Vendor:HP

Exam Code:HPE6-A85

Exam Name: Aruba Certified Campus Access Associate

Version: Demo

QUESTION 1

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)

Correct 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 randomnumber generated by supplicant (a device that wants to access network resources, such as an STA) , AA Authenticator Address (AA) is MAC address of authenticator , SA Supplicant Address (SA) is MAC address of supplicant using Pseudo-Random Function (PRF). PTK consists of four subkeys: KCK Key Confirmation Key (KCK) is used for message integrity check KEK Key Encryption Key (KEK) is used for encryption key distribution TK Temporal Key (TK) is used for data encryption MIC Message Integrity Code (MIC) key The subkey that is specifically used for data encryption is TK Temporal Key (TK). TK is also known as Pairwise Transient Key (PTK). TK changes periodically during communication based on time or number of packets transmitted. The other options are not part of WPA Key Hierarchy because: PMK: PMK is not part of WPA Key Hierarchy, but rather an input for deriving PTK. KCK: KCK is part of WPA Key Hierarchy, but it is not used for data encryption, but rather for message integrity check. Nonce: Nonce is not part of WPA Key Hierarchy, but rather an input for deriving PTK.

References: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA_key_hierarchy_and_management
https://www.cwnp.com/wp- content/uploads/pdf/WPA2.pdf

QUESTION 2

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

Correct Answer: D

Explanation: The solid amber radio status LED on an Aruba AP Access Point (AP) Access Point (AP) is a device that connects wireless devices to a wired network using Wi-Fi or other wireless standards . APs act as transmitters and receivers of wireless signals and provide wireless coverage for a specific area . APs can operate in different modes such as root , repeater , bridge , mesh , etc . APs can also support different features such as security , QoS , roaming , load balancing , etc . APs can be standalone devices or managed by controllers or cloud services . APs can be verified by using commands such as show ap active , show ap database , show ap bss-table , etc . indicates that the radio is enabled in monitor or spectrum analysis mode. Monitor mode is a mode that allows the AP to scan all channels and collect information about wireless traffic, interference, rogue devices, etc. Spectrum analysis mode is a mode that allows the AP to scan all channels and collect information about RF Radio Frequency (RF) Radio Frequency (RF) is a term that refers to electromagnetic waves that have frequencies between 3 kHz and 300 GHz . RF waves are used for various purposes such as communication , broadcasting , radar , navigation , remote control , etc . RF waves can be modulated by changing their amplitude , frequency , or phase to encode information . RF waves can also be affected by various factors such as attenuation , reflection , refraction , diffraction , scattering , interference , noise , etc . RF waves can be measured by using devices such as spectrum analyzers , power meters , antennas , etc . environment, noise sources, channel utilization, etc. Both modes are useful for troubleshooting and optimizing wireless performance, but they disable normal data transmission and reception on the radio. The other options are not indicated by a solid amber radio status LED on an Aruba AP because: Not enough PoE is provided from the switch to power both radios of the AP: This option is false because not enough PoE Power over Ethernet (PoE) Power over Ethernet (PoE) is a technology that allows network devices to receive power and data over the same Ethernet cable . PoE eliminates the need for separate power sources and cables for devices such as IP phones , cameras , access points , etc . PoE is defined in IEEE 802.3af and IEEE 802.3at standards and supports different power classes and modes . PoE can be provided by switches or injectors that act as power sourcing equipment (PSE) and received by devices that act as powered devices (PD) . PoE can be verified by using commands suchas show power inline , show power-over-ethernet , debug ip device tracking , etc . is indicated by a blinking amber power status LED on an Aruba AP, not by a solid amber radio status LED. A blinking amber power status LED means that the AP is receiving insufficient power from the switch or injector and cannot operate normally. A solid green power status LED means that the AP is receiving sufficient power from the switch or injector and can operate normally. The radio is working in mesh mode: This option is false because the radio working in mesh mode is indicated by a solid green radio status LED on an Aruba AP, not by a solid amber radio status LED. A solid green radio status LED means that the radio is working in normal mode or mesh mode and can transmit or receive data on the assigned channel. Mesh mode is a mode that allows the AP to connect wirelessly to other APs and form a mesh network without requiring wired connections. The radio is working the 5 GHz band only: This option is false because the radio working in the 5 GHz band only is indicated by a solid blue radio status LED on an Aruba AP, not by a solid amber radio status LED. A solid blue radio status LED means that the radio is working in dual-band mode and can transmit or receive data on both 2.4 GHz and 5 GHz bands. References: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/ap-led- behavior.htm https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant- ug/troubleshooting/ap-monitor-mode.htm https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant- ug/troubleshooting/ap-spectrum-analysis.htm

