HPE7-A01$^{\text{Q\&As}}$

Aruba Certified Campus Access Professional

Pass HP HPE7-A01 Exam with 100% Guarantee

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

What is used to retrieve data stored in a Management Information Base (MIS)?

A. SNMPv3

B. DSCP

C. TLV

D. CDP

Correct Answer: A

Explanation: The correct answer is A. SNMPv3.

SNMPv3 is a protocol that is used to retrieve data stored in a Management Information Base (MIB), which is a database of managed objects in a network. SNMPv3 provides security and access control features that are not available in earlier

versions of SNMP. SNMPv3 can also use encryption to protect the data from unauthorized access or modification.

According to the Aruba Certified Professional ?Campus Access document1, one of the skills that this certification validates is:

Implement and Analyze the output from common network monitoring tools The document also mentions that the candidate should have a distinguished understanding of different protocols across vendors, which implies that they should be

familiar with SNMPv3 and how it can be used to access MIB data.

QUESTION 2

Which feature allows the device to remain operational when a remote link failure occurs between a Gateway cluster and a RADIUS server that is either in the cloud or a datacenter?

A. MAC caching

B. MAC Authentication

C. Authentication survivability

D. Opportunistic key caching

Correct Answer: C

Explanation: Authentication survivability is a feature that allows the device to remain operational when a remote link failure occurs between a Gateway cluster and a RADIUS server that is either in the cloud or a datacenter. Authentication survivability enables the Gateway cluster to cache successful authentication requests from the RADIUS server and use them to authenticate clients when the RADIUS server is unreachable. Authentication survivability also allows clients to use MAC caching or MAC authentication bypass (MAB) methods to access the network when the RADIUS server is down. References: https://www.arubanetworks.com/assets/tg/TG_AuthSurvivability.pdf

QUESTION 3

What are two advantages of splitting a larger OSPF area into a number of smaller areas? (Select two)

A. It extends the LSDB

B. It increases stability

C. it simplifies the configuration.

D. It reduces processing overhead.

E. It reduces the total number of LSAs

Correct Answer: BD

Explanation: Splitting a larger OSPF area into a number of smaller areas has several advantages for network scalability and performance. Some of these advantages are: It increases stability by limiting the impact of topology changes within an area. When a link or router fails in an area, only routers within that area need to run the SPF algorithm and update their routing tables. Routers in other areas are not affected by the change and do not need to recalculate their routes. It reduces processing overhead by reducing the size and frequency of link-state advertisements (LSAs). LSAs are packets that contain information about the network topology and are flooded within an area. By dividing a network into smaller areas, each area has fewer LSAs to generate, store, and process, which saves CPU and memory resources on routers. It reduces bandwidth consumption by reducing the amount of routing information exchanged between areas. Routers that connect different areas, called area border routers (ABRs), summarize the routing information from one area into a single LSA and advertise it to another area. This reduces the number of LSAs that need to be transmitted across area boundaries and saves network bandwidth. References: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-pathfirst- ospf/7039-1.html https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first- ospf/13703-8.html

QUESTION 4

You are setting up a customer\\'s 15 headless IoT devices that do not support 802.1X. What should you use?

A. Multiple Pre-Shared Keys (MPSK) Local

B. Clearpass with WPA3-PSK

C. Clearpass with WPA3-AES

D. Multiple Pre-Shared Keys (MPSK) with WPA3-AES

Correct Answer: A

Explanation: MPSK Local is a feature that can be used to set up 15 headless IoT devices that do not support 802.1X authentication. MPSK Local allows the switch to automatically generate and assign unique pre-shared keys for devices based on their MAC addresses, without requiring any configuration on the devices or an external authentication server. The other options are incorrect because they either require 802.1X authentication, which is not supported by the IoT devices, or WPA3 encryption, which is not supported by Aruba CX switches. References:
https://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-ch05.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01- ch06.html

QUESTION 5

A company deployed Dynamic Segmentation with their CX switches and Gateways After performing a security audit on their network, they discovered that the tunnels built between the CX switch and the Aruba Gateway are not encrypted. The company is concerned that bad actors could try to insert spoofed messages on the Gateway to disrupt communications or obtain information about the network.

Which action must the administrator perform to address this situation?

A. Enable Secure Mode Enhanced

B. Enable Enhanced security

C. Enable Enhanced PAPI security D. Enable GRE security

Correct Answer: C

Explanation: PAPI is the protocol that is used to establish tunnels between the CX switch and the Aruba Gateway for Dynamic Segmentation1. By default, PAPI uses a simple checksum to verify the integrity of the messages, but it does not encrypt the payload2. This could expose the network to spoofing or replay attacks by malicious actors. To address this situation, the administrator must enable Enhanced PAPI security, which uses AES-256 encryption and HMAC-SHA1 authentication to protect the tunnel traffic2. Enhanced PAPI security can be enabled on the CX switch by using the command system papi enhanced- security enable3. This will ensure that the tunnels built between the CX switch and the Aruba Gateway are encrypted and authenticated.