Free Questions for HPE6-A73 by ebraindumps

Shared by Mcintyre on 05-09-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

How does PIM build the IP multicast routing table to route traffic between a multicast source and one or more receivers9

Options:

A) It uses IGMP and calculates a shortest path tree (SPT).

B) It uses the shortest path first (SPF) algorithm derived from link state protocols.

C) It uses the Bellman-Ford algorithm derived from distance vector protocols

D) It uses the unicast routing table and reverse path forwarding (RPF)

Answer:

D

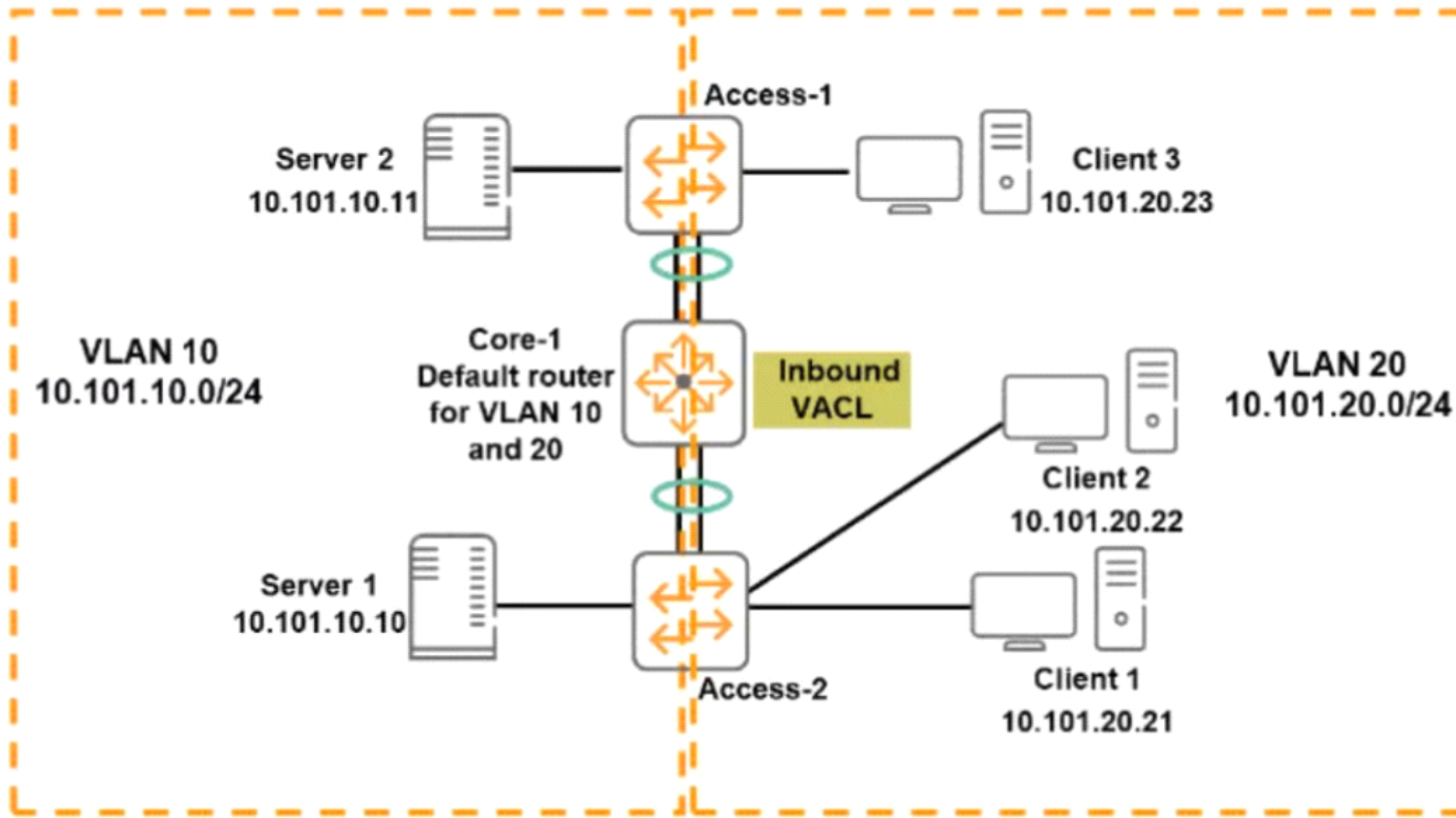# Question 2

Refer to the exhibit.

