruba Central for management and configuration purposes. DNS, on the other hand, is not strictly required for manual provisioning as direct IP addresses or other methods can be used to connect to Aruba Central or other management interfaces.

Question: 44

Where are wireless client roaming decisions made?

A. Client device
B. Virtual Controller
C. Joint decision made by the origination and destination APs
D. Aruba Central

Answer: A

Explanation:

Wireless client roaming decisions are made by the client device based on its own criteria, such as signal strength, noise level, data rate, etc. The network can influence the client's roaming decision by providing information such as neighbor reports, load balancing, band steering, etc., but the final decision is up to the client. Reference: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/wlan- roaming/client-roaming.htm

Wireless client roaming decisions are primarily made by the client device itself. The client device monitors the signal strength and quality of the current connection and decides to roam to a different Access Point (AP) when the current signal deteriorates below a certain threshold or a better option is available. While APs and controllers can provide information and support for roaming decisions through protocols like 802.11k and 802.11v, the ultimate decision to roam is made by the client device based on its algorithms and thresholds.

Question: 45

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?

A. EAP-TTLS
B. EAP-TLS
C. EAP-TEAP
D. PEAP

Answer: B

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

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) is an EAP method that requires both server-side and client-side certificates for authentication. It is considered one of the most secure EAP methods because it uses a mutual authentication process where both the user and the authentication server must prove their identities to each other through the use of certificates. Implementing user and device certificates via a Group Based Policy (GPO) aligns well with EAP-TLS requirements for client-side certificates.

Question: 46

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 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

D. Create an SVl in the subnet on the 6300M stack.

Answer: D

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 routed interface 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 interVLAN 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.

Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/index.htmlhttps://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3- routing-overview.htm https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-config.htm

Question: 47

DRAG DROP

What is the correct order of the TCP 3-Way Handshake sequence?

TCP 3-Way Handshake sequence	Order
A flow-controlled connection ts established	
The Initiating host sends a packet with no data to the target host with a SEO1 and sets the SYN flag to 1	
The initiating host sends a packet with SEQ=2 ACK=9, and ACK flag is raised	
The target host sends a packet with ACK=2 SEQ=8. and the SYN and ACK flags are set to 1	

Answer:

Explanation:

TCP 3-Way Handshake sequence is:

Step 1: The initiating host sends a packet with no data to the target host with a SEQ=1 and sets the SYN flag to 1.

Step 2: The target host responds with a packet with ACK=2, SEQ=8, and the SYN and ACK flags set to 1.

Step 3: The initiating host sends a packet with SEQ=2, ACK=9, and the ACK flag set to 1.

Step 4: A normal-controlled connection is established.

Reference: https://en.wikipedia.org/wiki/Transmission_Control_Protocol

https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

Question: 48

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

Bonding multiple 20MHz wide 802.11 channels is a technique used to increase the throughput between the client device and the Access Point (AP). By combining two or more 20MHz channels into a wider channel (e.g., 40MHz, 80MHz, or even 160MHz), the data carrying capacity and, consequently, the overall throughput of the wireless connection are increased. This method is particularly useful in high-bandwidth applications or environments where higher data rates are required.

Question: 49

Which authentication does Aruba's Captive Portal use?

A. Layer 3 authentication
B. MAC authentication
C. 802.1x authentication
D. Layer 2 authentication

Answer: A

Explanation:

Aruba's Captive Portal uses Layer 3 authentication, which means that it intercepts the client's HTTP requests and redirects them to a web page where the client can enter their credentials. The credentials are then verified by a RADIUS server or a local database before granting network access. Reference: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/captive-portal/captive-portal-auth.htm

Aruba's Captive Portal primarily uses Layer 3 authentication, which operates at the network layer. When a user connects to a network with a Captive Portal, they are redirected to a web page for authentication. This process involves the user entering credentials or accepting terms and conditions through a web interface before gaining full access to the network. The Captive Portal intercepts the user's web traffic at Layer 3, requiring them to authenticate before proceeding, which is why it's considered a form of Layer 3 authentication.

Question: 50

DRAG DROP

Match each AAA service with its correct definition (Matches may be used more than once or not at all)

Definition	AAA Service
A list of rules that specifies which entitles are permittee! or denied access	Accounting
Control users access on ttie network	Authentication
Tracking user activity on the network	Authorization
Who can access the network based on credentialsfcertificates	

Answer:

Explanation:

AAA Authentication, Authorization, and Accounting (AAA) Authentication, Authorization, and Accounting (AAA) is a framework that provides security services for network access control . AAA consists of three components: Authentication: The process of verifying the identity of a user or device that wants to access the network based on credentials such as username and password , certificates , tokens , etc . Authentication can use different protocols such as PAP , CHAP , EAP , RADIUS , TACACS+ , etc . Authorization: The process of granting or denying access to network resources based on the identity and privileges of a user or device . Authorization can use different methods such as ACLs , RBAC , MAC , DAC , etc .

Accounting: The process of recording and reporting the activities and usage of network resources by users or devices . Accounting can use different formats such as syslog , SNMP , NetFlow , etc . service. Here is my answer:

The correct match for each AAA service with its definition is:

Accounting: C. Tracking user activity on the network

Authentication: D. Who can access the network based on credentials/certificates

Authorization: B. Control users access on the network

The other options are not correct matches because:

A list of rules that specifies which entities are permitted or denied access: This option is a definition of an access control list (ACL) Access Control List (ACL) Access Control List (ACL) is a list of rules that specifies which entities are permitted or denied access to a network resource such as a router , switch , firewall , server , etc . ACLs can be based on different criteria such as source and destination IP addresses , port numbers , protocol types , time of day , etc . ACLs can be applied to different interfaces or directions such as inbound or outbound . ACLs can be verified by using commands such as show access-lists , show ip access-lists , debug ip packet , etc . , not an AAA service.

Who can access the network based on credentials/certificates: This option is a definition of authentication, not authorization. Authorization is the process of granting or denying access to network resources based on the identity and privileges of a user or device, not based on credentials/certificates.

