350-401 Implementing Cisco Enterprise Network Core Technologies (ENCOR)

Question #1 *Topic 1*

What is the difference between a RIB and a FIB?

A. The FIB is populated based on RIB content.

B. The RIB maintains a mirror image of the FIB.

C. The RIB is used to make IP source prefix-based switching decisions.

D. The FIB is where all IP routing information is stored.

Correct Answer: *A*

Community vote distribution

A (100%)

gisare1660 Highly Voted 3 days, 3 hours ago

Thank you so much for providing excellent exam dumps. I prepared for my 350-501 certification exam using these and aced the exam with 92% score. Highly suggested to all. https://rb.gy/d8brg4

upvoted 16 times

edg Highly Voted 3 years, 3 months ago

The answer is A.
https://tools.ietf.org/id/draft-ietf-i2rs-rib-info-model-17.html
"Traditionally routers run routing protocols and the routing protocols (along with static configuration information) populate the Routing Information Base (RIB) of the router. The RIB is managed by the RIB manager and the RIB manager provides a northbound interface to its clients, i.e., the routing protocols, to insert routes into the RIB. The RIB manager consults the RIB and decides how to program the Forwarding Information Base (FIB) of the hardware by interfacing with the FIB manager."

upvoted 14 times

Brandonkiaora Most Recent 3 weeks, 6 days ago

Hi. I have learned ENCOR from Udemy courses, can I pass the exam if I finish and memorize all these 800 dump questions? If you see this, please come back to tell me.

02,Nov.,2023

upvoted 1 times

cccna 2 months, 1 week ago

Answer: A

B - RIB is the routing table, it contains way more information than FIB. FIB is one of the two tables that CEF uses, it is built based on information found in RIB, but has fewer info.
C - FIB contains IP source and prefixes information, not RIB.
D - RIB is where all the IP routing information is stored, FIB is where only part of that information is summarized/stored.

upvoted 2 times

Specialdork 2 months, 3 weeks ago

The problem with this question and these answers is that the question is asking what is the DIFFERENCE between the FIB and RIB. C and D kind of answer that but not exactly.

upvoted 1 times

techriese 5 months ago

Selected Answer: A

A is correct

upvoted 2 times

PatEvra 5 months, 1 week ago

The Answer is A

upvoted 1 times

nana_amp 7 months ago

Passed the Encor yesterday! had 94 questions and was expecting three labs:
1st was etherchannel configuration, with some stp configs (basic)
2nd was etherchannel config troubleshooting (also basic)
3rd was HSRP configs (pretty straightforward)
now after this i was very relaxed like lab's are all done, just 35 more multiple choice and its done cos i had a feeling it was going well.
20 questions left, the screen blanks out again for lab abd im screaming in my head like WTF!!??#
4th was an archive log config, second part was literally "what command do you need on int Gi0/1 to activate the ip flow-top-talkers already configured on the switch/router?"
guessing they are testing the archive log labs and prolly some others because the 4th lab felt kinda experimental i dunno. Archive log is not in the lab manual so a bit confused when i saw a post about that here. I mean i read on it just in case and look what happened SMH cisco goddamn!

upvoted 4 times

YTAKE 6 months ago

Thank you nana_amp!

What number are the lab questions in this site please?

All I see are multiple choice questions.

upvoted 1 times

Ray_Sang 8 months, 1 week ago

Selected Answer: A

A is correct

upvoted 3 times

B453yg2023 9 months, 1 week ago

Passed today. 90 percent of the questions were from here.
Got 3 labs:
- Etherchannel config + Vlan 10 native on portchannel.
- Configure archive log
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/15-sy/config-mgmt-15-sy-book/cm-config-logger.html
- Configure GLBP
Goodluck all!

upvoted 3 times

Jey117 9 months, 1 week ago

Selected Answer: A

In case you wonder. Questions are still valid,, I passed the exam 2 days ago.
Remember that you'll have:
- 98 questions
- 3 study cases (in my case they were OSPF and EEM related).

I got like 10 new questions though.

Good luck in your careers Engineers. Keep it up

upvoted 3 times

alirezabavi 10 months, 2 weeks ago

the answer is A

upvoted 2 times

ciscokoolaid 11 months, 2 weeks ago

A is correct. The Forwarding Information Base (FIB) table - CEF uses a FIB to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and these changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths such as fast switching and optimum switching.

Adjacency table - Nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. In addition to the FIB, CEF uses adjacency tables to append Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries.
Source: https://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html

upvoted 1 times

shikima 11 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

The answer is A.

upvoted 1 times

flash007 1 year, 6 months ago

fib is populated with rib information. fib is the forwarding information base and rib is the routing informaition database

upvoted 2 times

Question #2 *Topic 1*

Which QoS component alters a packet to change the way that traffic is treated in the network?

A. policing

B. classification

C. marking

D. shaping

Correct Answer: *C*

Community vote distribution

C (100%)

ArShuRaZ Highly Voted 2 years, 10 months ago

Question is "Alter the packet". so it is packet "Marking"

upvoted 16 times

newbietech1979 Most Recent 1 month, 2 weeks ago

Answer is A
RIB: The RIB is a database that stores all the routing information learned from various sources such as static routes, dynamic routing protocols, or administrative configurations. It contains the full set of routing information available within a router, including multiple possible routes for a destination network. The RIB is typically used to calculate the best path for forwarding packets.

FIB: The FIB, on the other hand, is a subset of the RIB. It is a data structure that contains the forwarding table entries used by the router for actual packet forwarding decisions. The FIB is optimized for fast lookup and efficient packet forwarding. It contains only the best routes selected from the RIB based on various metrics like administrative distance, route preference, or path cost.

upvoted 1 times

techriese 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

ciscokoolaid 11 months, 2 weeks ago

C is correct.
Traffic marking allows you to mark (that is, set or change) a value (attribute) for the traffic belonging to a specific class.
Source: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_classn/configuration/xe-16/qos-classn-xe-16-book/qos-classn-mrkg-ntwk-trfc-xe.html

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

mnhabatsi7 1 year, 3 months ago

The actions that are carried out by the marker include the following:
• Passing through the packet without modification
• Dropping the packet
• Modifying (marking down) the assigned DSCP or CoS value of the packet and allowing the packet to pass through

from Bacha D. book CCNP and CCIE Enterprise Core ENCOR 350-401

upvoted 1 times

mnhabatsi7 1 year, 3 months ago

The answer is policing

upvoted 1 times

flash007 1 year, 4 months ago

once the packet is marked the packet is then classified

upvoted 2 times

Pudu_vlad 1 year, 6 months ago

The answer is C.

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: C

Altering the packet implies marking

upvoted 3 times

Asymptote 1 year ago

Passed Cisco English Test.

upvoted 4 times

CiscoTerminator 1 year, 10 months ago

Guys C is wrong - "in order to change the way traffic is treated in the network" - only policing can do that. Marking does not alter traffic movement!

upvoted 1 times

Eddgar0 1 year, 7 months ago

The key point in the question is "Alters the packet" Marking implies altering the Frame or IP header to set a Value (a mark). With this value then you can do policy.

upvoted 3 times

cloud29 2 years ago

Selected Answer: C

QoS Packet Marking refers to changing a field within a packet either at Layer 2 (802.1Q/p CoS, MPLS EXP) or Layer 3 (IP Precedence, DSCP and/or IP ECN). It also refers to preserving any classification decision that was reached previously.

upvoted 2 times

Richview 2 years, 3 months ago

Answer is C: Marking

upvoted 1 times

Exam_khan 2 years, 4 months ago

when traffic is classified it is then labelled so it is identifyable by the devices

upvoted 1 times

AliMo123 2 years, 7 months ago

after classifying the packet, the field in the packet change via marking process.

upvoted 2 times

davdtech 2 years, 8 months ago

It can not be policing or either shaping. They are both Qos mechanisms. Marking is the distinction between a packet with qos and a packet with no qos. So best answer is marking

upvoted 1 times

MarkJames 2 years, 9 months ago

Note this Marking yes alters the packet, but marking does nothing to how its treated if there is no policy. Its like having a marked man, but no police to enforce his arrest. Marking and classification do nothing by themselves without policing. The question is a bit vague. My answer will be A

upvoted 1 times

Wesgo 2 years, 9 months ago

Marking... ENCOR 350-401 Official Cert Guide: "Packet marking is a QoS mechanism that COLORS a packet by CHANGING a field within a packet or a frame header with a traffic descriptor so it is DISTINGUISHED from other packets during the application of other QoS mechanisms (such as re-marking, policing, queuing, or congestion avoidance)."

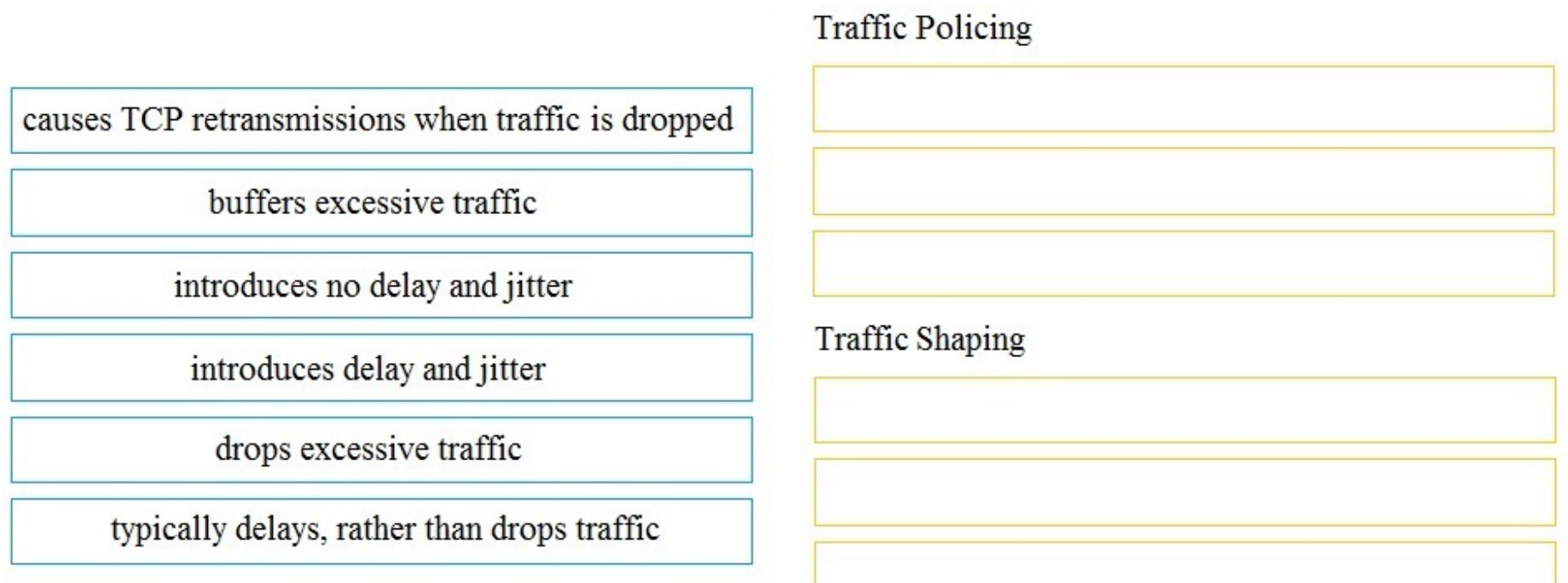
upvoted 2 times

DRAG DROP -

Drag and drop the descriptions from the left onto the correct QoS components on the right.

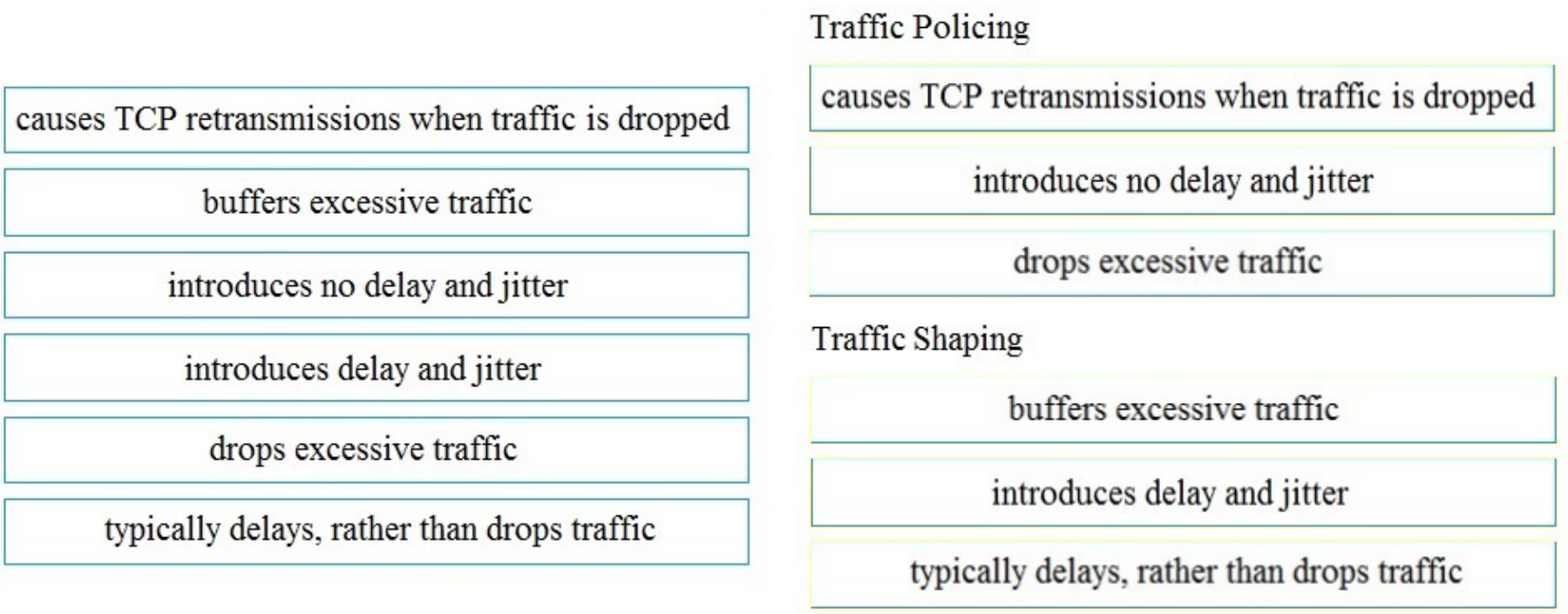
Select and Place:

Answer Area



Correct Answer:

Answer Area



chris7411 Highly Voted 3 years, 6 months ago

not correct, both answer with delay and jitter must be swap... (from Policing to shaping)

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

Shaping implies the existence of a queue and of sufficient memory to buffer delayed packets, while policing does not.

upvoted 48 times

[Removed] 4 months, 3 weeks ago

Just FYI for those wondering what chris7411 is talking about.

It looks like admins fixed the answer so it is now correct

upvoted 4 times

dave369 Highly Voted 3 years, 6 months ago

Another logical reason that chris7411's answer is correct is that traffic shaping cannot both "introduce no delay" and "typically delay" simultaneously.

upvoted 13 times

techriese Most Recent 5 months ago

provided answer is correct

upvoted 1 times

JackyChon 6 months, 2 weeks ago

Traffic policing
cause TCP retransmissions when traffic is dropped.
introduce delay and jitter.
drops excessive traffic.

Traffic shaping
buffers excessive traffic.
introduces no delay and jitter.
delays, rather than drops, traffic.

upvoted 3 times

ciscokoolaid 11 months, 2 weeks ago

Answer is Correct.
Policing Advantages:
- Drop (or remark) excess packets over the committed rates. Does not buffer.
- Controls the output rate through packet drops. Avoids delays due to queuing.
Policing Disadvantages:
- Propagates bursts. Does no smoothing.
- Drops excess packets (when configured), throttled TCP window sizes and reduces the overall output rate of affected traffic streams. Overly aggressive burst sizes can lead to excess packet drops and throttle the overall output rate, particularly with TCP-based flows.
Shaping Advantages
- Buffer and queue excess packets over the committed rates.
- Controls bursts and smooths the output rate over at least eight-time intervals. Uses a leaky bucket to delay traffic, which achieves a smoothing effect.
- Less likely to drop excess packets since excess packets are buffered. (Buffers packets up to the length of the queue. Drops can occur if excess traffic is sustained at high rates.) Typically avoids retransmissions due to dropped packets.
Shaping Disadvantage:
- Can introduce delay due to queuing, particularly deep queues.

upvoted 3 times

RREVECO 1 year, 2 months ago

DRAG AN DROP IT´S CORRECT
BOOK: ccnp-350-401-official-cert-guide
Chapter 14. QoS
-Implement traffic policing to drop low-priority packets and allow high-priority traffic through.
Then: " Drops excessive traffic"

- Implement traffic shaping to delay , is not recommended for RTP,it relies on queuing that can cause jitter.
Then: "introduces delay and jitter"
whereby: traffic policing = "introduces no delay and jitter"

-Shapers: Buffer and delay egress traffic rates ***deleted for space***
then: "Buffers excessive traffic"

-Policers for incoming traffic ***deleted for space***. A downside of policing is that it causes TCP retransmissions when it drops traffic.
the: "Cuase TCP retransmission when traffic is dropped"

- Shapers are used for egress traffic ***deleted for space***. Shaping buffers and delays traffic rather than dropping it, and this causes fewer TCP retransmissions compared to policing.
then: "typically delays ,rather than drops traffic"

upvoted 2 times

pepgua 1 year, 2 months ago

The provided answer seems correct. Policing drops packets which will cause TCP retransmission and no need for delay. Shaping buffers instead of dropping packets which will lead to queuing causing delays. Based on many comments, the provided answer is also valid.

upvoted 4 times

Ken99 1 year, 4 months ago

Shaping definitely introduces delay due to queuing.... So 'Introduces delay and jitter' should be under 'traffic shaping'..

upvoted 1 times

BigMouthDog 1 year, 5 months ago

Shaping places packets into queues when the actual traffic rate exceeds the traffic contract, which causes more delay, and more jitter.
Policing when making a simple decision to either discard or forward each packet causes more packet loss, but less delay and jitter for the packets that do make it through the network

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

Traffic Policing
causes tcp retransmitions
Introduces no delay and jitter
drops excessive traffic

Traffic Shapping
buffer excessive traffic
Introduces delay and jitter
typically delays , rather than drops traffic

upvoted 12 times

rquintana 1 year, 6 months ago

Traffic Shaping according to the book: Implement traffic shaping to delay packets instead of dropping them since traffic may burst and exceed the capacity of an interface buffer. Traffic shaping is not recommended for real-time traffic BECAUSE IT RELIES ON QUEUING THAT CAUSE JITTER.

upvoted 2 times

flash007 1 year, 6 months ago

policing drops and shaping buffers the traffic

upvoted 1 times

BigMouthDog 1 year, 6 months ago

For traffic shaping, one says, "no delays", the other says, "typically delay". I am getting confused. For shaping, the traffic must be delayed

upvoted 1 times

xeler 1 year, 8 months ago

Based on AndresV 1, policing generates more TCP retransmissions than shapping.

then, for tcp retransmissions to be generated, you have to wait for their timers (acknowledgment) to expire in order to carry out the retransmission, in the case of shaping you do not wait for those timers to retransmit (or at least not as long as in the case of policing)

In conclusion, I think that policing does introduce latency and jitter due to the elimination of packets that it does and shaping does not (at least not directly since it only makes the packets wait) since it does not eliminate packets.

upvoted 1 times

Eddgar0 1 year, 7 months ago

Not correct, I disaggre with xeler, because retransmittion and delay are different stuff, and your logic are not taking in account UDP where retransmition does not exist. (even on tcp a retranssmition can be delayed). Shaping by default buffers the transmition of a packet until traffic is below of a traffic rate, so this buffering in other words will delay the packet until the rate goes below the committed rate.

upvoted 1 times

LittleMing 1 year, 9 months ago

introduce delay and jitter is shaping

upvoted 1 times

sleek1 1 year, 9 months ago

introduce delay and jitter need to go under shaping

upvoted 1 times

GATUNO 2 years ago

Delay an jitter needs to swap

upvoted 2 times

Question #4 *Topic 1*

Which statement about Cisco Express Forwarding is true?

A. The CPU of a router becomes directly involved with packet-switching decisions.

B. It uses a fast cache that is maintained in a router data plane.

C. It maintains two tables in the data plane: the FIB and adjacency table.

D. It makes forwarding decisions by a process that is scheduled through the IOS scheduler.

Correct Answer: *C*

Community vote distribution

C (100%)

DJOHNR Highly Voted 3 years, 3 months ago

https://www.fir3net.com/Routers/Cisco/what-is-cef-cisco-express-forwarding.html

CEF is built around 2 main components - the Forwarding Information Base (FIB) and the Adjacency Table.

Answer, C

upvoted 16 times

em6868 2 months, 1 week ago

Thanks man!

upvoted 1 times

hku68 2 years, 10 months ago

Yes. Thanks DJOHNR for explanation.

upvoted 1 times

vava_exam Most Recent 3 months, 1 week ago

answer C

upvoted 1 times

ciscokoolaid 11 months, 2 weeks ago

Correct Answer is C. CEF maintains two tables in the data plane: the FIB and adjacency table.
Answers A & D describe Process Switching and Fast Switching (when processing the first packet). B describes Fast Switching also known as Route Caching.
Source: http://www.patrickdenis.biz/blog/1-1-b-identify-cisco-express-forwarding-concepts/

upvoted 1 times

nushadu 11 months, 2 weeks ago

C.
cisco#show adjacency
Protocol Interface Address
IP Ethernet0/0.10 192.168.255.1(7)
cisco#show ip cef
Prefix Next Hop Interface
0.0.0.0/0 no route
0.0.0.0/8 drop
...

upvoted 1 times

Asymptote 1 year ago

Selected Answer: C

C

Reference:
https://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html#:~:text=The%20Forwarding%20Information,all%20FIB%20entries.

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

The answer is C.

upvoted 1 times

flash007 1 year, 6 months ago

cef has 2 tables the fib and the adjacency table

upvoted 1 times

Aldebeer 1 year, 8 months ago

This will be executed in control plane rather than in data plane . Right ?

upvoted 1 times

LittleMing 1 year, 9 months ago

Selected Answer: C

The answer is C

upvoted 1 times

Exam_khan 2 years, 4 months ago

cef components are 2 tables. fib table and the adjacency table

upvoted 1 times

CiscoDudeee 2 years, 7 months ago

CEF utilises the adjacency table and forwarding information base (FIB). C is the correct answer.

upvoted 1 times

Question #5 *Topic 1*

What is a benefit of deploying an on-premises infrastructure versus a cloud infrastructure deployment?

A. ability to quickly increase compute power without the need to install additional hardware

B. less power and cooling resources needed to run infrastructure on-premises

C. faster deployment times because additional infrastructure does not need to be purchased

D. lower latency between systems that are physically located near each other

Correct Answer: *D*

Community vote distribution

D (100%)

hku68 Highly Voted 2 years, 10 months ago

%100 D is correct

upvoted 9 times

PatEvra Most Recent 3 months, 4 weeks ago

"D" is the answer that makes the most sense to me

upvoted 1 times

techriese 5 months ago

Selected Answer: D

nothing else makes sense

upvoted 1 times

net_eng10021 6 months, 3 weeks ago

Selected Answer: D

relatively simple question. **D** is the correct answer

upvoted 1 times

Nnandes 10 months, 1 week ago

When you have devices in the same place, you have lower latency between systems that's why D is correct.

upvoted 1 times

dan_4_stone 10 months, 3 weeks ago

D is correct

upvoted 1 times

obiey 1 year, 1 month ago

Selected Answer: D

dedicated hardware resources

upvoted 1 times

Gedson 1 year, 1 month ago

Selected Answer: D

D correct

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: D

D is correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

The answer is D.

upvoted 1 times

flash007 1 year, 6 months ago

on premesis will produce lower latency as the devices are in the same data network as when in the cloud you are dependant on bandwidth and latency will be much higher

upvoted 2 times

ayodejiadeyemi 2 years, 6 months ago

D is right...

upvoted 3 times

nubje 2 years, 11 months ago

D is correct nothing else

upvoted 2 times

Helloory 3 years ago

D is correct

upvoted 3 times

juniper 3 years ago

D is correct

upvoted 3 times

Jasim_Nayan 3 years, 1 month ago

On-premise software requires that an enterprise purchases a license or a copy of the software to use it. Because the software itself is licensed and the entire instance of software resides within an organization's premises, there is generally greater protection than with a cloud computing infrastructure.

upvoted 1 times

Jasim_Nayan 3 years, 1 month ago

pls give answer

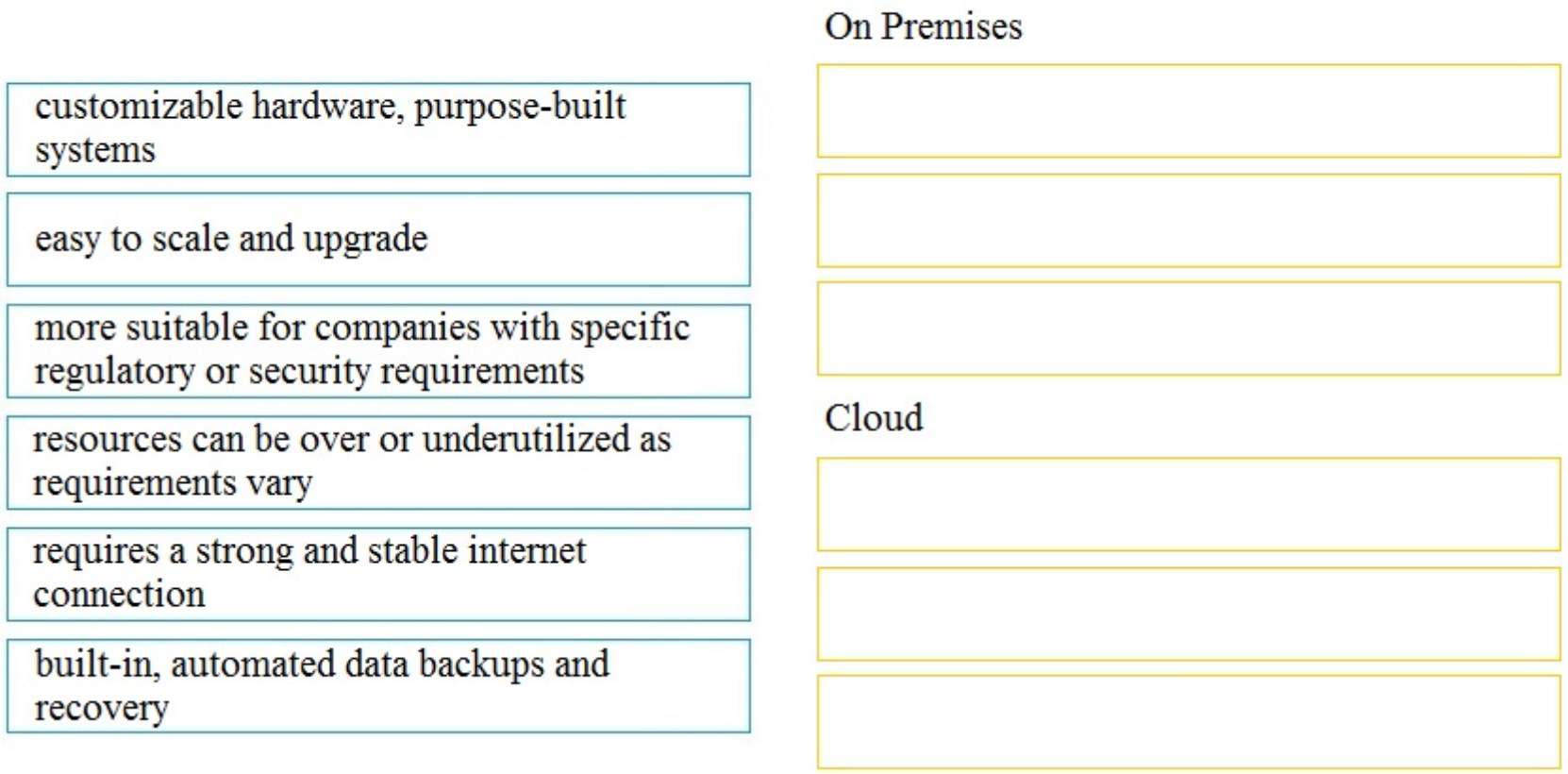
upvoted 1 times

DRAG DROP -

Drag and drop the characteristics from the left onto the appropriate infrastructure deployment types on the right.

