EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

Which statement is correct regarding ACLs and TCAM usage?

A. Applying an ACL to a group of ports consumes the same resources as specific ACE entries

B. Using object groups consumes the same resources as specific ACE entries

C. Compression is automatically enabled for ASIC TCAMs on AOS-CX switches

D. Applying an ACL to a group of VLANs consumes the same resources as specific ACE entries

Suggested Answer: *B*

Community vote distribution

B (100%)

cloud29 Highly Voted 5 years, 6 months ago

B is correct

upvoted 11 times

Kevin1983 Highly Voted 5 years, 4 months ago

B

upvoted 5 times

demanmetdehamer Most Recent 2 years ago

B is correct, study guide says exactly the same sentence

upvoted 1 times

f52f6e6 2 years, 2 months ago

Object groups make ACL management easier, do not reduce TCAM resource consumption.

upvoted 1 times

LANBLAST 2 years, 7 months ago

B is correct

upvoted 1 times

riadyoussef 3 years, 7 months ago

does any one have the study guide ?

upvoted 1 times

omen 4 years, 1 month ago

B is correct

upvoted 1 times

sentinel44 4 years, 10 months ago

Using an object group uses the same resources as specific ACE entries

upvoted 3 times

AM1234 5 years, 4 months ago

B is Correct

upvoted 2 times

Question #2 *Topic 1*

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

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

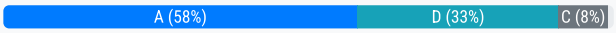
B. Limits can be defined only for broadcast and multicast traffic

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

D. Rate limiting and egress queue shaping can be applied globally

Suggested Answer: *A*

Community vote distribution



Funtomcz Most Recent 1 year, 8 months ago

Option D: Incorrect. While rate limiting can be applied globally or per interface, egress queue shaping is configured per queue on an interface, not globally.

upvoted 1 times

OICU812 2 years ago

In the official HPE Study Guide, in the section "Egress Queue Shaping/Rate Limiting" it states, "1. Create a schedule profile" and "2. Apply profile to an interface."

upvoted 1 times

SeidorBruno 2 years, 10 months ago

Selected Answer: A

Egress queue shaping allows you to apply a maximum bandwidth to a priority queue, as well as a burst size. [Aruba Networks]

upvoted 1 times

SeidorBruno 2 years, 10 months ago

Egress queue shaping allows you to apply a maximum bandwidth to a priority queue, as well as a burst size. [Aruba Networks]Hi SeidorBruno, please could you supply me with your eamil address I wuold like to email you regarding a certain question I have please. Thank you, my email william.waller86.co.zaHi SeidorBruno, please could you supply me with your eamil address I wuold like to email you regarding a certain question I have please. Thank you, my email william.waller86.co.za

upvoted 1 times

Will86 1 year, 12 months ago

Hi SeidorBruno, please could you supply me with your eamil address I wuold like to email you regarding a certain question I have please. Thank you, my email william.waller86.co.za

upvoted 1 times

Greenmile84 2 years, 10 months ago

Should be A Click Quality of Service > General > Egress Shaping per Queue. The Egress Shaping Per Queue page displays the rate limit and burst size for each queue.

upvoted 1 times

Redrum702 2 years, 11 months ago

D: On Aruba AOS-CX, rate limiting and egress queue shaping can be applied globally on the switch or on specific interfaces

upvoted 1 times

abhi7815 3 years, 3 months ago

A is correct answer.

upvoted 1 times

MrBB 3 years, 5 months ago

Same question as the other one in the database. It should be A

upvoted 1 times

E_Nick 3 years, 6 months ago

Correct answer is A

upvoted 1 times

Alialo 3 years, 6 months ago

i think should be D, tested with 8325 and the qos queue and schedule profile could be apply globally and not must with intSorry i have tested again, answer should be A, in schedule profile, only bandwidth and burst can be defined. and the profile cannot be applied globally.

upvoted 1 times

Alialo 3 years, 6 months ago

Selected Answer: D

i think should be D, tested with 8325 and the qos queue and schedule profile could be apply globally and not must with int

upvoted 1 times

Alialo 3 years, 5 months ago

Sorry i have tested again, answer should be A, in schedule profile, only bandwidth and burst can be defined. and the profile cannot be applied globally.

upvoted 2 times

LRAndy 3 years, 6 months ago

Only answer, common to both questions is C: Rate limiting and egress queue shaping can be used to restrict inbound trafficdamn - no edit function should read D: Rate limiting and egress queue shaping can be applied globallyyou cannot control inbound traffic using QoS features, only outbound or egress traffic, so C is certainly wrong

upvoted 1 times

LRAndy 3 years, 6 months ago

Selected Answer: C

Only answer, common to both questions is C: Rate limiting and egress queue shaping can be used to restrict inbound traffic

upvoted 1 times

LRAndy 3 years, 6 months ago

damn - no edit function should read D: Rate limiting and egress queue shaping can be applied globally

upvoted 2 times

ripcurl 2 years, 4 months ago

you cannot control inbound traffic using QoS features, only outbound or egress traffic, so C is certainly wrong

upvoted 1 times

manrodman 3 years, 6 months ago

I think that D is correct because rate limiting can be applied globally by a policy and for egress queue shapping apply the global schedule profile when apply the queue profile. Based on the schedule profile, DWRR is being used and the queue and schedule profile are applied globally. A is not correct: traffic rate and burst size can be defined for only strict priority queue -> Egress queue shaping allows you to apply a maximum bandwidth to a priority queue, as well as a burst size. The port buffers excess traffic up to the burst size and sends the buffered traffic at the max rate, smoothing out bursts while also preventing the high priority queue from exceeding its maximum rate and starving out lower priority queues. Only process queues under the 7 queue if not have traffic in the 7 queue To process all queues Aruba-CX uses DWRR or WFQ -> In both algorithms, each queue receives a predictable share of the bandwidth based on the queue's relative priority, or weigh B is not correct: restrict unknow unicast C is not correct: egress queue shaping can be used to restrict outbound traffic

upvoted 3 times

stephen 3 years, 10 months ago

A you could apply egress queue shaping to the high priority queues to prevent starvation of low priority queues. Egress queue shaping allows you to apply a maximum bandwidth to a priority queue, as well as a burst size. The port buffers excess traffic up to the burst size and sends the buffered traffic at the max rate, smoothing out bursts while also preventing the high priority queue from exceeding its maximum rate and starving out lower priority queues.

upvoted 1 times

turanmuslim 4 years ago

Answer A

upvoted 1 times

poy4242 4 years ago

answer A

upvoted 2 times

darthandy 4 years, 6 months ago

b is incorrect because rate-limiting can also be applied to unknown unicasts.

upvoted 2 times

Ivan007 4 years, 6 months ago

The answer is Ahi, where you download the ebook ? or you purchased.

upvoted 4 times

Ivan007 4 years, 6 months ago

The answer is A

upvoted 4 times

Ben1009 4 years, 1 month ago

hi, where you download the ebook ? or you purchased.

upvoted 1 times

kup 4 years, 7 months ago

A

upvoted 3 times

Question #3 *Topic 1*

A network administrator needs to replace an antiquated access layer solution with a modular solution involving AOS-CX switches. The administrator wants to leverage virtual switching technologies. The solution needs to support high-availability with dual-control planes. Which solution should the administrator implement?

A. AOS-CX 8325

B. AOS-CX 6300

C. AOS-CX 6400

D. AOS-CX 8400

Suggested Answer: *A*

Reference: https://andovercg.com/datasheets/aruba-cx-8325-switch-series.pdf

Community vote distribution

C (100%)

poris27 Highly Voted 5 years, 6 months ago

I think the answer is C because 8325 is not modular like 6400why not 8400 ?as its mentioned for the access layer

upvoted 6 times

poris27 Highly Voted 5 years, 6 months ago

I think the answer is C because 8325 is not modular like 6400

upvoted 6 times

El3den 5 years, 4 months ago

why not 8400 ?

upvoted 3 times

El3den 5 years, 4 months ago

why not 8400 ?as its mentioned for the access layer

upvoted 3 times

AM1234 5 years, 4 months ago

as its mentioned for the access layer

upvoted 3 times

f52f6e6 Most Recent 2 years, 2 months ago

The AOS-CX 6400 series is the best fit for the described requirements, providing a modular, scalable, and high-availability solution with the support for dual-control planes through VSX.

upvoted 1 times

SeidorBruno 3 years, 4 months ago

For high availability (HA), the AOS- CX 6400 supports VSX Live Upgrades and also has redundant management cards, fans, power supplies, etc. [Aruba Networks]

upvoted 2 times

gcg 3 years, 4 months ago

Yes I think the answer is C because is modular switch

upvoted 1 times

Redrum702 3 years, 5 months ago

C: Correction - the key part of the question says virtual switching which is VSF so the only device listed is the 6400 - disregard my previous answer.

upvoted 2 times

Redrum702 3 years, 5 months ago

D: the Aruba 6400 switch series does not support high-availability with dual-control planes. The Aruba 6400 series switches are fixed-configuration switches designed for access and aggregation deployments in campus networks. While they offer advanced features and performance, including support for 10GbE and 40GbE interfaces, they do not incorporate dual-control planes for redundancy and high availability. However, Aruba offers other switch series, such as the Aruba 5400R zl2 and Aruba 8400, that do provide dual-control planes for enhanced resiliency. These series are typically targeted for more demanding network environments where high availability and redundancy are critical. If you require high availability and dual-control planes, it is recommended to consider the Aruba 5400R zl2 or Aruba 8400 series switches or consult the official Aruba documentation to explore other switch models that meet your specific requirements.

upvoted 1 times

IV2709 4 years ago

Answer is C

upvoted 1 times

cjoseph 4 years ago

Answer is C

upvoted 1 times

E_Nick 4 years ago

Mark key words, 'access layer', 'modular', 'high-availability', so only 6400

upvoted 1 times

omen 4 years, 1 month ago

CX6400 can VSX and could be usefull for access layer

upvoted 1 times

d_nat 4 years, 2 months ago

I think it is C as the CX 6400 is an access/aggregation layer switch, has dual plane capability and is modular.

upvoted 1 times

Moreson 4 years, 8 months ago

Mark key words, 'access layer', 'modular', 'high-availability', so only 6400

upvoted 1 times

Ivan007 5 years ago

The answer seems to be C: (See pages 4 & 13) - 6300 can't perform dual-plane (VSX) - Neither the 8325 nor the 8400 are modular - Neither the 8325 nor the 8400 are for the access layera bit correction... 8400 is modular

upvoted 3 times

Ivan007 5 years ago

The answer seems to be C: (See pages 4 & 13) - 6300 can't perform dual-plane (VSX) - Neither the 8325 nor the 8400 are modular - Neither the 8325 nor the 8400 are for the access layer

upvoted 3 times

jagoanneon 4 years, 9 months ago

a bit correction... 8400 is modular

upvoted 1 times

kup 5 years, 1 month ago

C Modular for Access

upvoted 2 times

clupato2 5 years, 2 months ago

C is the answer

upvoted 1 times

demifsud 5 years, 2 months ago

I would have gone C. 6400 is intended for access layer and has support for VSX for dual control planes.

upvoted 2 times

AM1234 5 years, 4 months ago

the Correct Answer is C

upvoted 3 times

Question #4 *Topic 1*

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 aruba123
What is the purpose of this configuration?

A. Implement replay protection for AAA messages

B. Define the account to implement downloadable user roles

C. Speed up the AAA authentication process

D. Define the account to implement change of authorization

Suggested Answer: *C*
Reference: https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/16-01/5200-0122_access_security_guide/content/ch09s02.html

Community vote distribution
C (100%)

cloud29 Highly Voted 4 years, 6 months ago
Radius service tracking Radius service tracking locates the availability of the RADIUS service configured on the switch. It helps to minimize the waiting period for new clients in the unauth-vid (Guest Vlan) when authentication fails because of service is not available, as well as previously authenticated clients in unauth-vid (Guest Vlan) when re-authentication fails because service is not available during the re-authentication period. Note that this feature is disabled by default. radius-server tracking Syntax [no] radius-server tracking True,
upvoted 7 times

cloud29 Highly Voted 4 years, 6 months ago
Radius service tracking Radius service tracking locates the availability of the RADIUS service configured on the switch. It helps to minimize the waiting period for new clients in the unauth-vid (Guest Vlan) when authentication fails because of service is not available, as well as previously authenticated clients in unauth-vid (Guest Vlan) when re-authentication fails because service is not available during the re-authentication period.

Note that this feature is disabled by default.

radius-server tracking Syntax [no] radius-server tracking
upvoted 7 times

slotblocker 2 years, 4 months ago
True,
upvoted 1 times

dodds 4 years, 6 months ago
C looks correct to me
upvoted 5 times

SeidorBruno Most Recent 2 years, 4 months ago
Effect of RADIUS tracking on pre- auth role: If RADIUS tracking is enabled and no RADIUS server is available for authentication, the port will be changed from a pre- auth role VLAN to a critical VLAN. The time taken to move from pre- auth role VLAN to critical VLAN depends on the time it takes for RADIUS tracker to inform the subsystem.
upvoted 2 times

Mar_a_Lagoon 3 years, 8 months ago
C is correct (although the link provided is referring to AOS-S, not CX)
upvoted 4 times

Ivan007 4 years ago
C, page 694
upvoted 2 times

kup 4 years, 1 month ago

C Form Radius config guide

upvoted 2 times

AM1234 4 years, 4 months ago

the correct Answer is C

upvoted 3 times

fasty 4 years, 6 months ago

I also think C is correct

upvoted 4 times

poris27 4 years, 6 months ago

I think the answer is A . radius server tracking is use to track the status of the radius server

upvoted 1 times

Question #5 *Topic 1*

A company has an existing wireless solution involving Aruba APs and Mobility controllers running 8.4 code. The solution leverages a third-party AAA solution. The company is replacing existing access switches with AOS-CX 6300 and 6400 switches. The company wants to leverage the same security and firewall policies for both wired and wireless traffic.
Which solution should the company implement?

A. RADIUS dynamic authorization

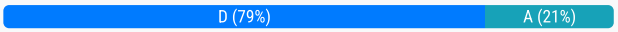
B. Downloadable user roles

C. IPSec

D. User-based tunneling

Suggested Answer: *A*

Community vote distribution



poris27 Highly Voted 5 years ago
I think the answer is D. we talk about UBT in this question where user connect to switch will go to MC by use Tunnel
upvoted 11 times

johnhenri Most Recent 2 years ago
A is incorrect because Radius dynamic authorization has not goal to guaranty same security & firewall policy for wired & wireless traffic B is incorrect because downloadable user role are only compatible with Aruba Clearpass and not with third party AAA. C is incorrect because switch do not use IPSec D is correct : ACSP Learning book Dynamic segmentation : "when to use UBT ? Wired and wireless traffic should have the same (or similar) policies applied to them
upvoted 1 times

SahilERT 2 years, 10 months ago
Correct answer should be A. As it says customer wants to leverage the existing AAA and firewall third party policy it could be CISCO Server as well. If he wants to use UBT he still can do it with LUR but it is new AAA setup for both wired and wireless.
upvoted 1 times

SeidorBruno 2 years, 10 months ago
Page 748 Study Guide: The bottom line is this: Use the tunneled- node feature whenever you want to apply Aruba controller- based security/control mechanisms to both wireless and wired traffic. You get unified access control – same policies regardless of whether they have a wired or wireless connection. [Aruba Networks]
upvoted 2 times

Redrum702 2 years, 10 months ago
A: Aruba ClearPass supports RADIUS dynamic authorization. RADIUS (Remote Authentication Dial-In User Service) is a protocol widely used for network access control, authentication, and accounting. It allows for the centralized management of user authentication and authorization for network devices.
upvoted 1 times

Redrum702 2 years, 10 months ago
A: Aruba ClearPass supports RADIUS dynamic authorization. RADIUS (Remote Authentication Dial-In User Service) is a protocol widely used for network access control, authentication, and accounting. It allows for the centralized management of user authentication and authorization for network devices.third-party AAA solution , not Clearpass.
upvoted 1 times

slotblocker 2 years, 10 months ago
third-party AAA solution , not Clearpass.
upvoted 2 times

Alialo 3 years, 6 months ago
should be D, LUR is used with CPPM and also with third party AAA servers
upvoted 1 times

E_Nick 3 years, 6 months ago

Answer is D. User based tunneling with LUR

upvoted 1 times

omen 3 years, 7 months ago

Agree with demanmetdehamer, its A. UBT ist only Supported with Clearpass and not with a third-party AAA solution.