Reference: https://en.wikipedia.org/wiki/AAA_(computer_security)

https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user- service-radius/13838-10.html

Question: 51

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 Reference:

https://www.rapidtables.com/convert/power/dBm_to_mW.html

The dBm is a logarithmic unit of power relative to 1 milliwatt (mW). -20 dBm means that the signal strength is 20 decibels lower than 1 mW. In terms of mW, this is 0.01 mW. Each 10 dB decrease represents a tenfold decrease in power. Therefore, -20 dBm is 10-210-2 or 0.01 mW.

Question: 52

DRAG DROP

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

Question: 53

You have been asked to onboard a new Aruba 6300M in a customer deployment You are working remotely rather than on-site You have a colleague installing the switch The colleague has provided you with a remote console session to configure the edge switch You have been asked to configure a link aggregation going back to the cores using interfaces 1/1/51 and 1/1/52 The Senior Engineer of the project has asked you to configure the switch and 1Q uplink with these guidelines

1. Add VLAN 20 to the local VLAN database with name Mgmt
2. Add L3 SVl on VLAN 20 for Management using address 10 in the 10.1.1 0/24 subnet 3. Add LAG 1 using LACP mode active for the uplink

4 use vlan 20 as the native vlan on the LAG 5. Make sure the interfaces are all ON.

Which configuration script will achieve the task?

A. Edge1# conf t vlan 20 name Mgmt interface vlan 20 ip address 10.1.1.10/24 no shut interface lag 1 shut vlan access 20 lacp mode active Int 1/1/51.1/1/52 shut no routing lag 1 interface lag 1 no shut B. Edgel# conf t vlan 20 name Mgmt interface vlan 20 ip address 10 1.1 10/24 no shut interface 1/1/51.1/1/52 shut vlan trunk native 20 vlan trunk allowed all lag 1 lacp mode active interface 1/1/51.1/1/52 no shut

C. Edgel# conf t vlan 20 name Mgmt interface vlan 20 ip address 10 1 1 10/24 no shut interface lag 1 shut vlan trunk native 20 vlan trunk allowed all lacp mode active Int 1/1/51.1/1/52 shut no routing lag 1 interface lag 1 no shut interface 1/1/51.1/1/52 no shut

D. conf t vlan 20 name Mgmt ip address 10 1 1.10/24 no shut interface lag 1 shut vlan trunk native 1 vlan trunk allowed all lacp mode active int 1/1/51.1/1/52 shut no routing interface lag 1 no shut interface 1/1/51.1/1/52 no shut

Answer: C

Explanation:

This configuration script will achieve the task as it follows the guidelines given by the Senior Engineer. It creates VLAN 20 with name Mgmt, adds L3 SVI on VLAN 20 with IP address 10.1.1.10/24, creates LAG 1 with LACP mode active for the uplink, uses VLAN 20 as the native VLAN on the LAG, and ensures that the interfaces are all ON. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790/GUID-8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html

Edge1# conf t vlan 20
name Mgmt interface vlan 20 ip address 10.1.1.10/24 no shut interface lag 1 no shut
vlan trunk native 20
vlan trunk allowed all
lacp mode active interface 1/1/51 no shut
lag 1
interface 1/1/52
no shut
lag 1
exit

This script correctly creates VLAN 20 with the name 'Mgmt', adds an L3 SVI for management using the specified IP address, and configures LACP for link aggregation (LAG 1) using the active mode. It also sets VLAN 20 as the native VLAN on the LAG and ensures all interfaces are enabled ('no shut' is the command to bring up the interface if it has been administratively shut down).

Question: 54

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

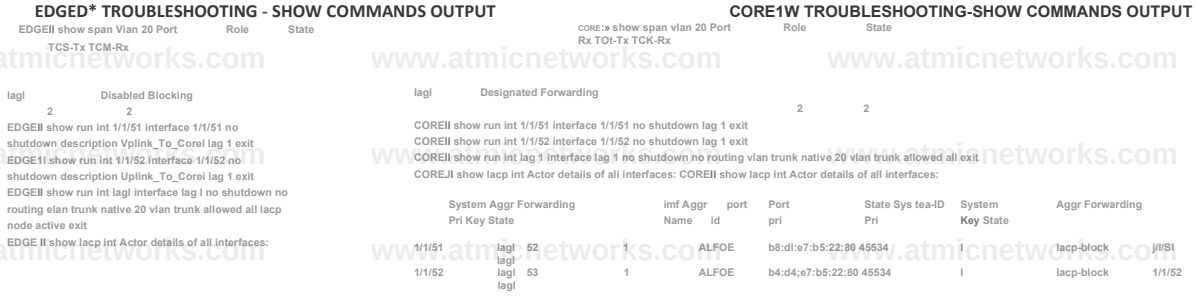
Explanation:

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. Reference: https://www.arubanetworks.com/techdocs/AOS-CX_10_04/CLI/GUID-8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html

Question: 55

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

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. Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/lacp.htm

Question: 56

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

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. Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/profiling.htm

Question: 57

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

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 as Ethernet, Wi-Fi, etc.
Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/networking-basics.htm

Question: 58

What is an advantage of using Layer 2 MAC authentication?

A. it matches user names to MAC address
B. No setup is required on the client
C. MAC allow lists are easily maintained over time
D. MAC identifiers are hard to spoof

Answer: B

Explanation:

Layer 2 MAC authentication is a method of authenticating devices based on their MAC addresses without requiring any client-side configuration or credentials. The switch sends the MAC address of the device to an authentication server such as ClearPass or RADIUS, which checks if the MAC address is authorized to access the network. If yes, the switch grants access to the device based on the assigned role and policies. If no, the switch denies access or redirects the device to a captive portal for further authentication. Reference:

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/mac-authentication.htm

Question: 59

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

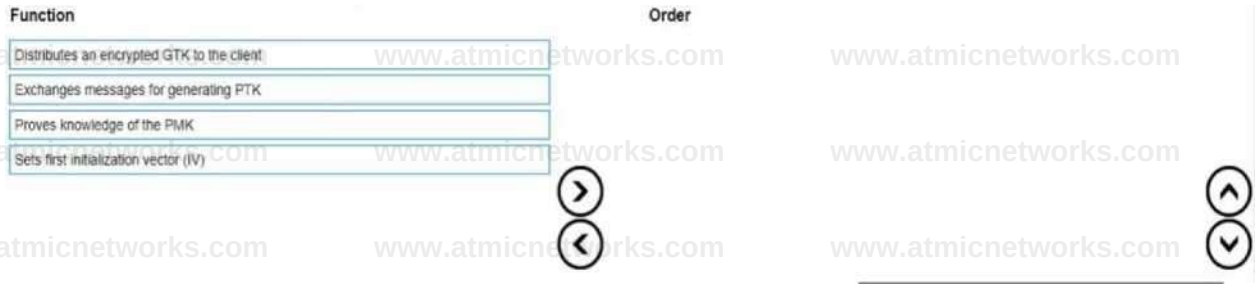
Answer: B

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. Reference: https://www.arubanetworks.com/assets/ds/DS_ArubaCentral.pdf

Question: 60

DRAG DROP
List the WPA 4-Way Handshake functions in the correct order.