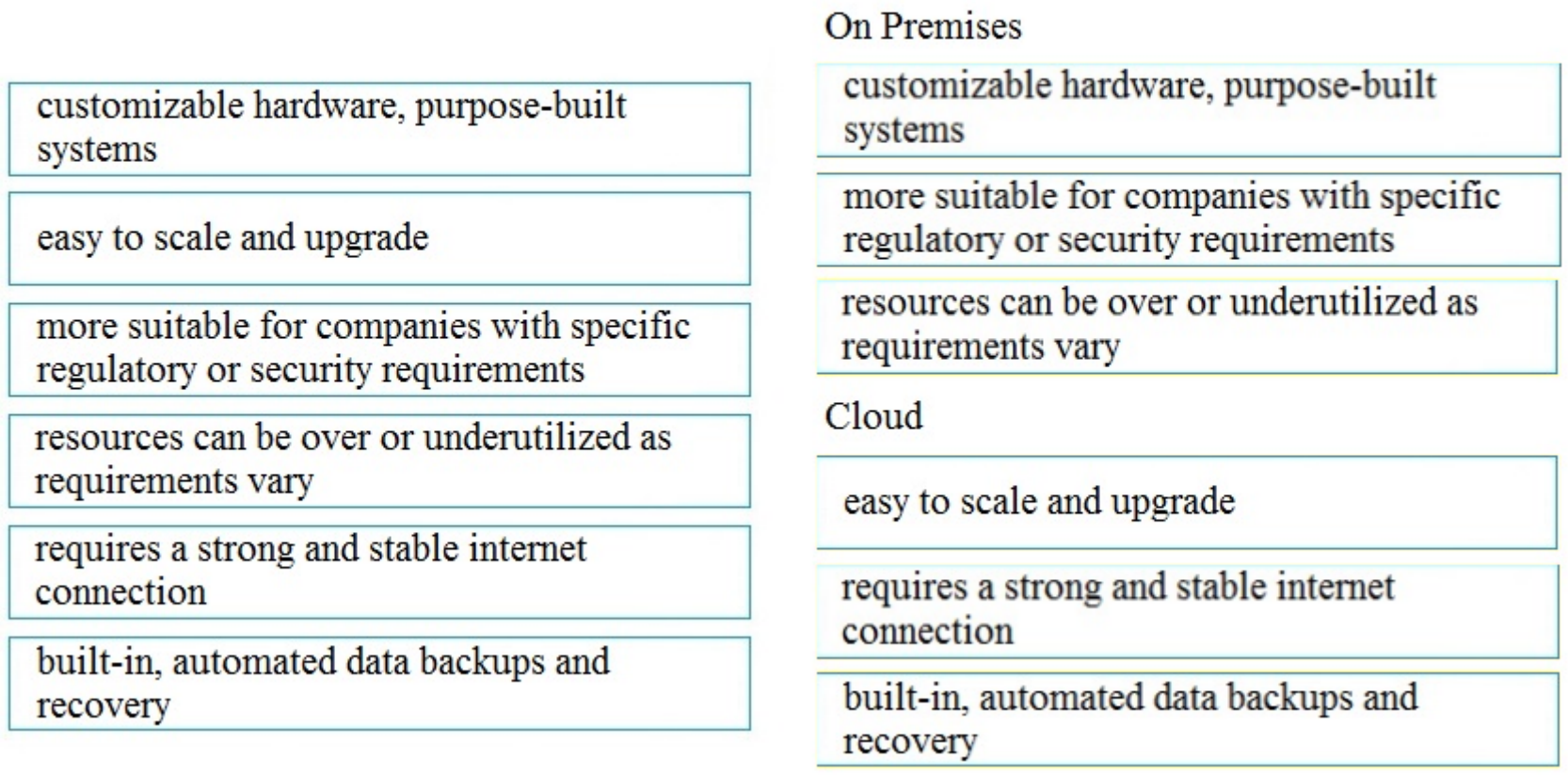
Select and Place:

Answer Area



Correct Answer:

Answer Area



Pudu_vlad Highly Voted 1 year, 6 months ago

On Premisses
customizable hardware
more suitable for companies
resources can be over or

Cloud
easy to scale and upgrade
requires a strong and stable internet connection
build-in, automated data backups and recovery

upvoted 5 times

techriese Most Recent 5 months ago

provided answer is correct

upvoted 1 times

Leon7942 7 months, 3 weeks ago

i wonder what does 'customizable hardware' means as non-native english worker.
i used translator but not satisfied with result...

upvoted 1 times

[Removed] 5 months, 3 weeks ago

i understand this as in the administrators built the server blade from purchased components of their choice. Think of building your own home/gaming computer with personal choice of CPU, RAM, GPU, Storage, Power, and Cooling.

upvoted 1 times

Neil101 1 year, 3 months ago

Answer is correct, but noting I've worked on 'Cloud' deployments that don't touch the Internet at all (by design), so Cloud 'requiring a strong and stable internet connection' is the world (and exam) according to Cisco. ExpressRoute or DirectConnect anyone as an alternative to Internet anyone?!! On the flip side, if Internet is a critical component of On Premises (let's say as an example a paging system for calling out ambulance drivers or doctors) - according to Cisco is it fine that it's flappy and weak?! Exams vs the real world....

upvoted 3 times

pepgua 1 year, 7 months ago

Correct!

upvoted 1 times

Amit12 1 year, 10 months ago

Looks correct!!

upvoted 1 times

Question #7 *Topic 1*

How does QoS traffic shaping alleviate network congestion?

A. It drops packets when traffic exceeds a certain bitrate.

B. It buffers and queues packets above the committed rate.

C. It fragments large packets and queues them for delivery.

D. It drops packets randomly from lower priority queues.

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

Community vote distribution
B (100%)

ayodejiadeyemi Highly Voted 2 years, 6 months ago
B is the accepted answer. traffic shaping support packet buffer while traffic policing support packet drop.
upvoted 11 times

techriese Most Recent 5 months ago
Selected Answer: B
B is correct
upvoted 1 times

ciscokoolaid 11 months, 2 weeks ago
B is Correct. During congestion, traffic shaping buffers and queues packets above the committed rate.
Answer A describes Policing dropping packets exceeding a certain bitrate. Answer C is describing packet fragmentation when the router receives an IP packet above 1500 bytes. Answer D is sort of describing Random Early Detection (RED) which is a congestion avoidance mechanism that randomly drops packets from RED-enabled interfaces or queues during periods of high congestion. RED tells the packet source to decrease its transmission rate.
Source: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/xe-16/qos-conavd-xe-16-book/qos-conavd-cfg-wred.html#GUID-F7BA5018-770F-48B7-8103-EEF22A7FC479
upvoted 3 times

cloud29 1 year, 1 month ago
Selected Answer: B
B is correct
upvoted 1 times

Pudu_vlad 1 year, 6 months ago
B is correct
upvoted 1 times

rquintana 1 year, 6 months ago
Selected Answer: B
B is correct
upvoted 1 times

flash007 1 year, 6 months ago
traffic shaping buffers whereas policing drops the traffic
upvoted 3 times

pepgua 1 year, 7 months ago
Answer is correct.
upvoted 1 times

mjunior 2 years, 2 months ago
Strong agree
upvoted 3 times

examShark 2 years, 6 months ago
The correct answer is B
upvoted 4 times

AliMo123 2 years, 7 months ago
During shaping phase, it uses queues to force some traffic to wait (buffered traffic) to avoid congestion

upvoted 4 times

Question #8 *Topic 1*

An engineer is describing QoS to a client.
Which two facts apply to traffic policing? (Choose two.)

A. Policing should be performed as close to the source as possible.

B. Policing adapts to network congestion by queuing excess traffic.

C. Policing should be performed as close to the destination as possible.

D. Policing drops traffic that exceeds the defined rate.

E. Policing typically delays the traffic, rather than drops it.

Correct Answer: *AD*

Community vote distribution

AD (100%)

Helloory Highly Voted 3 years ago
answers are correct
upvoted 15 times

skh Highly Voted 3 years ago
i think correct A&D
Traffic policing propagates bursts. When the traffic rate reaches the configured maximum rate (or committed information rate), excess traffic is dropped (or remarked). The result is an output rate that appears as a saw-tooth with crests and troughs.
Unlike traffic shaping, traffic policing does not cause delay.
Classification (which includes traffic policing, traffic shaping and queuing techniques) should take place at the network edge. It is recommended that classification occur as close to the source of the traffic as possible.
upvoted 11 times

Sacuxipo Most Recent 1 week, 6 days ago
Provided answers are correct
upvoted 1 times

techriese 5 months ago
Selected Answer: AD
A D is correct
upvoted 1 times

Nnandes 10 months, 1 week ago
A and D
upvoted 1 times

Rose66 10 months, 4 weeks ago
Selected Answer: AD
answers are correct
upvoted 1 times

ciscokoolaid 11 months, 2 weeks ago
Selected Answer: AD
A & D are correct.
Police unwanted traffic flows as close to their sources as possible. Answers B & D referred to Shaping and its queueing strategy which achieves a smoothing effect. Answer C is not a QoS best practice for Policing.
Source: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2501.pdf
upvoted 3 times

Asymptote 1 year ago
Selected Answer: AD
AD correct,
upvoted 1 times

cloud29 1 year, 1 month ago
Selected Answer: AD
A and D are correct
upvoted 1 times

Pudu_vlad 1 year, 6 months ago
answers are correct

upvoted 1 times

roncr 1 year, 7 months ago

Selected Answer: AD

i think correct A&D

upvoted 1 times

pepgua 1 year, 7 months ago

A & D are correct.

upvoted 1 times

Question #9 *Topic 1*

Which component handles the orchestration plane of the Cisco SD-WAN?

A. vBond

B. vSmart

C. vManage

D. WAN Edge

Correct Answer: *A*
Reference:
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKCRS-2112.pdf page 8.

Community vote distribution

A (100%)

Nnandes Highly Voted 10 months, 1 week ago

vManager - is the controller and cisco considers it the management plane
vSmart - is the control plane.
vEdge is the data plane.
vBond is the orchestrator plane, and according to cisco it authenticates the vSmart controllers and the SD-WAN routers and orchestrates connectivity between them. It is the only device that must have a public IP
address so that all SD-WAN devices in the network can connect to it. A vBond orchestrator
is an SD-WAN router that only performs vBond orchestrator functions.

upvoted 12 times

ando2023 5 months, 1 week ago

Great write up, thank you

upvoted 1 times

examShark Highly Voted 2 years, 6 months ago

The given answer is correct

upvoted 7 times

CCNPWILL Most Recent 3 months, 3 weeks ago

vBond is correct. that language is typically used when describing the vBond.

upvoted 1 times

techriese 4 months, 4 weeks ago

Mods please update the reference - Error 404

upvoted 1 times

techriese 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

ciscokoolaid 11 months, 2 weeks ago

Selected Answer: A

A is correct. vBond handles the orchestration plane.
vManage is a centralized network management system that lets you configure and manage the entire overlay network from a simple graphical dashboard.
vSmart Controller is the centralized brain of the Cisco SD-WAN solution, controlling the flow of data traffic throughout the network. The vSmart Controller works with the vBond Orchestrator to authenticate vEdge devices as they join the network and to orchestrate connectivity among the edge routers.
vBond Orchestrator automatically orchestrates connectivity between edge routers and vSmart Controllers. If any edge router or vSmart Controller is behind a NAT, the vBond Orchestrator also serves as an initial NAT-traversal orchestrator.
The edge routers sit at the perimeter of a site and provide connectivity among the sites. They are either hardware devices or software (Cloud router), that runs as a virtual machine. The edge routers handle the transmission of data traffic.
Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html

upvoted 3 times

Vlad_Is_Love_ua 12 months ago

Selected Answer: A

The Cisco vBond orchestrator is a multitenant element of the Cisco SD-WAN fabric. Cisco vBond is the first point of contact and performs initial authentication when devices are connecting to the organization overlay. Cisco vBond facilitates the mutual discovery of the control and management elements of the fabric by using a zero-trust certificate-based allowed-list model. Cisco vBond automatically distributes a list of Cisco vSmart controllers and the Cisco vManage system to the Cisco WAN Edge routers during the deployment process.

upvoted 1 times

Abbribas 1 year ago

vBond – initiates the bring up process of every vEdge device, at the first step it creates secure tunnel with vEdge and informs vSmart and vManage about its parameters like for instance ip address. It has to be fully connected with every device.

upvoted 1 times

Asymptote 1 year ago

Selected Answer: A

A is correct.

Reference:
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html#_Toc39479328:~:text=secure%20connection%20to-,the%20vBond%20orchestrator.,-The%20following%20figure

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

JETO 1 year, 1 month ago

YES vBond

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

The given answer is correct

upvoted 1 times

flash007 1 year, 6 months ago

orchestraiton is done at the vbond device

upvoted 1 times

[Removed] 1 year, 7 months ago

Selected Answer: A

vbond is the first point f contact for sd-wan

upvoted 1 times

mailmivhan 1 year, 10 months ago

Selected Answer: A

vBond (Also called the Orchestration Plane): Is the Orchestrator (or a better word "facilitator")

upvoted 2 times

Question #10 *Topic 1*

What are two device roles in Cisco SD-Access fabric? (Choose two.)

A. edge node

B. vBond controller

C. access switch

D. core switch

E. border node

Correct Answer: *AE*

Community vote distribution

AE (100%)

Skliffi Highly Voted 3 years, 3 months ago

SD-Access Fabric Roles and Terminology

Control Plane Node, Border Node, Edge Node, and other Fabric elements

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

upvoted 13 times

domac385 Most Recent 4 months, 1 week ago

Selected Answer: AE

A and E

upvoted 1 times

techriese 5 months ago

Selected Answer: AE

A + E is correct

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: AE

A and E are correct

upvoted 1 times

cloud29 1 year, 1 month ago

A and E are correct

upvoted 2 times

cloud29 1 year, 4 months ago

Selected Answer: AE

A and E

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

A & E are correct.

upvoted 1 times

flash007 1 year, 6 months ago

edge and border nodes are part of the SD-Wan fabric. Access and core is not part of the fabric

upvoted 1 times

cvndani 1 year, 10 months ago

Selected Answer: AE

A & E are correct.

upvoted 1 times

flash007 2 years, 5 months ago

and edge node in SD-Access

upvoted 1 times

flash007 2 years, 5 months ago

Question mentions sd roles well there is a border edge node

upvoted 1 times

examShark 2 years, 6 months ago

Provided answer is correct

upvoted 1 times

Question #11 *Topic 1*

What is the role of the vSmart controller in a Cisco SD-WAN environment?

A. It performs authentication and authorization.

B. It manages the control plane.

C. It is the centralized network management system.

D. It manages the data plane.

Correct Answer: *B*

Community vote distribution

B (100%)

iGlitch Highly Voted 1 year ago

Selected Answer: B

- It performs authentication and authorization. (vBond)
- It manages the control plane. (vSmart)
- It is the centralized network management system. (vManage)
- It manages the data plane. (vEdge)

upvoted 21 times

Rockford Highly Voted 2 years, 6 months ago

Control Plane – vSmart is the Controller in Viptela solution and manages the Control Plane. vSmart does all the complex work of path calculation, route advertisement etc. there by offloading the Data Plane to do only packet forwarding.

upvoted 11 times

CCNPWILL Most Recent 3 months, 3 weeks ago

vSmart manages the control plane by advertising routing information via the control connections using OMP to relay this data. Given answer is correct.

upvoted 1 times

LanreDipeolu 4 months ago

vSmart is the "Governor" of SD-WAN just as LISP is for SD-Access

upvoted 1 times

techriese 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

Vlad_Is_Love_ua 12 months ago

Selected Answer: B

Cisco vSmart controllers are a scale-out control plane function of the Cisco SD-WAN fabric.

The main characteristics of the control plane with Cisco vSmart controllers are as follows:

Facilitates fabric discovery

Disseminates control plane information between the Cisco WAN Edge routers

Distributes data plane and application-aware routing policies to the Cisco WAN Edge routers

Implements control plane policies, such as service chaining, multitopology, and multihop

Dramatically reduces control plane complexity

Highly resilient

upvoted 2 times

cloud29 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

cloud29 1 year, 1 month ago

B is correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

B is correct

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: B

Vsmart perform all the calcularion work of the overlay network

upvoted 2 times

CCNA_beast_69 1 year, 10 months ago

Selected Answer: B

B is correct

upvoted 1 times

rpidcock 2 years, 3 months ago

vSmart controllers also implement all the control plane policies created on vManage
CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide p634

upvoted 4 times

examShark 2 years, 6 months ago

Provided answer is correct

upvoted 4 times

Question #12 *Topic 1*

When a wired client connects to an edge switch in a Cisco SD-Access fabric, which component decides whether the client has access to the network?

A. edge node

B. Identity Services Engine

C. RADIUS server

D. control-plane node

Correct Answer: *B*

Community vote distribution

B (100%)

telefonica Highly Voted 2 years, 8 months ago

I think its B: ISE

upvoted 25 times

SandyIndia 2 years, 3 months ago

Identity Service Engine (ISE) identify user gives users specific permission & policy.

upvoted 4 times

P1Z7C Highly Voted 2 years, 8 months ago

poor question if asked that way since both are technically correct (B & C). ISE is of course a radius server, and you can leverage a third party radius server + ISE for SDA. If they had used creative wording then maybe they were trying to trick you, you can't run SDA with only a third party radius server, you still need ISE.

ex. https://community.cisco.com/t5/networking-documents/how-to-use-group-based-policies-with-3rd-party-radius-using/ta-p/3930041

upvoted 17 times

techriese Most Recent 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

networkingXIV 6 months, 3 weeks ago

Selected Answer: B

When a wired client connects to an edge switch in a Cisco SD-Access fabric, the component that decides whether the client has access to the network is the Identity Services Engine (ISE). Therefore, option B is the correct answer.

The ISE is a key component of the Cisco SD-Access architecture that provides authentication, authorization, and accounting (AAA) services. When a client connects to an edge switch, the ISE is responsible for determining the client's identity and checking its credentials against a policy database. If the client is authorized to access the network, the ISE instructs the edge switch to assign the appropriate VLAN and apply the appropriate policies. If the client is not authorized, the ISE instructs the edge switch to quarantine the client and provide limited network access.

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

walidbedawy 1 year, 3 months ago

I think should be B

upvoted 1 times

BigMouthDog 1 year, 4 months ago

The answer i think is "B". Why ? 1. Radius does not have ISE feature, 2. ISE has Radius , 3. the key word "Cisco SD-Access fabric" - ISE is part of the SDN concept

upvoted 2 times

flash007 1 year, 6 months ago

ise is used to allow or not allow access to the network there are policys and permissions assigned in the ise management portal

upvoted 1 times

rquintana 1 year, 6 months ago

it should be B

upvoted 3 times

MrBishop 1 year, 6 months ago

The correct answer is B, it was even in the CBT nuggets videos. Specifically Explain SD-Access Fabric Operation/User Authentication. So, B is your correct answer.

upvoted 3 times

Leoloren 1 year, 7 months ago

Correct answer is B ISE

You can't run SDA with only a third party radius server, you need ISE

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: B

Eventhought 802.1X can run with a 3rd party radius server, for SDA policy to work must be with ISE as use trusect for the security plane.

upvoted 1 times

hennel 1 year, 8 months ago

Selected Answer: B

-B-: It has to be an ISE , a standard RADIUS server isn't sufficient

upvoted 1 times

AlbertoStu 1 year, 8 months ago

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#Solution_Components

Components of an SD-Access solution include:

Cisco DNA Center Hardware Appliance

Cisco DNA Center Software

Identity Services Engine

upvoted 2 times

Aldebeer 1 year, 8 months ago

Selected Answer: B

De ISE server operate as Tacacs+ and the Radius server. If you ask in a SD-Access fabric environment then the answer must be B!

upvoted 1 times

Aldebeer 1 year, 8 months ago

nou, the question is "which component decides"..? Is Radius or ISE ? Radius is a protocol and ISE is a service designed to deliver Radius.. Its tricky..

upvoted 1 times

LittleMing 1 year, 9 months ago

Selected Answer: B

Answer is B

upvoted 1 times

Question #13 *Topic 1*

Which benefit is offered by a cloud infrastructure deployment but is lacking in an on-premises deployment?

A. virtualization

B. supported systems

C. storage capacity

D. efficient scalability

Correct Answer: *D*

Community vote distribution

D (100%)

examShark Highly Voted 2 years, 6 months ago

Provided answer is correct

upvoted 8 times

LanreDipeolu Most Recent 4 months ago

"D" is the answer because Cloud option quickly produces the needed and sufficient. Unlike on-premises that provides more than or less than necessary, at less cost effectiveness.

upvoted 1 times

techriese 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

networkingXIV 6 months, 3 weeks ago

Selected Answer: D

One of the benefits offered by a cloud infrastructure deployment that is lacking in an on-premises deployment is efficient scalability. Therefore, option D is the correct answer.

Efficient scalability refers to the ability of a system to quickly and easily increase its capacity in response to changing demand. In a cloud infrastructure deployment, this is achieved through the use of elastic resources, which can be automatically provisioned and deprovisioned in response to changes in workload. This allows cloud users to easily scale up or down their infrastructure as needed, without having to worry about the cost and complexity of purchasing and configuring new hardware.

In contrast, an on-premises deployment typically requires organizations to purchase and install new hardware to scale their infrastructure. This process can be time-consuming and expensive, and may not be feasible for organizations with limited resources or a rapidly-changing workload.

upvoted 2 times

PedroPicapiedra 1 year, 1 month ago

Selected Answer: D

D is correct

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: D

D is correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

D. efficient scalability

upvoted 1 times

flash007 1 year, 6 months ago

cloud can be scalled up or down and in and out if the load requires it

upvoted 1 times

pepgua 1 year, 7 months ago

Provided answer is the best option.

upvoted 1 times

mailmivhan 1 year, 10 months ago

Selected Answer: D

D. efficient scalability

upvoted 1 times

flash007 2 years, 5 months ago

cloud deployments can scale up and down

upvoted 3 times

Question #14 *Topic 1*

Which action is the vSmart controller responsible for in a Cisco SD-WAN deployment?

A. onboard WAN Edge nodes into the Cisco SD-WAN fabric

B. gather telemetry data from WAN Edge routers

C. distribute policies that govern data forwarding performed within the Cisco SD-WAN fabric

D. handle, maintain, and gather configuration and status for nodes within the Cisco SD-WAN fabric

Correct Answer: *C*

Community vote distribution

C (100%)

Rockford Highly Voted 2 years, 6 months ago

vSmart functions:
1. vSmart is the brain of the entire system.
2. Works with vBond to authenticate Viptela devices as they join the network.
3. Builds Control Plane connections with vEdge using TLS.
4. Orchestrate connectivity between vEdges via the policies there by creating the network topology.
5. Acts as a Route reflector by advertising the branches prefixes based on the policy.
6. Shares the data plane keys of a vEdge with other vEdges based on the policy to allow them to build the tunnels – IKEless IPSEC.
7. Policies are configured on vSmart.

upvoted 14 times

rpidcock Highly Voted 2 years, 3 months ago

Provided answer is correct.
vSmart controllers also implement all the control plane policies created on vManage
CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide Pg 634

upvoted 7 times

CCNPWILL Most Recent 3 months, 3 weeks ago

correct, in the cEdge router you can run: ' show sdwan policy from-vsmart " this gives you the policies for data policy and app route policy given to the router by the vSmart.

upvoted 1 times

LanreDipeolu 3 months, 4 weeks ago

Selected Answer: C

It is the distributor of policies. "C" is the correct answer

upvoted 1 times

x3rox 9 months, 2 weeks ago

Correct Answer: C
As with centralized control policy, you provision centralized data policy on the Cisco vSmart controller, and that configuration remains on the Cisco vSmart controller. The effects of data policy are reflected in how the Cisco vEdge devices direct data traffic to its destination.

Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/data-policies.html

upvoted 1 times

Vlad_Is_Love_ua 9 months, 2 weeks ago

Selected Answer: C

The main characteristics of the control plane with Cisco vSmart controllers are as follows:

Facilitates fabric discovery

Disseminates control plane information between the Cisco WAN Edge routers

Distributes data plane and application-aware routing policies to the Cisco WAN Edge routers

Implements control plane policies, such as service chaining, multitopology, and multihop

Dramatically reduces control plane complexity

Highly resilient

upvoted 1 times

iGlitch 1 year ago

Selected Answer: C

- onboard WAN Edge nodes into the Cisco SD-WAN fabric. (vBond)
- gather telemetry data from WAN Edge routers. (vAnalytics)

- distribute policies that govern data forwarding performed within the Cisco SD-WAN fabric. (vSmart)
- handle, maintain, and gather configuration and status for nodes within the Cisco SD-WAN fabric. (vManage)

upvoted 2 times

cloud29 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

cloud29 1 year, 1 month ago

C is correct

upvoted 1 times

pyrokar 1 year, 4 months ago

Selected Answer: C

Given answer is correct.

upvoted 1 times

Rockford 2 years, 6 months ago

Control Plane – vSmart is the Controller in Viptela solution and manages the Control Plane. vSmart does all the complex work of path calculation, route advertisement etc. there by offloading the Data Plane to do only packet forwarding.

upvoted 2 times

examShark 2 years, 6 months ago

Provided answer is correct

upvoted 5 times

Question #15 *Topic 1*

Where is radio resource management performed in a Cisco SD-Access wireless solution?

A. DNA Center

B. control plane node

C. wireless controller

D. Cisco CMX

Correct Answer: *B*

Community vote distribution

C (100%)

jmaroto Highly Voted 2 years, 8 months ago

C is the correct answer.

Fabric wireless controllers manage and control the fabric-mode APs using the same general model as the traditional local-mode controllers which offers the same operational advantages such as mobility control and radio resource management. A significant difference is that client traffic from wireless endpoints is not tunneled from the APs to the wireless controller. Instead, communication from wireless clients is encapsulated in VXLAN by the fabric APs which build a tunnel to their first-hop fabric edge node. Wireless traffic it tunneled to the edge nodes as the edge nodes provide fabric services such as the Layer 3 Anycast Gateway, policy, and traffic enforcement.

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

upvoted 32 times

Dudu84 Most Recent 5 days, 3 hours ago

The correct answer is C. The WLC is still responsible for AP image/configuration, radio resource management, client session management and roaming, and all the other
wireless control plane functions.
https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf

upvoted 1 times

BMP078 1 month ago

Selected Answer: C

gestão da controller

upvoted 1 times

Haidary 1 month ago

RRM is a feature built into wireless controllers that continously monitor your wireless RF environmen.
The correct answer is C.

upvoted 1 times

Wissammawas 1 month, 1 week ago

Selected Answer: C

C ist richtig

upvoted 1 times

LanreDipeolu 4 months ago

I agree that B is the answer because of the new role of VXLAN that replaces the traditional CAPWAP in onboarding of wireless Clients to the Fabric node.

upvoted 1 times

techriese 5 months ago

Selected Answer: C

C is correct
WLC is managing the RRM

upvoted 2 times

Chiaretta 7 months, 2 weeks ago

Selected Answer: C

wireless lan controller is the correct answer

upvoted 1 times

habibmangal 7 months, 4 weeks ago

Selected Answer: C

In a Cisco SD-Access wireless solution, radio resource management is typically performed in the wireless controller. The wireless controller manages the radio resources and ensures that each client device is assigned the appropriate radio channel, transmit power, and other settings to ensure optimal performance and minimal interference. The DNA Center and Cisco CMX are other components of the Cisco SD-Access solution that provide network management and location analytics, respectively, but they do not perform radio resource management. The control plane node is a component of the Cisco SD-Access fabric that is responsible for controlling network traffic and enforcing network policies, but it also does not perform radio resource management.

upvoted 3 times

paulosrsf 9 months ago

Selected Answer: C

Page 7 of Cisco Official SD-Access Wireless Design and Deployment Guide.
"The WLC is still responsible for AP image/configuration, RRM, client session management and roaming, and all the other wireless control plane functions."

https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf

upvoted 4 times

Hosein 9 months, 2 weeks ago

Selected Answer: C

Control and Provisioning of Wireless Access Points (CAPWAP) tunnel is maintained between APs and WLC

upvoted 2 times

kewokil120 11 months ago

Selected Answer: C

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjcuLegiJ38AhUcATQIHU47CI4QFnoECA4QAQ&url=https%3A%2F%2Fwww.cisco.com%2Fc%2Fdam%2Fen%2Fus%2Ftd%2Fdocs%2Fcloud-systems-management%2Fnetwork-automation-and-management%2Fdna-center%2Fdeploy-guide%2Fcisco-dna-center-sd-access-wl-dg.pdf&usg=AOvVaw0KWdfH-FyIpRyKFTtmcgbS

upvoted 3 times

PedroPicapiedra 1 year, 1 month ago

Selected Answer: C

I think C is correct

upvoted 2 times

Jasper 1 year, 1 month ago

The right answer is C.

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

HBL_203 1 year, 3 months ago

Correct answer is B
"In SD-Access, the
wireless control plane remains centralized, but the data plane is distributed using VXLAN
directly from the fabric-enabled APs." Official Cert Guide page 625

upvoted 1 times

BigMouthDog 1 year, 5 months ago

C is the correct answer. Control plane node is too generic , not not special. The question is about Radio Resource Management. Fabric wireless LAN controller is the WLC that is fabric enabled.

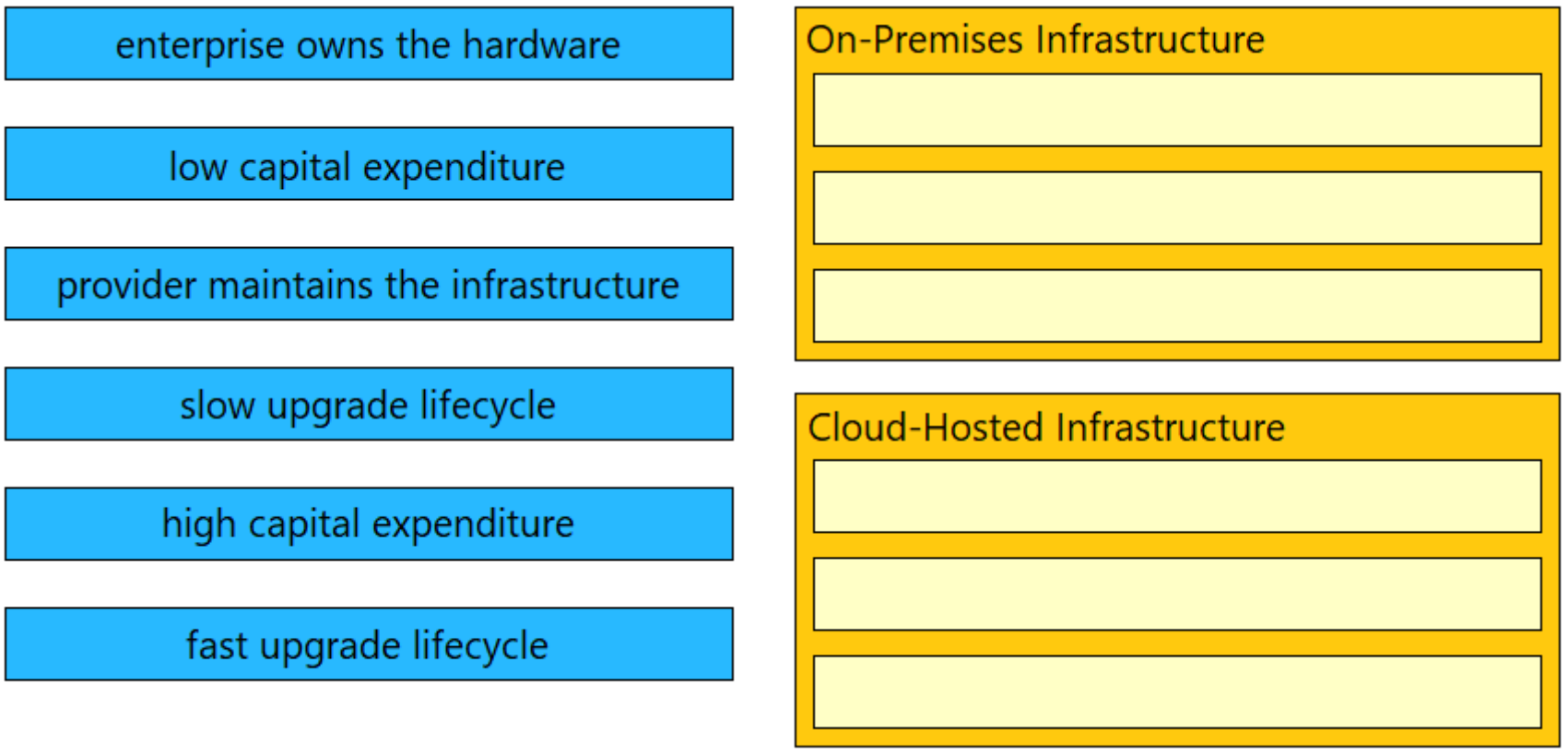
upvoted 1 times

Question #16 *Topic 1*

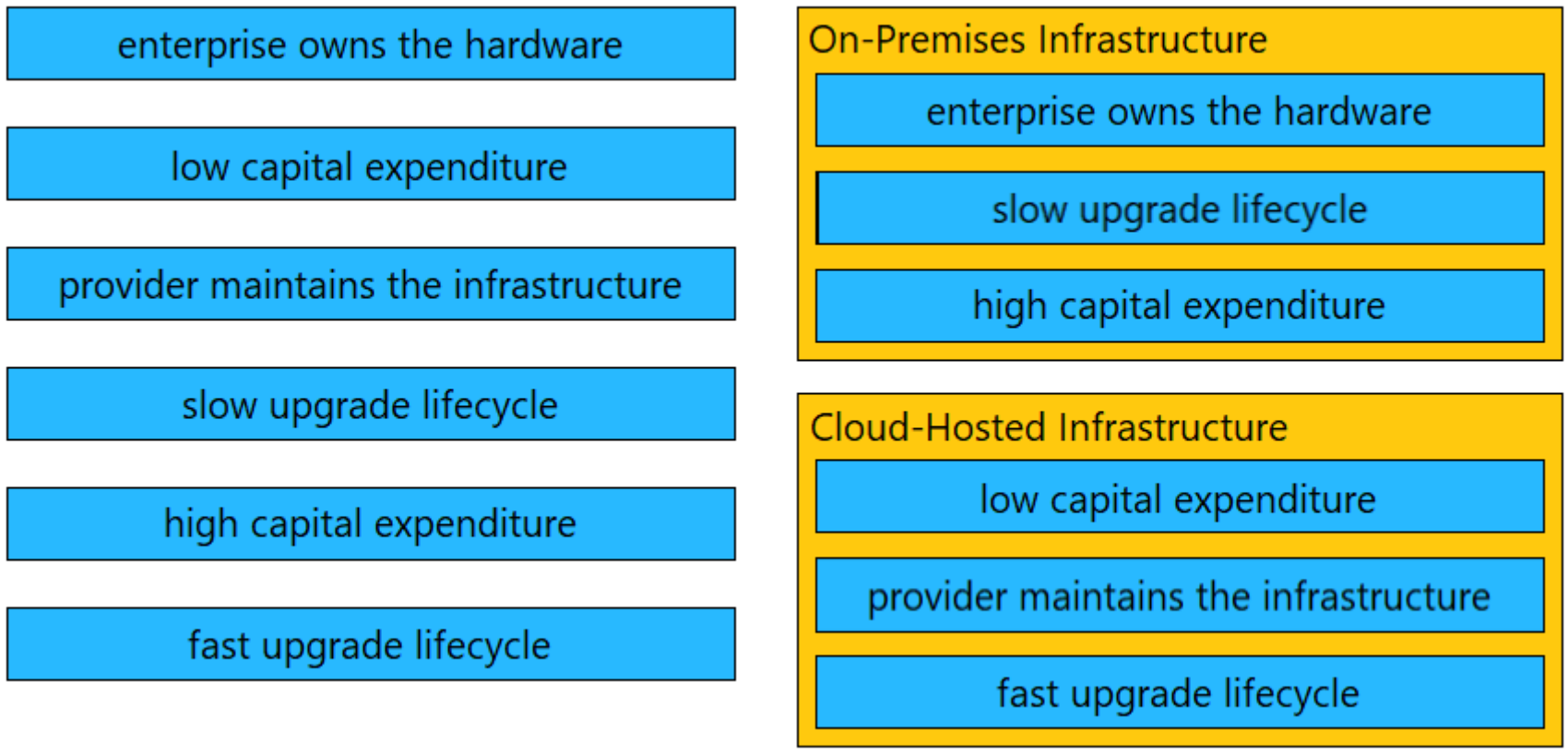
DRAG DROP -

Drag and drop the characteristics from the left onto the infrastructure types on the right.