---

QUESTION 3

Which authentication does Aruba\\'s Captive Portal use?

A. Layer 3 authentication

B. MAC authentication

C. 802.1x authentication

D. Layer 2 authentication

Correct 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. References:https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instan t-ug/captive-portal/captive-portal-auth.htm

---

QUESTION 4

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

Correct 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.

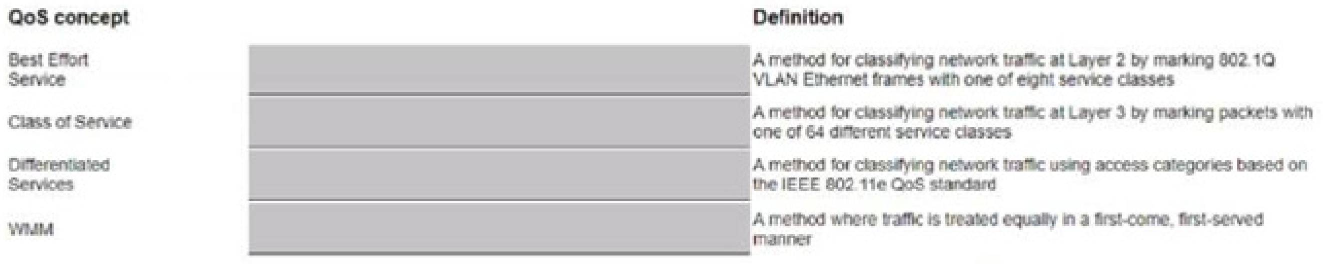
References: https://en.wikipedia.org/wiki/Rate_limiting https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx- noscg/qos/storm-control.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/dwrr.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx- noscg/qos/shaping.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/strict.htm

---

QUESTION 5

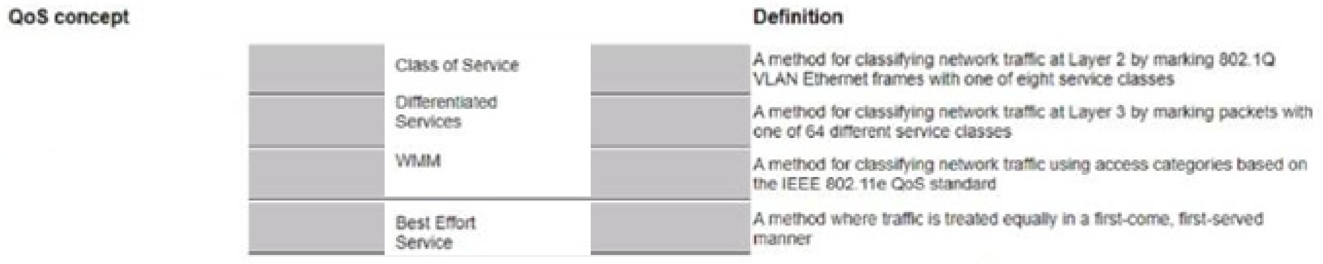
Match the appropriate QoS concept with its definition.

