Free Questions for HPE7-A01 by certscare

Shared by Parrish on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Your customer is having issues with Wi-Fi 6 clients staying connected to poor-performing APs when a higher throughput APs are closer. Which technology should you implement?

Options:

A- Clearpass

B- ClientMatch

C- Airmatch

D- ARM

Answer:

B

Explanation:

Wi-Fi 6 is an industry certification for products that support the new wireless standard 802.11ax, also known as "high-efficiency wireless". Wi-Fi 6 offers increased capacities, improved resource utilization and higher throughput speeds than previous standards.

Option B: ClientMatch

This is because option B shows how to use ClientMatch to optimize the wireless performance of Wi-Fi 6 clients on a UniFi network.ClientMatch is a feature that uses machine learning to analyze the traffic patterns of each client and assign them to the best available AP based on their location, device type, and network conditions2.

Therefore, option B is the best technology to implement for your customer's issue.

1: https://help.ui.com/hc/en-us/articles/221029967-UniFi-Network-Optimizing-Wireless-Connectivity2: https://help.ui.com/hc/en-us/articles/360012947634-UniFi-Network-Optimizing-Wireless-Speeds

Question 2

Question Type: MultipleChoice

When configuring UBT on a switch what will happen when a gateway role is not specified?

Options:

A- The switch will put the client on the access VLAN

B- The gateway will assign a default role to the client

C- The switch will assign the default deny role to the client.

D- The gateway will send back the deny role to the client.

Answer:

A

Explanation:

According to the Aruba Documentation Portal1, user-based tunneling (UBT) is a feature that uses GRE to tunnel ingress traffic on a switch interface to a gateway for further processing. UBT enables a switch to provide a centralized security policy, using per-user authentication and access control to ensure consistent access and permissions.

Option A: The switch will put the client on the access VLAN

This is because option A shows how UBT works on an Aruba switch. When a device connects to the network, it is authenticated using either MAC Authentication or 802.1X and triggers an enforcement policy from ClearPass, which contains an enforcement profile with a user role configuration. The user role can be assigned locally on the switch or on ClearPass as part of an enforcement profile.The user role determines the VLAN that the device belongs to and the access policies that apply to it23.

Therefore, option A is correct.

1: https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-ubt.htm2: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html3: https://community.arubanetworks.com/viewdocument/?DocumentKey=c740df4e-3e26-4cc5-9126-355a18709c44&CommunityKey=2fd943a6-8898-4dbe-915f-4f09e4d3c317&tab=librarydocuments

Question 3

Question Type: MultipleChoice

What does the 802.3bz standard describe?

Options:

A- 2.5Gb and 5Gb Ethernet ports

B- 60 W and 90W PoE

C- AP directed roaming between APs

D- 60 GHz P2P Wi-Fi

Answer:

A

Explanation:

802.3bz is a standard for Ethernet over twisted pair at speeds of 2.5 and 5 Gbit/s. These use the same cabling as the ubiquitous Gigabit Ethernet, yet offer higher speeds. The resulting standards are named 2.5GBASE-T and 5GBASE-T.

Option A: 2.5Gb and 5Gb Ethernet ports

This is because option A shows how to identify the speed of an Ethernet port based on its name and the standard it supports.A port that supports 2.5GBASE-T or 5GBASE-T is a multi-gigabit port that can operate at speeds of up to 2.5 Gbit/s or 5 Gbit/s over twisted pair cables23.

Therefore, option A is correct.

1: https://en.wikipedia.org/wiki/2.5GBASE-T_and_5GBASE-T2: https://kb.netgear.com/000049004/What-is-Multi-Gigabit-Ethernet-and-how-can-I-benefit-from-using-NETGEAR-Multi-Gigabit-Ethernet-Switches-in-my-network3: https://arstechnica.com/gadgets/2016/09/5gbps-ethernet-standard-details-8023bz/

Question 4

Question Type: **MultipleChoice**

A customer is concerned about me unprotected traffic between an AOS-CX switch and a gateway, running on AOStO. What is a feasible option to protect this traffic?