Answer:

Explanation:

Proves knowledge of the PMK Exchanges messages for generating PTK Distributes an encrypted GTK to the client Sets first initialization vector (IV)

Question: 61

Which statement is true for a device with a MAC address of B8-31-B5-80-41-4F?

A. The device OUI is B8-31-B5 and the device NIC serial number is 80-41-4F

B. The device OUI is B8-31 and the device NIC serial number is B5-80-41-4F

C. The device OUI is 80-41-4F and the device NIC serial number is B8-31-B5

D. The device OUI is B8-31-B5 and the device serial number is MD5 hash is 80-41-4F

Answer: A

Explanation:

A MAC address is divided into two parts: the Organizationally Unique Identifier (OUI) and the Network Interface Controller (NIC) serial number. The OUI is the first three octets of the MAC address and is unique to the manufacturer. The NIC serial number is the last three octets and is unique to the device itself. Therefore, for the MAC address B8-31-B5-80-41-4F, the OUI is B8-31-B5, and the NIC serial number is 80-41-4F.

Question: 62

What information is required when using the ClearPass self-service registration page to generate a Multiple Pre-Shared Key (MPSK) for headless devices?

A. The device's model number

B. The device's MAC address

C. The device's IP address

D. The device's OS type

Answer: B

Explanation:

When generating a Multiple Pre-Shared Key (MPSK) for headless devices using the ClearPass selfservice registration page, the MAC address of the device is required. MPSK associates a unique PSK with the MAC address of a device, providing a way to authenticate devices that may not have a user interface.

Question: 63

You are in a meeting with a customer where you are asked to explain how the network redundancy feature VRRP works. What is the correct statement for this feature?

A. VRRP uses BPDUs for messaging

B. VRRP uses multicast for messaging

C. VRRP uses unicast for messaging

D. VRRP uses broadcast for messaging

Answer: B

Explanation:
Virtual Router Redundancy Protocol (VRRP) is a network protocol that provides automatic assignment of available Internet Protocol (IP) routers to participating hosts. VRRP sends its messages over multicast for communication among routers for the election process of the master and advertisement of the virtual IP address.

Question: 64

Describe the functionality of ARP.

A. Clients do not have an ARP cache and always ask for the default gateway.

B. ARP maps MAC addresses to switch ports.

C. ARP maps layer-3 IP addresses to layer-2 MAC addresses.

D. ARP uses multicast to build the ARP table.

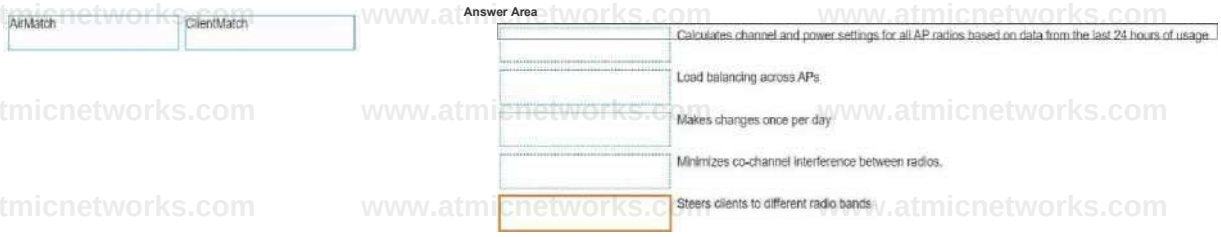
Answer: C

Explanation:
The Address Resolution Protocol (ARP) is used to map layer-3 IP addresses to layer-2 MAC addresses. When a device on a network wants to communicate with another device, it uses ARP to find the MAC address that corresponds to the IP address it wishes to communicate with, allowing it to construct a frame for the local network.

Question: 65

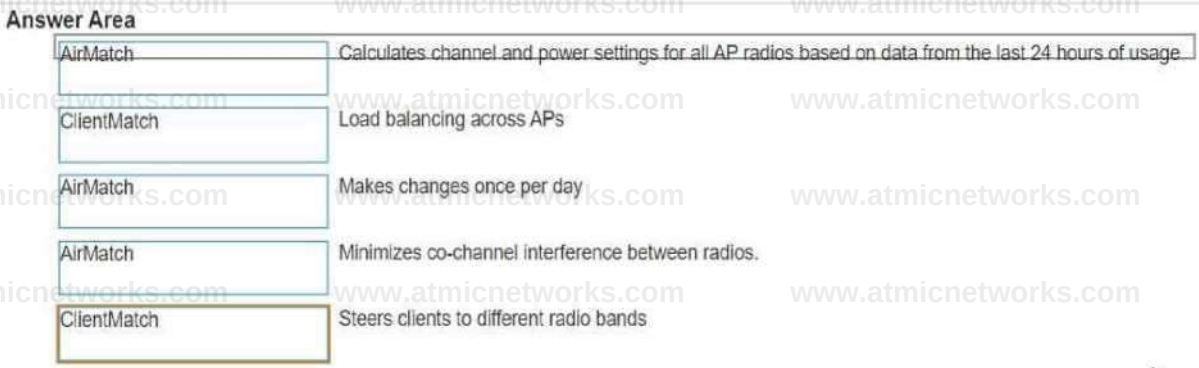
DRAG DROP

Match the Aruba Central technology to the appropriate feature. (Matches may be used more than once.)