upvoted 3 times

Moreson 4 years, 2 months ago

Mark key words, 'Aruba APs and MC', '3rd Party AAA', 'FW for both Wired and wireless means same user can be either', so need to be Aruba tunneling using LUR

upvoted 2 times

jagoanneon 4 years, 3 months ago

Answer is D. User based tunneling with LUR

upvoted 4 times

sentinel44 4 years, 3 months ago

correct answer is D

upvoted 2 times

demanmetdehamer 4 years, 6 months ago

Answer A is correct. UBT is only supported with Clearpass as radius server. The question clearly states that the company has a third party solution.UBT is only supported with Clearpass when you use DUR , but when you use LUR you d'ont need clearpass

upvoted 1 times

demanmetdehamer 4 years, 6 months ago

Answer A is correct. UBT is only supported with Clearpass as radius server. The question clearly states that the company has a third party solution.

upvoted 1 times

kadis500 Highly Voted 4 years, 4 months ago

UBT is only supported with Clearpass when you use DUR , but when you use LUR you d'ont need clearpass

upvoted 6 times

Ivan007 4 years, 6 months ago

Answer is D, see pages 789 791

upvoted 2 times

AM1234 4 years, 10 months ago

the Correct answer is D

upvoted 2 times

Question #6 *Topic 1*

A network engineer is having a problem adding a custom-written script to an AOS-CX switch's NAE GUI. The script was written in Python and was successfully added on other AOS-CX switches. The engineer examines the following items from the CLI of the switch:

What should the engineer perform to fix this issue?

```
switch# show capacities-status nae

System Capacities Status: Filter NAE
```

Capacity Status Name	Value	Maximum
Number of configured NAE agents currently active in the system	1	100
Number of configured NAE monitors currently active in the system	7	500
Number of configured NAE scripts currently active in the system	50	50

```
switch# show ntp status
NTP Status Information

NTP : Disabled
NTP Authentication : Disabled
NTP Server Connections : Using the default VRF

System time : Sat May 2 11:50:55 UTC 2020
NTP uptime : 0 minutes, 0 seconds

Not synchronized with an NTP server.

switch# show crypto pki certificate
```

Certificate Name	Cert Status	Associated Applications
local-cert	installed	captive-portal, hsc, https-server,
syslog-client		

```
switch# show crypto pki application
```

Associated Applications	Certificate Name	Cert Status
captive-portal		not configured, using local-cert
hsc		not configured, using local-cert
https-server		not configured, using local-cert
syslog-client		not configured, using local-cert

A. Install the script's signature before installing the new script

B. Ensure the engineer's desktop and the AOS-CX switch are synchronized to the same NTP server

C. Enable trust settings for the AOS-CX switch's SSL certificate

D. Remove a script that is no longer used before installing the new script

Suggested Answer: *D*

Community vote distribution

D (100%)

SeidorBruno Most Recent 2 years, 4 months ago

Reached Maximum Scripts Capacity. NTP doesn't matter here.

upvoted 2 times

E_Nick 3 years ago

D, I think is the most correct answer given that it is impossible to deploy more scripts than the switch capacity allows for.

upvoted 3 times

Mar_a_Lagoon 3 years, 8 months ago

D. The script is not yet uploaded (to this particular switch) and the capacity has been reached. NTP is not relevant here.

upvoted 4 times

Ivan007 4 years ago

D is correct, see page 176 "show capacities-status nae" tells us that the script capacity has been reached B is not the best answer here. NTP should always be in sync but the web GUI is not being used in this scenario, which is dependent on NTP, the CLI is not.

upvoted 2 times

pabx31 4 years ago

B stands out but the book clearly states the NTP sync is for the WEB GUI between your browser/PC and the switch. This is CLI so I don't see how NTP affects anything. The command is being ran directly on the switch. I am betting on D being correct.

upvoted 3 times

Emad 4 years, 1 month ago

B seems Correct, the scrip and NAE Agents are installed on the system. however, NTP is not in sync with Desktop which may not show the actual status on the GUI. Lab guide starts with having NTP Setup and to make sure time matches with Desktop from where the GUI is accessed. The time difference should be within seconds. The NAE web UI is using the client browser time to get the time for the 'live' graphs, so therefore it is important to have correct time on the PC client and the switch.

upvoted 1 times

I_C_U 4 years, 1 month ago

D is the answer, you can still add a script if the time is out and it will just warn you.

upvoted 2 times

clupato2 4 years, 2 months ago

D is the answer

upvoted 1 times

demifsud 4 years, 2 months ago

D, I think is the most correct answer given that it is impossible to deploy more scripts than the switch capacity allows for.

upvoted 4 times

Itachi22 4 years, 3 months ago

the answer should be B as a User guide explain : the time zone for Web client and the switch based on NTP sync or based on UTC .

upvoted 1 times

AM1234 4 years, 4 months ago

the correct Answer is D

upvoted 2 times

dodds 4 years, 5 months ago

I think the answer is D. if switch and browser time is not in sync, only information displayed in the web ui might not be accurate. From ACSP student guide p.156B is correct : user guide page 73

upvoted 2 times

dodds 4 years, 5 months ago

I think the answer is D.

if switch and browser time is not in sync, only information displayed in the web ui might not be accurate.

From ACSP student guide p.156

upvoted 2 times

WifiX 4 years, 5 months ago

B is correct : user guide page 73

upvoted 4 times

kur0 4 years, 6 months ago

I think B is the correct answer because NTP should be in synchronization with the NAE agent.

upvoted 2 times

Question #7 *Topic 1*

Which option correctly defines how to identify a VLAN as a voice VLAN on an AOS-CX switch?

A. Switch(config)# port-access lldp-group Switch(config-lldp-group)# vlan

B. Switch(config)# port-access role Switch(config-pa-role)# vlan access

C. Switch(config)# vlan Switch(config-vlan-)# voice

D. Switch(config)# vlan voice

Suggested Answer: *C*

Community vote distribution

C (100%)

SeidorBruno Most Recent 2 years, 4 months ago

To create a voice VLAN, configure the voice command in the VLAN context, like this: Switch(config)# vlan Switch(config-vlan)# voice [Aruba Networks]

upvoted 1 times

IV2709 3 years ago

Answer C ! Sure !

upvoted 1 times

d_nat 3 years, 2 months ago

See student guide vol. 2,

upvoted 1 times

d_nat 3 years, 2 months ago

Student Guide, Vol2, Voice VLANs To create a voice VLAN, configure the voice command in the VLAN context, like this: Switch(config)# vlan Switch(config-vlan)# voice So answer C

upvoted 3 times

AM1234 4 years, 4 months ago

the correct Answer is C

upvoted 3 times

cloud29 4 years, 6 months ago

C is correct

upvoted 2 times

Question #8 *Topic 1*

An administrator will be replacing a campus switching infrastructure with AOS-CX switches that support VSX capabilities. The campus involves a core, as well as multiple access layers. Which feature should the administrator implement to allow both VSX-capable core switches to process traffic sent to the default gateway in the campus VLANs?

A. VRF

B. VRRP

C. IP helper

D. Active gateway

Suggested Answer: *B*

Community vote distribution

D (100%)

poris27 Highly Voted 4 years, 6 months ago

I think the answer is D since in VSX the best practise is we use Active gateway instead of VRRP

upvoted 15 times

Mikie2825 Most Recent 2 years, 1 month ago

The question just states that the switches are VSX capable. It does not say they are configured with VSX enabled. I would say that B is the correct answer given the stated question.

upvoted 1 times

SeidorBruno 2 years, 4 months ago

Remember that the VSX pair acts as the default gateway for the access VLANs. To do so, the pair uses the active gateway feature. [Aruba Networks]

upvoted 3 times

beerdeliveryguy 2 years, 4 months ago

VSX active gateway is the only answer

upvoted 1 times

Alialo 2 years, 12 months ago

should be D, the question need to allow both VSX-capable core switches to process traffic.

upvoted 1 times

E_Nick 3 years ago

D is correct

upvoted 1 times

Rockford 3 years ago

D: Remember that the VSX pair acts as the default gateway for the access VLANs. To do so, the pair uses the active gateway feature. This feature allows each switch in the pair to act as an active default gateway for the VLAN using a shared virtual IP address (VIP) and virtual MAC address. It eliminates the need for Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP). Simple to configure, the active gateway feature relies on VSX operations so it does not add any protocol overhead. It also supports redundancy for DHCP relay functions.

upvoted 1 times

Araz 3 years ago

D is correct

upvoted 1 times

d_nat 3 years, 2 months ago

Student Guide Vol.1, page 190: It eliminates the need for Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP). So D is correct

upvoted 1 times

sentinel44 3 years, 9 months ago

Answer is D, page 216 Active gateway = both devices route/forward traffic VRRP = Active-standbye, only active member routes/forwards traffic

upvoted 4 times

Ivan007 4 years ago

Answer is D, page 216 Active gateway = both devices route/forward traffic VRRP = Active-standbye, only active member routes/forwards traffic

upvoted 3 times

kup 4 years, 1 month ago

D - 189 page of study book

upvoted 1 times

I_C_U 4 years, 1 month ago

D is the correct answer as. Understand the Active Gateway principle In a VSX system, active gateway provides redundant default gateway functionality for the end-hosts. The default gateway of the end-host is automatically handled by both the VSX systems.

upvoted 3 times

clupato2 4 years, 2 months ago

D is the answer

upvoted 2 times

AM1234 4 years, 4 months ago

the correct Answer is D

upvoted 4 times

clupato2 4 years, 4 months ago

D is the answer.

upvoted 4 times

cloud29 4 years, 6 months ago

D is the answer

upvoted 4 times

Question #9 *Topic 1*

What is correct regarding the tunneling of user traffic between AOS-CX switches and Aruba Mobility Controllers (MCs)?

A. Uses IPSec to protect the management and data traffic

B. Uses IPSec to protect the management traffic

C. Supports only port-based tunneling

D. Uses the same management protocol as Aruba APs

Suggested Answer: *C*

Community vote distribution

D (100%)

poris27 Highly Voted 4 years, 6 months ago

I think the answer is D because both AP and Switch use PAPI . Moreover in AOS-CX switch currently not support port based tunnel. AOS-CX switch only support User Based Tunnel (UBT)

upvoted 5 times

SeidorBruno Most Recent 2 years, 4 months ago

Page 749 Study Guide: The switch uses two protocols to connect to an Aruba Mobility Controller (MC) The control plane uses PAPI (UDP port 8211) - the same protocol used by AP- to- MC communications. However, where APs use IPSec to protect the PAPI connection between the AP and MC, AOS-CX switches do not support this protection. Instead, you can optionally implement an MD5 HMAC function to protect PAPI between the AOS- CX switches and MCs. [Aruba Networks]

upvoted 1 times

Alialo 2 years, 12 months ago

should be D, the switch uses two protocols to connect to an MC: PAPI (control plane) and GRE (data plane). However, where APs use IPSec to protect the PAPI connection between the AP and MC, AOS-CX switches do not support this protection. Instead, you can optionally implement an MD5 HMAC function to protect PAPI between the AOS-CX switches and MCs

upvoted 2 times

E_Nick 3 years ago

Answer is D

upvoted 1 times

Araz 3 years ago

D is correct

upvoted 1 times

omen 3 years, 1 month ago

Answer is D

upvoted 1 times

sentinel44 3 years, 9 months ago

Answer is D, see page 784 Switches do not use IPsec or port-based tunneling

upvoted 1 times

Ivan007 4 years ago

Answer is D, see page 784 Switches do not use IPsec or port-based tunneling

upvoted 1 times

clupato2 4 years, 2 months ago

D is the answer

upvoted 2 times

AM1234 4 years, 4 months ago

the correct Answer is D

upvoted 4 times

fasty 4 years, 6 months ago

D is correct

upvoted 3 times

Question #10 *Topic 1*

An administrator is implementing a multicast solution in a multi-VLAN network. Which statement is true about the configuration of the switches in the network?

A. IGMP snooping must be enabled on all interfaces on a switch to intelligently forward traffic

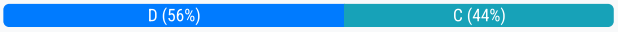
B. IGMP requires join and leave messages to graft and prune multicast streams between switches

C. IGMP must be enabled on all routed interfaces where multicast traffic will traverse

D. IGMP must be enabled on all interfaces where multicast sources and receivers are connected

Suggested Answer: *B*

Community vote distribution



watermellonhead Highly Voted 5 years, 1 month ago

Looks like C is correct. Found a PDF the specifically says this. Google "AOS-CX switch igmp", first result (pdf), then go to "Multicast Deployment Summary". A - incorrect. This is configured globally on the switch, not per-interface. B - incorrect. This is a PIM function. Not IGMP. D - incorrect. IGMP is enabled on L3 interfaces towards the sources/receivers. Not ALL interfaces.Thanks bro i have tomorrow my exam.did you pass?

upvoted 12 times

watermellonhead Highly Voted 5 years, 1 month ago

Looks like C is correct. Found a PDF the specifically says this. Google "AOS-CX switch igmp", first result (pdf), then go to "Multicast Deployment Summary". A - incorrect. This is configured globally on the switch, not per-interface. B - incorrect. This is a PIM function. Not IGMP. D - incorrect. IGMP is enabled on L3 interfaces towards the sources/receivers. Not ALL interfaces.

upvoted 12 times

Linares1234 5 years ago

Thanks bro i have tomorrow my exam.did you pass?

upvoted 2 times

Linares1234 5 years ago

Thanks bro i have tomorrow my exam.

upvoted 2 times

davo92726 4 years, 11 months ago

did you pass?

upvoted 1 times

seb6869 5 years, 2 months ago

D is correct. IGMP is enabled only on clients and multicast servers VLAN. PIM is enabled on routed interfaces between clients and servers VLAN to route multicast flow

upvoted 6 times

BFDS Most Recent 1 year, 11 months ago

answer is D

upvoted 1 times

BFDS 1 year, 11 months ago

If you read the question correctly, it is talking about a multi-VLAN network, so it involves multicast routing, which is PIM, in that regard, C is incorrect. I think D is the answer.

upvoted 1 times

Luke80 2 years ago

I would go for D as well. C is wrong because it's not IGMP that needs to be enabled to allow multicast-routing but PIM!

upvoted 2 times

johnhenri 2 years, 6 months ago

A is false because IGMP snooping is enable on vlan and not on interface B is false because Graft & Prune are used by PIM D is false because they sayd only "interface" and not "routed interface", IGMP cannot be enable on switch interface, only on "routed interface" C seems to be correct

upvoted 1 times

SeidorBruno 3 years, 4 months ago

Page 567 Study Guide: A querier is required for proper IGMP operation. For this reason, you must enable IGMP on the L3 Interface. If the querier functionality is not configured or disabled, you must ensure that there is an IGMP querier in the same VLAN. [Aruba Networks]

upvoted 1 times

Redrum702 3 years, 5 months ago

C: IGMP has to be configured on routed interfaces

upvoted 1 times

Redrum702 3 years, 5 months ago

C: IGMP must be enabled on all routed interfaces. This allows the routers to participate in IGMP signaling and properly handle the multicast traffic.

upvoted 1 times

E_Nick 3 years, 12 months ago

C is correct

upvoted 1 times

a__p 4 years ago

I think D is correct A - incorrect, switches will always forward traffic B - Graft and Prune are PIM functions C - IGMP is only required on the VLAN where the receivers and source are connected, PIM is required across L3 domains. IGMP manages flooding of multicast on a segment. D - Correct - VLAN interfaces where source and receivers are connected

upvoted 2 times

mindaugasv 4 years ago

C is correct

upvoted 1 times

gondolf 4 years, 6 months ago

None of these are correct. I'm going to assume they are talking about VLAN interfaces, and go with answer D if I get this question on the test. https://i.imgur.com/vW7V2UL.png

upvoted 2 times

gondolf 4 years, 6 months ago

None of these are correct. I'm going to assume they are talking about VLAN interfaces, and go with answer D if I get this question on the test. https://i.imgur.com/vW7V2UL.pngin the picture you shared is saying that "igmp enable snooping optional but recommended" but answer "D" is saying it must be enabled. so D is not correctbe carefull, "igmp snooping" is different from "igmp", on the picture they sayed "PIM-DM and IGMP enabled on correct interface"

upvoted 2 times

guidogiesen 4 years, 6 months ago

in the picture you shared is saying that "igmp enable snooping optional but recommended" but answer "D" is saying it must be enabled. so D is not correct

upvoted 1 times

guidogiesen 4 years, 6 months ago

in the picture you shared is saying that "igmp enable snooping optional but recommended" but answer "D" is saying it must be enabled. so D is not correctbe carefull, "igmp snooping" is different from "igmp", on the picture they sayed "PIM-DM and IGMP enabled on correct interface"

upvoted 1 times

johnhenri 2 years, 6 months ago

be carefull, "igmp snooping" is different from "igmp", on the picture they sayed "PIM-DM and IGMP enabled on correct interface"

upvoted 1 times

Mar_a_Lagoon 5 years ago

D is correct. See "AOS-CX Multicast deployment and troubleshooting guide" page 8 Multicast Deployment Summary point 6: "Enable IGMP/MLD on L3 interfaces towards receiver subnets"It's C. You answer says it. "L3 interfaces" Option D says nothing about routed interfaces.

upvoted 1 times

Mar_a_Lagoon 5 years ago

D is correct. See "AOS-CX Multicast deployment and troubleshooting guide" page 8 Multicast Deployment Summary point 6: "Enable IGMP/MLD on L3 interfaces towards receiver subnets"

upvoted 1 times

filthyx 4 years, 12 months ago

It's C. You answer says it. "L3 interfaces" Option D says nothing about routed interfaces.

upvoted 2 times

pabx31 5 years ago

C - Book states "If you want the benefits of IGMP in VLAN 30, you must enable it on the routed interface for VLAN 30" and "You enable IGMP on a per VLAN basis."

upvoted 4 times

Pcpimp 5 years ago

Look at module 9 page 17 and 18. I think D is correct.

upvoted 2 times

kup 5 years, 1 month ago

C page 531when are you planning to do the exam? or have you already done it?

upvoted 1 times

kup 5 years, 1 month ago

C page 531

upvoted 1 times

I_C_U 5 years, 1 month ago

when are you planning to do the exam? or have you already done it?

upvoted 1 times

Question #11 *Topic 1*

How is voice traffic prioritized correctly on AOS-CX switches?