Select and Place:



Correct Answer:



examShark Highly Voted 2 years, 6 months ago

Provided answer is correct

upvoted 14 times

LanreDipeolu Most Recent 4 months ago

Posted answer is correct. Captial outlay with rapid frequency of on-premises is NOT budget-attractive nor cost-friendly /efficient.

upvoted 1 times

[Removed] 4 months, 3 weeks ago

Correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

On Premisses
enterprise owns the hardware
slow upgrade lifecycle
high capital expenditure

Cloud-Hosted
low capital expenditure
provider maintains the infrastructure
fast upgrade lifecycle

upvoted 2 times

Question #17 *Topic 1*

How does the RIB differ from the FIB?

A. The FIB maintains network topologies and routing tables. The RIB is a list of routes to particular network destinations.

B. The FIB includes many routes to a single destination. The RIB is the best route to a single destination.

C. The RIB is used to create network topologies and routing tables. The FIB is a list of routes to particular network destinations.

D. The RIB includes many routes to the same destination prefix. The FIB contains only the best route.

Correct Answer: *C*

Community vote distribution

D (60%) C (38%)

tonght Highly Voted 2 years, 9 months ago

I think correct answer is D

upvoted 36 times

SandyIndia 2 years, 3 months ago

The best paths from EIGRP's RIB and the best paths from BGP's RIB are passed into the routing table RIB. Where competing paths exist from multiple routing protocols then Administrative Distance (AD) as a tiebreaker – lower is better.The winning paths are then passed to the FIB to be used for forwarding packets on to the next-hop router. The same process has also happened on the next router and the next one, until the packet reaches its destination.

upvoted 12 times

HungarianDish 8 months ago

https://writemem.co.uk/what-is-a-rib-and-a-fib/

upvoted 3 times

mortyxreborn 2 years, 9 months ago

I agree with D

upvoted 5 times

circledan 2 years, 8 months ago

I agree.
According to Wikipedia...(Weird) https://en.wikipedia.org/wiki/Routing_table
In computer networking a routing table, or routing information base (RIB), is a data table stored in a router or a network host that "lists the routes to particular network destinations"

upvoted 1 times

noov 2 years, 8 months ago

i agree

upvoted 1 times

AliMo123 Highly Voted 2 years, 6 months ago

C is correct
FIB has info about next hop and interface identifier so it has the routes for particular network destination

upvoted 18 times

Johnconnor2021 1 year, 12 months ago

but you CREATE a routing table with RIB? Does RIB just receive the route but does not create it?

upvoted 1 times

Tadese Most Recent 1 day, 22 hours ago

the correct answer is D

upvoted 1 times

Dudu84 5 days, 3 hours ago

I agree with D.
RIB is, in essence, a comprehensive database, housing a myriad of routing entries. Each routing entry includes vital data such as the network destination, associated subnet mask, next-hop IP address, and various attributes relevant to routing decisions.
Conversely, the Forwarding Information Base, or FIB, has a more focused role within the router. Derived directly from the RIB, the FIB contains a subset of information critical to packet forwarding. FIB distills this comprehensive information into an efficient and streamlined set of next-hop entries. It represents the best path to reach each destination, ensuring optimal packet forwarding.

https://www.youtube.com/watch?v=GaKmC7QK7E8

upvoted 1 times

Passionaire 2 months, 2 weeks ago

Selected Answer: C

Routing protocols such as OSPF, EIGRP, and BGP each have their own Routing Information Base (RIB). The best routes to each destination network are selected to be installed in the global RIB, or the IP routing table from each routing protocol RIB. If more than one routing protocol is being executed on a router, the best routes from each RIB will be chosen by a parameter called administrative distance.

Administrative distance is the feature that routers use to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with the help of an administrative distance value.

The FIB is derived from the IP routing table and is arranged for maximum lookup throughput.

upvoted 1 times

Passionaire 2 months, 2 weeks ago

Answer options mentions RIB not RIBs. Answer is C. Each routing protocol has its own RIB and each RIB contains only one route to destination.

Routing protocols such as OSPF, EIGRP, and BGP each have their own Routing Information Base (RIB). The best routes to each destination network are selected to be installed in the global RIB, or the IP routing table from each routing protocol RIB. If more than one routing protocol is being executed on a router, the best routes from each RIB will be chosen by a parameter called administrative distance.

Administrative distance is the feature that routers use to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with the help of an administrative distance value.

The FIB is derived from the IP routing table and is arranged for maximum lookup throughput.

upvoted 1 times

djedeen 3 months ago

Selected Answer: D

..best route..

upvoted 1 times

Schr0dinger 3 months, 3 weeks ago

Selected Answer: C

Each change in the IP routing table triggers a similar change in the FIB table because it contains all next-hop addresses that are associated with all destination networks.

upvoted 1 times

Schr0dinger 3 months, 3 weeks ago

Each change in the IP routing table triggers a similar change in the FIB table because it contains all next-hop addresses that are associated with all destination networks. << this sentence come from cisco official self training so I think answer should be C.

upvoted 1 times

Lalag 4 months, 2 weeks ago

Guys C is the best answer ..Routing Information Base (RIB) is a distributed collection of information about routing connectivity among all nodes of a network. Each router maintains a RIB containing the routing information for that router. RIB stores the best routes from all routing protocols that are running on the system.

https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/61x/b-ncs5500-routing-configuration-guide-61x/b-ncs5500-routing-configuration-guide-61x_chapter_0100.html#:~:text=Routing%20Information%20Base%20(RIB)%20is,are%20running%20on%20the%20system.

upvoted 2 times

rogue_user 4 months, 3 weeks ago

Selected Answer: C

FIB can also contain several routes since otherwise ECMP forwarding wouldn't work

upvoted 1 times

[Removed] 4 months, 3 weeks ago

Selected Answer: D

The RIB accepts or rejects the route based on the information presented by each routing protocol.
The RIB looks at the Destination network, Next Hop, Administrative Distance, and Metrics
The RIB will install the route if the route does not exists in the table
The RIB will then compare AD if its presented with an already existing route, if the AD is lower, then it installs the route, if its higher it rejects it.

The FIB is directly built from the Routing Table and contains the next-hop IP address of each destination network.

upvoted 1 times

techriese 5 months ago

Selected Answer: D

for me D is correct.
FIB contains only the best route.

upvoted 1 times

Burik 5 months, 3 weeks ago

Selected Answer: D

See https://datatracker.ietf.org/doc/html/rfc3222:

The forwarding information base is distinct from the "routing table" (or, the Routing Information Base), which holds all routing information received from routing peers.

The forwarding information base contains unique paths only (i.e. does not contain secondary paths).

upvoted 1 times

msstanick 5 months, 3 weeks ago

Looks to me like C per Cisco's 31 days before the CCNP exam book page 24: "The FIB table is updated after each network change, but only once, and it contains all known routes; there is no need to build a route cache by centrally processing initial packets from each data flow. Each change in the IP routing table triggers a similar change in the FIB table because it contains all next-hop addresses that are associated with all destination networks."

upvoted 1 times

pwmc6302 6 months, 1 week ago

The choice D is not correct because Cisco Express Forwarding (CEF) does not make forwarding decisions through a process scheduled by the IOS scheduler. Instead, CEF uses forwarding tables (such as the FIB and adjacency table) to make packet forwarding decisions more efficiently, avoiding direct involvement of the router's CPU in those decisions.

upvoted 1 times

wr4net 6 months, 3 weeks ago

this is a rick question. with D, the FIB part is likely correct, but the RIB part is not necessarily correct for two reasons: A. if the RIB had multiple paths, there were be some instances of a single path, so the logic of the phrase is wrong, by suggesting that all all roues in the RIB are mult-path. B. with ecmp enables (and it can be diabled), that will actually install multiple routes in the RIB. lookup ECMP. this implies that the RIB often doesnt have multiple routes in it. In my simple mind, route protocol database (sh ip ospf database) feeds into the RIB, and RIB coudl get overwritten by lets say a same prefix EIGRP route (ad=90, rather than ad=110). this would install in the RIB. then the RIB would feed the FIB, which combines the adjacency table to the route. so C is likely the best answer in a very strict case. but its a tricky question.

upvoted 1 times

Question #18 *Topic 1*

Which technology is used to provide Layer 2 and Layer 3 logical networks in the Cisco SD-Access architecture?

A. underlay network

B. VPN routing/forwarding

C. easy virtual network

D. overlay network

Correct Answer: *D*

Community vote distribution

D (100%)

techriese 5 months ago

Selected Answer: D

D is correct
pysical = underlay
logical = overlay
upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: D

D is correct
upvoted 1 times

timtgh 1 year, 6 months ago

Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths, such as fast switching and optimum switching.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/44sg/configuration/guide/Wrapper-44SG/cef.pdf

Page 3
upvoted 1 times

flash007 1 year, 6 months ago

logical network will be the overlay and physical network would be the underlying devices under the sd-wan fabric
upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: D

D is correct
upvoted 1 times

youtri 2 years ago

correct ,he said logicall network,if it was physical network it would be underlay network
upvoted 3 times

schattencr 2 years, 3 months ago

Yes it is
upvoted 2 times

Hack4 2 years, 5 months ago

I agree
upvoted 1 times

examShark 2 years, 6 months ago

Provided answer is correct
upvoted 4 times

Question #19 *Topic 1*

What is the difference between CEF and process switching?

A. CEF processes packets that are too complex for process switching to manage.

B. Process switching is faster than CEF.

C. CEF uses the FIB and the adjacency table to make forwarding decisions, whereas process switching punts each packet.

D. CEF is more CPU-intensive than process switching.

Correct Answer: *C*

Community vote distribution

C (100%)

examShark Highly Voted 2 years, 6 months ago

Provided answer is correct

upvoted 6 times

LanreDipeolu Most Recent 4 months ago

"C" is correct. CEF uses line-card unlike process-switching that uses CPU for its decision-making.

upvoted 1 times

techriese 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

ibogovic 6 months, 3 weeks ago

Selected Answer: C

Answer is correct

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

provided answer is correct

upvoted 1 times

certtaker202 2 years, 3 months ago

Agree that C is the way more correct answer.

"Punt" is often used to describe the action of moving a packet from the fast path (CEF) to the route processor for handling.
Cisco Express Forwarding (CEF) provides the ability to switch packets through a device in a very quick and efficient way while also keeping the load on the router's processor low. CEF is made up of two different main components: the Forwarding Information Base (FIB) and the Adjacency Table.
Process switching is the slowest switching methods (compared to fast switching and Cisco Express Forwarding) because it must find a destination in the routing table. Process switching must also construct a new Layer 2 frame header for every packet. With process switching, when a packet comes in, the scheduler calls a process that examines the routing table, determines which interface the packet should be switched to and then switches the packet. The problem is, this happens for the every packet.

upvoted 4 times

understandingson 2 years, 3 months ago

Process switching requires the CPU to be personally involved with every forwarding decision
C is only correct answer

upvoted 1 times

Hack4 2 years, 5 months ago

Provided answer is correct

upvoted 1 times

flash007 2 years, 5 months ago

cef is less cpu intenive than process switching

upvoted 2 times

flash007 2 years, 5 months ago

Process switching is much slower then cef

upvoted 1 times

Question #20 *Topic 1*

What are two considerations when using SSO as a network redundancy feature? (Choose two.)

A. requires synchronization between supervisors in order to guarantee continuous connectivity

B. the multicast state is preserved during switchover

C. must be combined with NSF to support uninterrupted Layer 3 operations

D. both supervisors must be configured separately

E. must be combined with NSF to support uninterrupted Layer 2 operations

Correct Answer: *AC*

Community vote distribution

AC (73%) AE (27%)

examShark Highly Voted 2 years, 6 months ago

Provided answer is correct

upvoted 15 times

Dudu84 Most Recent 4 days, 20 hours ago

I agree with A+C

NSF Operation
Cisco NSF always runs with SSO and provides redundancy for Layer 3 traffic. NSF works with SSO to minimize the amount of time that a network is unavailable to its users following a switchover. The main purpose of NSF is to continue forwarding IP packets following a supervisor engine switchover.

https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/nsfsso.html#wp1023627

upvoted 1 times

djedeen 3 months ago

Selected Answer: AC

SSO:This type of switchover ensures that Layer 2 traffic is not interrupted
NSF: Cisco NSF always runs with SSO and provides redundancy for Layer 3 traffic. NSF works with SSO to minimize the amount of time that a network is unavailable to its users following a switchover. The main purpose of NSF is to continue forwarding IP packets following a supervisor engine switchover.

upvoted 1 times

LanreDipeolu 4 months ago

I vote for A+C

upvoted 1 times

rogue_user 4 months, 3 weeks ago

Selected Answer: AE

NSF = Non-stop FORWARDING which means Layer 2.
NSR = Non-stop ROUTING.

upvoted 2 times

ihateciscoreally 3 months, 1 week ago

in reality it is other way around. SSO uses NSF by default and it used for uninterrupted Layer 3 forwarding (SSO guarantees uninterrupted Layer 2 forwarding).

you will use NSR to Layer 3 forwarding be operational, because NSF kind of "enables" Layer 3 forwarding, but without NSR it won't work at all.

upvoted 1 times

techriese 5 months ago

Selected Answer: AC

A + C are correct

upvoted 1 times

HungarianDish 8 months ago

Selected Answer: AC

https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/nsfsso.html
"NSF Operation
Cisco NSF always runs with SSO and provides redundancy for Layer 3 traffic."

upvoted 3 times

cerf 9 months, 3 weeks ago

AC are the correct
upvoted 2 times

SheldonC 10 months, 1 week ago

A & C - From Cisco:

[...] SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs. <<<<<<<<<< A) IS CORRECT >>>>>>>>>>

SSO is generally used with Cisco nonstop forwarding (NSF). Cisco NSF enables forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With NSF, users are less likely to experience service outages. <<<<<<<<<< C IS CORRECT >>>>>>>>>>

SOURCE: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-sy/fhp-15-sy-book/fhp-hsrp-sso.pdf
upvoted 2 times

kewokil120 11 months ago

Selected Answer: AC

just google is non stop forwarding layer 3
upvoted 1 times

Asymptote 1 year ago

Selected Answer: AC

AC

While SSO is happening, routing protocol communication between 2 supervisor stopped because lost of adjacency.

It and cause interuption, to avoid this we need NFS.

in order for NFS to work properly,
both supervisor must NFS.
upvoted 1 times

Rumbrum 1 year, 1 month ago

Selected Answer: AE

NSF only works for L2 uninterrupted failover
upvoted 1 times

Ayman_B 11 months ago

To support uninterrupted Layer 2 operations in SSO , you have to use additional technologies like (VRRP) or (HSRP) can help to ensure that there is always a active router available to forward packets at the Layer 2 level
upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: AC

A and C are correct
upvoted 1 times

Wooker 1 year, 2 months ago

Selected Answer: AC

AC is correct.
upvoted 1 times

gcata 1 year, 3 months ago

Selected Answer: AC

AC
NSF allow forwarding during route recalculations
upvoted 2 times

McBeano 1 year, 4 months ago

AC - NSF is layer 3

NSF Operation
Cisco NSF always runs with SSO and provides redundancy for Layer 3 traffic. NSF works with SSO to minimize the amount of time that a network is unavailable to its users following a switchover. The main purpose of NSF is to continue forwarding IP packets following a supervisor engine switchover.
upvoted 2 times

Dryra1n 1 year, 4 months ago

Selected Answer: AC

AC is correct
upvoted 2 times

DRAG DROP -

Drag and drop the characteristics from the left onto the correct infrastructure deployment type on the right.

Select and Place:

Answer Area

significant initial investment but lower reoccurring costs	On-premises
pay-as-you-go model	
physical location of data can be defined in contract with provider	
very scalable and fast delivery of changes in scale	Cloud
company has control over the physical security of equipment	

Correct Answer:

Answer Area

significant initial investment but lower reoccurring costs	On-premises
pay-as-you-go model	significant initial investment but lower reoccurring costs
physical location of data can be defined in contract with provider	company has control over the physical security of equipment
very scalable and fast delivery of changes in scale	Cloud
company has control over the physical security of equipment	pay-as-you-go model
	physical location of data can be defined in contract with provider
	very scalable and fast delivery of changes in scale

examShark Highly Voted 2 years, 6 months ago

Provided answer is correct

upvoted 10 times

[Removed] Most Recent 4 months, 3 weeks ago

Correct answer provided

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

On-Premisses
significant initial investiment
company has control over the physical

Cloud
pay-as-you-go model
physical location of data can be
very scalable and fast delivery

upvoted 4 times

Venuste_Rwanda 1 year, 9 months ago

The provided answer is correct 100

upvoted 1 times

Question #22 *Topic 1*

In a Cisco SD-Access fabric, which control plane protocol is used for mapping and resolving endpoints?

A. DHCP

B. VXLAN

C. SXP

D. LISP

Correct Answer: *D*

Community vote distribution

D (100%)

examShark Highly Voted 2 years, 6 months ago

Provided answer is correct

upvoted 11 times

Schr0dinger Most Recent 3 months, 3 weeks ago

D.
LISP = Control Plane
VXLAN = Data Plane
TrustSec = Policy Plane

upvoted 1 times

LanreDipeolu 4 months ago

D is correct. LISP controls MS and MR

upvoted 1 times

techriese 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

ermanzan 5 months, 2 weeks ago

Provided answer is correct!! D

upvoted 1 times

networkingXIV 6 months, 3 weeks ago

Selected Answer: D

D. LISP (Locator/ID Separation Protocol) is used for mapping and resolving endpoints in a Cisco SD-Access fabric.

upvoted 2 times

mtaufik_89 7 months, 1 week ago

LISP is correct

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: D

D is correct

upvoted 2 times

Venuste_Rwanda 1 year, 9 months ago

True LISP is correct

upvoted 2 times

krn007 1 year, 11 months ago

Selected Answer: D

LISP is correct

upvoted 1 times

pierresadou 2 years, 1 month ago

D is correct

upvoted 2 times

Darcy42 2 years, 5 months ago

LISP is correct

upvoted 3 times

Hack4 2 years, 5 months ago

i agree

upvoted 2 times

flash007 2 years, 5 months ago

Lisp is a control plane protocol

upvoted 3 times

Question #23 *Topic 1*

What are two differences between the RIB and the FIB? (Choose two.)

A. FIB is a database of routing prefixes, and the RIB is the information used to choose the egress interface for each packet.

B. The FIB is derived from the data plane, and the RIB is derived from the FIB.

C. The RIB is a database of routing prefixes, and the FIB is the information used to choose the egress interface for each packet.

D. The RIB is derived from the control plane, and the FIB is derived from the RIB.

E. The FIB is derived from the control plane, and the RIB is derived from the FIB.

Correct Answer: *CD*

Community vote distribution

CD (100%)

examShark Highly Voted 2 years, 6 months ago

Provided answer is correct

upvoted 6 times

LanreDipeolu Most Recent 3 months, 4 weeks ago

Selected Answer: CD

RIB is routing prefixes while FIB is from RIB therefore, C and D are the answers

upvoted 1 times

LanreDipeolu 4 months ago

C+D are the answers.

upvoted 1 times

techriese 5 months ago

Selected Answer: CD

C + D are correct

upvoted 1 times

stan3435 10 months, 3 weeks ago

Selected Answer: CD

C and D are correct

upvoted 1 times

ciscokoolaid 11 months, 1 week ago

Selected Answer: CD

Provided answer is correct.

Both the RIB and FIB contain network prefixes with egress interface listed. If you execute an “show ip cef” command to display the contents of the CEF table (FIB), you will see the CEF entries listing the egress interface. Additionally, if CEF is enabled, the FIB is used to make forwarding decisions – RIB table is not referenced at all to determine the egress interface.

upvoted 1 times

iGlitch 1 year ago

D is correct but,

A and C both could be the answer, RIB operates at the control plane and FIB operates at the data plane, when FIB is enabled it takes a copy from the RIB.

based on that I'm leaning toward C.

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: CD

C and D are correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

C-D are correct

upvoted 1 times

wwwwaaaa 1 year, 11 months ago

Selected Answer: CD

C-D are correct

upvoted 2 times

XalaGyan 2 years, 2 months ago

C & D

Router# show ip cef adjacency GigabitEthernet 3/0 172.20.26.29
Prefix Next Hop Interface
10.1.1.0/24 10.20.26.29 GigabitEthernet3/0

the interface is there in the adjacency table which is part of FIB and CEF

upvoted 2 times

mungeri 2 years, 7 months ago

Also, the only table that has the egress interface is RIB and Adjacency Table. Not sure if you can term "FIB - a database of routing prefixes". IMO, it can be since, it does contain all the prefixes/length. If that's the case, i would pick A and D as the correct answer.

upvoted 3 times

mungeri 2 years, 7 months ago

D is correct but there is a doubt re: C. Since, FIB doesn't have the information to choose the egress interface for each packet. Just the prefix/length and next-hop

upvoted 1 times

nopenotme123 1 year, 4 months ago

It has the Prefix, Next Hop and the interface...

upvoted 1 times

DaniOcampo1992 2 years, 5 months ago

The egress interface is chosen by the RIB. Could it be A and D?

upvoted 3 times

Question #24 *Topic 1*

Which two network problems indicate a need to implement QoS in a campus network? (Choose two.)

A. port flapping

B. excess jitter

C. misrouted network packets

D. duplicate IP addresses

E. bandwidth-related packet loss

Correct Answer: *BE*

Community vote distribution

BE (100%)

flash007 Highly Voted 2 years, 7 months ago

Packet Loss and Jitter will be a good reason for implementing QoS

upvoted 8 times

examShark Highly Voted 2 years, 6 months ago

Provided answer is correct

upvoted 6 times

LanreDipeolu Most Recent 4 months ago

Certainly, B & E are the correct answers.

upvoted 1 times

techriese 5 months ago

Selected Answer: BE

B + E are correct

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: BE

B and E are correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

B and E

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: BE

voting, provided answer is correct.

upvoted 1 times

Gift07_Cisco 2 years, 2 months ago

Given two answers are correct.

upvoted 2 times

Question #25 *Topic 1*

In a Cisco SD-Access wireless architecture, which device manages endpoint ID to edge node bindings?

A. fabric control plane node

B. fabric wireless controller

C. fabric border node

D. fabric edge node

Correct Answer: *A*

Community vote distribution

A (100%)

uncookie Highly Voted 2 years, 7 months ago

Correct.
https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf
Page 6
upvoted 15 times

examShark Highly Voted 2 years, 6 months ago

Provided answer is correct
upvoted 7 times

techriese Most Recent 5 months ago

Selected Answer: A

A is correct
upvoted 1 times

eww_cybr 5 months ago

The Control plane node is the host database, tracking endpoint ID (EID) to edge node bindings, along with other attributes. It does the following:
• Supports multiple types of EID lookup keys (IPv4/32, IPv6/128, or MAC addresses).
• Receives prefix registrations from edge nodes and fabric WLCs for wired local endpoints and wireless clients, respectively.
• Resolves lookup requests from remote edge nodes to locate endpoints.
• Updates fabric edge nodes and border nodes with wireless client mobility and routing locator (RLOC) information.

https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf
upvoted 3 times

JackyChon 6 months, 2 weeks ago

Selected Answer: A

in Cisco SD-Access wireless architecture, the device responsible for managing endpoint ID to edge node bindings is the Control Plane Node (CPN).
upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: A

A is correct
upvoted 2 times

smithkeith0023366 1 year, 3 months ago

Selected Answer: A

Fabric Control-Plane Node is based on a LISP Map Server / Resolver
Runs the LISP Endpoint ID Database to provide overlay reachability information

---> A simple Host Database, that tracks Endpoint ID to Edge Node bindings (RLOCs)

https://www.ciscolive.com/c/dam/r/ciscolive/latam/docs/2018/pdf/BRKEWN-2020.pdf Page 54
upvoted 5 times

nour 1 year, 4 months ago

@uncookie, According to your file, the answer is D- fabric edge node
upvoted 1 times

[Removed] 1 year, 7 months ago

Selected Answer: A

fabric Control plane uses lisp for this function
upvoted 3 times

kthekillerc 2 years, 2 months ago
Provided answer is correct
upvoted 1 times

noov 2 years, 7 months ago
i think that the correct answer is B
upvoted 2 times

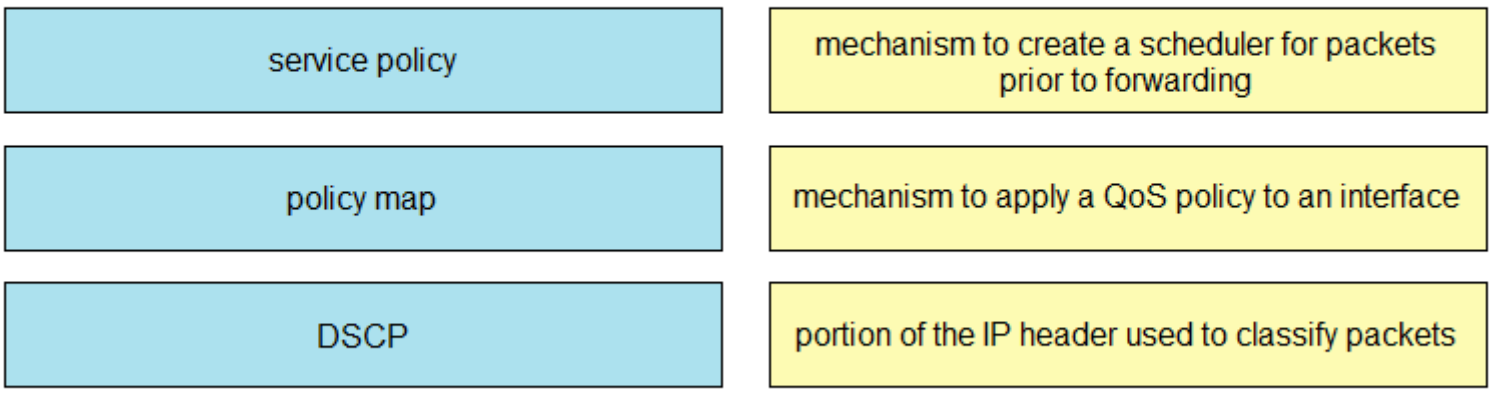
rggod 2 years, 7 months ago
The control plane receives registrations from fabric edge or border nodes for known EID prefixes from wired endpoints and from fabric mode WLCs for wireless clients. It also resolves lookup requests from fabric edge or border nodes to locate destination EIDs and updates fabric edge nodes and border nodes with wired and wireless client mobility and RLOC information.
upvoted 9 times

DRAG DROP -

Drag and drop the QoS mechanisms from the left onto their descriptions on the right.