Access-1

Server 2
10.101.10.11

Client 3
10.101.20.23

VLAN 10
10.101.10.0/24

Core-1
Default router
for VLAN 10
and 20

Inbound
VACL

VLAN 20
10.101.20.0/24

Client 2
10.101.20.22

Server 1
10.101.10.10

Client 1
10.101.20.21

Access-2

The ACL configuration defined on Core-1 is as follows:

```
Core-1(config)# access–list ip example
Core-1(config-acl-ip)# permit ip 10.101.20.21/32 any eq 23
Core-1(config-acl-ip)# permit ip 10.101.20.21/32 eq 23 any
Core-1(config-acl-ip)# exit
Core-1(config)# vlan 20
Core-1(config-if)# apply access-list example in
```

if telnet was being used which device connection would he permitted and functional in both directions? (Select two)

Options:

A) Server 2 to Client 2

B) Client 1 to Client 2

C) Server 1to Client 1

D) Client 1 to Client 3

E) Client 3 to Client 2

Answer:

B, C

Question 3

Examine the following ACL rule policies:

* Permit traffic from 10.2.2.1 through 10.2.2.30 to anywhere

* Permit traffic from 10 2.2 40 through 10 2 2 55 to anywhere

* Deny all others

Based on this policy, place the following ACL rule statements in the correct order to accomplish the above filtering policy.

Options:

A) deny ip 10 ,2.2.31 255.255.255.255 any
permit ip 10 2 2 40 255 255 255 248 any
deny ip 10 2.2.32 255 255.255.224 any
permit ip 10 2 2 48 255 255 255.248 any
permit tp 10.2.2.0 255.255.255.192 any

B) deny ip 10 2 2.31 255 255.255.255 any
permit ip 10,2.2 40 255 255 255.248 any
permit ip 10.2.2.48 255.255.255.248 any
deny ip 10 2 2.32 255 255 255 224 any

permit ip 10.2.2.0 255.255.255.192 any

C) permit ip 10 2 2 40 255 255 255 248 any

permit ip 10 2.2 48 255 255 255.248 any

permit ip 10 2.2 0 255 255.255.192 any

deny ip 10.2.2.31 255.255.255.255 any

deny ip 10 2 2 32 255 255 255 224 any

D) denv ip 10 2 2.31 255 255.255.255 any

deny ip 10 2.2.32 255 255.255.224 any

permit ip 10 2 2 40 255 255 255 248 any

permit ip 10.2.2 48 255 255 255.248 any

permit ip 10 2.2 0 255 255 255.192 any

Answer:

B

Question 4

An administrator is replacing the current access switches with AOS-CX switches. The access layer switches must authenticate user and networking devices connecting to them. Some devices support no form of authentication and some support S02 1X Some ports have a VoIP phone and a PC connected to the same port where the PC is connected to the data port of the phone and the phone's LAN port is

connected to the switch.

Which statement is correct about this situation?

Options:

A) 8G2.1X must be configured to work in fallback mode

B) Device mode should be implemented.

C) Device fingerprinting is required for authentication.

D) The client-limit setting for port access needs to be changed

Answer:

D

Question 5

Question Type: MultipleChoice

An administrator creates an ACL rule with both the "count" and "log'; option enabled What is correct about the action taken by an AOS-CX switch when there is a match on this rule?

Options:

A) The total in the u\og' record and the count could contain different rule matching statistics

B) Logging will not include certificate and TLS events but counting will

C) By default a summarized log is created every minute with a count of the number of matches.

D) The 'count' and log' options are processed by the AOS-CX switches hardware ASIC

Answer:

D

Question 6

Question Type: MultipleChoice

A network engineer is examining NAE graphs from the Dashboard but notices that the time shown in the graph does not represent the current time The engineer verifies that the AOS-CX switch is configured for NTP and is successfully synchronized. What should be done to fix this issue?