A. By defining device profiles with QOS settings

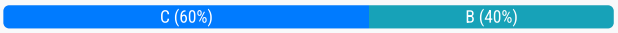
B. By placing it in the strict priority queue

C. By implementing voice VLANs

D. By implementing weighted fair queueing (WFQ)

Suggested Answer: *C*

Community vote distribution



poris27 Highly Voted 5 years, 6 months ago

I think the answer is B because in Strict Priority (SP) we can put VOIP traffic in top priority (priority 7)just wondering what is the point to have voice key word under vlan interface then? give you this option, there is a reason. though you can achieve in multiple ways, but most optimized option is C

upvoted 5 times

poris27 Highly Voted 5 years, 6 months ago

I think the answer is B because in Strict Priority (SP) we can put VOIP traffic in top priority (priority 7)

upvoted 5 times

Moreson 4 years, 8 months ago

just wondering what is the point to have voice key word under vlan interface then? give you this option, there is a reason. though you can achieve in multiple ways, but most optimized option is C

upvoted 3 times

Luke80 Most Recent 1 year, 12 months ago

Why does nobody go for answer A? Look at the study guide Vol-2 Page 270. I think that would be the correct way to be sure, that VoIP traffic is detected and prioritized correctly.

upvoted 1 times

demanmetdehamer 2 years ago

Marking the vlan as voice is only used to direct phones to the "right" vlan. Answer should be b in my opinion because this is the only answer that says something about prioritizing the traffic

upvoted 1 times

johnhenri 2 years, 6 months ago

I hate this kind of question because different option are possible. We can use answer A because a device profile can assign QoS to voice traffic come from IP Phone, but i think it is not the "correctly" way to prioritize Voice traffic. We can use answer B because we can assigne voice traffic to high queue with strict priority but i think again this is not the best way to prioritize voice traffic. We can use answer C because best way to prioritize voice traffic is to enable voice vlan but not only, we need to trust DSCP/CoS or remark then prioritize... So I vote for C but not sure...

upvoted 2 times

alper3192 3 years, 1 month ago

"Sensitive traffic like VOIP uses Strict Priority queuing " B is correct

upvoted 1 times

SeidorBruno 3 years, 4 months ago

Page 868-869 Study Guide

upvoted 1 times

Redrum702 3 years, 5 months ago

B" voice traffic can be prioritized correctly on an Aruba AOS-CX switch by placing it in the strict priority queue. The strict priority queue is a QoS mechanism that gives the highest priority to specific types of traffic, such as voice or real-time communication traffic. Here's how you can achieve this: Enable Strict Priority Queue: Configure the AOS-CX switch to support strict priority queuing. This ensures that traffic assigned to the strict priority queue will be given the highest priority and processed before other queues.

upvoted 2 times

alex711 3 years, 8 months ago

C is Correct

upvoted 1 times

devadarshan91730 4 years ago

B is correct. The qos priority default setting is 0 (normal), with 1 as the lowest priority and 7 as the highest priority. If you configure a voice VLAN with a VID of 10, and want the highest priority for all traffic on this VLAN, execute the following commands: HP Switch(config) #: vlan 10 qos priority 7 HP Switch (config) #: write memory

upvoted 3 times

d_nat 4 years, 2 months ago

In the student guide vol.2 on page 267 it is stated , that you enable voice VLAN with a command in the vlan configuration context.

upvoted 1 times

gondolf 4 years, 6 months ago

The question is how is voice traffic prioritized *correctly*. I'm positive they are looking for the VLAN "voice"-command, even though a manual SP could give it a higher priority.

upvoted 1 times

Mar_a_Lagoon 4 years, 7 months ago

By tagging the port as voice (Alt C) the switch will by default honor whatever priority the end device uses. This can be changed if needed.

upvoted 2 times

sentinel44 4 years, 9 months ago

I think the answer is B because in Strict Priority (SP) we can put VOIP traffic in top priority (priority 7)

upvoted 2 times

AM1234 5 years, 4 months ago

the correct Answer is C

upvoted 1 times

cloud29 5 years, 6 months ago

I think they ask us about something else. With SP we can put priority at any traffic. But they want us to know that turning on voice vlan will put voice vlan in a higher priority. Thats why the answer i think should be C

upvoted 3 times

Question #12 *Topic 1*

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 802.1X. 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?

A. 802.1X must be configured to work in fallback mode

B. Device fingerprinting is required for authentication

C. The client-limit setting for port access needs to be changed

D. Device mode should be implemented

Suggested Answer: *A*

Community vote distribution

C (100%)

SeidorBruno Most Recent 2 years, 4 months ago

Page 693 Study Guide After you set the limit, the port begins tracking MAC addresses and defines the authorization status and settings for each separately. For example, in the scenario with the computer and VoIP phone, the switch port sends an EAP Request/Identity to each separate MAC address detected on the port. If the VoIP phone authenticates successfully, but the computer fails, the computer traffic is blocked. [Aruba Networks]

upvoted 2 times

Alialo 2 years, 12 months ago

if you want the computer and IP phone to authenticate separately so that an unauthorized user cannot piggyback on the IP phone's session. Make sure to set the 802.1X client-limit to 2 so that the port operates in user-mode and authenticates each device separately. what is the meaning in A, fallback mode, just combine the MAC-Auth and 802.1X, not fallback

upvoted 1 times

a__p 3 years ago

The default for client-limit is 1 "Command specifies the maximum number of clients. Default: 1. Range: 1 to 32 (6200). 1 to 256 (6300, 6400)." Therefore this needs to be change C is correct

upvoted 2 times

d_nat 3 years, 2 months ago

If B refers to MAC authentication, I would chose this, else A. Why I do not believe the answer to be C: the question says: "Some devices support no form of authentication, and some support 802.1X. Some ports have a VoIP phone and a PC connected to the same port," There are devices who support 802.1X and some no authentication at all, which leaves MAC auth as only possibility - or bypassing 802.1X (fallback)

upvoted 3 times

poy4242 3 years, 6 months ago

fallback mode if for the radius part; client limit is for multiple authent on one port (ie phone + pc) From doc : aaa port-access authenticator client-limit Used after executing aaa port-access authenticator to convert authentication from port-based to user-based. Specifies user-based 802.1X authentication and the maximum number of 802.1X-authenticated client sessions allowed on each of the ports in . If a port currently has no authenticated client sessions, the next authenticated client session the port accepts determines the untagged VLAN membership to which the port is assigned during the session. If another client session begins later on the same port while an earlier session is active, the later session will be on the same untagged VLAN membership as the earlier session.

upvoted 1 times

sentinel44 3 years, 9 months ago

C - absolutely correct

upvoted 1 times

aru_n 3 years, 10 months ago

Correct answer is C

upvoted 1 times

Mar_a_Lagoon 4 years ago

Pretty sure both A and C are necessary here.

upvoted 1 times

kup 4 years, 1 month ago

C - absolutely correct

upvoted 1 times

AM1234 4 years, 4 months ago

the correct Answer is C

upvoted 2 times

WifiX 4 years, 5 months ago

C is correct page 306 user guide

upvoted 1 times

poris27 4 years, 6 months ago

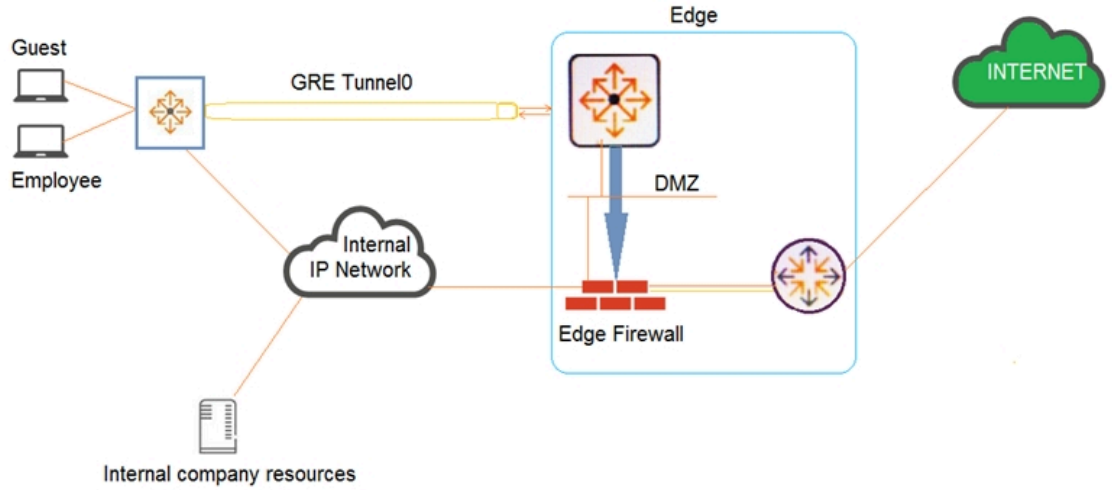
I think the answer is C. we need to chnage the client device limit . A is not correct because VOIP device is not for 802.1X

upvoted 4 times

Question #13 *Topic 1*

Examine the network exhibit.

A company has a guest implementation for wireless and wired access. Wireless access is implemented through a third-party vendor. The company is concerned about wired guest traffic traversing the same network as the employee traffic. The network administrator has established a GRE tunnel between AOS-CX switches where guests are connected to a routing switch in the DMZ.
Which feature should the administrator implement to ensure that the guest traffic is tunneled to the DMZ while the employee traffic is forwarded using OSPF?



A. OSPF route maps using the ɹ€set metricɹ€ command

B. Policy-based routing (PBR)

C. User-based tunneling (UBT)

D. Classifier policies

Suggested Answer: *C*

Community vote distribution

B (100%)

pabx31 Highly Voted 4 years ago

B - my book has this on page 410. Guest traffic can be routed with PBR to use GRE tunnels that terminate in the DMZ.

upvoted 6 times

SeidorBruno Most Recent 2 years, 3 months ago

Page 896 Study Guide: Policy- Based Routing (PBR) - to override normal destination- based routing entries learned by static, OSPF, or BGP routes. [Aruba Networks] Page 905 Study Guide: interface tunnel: Specify a GRE, 6in4 or 6in6 tunnel as the outbound interface for all matching packets. The tunnel must exist before configuring. Packets sent into the tunnel interface egress at the router at the endpoint of the tunnel. If the tunnel is misconfigured or down the traffic may be lost. [Aruba Networks]

upvoted 1 times

Neyce 2 years, 6 months ago

B: Guest traffic can be routed with PBR to use GRE tunnels that terminate in the DMZ

upvoted 1 times

NetExpert 3 years, 1 month ago

B is correct

upvoted 1 times

d_nat 3 years, 2 months ago

B makes most sense to me. As previously mentioned, there is already a GRE tunnel, so no need for an additional tunnel. With PBR you can steer the traffic to where you want it

upvoted 1 times

Moreson 3 years, 8 months ago

the key words are 'The network administrator has established a GRE tunnel', so the tunnel is there, no need to build UBT, just a matter of split the traffic from OSPF, so B should be the one

upvoted 2 times

sentinel44 3 years, 9 months ago

B - my book has this on page 410. Guest traffic can be routed with PBR to use GRE tunnels that terminate in the DMZ.

upvoted 3 times

DianaDecker 3 years, 10 months ago

B is correct

upvoted 1 times

maccchinguwo 4 years, 1 month ago

SORRY B is the correct answer

upvoted 1 times

maccchinguwo 4 years, 1 month ago

the correct answer is C

upvoted 1 times

clupato2 4 years, 2 months ago

I think it's C

upvoted 1 times

AM1234 4 years, 4 months ago

the correct Answer is B

upvoted 1 times

WifiX 4 years, 5 months ago

B is correct page 411 guide

upvoted 3 times

cloud29 4 years, 6 months ago

B is correct

upvoted 2 times

dodds 4 years, 6 months ago

Agreed, B should be the correct answer

upvoted 1 times

poris27 4 years, 6 months ago

I think the answer is B. With PBR we can separate the traffic

upvoted 1 times

Question #14 *Topic 1*

An administrator has an AOS-CX switch configured with:
router ospf 1
area 0
area 1 stub no-summary
It is the only ABR for area 1. The switch has the appropriate adjacencies to routing switches in areas 0 and 1. The current routes in each area are:
Area 0: 5 routes (LSA Type 1 and 2)
Area 1: 10 routes (LSA Type 1 and 2)
External routes: 2 (LSA Type 5)
Based on the above configuration, how many OSPF routes will routing switches see in Area 1?

A. 15

B. 6

C. 11

D. 12

Suggested Answer: *C*

Community vote distribution

C (100%)

WifiX Highly Voted 4 years, 5 months ago
default route + 10 routes =11
upvoted 18 times

SeidorBruno Most Recent 2 years, 3 months ago
Page 397 Study Guide: The no- summary option transforms a stub area to a totally stub area – it suppresses all external route advertisements as normal for a stub area. It also prevents the ABR from generating non- aggregated Inter- Area (IA) summary routes for this area. [Aruba Networks]
upvoted 2 times

devadarshan91730 3 years ago
Option c : Totally stub area = intra area routes (local route) + default route
upvoted 2 times

E_Nick 3 years ago
Its a completely stub area so no type 5 lsa will come in, only the local routes and the default so 11 is the correct answer for sure.
upvoted 1 times

I_C_U 4 years, 1 month ago
Its a completely stub area so no type 5 lsa will come in, only the local routes and the default so 11 is the correct answer for sure.
upvoted 2 times

AM1234 4 years, 4 months ago
the correct Answer is B
upvoted 2 times

AM1234 4 years, 4 months ago
the correct Answer is BHow come it's B? The area itself already has 10 routes.No its C
upvoted 2 times

jagoanneon 3 years, 9 months ago
How come it's B? The area itself already has 10 routes.
upvoted 1 times

AM1234 4 years, 4 months ago
No its C
upvoted 4 times

Question #15 *Topic 1*

A network administrator is managing a network that deploys a multicast service. The administrator has multiple streams successfully being routed by PIM-DM in the network. The administrator then adds a new stream with a destination address of 239.0.0.1. However, clients who have not joined the stream are receiving it.
What should the administrator do to fix this problem?