Options:

A- Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway

B- Implement an MD5 HMAC function lo protect PAPI between the AOS-CX switches and the gateway

C- Implement a GRE tunnel to protect PAPI between the AOS-CX switches and the gateway

D- no action is needed, an RSA certificate already encrypts the traffic

Answer:

A

Explanation:

According to the Aruba Documentation Portal1, PAPI (Port Aggregation Protocol) is a protocol that allows multiple physical ports to be aggregated into a single logical port for increased bandwidth and performance. PAPI can be used between AOS-CX switches and gateways, or between AOS-CX switches and other devices.

Option A: Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway

This is because option A shows how to implement an IPSec tunnel between two devices using the interface command and the ipsec command.An IPSec tunnel can provide encryption and authentication for PAPI traffic between two devices, such as an AOS-CX switch and a gateway2.

Therefore, option A is a feasible option to protect this traffic.

I hope this helps you. If you need more information, please let me know.

1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7727/Content/Chp_prev_traf_loss/Act_gtw_act_fwd/act-gat-ove-vsx-10.htm2: https://community.arubanetworks.com/blogviewer?blogkey=989fc43a-e0df-42db-9c0b-f96d6565a1fa

Question 5

Question Type: **MultipleChoice**

Which statements are true regarding a VXLAN implementation on Aruba Switches? (Select two.)

Options:

A- MTU size must be increased beyond the default

B- VNIs encapsulate and decapsulate VXLAN traffic

C- VTEPs encapsulate and decapsulate VXLAN traffic

D- They are only available for datacenter switches (CX 8k, 9k,10k)

E- All Aruba CX switches support VXLAN.

Answer:

A, B

Explanation:

Option A: MTU size must be increased beyond the default

This is because option A shows how to configure the MTU size for VXLAN tunnels on Aruba switches using the interface command and the vxlan command.The MTU size must be increased beyond the default value of 1500 bytes to accommodate the VXLAN header and payload2.

Therefore, option A is true regarding a VXLAN implementation on Aruba switches.

Option B: VNIs encapsulate and decapsulate VXLAN traffic

This is also true regarding a VXLAN implementation on Aruba switches. VNIs are used to encapsulate and decapsulate VXLAN traffic between two devices, such as a switch and a server.VNIs are also used to map VXLAN tunnels to overlay networks3.

Therefore, option B is also true regarding a VXLAN implementation on Aruba switches.

VXLAN is a Layer 2 encapsulation technology that substitutes the usage of VLAN numbers to label Ethernet broadcast domains with VXLAN numbers. VXLAN supports 224 Ethernet broadcast domains or VXLAN numbers. A VXLAN number ID is referred to as VNI. There is a one-to-one relationship between an Ethernet broadcast domain and a VNI. A single Ethernet broadcast domain can't have more than one VNI.

Question 6

Question Type: **MultipleChoice**

You are building a configuration in Central that will be used for a standardized network design for small sites for your company, you want to use GUI configuration for gateways and Aps, while template configuration for switches. You need to align with Aruba best practices.

Which set of actions will satisfy these requirements?

Options:

A- Create one group in Central for switches a second group for APs. and a third group for gateways Create a unique site for each location, and assign devices to the appropriate site.

B- Create one group in Central for switches and a second group for APs and gateways. Create a unique site for each location, and assign devices to the appropriate site.

C- Create a single group in Central. Create a unique site for each location, and assign devices to the appropriate site.

D- Create a single group in Central. Create a unique site for each type of device, and assign devices to the appropriate site.

Answer:

C

Explanation:

This is because option C shows how to create a single group in Central with different configuration methods defined for each device type. For example, you can create a group with the name Group1, and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (Group1). If a device type in the group is marked for template-based configuration method, the group name is prefixed with TG (TG Group1).You can use Group1 as the group ID for workflows such as user management, monitoring, reports, and audit trail2.

https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/abt-groups.htm2:
https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/groups.htm

Question 7

Question Type: **MultipleChoice**

For an Aruba AOS10 AP in mixed mode, which factors can be used to determine the forwarding role assigned to a client? (Select two.)