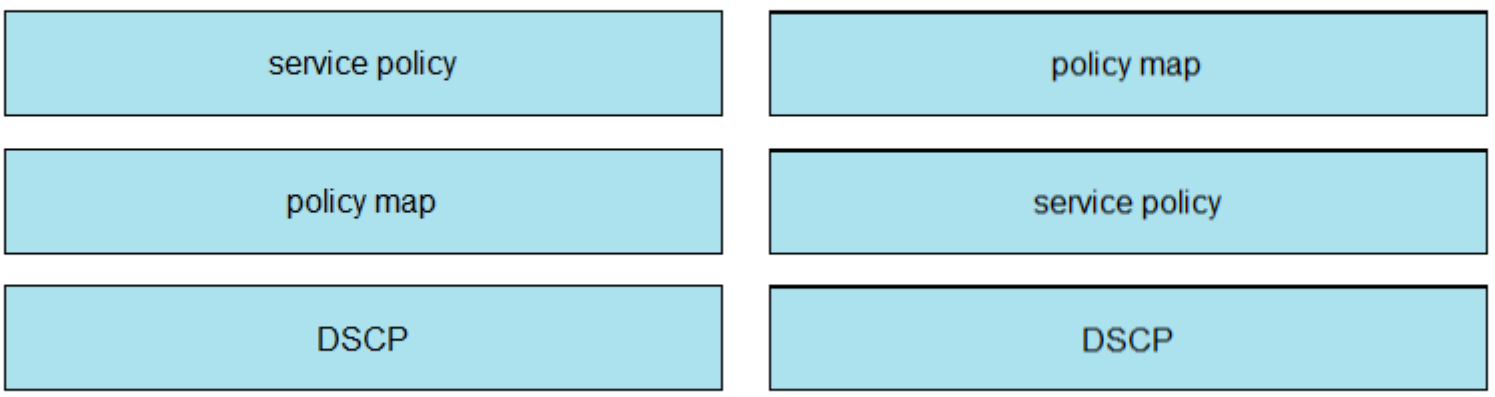
Select and Place:

Answer Area



Correct Answer:

Answer Area



mungeri Highly Voted 2 years, 7 months ago

Mod, pls fix the answer.
Correct answer imo,
DSCP == portion of the IP header used to classify the packets
policy map == mechanism to create a scheduler for packets prior to forwarding
service policy == mechanism to apply a QoS policy to an interface

upvoted 35 times

Pudu_vlad Highly Voted 1 year, 6 months ago

Service policy Mechanism to apply
policy-map mechanism to create
DSCP portion of ip header

upvoted 5 times

H3kerman Most Recent 1 year, 1 month ago

A policy map is used to perform an action (permit, deny, and so on). A service policy is a used to apply a policy on either all interfaces or a single interface

upvoted 1 times

flash007 2 years, 6 months ago

DSCP are inserted into the ip packet this is what marks the traffic.the service policy is used to assign the class map to the interface

upvoted 2 times

Rockford 2 years, 6 months ago

service-policy
To attach a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface or VC, use the service-policy command in the appropriate configuration mode. To remove a service policy from an input or output interface or from an input or output VC, use the no form of this command.

upvoted 3 times

Question #27 *Topic 1*

Which control plane protocol is used between Cisco SD-WAN routers and vSmart controllers?

A. TCP

B. OMP

C. UDP

D. BGP

Correct Answer: *B*

Community vote distribution

B (100%)

flash007 Highly Voted 2 years, 7 months ago

OMP overlay management protocol is used in sd-wan its a lot like IP-Sec tunnels

upvoted 17 times

CCNPWILL Most Recent 3 months, 3 weeks ago

OMP is correct

upvoted 1 times

techriese 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

Pilgrim5 8 months ago

Selected Answer: B

D is wrong. BGP can't be used
C is wrong. UDP can't be used.
A is wrong. TCP can't be used.
Only reasonable option is B

upvoted 1 times

Vlad_Is_Love_ua 9 months, 2 weeks ago

Selected Answer: B

Cisco vSmart controllers facilitate fabric discovery by running the Overlay Management Protocol (OMP) between each other and between Cisco vSmart and the Cisco WAN Edge routers. Cisco WAN Edge routers and Cisco vSmart controllers act as a distribution system for the pertinent information required to establish the data plane connectivity directly between the Cisco WAN Edge routers. This information includes service-side (LAN) reachability, transport-side IP addressing, IPsec encryption keys, site identifiers, and so on.

upvoted 1 times

Dataset 9 months, 3 weeks ago

Selected Answer: B

thats correct, OMP (Overlay Management Protocol)
Regards!

upvoted 1 times

Asymptote 1 year ago

Selected Answer: B

B

The Viptela Overlay Management Protocol (OMP) establishes and maintains the Viptela control plane.

OMP is enabled by default on all vEdge routers, vManage NMSs, and vSmart controllers, so there is no need to explicitly configure or enable OMP. OMP must be operational for the Viptela overlay network to function. If you disable it, you disable the overlay network.

Reference:
https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Templates/OMP#:~:text=The%20Viptela%20Overlay,the%20overlay%20network.

upvoted 2 times

GeorgeFortiGate 1 year ago

Selected Answer: B

B is correct

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

B is correct

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: B

Overlay management Protocol used as the control plane protocol for SDWAN

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: B

Voting. provided answer is correct.

upvoted 1 times

diegodavid82 2 years, 3 months ago

Provided answer is correct

upvoted 4 times

Question #28 *Topic 1*

In a three-tier hierarchical campus network design, which action is a design best-practice for the core layer?

A. provide QoS prioritization services such as marking, queueing, and classification for critical network traffic

B. provide redundant Layer 3 point-to-point links between the core devices for more predictable and faster convergence

C. provide advanced network security features such as 802.1X, DHCP snooping, VACLs, and port security

D. provide redundant aggregation for access layer devices and first-hop redundancy protocols such as VRRP

Correct Answer: *B*

Community vote distribution

B (100%)

SandyIndia Highly Voted 2 years, 3 months ago

A. provide QoS prioritization services such as marking, queueing, and classification for critical network traffic.
Distribution layer.
B. provide redundant Layer 3 point-to-point links between the core devices for more predictable and faster convergence.
Core Layer.
C. provide advanced network security features such as 802.1X, DHCP snooping, VACLs, and port security.
Access Layer.
D. provide redundant aggregation for access layer devices and first-hop redundancy protocols such as VRRP.
Distribution layer.
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

upvoted 17 times

techriese Most Recent 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

SheldonC 10 months, 1 week ago

B) - From Cisco:

[...] Use redundant point-to-point L3 interconnections in the core (triangles, not squares) wherever possible, because this design yields the fastest and most deterministic convergence results. <<<<< B) IS CORRECT>>>>>

DEIGN DOCUMENT - [CORE SECTION]
SOURCE: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

upvoted 1 times

GeorgeFortiGate 1 year ago

B is the correct answer.

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

Answer B,

upvoted 1 times

GreatDane 1 year, 6 months ago

Ref: Cisco Three-Tier Architecture Explained - ICTShore.com

"...
Connecting the Three Tier Architecture
...
As a best practice, this link must be a Layer 3 point-to-point link. If this is not available due to software limitations, you should avoid a Layer 2 link and have no link at all. This way you will prevent loop and spanning-tree convergence time. Sometimes, even in networking the less is more.
..."

A. provide QoS prioritization services such as marking, queueing, and classification for critical network traffic

Wrong answer.

B. provide redundant Layer 3 point-to-point links between the core devices for more predictable and faster convergence

Correct answer.

C. provide advanced network security features such as 802.1X, DHCP snooping, VACLs, and port security

Wrong answer.

D. provide redundant aggregation for access layer devices and first-hop redundancy protocols such as VRRP

Wrong answer.
upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: B

All policies are configured an the access and distribution layer, CORE must be use ony to forward packets and be highly redundant an usually be on L3
upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: B

voting. provided answer is correct.
upvoted 1 times

diegodavid82 2 years, 3 months ago

I agree with all us, the correct answer is B.
upvoted 2 times

Hack4 2 years, 5 months ago

QoS can be applied close to a source as possible. Then the best answer is B
upvoted 2 times

flash007 2 years, 6 months ago

B removes the need for spanning tree by using redundant links
upvoted 1 times

powerslave666 2 years, 6 months ago

Answer B,
upvoted 2 times

ind_RuzRb 2 years, 7 months ago

Is B a correct answer or Is it D?
Please review and confirm!!!
upvoted 1 times

Mac13 2 years, 7 months ago

I'd say "B" is the correct answer.

In a three tier model, access layer aggregation and FHRP is done at the distribution layer. Not core.

The core is all about speed and reliability/redundancy.
upvoted 6 times

Question #29 *Topic 1*

What is a VPN in a Cisco SD-WAN deployment?

A. common exchange point between two different services

B. attribute to identify a set of services offered in specific places in the SD-WAN fabric

C. virtualized environment that provides traffic isolation and segmentation in the SD-WAN fabric

D. virtual channel used to carry control plane information

Correct Answer: *C*

Community vote distribution

C (100%)

examShark Highly Voted 2 years, 6 months ago

Provided answer is correct

upvoted 7 times

Barry_Allen 2 years, 6 months ago

@examShark Thanks mate !

upvoted 1 times

techriese Most Recent 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

SheldonC 10 months, 1 week ago

C - From Cisco:

[...] VPN Segmentation: Traffic isolation is key to any security strategy. Traffic that enters the router is assigned to a VPN, which not only isolates user traffic, but also provides routing table isolation. This ensures that a user in one VPN cannot transmit data to another VPN unless explicitly configured to do so. When traffic is transmitted across the WAN, a label is inserted after the ESP header to identify the VPN that the user's traffic belongs to when it reaches the remote destination. <<<<< C IS CORRECT>>>>>

Cisco SD-WAN Design Guide
SOURCE: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

upvoted 3 times

GeorgeFortiGate 1 year ago

Selected Answer: C

C is the correct answer.

upvoted 1 times

turbosteam888 1 year, 1 month ago

anyone can enlight me where the B answer is wrong? thank you

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

GreatDane 1 year, 6 months ago

Ref: Cisco SD-WAN (Viptela) Configuration Guide, Release 18.1

"...
Segmentation (VPN) Overview

This article illustrates the segmentation and VPN capabilities of the Viptela overlay network solution.

Network segmentation has existed for over a decade and has been implemented in multiple forms and shapes. At its most rudimentary level, segmentation provides traffic isolation. The most common forms of network segmentation are virtual LANs, or VLANs, for Layer 2 solutions, and virtual routing and forwarding, or VRF, for Layer 3 solutions.
..."

A. common exchange point between two different services

Wrong answer.

B. attribute to identify a set of services offered in specific places in the SD-WAN fabric

Wrong answer.

C. virtualized environment that provides traffic isolation and segmentation in the SD-WAN fabric

Correct answer.

D. virtual channel used to carry control plane information

Wrong answer.

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct.

upvoted 1 times

diegodavid82 2 years, 3 months ago

The correct answer is C, the VPN service is not alway related with "Secure", into MPLS architecture is used for provide isolated traffic without "Secure" component, same as SD-WAN.

upvoted 1 times

flash007 2 years, 4 months ago

the V in VPN is for virtual.A vpn is a secure encrypted tunnel that does provide traffic segmentation so the answer is C 100%

upvoted 1 times

Question #30 *Topic 1*

Which function does a fabric edge node perform in an SD-Access deployment?

A. Connects endpoints to the fabric and forwards their traffic.

B. Encapsulates end-user data traffic into LISP.

C. Connects the SD-Access fabric to another fabric or external Layer 3 networks.

D. Provides reachability between border nodes in the fabric underlay.

Correct Answer: *A*

Community vote distribution

A (90%) 10%

edg Highly Voted 3 years, 3 months ago

Answer is "A":
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/vxlan/configuration/guide/b_NX-OS_VXLAN_Configuration_Guide/campus-fabric.pdf
"Fabric Edge Node : Fabric edge nodes are responsible for admitting, encapsulating/decapsulating and forwarding traffic to and from endpoints connected to the fabric edge"

upvoted 14 times

djedeen Most Recent 2 months, 2 weeks ago

Selected Answer: A

Subtle nuance, B is wrong because encap is VLXAN, LISP is the control plane EID/RLOC mgmt.

upvoted 1 times

Arodoeth 3 months, 2 weeks ago

Selected Answer: B

A is true and B is equally true. Consider that an SD-Access Fabric Edge Node is a LISP tunnel router (xTR). Given the LISP definition of xTR from the Official Cert Guide:
* Ingress tunnel router (ITR): ITRs are LISP routers that LISP encapsulate IP packets coming from EIDs that are destined outside the LISP site.
* Egress tunnel router (ETR): ETRs are LISP routers that de-encapsulate LISP-encapsulated IP packets coming from sites outside the LISP site and destined to EIDs within the LISP site.
* Tunnel router (xTR): xTR refers to routers that perform ITR and ETR functions (which is most routers).
Therefore the Edge Node is tunneling endpoint (EID) traffic.

upvoted 1 times

[Removed] 3 months, 1 week ago

So I agree here but there's an extra cavate in that the SD-Access could be using VXLAN for the data plane which would mean that the end-user data is technically encapsulated by VXLAN then LISP on top of it. B is true in some regards but this interpretation would mean that choice A is more true.

upvoted 1 times

techriese 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

flash007 8 months ago

fabric edge nodes connect the endpoints to the fabric

upvoted 1 times

Vlad_Is_Love_ua 9 months ago

Selected Answer: A

Control Plane Nodes: Map system that manages endpoint-to-device relationships

Fabric Border Nodes: A fabric device (for example, Core) that connects the external Layer 3 networks to the SD-Access fabric

Fabric Edge Nodes: A fabric device (for example access or distribution) that connects wired endpoints to the SD-Access fabric

upvoted 2 times

GeorgeFortiGate 1 year ago

Selected Answer: A

A is the correct answer.

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: A

The provied answer is the correct

upvoted 1 times

Marving 1 year, 10 months ago

Selected Answer: A

The role of the fabric Edge node is to provide connectivity to wired endpoint by forwarding traffic to and from endpoints connected to the fabric edge.

upvoted 2 times

error_909 2 years, 2 months ago

B is not wrong but its not its main job:

A fabric edge provides a single Layer 3 anycast gateway (that is, the same SVI with the same IP address on all fabric edge nodes) for its connected endpoints and also performs the encapsulation and de-encapsulation of host traffic to and from its connected endpoints.

From cisco official book.

upvoted 4 times

Eddgar0 1 year, 7 months ago

B is wrong because SD-access uses VXLAN encapsulation (not LISP), LISP is only used as a control plane. Mapping EID RLOC.

upvoted 6 times

hasanozdemirrr 2 years, 5 months ago

A is correct

upvoted 2 times

flash007 2 years, 7 months ago

The edge node connects endpoints to the fabric

upvoted 3 times

anonymous1966 2 years, 10 months ago

Book: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide
Page: 622
Fabric edge node: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.

upvoted 4 times

hku68 2 years, 10 months ago

A is correct

upvoted 1 times

Afie 3 years, 2 months ago

my Answer is "A"

upvoted 3 times

Question #31 *Topic 1*

What is the role of a fusion router in an SD-Access solution?

A. acts as a DNS server

B. provides additional forwarding capacity to the fabric

C. performs route leaking between user-defined virtual networks and shared services

D. provides connectivity to external networks

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/dna-center/213525-sda-steps-to-configure-fusion-router.html#anc1

Community vote distribution

C (100%)

techriese 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

kalbos 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

Asymptote 1 year ago

Selected Answer: C

C

A Fusion device enables Virtual routing and forwarding (VRF) leaking across SD-Access Fabric domains, and enables host connectivity to shared services, such as DHCP, DNS, NTP, ISE, Cisco DNA Center, Wireless LAN Controllers (WLC), and similar. While this role can be performed by other devices than routers, this document focuses on routers as Fusion devices.

Reference:
https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/dna-center/213525-sda-steps-to-configure-fusion-router.html

upvoted 2 times

cloud29 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

kingkongkzw 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

Mohammad20 1 year, 6 months ago

Hi everyone,
I can not do checkout for activating "Contributor Access" since 3 days ago. The PayPal option doesn't work.
Also, I sent email to team@...., no answer still !!
Who can help me about it ?
Thank you

upvoted 1 times

SVN05 3 months ago

Can't use debit or credit card?

upvoted 1 times

ayodejiadeyemi 1 year, 6 months ago

fusion router enables Virtual routing and forwarding (VRF) leaking across SD-Access

upvoted 2 times

examShark 2 years, 6 months ago

Provided answer is correct

upvoted 3 times

flash007 2 years, 7 months ago

The Fusion router performs route leaking

upvoted 3 times

Question #32 *Topic 1*

Which action is the vSmart controller responsible for in an SD-WAN deployment?

A. onboard vEdge nodes into the SD-WAN fabric

B. gather telemetry data from vEdge routers

C. distribute security information for tunnel establishment between vEdge routers

D. manage, maintain, and gather configuration and status for nodes within the SD-WAN fabric

Correct Answer: *C*

Community vote distribution

C (100%)

iGlitch Highly Voted 1 year ago

Selected Answer: C

- onboard vEdge nodes into the SD-WAN fabric (vBond)
- gather telemetry data from vEdge routers (vAnalytics)
- distribute security information for tunnel establishment between vEdge routers (vSmart)
- manage, maintain, and gather configuration and status for nodes within the SD-WAN fabric (vManage)

upvoted 17 times

james4231 Highly Voted 3 years, 2 months ago

C should be the answer. Vsmart should be controlling edge routers

upvoted 13 times

techriese Most Recent 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

stan3435 10 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

smithkeith0023366 1 year, 3 months ago

Selected Answer: C

(vManage) is responsible for central configuration and monitoring. The vManage controller is the centralized network management system that provides a single pane of glass GUI interface to easily deploy, configure, monitor and troubleshoot all Cisco SD-WAN components in the network. (-> Answer "manage, maintain, and gather configuration and status for nodes within the SD-WAN fabric" and answer "gather telemetry data from vEdge routers" are about vManage)

upvoted 1 times

GreatDane 1 year, 6 months ago

Ref: Cisco SD-WAN Getting Started Guide - The Cisco SD-WAN Solution [Cisco SD-WAN] – Cisco

"...
Cisco SD-WAN Components
...
Primary Cisco SD-WAN Components
...
Cisco vSmart Controller
...
Each Cisco vSmart Controller establishes and maintains a control plane connection with each edge router in the overlay network.
...
Each connection, which runs as a DTLS tunnel, is established after device authentication succeeds, and it carries the encrypted payload between the Cisco vSmart Controller and the edge router.
..."

A. onboard vEdge nodes into the SD-WAN fabric

Wrong answer.

B. gather telemetry data from vEdge routers

Wrong answer.

C. distribute security information for tunnel establishment between vEdge routers

Correct answer.

D. manage, maintain, and gather configuration and status for nodes within the SD-WAN fabric

Wrong answer.
upvoted 1 times

Marving 1 year, 10 months ago

Selected Answer: C

It provides the control plane for the network fabric, facilitates the data plane encryption between WAN edges, and propagates the centralized policies that establish and direct the fabric
upvoted 2 times

rpidcock 2 years, 3 months ago

C is the correct answer because it established the DTLS Tunnel.
After successful authentication, each vSmart controller establishes a permanent DTLS tunnel to each SD-WAN router in the SD-WAN fabric and uses these tunnels to establish Overlay Management Protocol (OMP) neighborships with each SD-WAN router
upvoted 1 times

flash007 2 years, 7 months ago

I would say C as the vsmart device is connected with security
upvoted 2 times

Metro 2 years, 8 months ago

C 100% correct
upvoted 2 times

GustavBP 2 years, 10 months ago

C. From the SD-WAN Design Guide: Each WAN Edge router generates one AES key per TLOC and transmits this information to the vSmart controller in OMP route packets, which is then distributed to all WAN Edge routers.
upvoted 3 times

Helloory 3 years ago

Correct answer is C
upvoted 4 times

Benzzyy 3 years, 1 month ago

The correct answer is C according to Boson
The vSmart controller distributes security information between vEdge routers to facilitate data plane IPSEC tunnel creation. The vSmart uses OMP to distribute routing information, security keys, and policy configurations through DTLS tunnels th the vEdge routers. The vEdge routers can then use this information to determine the appropriate next hop for data plane traffic, to create IP Sec tunnels to other vEdge routers for data plane traffic, and to ensure that SLAs are met and that traffic policies are enforced.

Remember, the vBond authenticates the vEdge to the vSmart controller during the INITIAL sequences. The vSmart helps orchestrate the tunnel creation between vEdges.
upvoted 5 times

TheNetworkStudent 3 years, 2 months ago

Role of the vBond Orchestrator is to authenticate and orchestrate connectivity between SD-WAN routers and vSmart controllers, the correct answer cannot be C because vBond does it and not vSmart, for the same reason B cannot be the correct answer...

I'm split between A and D, because it does contain the credentials to authenticate the vEdge devices but the communication is again done by vBond, so A doesn't feel right either.

Because of OMP I think it is D because the communication is done by vSmart after vBond has facilitated everything it needs to facilitate.
upvoted 1 times

TheNetworkStudent 3 years, 2 months ago

Checked a couple websites and apparantly the SD-WAN roles per answer were:

A. vBond
B. vManage
C. vSmart
D. vManage

C is right
upvoted 8 times

ic0n88 3 years, 2 months ago

Should be "C" is the correct answer.

vSmart controller – This software-based component is responsible for the centralized control plane of the SD-WAN network. It establishes a

secure connection to each vEdge router and distributes routes and policy information via the Overlay Management Protocol (OMP), acting as a route reflector. It also orchestrates the secure data plane connectivity between the vEdge routers by distributing crypto key information, allowing for a very scalable, IKE-less architecture.

upvoted 4 times

patrickni 3 years, 2 months ago

I would go with A (onboarding vEdge nodes) -Dumb Lemon

upvoted 1 times

Question #33 *Topic 1*

What is one fact about Cisco SD-Access wireless network deployments?

A. The access point is part of the fabric overlay.

B. The wireless client is part of the fabric overlay.

C. The access point is part of the fabric underlay.

D. The WLC is part of the fabric underlay.

Correct Answer: *A*

Community vote distribution

A (88%) 13%

Heim_Ox Highly Voted 1 year, 5 months ago

Page 10. AP must be part of the fabric overlay. https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf

upvoted 8 times

nebtashi Highly Voted 1 year, 5 months ago

From ENCOR official guide chapter 23 (SD-ACCESS) "While Cisco SD-Access is designed for user simplicity, abstraction, and virtual environments, everything runs on top of physical network devices—namely switches, routers, servers, wireless LAN controllers (WLCs), and wireless access points (APs)" - Why do you say APs are part of the overlay and not the underlay?

upvoted 8 times

Frix83 1 month, 1 week ago

Cisco SD Access Architecture is divided into 4 layers: Physical, network, controller and management layer. Overlay network and underlay network is defined in the network layer of Cisco SD Access Architecture. The quoted text are referring to the physical layer, ie. the components the physical network is comprised of.

upvoted 2 times

rogue_user Most Recent 4 months, 3 weeks ago

Selected Answer: A

AP forwards traffic which is a function of overlay. WLC is external to fabric. Client is a catch since it's end user.

upvoted 1 times

techriese 5 months ago

Selected Answer: A

A is correct
Access points must be deployed as follows:
• Be directly connected to the fabric edge (or to an extended node switch)
• Be part of the fabric overlay
• Belong to the INFRA_VN, which is mapped to the global routing table
• Join the WLC in Local mode

eww_cybr 5 months ago

A

Access points must be deployed as follows:
• Be directly connected to the fabric edge (or to an extended node switch)
• Be part of the fabric overlay
• Belong to the INFRA_VN, which is mapped to the global routing table
• Join the WLC in Local mode

https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf

upvoted 1 times

siyamak 6 months ago

The correct answer is A.
SD-Access Wireless network deployment
This section gives some important considerations for deploying WLC and APs in an SD-Access Wireless network. please refer to the picture below:
Access points must be deployed as follows:
• Be directly connected to the fabric edge (or to an extended node switch)
• Be part of the fabric overlay
• Belong to the INFRA_VN, which is mapped to the global routing table
• Join the WLC in Local mode

upvoted 2 times

VincentY 7 months, 1 week ago

Client traffic from wireless endpoints is not tunneled from the APs to the wireless controller. Instead, communication from wireless clients is encapsulated in VXLAN by the fabric APs which build a tunnel to their first-hop fabric edge node.
A is the correct answer.

upvoted 1 times

Chiaretta 9 months, 2 weeks ago

Selected Answer: C

AP as equipment is part of the underlay

upvoted 2 times

Chiaretta 9 months, 2 weeks ago

AP as equipment is part of the underlay

upvoted 1 times

dnjJ56 11 months, 1 week ago

Selected Answer: A

In the SD-Access solution, Cisco DNA Center configures wireless APs to reside within an overlay VN named INFRA_VN which maps to the global routing table.

Ref: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

upvoted 3 times

Asymptote 1 year ago

Selected Answer: A

the fabric AP also form a VXLAN tunnel to the up-stream switch for data plane traffics, means the users would stay within the overlay and connect directly to those switches in the fabric.

upvoted 4 times

cloud29 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

gcata 1 year, 3 months ago

Selected Answer: A

A - AP is part of overlay network from design point of view.
(talk to WLC using underlay network)

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: A

Indeed, WLC's, like AP's are part of the Fabric SD-Access.

upvoted 1 times

alawi2 1 year, 5 months ago

yes they are a part of fabric alright, but i never once found a mention whether it is underlay or overlay, any links?

upvoted 1 times

Marving 1 year, 10 months ago

Selected Answer: A

In SD-Access Wireless, The WLC and APs are integrated into the fabric, and the APs connect to the fabric overlay.

upvoted 2 times

Question #34 *Topic 1*

In a Cisco SD-Access solution, what is the role of a fabric edge node?

A. to connect external Layer 3 networks to the SD-Access fabric

B. to connect wired endpoints to the SD-Access fabric

C. to advertise fabric IP address space to external networks

D. to connect the fusion router to the SD-Access fabric

Correct Answer: *B*

Community vote distribution

B (100%)

litbe Highly Voted 2 years, 11 months ago

B Correct
Refer to https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjF37T9udPtAhXwo4sKHfwzDKoQFjAAegQIAxAC&url=https%3A%2F%2Fwww.cisco.com%2Fc%2Fdam%2Fm%2Fhr_hr%2Ftraining-events%2F2019%2Fcisco-connect%2Fpdf%2FVH-Cisco-SD-Access-Connecting.pdf&usg=AOvVaw26SeDD9KzfyOqR-hk_vF3q

upvoted 11 times

SandyIndia 2 years, 1 month ago

A. to connect external Layer 3- network to the SD-Access fabric (Fabric Border Nodes - A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric like Routers)
B. to connect wired endpoint to the SD-Access fabric (Fabric Edge Nodes - A Fabric device
(e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric.
C. to advertise fabric IP address space to external network (Border Nodes Connects to any "known" IP subnets available from the outside network (e.g. DC, WLC, FW, etc.)
D. to connect the fusion router to the SD-Access fabric. (Border Nodes Connects to any "known" IP subnets available from the outside network (e.g. Fusion Router, DC, WLC, FW, etc.)

upvoted 3 times

techriese Most Recent 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

Stylar 11 months ago

Fabric APs are part of overlay as they establish a VXLAN tunnel to the fabric edge to transport wireless client data traffic through the VXLAN tunnel instead of the CAPWAP tunnel > Increases performance

upvoted 1 times

iGlitch 1 year ago

Selected Answer: B

A,C and D = Fabric Border node
B = Fabric Edge node

upvoted 1 times

GeorgeFortiGate 1 year ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

ayodejiadeyemi 1 year, 6 months ago

provided answer is correct.

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: B

voting. provided answer is correct.

upvoted 1 times

hasanozdemirrr 2 years, 5 months ago

Sorry B is correct

upvoted 1 times

hasanozdemirrr 2 years, 5 months ago

Wireless Controller – A Fabric device (WLC) that connects APs and Wireless Endpoints to the SDA Fabric,
So C correct

upvoted 1 times

flash007 2 years, 7 months ago

The fabric edge node is used to connect the end devices to the SD access fabric network

upvoted 2 times

skh 3 years ago

C correct
+ Fabric edge node: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.

upvoted 1 times

iking 2 years, 9 months ago

your description is B, y do you answer C. B is the correct answer

upvoted 2 times

Question #35 *Topic 1*

What are two reasons a company would choose a cloud deployment over an on-prem deployment? (Choose two.)

A. Cloud costs adjust up or down depending on the amount of resources consumed. On-prem costs for hardware, power, and space are on-going regardless of usage.

B. Cloud resources scale automatically to an increase in demand. On-prem requires additional capital expenditure.

C. In a cloud environment, the company is in full control of access to their data. On-prem risks access to data due to service provider outages.

D. In a cloud environment, the company controls technical issues. On-prem environments rely on the service provider to resolve technical issues.

E. Cloud deployments require long implementation times due to capital expenditure processes. On-prem deployments can be accomplished quickly using operational expenditure processes.

Correct Answer: *AB*

Community vote distribution

AB (100%)

examShark Highly Voted 2 years, 6 months ago

Provided answer is correct

upvoted 9 times

Hamo1 Most Recent 3 months ago

A&bB is correct

upvoted 1 times

techriese 5 months ago

Selected Answer: AB

A + B is correct

upvoted 1 times

ermanzan 5 months, 2 weeks ago

A and B are correct!!!

upvoted 1 times

Splashisthegreatestmovie 5 months, 2 weeks ago

A&B are literally paraphrases of each other

upvoted 1 times

stan3435 10 months, 3 weeks ago

Selected Answer: AB

A and B

upvoted 1 times

MarkThomson 1 year ago

Selected Answer: AB

A & B are correct

upvoted 1 times

GeorgeFortiGate 1 year ago

Selected Answer: AB

A & B for sure

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: AB

A and B are correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: AB

voting. provided answer is correct.

upvoted 1 times

Question #36 *Topic 1*

What is the difference between the MAC address table and TCAM?

A. TCAM is used to make L2 forwarding decisions. CAM is used to build routing tables.

B. Router prefix lookups happen in CAM. MAC address table lookups happen in TCAM.

C. The MAC address table supports partial matches. TCAM requires an exact match.

D. The MAC address table is contained in CAM. ACL and QoS information is stored in TCAM.

Correct Answer: *D*

Community vote distribution

D (71%) B (29%)

Rockford Highly Voted 2 years, 6 months ago

There's a typo on D, should read "MAC are stored in CAM not TCAM...

upvoted 17 times

diegodavid82 2 years, 3 months ago

Yes, the answer have a type mistake, in the first part is MAC not TCAM.

upvoted 3 times

raizer 2 years, 2 months ago

yes, agree with D as correct answer.
When using Ternary Content Addressable Memory (TCAM) inside routers it's used for faster address lookup that enables fast routing.

In switches Content Addressable Memory (CAM) is used for building and lookup of mac address table that enables L2 forwarding decisions.