A. Verify that IGMP is enabled between the switches connecting the multicast source and receivers

B. Change the destination multicast address to 239.1.1.1

C. Define the 239.0.0.1 stream on the rendezvous point (RP)

D. Define the 239.0.0.1 stream on the PIM candidate bootstrap router

Suggested Answer: *C*

Community vote distribution

B (100%)

SeidorBruno Highly Voted 2 years, 10 months ago

Page 536 Study Guide: As a recommendation do not use x.0.0.x or x.128.0.x, since these addresses will overlay with the Link- Local Multicast address scope. [Aruba Networks]

upvoted 5 times

johnhenri Most Recent 2 years ago

Ebook ACSP Chapter IGMP - Multicast adressing - Overlapping adress issues: "Because only 23 bits of the 28 bits address are carried from the L3 to the L2 multicast adress, you will over some layer-3 multicast adress share the same L2 multicast adress. You should AVOID this situation. Basically, multicast adresses that include x.0.0.x and x.128.0.x will overlap. Multicast adresses in the 224.0.0.0/24 range are link local multicast adresses. They are used for protocol discovery and are flooded to every port... For a switch that is doing IGMP snooping, these are NOT added to the snooping list and thus are not filtered. Therefor, if you would use an IP adresse like 239.0.0.1, IGMP snooping would not filter its corresponding L2 multicast adress, thinking that this was an IGMP-related message."

upvoted 2 times

Neyce 3 years ago

B: MAC/IP overlap. 239.0.0.1 would be the same MAC for 224.0.0.1. 224.0.0.0/24 is always flooded over every port.

upvoted 1 times

Unkn0wnProtocol2 4 years, 2 months ago

B is coorect. MAC/IP overlap. 239.0.0.1 would be the same MAC for 224.0.0.1. 224.0.0.0/24 is always flooded over every port.

upvoted 1 times

sentinel44 4 years, 3 months ago

B correct. Due to MAC/IP overlap, guidelines is to not use x.0.0.x or x.128.0.x addresses.

upvoted 2 times

Disposable_Me_2018 4 years, 7 months ago

A wrong as solution already works. C wrong as this is PIM-DM D wrong as this is PIM-DM B correct. Due to MAC/IP overlap, guidelines is to not use x.0.0.x or x.128.0.x addresses.

upvoted 4 times

kup 4 years, 7 months ago

B correct not use x.0.0.x as destination because overlaps with linklocal - Study bookWhich study book are you referring to and what page?

upvoted 4 times

kup 4 years, 7 months ago

B correct not use x.0.0.x as destination because overlaps with linklocal - Study book

upvoted 4 times

I_C_U 4 years, 7 months ago

Which study book are you referring to and what page?

upvoted 1 times

mgruber 4 years, 9 months ago

I think it's A. Cause without IGMP enabled on switches between the streams it will be broadcasted to all known devices/clients.

upvoted 2 times

WifiX 4 years, 11 months ago

B is correct page 252

upvoted 2 times

poris27 5 years ago

We should never use x.0.0.x as destination

upvoted 4 times

cloud29 5 years ago

Why B?

upvoted 1 times

poris27 5 years ago

I think the answer is B

upvoted 1 times

Question #16 *Topic 1*

Which protocols are used by NetEdit to interact with third-party devices? (Choose two.)

A. telnet

B. SNMP

C. SSH

D. Restful API

E. CDP

Suggested Answer: *B, C*

Community vote distribution

BC (100%)

johnhenri Most Recent 2 years ago

Learning Book ACSP Chap "NetEdit" : "NetEdit will now also discover and display third-party devices that are using the standard MIBs. Using SNMP with NetEdit, administrators can also enter SSH credentials for third-party devices."

upvoted 1 times

SeidorBruno 2 years, 10 months ago

Page 73 Study Guide: NetEdit will now also discover and display 3rd party devices that are using standard SNMP MIB's, and you can enter SSH credentials for 3rd party devices. [Aruba Networks]

upvoted 2 times

slotblocker 2 years, 11 months ago

REST APIs ONLY for Aruba-CX https://www.arubanetworks.com/assets/ds/DS_NetEdit.pdf

upvoted 1 times

d_nat 3 years, 6 months ago

For 3rd party devices it is SNMP and SSH.

upvoted 1 times

Rockford 3 years, 6 months ago

BC For further simplicity, NetEdit automatically discovers new network infrastructure devices using the Link Layer Discovery Protocol (LLDP), using REST APIs for Aruba CX switches and SNMP for Aruba wireless and third- party devices. Newly connected switches appear automatically in the Network tab, so you can automate switch configuration change workflows without programming. NetEdit will now also discover and display 3rd party devices that are using standard SNMP MIB's, and you can enter SSH credentials for 3rd party devices.

upvoted 3 times

gravyboy 4 years, 6 months ago

The key point here is 3rd party devices. B & C.

upvoted 1 times

Yoshiki 4 years, 9 months ago

Correct answer should be B and D. NetEdit automatically discovers new network infrastructure devices using the Link Layer Discovery Protocol (LLDP), using REST APIs for Aruba CX switches and SNMP for Aruba wireless and third-party devices.
https://www.arubanetworks.com/assets/ds/DS_NetEdit.pdf

upvoted 1 times

Yoshiki 4 years, 9 months ago

Correct answer should be B and D. NetEdit automatically discovers new network infrastructure devices using the Link Layer Discovery Protocol (LLDP), using REST APIs for Aruba CX switches and SNMP for Aruba wireless and third-party devices.
https://www.arubanetworks.com/assets/ds/DS_NetEdit.pdfbut the study guide specifies that third-party devices discovered by netedit using SNMP and sshso its B & CD used for AOS-CX for others not

upvoted 1 times

Itachi22 4 years, 8 months ago

but the study guide specifies that third-party devices discovered by netedit using SNMP and sshso its B & C

upvoted 3 times

Itachi22 4 years, 8 months ago

but the study guide specifies that third-party devices discovered by netedit using SNMP and ssh

upvoted 3 times

Itachi22 4 years, 8 months ago

so its B & C

upvoted 1 times

kup 4 years, 7 months ago

D used for AOS-CX for others not

upvoted 2 times

Question #17 *Topic 1*

An administrator is implementing a downloadable user role solution involving AOS-CX switches. The AAA solution and the AOS-CX switches can successfully authenticate users; however, the role information fails to download to the switches. What policy should be added to an intermediate firewall to allow the downloadable role function to succeed?

A. Allow TCP 443

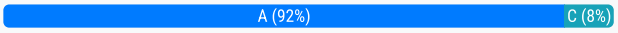
B. Allow UDP 1811

C. Allow UDP 8211

D. Allow TCP 22

Suggested Answer: *C*

Community vote distribution



Letu Most Recent 1 year, 12 months ago

If any firewall or network infrastructure device with ACLs are in the path, they must allow GRE and PAPI traffic. Enable GRE on IP protocol 47 and PAPI on UDP 8211

upvoted 1 times

SeidorBruno 2 years, 3 months ago

Page 775 Study Guide: This means that a HTTPS certificate has to be installed on the edge switch. [Aruba Networks]

upvoted 3 times

E_Nick 3 years ago

HTTPS uses TCP 443, so it is A and not C

upvoted 1 times

NetExpert 3 years, 1 month ago

A is correct

upvoted 1 times

d_nat 3 years, 2 months ago

Answer A is correct. Student Guide Vol2, page 115: "Roles can be configured locally on the switch using a Local User Role (LUR) or on a ClearPass server, using a downloadable user role (DUR). Roles that are configured locally can be assigned via any RADIUS server, using the Aruba-User-Role VSA. When using DUR, the ClearPass HPE-CPPM-Role VSA is used in combination with HTTPS to transfer the role to the switch."

upvoted 4 times

JazzyJ151 3 years, 5 months ago

DUR is a CPPM feature, so assumption is that the AAA is CPPM. AOS switches download their roles from CPPM using HTTPS, you just have to put a CA cert on the switch for the CPPM and reference the FQDN. Definitely A.

upvoted 2 times

SniBBz 3 years, 6 months ago

Answer is A

upvoted 1 times

jordib4 3 years, 9 months ago

pg 681 from the Aruba guide - "When using DUR, the ClearPass HPE-CPPM-Role VSA is used in combination with HTTPS to transfer the role to the switch." UDP 8211 (PAPI) is related to dynamic segmentation and the communication to the MC not DUR.

upvoted 2 times

sentinel44 3 years, 9 months ago

HTTPS uses TCP 443, so it is A and not C

upvoted 3 times

Mar_a_Lagoon 4 years ago

REST API is used for this, so A HTTPS

upvoted 3 times

kup 4 years, 1 month ago

C only this port mentioned in study book. v2-169

upvoted 1 times

Mrvn 4 years, 3 months ago

C is correct (HTTPS is used between switch and CPPM)

upvoted 1 times

AM1234 4 years, 4 months ago

The correct Answer is A

upvoted 1 times

fasty 4 years, 6 months ago

Correct it is A

upvoted 2 times

poris27 4 years, 6 months ago

I think the answer Should be A because something wrong with HTTPS maybe the switch failed to download the certificate or there is firewall block TCP443. If UDP 8211 (PAPI) is related for dynamic segmentation instead of DUR

upvoted 3 times

Question #18 *Topic 1*

A network administrator is attempting to troubleshoot a connectivity issue between a group of users and a particular server. The administrator needs to examine the packets over a period of time from their desktop; however, the administrator is not directly connected to the AOS-CX switch involved with the traffic flow.
What is correct regarding the ERSPAN session that needs to be established on an AOS-CX switch? (Choose two.)

A. On the source AOS-CX switch, the destination specified is the switch to which the administrator's desktop is connected

B. On the source AOS-CX switch, the destination specified is the administrator's desktop

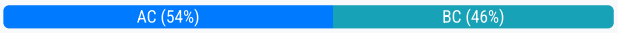
C. The encapsulation protocol used is GRE

D. The encapsulation protocol used is VXLAN

E. The encapsulation protocol is UDP

Suggested Answer: *B, C*

Community vote distribution



vrvinod Highly Voted 5 years, 4 months ago

In AOS CX the remote mirroring is done using a tunnel interface, so the Mirror source and destination must be configured on each Switch. On the source Switch, the source interface (from where the traffic is mirrored) and destination interface (the tunnel interface to where the traffic is sent to). In the destination Switch, the source interface (which would be the tunnel interface (receiving the traffic from the source switch tunnel)) and the destination would be the client where Wireshark enabled client is connected. So, the answer is A & C.

upvoted 14 times

cloud29 Highly Voted 5 years, 6 months ago

Acording to student guide, page 149. "AOS switches support mirroring to other AOS switches. AOS-CS switches, however, do not support this feature. Instead, the remote mirroring must be to a device that supports it, like Wireshark" Thats why, I think that the answer is B and C

upvoted 10 times

Flush_All Most Recent 1 year, 10 months ago

In ERSPAN, the traffic is encapsulated in GRE and is routed across layer 3 network between the source switch and the destination device, like a packet sniffer. so it B&C. A&C would be correct if we talk about remote port mirroring not ERSPAN

upvoted 1 times

BFDS 1 year, 11 months ago

AOS-CX don't support switch-to-switch mirroring. The answer is B and C

upvoted 1 times

johnhenri 2 years, 6 months ago

Selected Answer: AC

Learning book ACSP chap "Network Analytics Engine - Remote traffic Mirroring : ERSPAN" : "The traffic is encapsulated in generic routing encapsulation (GRE) and is, therefore, routable across layer 3 network between the source switch and the destination device, like a packet sniffer, for exemple Wireshark" "AOS switches support mirroring to other AOS switches. AOS-CX switches, however, do not support this feature. Instead, the remote mirroring must be to a device that support it, like Wireshark"

upvoted 1 times

johnhenri 2 years, 6 months ago

Learning book ACSP chap "Network Analytics Engine - Remote traffic Mirroring : ERSPAN" : "The traffic is encapsulated in generic routing encapsulation (GRE) and is, therefore, routable across layer 3 network between the source switch and the destination device, like a packet sniffer, for exemple Wireshark" "AOS switches support mirroring to other AOS switches. AOS-CX switches, however, do not support this feature. Instead, the remote mirroring must be to a device that support it, like Wireshark"error, i wan to say BC

upvoted 1 times

johnhenri 2 years, 6 months ago

error, i wan to say BC

upvoted 1 times

IngenieriaEGlobal 2 years, 7 months ago

BC correct options: ERSPAN is an acronym that stands for encapsulated remote switched port analyzer. ERSPAN mirrors traffic on one or more source ports and forwards the mirrored traffic to a destination on a remote device. The traffic is encapsulated in generic routing encapsulation (GRE) and is, therefore, routable across a layer 3 network between the source switch and the destination device, like a packet sniffer, e.g. Wireshark

upvoted 1 times

joalv 3 years, 1 month ago

BC. ERSPAN uses layer 3, so can send traffic directly to a device. https://community.arubanetworks.com/community-home/librarydocuments/viewdocument?DocumentKey=43a0aad6-4f7a-4cd2-83a0-3aa846accefd&CommunityKey=2fd943a6-8898-4dbe-915f-4f09e4d3c317&tab=librarydocuments

upvoted 1 times

OscarChew 3 years, 2 months ago

AOS-CX switches also support remote port mirroring, in which the switch forwards the mirrored packets to a destination device. The switch achieves this by encapsulating the mirrored packets in a GRE header that uses the remote switch's IP address as the destination. The remote, or destination, switch is configured to decapsulate traffic from this GRE tunnel and to forward the traffic out an exit port (see the previous slide on setting up local mirroring).

upvoted 4 times

SeidorBruno 3 years, 3 months ago

Page 159 Study Guide: ERSPAN is an acronym that stands for encapsulated remote switched port analyzer . ERSPAN mirrors traffic on one or more source ports and forwards the mirrored traffic to a destination on a remote device. The traffic is encapsulated in generic routing encapsulation (GRE) and is, therefore, routable across a layer 3 network between the source switch and the destination device, like a packet sniffer, e.g. Wireshark [Aruba Networks] In addition in page 160 it says: Note: AOS switches support mirroring to other AOS switches. AOS- CX switches, however, do not support this feature. Instead, the remote mirroring must be to a device that supports it, like Wireshark. [Aruba Networks] So, definetely B&C

upvoted 3 times

gcg 3 years, 4 months ago

the desktop of administrator is in other switch and the ERSPAN can send it traficc to the desktop administrator.

upvoted 1 times

slotblocker 3 years, 5 months ago

B and C, I found a guide for Aruba - ERSPAN solution with a workstation as a destination address. https://community.arubanetworks.com/community-home/librarydocuments/viewdocument?DocumentKey=43a0aad6-4f7a-4cd2-83a0-3aa846accefd&CommunityKey=2fd943a6-8898-4dbe-915f-4f09e4d3c317&tab=librarydocuments

upvoted 2 times

alex711 3 years, 8 months ago

BC is correct.

upvoted 1 times

tcan4075 3 years, 10 months ago

BC based on Airheads community

upvoted 2 times

sirtack 3 years, 11 months ago

https://community.arubanetworks.com/blogs/esupport1/2021/06/28/arubaos-cx-send-mirrored-traffic-to-workstation-with-erspan So BC

upvoted 1 times

IV2709 3 years, 12 months ago

GRE tunnel to the admin's desktop directly

upvoted 1 times

IV2709 3 years, 12 months ago

GRE to the admin's wireshark directly

upvoted 1 times

devadarshan91730 4 years ago

The question clearly says "the administrator is not directly connected to the AOS-CX switch" how come option A comes in. Answer is B and C.

upvoted 1 times

Question #19 *Topic 1*

What is correct regarding the operation of VSX and multicasting with PIM-SM routing configured?