Answer:

Explanation:



Question: 66

What does a wireless client do first when its countdown timer reaches zero and it receives a Transmit Opportunity (TXOP)?

A. It immediately sends its Data Frames and receives an ACK from the AP.

B. It sends a CTS-to-self announcement to the ESP gateway.

C. It sends a CTS-to-self announcement to the AP and all other clients.

D. It sends a reassociation request frame to the AP and sends its Data Frames.

Answer: A

Explanation:

When a wireless client's countdown timer (also known as a backoff timer) reaches zero during contention-based access periods, and it receives a Transmit Opportunity (TXOP), it has the right to transmit its data frames on the medium. After sending the data frames, it expects an acknowledgment (ACK) from the Access Point (AP) to ensure the frames were received successfully.

Question: 67

What is an advantage of using Layer 2 MAC authentication?

A. MAC allow lists are easily maintained over time.

B. No setup is required on the client.

C. It matches user names to MAC address.

D. MAC identifiers are hard to spoof.

Answer: B

Explanation:
The advantage of Layer 2 MAC authentication is that it does not require any setup or configuration on the client device. The network devices (like switches or access points) perform the authentication automatically based on the MAC address of the device when it tries to connect to the network.

Question: 68

The customer requires two Aruba CX 6200F 48G switches to be connected to each other with a distance of 80m/252ft between wiring closets. Switches need to have reservation for VSF expansion with ring topology in each cabinet.

What is a valid configuration for a redundant link-aggregation port configuration?

A. Ports 1/1/49 and 1/1/50 with SFP28 for LAG

B. Ports 1/1/47 and 1/1/48 for LAG

C. Ports 1/1/1 and 1/1/2 for LAG

D. Ports 1/1/51 and 1/1/52 with SFP+ for LAG

Answer: D

Explanation:
For an 80m distance between wiring closets, using SFP+ transceivers is appropriate as they can support longer distances than standard copper interfaces. Ports 1/1/51 and 1/1/52 are typically reserved for uplinks on Aruba CX 6200F 48G switches and can support SFP+ transceivers, making them suitable for a redundant link-aggregation port configuration.

Question: 69

When using the network check page in Central, what kind of tests can you run on switches? (Select two.)

A. Speed test (iperf)

B. Ping test

C. A full hardware check, including a heavy memory check

D. LED-check.

E. PoE-check

Answer: BE

Explanation:

In Aruba Central's network check page, you can run several diagnostic tests on switches. A ping test is a common utility to check the reachability of a host on an IP network. A Power over Ethernet (PoE) check can help verify the power delivery status to PoE-capable devices. These tests are crucial for ensuring connectivity and power supply to network devices

Question: 70

You need to troubleshoot an Aruba CX 6300F switch that fails to boot correctly. Select the option that allows you to access the switch and see the boot options available for OS images and ServiceOS.

A. USB-C console port

B. RJ-45 console port

C. USB-A console port

D. Omgmt port using SSH

Answer: A

Explanation:

To troubleshoot an Aruba CX 6300F switch that is failing to boot correctly, you would typically use the USB-C console port. This port allows you to connect to the switch directly with a console cable and access the boot loader menu, where you can see the available OS images and the ServiceOS for recovery and troubleshooting purposes.

Question: 71

Which device configuration group types can a user define in Aruba Central during group creation? (Select two.)

A. ESP group

B. Security group

C. Ul group

D. Default group

E. Template group

Answer: BE

Explanation:

In Aruba Central during group creation, users can define various configuration groups to manage settings for multiple devices. A Security group allows you to apply consistent security settings across devices, and a Template group enables you to apply pre-defined configurations to devices. These groups help streamline the deployment and management of network devices in Aruba Central.

Question: 72

You need to ensure that voice traffic sent through an ArubaOS-CX switch arrives with minimal latency. What is the best scheduling technology to use for this task?

A. QoS shaping

B. Rate limiting

C. Strict queuing

D. DWRR queuing

Answer: C

Explanation:

Strict queuing is the best scheduling technology for ensuring that voice traffic, which is sensitive to latency, is prioritized above other types of traffic. This method ensures that voice traffic is sent first before other queued traffic, effectively reducing the possibility of delay.

Question: 73

Where can you set the client's broadcast domain when configuring an ArubaOS firewall role?

A. WLAN Settings

B. Bandwidth Controls

C. Access Control Rules

D. Role-based VLAN override

Answer: D

Explanation:

The client's broadcast domain in ArubaOS can be set with role-based VLAN overrides within the firewall role settings. This allows for dynamic assignment of VLANs to users based on their role, which determines their level of network access, including their broadcast domain.

Question: 74

How does a single Aruba CX 6300M switch configuration use L3 connectivity to establish routing traffic between switch virtual interfaces 120 and 130?

A. Routing is enabled by default with Aruba 6300M.

B. Route leaking must be configured in default VRF.

C. Delete 'no routing' from the SVI interfaces.

D. Create static routes between SVI 120 and 130.

Answer: A

Explanation:

On an Aruba CX 6300M switch, routing between Switch Virtual Interfaces (SVIs) is enabled by default. Therefore, traffic between SVIs, like 120 and 130, can be routed internally without the need for additional configuration such as route leaking or static routes, as long as there is no 'no routing' configuration present on the SVIs.

Question: 75

An AP signal strength of .0000001 milliwatts equals how many dBm?

A. -90 dBm

B. -60 dBm

C. -70 dBm

D. -80 dBm

Answer: D

Explanation:
An AP signal strength of .0000001 milliwatts is equivalent to -80 dBm. The dBm scale is logarithmic, with every 10 dBm representing a tenfold increase or decrease in power. A signal strength of 1 milliwatt (mW) is 0 dBm, so a signal strength of .0000001 mW is 80 decibels less than 1 mW, which is -80 dBm.

Question: 76

A network technician is verifying that a customer successfully connected to the guest network after completing the captive portal. The network technician looks at the access tracker in ClearPass.
Which role should be seen when looking at the OUTPUT tab for the customer's session?