Besides Longest-Prefix Matching, TCAM in today's routers and multilayer Switch devices are used to store ACL, QoS and other things from upper-layer processing.

upvoted 1 times

certtaker202 2 years, 3 months ago

Absolutely agree with the typo.

upvoted 2 times

wwwwaaaa 1 year, 11 months ago

They are saying "contained" which is not wrong.
You are right, MACs are in CAM and CAM contained in TCAM, and all of us are winners

upvoted 3 times

arieldesamachado Highly Voted 2 years, 7 months ago

the correct answer is B

upvoted 11 times

noov 2 years, 7 months ago

i think so

upvoted 1 times

Dudu84 Most Recent 5 days, 1 hour ago

D is the correct answer

https://www.ciscopress.com/articles/article.asp?p=101629&seqNum=4

upvoted 1 times

Johalobe 2 months ago

Selected Answer: D

Correct answer is D

upvoted 1 times

CCNPWILL 3 months, 3 weeks ago

Correct answer is D.

upvoted 1 times

anaz691011 4 months ago

which one is good

upvoted 1 times

rogue_user 4 months, 3 weeks ago

Selected Answer: D

CAM requires an exact match to return a result. This means that the value that is being searched for (in binary) must contain either 0s or 1s. TCAM does not require an exact match, and is queried using 0s, 1s, and Xs, where X essentially means “anything” (that is, either 0 or 1). It's kind of like a wildcard state.

upvoted 1 times

techriese 5 months ago

Selected Answer: D

D is correct for me

upvoted 1 times

helmerpach 5 months ago

I took the exam yesterday and passed it. I confirm the question as it appears in the exam. It is not the administrator's fault.

upvoted 1 times

Blue_Water 7 months, 1 week ago

Selected Answer: D

Correct is D

upvoted 1 times

Chiaretta 7 months, 2 weeks ago

Selected Answer: D

D is the correct answer

upvoted 1 times

paulosrsf 8 months, 2 weeks ago

Selected Answer: D

Correct is D. CAM contains the MAC address table and their VLANS. TCAM is used for ACL and QoS purposes.
TCAM is the table that supports partial matches, for ACL purposes.
People answering option B as correct are badly wrong. Routing lookups are made in RIB, wich is the routing database.

upvoted 1 times

Chiaretta 9 months, 2 weeks ago

Selected Answer: D

CAM stores only MAC addresses.

upvoted 1 times

cerf 9 months, 3 weeks ago

D is the correct! https://community.cisco.com/t5/networking-knowledge-base/cam-content-addressable-memory-vs-tcam-ternary-content/ta-p/3107938

upvoted 2 times

eff3 10 months, 1 week ago

Selected Answer: D

CAM L2 - TCAM L2/L3

upvoted 2 times

Chiaretta 10 months, 2 weeks ago

D is correct

upvoted 1 times

kewokil120 10 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

Question #37 *Topic 1*

Which controller is the single plane of management for Cisco SD-WAN?

A. vBond

B. vSmart

C. vManage

D. vEdge

Correct Answer: *C*
Reference:
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf

Community vote distribution
C (100%)

Multicast01005e Highly Voted 2 years, 1 month ago
I wish there were more questions related to technology in general, deep into TCP, with SDWAN and SD Access it feels like I am becoming a product specialist not a technologist.
upvoted 12 times

DJOHNR Highly Voted 3 years, 3 months ago
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

Management Plane

vManage is the Cisco SD-WAN centralized GUI that allows to manage the SD-WAN network from end to end from a single dashboard.

Answer C
upvoted 6 times

techriese Most Recent 5 months ago
Selected Answer: C
C is correct
upvoted 1 times

Abbribas 11 months, 4 weeks ago
vManage is the centralized management dashboard.
upvoted 1 times

cdanielz 1 year ago
Selected Answer: C
Selected answer is correct
upvoted 1 times

cloud29 1 year, 1 month ago
Selected Answer: C
C is correct
upvoted 1 times

jaz600 1 year, 4 months ago
Selected Answer: C
vManage
upvoted 1 times

Pudu_vlad 1 year, 6 months ago
Answer C
upvoted 1 times

ciscolessons 1 year, 9 months ago
Selected Answer: C
voting. provided answer is correct.
upvoted 1 times

flash007 2 years, 7 months ago
Vmanage is the single plain of glass to manage the SD-Wan infrastructure

upvoted 2 times

Question #38 *Topic 1*

A company plans to implement intent-based networking in its campus infrastructure.
Which design facilitates a migration from a traditional campus design to a programmable fabric design?

A. two-tier

B. Layer 2 access

C. three-tier

D. routed access

Correct Answer: *D*

Community vote distribution

D (89%) 11%

emily3221 Highly Voted 3 years, 2 months ago

There is a paragraph in the book that says it's routed access!!!
upvoted 28 times

RexChen 3 years, 2 months ago

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/BRKCRS-2812.pdf
upvoted 5 times

hualim 2 years, 4 months ago

page 35 go
upvoted 2 times

vdsdrs 2 years, 4 months ago

Routed access is correct answer.
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.pdf#%5B%7B%22num%22%3A37%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C272%2C708%2C0%5D
upvoted 5 times

james4231 Highly Voted 3 years, 2 months ago

Ideal design is routed access – allows fabric to extend
to very edge of campus network
upvoted 8 times

Njavwa Most Recent 3 months ago

routed access or layer 3 access
upvoted 1 times

rogue_user 4 months, 3 weeks ago

Selected Answer: D

SD-WAN builds on top of IP fabric
upvoted 1 times

techriese 5 months ago

Selected Answer: D

D is correct. SDA is full routed access
upvoted 1 times

mrtattoo 6 months, 4 weeks ago

Selected Answer: D

D. Routed access is the design that facilitates a migration from a traditional campus design to a programmable fabric design.

In a traditional campus design, the access layer is typically implemented using a Layer 2 switch with VLANs, and the distribution layer performs the routing between VLANs. In contrast, a programmable fabric design uses a routed access layer, where each access switch has an IP address and performs routing locally, eliminating the need for a separate distribution layer.

By implementing a routed access design, the company can gradually migrate from a traditional campus design to a programmable fabric design. The Layer 2 access and two-tier designs are both traditional campus designs and do not facilitate the migration to a programmable fabric design. The three-tier design includes a distribution layer, which is not needed in a programmable fabric design with routed access.
upvoted 3 times

habibmangal 7 months, 3 weeks ago

Selected Answer: C

Option D (routed access) is not necessarily wrong, but it is not the best answer to the question. Routed access can be used with a programmable fabric design, but it does not necessarily facilitate the migration from a traditional campus design to a programmable fabric design.

In a routed access design, the access layer switches are configured as Layer 3 devices, and traffic is routed directly from the access layer to the distribution or core layer. This approach can provide greater flexibility and scalability than traditional Layer 2 access designs, but it does not necessarily facilitate the migration to a programmable fabric design.

On the other hand, a three-tier architecture provides the necessary separation between the access, distribution, and core layers, which allows for greater flexibility and scalability when implementing programmable fabric designs. This is why option C (three-tier) is a better answer to the question.

upvoted 2 times

Asymptote 1 year ago

Selected Answer: D

D

Layer 3 Routed Access—The use of a Layer 3 routed access network for the fabric provides the highest level of availability without the need to use loop avoidance protocols such as Spanning-Tree (STP), interface bundling techniques using link aggregation technologies such as EtherChannel, and Layer 2 redundancy technologies like StackWise Virtual (SVL), Virtual Switching System (VSS), or Nexus Virtual Port-Channels (vPCs).

Reference:
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.pdf#%5B%7B%22num%22%3A37%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C272%2C708%2C0%5D

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: D

D is correct

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

Router-Access

upvoted 1 times

GreatDane 1 year, 6 months ago

Ref: CCDE Study Guide: Enterprise Campus Architecture Design

"C H A P T E R 3
Access-Distribution Design Model
...
• Classical multitier STP based: This model is the classical or traditional way of connecting access to the distribution layer in the campus network. In this model, the access layer switches usually operate in Layer 2 mode only, and the distribution layer switches operate in Layer 2 and Layer 3 modes.
...
• Routed access: In this design model, access layer switches act as Layer 3 routing nodes, providing both Layer 2 and Layer 3 forwarding. In other words, the demarcation point between Layer 2 and Layer 3 is moved from the distribution layer to the access layer. Based on that, the Layer 2 trunk links from access to distribution are replaced with Layer 3 point-to-point routed links,
...
The routed access design model has several advantages compared to the multitier classical STP-based access-distribution design model,
..."

A. two-tier

Wrong answer.

B. Layer 2 access

Wrong answer.

C. three-tier

Wrong answer.

D. routed access

Correct answer.

upvoted 1 times

ayodejiadeyemi 1 year, 6 months ago

routed access is the correct answer

upvoted 1 times

DLLLLLLLL 1 year, 6 months ago

Selected Answer: D

routed access

upvoted 1 times

danny_f 1 year, 7 months ago

The SDA Cisco Validated Design mentioned two-tier and three-tier with regard to the size of the network. Traditional three tier vs collapsed core. So it's probably routed access.

upvoted 2 times

GABSI08W 1 year, 7 months ago

A
Intent-based Networking (IBN) transforms a hardware-centric, manual network into a controller-led network that captures business intent and translates it into policies that can be automated and applied consistently across the network. The goal is for the network to continuously monitor and adjust network performance to help assure desired business outcomes. IBN builds on software-defined networking (SDN). SDN usually uses spine-leaf architecture, which is typically deployed as two layers: spines (such as an aggregation layer), and leaves (such as an access layer).

upvoted 6 times

Eddgar0 1 year, 7 months ago

Selected Answer: D

ON SD-ACCESS topic and SD-ACCESS cisco desing page explicit says routed access for facilitated SDWAN deployment.

upvoted 3 times

Aldebeer 1 year, 7 months ago

Selected Answer: D

I'm convinced: D

upvoted 1 times

Question #39 *Topic 1*

Which statement about a fabric access point is true?

A. It is in local mode and must be connected directly to the fabric edge switch.

B. It is in local mode and must be connected directly to the fabric border node.

C. It is in FlexConnect mode and must be connected directly to the fabric border node.

D. It is in FlexConnect mode and must be connected directly to the fabric edge switch.

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.html

Community vote distribution
A (100%)

arminio89 Highly Voted 2 years, 3 months ago
A is correct:
"A fabric AP is a local mode AP and needs to be directly connected to the fabric edge switch "
https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf
upvoted 10 times

Feliphus 12 months ago
Only to add more exam info, the B would be correct if it asked the WLC, ISE, DNA Center who are connected to the fabric border node
upvoted 4 times

LeGrosMatou Highly Voted 2 years, 6 months ago
A sounds correct :

"The fabric-mode APs are Cisco Wi-Fi 6 (802.11ax) and 802.11ac Wave 2 APs associated with the fabric WLC that have been configured with one or more fabric-enabled SSIDs. Fabric-mode APs continue to support the same wireless media services that traditional APs support such as applying AVC, quality of service (QoS), and other wireless policies. Fabric APs establish a CAPWAP control plane tunnel to the fabric WLC and join as local-mode APs. They must be directly connected to the fabric edge node or extended node switch in the fabric site. For their data plane, Fabric APs establish a VXLAN tunnel to their first-hop fabric edge switch where wireless client traffic is terminated and placed on the wired network. "

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html
upvoted 5 times

techriese Most Recent 5 months ago
Selected Answer: A
A is correct
upvoted 1 times

eww_cybr 5 months ago
Access points must be deployed as follows:
• Be directly connected to the fabric edge (or to an extended node switch)
• Be part of the fabric overlay
• Belong to the INFRA_VN, which is mapped to the global routing table
• Join the WLC in Local mode
upvoted 2 times

cloud29 1 year, 1 month ago
Selected Answer: A
A is correct
upvoted 1 times

Wooker 1 year, 2 months ago
Selected Answer: A
Local mode
upvoted 1 times

Aldebeer 1 year, 7 months ago
connect the EID's, right?
upvoted 1 times

ArchBishop 1 year, 10 months ago
At this time, FlexConnect is NOT supported in SD-Access.

upvoted 2 times

Nhan 2 years, 1 month ago

A is correct answer

upvoted 1 times

examShark 2 years, 6 months ago

D is correct, local mode is for SOHO deployments.

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct.
(D is not correct)

upvoted 6 times

timtgh 1 year, 6 months ago

Local mode is for all Fabric APs.

upvoted 1 times

Question #40 *Topic 1*

A customer requests a network design that supports these requirements:

☞ FHRP redundancy

☞ multivendor router environment

☞ IPv4 and IPv6 hosts

Which protocol does the design include?

A. VRRP version 2

B. VRRP version 3

C. GLBP

D. HSRP version 2

Correct Answer: *B*

Community vote distribution

B (100%)

Jheax Highly Voted 1 year, 8 months ago

Selected Answer: B

HSRP and GLBP are Cisco propietary, so they won't work in a multivendor setup. VRRPv3 us multivendor and supports IPv4 and 6.

upvoted 10 times

rpidcock Highly Voted 2 years, 3 months ago

B is the correct answer because it supports IPv4 and IPv6
VRRPv3: Supports IPv4 and IPv6
Chapter 15 IP Services Pg. 409

upvoted 6 times

techriese Most Recent 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

cloud29 9 months, 2 weeks ago

VRRP version 3 is the answer.

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: B

cisco(config)#fhrp version vrrp ?
v2 Legacy VRRP - VRRPv2 for IPv4
v3 Unified VRRP - VRRPv3 for IPv4 and IPv6

cisco(config)#fhrp version vrrp

upvoted 3 times

Pudu_vlad 1 year, 6 months ago

VRRPv3

upvoted 1 times

ayodejiadeyemi 1 year, 6 months ago

the provided answer is correct.

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: B

voting. provided answer is correct.

upvoted 1 times

Tahi 2 years, 2 months ago

It is correct

upvoted 3 times

Question #41 *Topic 1*

While configuring an IOS router for HSRP with a virtual IP of 10.1.1.1, an engineer sees this log message.
Jan 1 12:12:12.111 : %HSRP-4-DIFFVIP1: GigabitEthernet0/0 Grp 1 active routers virtual IP address 10.1.1.1 is different to the locally configured address 10.1.1.25
Which configuration change must the engineer make?

A. Change the HSRP group configuration on the local router to 1.

B. Change the HSRP virtual address on the local router to 10.1.1.1.

C. Change the HSRP virtual address on the remote router to 10.1.1.1.

D. Change the HSRP group configuration on the remote router to 1.

Correct Answer: *B*

Community vote distribution

B (100%)

XalaGyan Highly Voted 1 year, 12 months ago

Selected Answer: B

Gentlemen, i strongly agree with Goathammer and Amansoor. Here is my thinking to the topic. since we are configuring a NEW member of HSRP> I ASSUME !!!! that router 1 is the active and already in the network forwarding traffic.

if i changed the remote ip address to my newly configured 10.1.1.25 then i run the danger of disrupting network forwarding even for a short time.

to not cause any CHANGE to the state of the existing network i would opt to change the NEWLY Configured router 10.1.1.25 to the already running one of 10.1.1.1

long story short the message says that members of the group do not agree on the same virtual ip.

so it is up to you to change the running router(s) to the new config risking a short downtime due to Role Selection OR to be on the safe side, just change the NEWLY added router to match the existing setup.

i hope my explanations or the way i thought about the problem makes sense.

thanks all

upvoted 7 times

MasterMatt 1 year, 2 months ago

Eliminating the fact that there is no option to configure the remote node with HSRP virtual IP of 10.1.1.25. You always need to pay attention to where its active as XalaGyan mentioned.

upvoted 1 times

Goathammer Highly Voted 2 years ago

Selected Answer: B

Syslog points to local router having VIP ip 10.1.1.25, and remote router in g0/0 interface having 10.1.1.1. We want latter to all routers in HSRP so we need to configure local router, hence B.
"is different to the locally configured..."

upvoted 5 times

JochenStacker Most Recent 3 months, 3 weeks ago

The question makes zero sense, analyzing the log message notwithstanding
An network engineer configures the router with 10.1.1.1 and now has to change the router he is *currently configuring with 10.1.1.1 to 10.1.1.1*
Unless the engineer made a typo and typed .25 when he meant to type .1
Unless he watches the terminal of the other router as he configures the new router, but that STILL doesn't make sense.
This is the typical rotten, dirty, low-down, sneaky question I have come to expect of Cisco, instead of asking clear-cut questions, they leave everything open to 2-3 different interpretations. If a customer gave me this info I would tell him to go away and come back when he has more than just confusing nonsense as info.

upvoted 1 times

danman32 4 months, 1 week ago

What confused me was that the syslog said the remote router's VIP was 10.1.1.1 while the local router's VIP was 10.1.1.25. But how could the local VIP be 10.1.1.25 if it says the engineer configured it for 10.1.1.1?
Then figured WHILE the engineer was configuring. Perhaps he intended to make it 10.1.1.1 but made a typo in the process.

upvoted 1 times

techriese 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

[Removed] 5 months ago

Selected Answer: B

B is the best answer.

You could make an argument for C, but as an engineer, you should avoid disrupting operations as much as possible. If you follow through with C, there will have to be a reconvergence and disrupt forwarding until HSRP goes through its states.
Moreover! and probably a good possibility, the DHCP servers for endpoints more than likely are already configured with the Active Router's virtual IP as the default gateway when assigning addresses within the subnet, and changing that will prevent endpoints from communicating outside their domain.

upvoted 1 times

Rose66 10 months, 4 weeks ago

Selected Answer: B

Definitly B

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

youtri 2 years ago

the ip just ip (10.1.1.25) is diferrent to te Virtual Ip (10.1.1.1),should to change it to the VIp

upvoted 1 times

Amansoor79 2 years ago

I tested it on Packet tracer,
configure HSRP group first with VIP 10.1.1.25. And then try to configure a new VIP 10.1.1.1. You will get the exact same syslog message.
To stop that error you have to make the same change (Configuring new VIP in the remote router 10.1.1.1)

upvoted 3 times

Amansoor79 2 years ago

So the correct answer is C

upvoted 2 times

error_909 2 years, 2 months ago

Tested in GNS3 and correct.

upvoted 4 times

Question #42 *Topic 1*

A network administrator has designed a network with two multilayer switches on the distribution layer, which act as default gateways for the end hosts. Which two technologies allow every end host in a VLAN to use both gateways? (Choose two.)

A. VRRP

B. GLBP

C. VSS

D. MHSRP

E. HSRP

Correct Answer: *BD*

Community vote distribution

BC (58%) BD (38%) 2%

TTTTTT Highly Voted 2 years, 3 months ago

GLBP and MHSRP ------Correct

upvoted 33 times

mhizha 7 months, 3 weeks ago

I agree with your 2 answers. People need to understand that VSS is NOT classified as a FHRP

upvoted 7 times

Matt2727 5 months, 3 weeks ago

The question is asking which 'technology' allows 'every' end host. Its not asking about a specific protocol. B & C make the most sense since 'every' end host can use both gateways. MHSRP requires a splitting of end hosts to use 1 particular gateway and is configured with 2 groups on the active standby routers.

upvoted 5 times

laterst Highly Voted 1 year, 8 months ago

Selected Answer: BC

I'm going for B and C.
VRRP - and HSRP suffer from that fact that they both have one primary/master router which provides the _single_ default gateway (single VIP, single virtual MAC)
MHSRP provides two Virtual IPs, so end hosts would have to be configured with two default gateways - not common for end hosts. The same concept would apply to multiple VRRP groups.
GLBP provides one virtual IP and multiple virtual MAC Addresses; the ARP replies from the Active Virtual Gateway to the hosts will use all the virtual MACs (one for each virtual forwarder) in round robin fashion, so B is correct.
which leaves VSS, where both ML Switches form a single virtual switch and no FHRP is required at all to use them both.

upvoted 25 times

post20 Most Recent 2 days, 11 hours ago

B and C

upvoted 1 times

IgorLVG 1 week ago

A & B are the answers. GLBP can serve the traffic of the same vlan (load balance) and VRRP does the same too. VSS would be a good answer but the devbice would need to connect to both switches via echannel

upvoted 2 times

wamendoza 1 week, 1 day ago

After reviewing carefully, i see this in the question:
"A network administrator has designed a network with two multilayer switches on the distribution layer,"

This it makes me think that he is talking about two separate switches (sw 1 & sw 2)... This is the problem, VSS cannot be a options because is a physical switch that see how one, so I would rule out this option...

upvoted 2 times

Klimy 2 weeks, 5 days ago

Selected Answer: BC

VSS makes more sense than "MHSRP". MHSRP is just an administrative load balancing, so "in a VLAN" PCs wouldn's use both gateways. As D is incorrect and you still have to X something, i would go with VSS. This question is faulty.

upvoted 1 times

Brandonkiaora 3 weeks, 2 days ago

The answer should be BC.
GLBP, VSS, and MHSRP are all amazing protocols that allow load balance and redundancy. But this question asks the host in the same VLAN to use

both gateways, so you must dig deeper into MHSRP.

MHSRP is simply a combination of two HSRP protocols at the same time, configuring two routers with two HSRP sessions, enabling two virtual IPs representing R1 and R2 as active routers separately.

So any host can only choose one default gateway at a time, like host A on R1 chooses R1, and host B on R2 chooses R2; it's globally loadbalance and redundant, but host A can't use both gateways at the same time, it's just simple HSRP in a local view.

upvoted 1 times

Hamo1 3 months ago

I think B & E,
check this link please
https://search.cisco.com/search?query=Cisco%20Nexus%209000%20Series%20Switches%20:%20HSRP%20Load%20Sharing&locale=enUS&bizcontext=&cat=DeepQA&mode=text&clktyp=click&autosuggest=true&istadisplayed=false&tareqid=&categoryvalue=Cisco%20Nexus%209000%20Series%20Switches

upvoted 1 times

Soggyt74 4 months ago

Selected Answer: BC

GLBP and VSS both support allowing all hosts to use both pathways. MHSRP ties hosts to a single pathway, and will only use the other pathway in failover.

upvoted 2 times

teikitiz 4 months, 2 weeks ago

Selected Answer: BC

I don't think "allow every end host in a VLAN to use both gateways" can be met with MHSRP. True, VSS isn't a FHRP but can't agree with MHSRP as a solution that meets the above criteria

upvoted 3 times

JesssRoney 4 months, 2 weeks ago

I would go BC

upvoted 2 times

rogue_user 4 months, 3 weeks ago

Selected Answer: BD

GLBP and MHSRP both support load balancing. VSS is not FHRP.

upvoted 2 times

Burik 5 months, 3 weeks ago

Selected Answer: BC

It's obviously B and C. It's asking which two TECHNOLOGIES allow to use BOTH gateways, it's not asking which redundancy PROTOCOLS you could use.

GLBP will provide load balancing at Layer 3, VSS will provide load balancing at Layer 2. Therefore meeting the design request.

As mentioned in the question, this is a design question, and no designer in his right mind would use MHSRP if VSS and GLBP are an option.

The other FHRP answers are there just to confuse you.

upvoted 2 times

msstanick 5 months, 3 weeks ago

Selected Answer: BD

It is B & D. 31 days before CCNP exam page 194: "HSRP does not support load sharing as part of the protocol specification. However, load sharing can be achieved through the configuration of MHSRP". I "love" Cisco - their official CERT guide says nothing about that solution so you basically need to buy another book...

upvoted 4 times

goomisch 6 months, 2 weeks ago

C also correct but not all switches. GLBP and MHSRP are correct to all Cisco switches.

upvoted 1 times

Blue_Water 7 months, 1 week ago

Selected Answer: BD

GLBP and MHSRP

upvoted 3 times

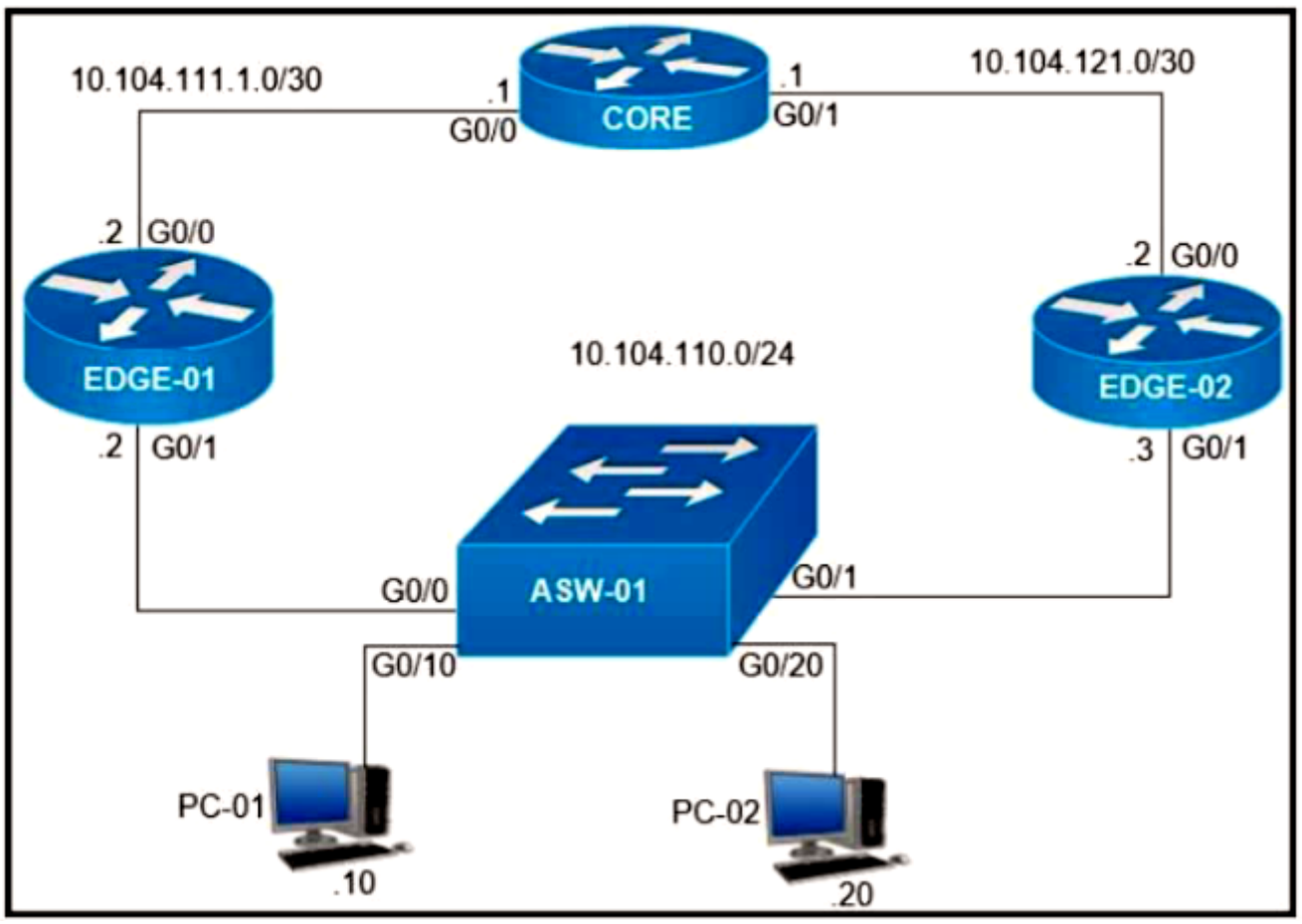
Chiaretta 7 months, 2 weeks ago

Selected Answer: BD

The core question is "use the two distribution switch simultaneously" B and D are correct

upvoted 2 times

Question #43 *Topic 1*



Refer to the exhibit. On which interfaces should VRRP commands be applied to provide first hop redundancy to PC-01 and PC-02?

A. G0/0 and G0/1 on Core

B. G0/0 on Edge-01 and G0/0 on Edge-02

C. G0/1 on Edge-01 and G0/1 on Edge-02

D. G0/0 and G0/1 on ASW-01

Correct Answer: *C*

Community vote distribution

C (100%)

TTTTTT Highly Voted 2 years, 3 months ago

correct ans provided

upvoted 5 times

techriese Most Recent 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

rami_mma 8 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

errepe_ 8 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

Latdiorice 9 months ago

That is the correct answer. The subnet range is what they have in common

upvoted 1 times

Rose66 10 months, 4 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

Parot 1 year, 1 month ago

Correct answer is C

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

correct ans provided

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: C

Correct as the FRRP protocol should be configured on interfaces that have the end nodes network.

upvoted 4 times

Violator 1 year, 9 months ago

This question is still asked. Passed today.

upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct.

upvoted 1 times

pierresadou 1 year, 9 months ago

C is correct

upvoted 1 times

Tsewaman 1 year, 10 months ago

C is Correct

upvoted 1 times

Question #44 *Topic 1*

Under which network conditions is an outbound QoS policy that is applied on a router WAN interface most beneficial?

A. under traffic classification and marking conditions

B. under interface saturation conditions

C. under all network conditions

D. under network convergence conditions

Correct Answer: *A*

Community vote distribution

B (94%) 4%

XalaGyan Highly Voted 1 year, 12 months ago

Selected Answer: B

Hi gents,
here my thinking to this topic

A. under traffic classification and marking conditions --> this is not a condition but rather an action and therefore WRONG

B. under interface saturation conditions
Saturation is a condition and NOT BAD

C. under all network conditions
well if this was the case, then the vendor Cisco would have made this a default state and thats it. also WRONG

D. under network convergence conditions
Well the wording is very vague here. a service policy can assign utmost priority to system level tasks that help in convergence, for example try putting OSPF protocol into CS6 or EF marking and implement a Priority Queueing (PQ) then you have made convergence faster but starved out everything else.
Also NOT BAD but why would any clear thinking admin interfere with system level priorities?

as far as i can see, there is only answer B which is NOT BAD answer for a question worded like that.

Answer B

upvoted 30 times

uhljeb 7 months, 3 weeks ago

This question structure is kind of lame. I agree with your reasoning and answer elaboration.

upvoted 1 times

velozkenneth Highly Voted 2 years, 3 months ago

B is correct!

upvoted 15 times

Haidary Most Recent 1 month ago

B is correct answer

upvoted 1 times

orenoren 1 month, 3 weeks ago

b is correct

upvoted 1 times

ermanzan 5 months, 2 weeks ago

I think B is correct for me!!!

upvoted 1 times

wr4net 6 months, 1 week ago

another stupidly phrased question. if the answer is really A, i think the question needs to be phrased like this: under which conditions will an outbound QoS policy be most beneficial. given this, it would be most beneficial if traffic was marked and classified first. If it wasnt marked or classified, then interface saturation would make no difference. But test makers are trying to craft words in a tricky way, resulting in B seeming like the best answer. I dunnow! dumb question. I hope I don't see this on the exam!

upvoted 2 times

Blue_Water 7 months, 1 week ago

Selected Answer: B

The congestion condition

upvoted 1 times

ruiolegario 9 months ago

Selected Answer: B

MY SELECT CORRECT. SORRY

upvoted 1 times

ruiolegario 9 months ago

Selected Answer: C

RUI OLEGARIO DE SIQUEIRA - VOT IS C

upvoted 1 times

cerf 9 months, 3 weeks ago

B is correct!

upvoted 1 times

Specialdork 11 months ago

Selected Answer: B

I agree with B.

upvoted 2 times

Parot 1 year, 1 month ago

Answer is B

upvoted 1 times

Wooker 1 year, 2 months ago

Selected Answer: B

The answer is B

upvoted 1 times

BigMouthDog 1 year, 5 months ago

does not matter in which condition, traffic classification and marking are done via configuration of the router. But it is obvious under the congestion condition that QoS policy would be most beneficial

upvoted 2 times

DiscardedPacket 1 year, 5 months ago

Selected Answer: B

Marking is done at the edge, QOS performs no useful functions other than marking unless there is congestion.