A. Each VSX peers runs PIM and builds its own group database. One of the VSX peers is elected as the designated router (DR) to forward multicast streams to a receiver VLAN

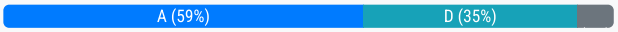
B. Each VSX peers runs PIM and creates a shared group database. Both VSX peers can forward multicast streams to receivers in a VLAN, achieving load sharing

C. Each VSX peers runs PIM and builds its own group database. Both VSX peers can forward multicast streams to receivers in a VLAN, achieving load sharing

D. Each VSX peers runs PIM and creates a shared group database. One of the VSX peers is elected as the designated router (DR) to forward multicast streams to a receiver VLAN

Suggested Answer: *B*

Community vote distribution



d_nat Most Recent 1 year, 10 months ago

B&C is correct It is stated in the Study Guide, as mentioned above: "AOS-CX switches, however, do not support this feature. Instead, the remote mirroring must be to a device that supports it, like Wireshark."

upvoted 1 times

SeidorBruno 3 years, 3 months ago

Page 634 Study Guide: Both VSX peers have the same Control Plane information. This means that both members will be able to establish PIM neighborships, send PIM Join messages to the RP and Build a Shortest Path Tree (SPT). However, multicast traffic (data plane) is only routed from the VSX peer that acts as the PIM DR. The mechanism to have a pre- established Control Plane on both VSX peers permits the VSX cluster to achieve a fast fail over in case the PIM DR fails. [Aruba Networks]

upvoted 3 times

Redrum702 3 years, 5 months ago

A: In Aruba VSX (Virtual Switching Extension), the VSX peers do not run PIM (Protocol Independent Multicast) individually and maintain their own multicast group databases.

upvoted 1 times

Redrum702 3 years, 5 months ago

A: Multicast Traffic Flow: In a VSX environment with PIM-SM, multicast traffic is forwarded based on the multicast distribution tree established by PIM-SM. Each physical switch in the VSX pair independently participates in the PIM-SM operations, including joining the appropriate multicast distribution tree and forwarding multicast traffic accordingly. VSX and Multicast: When operating VSX and using PIM-SM routing, each physical switch within the VSX pair independently runs PIM-SM. This means that each switch has its own RP and maintains its own multicast routing tables.

upvoted 1 times

slotblocker 3 years, 5 months ago

Answer is A: Multicast traffic to these IGMP groups is pruned/forwarded based on the individual IGMP group database on each VSX node. ISLP does not synchronize IGMP groups between VSX peers. Source: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7727/Content/Chp_prev_traf_loss/igm-sno-10.htm

upvoted 2 times

Alialo 3 years, 12 months ago

i think the Answer is A. Each VSX switch has an identical IGMP group database: • Each VSX node individually learns any JOIN/LEAVE message received from a downstream VSX LAG. • The VSX IGMP process translates the received IGMP from the ISL into an IGMP join message from the VSX LAG. Multicast traffic to these IGMP groups is pruned/forwarded based on the individual IGMP group database on each VSX node. ISLP does not synchronize IGMP groups between VSX peers. The IGMP database construction is a data-plane based process. - Chapter 7, Preventing traffic loss, "ArubaOS-CX Virtual Switching Extension (VSX) Guide for 10.03"

upvoted 3 times

IV2709 4 years ago

Answer D Same routing table for fast failover and one is elected DR and share traffic and the other one is DR Proxy.

upvoted 3 times

E_Nick 4 years ago

As the question stands A is correct.

upvoted 2 times

omen 4 years, 1 month ago

In my opinion it is D... A also sounds quite good, but it is crucial that both VSX peers have and use the same multicast tables. "Both the DR and proxy DR maintain the same multicast tables and build the shortest path tree." Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7888/Content/Chp_Pre_tra_loss/ip-mul-rou-10.htmI have to correct my statement, it is answer A. The IGMP Group DB is a copy, each peer has its own database

upvoted 3 times

omen 4 years, 1 month ago

Selected Answer: D

In my opinion it is D... A also sounds quite good, but it is crucial that both VSX peers have and use the same multicast tables. "Both the DR and proxy DR maintain the same multicast tables and build the shortest path tree." Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7888/Content/Chp_Pre_tra_loss/ip-mul-rou-10.htm

upvoted 3 times

omen 4 years, 1 month ago

I have to correct my statement, it is answer A. The IGMP Group DB is a copy, each peer has its own database

upvoted 2 times

Moreson 4 years, 8 months ago

"both VSX switches as a PIM Designate Router (DR). One node is the actual DR, the other node is the proxy DR." "Only the actual DR performs multicast routing and forward traffic destined to groups to its downstream VLANs in the data-path." https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7888/Content/Chp_Pre_tra_loss/ip-mul-rou-10.htm

upvoted 2 times

sentinel44 4 years, 9 months ago

it should be A

upvoted 2 times

Mar_a_Lagoon 5 years ago

As the question stands A is correct. As Mrvn says, each VSX peer can be the DR for a VLAN, but not both at the same time.

upvoted 2 times

kup 5 years, 1 month ago

In stufy book we can see that on peer stands as DR. meanst its A or D. I perefered A

upvoted 2 times

Mrvn 5 years, 4 months ago

C answer can be misleading though.. Each VSX peers runs PIM and builds its own group database.= correct Both VSX peers can forward multicast streams to receivers in a VLAN, = not same VLAN ! achieving load sharing = correct only if each VSX is configured as DR for different VLANs so answer A could be more correct as it is less open for misinterpretation

upvoted 4 times

Mrvn 5 years, 4 months ago

C is correct

upvoted 3 times

AM1234 5 years, 4 months ago

The correct Answer is A

upvoted 1 times

clupato2 5 years, 4 months ago

Yes: it should be A.

upvoted 1 times

Question #20 *Topic 1*

An administrator wants to track what configuration changes were made on a switch. What should the administrator implement to see the configuration changes on an AOS-CX switch?

A. AAA authorization

B. Network Analysis Engine (NAE)

C. AAA authentication

D. VSX synchronization logging

Suggested Answer: *B*

Community vote distribution

B (100%)

johnhenri Most Recent 2 years ago

On Chapitre 3 "Network Analytics Engine" from ACSP learning book : "NAE agents can continuously monitor many different aspects of the system. They will begin to detect issues before they cause problems for users. NAE agents also help to collect all relevant information at the moment that an issue is occurring. Relevant information may include what has changed on the system, output from CLI show commands, log files, configuration outputs, and tests such as traceroute, ping, and packet capture."

upvoted 1 times

SeidorBruno 2 years, 10 months ago

Page 85 Study Guide: The Audit feature records all hardware and software versions, as well as other configuration changes. You can then search and view all changes, or groups of changes. This allows you to track all changes to hardware, software, and configurations with automated versioning whether made through NetEdit or directly on the switch. You can immediately rollback to any previous configuration. You can perform these rollbacks selectively, based upon factors such as the location of the switches or the date of the changes. [Aruba Networks]

upvoted 1 times

E_Nick 3 years, 6 months ago

B is correct

upvoted 1 times

darthandy 4 years, 5 months ago

There's an agent you can install on a switch that tracks all network configurations using NAE.

upvoted 1 times

Mar_a_Lagoon 4 years, 6 months ago

I think B is supposed to be NetEdit, not NAE

upvoted 2 times

Disposable_Me_2018 4 years, 7 months ago

How is B correct?

upvoted 1 times

I_C_U 4 years, 7 months ago

B is the answer

upvoted 1 times

Kevin1983 4 years, 10 months ago

B is correct

upvoted 3 times

Question #21 *Topic 1*

Examine the AOS-CS switch output:

Based on this output, what is correct?

```
Switch# show aaa authentication port-access interface 1/1/1 client-status

Port Access Client Status Details

Client 00:50:56:b1:7a:37, icx-employee

Session Details
------------------------------------------------------------
  Port         : 1/1/3
  Session Time : 31273s

Authentication Details
------------------------------------------------------------
  Status          : dot1x Authenticated
  Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted

Authorization Details
------------------------------------------------------------
  Role      : aruba_contractor-3044-7
  Status    : Applied
```

A. 802.1X authentication was successful, but MAC authentication is yet to start

B. 802.1X authentication occurred and downloadable user roles are deployed

C. A local user role was deployed using a ClearPass solution

D. Only 802.1X authentication is configured on the port

Suggested Answer: *B*

Community vote distribution



SeidorBruno Highly Voted 3 years, 3 months ago

Page 435 Lab Guide: In this example, the numbers 3044 and 7. 3044: Every enforcement profile in ClearPass has an internal object number, the range starts at 3000. This is the unique identifier of the enforcement profile, while the name makes it easy to recognize it. 7: This is the version number. Every time an enforcement profile is saved, the version number is incremented with 1. The complete DUR consists of: • Enforcement Profile name: aruba_contractor • Enforcement Profile internal object number: 3044 • Enforcement Profile version number: 7

upvoted 5 times

Redrum702 3 years, 5 months ago

Correction B: When the configuration status shows "applied," it means that the specified AAA settings are in effect and active on the AOS-CX switch. This confirms that the configured authentication and authorization parameters are being used to control user access and permissions on the network.

upvoted 3 times

Redrum702 3 years, 5 months ago

D: If the output of the command show aaa authentication port-access interface client-status on an Aruba switch shows that "dot1x" is authenticated but "mac-auth" is not attempted, it means that the switch is successfully performing 802.1X authentication for clients on that interface, but it is not attempting MAC authentication.

upvoted 1 times

Killorp 4 years, 4 months ago

I too think it's B. The role 'aruba_contractor-3044-7' is the exact correct format for a DUR. See page 814.what do you mean by correct format ? you can name the role as you wish , the name doesnt point whether role is locally pushed or downloaded via clearpass. Actually, the role information section from the show command is where we can find out whether its local or clearpass, since its shown in the output so what we only conclude from this that 802.1x is the only method of authentication , so D is the correct answerMAC-auth has not been attempted does not mean, that it has not been configured on the switch port. So D is not correct in my opinion.

upvoted 1 times

Killorp 4 years, 4 months ago

Selected Answer: B

I too think it's B. The role 'aruba_contractor-3044-7' is the exact correct format for a DUR. See page 814.

upvoted 1 times

moe706706 3 years, 5 months ago

what do you mean by correct format ? you can name the role as you wish , the name doesnt point whether role is locally pushed or downloaded via clearpass. Actually, the role information section from the show command is where we can find out whether its local or clearpass, since its shown in the output so what we only conclude from this that 802.1x is the only method of authentication , so D is the correct answerMAC-auth has not been attempted does not mean, that it has not been configured on the switch port. So D is not correct in my opinion.

upvoted 1 times

moe706706 3 years, 5 months ago

what do you mean by correct format ? you can name the role as you wish , the name doesnt point whether role is locally pushed or downloaded via clearpass. Actually, the role information section from the show command is where we can find out whether its local or clearpass, since its shown in the output so what we only conclude from this that 802.1x is the only method of authentication , so D is the correct answer

upvoted 1 times

Luke80 Most Recent 1 year, 12 months ago

MAC-auth has not been attempted does not mean, that it has not been configured on the switch port. So D is not correct in my opinion.

upvoted 1 times

Luke80 4 years, 9 months ago

Look at the role that has been applied - looks like a typical DUR

upvoted 4 times

jordib4 4 years, 9 months ago

I think that its B. because the Role has been assigned as per the book page 723.

upvoted 3 times

DianaDecker 4 years, 10 months ago

It is D. (Book pages 703 & 711) No mac-auth configured.

upvoted 2 times

filthyx 4 years, 12 months ago

B seems correct. The precedense is: 802.1x and if it times out, mac-auth.

upvoted 3 times

Cloudeiv 5 years, 3 months ago

B is correcti think that it's A

upvoted 3 times

Cloudeiv 5 years, 3 months ago

B is correct

upvoted 3 times

Linares1234 5 years ago

i think that it's A

upvoted 1 times

Question #22 *Topic 1*

An administrator in a company of 349 users has a pair of AOS-CX switches with connections to external networks. Both switches are configured for OSPF. The administrator wants to import external routes on both switches, but assigns different seed metrics to the routes, as well as imports them as external type-1 routes.
What is the best way for the administrator to accomplish this?

A. Create a route map with the correct route type and metrics

B. Define the route type and metrics in the OSPF process

C. Create a classifier policy with the correct route type and metrics

D. Define a class and policy map with the correct route type and metrics

Suggested Answer: *A*

Community vote distribution

A (100%)

AM1234 Highly Voted 4 years, 10 months ago

The correct Answer is A

upvoted 6 times

johnhenri Most Recent 2 years ago

Chapitre 6 Advanced OSPF from ACSP learning book: "By default, all the routes from the route type will be redistributed unless you employ route maps. When you redistribute routes into OSPF, they are assigned a seed metric to them; a beginning cost value. If you specify a default metric with "default-metric" command, that would be applied to redistributed routes; if you want to have different metrics for different external routes, then use a route map to accomplish this task."

upvoted 1 times

SeidorBruno 2 years, 10 months ago

Page 381 Study Guide Page 235 Lab Guide: Configure a route map to control external cost types, such as Metric type1 and type2.

upvoted 2 times

E_Nick 3 years, 6 months ago

A is correct

upvoted 1 times

WifiX 4 years, 11 months ago

A is correct page 182 user guide

upvoted 2 times

cloud29 5 years ago

Sorry, A is correct. "To change the LSA metric-type (type 1 or 2), you must use a route map.

upvoted 1 times

cloud29 5 years ago

Shouldnt it be B?

upvoted 1 times

Question #23 *Topic 1*

An administrator is concerned about the security of the control plane connection between an AOS-CX switch and an Aruba Mobility Controller (MC) when implementing user-based tunneling. How should the administrator protect this traffic?

A. IPSec with a digital certificate

B. GRE with a pre-shared key

C. PAPI with an MD5 pre-shared key

D. IPSec with a pre-shared key

Suggested Answer: *C*

Community vote distribution

C (100%)

SeidorBruno Most Recent 2 years, 3 months ago

Page 762 Study Guide: Important: You should always implement PAPI MD5 security to protect communications between the controller and switch, as well as protecting against malicious misuses of licenses, since each switch request consumes a license(s) on the MC. [Aruba Networks]

upvoted 2 times

d_nat 3 years ago

I think it is C. Implementing ArubaOS-CX Switching Rev 20.21, page 164: "(...) However, where APs use IPSec to protect the PAPI connection between the AP and MC, AOS-CX switches do not support this protection. Instead, you can optionally implement an MD5 HMAC function to protect PAPI between the AOS-CX switches and MCs"

upvoted 1 times

omen 3 years, 1 month ago

Agreed, answer is C

upvoted 1 times

Kevin1983 4 years, 4 months ago

C (page 785 Study Book)

upvoted 3 times

AM1234 4 years, 4 months ago

The correct Answer is C

upvoted 1 times

Moshiko 4 years, 5 months ago

The answer is C, Page 343

upvoted 2 times

Question #24 *Topic 1*

A network administrator is implementing a configuration plan in NetEdit. The administrator used NetEdit to push the configuration plan to the switch. Which option in the NetEdit planning section should the administrator select to save the configuration running on the switch to the startup-config?

A. EDIT

B. VALIDATE

C. COMMIT

D. DEPLOY

Suggested Answer: *C*

Community vote distribution

C (100%)

Kaldimaar Highly Voted 4 years, 3 months ago

C. Deploy puts the config to running-config, Commit saves it to startup-config.

upvoted 7 times

SeidorBruno Most Recent 2 years, 3 months ago

Page 83 Study Guide: Write (Commit) the deployed running configuration to startup. [Aruba Networks]

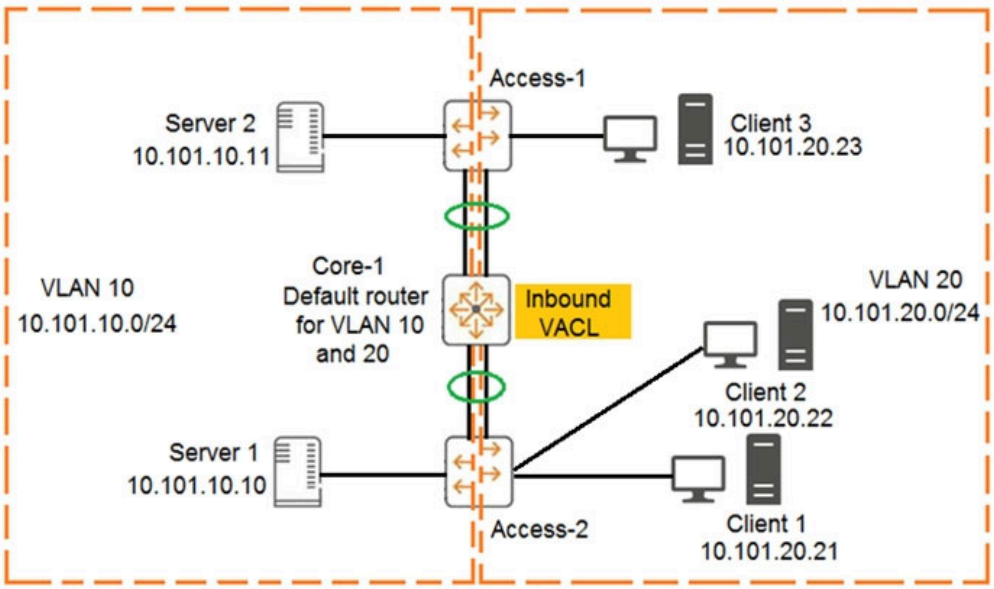
upvoted 2 times

Question #25 *Topic 1*

Examine the network exhibit:

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

If telnet was being used, which device connection would be permitted and functional in both directions? (Choose two.)




```
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
```

A. Client 3 to Client 2

B. Client 1 to Client 2

C. Server 2 to Client 2

D. Server 1 to Client 1

E. Client 1 to Client 3

Suggested Answer: *B, E*

Community vote distribution

BD (92%)

pabx31 Highly Voted 5 years ago

E is wrong Inbound VACL will apply to all ports that are receiving the VLAN traffic. Client 1 may be able to reach client 3 but the traffic will not return since it will be dropped by the VACL. B is correct because the traffic never crosses the core so the VACL is not used. D is correct because the server is inbound to VLAN 10 so VACL is not used and return traffic is permitted by VACL. C is wrong because the return traffic will cross the ACL and is not permitted for client 2. This picture is in my book and traffic flow is explained.

upvoted 7 times

sentinel44 Highly Voted 4 years, 9 months ago

BD is correct

upvoted 6 times

johnhenri 2 years, 7 months ago

BD is correct

upvoted 1 times

udo2020 3 years, 1 month ago

The only valid solution is B and E because traffic within vlan 20 is not affected from the VACL. Traffic from server 1 will be blocked because of a wrong IP source.This one is correct

upvoted 2 times

udo2020 3 years, 1 month ago

The only valid solution is B and E because traffic within vlan 20 is not affected from the VACL. Traffic from server 1 will be blocked because of a wrong IP source.