Select and Place:



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 802.11e QoS standard
WMM		A method where traffic is treated equally in a first-come, first-served manner

Correct Answer:



QoS concept		Definition
	Class of Service	A method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
	Differentiated Services	A method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes
	WMM	A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard
	Best Effort Service	A method where traffic is treated equally in a first-come, first-served manner

QUESTION 6

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

Correct 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.

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

QUESTION 7

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

Correct Answer: B

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

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

---

QUESTION 8

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)

Correct Answer: A

Explanation: The source that WPA3-Personal uses to generate a different Pairwise Master Key (PMK) each time a station connects to the wireless network is session-specific information (MACs and nonces). WPA3-Personal uses

Simultaneous Authentication of Equals (SAE) to replace PSK authentication in WPA2-Personal. SAE is a secure key establishment protocol that uses a Diffie-Hellman key exchange to derive a shared secret between two parties without

revealing it to an eavesdropper. SAE involves the following steps:

The station and the access point exchange Commit messages that contain their MAC addresses and random numbers called nonces.

The station and the access point use their own passwords and the received MAC addresses and nonces to calculate a shared secret called SAE Password Element (PE).

The station and the access point use their own PE and the received MAC addresses and nonces to calculate a shared secret called SAE Key Seed (KS). The station and the access point use their own KS and the received MAC addresses

and nonces to calculate a shared secret called SAE Key Confirmation Key (KCK).

The station and the access point use their own KCK and the received MAC addresses and nonces to calculate a confirmation value called SAE Confirm. The station and the access point exchange Confirm messages that contain their SAE

Confirm values.

The station and the access point verify that the received SAE Confirm values match their own calculated values. If they match, the authentication is successful and the station and the access point have established a shared secret called SAE

PMK.

The SAE PMK is different for each session because it depends on the MAC addresses and nonces that are exchanged in each authentication process. The SAE PMK is used as an input for the 4-way handshake that generates the Pairwise

Temporal Key (PTK) for encrypting data frames.

The other options are not sources that WPA3-Personal uses to generate a different PMK each time a station connects to the wireless network because:

Opportunistic Wireless Encryption (OWE): OWE is a feature that provides encryption for open networks without requiring authentication or passwords. OWE uses a similar key establishment protocol as SAE, but it does not generate a PMK.

Instead, it generates a Pairwise Secret (PS) that is used as an input for the 4-way handshake that generates the PTK.

Simultaneous Authentication of Equals (SAE): SAE is not a source, but a protocol that uses session-specific information as a source to generate a different PMK each time a station connects to the wireless network. Key Encryption Key (KEK): KEK is not a source, but an output of the 4-way handshake that generates the PTK. KEK is used to encrypt group keys that are distributed by the access point.

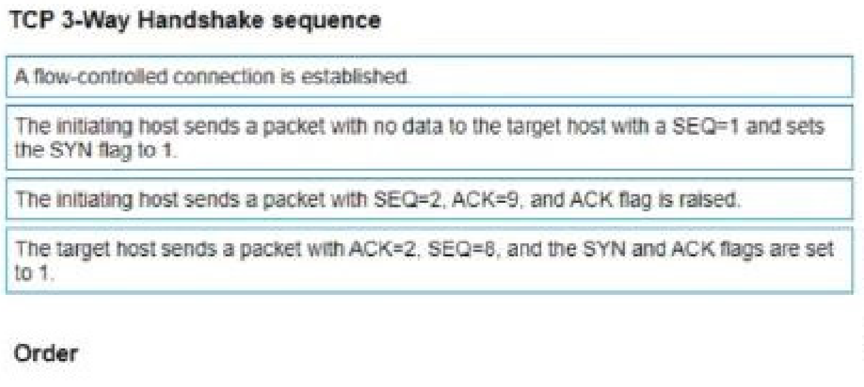
References: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e https://www.wi-fi.org/file/wi- fi-alliance-unlicensed-spectrum-in-the-us https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access- points/wpa3-dep-guide-og.html https://info.support.huawei.com/info- finder/encyclopedia/en/WPA3.html https://rp.os3.nl/2019-2020/p99/presentation.pdf

---

QUESTION 9

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

Select and Place:



TCP 3-Way Handshake sequence

A flow-controlled connection is established.