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

B is Correct

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: B

The answer must be: under interface saturation conditions

upvoted 2 times

Question #45 *Topic 1*

An engineer must configure HSRP group 300 on a Cisco IOS router. When the router is functional, it must be the active HSRP router. The peer router has been configured using the default priority value. Which command set is required?

A. standby version 2 standby 300 priority 110 standby 300 preempt

B. standby 300 priority 110 standby 300 timers 1 110

C. standby version 2 standby 300 priority 90 standby 300 preempt

D. standby 300 priority 90 standby 300 preempt

Correct Answer: *A*

Community vote distribution

A (86%) 14%

error_909 Highly Voted 2 years, 2 months ago

HSRP v1 allow only 265 group numbers.
HSRP v2 allow 4096 group number
upvoted 17 times

youtri 2 years ago

v1 256 groups (0-255)
upvoted 7 times

KZM Highly Voted 1 year, 2 months ago

In HSRP version 1, group numbers are supported the range from 0 to 255 and HSRP version 2 expands the group number range from 0 to 4095.
* So it should HSRP v2 to assign the group no. 300 (So. the ans should A or C).
* Default priority of the HSRP is 100 and the Router with higher priority no. will become Active Router. So the priority set over 100 for active router.

So, the answer is "A".
upvoted 11 times

Haidary Most Recent 1 month ago

A is correct
upvoted 1 times

CCNPWILL 3 months, 3 weeks ago

Correct answer is indeed A.
upvoted 1 times

anaz691011 3 months, 4 weeks ago

Default priority value is 100 so if we make priority from 101 they router will act as primary router to forward the traffic
upvoted 1 times

techriese 5 months ago

Selected Answer: A

A is correct
upvoted 2 times

NIL8891 5 months, 2 weeks ago

Answer A
standby version 2
standby 300 priority 110
standby 300 preempt
upvoted 5 times

ibogovic 6 months, 3 weeks ago

Selected Answer: B

B. standby 300 priority 110 standby 300 timers 1 110

Explanation:

The "standby 300 priority 110" command sets the priority of the router to 110, making it higher than the default priority of the peer router.
The "standby 300 timers 1 110" command sets the hello timer to 1 second and the hold timer to 110 seconds for HSRP group 300.
upvoted 1 times

toppystar2003 6 months ago

preempt is what allows it to take over once it has a higher priority than the already active hsrp router.

upvoted 1 times

nushadu 11 months, 2 weeks ago

cisco(config)#interface e0/2.22
cisco(config-subif)#standby ?
<0-255> group number
...
cisco(config-subif)#standby version 2
cisco(config-subif)#standby ?
<0-4095> group number

upvoted 2 times

snowblack 11 months, 3 weeks ago

A. The configuration bellow:
standby version 2
standby 300 priority 110
standby 300 preempt

upvoted 2 times

TenaciousGamer98 1 year, 5 months ago

'preempt' is only needed on the higher HSRP priority router as the lowest HSRP priority router will only take over when the higher HSRP priority router is not available hence no need to preempt an existing HSRP router.

The higher priority HSRP router will need to preempt the current HSRP router which has the lesser HSRP priority value.

upvoted 3 times

Pudu_vlad 1 year, 6 months ago

A is correct

upvoted 1 times

Ondskan 1 year, 6 months ago

Question is tricky as there are multiple commands on the same row. Answer is correct

upvoted 1 times

KeepUpE 1 year, 6 months ago

Want to mention that two of the answers are similar, one with a priority value of 110 and the other with a value of 90. By default, the priority value is 100; to make this one active (as per the intent of the question), this router must have a higher priority value than its peer (which is using the default of 100).

upvoted 3 times

Aldebeer 1 year, 8 months ago

Selected Answer: A

Group (instance) number 255 (max) is exceeded, thus, Device(config-if)# standby version 2

upvoted 3 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct.

upvoted 1 times

certtaker202 2 years, 3 months ago

Answer is correct.

upvoted 2 times

Question #46 *Topic 1*

What is the function of a fabric border node in a Cisco SD-Access environment?

A. To collect traffic flow information toward external networks.

B. To connect the Cisco SD-Access fabric to another fabric or external Layer 3 networks.

C. To attach and register clients to the fabric.

D. To handle an ordered list of IP addresses and locations for endpoints in the fabric.

Correct Answer: *B*

Community vote distribution

B (100%)

rpidcock Highly Voted 2 years, 3 months ago

B is the correct answer.
Border bode: The border nodes serve as the gateways between the Cisco SD-Access fabric and external networks.
upvoted 9 times

techriese Most Recent 5 months ago

Selected Answer: B

B is correct
upvoted 1 times

Asymptote 1 year ago

Selected Answer: B

Border Node is an Entry & Exit point for data traffic going Into & Out of a Fabric

Referenced:
https://www.cisco.com/c/dam/m/hr_hr/training-events/2019/cisco-connect/pdf/VH-Cisco-SD-Access-Connecting.pdf
upvoted 1 times

Dataset 1 year, 2 months ago

B is correct
upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: B

voting. provided answer is correct.
upvoted 3 times

Question #47 *Topic 1*

In a wireless Cisco SD-Access deployment, which roaming method is used when a user moves from one AP to another on a different access switch using a single
WLC?

A. Layer 3

B. inter-xTR

C. auto anchor

D. fast roam

Correct Answer: *D*

Community vote distribution

B (73%) D (27%)

Ratul0408 Highly Voted 2 years, 3 months ago

Answer is B:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html

upvoted 28 times

error_909 2 years, 2 months ago

Correct answer is B

upvoted 4 times

Eng_H Most Recent 3 months, 2 weeks ago

The answer is D. Fast Roam.

In a wireless Cisco SD-Access deployment, Fast Roam is the preferred method for seamless roaming between access points on the same fabric. It uses a pre-authentication and pre-association process to allow the client device to establish a connection to the new access point before it physically moves to the new location. This minimizes the amount of time the client device is disconnected from the network.

Inter-xTR roaming is used in a Cisco SD-Access deployment where the user is moving between different virtual networks. Auto anchor roaming is used in a multi-WLC deployment where the user is moving between different physical locations.

Layer 3 roaming is not used in a wireless Cisco SD-Access deployment. It is a method of roaming that uses Layer 3 routing to move a client device from one access point to another. However, in a Cisco SD-Access deployment, all access points are part of the same fabric and are interconnected using Layer 2. Therefore, there is no need to use Layer 3 routing for roaming.

upvoted 3 times

khaganiabbasov 3 months, 3 weeks ago

roaming :

inter-xTR = different switch
intra-xTR = same switch

upvoted 1 times

techriese 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

msstanick 5 months, 3 weeks ago

Selected Answer: B

Has to be B as it is almost like word by word in line with Cisco's definition as below .

"SDA supports two additional types of roaming, which are Intra-xTR and Inter-xTR. In SDA, xTR stands for an access-switch that is a fabric edge node. It serves both as an ingress tunnel router as well as an egress tunnel router.

When a client on a fabric enabled WLAN, roams from an access point to another access point on the same access-switch, it is called Intra-xTR. Here, the local client database and client history table are updated with the information of the newly associated access point.

When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter-xTR. Here, the map server is also updated with the client location (RLOC) information. Also, the local client database is updated with the information of the newly associated access point."

upvoted 4 times

Burik 5 months, 3 weeks ago

Selected Answer: B

"When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter-xTR."

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html
upvoted 1 times

jordigisbert 6 months ago

Selected Answer: D

D. is the same wlc.
upvoted 2 times

ibogovic 6 months, 3 weeks ago

Selected Answer: D

D. fast roam

Fast roam, also known as Fast Secure Roaming (FSR) or Fast Transition, is a mechanism that allows a wireless client to quickly and securely roam between APs without experiencing significant disruption or reauthentication delays. It enables seamless mobility for the client by minimizing the interruption during the handoff process.
upvoted 2 times

Burik 5 months, 3 weeks ago

No. We're in SD-Access context here, the method is Inter-XTR.
upvoted 2 times

mrtattoo 6 months, 4 weeks ago

Selected Answer: D

In a wireless Cisco SD-Access deployment, when a user moves from one AP to another on a different access switch using a single WLC, the roaming method used is "Fast Roam" or "802.11r Fast Transition."

Fast Roaming enables a client device to quickly and seamlessly roam from one AP to another on the same network without requiring the client to reauthenticate or reassociate with the new AP. This feature improves the quality of real-time applications such as voice and video by reducing the amount of time required to re-establish a wireless connection after a roam.

The other options mentioned, Layer 3 Roaming, Inter-xTR Roaming, and Auto Anchor Roaming are typically used in different wireless deployment scenarios and are not specific to Cisco SD-Access.
upvoted 1 times

HarwinderSekhon 7 months ago

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html

SDA Roaming
SDA supports two additional types of roaming, which are Intra-xTR and Inter-xTR. In SDA, xTR stands for an access-switch that is a fabric edge node. It serves both as an ingress tunnel router as well as an egress tunnel router.

When a client on a fabric enabled WLAN, roams from an access point to another access point on the same access-switch, it is called Intra-xTR. Here, the local client database and client history table are updated with the information of the newly associated access point.

When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter-xTR. Here, the map server is also updated with the client location (RLOC) information. Also, the local client database is updated with the information of the newly associated access point.
upvoted 1 times

mikhailov_ivan90 10 months, 2 weeks ago

Selected Answer: D

In my oppinion the correct answer is D due to only one simple reason - there isn't any infor about Inter-xTR in the official ENCOR book and they can't ask you about anything that isn't in the book\course from the legal point of view. So in real life the answer is B, for the cisco exam- D
upvoted 2 times

Splashisthegreatestmovie 5 months, 2 weeks ago

Hey friend, I have been taking cisco exams for 20 years and they are the most unfair, ridiculous, and bullshit tests in the world. Just because it's not in the book doesn't mean that it's not on the test.
upvoted 2 times

x3rox 9 months, 4 weeks ago

99% of the questions are not in the OCG. That's why here we share documents from outside. Like Design Guides from Cisco.com ¯_(ツ)_/¯
upvoted 3 times

endy023 10 months, 3 weeks ago

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html
upvoted 2 times

M_B 10 months, 3 weeks ago

B
When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter-xTR. Here, the map server is also updated with the client location (RLOC) information. Also, the local client database is updated with the information of the newly associated access point.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html
upvoted 1 times

Faridtnx 11 months ago

Selected Answer: B

Inter-xTR
upvoted 1 times

Specialdork 11 months ago

Selected Answer: B

The Answer is B
upvoted 1 times

kewokil120 11 months ago

Selected Answer: B

Answer is B:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html
upvoted 1 times

Abbribas 11 months, 1 week ago

SDA supports two additional types of roaming, which are Intra-xTR and Inter-xTR. In SDA, xTR stands for an access-switch that is a fabric edge node. It serves both as an ingress tunnel router as well as an egress tunnel router.
When a client on a fabric enabled WLAN, roams from an access point to another access point on the same access-switch, it is called Intra-xTR. So, option B is correct.
upvoted 1 times

Backward_CEE 5 months, 3 weeks ago

Option is Inter-xTR, not Intra
upvoted 1 times

Question #48 *Topic 1*

What is the recommended MTU size for a Cisco SD-Access Fabric?

A. 4464

B. 17914

C. 9100

D. 1500

Correct Answer: *C*

Community vote distribution

C (100%)

derpo Highly Voted 2 years, 3 months ago

Answer C is correct.

From cisco:
VXLAN adds 50 bytes to the original packet. The common denominator and recommended MTU value available on devices operating in a fabric role is 9100. Network should have a minimum starting MTU of at least 1550 bytes to support the fabric overlay. MTU values between 1550 and 9100 are supported along with MTU values larger than 9100 though there may be additional configuration and limitations based on the original packet size.
MTU 9100 is provisioned as part of LAN Automation. Devices in the same routing domain and Layer 2 domain should be configured with a consistent MTU size to support routing protocol adjacencies and packet forwarding without fragmentation.

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

upvoted 11 times

ihateciscoreally Most Recent 4 months ago

thank you for not covering it in OCG! :)

upvoted 2 times

techriese 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

GreatDane 1 year, 6 months ago

Ref: Cisco SD-Access – Connecting Multiple Sites in a Single Fabric Domain

"Cisco SD Access Transit Types
…
Cisco SD Access Multi Site
Key Considerations
…
Should accommodate the MTU setting used for SD Access in the campus network (typically 9100 bytes).
…"

A. 4464

Wrong answer.

B. 17914

Wrong answer.

C. 9100

Correct answer.

D. 1500

Wrong answer.

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct.

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 2 times

Question #49 *Topic 1*

What is the function of the fabric control plane node in a Cisco SD-Access deployment?

A. It is responsible for policy application and network segmentation in the fabric.

B. It performs traffic encapsulation and security profiles enforcement in the fabric.

C. It holds a comprehensive database that tracks endpoints and networks in the fabric.

D. It provides integration with legacy nonfabric-enabled environments.

Correct Answer: *C*

Community vote distribution

C (100%)

gtddrf Highly Voted 2 years, 3 months ago

C.
The control plane node's database tracks all endpoints in the fabric site and associates the endpoints to fabric nodes, decoupling the endpoint IP address or MAC address from the location (closest router) in the network.
upvoted 7 times

TenaciousGamer98 Highly Voted 1 year, 5 months ago

And this DB is known as Host Tracking Database (HTDB) - holds EID to RLOC bindings
upvoted 6 times

techriese Most Recent 5 months ago

Selected Answer: C

C is correct
upvoted 1 times

Pudu_vlad 1 year, 6 months ago

C is Correct
upvoted 1 times

GreatDane 1 year, 6 months ago

Ref: Cisco SD Access - Connecting to the Data Center, Firewall, WAN and More!

"...
Cisco SD Access

Fabric Roles & Terminology
...
• Control-Plane Nodes – Map System that manages Endpoint to Device relationships
..."

A. It is responsible for policy application and network segmentation in the fabric.

Wrong answer.

B. It performs traffic encapsulation and security profiles enforcement in the fabric.

Wrong answer.

C. It holds a comprehensive database that tracks endpoints and networks in the fabric.

Correct answer.

D. It provides integration with legacy nonfabric-enabled environments.

Wrong answer.
upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: C

Fabric based on LISP Control Plane.
upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct.
upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 2 times

Question #50 *Topic 1*

What is the data policy in a Cisco SD-WAN deployment?

A. list of ordered statements that define node configurations and authentication used within the SD-WAN overlay

B. set of statements that defines how data is forwarded based on IP packet information and specific VPNs

C. detailed database mapping several kinds of addresses with their corresponding location

D. group of services tested to guarantee devices and links liveliness within the SD-WAN overlay

Correct Answer: *B*

Community vote distribution

B (100%)

techriese 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

GreatDane 1 year, 6 months ago

Ref: Policies Configuration Guide for vEdge Routers, Cisco SD-WAN Releases 19.1, 19.2, and 19.3

"C H A P T E R 2
Policy Basics
...
Policy Overview

Policy influences the flow of data traffic and routing information among Cisco vEdge devices in the overlay network. Policy comprises:
...
• Data policy—which affects the flow of data traffic in the network's data plane
..."

A. list of ordered statements that define node configurations and authentication used within the SD-WAN overlay

Wrong answer.

B. set of statements that defines how data is forwarded based on IP packet information and specific VPNs

Correct answer.

C. detailed database mapping several kinds of addresses with their corresponding location

Wrong answer.

D. group of services tested to guarantee devices and links liveliness within the SD-WAN overlay

Wrong answer.

upvoted 2 times

DLLLLLLLL 1 year, 6 months ago

Selected Answer: B

The Cisco SD-WAN architecture implements two types of data policy:

Centralized data policy controls the flow of data traffic based on the source and destination addresses and ports and DSCP fields in the packet's IP header (referred to as a 5-tuple), and based on network segmentation and VPN membership. These types of data policy are provisioned centrally, on the Cisco vSmart controller, and they affect traffic flow across the entire network.

Localized data policy controls the flow of data traffic into and out of interfaces and interface queues on a Cisco vEdge device. This type of data policy is provisioned locally using access lists. It allows you to classify traffic and map different classes to different queues. It also allows you to mirror traffic and to police the rate at which data traffic is transmitted and received.

upvoted 4 times

Aldebeer 1 year, 7 months ago

Selected Answer: B

it is B

upvoted 1 times

brightsyds 1 year, 9 months ago

B!

It is definitely a forwarding policy

upvoted 1 times

XalaGyan 1 year, 12 months ago

Selected Answer: B

hi folks,
here is my opinion this matter.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/data-policies.html

"Data policy can be applied to data traffic based on the packet header fields, such as the prefix, port, protocol, and DSCP value, and they can also be applied based on the VPN in the overlay network to which the traffic flows."

Answer: B

upvoted 4 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

rpidcock 2 years, 3 months ago

B is the correct answer.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html

upvoted 1 times

Question #51 *Topic 1*

In Cisco SD-WAN, which protocol is used to measure link quality?

A. IPsec

B. OMP

C. RSVP

D. BFD

Correct Answer: *D*

Community vote distribution

D (100%)

error_909 Highly Voted 2 years, 2 months ago

The BFD (Bidirectional Forwarding Detection) is a protocol that detects link failures as part of the Cisco SD-WAN (Viptela) high availability solution, is enabled by default on all vEdge routers, and you cannot disable it.

upvoted 11 times

Dudu84 Most Recent 4 days, 2 hours ago

BFD is correct
Cisco Catalyst SD-WAN BFD
This type of BFD detects failures in the overlay tunnel and has the following haracteristics:
Is enabled by default and cannot be disabled. Is typically enabled for the Cisco Catalyst SD-WAN Overlay Management Protocol (OMP). Besides link failures, Cisco Catalyst SD-WAN BFD also measures latency, loss, jitter, and other link statistics used by application-aware routing. For more information on Cisco Catalyst SD-WAN BFD for measuring latency, loss, and jitter used by application-aware routing, see https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/application-aware-routing.html.

upvoted 1 times

poy4242 11 months, 1 week ago

Selected Answer: D

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_17.1/07Policy_Applications/01Application-Aware_Routing

The Viptela software uses BFD packets to continuously monitor the data traffic on the data plane tunnels between vEdge routers

Application-aware routing uses the BFD Hello packets to measure the loss, latency, and jitter on the links.

upvoted 3 times

jorgenn 1 year, 3 months ago

B is The Correct Answer

upvoted 1 times

jorgenn 1 year, 3 months ago

BFD....

upvoted 1 times

Pudu_vlad 1 year, 6 months ago

BFD is correct

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: D

BFD, monitor the link quality and detect failures.

upvoted 2 times

Aldebeer 1 year, 7 months ago

Selected Answer: D

BFD packets continuously monitor the data traffic, overlay.

upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: D

Voting. provided answer is correct.

upvoted 1 times

rpidcock 2 years, 3 months ago

D is the correct answer.
The following Cisco SD-WAN capabilities helps to address application performance optimization:

● Application-Aware Routing: Application-aware routing allows the ability to create customized SLA-policies for traffic and measures real-time performance taken by BFD probes

upvoted 2 times

Question #52 *Topic 1*

What is used to perform QoS packet classification?

A. the Type field in the Layer 2 frame

B. the Options field in the Layer 3 header

C. the TOS field in the Layer 3 header

D. the Flags field in the Layer 3 header

Correct Answer: *C*

Community vote distribution

C (100%)

youtri Highly Voted 2 years ago

when we talk about PACKET, means layer 3

upvoted 11 times

ciscolessons Highly Voted 1 year, 9 months ago

Selected Answer: C

TOS is L3, COS is L2.

upvoted 9 times

LanreDipeolu Most Recent 3 months, 4 weeks ago

Selected Answer: C

"C" is the correct answer: ToS is an eight bit field, comprising of 3-bit IP Precedence (IPP) used for marking and the rest bits unused. This filed has been redefined as 8-bits Differentiated Service (DiffServ) for both IPv4 and IPv6 class fields for backward compatible with IPP

upvoted 1 times

techriese 5 months ago

Selected Answer: C

C is correct

upvoted 2 times

Pudu_vlad 1 year, 6 months ago

C is correct

upvoted 2 times

danny_f 1 year, 7 months ago

Selected Answer: C

Agreed, DSCP is used for marking, within the TOS which is in the IP header

upvoted 4 times

Nhan 2 years, 1 month ago

Type of service

upvoted 2 times

Question #53 *Topic 1*

How do cloud deployments differ from on-premises deployments?

A. Cloud deployments require longer implementation times than on-premises deployments.

B. Cloud deployments are more customizable than on-premises deployments.

C. Cloud deployments have lower upfront costs than on-premises deployments.

D. Cloud deployments require less frequent upgrades than on-premises deployments.

Correct Answer: *C*

Community vote distribution

C (100%)

IgorLVG 2 months ago

teh best is C, the cloud is more accesible if the time is lower than 3 years. if you requere on-premise, you will need to have a medium/high budget

upvoted 1 times

Sid40 4 months ago

b is correct

upvoted 1 times

techriese 5 months ago

Selected Answer: C

C is correct

upvoted 2 times

Pudu_vlad 1 year, 6 months ago

Correct C

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct

upvoted 1 times

Lar20 2 years, 1 month ago

Correct C

upvoted 1 times

Question #54 *Topic 1*

Which controller is capable of acting as a STUN server during the onboarding process of Edge devices?

A. vBond

B. vSmart

C. vManage

D. PNP Server

Correct Answer: *A*

Community vote distribution

A (100%)

error_909 Highly Voted 2 years, 2 months ago

vBond plays a crucial role and acts as a Session Traversal Utilities for NAT (STUN) server, which allows other controllers and SD-WAN routers to discover their own mapped/translated IP addresses and port numbers. SD-WAN devices advertise this information along with their TLOCs so other SD-WAN devices have information in order to make successful connections.

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

upvoted 16 times

KZM Most Recent 1 month, 3 weeks ago

Selected Answer: A

The SD-WAN Validator (Former name vBond) plays a crucial role and acts as a Session Traversal Utilities for NAT (STUN) server, which allows other control components and SD-WAN routers to discover their own mapped/translated IP addresses and port numbers.

upvoted 1 times

ihateciscoreally 3 months ago

i dont know what STUN is, but when i see "onboarding" i click vBond.

upvoted 3 times

Vlad_Is_Love_ua 9 months, 2 weeks ago

Selected Answer: A

Cisco vBond plays a crucial role and acts as a Session Traversal Utilities for NAT (STUN) server, which allows other controllers and Cisco SD-WAN routers to discover their own mapped and translated IP addresses and port numbers. Cisco SD-WAN devices advertise this information along with their TLOCs, so other Cisco SD-WAN devices have information to make successful connections.

upvoted 1 times

danny_f 1 year, 7 months ago

Selected Answer: A

The Cisco SD-WAN solution is comprised of separate orchestration, management, control and data plane.
• Orchestration plane assists in securely onboarding the SD-WAN WAN Edge routers into the SD-WAN overlay. The vBond controller, or orchestrator, authenticates and authorizes the SD-WAN components onto the network. The vBond orchestrator takes an added responsibility to distribute the list of vSmart and vManage controller information to the WAN Edge routers.

upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct

upvoted 1 times

Question #55 *Topic 1*

How is 802.11 traffic handled in a fabric-enabled SSID?

A. centrally switched back to WLC where the user traffic is mapped to a VXLAN on the WLC

B. converted by the AP into 802.3 and encapsulated into VXLAN

C. centrally switched back to WLC where the user traffic is mapped to a VLAN on the WLC

D. converted by the AP into 802.3 and encapsulated into a VLAN

Correct Answer: *B*

Community vote distribution

B (100%)

Nathan_ 4 months, 1 week ago

the AP converts 802.11 traffic to 802.3 and encapsulates it into VXLAN, encoding the VNI and SGT information of the client.
https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf
upvoted 2 times

techriese 5 months ago

Selected Answer: B

B is correct
upvoted 1 times

timtgh 1 year, 6 months ago

https://community.cisco.com/t5/software-defined-access-sd/sd-access-ssid-vs-non-fabric-ssid/td-p/3863542
upvoted 3 times

danny_f 1 year, 7 months ago

Selected Answer: B

B is the best answer but vauge and technically wrong. Shouldn't it be 802.3ab? 802.3 without ad is "10BASE5 10 Mbit/s (1.25 MB/s) over thick coax. Same as Ethernet II (above) except Type field is replaced by Length, and an 802.2 LLC header follows the 802.3 header. Based on the CSMA/CD Process."
upvoted 4 times

AlbertoStu 1 year, 7 months ago

B is almost word for word out of the Cisco documentation.
https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf
upvoted 5 times

[Removed] 1 year, 7 months ago

Selected Answer: B

Fabric AP communicates with fabric WLC using capwap for control plnae comms ony. To communicate with the SD-Access fabric, the AP will use vxlan encapsulation.
upvoted 3 times

Eddgar0 1 year, 7 months ago

Selected Answer: B

Correct encapsulated into vxlan to be forwarded locally by a switch in sdfabric.
upvoted 1 times

AlbertoStu 1 year, 8 months ago

Selected Answer: B

https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf

• For a fabric-enabled SSID, the AP converts 802.11 traffic to 802.3 and encapsulates it into VXLAN, encoding the VNI and SGT information of the client
upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: B

voting. provided answer is correct
upvoted 1 times

Nhan 2 years, 1 month ago

The given answer is correct 802.1 is WiFi 802.3 is Ethernet in the frabric the ap conver the wireless signal to Ethernet and send over the xvlan

upvoted 3 times

rpidcock 2 years, 3 months ago

B is correct answer.
For a fabric-enabled SSID, the AP converts 802.11 traffic to 802.3 and encapsulates it into VXLAN, encoding the VNI and SGT information of the client

upvoted 3 times

Refer to the exhibit.

R1	R2
key chain cisco 123 key 1 key-string Cisco123!	key chain cisco 123 key 1 key-string Cisco123!
Ethernet0/0 - Group 10 State is Active 8 state changes, last state change 00:02:49 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a Local virtual MAC address is 0000.0c07.ac0a (v1 default) Hello time 5 sec, hold time 15 sec Next hello sent in 2.880 secs Authentication MD5, key chain "cisco123" Preemption enabled Active router is local Standby router is unknown Priority 255 (configured 255) Group name is "workstation-group" (cfgd)	Ethernet0/0 - Group 10 State is Active 17 state changes, last state change 00:02:17 Virtual IF address is 192.165.0.1 Active virtual HAC address is 0000.0c07.ac0a Local virtual MAC address is 0000.0c07.ac0a (v1 default) Hello time 10 sec, hold time 30 sec Next hello sent in 6.720 secs Authentication MD5, key-chain "cisco123" Preemption disabled Active router is local Standby router is unknown Priority 200 (configured 200) Group name is "workstation-group" (cfgd)

An engineer is installing a new pair of routers in a redundant configuration. When checking on the standby status of each router, the engineer notices that the routers are not functioning as expected.
Which action will resolve the configuration error?

A. configure matching hold and delay timers

B. configure matching key-strings

C. configure matching priority values

D. configure unique virtual IP addresses

Correct Answer: *B*

Community vote distribution

D (59%) B (31%) 11%

Eddgar0 Highly Voted 1 year, 7 months ago

Selected Answer: D

The most situable for this question is D (configure unique virtual address) as is one of requirements for a group to work, as seeing in the image.
The others are wrong for the following reason. (so Wrong based in the question)
A) Not mandatory the timers must match to work on HSRP. on HSRP negotiation the active router will override the standby timers.
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.pdf
B) On the image key string match so is not this reason HSRP cant be seen each other
C) Wrong, priority is for selecing the active router, the best practice is should be different thus (WRONG)
D) Different virtual Gateway configured on the same group number indeed will make HSRP routers negotiation fail for that group thus (CORRECT)

upvoted 21 times

Eddgar0 1 year, 7 months ago

Correction of the link source
https://community.cisco.com/t5/switching/hsrp-timers/td-p/1760156

upvoted 6 times

iz_m6 Highly Voted 1 year, 6 months ago

There must be a typo in the possible answers as none of them are correct!
D says to configure unique IP - they are already unique, but for HSRP to function, the virtual IP needs to match

upvoted 14 times

pierresadou 1 year, 4 months ago

Where do get this unique IP?

upvoted 1 times

[Removed] 6 months, 1 week ago

R2 is 192.165.0.1.

upvoted 4 times

KZM Most Recent 1 month, 3 weeks ago

Selected Answer: D

Answer :D

As per the output result, R1 was configured as an Active Router due to the high priority number 255. Authentication will pass due to the same on both sides. Timer mismatch in both sites is not a problem in this case. Because the timer of the Active router is less than the Standby router's. I mean the active Router will send a Hello packet every 5 seconds and it is met with the Standby router timer.The main mismatch is the virtual IP address. The virtual IP address must be the same in both Routers' configuration.

upvoted 1 times

Hamo1 3 months ago

D is correct,
R1 VIP is 192.168.0.1
R2 VIP is 192.165.0.1
They have to match

upvoted 1 times

PureInertiaCopy 3 months, 2 weeks ago

Admin need to correct this as there is no correct answer.

The Virtual IPs MUST MATCH.

If you look at the exhibit, you will see that R1 and R2 have different VIPs.

upvoted 1 times

PPPx 3 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

danman32 4 months ago

In the exhibit, the VIPs do not match; second octet are different (168 vs 165)
Assuming that the two routers do have connectivity between them for the interfaces configured for hsrp, they both would have IPs in either 192.168.0.0/24 or 192.165.0.0/24
Latter not likely since 192.165.0.0 is not one of the reserved private IPs.
But hsrp configuration won't let you configure a VIP that doesn't match the interface subnet.
So it is really unlikely D is the situation on the actual exam even if the exam had it as MATCHING since on the exam, they would already be matching.

upvoted 2 times

flash007 4 months, 1 week ago

D the keys are the same in the exhibit

upvoted 1 times

lnm3r 4 months, 1 week ago

In some places this question has a reference photograph and I see that the Virual IP is the same on both sides

upvoted 1 times

[Removed] 4 months, 3 weeks ago

Selected Answer: D

The configuration is already got matching keys, the Virtual IP is not matching

upvoted 2 times

imbhebhi 4 months, 3 weeks ago

I also go with D, if they can ask this exact question on the exam, they should give it as correct or they must say choose 2

upvoted 1 times

techriese 5 months ago

Selected Answer: D

D is correct - key string is equal

upvoted 1 times

Burik 5 months, 3 weeks ago

Most likely there are two versions of this question in the actual exam, one with non-matching key-strings and one with non-matching virtual IP addresses. The question here is a mix of the two, it shows the exhibit of one version and the answers of the other one. So no correct answer exists in this case.

upvoted 2 times

Burik 5 months, 3 weeks ago

Hold up.. I didn't read the exhibit properly. It shows 192.168.0.1 and 192.165.0.1 so in this case the answer is D, as the two virtual IP addresses must match.

upvoted 1 times

Burik 5 months, 2 weeks ago

Again, scratch that. "Unique" as "different", which is wrong. It should say "matching". No answer is correct.

upvoted 1 times

Anis76 7 months, 3 weeks ago

Selected Answer: D
upvoted 1 times

paulosrsf 8 months, 2 weeks ago

Selected Answer: B

In the exam, this question has a difference in the key-strings of the routers. One is written with an uppercase C (Cisco123!) and the other one with a lowercase c (cisco123!).
So the option B makes more sense for the wright answer.