A. Guest authenticated

B. Captive portal login

C. Captive portal redirect

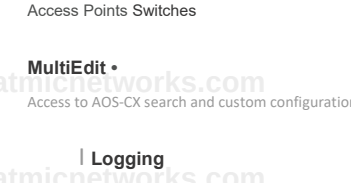
D. Guest logon

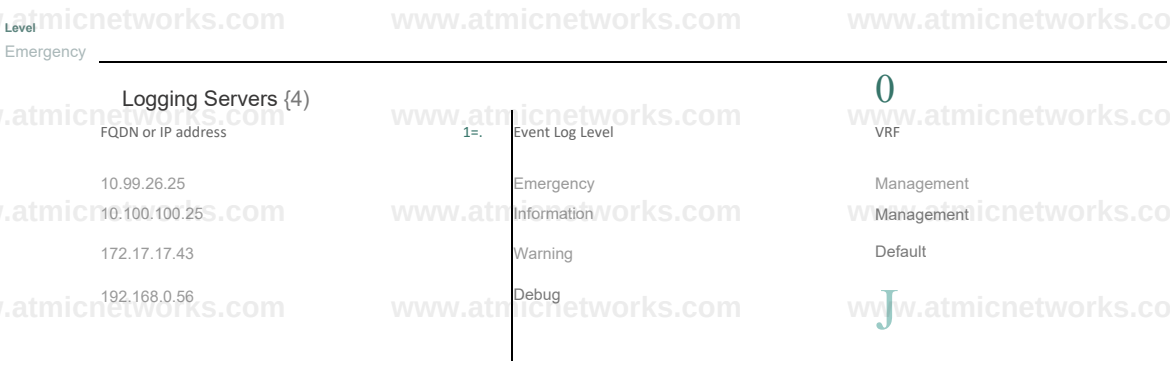
Answer: A

Explanation:
In the access tracker of ClearPass, after a customer successfully connects to a guest network through a captive portal, the OUTPUT tab should show a role indicating that the user is authenticated, such as "Guest authenticated." This role confirms that the user has passed the authentication process and has been granted access.

Question: 77

Refer to Exhibit.





Which server will receive the smallest quantity of data?

A. 172.17.17.43

B. 10.100.100.25

C. 10.99.26.25

D. 192.168.0.56

Answer: A

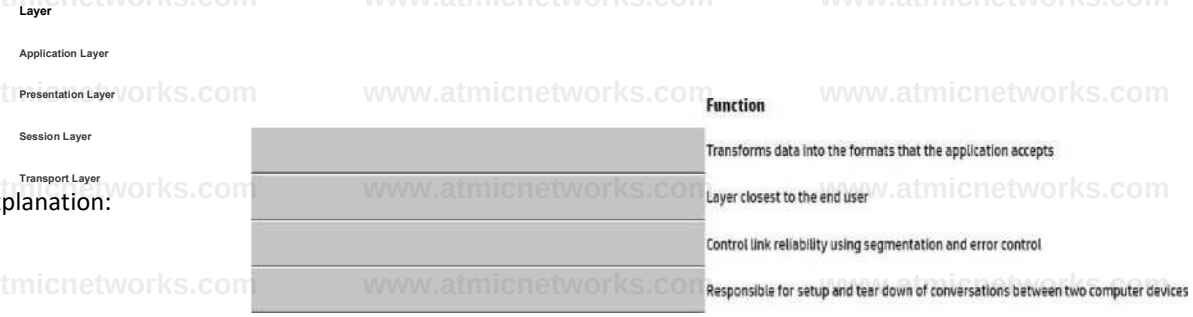
Explanation:

Based on the exhibit showing the logging server configurations, server 172.17.17.43 will receive the smallest quantity of data because it is set to the "Warning" event log level. This means it will only log events that are categorized as warnings or higher severity, which are typically less frequent than lower severity levels such as "Information," "Debug," or "Emergency."

Question: 78

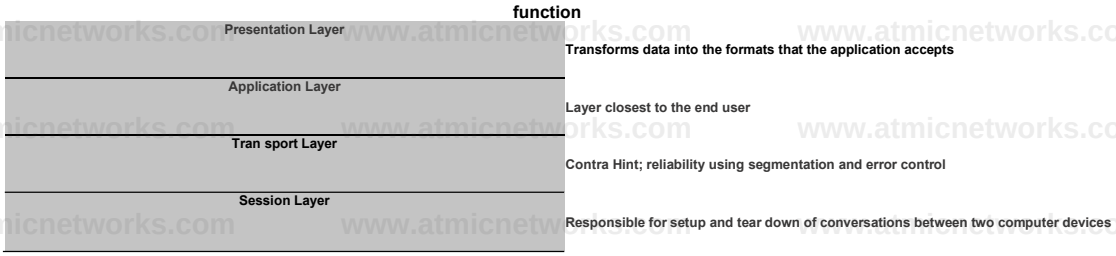
DRAG DROP

Match the Open Systems Interconnection (OSI) layer with its function.



Explanation:

Answer:



Question: 79

Which Aruba technology provides load balancing across radio bands and AP radios?

A. Aruba ESP

B. Aruba ClientMatch

C. Aruba AirWave

D. Aruba Central

Answer: B

Explanation:

Aruba ClientMatch is a technology that continuously monitors client behavior and automatically adjusts client connections to optimize Wi-Fi performance. This includes steering clients to the least congested access point and the best radio on the WLAN, which effectively provides load balancing

across different radio bands and AP radios.

Question: 80

A network technician is deploying "headless" devices in the warehouse at the HQ location. So far, an SSID with 802.1X has been configured. However, these new devices lack 802.1X support.

Which option would provide enhanced security for these devices?

A. WPA3-Personal

B. Multi-Preshared keys (mPSK)

C. WPA2-Enterprise

D. Opportunistic Wireless Encryption (OWE)

Answer: B

Explanation:

For "headless" devices that lack 802.1X support, Multi-Preshared Keys (mPSK) provide a more secure alternative to WPA2-Personal, which uses a single preshared key. mPSK allows for the assignment of unique PSKs to devices or groups of devices, which enhances security by not sharing a single PSK across multiple devices.

Question: 81

What is the recommended UXI monitoring solution in large logistic facilities?