Options:

A- Client IP address

B- 802.1X authentication result

C- Client MAC address

D- Client SSID

E- Client VLAN

Answer:

A, D

Explanation:

Client IP address: This factor can be used to determine if the client is on the same VLAN as the AP or not. If the client IP address is on the same VLAN as the AP, then the client traffic is bridged locally.If the client IP address is on a different VLAN than the AP, then the client traffic is forwarded to the gateway cluster through a secure tunnel12.

Client VLAN: This factor can be used to determine if the client belongs to a specific VLAN or not.If the client belongs to a specific VLAN, then the client traffic is forwarded to that VLAN based on its IP address and security profile12.

Question 8

Question Type: MultipleChoice

You are deploying Aruba CX 6300's with the customers requirement to only allow one (1) VoIP phone and one (1) device.

The following local role gets assigned to the phone

port-access rote VoIP device-traffic-class voice

What set of commands best fits this requirement?

Options:

A- interface 1/1/1
aaa authentication port-access client-limit 2
aaa authentication port-access auth-mode client-mode

B- interface 1/1/1
aaa authentication port-access auth-mode multi-domain

C- interface 1/1/1
aaa authentication port-access client-limit multi-domain 2 aaa authentication port-access auth-mode multi-domain

D- interface 1/1/1
aaa authentication port-access client-limit 1
aaa authentication port-access auth-mode device-mode

Answer:

C

Explanation:

Aruba CX 6300 switches support various features to control the port access for different types of devices, such as client mode, device mode, and multidomain mode. These features can help limit the number of clients that can connect to a port and prevent unauthorized devices from accessing the network.

This is because option C shows how to configure the client limit and the auth-mode for a specific port using the interface command and the aaa authentication port-access command. The client limit specifies the maximum number of clients that can connect to a port. The auth-mode specifies the authentication mode for the port.In this case, option C sets both parameters to multi-domain mode, which allows only one voice device and one data device to be authenticated on a port

https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm2: https://www.arubanetworks.com/products/switches/6300-series/3: https://www.arubanetworks.com/techdocs/AOS-CX/10.11/HTML/security_6200-6300-6400/Content/Chp_Port_acc/Port_acc_gen_cmds/aaa-aut-por-acc-aut-mod-fl-109.htm

Question 9

Question Type: **MultipleChoice**

A customer has a site with 200 AP-515 access points 75AP-565 access points installed. The customer is rolling out new mobile phones with Wi-Fi-calling. 802.1X is in use for authentication

What should be enabled to ensure the best roaming experience?

Options:

A- 802.1X

B- 802. 11r

C- 802.11W

D- 802 .11h

Answer:

A

Explanation:

https://www.howtogeek.com/794724/what-is-wi-fi-calling/2: https://www.networkcomputing.com/networking/your-network-optimized-wifi-calling3: https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm

Wi-Fi calling is a feature that allows you to make or receive voice calls over Wi-Fi instead of cellular network. Wi-Fi calling can provide better voice quality and reliability in areas with poor or no cellular coverage.

Question 10

Question Type: MultipleChoice

A company recently upgraded its campus switching infrastructure with Aruba 6300 CX switches. They have implemented 802.1X authentication on edge ports where laptop and IoT devices typically connect An administrator has noticed that for PoE devices the pons are delivering the maximum wattage instead of what the device actually needs Upon connecting the IoT devices, the devices request their specific required wattage through information exchange

Options:

A- Concerned about this waste of electricity, what should the administrator implement to solve this problem?

B- Enable AAA authentication to exempt LLDP and/or CDP information

C- Globally enable the QoS trust setting for LLDP and/or CDP

D- Create device profiles with the correct power definitions.

E- implement a classifier policy with the correct power definitions.

Answer:

D

Explanation:

According to the Aruba Documentation Portal1, the Aruba 6300 CX switches support various features to control the PoE devices on specific ports, such as device profiles and classifier policies. These features can help reduce the power consumption and improve the performance of the PoE devices.

1: https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm2: https://www.arubanetworks.com/products/switches/6300-series/3: https://docs.samsungknox.com/admin/knox-manage/configure/profile/configure-profile-policies/configure-profile-policies-by-device-platform/