In the link below there's a printscreen of the real exam statement.
https://www.pass4success.com/cisco/discussions/exam-350-401-topic-4-question-34-discussion
upvoted 10 times

andrecmw 6 months ago

Paulo, in your printscreen, notice that virtual ip address are the same, so, the answer B makes sense. Please note that on THAT question, the keystrings are the same, while the virtual IP not. D is the right answer here is this question, while in your link with a different question, the answer B would be correct.
upvoted 2 times

net_eng10021 6 months ago

Spot on, andrecmw...glad I stumbled onto your post
upvoted 1 times

net_eng10021 6 months ago

Upon further inspection, I'm not convinced that D is correct as it mentions 'unique' IP address. Need matching or identical IP address as other have mentioned. Brings me back to mismatched timers. Unfortunately, I'm finding conflicting data on whether timers need to match or not.
upvoted 1 times

dragonwise 8 months, 3 weeks ago

I have simulated the exact scenario and I have found the following:

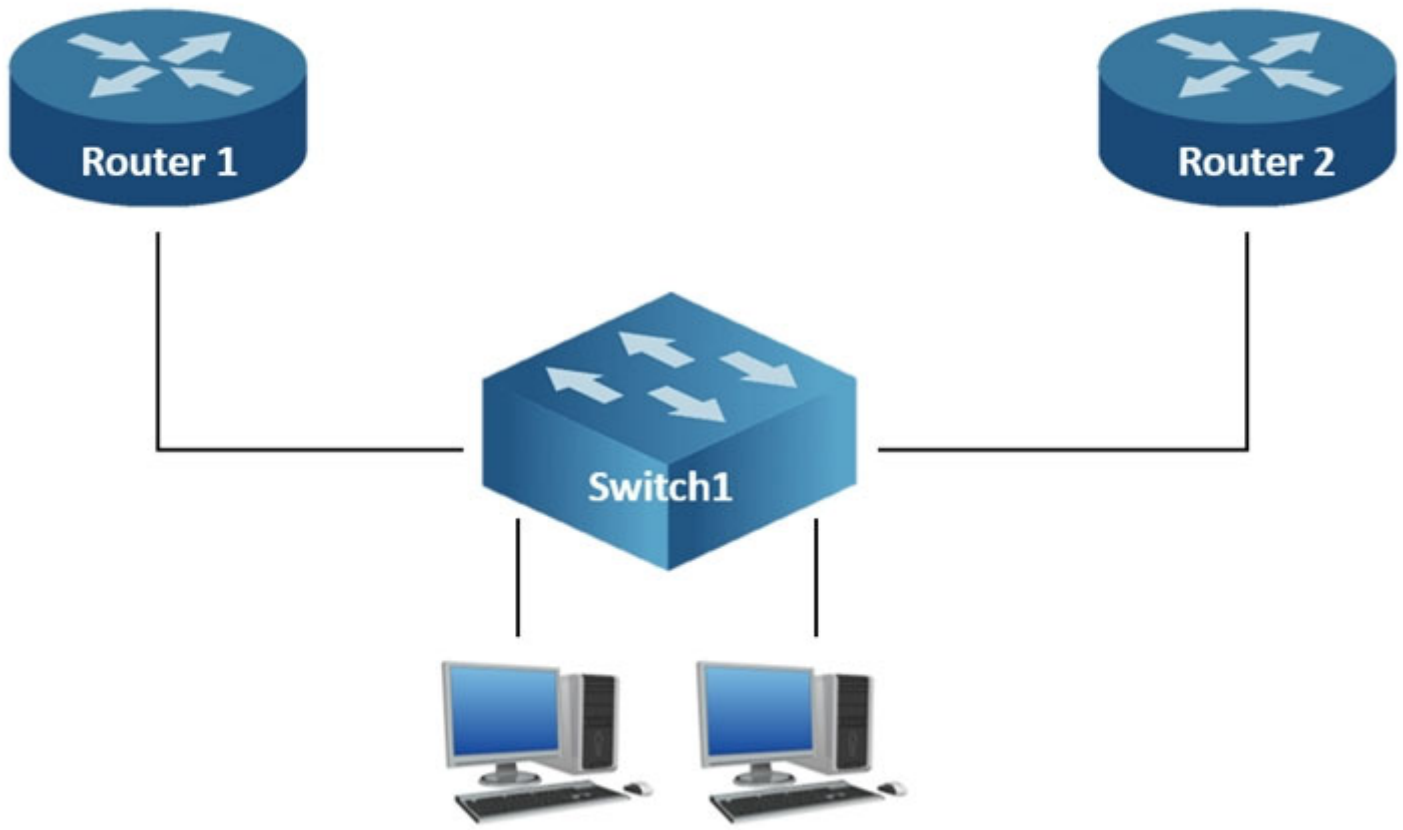
A. (Wrong) because the cluster can operate with given timers
B. (Wrong) keys are identical
C. (Wrong) absolutely wrong
D. They should've used the word "identical" instead of "unique"
upvoted 3 times

Clauster 9 months ago

Selected Answer: A

The Answer is A and here's Why
B. The KeyStrings match.
C. Priority Values don't have to match
D. HSRP or Any FHRP will NEVER form with UNIQUE Virtual IP Addresses, they have to be the SAME IP ADDRESS not UNIQUE.
They got you guys. BTW TIMERS MUST MATCH.
upvoted 2 times

Refer to the exhibit.



Router1 is currently operating as the HSRP primary with a priority of 110. Router1 fails and Router2 takes over the forwarding role. Which command on Router1 causes it to take over the forwarding role when it returns to service?

A. standby 2 priority

B. standby 2 preempt

C. standby 2 track

D. standby 2 timers

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/13780-6.html

Community vote distribution

B (100%)

[Removed] 2 months, 3 weeks ago

Let's have B 😎

upvoted 1 times

techriese 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: B

cisco(config-if)#standby 2 ?
authentication Authentication
follow Name of HSRP group to follow
ip Enable HSRP IPv4 and set the virtual IP address
ipv6 Enable HSRP IPv6
mac-address Virtual MAC address
name Redundancy name string
preempt Overthrow lower priority Active routers
priority Priority level
timers Hello and hold timers
track Priority tracking

cisco(config-if)#standby 2

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

Answer provided is correct

upvoted 1 times

krn007 1 year, 11 months ago

Selected Answer: B

Answer provided is correct

upvoted 1 times

Question #58 *Topic 1*

An engineer has deployed a single Cisco 5520 WLC with a management IP address of 172 16.50.5/24. The engineer must register 50 new Cisco AIR-CAP2802I-
E-K9 access points to the WLC using DHCP option 43. The access points are connected to a switch in VLAN 100 that uses the 172.16.100.0/24 subnet. The engineer has configured the DHCP scope on the switch as follows:
Network 172.16.100.0 255.255.255.0

Default Router 172.16.100.1 -

Option 43 ASCII 172.16.50.5 -
The access points are failing to join the wireless LAN controller. Which action resolves the issue?

A. configure option 43 Hex F104.AC10.3205

B. configure option 43 Hex F104.CA10.3205

C. configure dns-server 172.16.50.5

D. configure dns-server 172. 16.100.1

Correct Answer: *A*

Reference:

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html

Community vote distribution

A (100%)

[Removed] Highly Voted 1 year, 10 months ago

The Option 43 hexadecimal string is assembled as a sequence of the TLV values for the Option 43 suboption: Type + Length + Value. Type is always the suboption code 0xf1. Length is the number of controller management IP addresses times 4 in hex. Value is the IP address of the controller listed sequentially in hex.

On this question, there is 1 controller with management interface IP addresses 172.16.50.5/24. The type is 0xf1. The length is 1 * 4 = 8 = 0x04. The mgmt IP addresses 172.16.50.5 translate to ac.10.32.05 (0xac103205). When the string is assembled, it yields f108c0a80a05c0a80a14. The Cisco IOS command that is added to the DHCP scope is:

option 43 hex f104ac103205

upvoted 11 times

nushadu Highly Voted 11 months, 2 weeks ago

Selected Answer: A

#python3
ip_addr = [int(i) for i in '172.16.50.5'.split('.')]
print(ip_addr)
for i in ip_addr:
print(f'dec={i}, hex={str(hex(i))[2:]}')
#output:
[172, 16, 50, 5]
dec=172, hex=ac
dec=16, hex=10
dec=50, hex=32
dec=5, hex=5

upvoted 7 times

ihateciscoreally Most Recent 3 months, 1 week ago

im here just to remember answer, if they want me to do hex maths in my head on the exam then they lost their mind.

upvoted 6 times

techriese 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

Asymptote 1 year ago

Selected Answer: A

check this article how to convert option 43 hexidecimal.
https://www.rapidtables.com/convert/number/hex-to-decimal.html?x=F104

Option 43 IP to hexi converter
https://shimi.net/services/opt43/
upvoted 2 times

dougj 1 year, 1 month ago

Using ASCII characters for the IP address are only supported for the older Cisco 1000 series APs, all the rest require HEX characters
upvoted 2 times

dranzer6 1 year, 4 months ago

Selected Answer: A

shimi.net/services/opt43
Vendor Cisco: f1 (hex)
IP count: 1
IP count * 4 bytes = 4 ---> 04 (hex)
172.16.50.5 = ac103205 (hex)
option 43 hex f104.ac10.3205
upvoted 3 times

Pudu_vlad 1 year, 5 months ago

provided answer is correct
upvoted 1 times

winder 1 year, 5 months ago

I dont get it, shouldn't the "Option 43 Ascii 172.16.50.5" work?
Why we have to use hex option here?
upvoted 3 times

mgiuseppe86 3 months ago

It works for Aruba environments on a Windows DHCP Server.

DHCP Option 43 10.200.20.10
DHCP Option 60 - aruba-ap
upvoted 1 times

platin 1 year, 5 months ago

I agree, anyone please check this comment.
upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: A

The answer provided is correct
https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1550/installation/guide/1550hig/1550_axf.pdf
upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct
upvoted 2 times

Question #59 *Topic 1*

What is the role of vSmart in a Cisco SD-WAN environment?

A. to establish secure control plane connections

B. to monitor, configure, and maintain SD-WAN devices

C. to provide secure data plane connectivity over WAN links

D. to perform initial authentication of devices

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html

Community vote distribution

A (94%) 6%

iGlitch Highly Voted 1 year, 2 months ago

Selected Answer: A

A) is vSmart using OMP to communicate with vEdge routers. (CORRECT)
B) is vManage.
C) is VPNs.
D) is vBond.

upvoted 16 times

Hamo1 Most Recent 3 months ago

i think it's D , check pag 634 of the Cert GUID

upvoted 1 times

CCNPWILL 3 months, 3 weeks ago

answer is A ... but question is poorly worded.

upvoted 1 times

Stylar 1 year ago

Selected Answer: A

A is the correct answer here.

upvoted 1 times

Dataset 1 year, 2 months ago

Selected Answer: C

I think C is correct to, vSmart authenticates devices connected to the SD-WAN network

upvoted 1 times

Niam77 9 months, 3 weeks ago

maybe right, but the answer c is data plane connection, so maybe that why the answer c is wrong because we know that vsmart is in control plane

upvoted 1 times

Dataset 1 year, 2 months ago

I think C is correct to, vSmart authenticates devices connected to the SD-WAN network

upvoted 1 times

kebkim 1 year, 2 months ago

vSmart controller distributes security information between vEdge routers to facilitate data plane IPSEC tunnel creation. vSmart uses OMP to distribute routing information, security keys and policy configuration through DTLS tunnels to the vEdge routers.

upvoted 1 times

Question #60 *Topic 1*

Which action is performed by Link Management Protocol in a Cisco StackWise Virtual domain?

A. It determines which switch becomes active or standby.

B. It determines if the hardware is compatible to form the StackWise Virtual domain.

C. It rejects any unidirectional link traffic forwarding.

D. It discovers the StackWise domain and brings up SVL interfaces.

Correct Answer: *C*

Community vote distribution

C (100%)

Mac13 Highly Voted 2 years, 7 months ago

C seems like the best fit:

The Link Management Protocol (LMP) is activated on each link of the StackWise Virtual link as soon as it is brought up online. The LMP performs the following functions:
• Verifies link integrity by establishing bidirectional traffic forwarding, and rejects any unidirectional links
• Exchanges periodic hellos to monitor and maintain the health of the links
• Negotiates the version of StackWise Virtual header between the switches

A = StackWise Discovery Protocol (SDP)

Page 7 - https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.pdf

upvoted 26 times

Mac13 2 years, 7 months ago

Sorry, correction... A,B and D are all SDP.

upvoted 5 times

powerslave666 Highly Voted 2 years, 6 months ago

AnswerC:
The Link Management Protocol (LMP) is activated on each link of the StackWise Virtual link as soon as it is brought up online. The LMP performs the following functions:
● Verifies link integrity by establishing bidirectional traffic forwarding, and rejects any unidirectional links
● Exchanges periodic hellos to monitor and maintain the health of the links

upvoted 7 times

RREVECO Most Recent 1 year, 2 months ago

Selected Answer: C

"C" is correct

ref https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.pdf
Page 7 Figure 6

A. WRONG (SDP) It determines which switch becomes active or standby.
B. WRONG (SDP) It determines if the hardware is compatible to form the StackWise Virtual domain.
C. OK It rejects any unidirectional link traffic forwarding.
D. WONRG ("Pre-parse configuration file") It discovers the StackWise domain and brings up SVL interfaces.

The Link Management Protocol (LMP) is activated on each link of the StackWise Virtual link as soon as it is brought up online. The LMP performs the following functions:
• Verifies link integrity by establishing bidirectional traffic forwarding, and rejects any unidirectional links

upvoted 3 times

GreatDane 1 year, 6 months ago

Ref: Troubleshoot SVL on Catalyst 9000 Switches - Cisco

"...
New LMP & SDP Counters
...
LMP - Link Management Protocol - L2 traffic to maintain the SVL.

The link Management protocol is a software component, which runs a hello between ends and decides if the physical link is eligible to be part of the StackWise Virtual. LMP also monitors each configured physical link while they are part of the SVL. LMP is a part of the Network Interface Manager (Nif Mgr) software process.
..."

A. It determines which switch becomes active or standby.

Wrong answer.

B. It determines if the hardware is compatible to form the StackWise Virtual domain.

Wrong answer.

C. It rejects any unidirectional link traffic forwarding.

Wrong answer.

D. It discovers the StackWise domain and brings up SVL interfaces.

Correct answer.
upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct
upvoted 1 times

arminio89 2 years, 3 months ago

Edit: C is correct
upvoted 1 times

arminio89 2 years, 3 months ago

A and B are correct:
"It ensures that the hardware and software versions are compatible to form the SVL and determines which switch becomes active or standby from a control plane perspective"
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/16-12/configuration_guide/ha/b_1612_ha_9600_cg/configuring_cisco_stackwise_virtual.html
upvoted 1 times

betashow 1 year, 7 months ago

All paragraphe is : "The Link Management Protocol (LMP) is activated on each link of the SVL as soon as the links are established. LMP ensure the integrity of the links and monitors and maintains the health of the links. The redundancy role of each switch is resolved by the StackWise Discovery Protocol (SDP). It ensures that the hardware and software versions are compatible to form the SVL and determines which switch becomes active or standby from a control plane perspective."

So C is Correct
upvoted 5 times

mustache 2 years, 7 months ago

it seams to be A

The Link Management Protocol (LMP) is activated on each link of the SVL as soon as the links are established. LMP ensure the integrity of the links and monitors and maintains the health of the links. The redundancy role of each switch is resolved by the StackWise Discovery Protocol (SDP). It ensures that the hardware and software versions are compatible to form the SVL and determines which switch becomes active or standby from a control plane perspective.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/16-12/configuration_guide/ha/b_1612_ha_9600_cg/configuring_cisco_stackwise_virtual.html
upvoted 1 times

noov 2 years, 7 months ago

i think thas the correcte answer is A
upvoted 1 times

Question #61 *Topic 1*

What are two reasons why broadcast radiation is caused in the virtual machine environment? (Choose two.)

A. vSwitch must interrupt the server CPU to process the broadcast packet.

B. The Layer 2 domain can be large in virtual machine environments.

C. Virtual machines communicate primarily through broadcast mode.

D. Communication between vSwitch and network switch is broadcast based.

E. Communication between vSwitch and network switch is multicast based.

Correct Answer: *AB*
Reference:
https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/net_implementation_white_paper0900aecd806a9c05.html

Community vote distribution
BC (63%) AB (32%) 5%

J_C_STUDY Highly Voted 3 years, 3 months ago
Thinking it is A and B. Based off the reference link.

Because the vswitch is software based, as broadcasts are received the vswitch must interrupt the server CPU to change contexts to enable the vswitch to process the packet. After the vswitch has determined that the packet is a broadcast, it copies the packet to all the VMNICs, which then pass the broadcast packet up the stack to process. This processing overhead can have a tangible effect on overall server performance if a single domain is hosting a large number of virtual machines
upvoted 48 times

MWoods Highly Voted 3 years, 1 month ago
B, C
It is asking what causes it not effect.
upvoted 16 times

wwwwaaaa 1 year, 11 months ago
C?... all VMs communication are broadcast based, yet not every VM environment suffer from Broadcast Radiation
A - B are the answer
upvoted 1 times

ArchBishop 1 year, 10 months ago
I imagine what MWoods is saying is, the combination of B and C will cause an overabundance of A.
B and C are the Cause, in that VMs use broadcast and there can be a LOT of VMs, resulting in a lot of broadcasts; therefore an over-utilization of the process described in A.

As far as I can tell, A, B, and C all seem to be correct... and this question kinda sucks....
upvoted 8 times

shefo1 Most Recent 2 weeks, 3 days ago
* from Google bard *

The two reasons why broadcast radiation is caused in the virtual machine environment are:

The Layer 2 domain can be large in virtual machine environments. (B)
Virtual machines communicate via broadcast too much. (C)
Explanation:

(B): Virtual machines can be easily created and destroyed, and they can be moved around between different physical hosts. This can lead to large Layer 2 domains, which is a major factor in broadcast radiation.

(C): Virtual machines often communicate through broadcast packets, such as Address Resolution Protocol (ARP) broadcasts and DHCP requests. This can flood the network with broadcast traffic, leading to broadcast radiation.
upvoted 1 times

djedeen 3 months ago
Selected Answer: BC
The two reasons why broadcast radiation is caused in the virtual machine environment are:

B. The Layer 2 domain can be large in virtual machine environments: In a physical network, broadcast traffic is typically limited to a single LAN segment, which can be controlled through the use of routers or VLANs. However, in a virtual machine environment, multiple VMs can be connected to the same virtual switch, which creates a larger Layer 2 broadcast domain.

C. Virtual machines communicate primarily through broadcast mode: In a traditional physical network, communication between devices typically occurs through unicast or multicast traffic. However, in a virtual machine environment, communication between VMs often relies on broadcast

traffic, which can be less efficient and create more network traffic than necessary. This is due to the fact that virtual machines are often configured to use broadcast traffic for tasks such as address resolution or service discovery.

upvoted 1 times

JackDRipper 8 months ago

Selected Answer: BC

The question is asking for "reasons". Only B and C addresses that.
Answer A is a "result" of broadcast radiation. D and E are just dead wrong.

upvoted 4 times

mykab 8 months, 4 weeks ago

Selected Answer: BD

The two possible reasons why broadcast radiation can occur in a virtual machine (VM) environment are:

B. The Layer 2 domain can be large in virtual machine environments.
D. Communication between vSwitch and network switch is broadcast based.

Explanation :-

B. In VM environments, the Layer 2 domain can be large, as multiple VMs may be connected to the same virtual switch. This can lead to broadcast radiation, as broadcast packets sent by one VM are replicated to all the other VMs on the same virtual switch.

D.Communication between vSwitch and network switch is typically based on Ethernet frames, which use broadcast for certain types of traffic, such as ARP requests and DHCP broadcasts. This can lead to broadcast radiation in VM environments.

upvoted 1 times

Quentin_ 9 months ago

A is true, but it's not the cause of broadcast radiation. It is the effect.
So, i think B and C

upvoted 1 times

TSKARAN 10 months, 1 week ago

A & B - Correct Answer.

INCORRECT: Virtual machines communicate primarily through broadcast mode

upvoted 1 times

kewokil120 10 months, 2 weeks ago

Selected Answer: AB

AB is right

upvoted 1 times

kewokil120 10 months, 3 weeks ago

Selected Answer: AB

AB is the answer

upvoted 1 times

StefanOT2 10 months, 3 weeks ago

Selected Answer: BC

Upfront: This question is just bad.
I think it is B and C. While C sounds strange at first glance... when VMs are using a lot of broadcasts, then there is broadcast radiation. If you take this answer as simple as it is, it sound logical...

upvoted 2 times

Ayman_B 11 months ago

Selected Answer: AB

interrupting the server CPU to process the packet causes broadcast radiation in a (VM) environment because it can result in increased traffic and congestion on the network (answer A).
on the other side all VMs communication are broadcast based but Broadcast radiation results in increased traffic and congestion on the network, there is no problem with broadcast unless there is increased traffic and congestion on the network (Answer C)

because of that I think the answer is : A and B

upvoted 1 times

kewokil120 11 months ago

Selected Answer: AB

C?... all VMs communication are broadcast based, yet not every VM environment suffer from Broadcast Radiation
A - B are the answer

upvoted 1 times

PedroPicapiedra 1 year ago

Selected Answer: AB

The correcto are A - B

upvoted 1 times

tckoon 1 year, 3 months ago

A: wrong answer . it dont caused broadcast radiation. vSwitch rx broadcast it will casue server high cpu utilization.
B : correct answer
C : correct answer - because if the VM tend to communicate through broadcast it will caused broadcast radiation/storm

upvoted 2 times

GP5724 1 year, 6 months ago

The question is asking what CAUSES broadcast radiation NOT what it's effects are!!!

upvoted 3 times

AlbertoStu 1 year, 8 months ago

Selected Answer: BC

Looking for the cause, not the effect.

upvoted 3 times

Question #62 *Topic 1*

Which two GRE features are configured to prevent fragmentation? (Choose two.)

A. TCP window size

B. IP MTU

C. TCP MSS

D. DF bit clear

E. MTU ignore

Correct Answer: *BC*
Reference:
https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html

Community vote distribution

Askhat Highly Voted 3 years, 2 months ago
Correct answer TCP MSS & PMTUD
upvoted 24 times

mimou Highly Voted 3 years, 3 months ago
From my perspective df is cleared means df is set to zero. That means fragmentation is allowed through the GRE tunnel. Anyone else to add more or any rectification?
upvoted 7 times

shofmans 3 years, 2 months ago
df = dont fragment, so if df is cleared, fragment is allowed
upvoted 7 times

nightstalker Most Recent 4 months, 1 week ago
if you clear DF bit allowing fragmentation you're breaking PMTUD, that relies on ICMP "fragmentation needed and DF set" message obviously TCP MSS and PMTUD (not present in this dump)

https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html
upvoted 1 times

Burik 5 months, 2 weeks ago
BAD DUMP! Option B is PMTUD.
upvoted 1 times

Ayman_B 9 months ago
Selected Answer: BC
For this question B,C .. but now it comes with one more choise (PMTUD) and this is more accurate .. beacause IP MTU is not a GRE feature but a parameter that defines the maximum size of the IP packet that can be transmitted over a network path without fragmentation, so we can controll it to control the fragmentation.
but PMTUD is a feature that detects the maximum transmission unit (MTU) of the path between two endpoints and adjusts the packet size to fit within that MTU
upvoted 3 times

kewokil120 11 months ago
Selected Answer: BC
df = dont fragment, so if df is cleared, fragment is allowed
upvoted 1 times

bora4motion 1 year ago
Selected Answer: BC
I;m going with B + C
upvoted 1 times

Asymptote 1 year ago
Selected Answer: BD
Question is asking how to prevent not how to find.
upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: BC

voting. provided answer is correct

upvoted 1 times

Labedu_Singh 1 year, 9 months ago

Options are:
A. TCP window size
B. TCP MSS
C. IP MTU
D. DF bit Clear
E. MTU ignore
F. PMTUD

BE correct.

upvoted 1 times

Labedu_Singh 1 year, 9 months ago

ignore it please, Correct answer TCP MSS & PMTUD

upvoted 6 times

error_909 2 years, 2 months ago

TCP MSS was used to find the MTU between the 2 end points.
PMTUD is used to find the whole path most suitable MTU.

upvoted 4 times

TTTTTT 2 years, 3 months ago

Some Sites will have this
A. TCP MSScorrect
B. IP MTU
C. TCP window size
D. DF bit Clear
E. MTU ignore
F. PMTUD

the right answer will be TCP MSS & PMTUD

upvoted 6 times

Tobias1 2 years, 4 months ago

Only B+C make sense here but why the hell should these be "GRE features"???
Every second question is so bad expressed that I tend to skip the recertification.

upvoted 5 times

examShark 2 years, 6 months ago

https://en.wikipedia.org/wiki/Path_MTU_Discovery
IP MTU allows the sending device to recognise and honour the configured value, TCP MSS is MSS clamping.

upvoted 2 times

Question #63 *Topic 1*

Which LISP device is responsible for publishing EID-to-RLOC mappings for a site?

A. ETR

B. MR

C. ITR

D. MS

Correct Answer: *A*

Reference:

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/locator-id-separation-protocol-lisp/white_paper_c11-652502.html

Community vote distribution

A (58%) D (42%)

DJOHNR Highly Voted 3 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html

A. ETR

An ETR connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to Map-Request messages, and decapsulates and delivers LISP-encapsulated user data to end systems at the site.

upvoted 17 times

Dudu84 Most Recent 2 days, 20 hours ago

A is correct
After the ITR receives the EID-to-RLOC mapping from the ETR (or MS, if the ETR requested a proxy map reply), it is ready to send data from host1 to host2.

upvoted 1 times

mahnazmohamz 1 month, 3 weeks ago

Selected Answer: A

ask google

upvoted 2 times

DJ_Yahia 2 months, 1 week ago

Selected Answer: D

The LISP device that is responsible for publishing EID-to-RLOC mappings for a site is the Mapping Server (MS).

The MS stores and manages the mapping database for a site or domain, and provides the mappings to the MR when requested. It is responsible for publishing EID-to-RLOC mappings to the Map-Resolvers (MRs) in the domain. When a router needs to find the RLOC for a given EID, it sends a Map-Request message to the MR. The MR then queries the MS for the mapping.

The other LISP devices are responsible for different tasks:

Ingress Tunnel Router (ITR): The ITR is responsible for encapsulating packets destined for LISP-capable sites in LISP headers and sending them to the MR.
Egress Tunnel Router (ETR): The ETR is responsible for decapsulating LISP packets from the ITR and forwarding them to their final destination.
Map-Resolver (MR): The MR is responsible for responding to Map-Request messages from ITRs and providing them with the RLOCs for the EIDs that they are requesting.

upvoted 1 times

omid8719 2 months, 2 weeks ago

Selected Answer: D

MS Service populates the HTDB
MR Service resolves HTDB queries

upvoted 1 times

rogue_user 4 months, 3 weeks ago

Selected Answer: A

Map server (MS): This is a network device (typically a router) that learns EID-to-prefix mapping entries from an ETR and stores them in a local EID-to-RLOC mapping database.

upvoted 1 times

nightstalker 4 months, 1 week ago

as you said, the MS LEARNS from an ETR, so it's the ETR that publishes

upvoted 2 times

ajeetnagdev 5 months ago

A is correct answer.

Egress Tunnel Router (ETR) is the device (or function) that connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to Map-Request messages, and decapsulates and delivers LISP-encapsulated user data to end systems at the site. During operation, an ETR sends periodic Map-Register messages to all its configured map servers.

https://www.digitaltut.com/lisp-tutorial

upvoted 3 times

foreignbishop 6 months, 1 week ago

Selected Answer: D

I'm going to be the outlier here. The Map Server is what actually populates the Host Tracking Database inside the Control Plane. The word used here is "publishes". When devices connect, they register with the Map Server. That is how the HTDB gets populated. The HTDB is "the central repository of EID-to-fabric-edge" node bindings (EID-RLOC)

upvoted 3 times

omid8719 2 months, 2 weeks ago

MS Service populates the HTDB
MR Service resolves HTDB queries

upvoted 1 times

rafaelinho88 9 months, 3 weeks ago

Selected Answer: A

n Egress Tunnel Router (ETR) connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to Map-Request messages, and decapsulates and delivers LISP-encapsulated user data to end systems at the site.

upvoted 2 times

Dataset 1 year, 1 month ago

Selected Answer: A

correct

upvoted 1 times

GreatDane 1 year, 6 months ago

Ref: IP Routing: LISP Configuration Guide, Cisco IOS Release 15M&T

“Locator ID Separation Protocol (LISP) Overview
…
LISP Network Element Functions
…
LISP Egress Tunnel Router
An ETR connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to Map-Request messages, and decapsulates and delivers LISP-encapsulated user data to end systems at the site.
…”

A. ETR

Correct answer.

B. MR

Wrong answer.

C. ITR

Wrong answer.