A. Use a special ruggedized UXI sensor.

B. Use the UXI App on all handheld devices running on Windows CE.

C. Add a UXI sensor in every aisle of the logistic space.

D. Use the UXI App direct on Zebra scanning devices running on Android.

Answer: C

Explanation:

In large logistic facilities, to ensure comprehensive monitoring and performance analysis, it's recommended to place a User Experience Insight (UXI) sensor in every aisle. This allows for detailed and specific monitoring of network performance across the extensive coverage area of such facilities.

Question: 82

What describes Clearpass OnGuard? (Select two.)

A. Onguard assings an unique identity to each device.

B. It is used for the self-registration of guest devices.

C. OnGuard is an agent, running on client systems.

D. OnGuard is doing posture checks on client systems.

E. It is an intuitive portal for users to securely configure their devices.

Answer: CD

Explanation:
ClearPass OnGuard is a component of the ClearPass Policy Manager that performs health and security posture checks on devices to ensure they meet the organization's compliance requirements before allowing access to the network. It operates as an agent on client systems to perform these checks.

Question: 83

Based on the "show ip route" output on an Aruba CX 8325, what type of route is "10.20.0.0/22, vrf default via 10.1.1.1, [110/200]"?

A. connected

B. local

C. OSPF

D. static

Answer: C

Explanation:
The route "10.20.0.0/22, vrf default via 10.1.1.1, [110/200]" indicates that it is an OSPF route. This is evidenced by the administrative distance and metric "[110/200]" where 110 is the default administrative distance for OSPF routes.

Question: 84

A client connects to an Aruba AP in tunnel mode and is assigned to a VLAN based on the client's MAC address.
Which client VLAN assignment was configured?

A. Mixed

B. Static

C. Native VLAN

D. Dynamic

Answer: D

Explanation:

When a client connects to an Aruba AP in tunnel mode and is assigned to a VLAN based on the client's MAC address, this indicates a Dynamic VLAN assignment. The VLAN is determined dynamically at the time of authentication based on the client's credentials or attributes, such as its MAC address.

Question: 85

What is the ideal mounting position for a typical Aruba indoor AP?

A. Horizontal, below a suspended ceiling

B. Under a office desk

C. Horizontal, above a suspended ceiling

D. Vertical, at a wall

Answer: A

Explanation:

The ideal mounting position for a typical Aruba indoor AP is horizontally, below a suspended ceiling. This positioning takes advantage of the AP's antenna radiation pattern and helps provide optimal wireless coverage and performance within the indoor environment.

Question: 86

A network technician is testing a new SSID for a branch office. They are able to connect, get an IP address, and resolve DNS names. However, they are not able to browse the internet.

On the existing SSID at the branch, connectivity to the internet works as expected on the same VLAN as the new SSID. The wireless client should have received a new role to allow internet access.

What should the network technician verify to ensure both SSIDs function in a similar way?

A. Verify each SSID's authentication and encryption parameters are enabled and the same.

B. Verify that the implicit 'deny all' is the last entry in the firewall policies.

C. Verify the new SSID is broadcasting on all the APs at the branch office.

D. Verify the firewall policies assigned, making sure the rules are correct and ordered properly.

Answer: D

Explanation:

When a network technician encounters an issue where a new SSID does not allow internet access despite successful connectivity and DNS resolution, they should verify the firewall policies associated with the new SSID. The firewall policies must include rules that permit traffic to and from the internet and should be correctly ordered to ensure that they are applied as intended. Since the existing SSID functions correctly, comparing the firewall rules between the two can be a useful method of troubleshooting.

Question: 87

When does the 802.1x authentication process begin when connecting to a secured enterprise mode WLAN?

A. After the firewall policies are applied to the session

B. After the client completes 802.11 association

C. After the captive portal authentication completes

D. After the WPA 4-Way Handshake is completed

Answer: B

Explanation:
The 802.1x authentication process begins after the client device completes the 802.11 association with the access point but before the WPA 4-Way Handshake. This is part of the EAP (Extensible Authentication Protocol) process, which authenticates the device before allowing full network access.

Question: 88

DRAG DROP
Match the Open Systems Interconnection (OSI) layer with its comparable member of the TCP/IP stack. (Options may be used more than once.)

Answer:

Explanation:

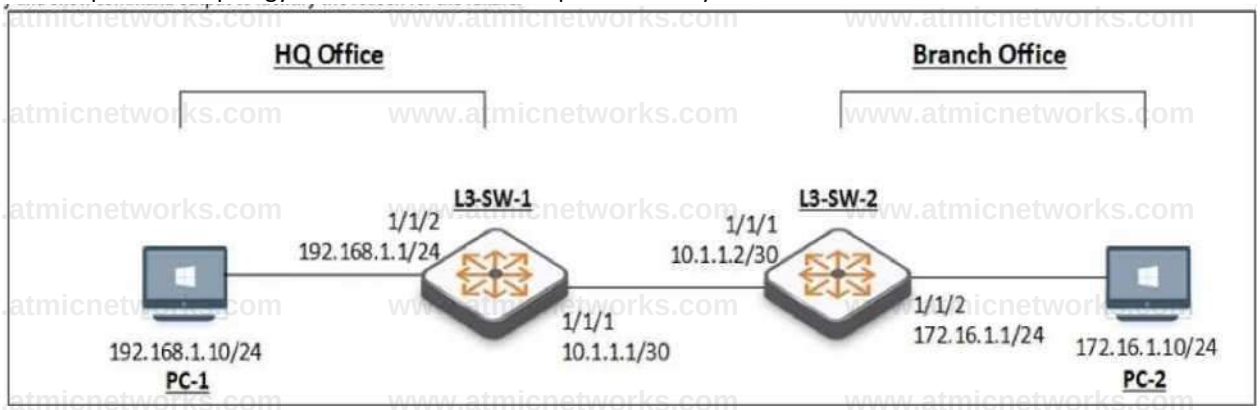
Answer Area

TCP/IP Network Interface	OSI Data Link
TCP/IP Network Interface	OSI Physical
TCP/IP Application	OSI Presentation
TCP/IP Application	OSI Session

Question: 89

You have been asked to troubleshoot failed connectivity between a local subnet in the HQ Office and a remote subnet in the Branch Office. PC1 is unable to ping PC2.