upvoted 2 times

demanmetdehamer Most Recent 2 years ago

This one is correct

upvoted 1 times

OscarChew 3 years, 2 months ago

BE is correct

upvoted 1 times

SeidorBruno 3 years, 3 months ago

CLIENT1 - CLIENT2 - pass - Forwarded by Access2, no need to go trough CORE1 SERVER1- CLIENT1 - pass - Server 1 inbound VLAN10 on CORE1 return traffic from CLIENT1 in VLAN 20 match the ACL and is permitted.

upvoted 3 times

poy4242 4 years, 6 months ago

CL3 - CL2 - drop on forward path by core1 cause match VLAN 20 and CL3 not CL1 as SRC IP CL1 - CL2 - pass - no ACL cause forwarded by Access2 SR2 - CL2 - pass on forward path by core1 cause match VLAN 10 Drop on return path by core1 cause match VLAN 20 and no CL1 as SRC IP SR1 - CL1 - pass on forward path by core1 cause match VLAN 10 pass on return path by core1 cause match VLAN 20 and CL1 as SRC IP CL1 - CL3 - pass on forward path by core1 cause match VLAN 20 and CL1 as SRC IP drop on return path by core1 cause match VLAN 20 and not CL1 but CL3 as SRC IP

upvoted 2 times

Mar_a_Lagoon 5 years ago

E is correct because that traffic never passes through core, so never hits the VACL.

upvoted 2 times

Disposable_Me_2018 5 years, 1 month ago

Only correct answer I can see is B. Can somebody explain how options D or E can operate in both directions through that VACL?

upvoted 1 times

Disposable_Me_2018 5 years, 1 month ago

Only correct answer I can see is B. Can somebody explain how options D or E can operate in both directions through that VACL?D - because initial traffic (inbound vlan 10) is not matched on VACL to the client, but return traffic (inbound vlan 20) is matched and permitted by ACL.

upvoted 1 times

gondolf 4 years, 6 months ago

D - because initial traffic (inbound vlan 10) is not matched on VACL to the client, but return traffic (inbound vlan 20) is matched and permitted by ACL.

upvoted 2 times

kup 5 years, 1 month ago

BE correct . Servers in another vlan and must go thru core from another interface and our rule will no mutch these traffic. a has a n implicit deny

upvoted 3 times

I_C_U 5 years, 1 month ago

what you seem to be forgetting here is the VACL will only apply on core 1 for traffic that is coming into the switch and into VLAN 20, so any device outside VLAN 20 will not have the source IP of the client. Hence B and E are correct.

upvoted 3 times

clupato2 5 years, 2 months ago

B & E is correct. ACL permits traffic only from 10.101.20.21/32 IP address that is Client1. The question asks for a connection "in both directions". So only devices in the same VLAN can communicate in both directions, as they are not affected by a VACL.

upvoted 3 times

seb6869 5 years, 2 months ago

The correct answer is B&D

upvoted 1 times

AM1234 5 years, 4 months ago

The correct Answer is B&D

upvoted 1 times

Williams926 5 years, 4 months ago

I think correct answer is B&D. Because inbound VACL filter all traffic arrives on a VLAN whether switched or routed.

upvoted 2 times

public2002 5 years, 5 months ago

So D&E are the only possible connections. Client1 to Client2 will work but not affected by the ACL

upvoted 1 times

public2002 5 years, 5 months ago

and the telnet traffic must flow through the core switch

upvoted 1 times

Question #26 *Topic 1*

An administrator has an aggregation layer of 8325CX switches configured as a VSX pair. The administrator is concerned that when OSPF network changes occur, the aggregation switches will respond to the changes slowly, and this will affect network connectivity, especially VoIP calls, in the connected access layer switches.
What should the administrator do on the aggregation layer switches to alleviate this issue?

A. Implement route aggregation

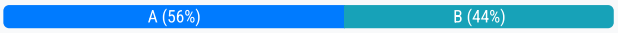
B. Implement bidirectional forwarding detection (BFD)

C. Reduce the hello and dead interval timers

D. Implement graceful restart

Suggested Answer: *A*

Community vote distribution



I_C_U Highly Voted 4 years, 7 months ago
Answer is A, question is asking about OSPF routing changes and not about the neighbour going down. BFD is useful only when neighbour goes down. If you aggregate routes then there will be less chance of the individual routing change impacting this router
upvoted 12 times

I_C_U Highly Voted 4 years, 7 months ago
Answer is A, question is asking about OSPF routing changes and not about the neighbour going down. BFD is useful only when neighbour goes down. If you aggregate routes then there will be less chance of the individual routing change impacting this router100% Agree. Answer is A. "Network Changes" mean route table updates not neighbors going down which would be the only reason B would make sense.
upvoted 12 times

watermellonhead 4 years, 7 months ago
100% Agree. Answer is A. "Network Changes" mean route table updates not neighbors going down which would be the only reason B would make sense.
upvoted 9 times

johnhenri Most Recent 2 years ago
On ACSP Learning book, chapitre 6 Advanced OSPF section "Need for Route and LSA Aggregation Between Areas" : Router do not require granular knowledge of other area : - Causes unnecessary disruptions when small changes occur - Clutter the LSDB and routing table Simply dividing an AS into multiple areas begins to decrease the size of OSPF router's LSDBs and to reduce the complexity of SPF calculations. However, to achieve the true benefits of multiple areas, you should further reduce the number of LSAs advertised between areas... You need to aggregate the Type 3 LSAs to hide the unnecessary information and to smooth over small changes, thereby gaining the true benefits of a multiple area OSPF configuration" & Question is talking about OSPF routing changes, BFD is used when neighbor is down.
upvoted 1 times

SeidorBruno 2 years, 10 months ago
Page 368 Study Guide
upvoted 3 times

Greenmile84 2 years, 10 months ago
Should be B. Fast convergence, including features like BFD, VSX operations with OSPF and OSPF graceful restart
upvoted 1 times

slotblocker 2 years, 11 months ago
BFD " We can tune timers for fast convergence, for example OSPF can be configured to use a dead interval of only one second. The problem however is that all of these protocols were never really designed for sub-second failover. Hello packets and such are processed by the control plane so there is quite some overhead. BFD was designed to be fast, its packets can be processed by some interface modules or line cards so there isn't much overhead. BFD runs independent from any other (routing) protocols. Once it's up and running, you can configure protocols like OSPF, EIGRP, BGP, HSRP, MPLS LDP etc. to use BFD for link failure detection instead of their own mechanisms. When the link fails, BFD will inform the protocol. "
upvoted 2 times

Redrum702 2 years, 11 months ago

A: the question implies a routing update has occurred so route aggregation is the only suitable answer

upvoted 1 times

Alialo 3 years, 6 months ago

i think B makes most sense in this scenario. It is one VSX is AGGREGATION layer, not Core Layer, and affect the service from Access layer. when i see the route aggregation in A, the first the that came to mind is ABR. BTW, in study guide, Aruba explained the BFD and how to use it direct after the chapter OSPF Failover and Convergence.

upvoted 4 times

devadarshan91730 3 years, 6 months ago

OSPF aggregation combines groups of routes with common addresses into a single routing table entry. However, The Bidirectional Forwarding Detection (BFD) protocol is a simple hello mechanism that detects failures in a network. The question says "network changes occur," which in case a link failure or link flap, where BFD fits well.

upvoted 1 times

d_nat 3 years, 6 months ago

For me, A makes most sense. As these are aggregation switches, aggregating the routes makes sense. B (BFD) concerns with a peer being not reachable anymore, so it does not apply in this case. C won't help, as it concerns also the reachability of peers. I fail to see the benefit in respond time of D

upvoted 1 times

rasmusbirkelund 3 years, 7 months ago

While I can certainly see that B would be the the answer, as it provides faster detection when a neighbor fails, the question states that the Administrator is concerned about network changes, and that the Agg-pair will respond slowly. Wouldn't Graceful Restart be the best option here?

upvoted 1 times

omen 3 years, 7 months ago

The question is about an aggregation switch and not about a core, therefore A makes the most sense... B,C and D would make sense if we were talking about the Core.

upvoted 2 times

JazzyJ151 3 years, 11 months ago

BFD - those echos will fail faster than the ospf hello/dead timers.

upvoted 1 times

poy4242 4 years ago

B will reduce neigbor failure detection, aggregating route will reduce the possibility of route calculation when topology change

upvoted 2 times

sentinel44 4 years, 3 months ago

B is correct (Book 437 & 438)

upvoted 1 times

DianaDecker 4 years, 3 months ago

B is correct (Book 437 & 438)

upvoted 1 times

AM1234 4 years, 10 months ago

The correct Answer is B

upvoted 2 times

cloud29 5 years ago

I think the answer is B "BFD tests the connectivity between two IP addresses in a BFD session. BFD reports when connectivity is lost. The router (or routing switch) can then use that information to take the appropriate actions, depending on the functions to which you have tied BFD"It states " BFD reports when connectivity is lost." So this is about a peer failure, not a routing change. That's why I think A is correct

upvoted 3 times

cloud29 5 years ago

I think the answer is B

"BFD tests the connectivity between two IP addresses in a BFD session. BFD reports when connectivity is lost. The router (or routing switch) can then use that information to take the appropriate actions, depending on the functions to which you have tied BFD"

upvoted 3 times

d_nat 3 years, 6 months ago

It states " BFD reports when connectivity is lost." So this is about a peer failure, not a routing change. That's why I think A is correct

upvoted 1 times

Question #27 *Topic 1*

How is NetEdit installed at a customer location?

A. Via an Aruba NetEdit hardware appliance

B. Via a DVD using a virtualized platform like Microsoft's Hyper-V

C. Via the Aruba Central cloud solution

D. Via an OVA file and a virtualized platform like VMware's ESXi

Suggested Answer: *D*

Community vote distribution

D (100%)

SeidorBruno Most Recent 2 years, 3 months ago

Page 61 Study Guide: NetEdit runs as an Open Virtualization Application (OVA) virtual machine (for example, VMware's ESXi , KVM, Hyper- V, etc.) on a server. [Aruba Networks]

upvoted 2 times

d_nat 3 years ago

You download the OVA from asp.arubanetworks.com and deploy it, so D is correct

upvoted 1 times

JazzyJ151 3 years, 5 months ago

Only available as OVA.

upvoted 1 times

SniBBz 3 years, 6 months ago

D is correct

upvoted 1 times

sentinel44 3 years, 10 months ago

D si correct

upvoted 3 times

AM1234 4 years, 4 months ago

D correct

upvoted 3 times

Question #28 *Topic 1*

What is correct regarding multicasting and AOS-CX switches?

A. IGMP snooping is disabled, by default, on Layer-2 VLAN interfaces

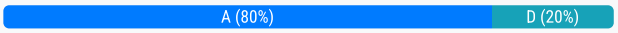
B. IGMP query functions are enabled, by default, on Layer-2 VLAN interfaces

C. IGMP snooping is enabled, by default, on Layer-3 VLAN interfaces

D. IGMP-enabled AOS-CX switches flood unknown multicast destinations

Suggested Answer: *D*

Community vote distribution



AM1234 Highly Voted 5 years, 4 months ago

The correct Answer is A

upvoted 7 times

sentinel44 Highly Voted 4 years, 9 months ago

Correct answer is A

upvoted 7 times

johnnyC_1704 Most Recent 2 years, 2 months ago

A is the correct aswer

upvoted 1 times

Wouter1976 2 years, 3 months ago

IGMP is a L3 protocol and disabled bu default. A/B/C do not match these criteria. Awnser = D

upvoted 1 times

onaicul 3 years, 3 months ago

A is correct : https://www.arubanetworks.com/techdocs/AOS-CX/10.11/HTML/cli_6200/Content/Chp_igmp_sno/igmp_sno_cmds/ip-igm-sno-vlan.htm

upvoted 1 times

SeidorBruno 3 years, 3 months ago

Selected Answer: D

Page 565 Study Guide: One exception applies: an IGMP snooping switch DOES forward both unknown and known multicasts on any port on which it has heard IGMP queries – port 1/1 in the figure. This behavior is required so that a multicast stream can reach the multicast router. In fact, by default, the switch forwards unknown multicasts that arrive on one VLAN on any port on which it has heard queries in any VLAN. To change this behavior and restrict forwarding to querier ports for that specific VLAN, enter the command: Switch(config)# ip igmp snooping drop- unknown vlan- exclusive [Aruba Networks]

upvoted 3 times

SeidorBruno 3 years, 3 months ago

Page 565 Study Guide: One exception applies: an IGMP snooping switch DOES forward both unknown and known multicasts on any port on which it has heard IGMP queries – port 1/1 in the figure. This behavior is required so that a multicast stream can reach the multicast router. In fact, by default, the switch forwards unknown multicasts that arrive on one VLAN on any port on which it has heard queries in any VLAN. To change this behavior and restrict forwarding to querier ports for that specific VLAN, enter the command: Switch(config)# ip igmp snooping drop- unknown vlan- exclusive [Aruba Networks]The IGMP enabled switch will filter the unknown traffic , but the IGMP-snooping switch will forward it. so I think D is not correct

upvoted 3 times

mammoura 3 years, 3 months ago

The IGMP enabled switch will filter the unknown traffic , but the IGMP-snooping switch will forward it. so I think D is not correct

upvoted 1 times

Redrum702 3 years, 5 months ago

Disregard my answer of B. The correct answer is A :)

upvoted 2 times

Redrum702 3 years, 5 months ago

B: On Aruba AOS-CX switches, IGMP query functions are enabled by default on Layer-2 VLAN interfaces. IGMP (Internet Group Management Protocol) queries are used to discover multicast group memberships and maintain the multicast group membership information within a VLAN. When IGMP snooping is enabled on a Layer-2 VLAN interface, the switch actively sends IGMP queries to the hosts within the VLAN to discover which multicast groups they are interested in. These queries allow the switch to build and maintain the multicast forwarding tables, ensuring that multicast traffic is forwarded only to the ports where interested receivers are located. A is incorrect: on Aruba AOS-CX switches, IGMP snooping is enabled by default on Layer-2 VLAN interfaces. IGMP snooping is a feature that allows switches to monitor IGMP messages exchanged between hosts and multicast routers, enabling the switch to learn which hosts are interested in receiving specific multicast traffic and selectively forward the multicast traffic to those hosts.

upvoted 1 times

QiQi 3 years, 6 months ago

IGMP default configuration: IGMP is disabled by default. The default IGMP version is IGMPv3. https://www.arubanetworks.com/techdocs/AOS-CX/10.07/PDF/5200-7876.pdf page17

upvoted 1 times

alex711 3 years, 7 months ago

I think it is D

upvoted 1 times

omen 4 years, 1 month ago

Correct answer is A

upvoted 2 times

aru_n 4 years, 10 months ago

Correct answer is A

upvoted 2 times

clupato2 5 years, 4 months ago

I think the answer is A

upvoted 3 times

Davidkanigui1 5 years, 5 months ago

I agree the answer should be A

upvoted 2 times

cloud29 5 years, 6 months ago

The answer should be A

upvoted 3 times

poris27 5 years, 6 months ago

I think the answer is A

upvoted 4 times

Question #29 *Topic 1*

A company has recently upgraded their campus switching infrastructure with AOS-CX switches. They have implemented 802.1X authentication on access ports where laptop and IOT devices typically connect. An administrator has noticed that for POE devices, the AOS-CX switch ports are delivering the maximum wattage to the port instead of what the device actually needs. Upon connecting the IoT devices, the devices request the maximum wattage through information exchange.
Concerned about this waste of electricity, what should the administrator implement to solve this problem?

A. Implement a classifier policy with the correct power definitions

B. Create device profiles with the correct power definitions

C. Enable AAA authentication to exempt LLDP and/or CDP information

D. Globally enable the QoS trust setting for LLDP and/or CDP

Suggested Answer: *B*

Community vote distribution

C (75%) B (25%)

Southpaw0125 Most Recent 1 year, 11 months ago
How can C Be correct if it says EXEMPT LLDP / CDP from the interface?
upvoted 2 times

SeidorBruno 2 years, 10 months ago
Page 875 Study Guide: Device profile with LLDP-MED First the devices do a handshake to negotiate PoE, if required. [Aruba Networks]..... If you are implementing authentication on the port, like 802.1X, MAC authentication, or captive portal, remember to allow LLDP: switch(config)# interface switch(config- if)# aaa authentication port- access allow- lldp- bpdu [Aruba Networks]
upvoted 2 times

Redrum702 2 years, 11 months ago
B: Device Profiles provide for PoE Priority and Allocation of power
upvoted 2 times

alex711 3 years, 2 months ago
B is correct, see the link. https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-switch/cfg/conf-device-profile.htm
upvoted 2 times

Jo2241 3 years, 6 months ago
Answer C - The negotiation must take place before the authentication. Whether for LLDP or CDP (e.g.: voip phone or camera)
upvoted 2 times

Jo2241 3 years, 6 months ago
Answer C - Disable LLDP on the switch makes no sense.
upvoted 2 times

Rockford 3 years, 6 months ago
Agree C: When phones receive Power over Ethernet (PoE) from the switch, LLDP- MED can help the switch allocate and deliver exactly the power that the phone needs. If you are implementing authentication on the port, like 802.1X, MAC authentication, or captive portal, remember to allow LLDP: switch(config)# interface switch(config- if)# aaa authentication port- access allow- lldp- bpdu
upvoted 2 times

Seegurke9 3 years, 7 months ago
Answer C; p.359
upvoted 4 times

Question #30 *Topic 1*

A company requires access by all users, guests, and employees to be authenticated. Employees will be authenticated using 802.1X, whereas guests will be authenticated using captive portal. Which type of authentication must be configured on an AOS-CX switch ports where both guests and employees connect?