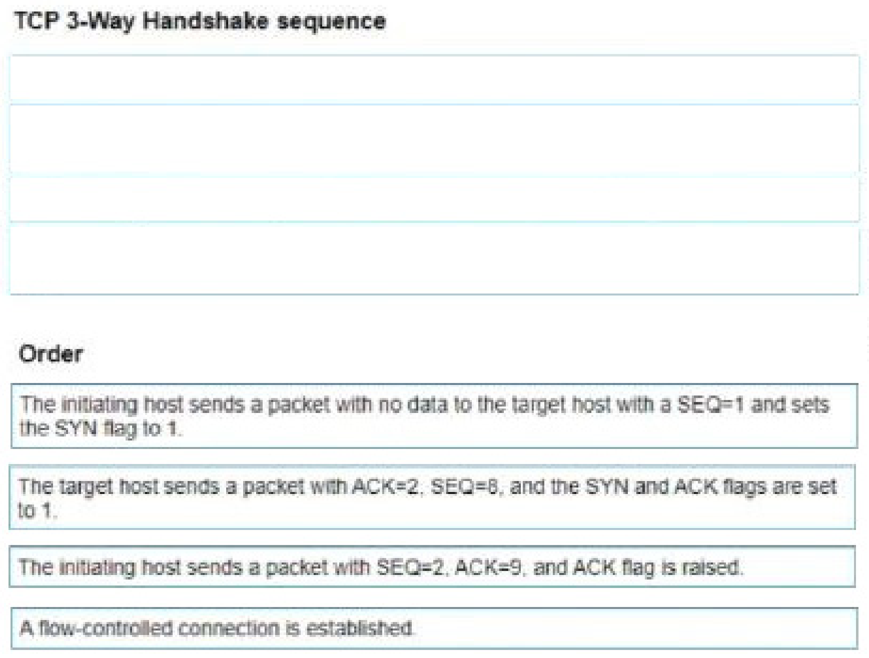
The initiating host sends a packet with no data to the target host with a SEQ=1 and sets the SYN flag to 1.

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.

Order

Correct Answer:



TCP 3-Way Handshake sequence

Order

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

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

The initiating host sends a packet with SEQ=2, ACK=9, and ACK flag is raised.

A flow-controlled connection is established.

QUESTION 10

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

Correct 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.

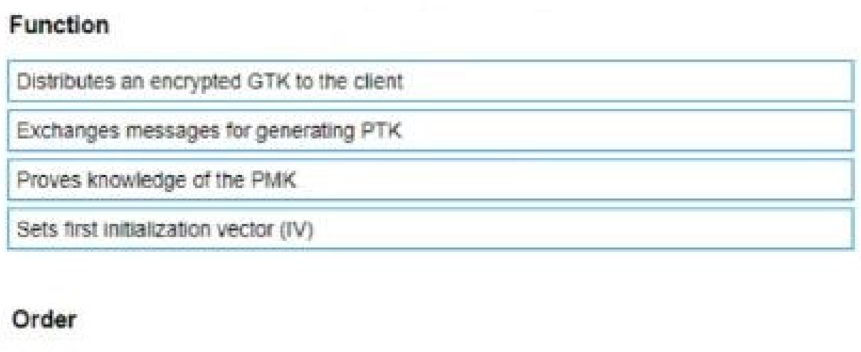
References: https://www.arubanetworks.com/techdocs/AOS- CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm

---

QUESTION 11

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

Select and Place:

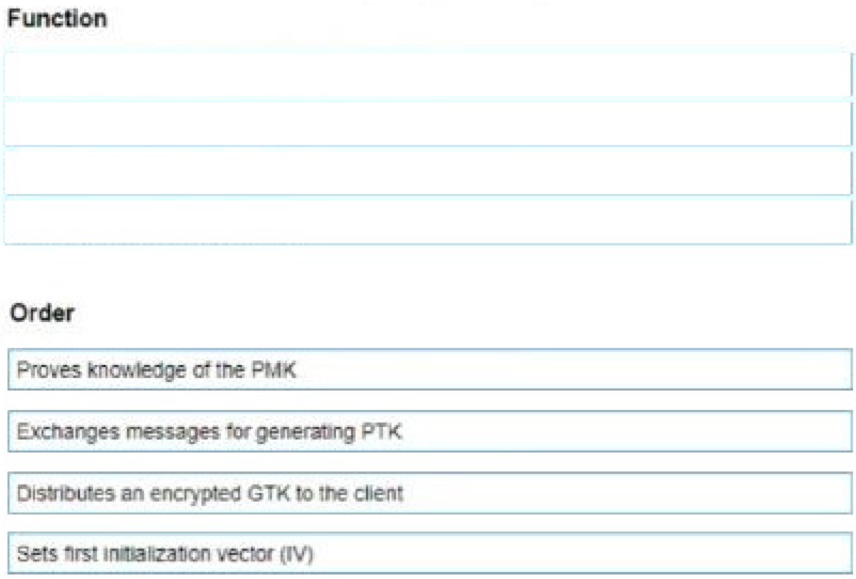


Function

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

Order

Correct Answer:



Function

Order

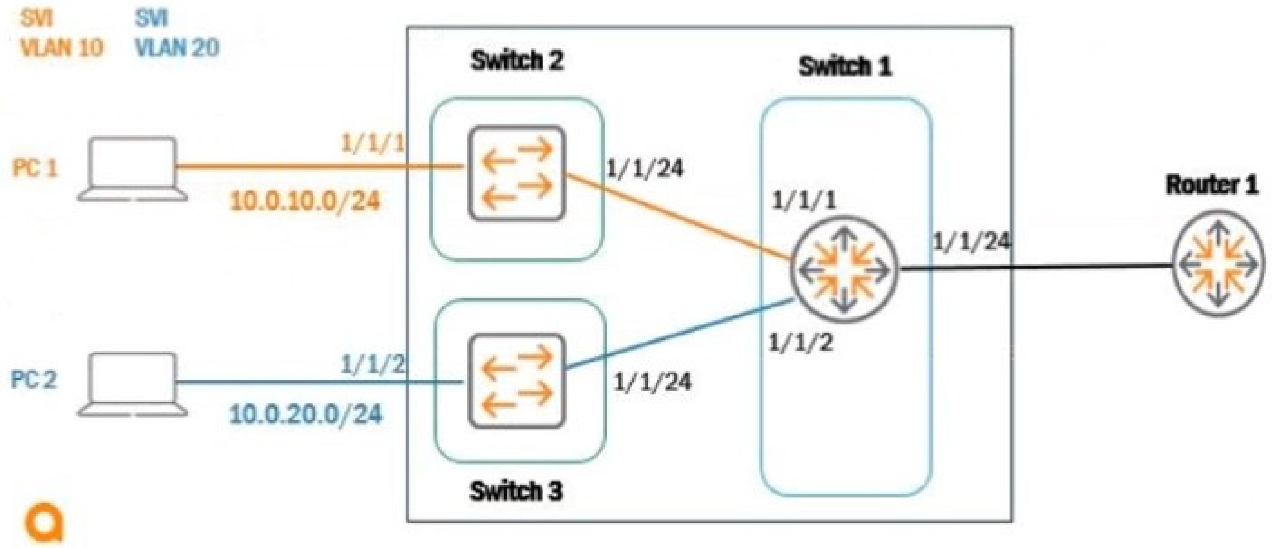
Proves knowledge of the PMK

Exchanges messages for generating PTK

Distributes an encrypted GTK to the client

Sets first initialization vector (IV)

QUESTION 12



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

Correct Answer: C

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

References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/lldp/lldp.htm