Use the provided topology and show command output to identify the reason for the failure:



L3-SW-1#SHOW IP INT BRIEF

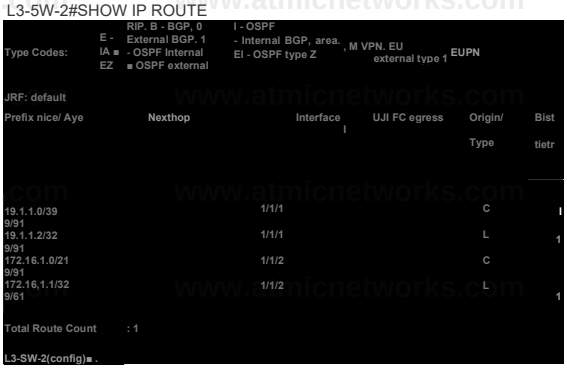
Interface	IP Address	Interface Status link/admin
1/1/1	10.1.1.1/30	up/up
1/1/2	192.168.1.1/24	up/up
1/1/3	No Address	down/down
1/1/4	No Address	down/down
1/1/5	No Address	down/down
1/1/6	No Address	down/down
1/1/7	No Address	down/down
1/1/8	No Address	down/down
1/1/9	No Address	down/down
1/1/10	No Address	down/down
1/1/11	No Address	down/down

L3-SW-2#SHOW IP INT BRIEF

Interface	IP Address	Interface Status link/admin
1/1/1	10.1.1.2/30	up/up
1/1/2	172.16.1.1/24	up/up
1/1/3	No Address	down/down
1/1/4	No Address	down/down
1/1/5	No Address	down/down
1/1/6	No Address	down/down
1/1/7	No Address	down/down
1/1/8	No Address	down/down
1/1/9	No Address	down/down
1/1/10	No Address	down/down
1/1/11	No Address	down/down

L3-SW-1#SHOW IP ROUTE

L3-5W-2#SHOW IP ROUTE



A. On Branch Office - L3-SW-2- There is no Layer 3 SVI configured in the correct subnet.

B. On HQ Office L3-SW-1 - There is no route to the Branch Office.

C. On HQ Office L3-SW-1 - The switch does not have a static default route to the internet.

D. On Branch Office L3-SW-2- The switch does not have a static route to the HQ Office Local Subnet.

Answer: D

Explanation:

Using the provided topology and show command output, it can be determined that L3-SW-2 in the Branch Office does not have a route to reach the subnet where PC1 resides (192.168.1.0/24 in the HQ Office). L3-SW-1 in the HQ Office has a route to the Branch Office subnet (172.16.1.0/24), but without the reciprocal route on L3-SW-2, traffic from the Branch Office will not be able to reach the HQ Office subnet, hence PC1 cannot ping PC2.

Question: 90

What is indicated by a flashing amber global status indicator LED on an Aruba CX6200M?

A. The switch has a recoverable fault.

B. Self-test is in progress.

C. The firmware image is corrupt.

D. The switch is booting the firmware image.

Answer: A

Explanation:

A flashing amber global status indicator LED on an Aruba CX6200M switch typically indicates that the switch has encountered a fault, but it is recoverable. This LED behavior serves as an alert to the network administrator that an issue needs to be addressed, but it does not necessarily mean that the switch is inoperable.

Question: 91

You are working with a pair of 6300M switches in a VSF stack. The switch has 48 SmartRate 5G ports, 2 SFP28 ports, and 2 SFP56 ports. Both SFP56 ports are used for stacking.

You need to provide an LACP connection to another identical stack with the maximum available bandwidth possible. What should you configure?

A. a 16-member LAG using 2 SFP28 ports and 6 SR5 ports on each switch

B. an eight-member LAG using 4 SR5 ports on each switch

C. an eight-member LAG using 2 SFP28 ports and 2 SR5 ports on each switch

D. a four-member LAG using 2 SFP28 ports on each switch

Answer: A

Explanation:
To provide an LACP connection with the maximum available bandwidth, one should configure a link aggregation group (LAG) using all available ports that can be used for data transfer. Since the SFP56 ports are used for stacking, the next best option is to use the 2 SFP28 ports and as many SmartRate 5G (SR5) ports as possible on each switch, which would allow for a 16-member LAG, with 2 SFP28 and 6 SR5 ports on each switch contributing to the LAG.

Question: 92

Which Protocol Data Unit (PDU) represents the network layer PDU?

A. PDU3 - Packet

B. PDU4 - Segment

C. PDU1 - Signal

D. PDU2 - Frame

Answer: A

Explanation:
In the context of the OSI model, the network layer is responsible for packet forwarding including routing through intermediate routers. Hence, the network layer PDU is known as a packet.

Question: 93

Which type of device type and group persona is required to manage a Microbranch environment?

A. ArubaOS 10 AP Group Persona

B. ArubaOS 10 Branch Gateway Group Persona

C. ArubaOS 8 AP Group Persona

D. ArubaOS 8 Branch Gateway Group Persona

Answer: B

Explanation:

In the context of Aruba networks, a Microbranch environment is managed using a group persona that aligns with the functionality required. ArubaOS 10 Branch Gateway Group Persona would be the correct device type and group persona for managing a Microbranch environment, as it would provide the necessary features and controls for branch networking requirements.

Question: 94

Which three channels can be used simultaneously in a 2.4GHz WLAN environment while avoiding any co-channel interference?

A. 1,6, 11

B. 1,5, 10

C. 3,6, 9

D. 2,7, 11

Answer: A

Explanation:
In a 2.4GHz WLAN environment, channels 1, 6, and 11 are recommended for use simultaneously to avoid co-channel interference because these channels do not overlap with each other. Each of these channels is separated by enough frequency space to ensure that the signals do not interfere, which is not the case with other channel combinations.

Question: 95

What change does a client make when it roams from one access point to another in a WLAN?