A. Both 802.1X and captive portal

B. 802.1X only

C. Both 802.1X and MAC-Auth

D. 802.1X, captive portal, and MAC-Auth

Suggested Answer: *B*

Community vote distribution

C (95%) (5%

sentinel44 Highly Voted 4 years, 3 months ago

C is correct. Employees use 802.1x The Aruba guest solution uses MAC-auth. The Portal is not configured on the switch port.

upvoted 9 times

poris27 Highly Voted 5 years ago

I think the answer should be C

upvoted 5 times

johnhenri Most Recent 2 years ago

C is correct On Chap 15 "Captive Portal Authentication" of learning book "Aruba Certified Switching Professionnal": "Since captive portal is implemented with MAC Authentication and RADIUS COA on the AOS-CX switches, only MAC authentication needs to be enabled on the port. Optionnally, you can enable both 802.1x and MAC-auth if you are not sure what type of authentication will be necessary on a switch"

upvoted 1 times

Pierrou 2 years, 6 months ago

https://www.arubanetworks.com/techdocs/Instant_85_WebHelp/Content/instant-ug/authentication/mac-cpportal-au.htm

upvoted 1 times

onaicul 2 years, 9 months ago

C is correct Not configurable captive portal on switch only MAC-auth and 802.1x

upvoted 1 times

SeidorBruno 2 years, 10 months ago

Page 929 Study Guide: The captive portal solution provides user access based on http/https redirection. First the client does MAC or 802.1X authentication. [Aruba Networks]

upvoted 2 times

hongducnp 3 years ago

B is correct.

upvoted 1 times

Alialo 3 years, 6 months ago

After successful authentication on captive portal server, the client will go through MAC authentication on the switch and upon successful authentication, the client will get the access to the internet.

upvoted 1 times

Killorp 3 years, 10 months ago

I think C is correct. See page 977 Study Guide. Unregistered device. Authentication on Port : Required: RADIUS MAC-Auth Optional add on: 802.1X (for employee onboarding solutions)

upvoted 3 times

guidogiesen 3 years, 12 months ago

Captive Portal should manage MAc-address itself, no need mac-auth configured on the switch port I belive. only 802.1x needed

upvoted 1 times

Luke80 4 years, 3 months ago

C is correct - also see page 334 on official student guide vol 2

upvoted 4 times

Disposable_Me_2018 4 years, 7 months ago

C is correct. Employees use 802.1x The Aruba guest solution uses MAC-auth. The Portal is not configured on the switch port.

upvoted 3 times

Mrvn 4 years, 10 months ago

C is the correct answer - MAC-auth (for captive portal) and 802.1x on port configAAA needed for captive, not MAC addressYou don't need MAC-auth for GUESTS users through a captive portal.

upvoted 4 times

Mrvn 4 years, 10 months ago

C is the correct answer - MAC-auth (for captive portal) and 802.1x on port config

upvoted 4 times

kup 4 years, 7 months ago

AAA needed for captive, not MAC address

upvoted 1 times

clupato2 4 years, 8 months ago

You don't need MAC-auth for GUESTS users through a captive portal.

upvoted 2 times

AM1234 4 years, 10 months ago

The correct Answer is C

upvoted 1 times

clupato2 4 years, 10 months ago

B is correct. You configure captive-portal authentication globally on the switch, but ON THE PORTS, you only need 802.1X

upvoted 4 times

cloud29 5 years ago

If they guest need to be authenticated with captive portal, why D is not the correct answere?

upvoted 1 times

Question #31 *Topic 1*

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?

A. The certificate that ClearPass uses in invalid

B. The AOS-CX switch does not have the ClearPass certificate involved

C. DNS fails to resolve the ClearPass server's FQDN

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

Suggested Answer: *A*

Community vote distribution

C (100%)

sentinel44 Highly Voted 3 years, 9 months ago
C is correct DNS - page -2/201
upvoted 5 times

SeidorBruno Most Recent 2 years, 3 months ago
Page 789: parsing_failed status, typically indicative of either a DNS or network connectivity issue. [Aruba Networks]
upvoted 3 times

Greenmile84 2 years, 4 months ago
Sorry, my mistake Answer C 100% a parsing failed status typically indicative of either a DNS, or network connectivity issue
upvoted 1 times

Greenmile84 2 years, 4 months ago
Answer D 100% a parsing failed status typically indicative of either a DNS, or network connectivity issue
upvoted 1 times

SirNebur85 3 years ago
C is correct DNS - page -2/201
upvoted 3 times

omen 3 years, 1 month ago
"Status: failed, parsing_failed" clearly indicates a DNS problem according to the guide. Answer is C
upvoted 3 times

kup 4 years, 1 month ago
C is correct DNS - page -2/201I can confirm this. "The top-right example shows a parsing_failed status, typically indicative of either a DNS or network connectivity issue."
upvoted 4 times

kup 4 years, 1 month ago
C is correct DNS - page -2/201
upvoted 4 times

Roebi 3 years, 10 months ago
I can confirm this. "The top-right example shows a parsing_failed status, typically indicative of either a DNS or network connectivity issue."
upvoted 4 times

Cloudeiv 4 years, 3 months ago

The correct answer is c. This information is in guide

upvoted 2 times

AM1234 4 years, 4 months ago

The correct Answer is C

upvoted 2 times

cloud29 4 years, 6 months ago

C is the answer

upvoted 1 times

poris27 4 years, 6 months ago

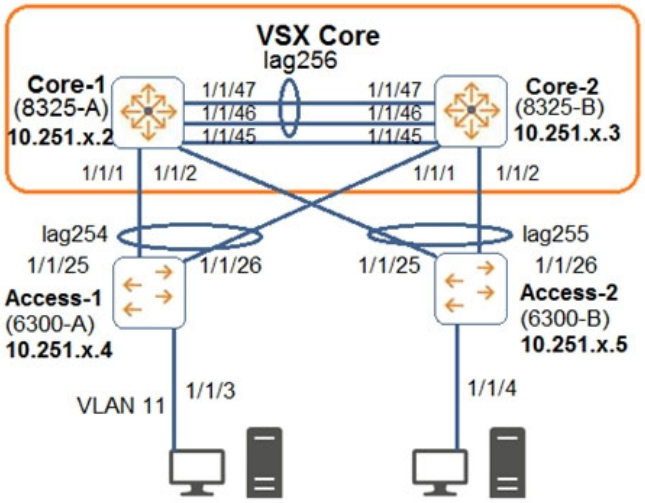
I think the answer should be C

upvoted 2 times

Question #32 *Topic 1*

Examine the attached diagram.

The two PCs are located in VLAN 11 (10.1.11.0/24). Which example defines how to implement active gateway on the VSX core for VLAN 11?



A. interface vlan 11 active-gateway ip 10.1.11.1 active-gateway mac 02:02:00:00:01:00

B. interface lag 254 active-gateway vlan 11 ip 10.1.11.1 active-gateway vlan 11 mac 02:02:00:00:01:00

C. interface lag 254 active-gateway ip 10.1.11.1 active-gateway mac 02:02:00:00:01:00

D. vsx vrrp group 1

Suggested Answer: *A*

Community vote distribution

A (100%)

cloud29 Highly Voted 4 years, 6 months ago

A is correct

upvoted 7 times

SeidorBruno Most Recent 2 years, 3 months ago

Page 417 Study Guide: The VSX pair is probably the default gateway for subnets such as those associated with VLANs 10 and 20 . You should typically set up the active gateway feature on those VLANs. [Aruba Networks]

upvoted 1 times

SirNebur85 3 years ago

A is correct

upvoted 2 times

Question #33 *Topic 1*

An administrator has configured the following on an AOS-CX switch:

What is the correct ACL rule configuration that would allow traffic from anywhere to reach the web ports on the two specified servers?

```
object-group ip address web-servers
  10.1.12.2
  10.1.12.3
  exit
object-group port web-ports
  eq 80
  eq 443
```

A. access-list ip server 10 permit tcp any web-servers group web-ports

B. access-list ip server 10 permit tcp any object-group web-servers object-group web-ports

C. access-list ip server 10 permit tcp any group web-servers group web-ports

D. access-list ip server 10 permit tcp any web-servers web-ports

Suggested Answer: *D*

Community vote distribution

A (100%)

clupato2 Highly Voted 4 years, 2 months ago

It's A: only port groups need to be preceded by the "group" parameter.

upvoted 6 times

AM1234 Highly Voted 4 years, 4 months ago

The correct Answer is A

upvoted 5 times

FAJE35 Most Recent 2 years, 1 month ago

A is correct

upvoted 1 times

SeidorBruno 2 years, 3 months ago

Page 296 Study Guide: The figure shows an example of configuring both IP and port object groups, which are then applied to an ACL. Note that you precede a port group in the ACL with the keyword group. [Aruba Networks]

upvoted 2 times

alex711 2 years, 8 months ago

A is Correct.

upvoted 1 times

omen 3 years, 1 month ago

Answer is A. CLI Context tested and approved Switch1(config-acl-ip)# show run cur access-list ip server 10 permit tcp any web-servers group web-portsThat's a helpful output. Thank you. So A it is

upvoted 5 times

omen 3 years, 1 month ago

Selected Answer: A

Answer is A. CLI Context tested and approved

Switch1(config-acl-ip)# show run cur access-list ip server 10 permit tcp any web-servers group web-ports

upvoted 5 times

d_nat 3 years ago

That's a helpful output. Thank you. So A it is

upvoted 1 times

Luke80 3 years, 9 months ago

A is correct

upvoted 1 times

DianaDecker 3 years, 10 months ago

A is correct. See book page 304

upvoted 1 times

Davidkanigui 4 years, 3 months ago

Sorry, correct answer is A

upvoted 4 times

Davidkanigui 4 years, 3 months ago

I think the correct answer is C See example on Page 303-304 student Guide Vo.1 Rev 20.21

upvoted 2 times

clupato2 4 years, 4 months ago

A is the answer

upvoted 4 times

cloud29 4 years, 6 months ago

A should be the answer

upvoted 3 times

poris27 4 years, 6 months ago

I think the answer should be A. Page 303 studeng guide Vo.1 Rev 20.21

upvoted 4 times

Question #34 *Topic 1*

A network administrator wants to centralize the management of AOS-CX switches by implementing NetEdit. How should the administrator purchase and/or install the NetEdit solution?

A. Install as a hardware appliance

B. Installed on a supported version of RedHat Enterprise Linux

C. Installed in a virtualized solution by using the Aruba-supplied OVA file

D. Installed on a supported version of Debian Linux

Suggested Answer: *C*

Community vote distribution

C (100%)

SeidorBruno Most Recent 2 years, 3 months ago

Page 61 Study Guide: NetEdit supports all switches running AOS- CX. NetEdit runs as an Open Virtualization Application (OVA) virtual machine (for example, VMware's ESXi , KVM, Hyper- V, etc.) on a server. [Aruba Networks]

upvoted 1 times

d_nat 3 years ago

Download the OVA from asp.arubanetworks.com

upvoted 1 times

E_Nick 3 years ago

C. Installed in a virtualized solution by using the Aruba-supplied OVA file

upvoted 1 times

AM1234 4 years, 4 months ago

C is Correct

upvoted 3 times

Question #35 *Topic 1*

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?

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

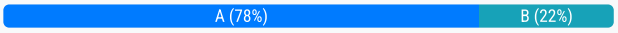
B. Disable LLDP globally on the AOS-CX switches where phones are connected

C. Disable SSH access on all the VoIP phones

D. Disable the RESTful API on all the VoIP phones

Suggested Answer: *A*

Community vote distribution



clupato2 Highly Voted 4 years, 2 months ago

I think it' A. Netedit uses LLDP to discover the devices, but it adds them in the topology only if the credentials set for the subnet work with those devices. Credential you can set are: - SNMP; - SSH; - SNMP. So, the best matching answer is A.

upvoted 8 times

haus24 Most Recent 2 years, 2 months ago

A is correct.

upvoted 1 times

SeidorBruno 2 years, 3 months ago

Page 79 Study Guide: Third- party support NetEdit supports any third- party devices that use SNMP. [Aruba Networks]

upvoted 3 times

Redrum702 2 years, 4 months ago

Correction - answer is A: To manage VoIP phones in Aruba NetEdit, you would typically configure the SNMP settings on the VoIP phone itself, such as specifying the SNMP community string and enabling SNMP-based management. Aruba NetEdit can then communicate with the VoIP phone using SNMP to retrieve its configuration and perform configuration management tasks.

upvoted 1 times

Redrum702 2 years, 5 months ago

B: If you prefer not to see the third-party VoIP phones in the NetEdit topology, you may have the option to disable CDP or LLDP on the switch ports to prevent the discovery and inclusion of those devices. However, disabling these protocols could limit the visibility and information available for network troubleshooting and monitoring.

upvoted 1 times

Alialo 2 years, 12 months ago

I think it should be A, refer to the Video "https://www.youtube.com/watch?v=DMpF4RoSE2I". For Answer B, disable global LLDP will affect the other devices connected to the Switches. I understand it is not good idea.

upvoted 1 times

omen 3 years, 1 month ago

A is Correct, agree with clupato2.

upvoted 2 times

Moreson 3 years, 8 months ago

initial discovery is using SNMP/REST API/SSH, for sure but once entering seed and found, it would use LLDP to discover all connected devices, so use B, as it is not practical to login each phone to change SNMP, as they are 'a lot'

upvoted 2 times

filthyx 3 years, 12 months ago

I think its A. It say's Third-party devices. From the study guide, page 40: "NetEdit will now algo discover and display third-party devices that are using the stantard MIB's. Using SNMP with NetEDit, administrators can also enter SSH credentials for third-party devices.

upvoted 1 times

clupato2 4 years, 2 months ago

Sorry, i repeated SNMP twice. I meant to write Restful API (that work only with Aruba OS-CX devices).

upvoted 1 times

Mrvn 4 years, 4 months ago

B is more correct here .. Netedit used LLDP by default as discovery.. so it will keep discovering every 5 minutes.

upvoted 2 times

AM1234 4 years, 4 months ago

A is Correct

upvoted 4 times

Question #36 *Topic 1*

Examine the following AOS-CX configuration:

Based on this configuration, which statement is correct regarding IoT traffic?

```
Switch(config)# class ip IoT-traffic
Switch(config-class-ip)# match ip 192.168.0.0/16 any
Switch(config-class-ip)# exit
Switch(config)# pbr-action-list reroute
Switch(config-prb-action-list)# default-nexthop 10.100.1.2
Switch(config-prb-action-list)# exit
Switch(config)# policy IoT-policy
Switch(config-policy)# class ip IoT-traffic action pbr reroute
Switch(config-policy)# exit
Switch(config)# interface vlan 999
Switch(config-if)# apply policy IoT-policy routed-in
Switch(config-if)# exit
```

A. If 10.100.1.2 is not reachable, the IoT traffic will be automatically dropped by the switch

B. If a specific route is not available in the routing table, the traffic will be routed to 10.100.1.2

C. The next hop of 10.100.1.2 can be one or more hops away from the AOS-CX switch

D. All routes are ignored in the routing table for IoT traffic, which is routed to 10.100.1.2

Suggested Answer: *B*

Community vote distribution

B (100%)

fasty Highly Voted 4 years, 6 months ago

I think B is correct

upvoted 9 times

SeidorBruno Most Recent 2 years, 3 months ago

Page 905 Study Guide: Unlike nexthop, default- nexthop only applies if there is no destination lookup match in the main routing table for matching packets. [Aruba Networks]

upvoted 2 times

omen 3 years, 1 month ago

B is correct

upvoted 1 times

AM1234 4 years, 4 months ago

B is correct

upvoted 4 times

poris27 4 years, 6 months ago

I think the answer is D ?Correct if the key word is not 'default-nexthop'

upvoted 1 times

poris27 4 years, 6 months ago

I think the answer is D ?

upvoted 1 times

Moreson 3 years, 8 months ago

Correct if the key word is not 'default-nexthop'

upvoted 4 times

Question #37 *Topic 1*

Which protocol does NetEdit use to discover devices in a subnet during the discovery process?