Options:

A) Ensure NetEdit and the AOS-CX switch are synchronized to the same NTP server.

B) Enable trust settings for the AOS-CX switch's SSL certificate

C) Ensure the engineers web browser is configured for the same timezone as the AOS-CX switch

D) Ensure the engineers PC is synchronized to the same NTP server as the AOS-CX switch

Answer:

D

Question 7

Question Type: **MultipleChoice**

A company has implemented 802 1X authentication on AOS-CX access switches, where two ClearPass servers are used to implement AAA Each switch has the two servers defined A network engineer notices the following command configured on the AOS'CX switches:

radius-server tracking user-name monitor password plaintext arubal23

What is the purpose of this configuration?

Options:

A) Define the account to implement change of authorization.

B) Speed up the AAA authentication process

C) implement replay protection for AAA messages

D) Define the account to implement downloadable user roles

Answer:

B

Question 8

Question Type: **MultipleChoice**

Examine the output from an AOS-CX switch implementing a dynamic segmentation solution involving downloadable user roles:

```
Switch# show port-access role clearpass

Role Information:

Name : icxarubadur_employee-3044-2
Type : clearpass
Status: failed, parsing_failed

        Reauthentication Period                    :
        Authentication Mode                        :
        Session Timeout                            :
```

The downloadable user roles are not being downloaded to the AOS-CX switch Based on the above output , what is the problem?

Options:

A) There is a date/time issue between the ClearPass server and the switch.

B) The certificate that ClearPass uses is invalid

C) DNS fails to resolve the ClearPass servers FQDN.

D) The AOS-CX swicth does not have the ClearPass certificate involved.

Answer:

C

Question 9

What is correct regarding rate limiting and egress queue shaping on AOS-CX switches'?

Options:

A) Only a traffic rate and burst size can be defined for a queue

B) Rate limiting and egress queue shaping can be used to restrict inbound traffic.

C) Rate limiting and egress queue shaping can be applied globally .

D) Limits can be defined only for broadcast and multicast traffic

Answer:

A

Question 10

A network administrator is implementing NAE on AOS-CX switches. When attempting to create an agent on a particular switch, the agent appears in the NAE Agents panel with a red triangle error symbol and a status of "Unknown".

What is the cause of this issue?

Options:

A) The number of scripts or agents has exceeded the hardware's capabilities.

B) The administrator does not have the appropriate credentials to interact with NAE.

C) The RESTful API has not been enabled on the AOS-CX switch.

D) A connectivity issue exists between NAE and the AOS-CX switch

Answer:

A

Question 11

Question Type: **MultipleChoice**

Examine the configuration performed on newly deployed AOS-CX switches;

```
Switch(config)# radius-server host cppm key plaintext aruba123 vrf mgmt
Switch(config)# aaa authentication port-access dot1x authenticator radius server-group cppm
Switch(config)# aaa authentication port-access dot1x authenticator enable
Switch(config)# interface 1/1/1 - 1/1/48
Switch(config-if)# aaa authentication port-access dot1x authenticator
Switch(config-if-dot1x-auth)# enable
Switch(config-if-dot1x-auth)# exit
Switch(config-if)# exit
```

After performing this configuration the administrator notices that the switch ports always remain in the EAP-start state. What should the administrator do to fix this problem?

Options:

A) Enable change of authorization (CoA)

B) Create and assign a local user role to the ports.

C) Set the ports to client-mode.

D) Define the server group cppm

Answer:

D

Question 12

A network engineer is using NetEdit to manage AOS-CX switches. The engineer notices that a lot of third-party VoIP phones are showing up in the NetEdit topology The engineer deletes these, but they are automatically rediscovered by NetEdit and added back in

What should the administrator do to solve this problem?

Options:

A) Disable SSH access on all the VoIP phones.

B) Disable the RESTful API on all the VoIP phones

C) Disable LLDP globally on the AOS-CX switches where phones are connected

D) Change the VoIP phone SNMP community string to something unknown by NetEdit.

Answer:

D