A. It changes the destination MAC address on its 802.11 frames.

B. It changes the SSID to match the SSID on the new access point.

C. It changes its default gateway to the IP of the new access point.

D. It changes its association with the new wireless controller's SSID.

Answer: A

Explanation:
When a client roams from one access point to another, it must change the destination MAC address on its 802.11 frames to match the new access point to which it is associated. The SSID does not change since it is typically consistent across an entire WLAN, and the default gateway remains the same as long as the client stays within the same IP subnet. The association to a new access point
involves updating the destination MAC address in the frames that the client sends.

Question: 96

A network technician at a branch office is connecting VoIP phones to a newly configured AOS-CX switch. Users are complaining that voice quality is not as good as at the corporate office. Further investigation
shows the local-priority value at the branch office is 1 while at the corporate office is 5.

What describes the issue regarding the default QoS behavior on the AOS-CX switch?

A. The QoS trust is set to DSCP by default, and the VoIP phone's local-priority value is mapped to 1.

B. The QoS trust is set to CoS by default, and the VoIP phone's local-priority value is mapped to 1.

C. The QoS trust is set to none by default, and each VoIP phone's local priority is configured for CoS map entry 1.

D. The QoS trust is set to none by default, and each VoIP phone's local priority is configured for CoS map entry 0.

Answer: C

Explanation:
In an AOS-CX switch, if the QoS trust mode is not configured, it is set to none by default. The VoIP phones will mark their traffic with a local-priority value, which, if the QoS trust mode is none, will correspond to CoS map entry 1 by default. The local-priority value of 1 at the branch office likely indicates that the traffic is not being prioritized correctly compared to the corporate office, where a local-priority of 5 suggests a higher level of prioritization for voice traffic.

Question: 97

What is a common use of LLDP for wireless access points?

A. testing the quality of the physical link between the access point and the switch

B. discovery of rogue access points

C. exchange of RF channel information with nearby access points

D. negotiation of PoE power level to be provided to the access point

Answer: D

Explanation:
LLDP (Link Layer Discovery Protocol) is commonly used by network devices, including wireless access points, to negotiate PoE (Power over Ethernet) power levels with the switch they are connected to. This allows the access point to communicate its power requirements to ensure it receives the necessary power for optimal operation.

Question: 98

A hacker has altered a user's 3-Way Handshake in order to gain access to their session.

Which security mechanism would intelligently deny this traffic?

A. Out-of-band management (00BM)

B. Stateless firewall

C. Access Control List (ACL)

D. Stateful firewall

Answer: D

Explanation:
A stateful firewall would intelligently deny traffic from a hacker attempting to alter a user's 3-Way Handshake to gain access to their session. Stateful firewalls keep track of the state of active connections and can recognize if an incoming packet is part of an established session. This allows them to detect and block unauthorized access attempts that do not match the known state of a connection.

Question: 99

What will perform a hard reset of an Aruba CX switch?

A. Press the reset button and hold the clear button while releasing the reset button for 5 seconds.

B. Press and hold the reset button for 5 seconds, then release.

C. Press the reset button and the clear button simultaneously.

D. Press the reset button three times.

Answer: B

Explanation:
Performing a hard reset on an Aruba CX switch typically involves pressing and holding the reset button for a specified amount of time, such as 5 seconds, and then releasing it. This action will initiate a reboot of the switch and return it to factory default settings, including the credentials.

Question: 100

You have physical access to an Aruba CX-Switch with unknown/lost credentials. What are the possible steps to rebuild the credentials? (Select two.)

A. Connect the switch via the console. Then, power cycle the switch.

B. Press and hold the clear button. Then, power-cycle the switch.

C. Press and hold the clear button. Then, press the reset button for 2 seconds and release both buttons.

D. Call Aruba support for a one-time password.

E. Use boot profile 0.

Answer: BE

Explanation:
To regain access to an Aruba CX switch when credentials are unknown or lost, one can press and hold the clear button, then power cycle the switch to reset the password. Additionally, using the boot profile 0 at the boot loader menu can be used to bypass the current startup configuration, which may include the unknown credentials.

Question: 101

What is used by network devices to send error and operational information related to IP communications?

A. Frame Check Sequence (FCS)

B. User Datagram Protocol (UDP)

C. Cyclic Redundancy Check (CRC)

D. Internet Control Message Protocol (ICMP)

Answer: D

Explanation:

ICMP (Internet Control Message Protocol) is used by network devices to send error and operational information related to IP communications. It is used to send messages like "destination unreachable" or "time exceeded" when there are issues in IP communication

Question: 102

What are two characteristics of ClientMatch? (Select two.)

A. It optimizes channels of an AP.

B. An algorithm to adjust RF patterns.

C. It is used to locate a client.

D. It is an Aruba patented technology.

E. It helps to move sticky clients to another AP.

Answer: DE

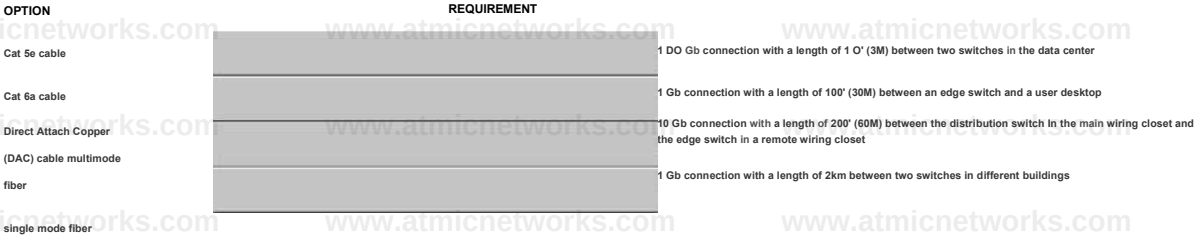
Explanation:

ClientMatch is an Aruba patented technology that helps to move sticky clients—clients that stay connected to an AP even when there are better APs available—to a more appropriate AP. This technology ensures that clients are always connected to the best available AP, optimizing both the client's performance and the overall performance of the wireless network.

Question: 103

DRAG DROP

Match the most cost-effective option for cabling each requirement. (All lengths indicate total cable length including patch cable(s), service loops, etc. where used.)



Answer:

Explanation:

Single mode
Cat 6a cable

Direct attach copper Multimode fiber Cat 5e cable