A. LLDP

B. ARP

C. DHCP

D. ICMP

Suggested Answer: *D*

Community vote distribution

A (100%)

AM1234 Highly Voted 4 years, 4 months ago

The correct Answer is A

upvoted 7 times

poris27 Highly Voted 4 years, 6 months ago

I think the answer should be A

upvoted 5 times

SeidorBruno Most Recent 2 years, 3 months ago

Page 79 Study Guide: Then define one seed device in the subnet that will then discover other devices based on LLDP. Assuming good connectivity, NetEdit finds all connected subnets that seed device. [Aruba Networks]

upvoted 2 times

gian911 2 years, 4 months ago

Agree A

upvoted 1 times

Jo2241 3 years ago

The correct Answer is A

upvoted 1 times

NetExpert 3 years, 1 month ago

A is the correct

upvoted 1 times

Cabron 3 years, 2 months ago

LLDP is the correct answer, To provide further simplicity, NetEdit automatically discovers new network infrastructure devices using the Link Layer Discovery Protocol (LLDP), using REST APIs for Aruba CX switches and SNMP for Aruba wireless and third-party devices

upvoted 4 times

clupato2 4 years, 2 months ago

A is the correct answer

upvoted 3 times

cloud29 4 years, 6 months ago

LLDP - A

upvoted 5 times

Simba80 4 years, 6 months ago

I agree. It should be LLDP.

upvoted 4 times

Question #38 *Topic 1*

Examine the following AOS-CX switch configuration:

Which statement correctly describes what is allowed for traffic entering interface 1/1/3?

```
Access(config)# access-list ip ext
Access(config-acl-ip)# permit ip any 10.0.11.0/255.0.255.0 count
Access(config-acl-ip)# permit ip any 10.0.12.0/255.0.255.0 log
Access(config-acl-ip)# exit
Access(config)# interface 1/1/3
Access(config-if)# apply access-list ip ext in
Access(config-if)# exit
```

A. IP traffic from 10.1.11.0/24 is allowed to access 10.1.110.0/24

B. IP traffic from 10.0.11.0/24 is allowed to access 10.1.12.0/24

C. Traffic from 10.0.12.0/24 will generate a log record when accessing 10.0.11.0/24

D. IP traffic from 10.1.12.0/24 is allowed to access 172.0.1.0/23

Suggested Answer: *C*

Community vote distribution

B (89%) D (11%)

cloud29 Highly Voted 5 years, 6 months ago

The question is " Which statement correctly describes what is allowed for traffic entering interface 1/1/3?" I think that what is allowed to enter the interface 1/1/3 is everything from: ANY TO -> 10.X.11.X(this is allowed and counted) or 10.X.12.X(this allowed and loged), thats why i think the answer is B Everything with other "destination" should be denny.

upvoted 15 times

BFDS Most Recent 2 years, 1 month ago

why no one is talking about the incorrect 255.0.255.0 subnet in the ACL

upvoted 2 times

SeidorBruno 3 years, 3 months ago

As per ACL definition: Matching seq 20 "permit ip any 10.0.12.0/255.0.255.0 log" So trafic from any source ip address is permitted to 10.x.12.x

upvoted 3 times

alex711 3 years, 8 months ago

B is correct

upvoted 1 times

Bahadorkh 3 years, 11 months ago

B is correct

upvoted 1 times

Jo2241 4 years ago

B is correct

upvoted 1 times

NetExpert 4 years, 1 month ago

B is correct

upvoted 1 times

Jo2241 4 years, 2 months ago

No wildcard mask with Aruba CX. B answer

upvoted 1 times

root2022 4 years, 4 months ago

B is correct

upvoted 1 times

gondolf 4 years, 6 months ago

People seem to be confused by inverted mask/wildcard masks. They would be correct for Cisco switches, but AOS-CX does NOT use wildcard masks; "AOX-CX switches do not support wildcard masks - only prefixes or subnet masks - when created ACEs." Cisco: 255.0.255.0 = xx.123.xx.123 AOS-CX: 255.0.255.0 = 123.xx.123.xx My answer is B.

upvoted 2 times

jagoanneon 4 years, 9 months ago

I think the answer is D. Here is the simplified access list with X=any (0-255) permit any -> X.0.X.0 count permit any -> X.0.X.0 log They are practically the same ACL with only different the top does count and bottom does log. A. IP traffic from 10.1.11.0/24 is allowed to access 10.1.110.0/24 We dont care with source (10.1.11.0/24). The source can be any. But the destination is 10.1.110.0/24 and it does not match. The second octet must be 0. B. IP traffic from 10.0.11.0/24 is allowed to access 10.1.12.0/24 Same with A. 10.1.12.0 does not match because second octet is 1 C. Traffic from 10.0.12.0/24 will generate a log record when accessing 10.0.11.0/24 This actually match both ACEs but since ACL matches from top to bottom, so it will match the top ACE (count). D. IP traffic from 10.1.12.0/24 is allowed to access 172.0.1.0/23 this would match the ACL. We dont care about source and destination 172.0.1.0 (match X.0.X.0) Samw

upvoted 1 times

pabx31 5 years ago

My opinion: B Only traffic destined TO the listed subs is allowed This excluded A and D Only traffic TO 10.1.12.0 is logged This excludes C This leaves B .11.0 is part of ANY so it is allowed to access .12.0 This traffic will be logged but that isn't part of the answer.

upvoted 1 times

clupato2 5 years, 2 months ago

I think it's C. ACL entries work with wildcard mask. The wildcard mask is 255.0.255.0. This is a wildcard mask and not a subnet mask also because it is not a valid subnet mask. In a wildcard mask made in this way you have to match bits where wildcard is 0. So, it matches packets where the DESTINATION IP ADDRESS is X.0.X.0. In a /24 network, you will never have a destination IP where the last octet is 0. So i think this ACL is not valid, by the way, the only answer that matches the ACL entries is the C BUT it matches the first entry, so it will never generate a log, but a counter increment. This is a bad question with no matching answers. The "best matching" answer is C even if it is wrong.In the official HPE study book, it clearly states that AOS-CX switches do not support Wildcard Masks when creating ACEs.Got it backwards. 10.0.12.0/255.0.255.0 will match 10.1.12.0/24 .Therefore B should be correct. Right from the student guide. 1's match 0's ignore. Ch. 5 - Task 2 , or search book for 255.0.255.0 "In this example any destination IP address that has '10' in the first byte, and '12' in the third byte will match the rule.

upvoted 3 times

clupato2 5 years, 2 months ago

I think it's C. ACL entries work with wildcard mask. The wildcard mask is 255.0.255.0. This is a wildcard mask and not a subnet mask also because it is not a valid subnet mask. In a wildcard mask made in this way you have to match bits where wildcard is 0. So, it matches packets where the DESTINATION IP ADDRESS is X.0.X.0. In a /24 network, you will never have a destination IP where the last octet is 0. So i think this ACL is not valid, by the way, the only answer that matches the ACL entries is the C BUT it matches the first entry, so it will never generate a log, but a counter increment. This is a bad question with no matching answers. The "best matching" answer is C even if it is wrong.

upvoted 3 times

OICU812 Highly Voted 5 years, 1 month ago

In the official HPE study book, it clearly states that AOS-CX switches do not support Wildcard Masks when creating ACEs.

upvoted 5 times

watermellonhead 5 years, 1 month ago

Got it backwards. 10.0.12.0/255.0.255.0 will match 10.1.12.0/24 .Therefore B should be correct. Right from the student guide. 1's match 0's ignore. Ch. 5 - Task 2 , or search book for 255.0.255.0 "In this example any destination IP address that has '10' in the first byte, and '12' in the third byte will match the rule.

upvoted 2 times

maccchinguwo 5 years, 3 months ago

B sound correct but check the ip addresses properly 10.0.11.0/24 and 10.0.12.0/24 where is 10.1.12.0/24 coming from? C is correct then

upvoted 1 times

Williams926 5 years, 4 months ago

I think answer is B.

upvoted 2 times

El3den 5 years, 4 months ago

but 10.1.12.0 is not matching the wild card mask. i see answer C more accurate, because count will generate syslog message right ?

upvoted 1 times

El3den 5 years, 4 months ago

but 10.1.12.0 is not matching the wild card mask. i see answer C more accurate, because count will generate syslog message right ?sorry it is subnet mask no wild card, B is correct

upvoted 1 times

El3den 5 years, 4 months ago

sorry it is subnet mask no wild card, B is correct

upvoted 2 times

Simba80 5 years, 6 months ago

It's possible that B is correct but look at the log and count entries in the commands. I think C is correct. A log entry will be generated for this subnet.the log count is only active for destination 10.x.12.xOnly log*AOS-CX does not support Wildcard / Inverted Subnet Masks... Study Guide states: "AOS-CX switches do not support wildcard masks - only prefixes or subnet masks - when creating ACEs". Therefore C is most probably the answer

upvoted 2 times

Simba80 5 years, 6 months ago

It's possible that B is correct but look at the log and count entries in the commands. I think C is correct. A log entry will be generated for this subnet.

upvoted 2 times

fasty 5 years, 6 months ago

the log count is only active for destination 10.x.12.x

upvoted 1 times

fasty 5 years, 6 months ago

the log count is only active for destination 10.x.12.xOnly log*AOS-CX does not support Wildcard / Inverted Subnet Masks... Study Guide states: "AOS-CX switches do not support wildcard masks - only prefixes or subnet masks - when creating ACEs". Therefore C is most probably the answer

upvoted 1 times

fasty 5 years, 6 months ago

Only log*

upvoted 1 times

LoneRaccoon 3 years ago

AOS-CX does not support Wildcard / Inverted Subnet Masks... Study Guide states: "AOS-CX switches do not support wildcard masks - only prefixes or subnet masks - when creating ACEs". Therefore C is most probably the answer

upvoted 1 times

Question #39 *Topic 1*

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?

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

B. Logging will not include certificate and TLS events, but counting will

C. The ɹ€countɹ€ and ɹ€logɹ€ options are processed by the AOS-CX switch's hardware ASIC

D. The total in the ɹ€logɹ€ record and the count could contain different rule matching statistics

Suggested Answer: *D*

Community vote distribution

D (100%)

clupato2 Highly Voted 4 years, 2 months ago

A cannot be correct because the default log times is 300s (5 minutes). The answer that best matches this is D

upvoted 10 times

Disposable_Me_2018 Highly Voted 4 years, 1 month ago

It's D. From the "AOS-CX 10.08 ACLs and Classifier Policies Guide" : "You may see a minor discrepancy between the ACL logging statistics and the hit counts statistics due to the time required to record the log message."

upvoted 8 times

SeidorBruno Most Recent 2 years, 3 months ago

Page 267 Study Guide: Note: You may see a minor discrepancy between the ACL logging statistics and the hit counts statistics due to the time required to record the log message. [Aruba Networks]

upvoted 2 times

fubofake92 4 years, 2 months ago

Correct answer is A

upvoted 1 times

Question #40 *Topic 1*

An administrator is defining a VSX LAG on a pair of AOS-CX switches that are defined as primary and secondary. The VSX LAG fails to establish successfully with a remote switch; however, after verification, the remote switch is configured correctly. The administrator narrows down the problem to the configuration on the
AOS-CX switches.
What would cause this problem?

A. Local optimization was not enabled on the VSX LAG

B. The VSX LAG hash does not match the remote peer

C. The VSX LAG interfaces are in layer-3 mode

D. LACP was enabled in active mode on the VSX LAG

Suggested Answer: *B*

Community vote distribution

C (100%)

Mrvn Highly Voted 5 years, 3 months ago

Answer should be C - VSX LAG are not supported at Layer 3 VSX LAG does support all the standard LAG adjustments: timers, L2 or L3 hashing, LACP fallback. It supports both LACP mode active or static mode, and only Layer 2 (i.e. no routed mode).

upvoted 16 times

clupato2 Highly Voted 5 years, 2 months ago

I think it's B, because, as the question is exposed, i understand that the VSX LAG has been configured, but fails to establish. If interfaces where in Layer 3 mode, you will not be able to configure them as a LAG.

upvoted 5 times

clupato2 5 years, 2 months ago

I think it's B, because, as the question is exposed, i understand that the VSX LAG has been configured, but fails to establish. If interfaces where in Layer 3 mode, you will not be able to configure them as a LAG.Switches can bring up VSX LAG with differently defined hashes, its not B IMO.try accessing the device from lab then you will find you are wrong, and hash is not something manual configured, so not a possible human error, this question is asking for trouble shooting skills.

upvoted 5 times

JazzyJ151 4 years, 7 months ago

Switches can bring up VSX LAG with differently defined hashes, its not B IMO.

upvoted 1 times

Moreson 4 years, 8 months ago

try accessing the device from lab then you will find you are wrong, and hash is not something manual configured, so not a possible human error, this question is asking for trouble shooting skills.

upvoted 1 times

yyppy Most Recent 1 year, 11 months ago

L3 interfaces (= configured as "routing") will refuse to join the MC-LAG at first. Stupid question.

upvoted 1 times

SeidorBruno 3 years, 3 months ago

Page 215 Study Guide: VSX LAGs are layer 2 only, [Aruba Networks]

upvoted 4 times

slotblocker 3 years, 4 months ago

This document says NO layer 3 interfaces for VSX LAG: https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/vsx/Content/Chp_Start/vsx-sol-req-10.htm Answer: C

upvoted 1 times

Redrum702 3 years, 5 months ago

In Aruba's Virtual Switching Extension (VSX) technology, the LAG interfaces can be configured in both Layer 2 and Layer 3 modes, depending on the specific requirements of your network design

upvoted 1 times

Redrum702 3 years, 5 months ago

B: Verify that the LAG hash settings match on both the local and remote VSX peers.

upvoted 1 times

alex711 3 years, 8 months ago

I think B is correct. check the following link. https://www.arubanetworks.com/techdocs/AOS-CX/AOSCX-CLI-Bank/cli_6200/Content/VSX_cmds/sho-lac-agg-10.htm

upvoted 4 times

Jo2241 4 years ago

I think C is the good answer. VSX LAG are not supported at Layer 3

upvoted 2 times

Davidkanigui 5 years, 3 months ago

B is correct.Pretty sure that switches do not negotiate the lag hash algorithm in the handshake. Cannot be B. I vote for C.

upvoted 1 times

Davidkanigui 5 years, 3 months ago

B is correct.

upvoted 1 times

Disposable_Me_2018 5 years, 1 month ago

Pretty sure that switches do not negotiate the lag hash algorithm in the handshake. Cannot be B. I vote for C.

upvoted 1 times

Williams926 5 years, 4 months ago

I think D is correct.

upvoted 1 times

Williams926 5 years, 4 months ago

I think D is correct.Why do you think it is correct?

upvoted 1 times

gbermudez11 5 years, 4 months ago

Why do you think it is correct?

upvoted 1 times

Question #41 *Topic 1*

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

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?

```
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
```

A. Define the server group cppm

B. Set the ports to client-mode

C. Create and assign a local user role to the ports

D. Enable change of authorization (CoA)

Suggested Answer: *D*

Community vote distribution

A (100%)

poris27 Highly Voted 4 years, 6 months ago

I think the answer is A

upvoted 12 times

AM1234 Highly Voted 4 years, 4 months ago

The correct Answer is A

upvoted 10 times

SeidorBruno Most Recent 2 years, 3 months ago

Page 679 Study Guide: The servers that you add are automatically added to the global RADIUS server group, which is called radius, and referred to as the global group [Aruba Networks] You might want to use only a subset of servers for a particular task, instead of all the globally defined ones. You can do this by creating RADIUS groups [Aruba Networks]

upvoted 3 times

Jo2241 3 years ago

the answer is A

upvoted 2 times

Linares1234 4 years ago

I think same that its A https://community.arubanetworks.com/blogs/esupport1/2020/04/29/downloadable-user-role-configuration-in-aruba-os-cx-with-mac-authentication

upvoted 3 times

kup 4 years, 1 month ago

D-student guide V2.88I agree, the switch will not accept that command if cppm group is not setup (i.e. switch throws an error).Just tryed it on GNS3 and the switch does allow the command even if cppm group is not setup.Taking this into consideration, i read on the guide that the "default" group when you add a server to RADIUS is called 'radius'. So in this case, the group would need to be created because is explicitly configuring cppm group.

upvoted 3 times

kup 4 years, 1 month ago

D-student guide V2.88

upvoted 3 times