D. MS

Wrong answer.

upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct

upvoted 1 times

jmm 1 year, 10 months ago

Answer is A

LISP Egress Tunnel Router
An ETR connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to Map-Request messages, and decapsulates and delivers LISP-encapsulated user data to end systems at the site.

upvoted 2 times

Net91 1 year, 11 months ago

Correct Answer

upvoted 1 times

sasatrickovic 2 years, 1 month ago

ETR is the correct answer.
An Egress Tunnel Router (ETR) connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to Map-Request messages, and decapsulates and delivers LISP-encapsulated user data to end systems at the site.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html

upvoted 2 times

GiorgioJK 2 years, 1 month ago

I think the right answer is: B.MR
Map-resolver—The LISP Map-Resolver (MR) responds to queries from fabric devices requesting RLOC mapping information from the HTDB in the form of an EID-to-RLOC binding. This tells the requesting device to which fabric node an endpoint is connected and thus where to direct traffic.

upvoted 1 times

AlbertoStu 1 year, 8 months ago

An ETR connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to Map-Request messages, and decapsulates and delivers LISP-encapsulated user data to end systems at the site.

upvoted 1 times

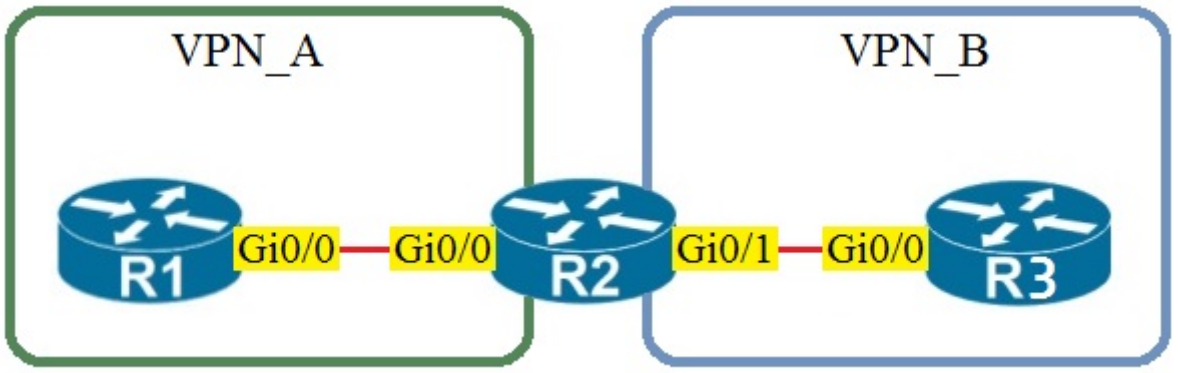
Hugh_Jazz 2 years, 3 months ago

Answer is correct.

upvoted 2 times

Question #64 *Topic 1*

Refer to the exhibit.



Assuming that R1 is a CE router, which VRF is assigned to Gi0/0 on R1?

A. default VRF

B. VRF VPN_A

C. VRF VPN_B

D. management VRF

Correct Answer: *A*

Community vote distribution

A (100%)

mdrama Highly Voted 3 years, 1 month ago

It makes an assumption that the PE (being a provider) has multiple customers, and VPN_A is one customer, and is likely not using VRFs at their border to the provider, i.e. they are using the Global routing table/GRT or 'default VRF'. If it was an enterprise network with mulitple CE VRFs mapped to PE VRFs, might be different but this is a simpler example. hope that helps.

upvoted 21 times

XalaGyan Highly Voted 2 years, 2 months ago

i understand the question as this.

R1 is a CE and therefore R3 must be a CE too.
The only one that a CE connects to is a PE Router which is R2.

Since we talk about VPN in sense of just simply two different routing tables without affecting or seeing eachother (VRF) should be configured.

That being said, neither CE needs to do any routing table partitioning as they are simply talking to their PE router.

the PE router R2 is the one needing to have separate VRF instances or so called VPNs etc.

therefore DEFAULT VRF on CE always
and VRF separation on PE.

thanks for reading this far

upvoted 17 times

Clauster 9 months ago

Thanks this helped

upvoted 3 times

danman32 4 months, 1 week ago

I agree

upvoted 3 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: A

Default VRF:
All Layer 3 interfaces exist in the default VRF until they are assigned to another VRF.
Routing protocols run in the default VRF context unless another VRF context is specified.
The default VRF uses the default routing context for all show commands.
The default VRF is similar to the global routing table concept in Cisco IOS.

upvoted 2 times

nushadu 11 months, 2 weeks ago

source:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/9-x/unicast/configuration/guide/l3_cli_nxos/l3_virtual.html

upvoted 2 times

Pudu_vlad 1 year, 5 months ago

A is correct

upvoted 1 times

Violator 1 year, 9 months ago

This question is still asked. Passed today.

upvoted 10 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct

upvoted 2 times

ArchBishop 1 year, 10 months ago

This is kinda a dumb question.. but it is important to remember:
1: What VRF concept they are challenging you to understand.
2: That VRFs are necessarily "locally significant."

In other words, the CE routers do not know, nor do they care, what VRF their upstream PE router assigns them to.
The important VRF concept here is, by NOT configuring and associating an interface to a VRF, that interface is said to be utilizing the "default VRF."

Technically, the CE router could have the interface associated with a "VRF BUTTERFLY", and it would not make a difference to how the PE router makes its decisions locally. But you'll want to recognize that this question is challenging your understanding of the above concept, that, while it does not matter, the client is still likely going to be assigned to default.. by default, and still work.

upvoted 6 times

molinux 1 year, 11 months ago

Default vrf could mean no vrf

upvoted 1 times

Tobias1 2 years, 4 months ago

These questions get more an more ridiculous. If it is a CE router, it is my router and I can configure any VRF I like. The Provider won´t even know or care what VRF I use.

upvoted 5 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

P1Z7C 2 years, 8 months ago

Even R1 is considered to be a Customer Edge(CE) this router is only connected to R2 that is assumed to be the Provider Edge (PE). Because the R1 is only connected to 1 SP (Service Provider) there is no need to use VRFs to separate the traffic of different SPs

upvoted 5 times

Bahmed 2 years, 8 months ago

There is nothing special with the configuration of Gi0/0 on R1. Only Gi0/0 interface on R2 is assigned to VRF VPN_A. The default VRF here is similar to the global routing table concept in Cisco IOS

upvoted 4 times

ABC123 2 years, 5 months ago

in drawing there's no G0/0 on R2! and that should be VRF_B for R2 anyway

upvoted 1 times

ABC123 2 years, 5 months ago

Sorry above was rushed comment, please remove it moderator !!

upvoted 1 times

Summa 3 years, 1 month ago

anybody know why?

upvoted 2 times

Question #65 *Topic 1*

What are two benefits of virtualizing the server with the use of VMs in a data center environment? (Choose two.)

A. reduced rack space, power, and cooling requirements

B. smaller Layer 2 domain

C. increased security

D. speedy deployment

E. reduced IP and MAC address requirements

Correct Answer: *AD*

Community vote distribution

AD (100%)

techriese 5 months ago

Selected Answer: AD

A + D are correct

upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: AD

voting. provided answer is correct

upvoted 2 times

flash007 2 years, 4 months ago

you can have a brand new server up and working in under 3 minutes with Azure , AWS and GCP

upvoted 2 times

flash007 2 years, 4 months ago

Virtualizing the environment does reduce rack space and cooling as its stored in the cloud provider datacentre

upvoted 2 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

Question #66 *Topic 1*

Which statement about route targets is true when using VRF-Lite?

A. Route targets control the import and export of routes into a customer routing table.

B. When BGP is configured, route targets are transmitted as BGP standard communities.

C. Route targets allow customers to be assigned overlapping addresses.

D. Route targets uniquely identify the customer routing table.

Correct Answer: *A*

Community vote distribution

A (100%)

edg Highly Voted 3 years, 3 months ago

The answer is "A".
https://www.cisco.com/c/en/us/td/docs/optical/15000r8_0/ethernet/454/guide/d80ether/r8vrf.pdf
Step: 3
Command: Router(config-vrf)# route-target {import | export | both} route-distinguisher
Purposes: Creates a list of import and/or export route target communities for the specified VRF.

upvoted 15 times

rpidcock Highly Voted 2 years, 3 months ago

Given answer A is correct.
B is incorrect because a RT is an extended communitty not standard
C is incorrect because a RD is what allows customers to have overlapping addresses
D is incorrect because RD is what identifies customer routing table.

upvoted 13 times

alawi2 1 year, 6 months ago

RT = Route Target
RD = Route Distinguisher

upvoted 5 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: A

cisco(config-vrf)#route-target ?
ASN:nn or IP-address:nn Target VPN Extended Community
both Both import and export Target-VPN community
export Export Target-VPN community
import Import Target-VPN community

cisco(config-vrf)#route-target

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

A is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct

upvoted 1 times

Helloory 3 years ago

A is correct

upvoted 2 times

Arsen_4 3 years, 1 month ago

The correct answer is A. Route targets are used mainly with exporting/importing route in MPBGP, but it could be use in VRF-lite during the route leaking between the VRF's:
https://community.cisco.com/t5/mpls/route-leaking-between-vrf-s-shared-services/td-p/1960139

upvoted 4 times

Summa 3 years, 1 month ago

I think the answer is "D". all the reset A/B/C are about VRF.
https://ipwithease.com/vrf-vs-vrf-lite/

upvoted 1 times

Multicast01005e 2 years, 1 month ago

Its not D, as that would be Route Distinguisher.

upvoted 1 times

ksuha 3 years, 3 months ago

I think the answer is A, since the route target is not the standard community

upvoted 2 times

DJOHNR 3 years, 3 months ago

This should be a choose two question... (Google the question)

A and B

upvoted 1 times

Multicast01005e 2 years, 1 month ago

Its not B, as RT are transmitted as BGP extended communities.

upvoted 1 times

Question #67 *Topic 1*

Which LISP infrastructure device provides connectivity between non-LISP sites and LISP sites by receiving non-LISP traffic with a LISP site destination?

A. PITR

B. map resolver

C. map server

D. PETR

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DCI/5-0/LISPmobility/DCI_LISP_Host_Mobility/LISPmobile_2.html

Community vote distribution

A (100%)

rezavage Highly Voted 3 years ago

A is correct
PITRs are for non-LISP sites that send traffic to EID destinations.

upvoted 13 times

ArchBishop 1 year, 10 months ago

Further simplified:
PITRs are for Non-LISP > LISP
PETRs are for LISP > Non-LISP

Always remember who is performing encapsulation and de-encapsulation. xITRs always encapsulate, whether [FROM] a LISP-RLOC or Non-LISP Site; while xETRs always de-encapsulate, whether [TO] a LISP-RLOC or Non-LISP Site.

upvoted 17 times

flash007 Most Recent 4 months, 1 week ago

pitr is ingress so is recieving the egress is sending out the other side of the device

upvoted 1 times

HungarianDish 8 months, 3 weeks ago

"A PITR is a LISP Infrastructure device that provides connectivity between non-LISP sites and LISP sites by attracting non-LISP traffic destined to LISP sites and encapsulating this traffic to ETRs devices deployed at LISP sites. "

upvoted 1 times

HungarianDish 8 months, 3 weeks ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DCI/5-0/LISPmobility/DCI_LISP_Host_Mobility/LISPmobile_2.html#:~:text=%E2%80%93%20Proxy%20ITR%20(PITR)%3A%20A,devices%20deployed%20at%20LISP%20sites.

" An ITR is a LISP Site edge device that receives packets from site-facing interfaces (internal hosts) and encapsulates them to remote LISP sites, or natively forwards them to non-LISP sites. "

upvoted 1 times

Vlad_Is_Love_ua 9 months, 2 weeks ago

Selected Answer: A

Proxy ITR (PITR): PITR is a LISP infrastructure device that provides connectivity between non-LISP sites and LISP sites by attracting non-LISP traffic that is destined to LISP sites and encapsulating this traffic to devices of ETR that are deployed at LISP sites.

upvoted 1 times

PS5 1 year ago

Q95. Which LISP component is required for a LISP site to communicate with a non-LISP site?

A. Proxy ITR
B. ITR
C. ETR
D. Proxy ETR

^^^ How is the answer to this one D - Proxy ETR?

upvoted 1 times

Caradum 1 year ago

As rezavage wrote:
PITRs are for Non-LISP --> LISP
PETRs are for LISP --> Non-LISP

Proxy ETR = PETR
upvoted 3 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct
upvoted 1 times

CISCO_CCNP 3 years, 1 month ago

Correct
upvoted 3 times

Question #68 *Topic 1*

Which statement explains why Type 1 hypervisor is considered more efficient than Type2 hypervisor?

A. Type 1 hypervisor is the only type of hypervisor that supports hardware acceleration techniques.

B. Type 1 hypervisor relies on the existing OS of the host machine to access CPU, memory, storage, and network resources.

C. Type 1 hypervisor runs directly on the physical hardware of the host machine without relying on the underlying OS.

D. Type 1 hypervisor enables other operating systems to run on it.

Correct Answer: *C*

Community vote distribution

C (100%)

skh Highly Voted 3 years ago

I think correct C

Type 1 hypervisors are an OS themselves, a very basic one on top of which you can run virtual machines. The physical machine the hypervisor is running on serves virtualization purposes only.
https://phoenixnap.com/kb/what-is-hypervisor-type-1-2

upvoted 8 times

flash007 Most Recent 4 months, 1 week ago

type 1 run on bare metal servers and type 2 run on an installed os

upvoted 1 times

M_B 10 months, 3 weeks ago

Answer C states "..without relying on the underlying OS". There is none so is this a catch in the wording . The best answer may actually be A as Type 1 hypervisors do require hardware acceleration

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

C is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct

upvoted 1 times

flash007 2 years, 4 months ago

type 1 hypervisors are known as bare metal and do not require a underlying OS this is called a type 2 hypervisor which does have a os on the bottom

upvoted 1 times

XalaGyan 2 years, 2 months ago

type 1 is bare metal meaning no OS needed to host the hypervisor and hypervisor is directly on hardware.

type 2 means that the hypervisor runs as an application on an existing OS that controls the hardware.

the answer here is C as skh indicated correctly above

upvoted 3 times

Question #69 *Topic 1*

Which statement about VXLAN is true?

A. VXLAN encapsulates a Layer 2 frame in an IP-UDP header, which allows Layer 2 adjacency across router boundaries.

B. VXLAN uses the Spanning Tree Protocol for loop prevention.

C. VXLAN extends the Layer 2 Segment ID field to 24-bits, which allows up to 4094 unique Layer 2 segments over the same network.

D. VXLAN uses TCP as the transport protocol over the physical data center network.

Correct Answer: *A*

Community vote distribution

A (100%)

juniper Highly Voted 3 years ago

A is correct

upvoted 8 times

edg Highly Voted 3 years, 3 months ago

https://tools.ietf.org/html/rfc7348

Due to this encapsulation, VXLAN could also be called a tunneling scheme to overlay Layer 2 networks on top of Layer 3 networks

upvoted 5 times

flash007 Most Recent 4 months, 1 week ago

vxlan is an encapsulation protocol where the traffic encaped into layer 3 traffic

upvoted 1 times

techriese 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

The correct is A

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct

upvoted 3 times

Question #70 *Topic 1*

Which TCP setting is tuned to minimize the risk of fragmentation on a GRE/IP tunnel?

A. MSS

B. MTU

C. MRU

D. window size

Correct Answer: *A*

Community vote distribution

A (75%) B (25%)

skh Highly Voted 3 years ago

The TCP Maximum Segment Size (TCP MSS) defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. This TCP/IP datagram might be fragmented at the IP layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. Contrary to popular belief, the MSS value is not negotiated between hosts. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.

TCP MSS takes care of fragmentation at the two endpoints of a TCP connection, but it does not handle the case where there is a smaller MTU link in the middle between these two endpoints. PMTUD was developed in order to avoid fragmentation in the path between the endpoints. It is used to dynamically determine the lowest MTU along the path from a packet's source to its destination.

upvoted 20 times

Ed394 Highly Voted 8 months, 3 weeks ago

Selected Answer: A

MSS is the TCP setting that can be tuned to minimise fragmentation.

MTU is the IP setting that can minimise fragmentation.

The question asks for the TCP setting

upvoted 6 times

alex711 Most Recent 3 months, 3 weeks ago

Selected Answer: A

This is really confusing. but after reading in the following link, it A for sure.

https://networkdirection.net/articles/network-theory/mtu-and-mss/

upvoted 1 times

tempaccount00001 4 months ago

The problem is the ambiguity.
If we are tuning the configuration on the networking device (i.e., Switch or Router), then we're tuning the MTU, right?
And if it's on the Host side, the host automatically tunes the MSS value. Correct me if I'm wrong, please.

upvoted 1 times

JCSantana20 1 month, 3 weeks ago

But the MTU is an IP configuration, not TCP itself. MSS value is specifically TCP.

upvoted 2 times

flash007 4 months, 1 week ago

MSS is maximum segment size where the packet can be adjusted to make it less chance of being fragmented

upvoted 1 times

[Removed] 5 months, 1 week ago

Selected Answer: B

are we ignoring the fact that this is in reference to GRE/IP tunnel?
What must we take into account when creating a GRE tunnel to avoid/minimize fragmentation? we have to take into account the extra header added to the packet, its why it is recommended to modify the MTU to 1476 as best practice. Because of this MTU is the best answer.

upvoted 2 times

[Removed] 5 months ago

Disregard my answer, I have now understood more about this subject, The correct answer is A

upvoted 2 times

Entivo 9 months ago

Selected Answer: B

The answer is B because according to Cisco, the value of the MSS field is determined by the MTU configuration on the host. The default MSS value for a PC is 1500 bytes.
https://www.bing.com/ck/a?!&&p=f2cac0a3083b6063JmltdHM9MTY3NzcxNTIwMCZpZ3VpZD0wNGRlYjE4NS0yZWYyLTZmZWQtMjQ3Yi1hM2VmMmYxMjZlNWEmaW5zaWQ9NTU0Mg&ptn=3&hsh=3&fclid=04deb185-2ef2-6fed-247b-a3ef2f126e5a&psq=tcp+mss&u=a1aHR0cHM6Ly93d3cuY2lzY28uY29tL2MvZW4vdXMvdGQvZG9jcy9zd2l0Y2hlcy9sYW4vY2F0YWx5c3Q5MzAwL3NvZnR3YXJlL3JlbGVhc2UvMTYtMTEvY29uZmlndXJhdGlvbl9ndWlkZS9pcC9iZE2MTFfaXBfOTMwMF9jZy9jb25maWd1cmluZ190Y3BfbXNzX2FkanVzdG1lbnQuaHRtbCM6fjp0ZXh0PVRoZSUyMHZhbHVlJTIwb2YlMjB0aGUlMjBNU1MlMjBmaWVsZA&ntb=1
upvoted 1 times

Arodoeth 3 months, 2 weeks ago
MTU is not a TCP setting.
upvoted 1 times

Pudu_vlad 1 year, 5 months ago
A is correct
upvoted 1 times

Eddgar0 1 year, 7 months ago
Selected Answer: A
TCP Maximum Segment Size Acomplish This.
upvoted 1 times

ciscolessons 1 year, 9 months ago
Selected Answer: A
voting. provided answer is correct
upvoted 1 times

DJOHNR 3 years, 3 months ago
https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html#anc3

A. MSS
upvoted 6 times

Question #71 *Topic 1*

Which statement describes the IP and MAC allocation requirements for virtual machines on Type 1 hypervisors?

A. Virtual machines do not require a unique IP or unique MAC. They share the IP and MAC address of the physical server.

B. Each virtual machine requires a unique IP address but shares the MAC address with the physical server.

C. Each virtual machine requires a unique IP and MAC addresses to be able to reach to other nodes.

D. Each virtual machine requires a unique MAC address but shares the IP address with the physical server.

Correct Answer: *C*

Community vote distribution

C (100%)

jrquissak 2 months, 4 weeks ago

Selected Answer: C

provided answer is correct

upvoted 1 times

MaxwellJK 4 months, 1 week ago

Selected Answer: C

C es la correcta, cada VM debe tener IP y MAC unicas

upvoted 1 times

dapardo 3 months, 4 weeks ago

completamente de acuerdo

upvoted 1 times

flash007 4 months, 1 week ago

Virtual machines need both a unique Mac address and also an unique IP

upvoted 2 times

Pudu_vlad 1 year, 5 months ago

C is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct

upvoted 1 times

fabot7 2 years, 3 months ago

Layer 2 and 3 addresses have to be unique for VMs to establish proper TCP/IP communication.

upvoted 4 times

XalaGyan 1 year, 12 months ago

is there any scenario in which UNICAST can be supported WITHOUT UNIQUE MAC AND IP ?? i think unicast traffic always requires unique L2 and L3 adresses.

thats my humble opinion on the matter.

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 4 times

Question #72 *Topic 1*

Which two namespaces does the LISP network architecture and protocol use? (Choose two.)

A. TLOC

B. RLOC

C. DNS

D. VTEP

E. EID

Correct Answer: *BE*
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html

Community vote distribution
BE (100%)

fabot7 Highly Voted 2 years, 3 months ago
EndPoint-Identifyer (EID) and RLOC (Routing Locator) are used to identify hosts in LISP architecture, to where send traffic.
upvoted 8 times

suepanda Highly Voted 2 years, 9 months ago
Answer is correct
upvoted 6 times

MaxwellJK Most Recent 4 months, 1 week ago
Selected Answer: BE
B y E son las correctas
upvoted 1 times

flash007 4 months, 1 week ago
Rloc are the region locator and the EID is the endpoint identifer
upvoted 1 times

GreatDane 1 year, 6 months ago
Ref: IP Routing: LISP Configuration Guide, Cisco IOS XE Release 3S

"C H A P T E R 1
Locator ID Separation Protocol (LISP) Overview

Locator ID Separation Protocol (LISP) is a network architecture and protocol that implements the use of two namespaces instead of a single IP address:
• Endpoint identifiers (EIDs)—assigned to end hosts.
• Routing locators (RLOCs)—assigned to devices (primarily routers) that make up the global routing system.
..."

A. TLOC

Wrong answer.

B. RLOC

Correct answer.

C. DNS

Wrong answer.

D. VTEP

Wrong answer.

E. EID

Correct answer.
upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: BE

voting. provided answer is correct

upvoted 1 times

Question #73 *Topic 1*

Which two entities are Type 1 hypervisors? (Choose two.)

A. Oracle VM VirtualBox

B. Microsoft Hyper-V

C. VMware server

D. VMware ESXi

E. Microsoft Virtual PC

Correct Answer: *BD*

Reference:

https://phoenixnap.com/kb/what-is-hypervisor-type-1-2

Community vote distribution

BD (100%)

hku68 Highly Voted 2 years, 10 months ago

Of course B and D. %100.

upvoted 6 times

MaxwellJK Most Recent 4 months, 1 week ago

Selected Answer: BD

B y D, no te confundas con la C

upvoted 1 times

flash007 4 months, 1 week ago

Type 1 are vmware ESXI and Also Hyper-V as they both can be installed on bare metal servers

upvoted 1 times

stan3435 10 months, 3 weeks ago

Selected Answer: BD

B and D

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

B and D are correct

upvoted 1 times

ayodejiadeyemi 1 year, 6 months ago

provided answer is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: BD

voting. provided answer is correct

upvoted 1 times

flash007 2 years, 5 months ago

Type 1 hypervisors are bare metal so esxi and hyper-v are both type 1

upvoted 2 times

ali_mousawi 2 years, 10 months ago

VMware ESXI

upvoted 1 times

Question #74 *Topic 1*

DRAG DROP -

Drag and drop the LISP components from the left onto the functions they perform on the right. Not all options are used.

Select and Place:

LISP map resolver	accepts LISP encapsulated map requests
LISP proxy ETR	learns of EID prefix mapping entries from an ETR
LISP route reflector	receives traffic from LISP sites and sends it to non-LISP sites
LISP ITR	receives packets from site-facing interfaces
LISP map server	

Correct Answer:

LISP map resolver	LISP map resolver
LISP proxy ETR	LISP map server
LISP route reflector	LISP proxy ETR
LISP ITR	LISP ITR
LISP map server	

Reference:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DCI/5-0/LISPmobility/DCI_LISP_Host_Mobility/LISPmobile_2.html#:~:text=%E2%80%93%20Proxy%20ITR%20(PITR)%3A%20A,devices%20deployed%20at%20LISP%20sites.

examShark Highly Voted 2 years, 6 months ago
The given answer is correct
upvoted 14 times

MaxwellJK Most Recent 4 months, 1 week ago
La respuesta esta correcta
upvoted 1 times

Entivo 4 months, 3 weeks ago
Pages 465/466 of the Cisco OCG states this very very clearly. The order is

Resolver (accepts map requests)
Server (learns EID mapping entries from an ETR)
Proxy ETR (LISP to non-LISP)
ITR (receives packets from site-facing interfaces)
upvoted 3 times

Nickplayany 9 months, 2 weeks ago
The answer is correct
upvoted 1 times

65briang 9 months, 4 weeks ago
Page 466 OCG - Map Server is a network device that learns EID-to-prefix mapping entries from and ETR and stores them in a local EID-to-RLOC database.
upvoted 1 times

mailmivhan 1 year, 10 months ago
Wrong , I believe this is the correct answer.
accept LISP encapsulated map request

LISP MAP RESOLVER
learns of EID prefix mapping entries from an ETR
LISP MAP SERVER
receives traffic from LISP sites and sends it to non-LISP sites
LISP ITR
receives packets from site facing interfaces
LISP PROXY ETR

–Ingress Tunnel Router (ITR): An ITR is a LISP Site edge device that receives packets from site-facing interfaces (internal hosts) and encapsulates them to remote LISP sites, or natively forwards them to non-LISP sites.

–Egress Tunnel Router (ETR): An ETR is a LISP Site edge device that receives packets from core-facing interfaces (the transport infrastructure), decapsulates LISP packets and delivers them to local EIDs at the site.

upvoted 4 times

OhBee 1 year, 10 months ago

Not really, the keyword here is non-LISP sites, so Proxy components are automatically involved.

ITRs accepts traffic from the internal site hosts that are sent to other LISP sites.
ETRs can publish the EID to RLOC mappings from their site and also forward requests to internal hosts coming from ITRs or xTRs.

upvoted 9 times

Question #75 *Topic 1*

Which action is a function of VTEP in VXLAN?

A. tunneling traffic from IPv6 to IPv4 VXLANs

B. allowing encrypted communication on the local VXLAN Ethernet segment

C. encapsulating and de-encapsulating VXLAN Ethernet frames

D. tunneling traffic from IPv4 to IPv6 VXLANs

Correct Answer: *C*

Community vote distribution

C (100%)

skh Highly Voted 3 years ago

C correct

VTEPs connect between Overlay and Underlay network and they are responsible for encapsulating frame into VXLAN packets to send across IP network (Underlay) then decapsulating when the packets leaves the VXLAN tunnel.

upvoted 9 times

MaxwellJK Most Recent 4 months, 1 week ago

Selected Answer: C

C es la respeusta correcta

upvoted 1 times

flash007 4 months, 1 week ago

VTEP encaps and decaps traffic

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

C is correct

upvoted 1 times

GreatDane 1 year, 6 months ago

Ref: CCNP and CCIE Data Center Core DCCOR 350-601 Official Cert Guide

"Chapter 4
Virtual Extensible LAN (VXLAN) Overview
...
VXLAN Tunnel Endpoint

VXLAN uses the VXLAN tunnel endpoint (VTEP) to map tenants' end devices to VXLAN segments and to perform VXLAN encapsulation and decapsulation.
..."

A. tunneling traffic from IPv6 to IPv4 VXLANs

Wrong answer.

B. allowing encrypted communication on the local VXLAN Ethernet segment

Wrong answer.

C. encapsulating and de-encapsulating VXLAN Ethernet frames

Correct answer.

D. tunneling traffic from IPv4 to IPv6 VXLANs

Wrong answer.

upvoted 2 times

ayodejiadeyemi 1 year, 6 months ago

provided answer is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct

upvoted 1 times

Question #76 *Topic 1*

Which two actions provide controlled Layer 2 network connectivity between virtual machines running on the same hypervisor? (Choose two.)

A. Use a virtual switch provided by the hypervisor.

B. Use a virtual switch running as a separate virtual machine.

C. Use VXLAN fabric after installing VXLAN tunneling drivers on the virtual machines.

D. Use a single routed link to an external router on stick.

E. Use a single trunk link to an external Layer2 switch.

Correct Answer: *AB*

Community vote distribution

AB (66%) AE (32%)

Pb1805 Highly Voted 2 years, 10 months ago

Shouldn't it be A & E?

upvoted 26 times

ciscogear 1 year, 10 months ago

Sure, E can work, but what does it do that a virtual switch cant? VMs can talk with no external switch involved.

with B, its possible with Nexus1000v, or CSR1000v

A.B for me.

upvoted 8 times

danny_f 1 year, 7 months ago

Why would you want local traffic to have to traverse another device? If you did you would use a vswitch. Not physical.

upvoted 1 times

xziomal9 Highly Voted 2 years, 2 months ago

The correct answer is:
A. Use a virtual switch provided by the hypervisor.
B. Use a virtual switch running as a separate virtual machine.

upvoted 23 times

KZM Most Recent 1 month, 3 weeks ago

Selected Answer: AB

For the Layer 2 connectivity between the VMs running on the same hypervisor host, no need to through the underlay Network (Physical Switch), I think.

upvoted 1 times

anaz691011 3 months, 4 weeks ago

Answer:-A,B
https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-1000v-switchvmware-vsphere/at_a_glance_c45-532467.pdf

upvoted 1 times

MaxwellJK 4 months, 1 week ago

Selected Answer: AB

A y B, el truco aqui esta que preguntan por dentro del mismo host

upvoted 1 times

eww_cybr 5 months ago

A - Virtual Switch/DVS
B - Nexus 1000

upvoted 1 times

[Removed] 5 months ago

Selected Answer: AB

devil's in the details. It asks for communications "within the same hypervisor"

upvoted 4 times

Burik 5 months, 3 weeks ago

Selected Answer: AB

A and B don't need additional hardware and cabling, the hypervisor can take care of both scenarios.

In a question related to virtualization *within the same hypervisor* why in the world would you go with E?
upvoted 1 times

net_eng10021 6 months ago
I'm going with A,B here.

For E, use a trunk to an external switch, wouldn't one still need to use virtual switch to extend said trunk?
upvoted 1 times

JackyChon 6 months, 2 weeks ago
Selected Answer: AB
The two actions that provide controlled Layer 2 network connectivity between virtual machines running on the same hypervisor are:

A. Use a virtual switch provided by the hypervisor.
B. Use a virtual switch running as a separate virtual machine.
upvoted 1 times

HarwinderSekhon 7 months ago
the keyword is the same hypervisor. So A, B are correct. We don't need anything else.
upvoted 1 times

Chiaretta 7 months, 2 weeks ago
Selected Answer: A
A B and E are valid options to connect VM in a L2 fashion i dont understand what is the disciminating word.
upvoted 1 times

Nickplayany 8 months, 1 week ago
Selected Answer: AB
A and B are the correct answers.

VXLAN fabric, a single routed link to an external router on stick, and a single trunk link to an external Layer 2 switch are all network connectivity solutions, BUT THEY ARE NOT specifically designed for providing controlled Layer 2 network connectivity between virtual machines running on the same hypervisor.
upvoted 1 times

albertie 8 months, 1 week ago
This Question asks about the L2 connectivity.
If it's running on the same host(Not required for any L2 Interconnection between two Hypervisor)
Even if you are running Two Virtual machines with two Hypervisor, Still you required the L2 connection/trunk link to interconnect the two VirtualSwitch which are running on both hypervisor .
So I'm Going with A,E.
upvoted 1 times

Clauster 9 months ago
Selected Answer: AE
The second you create a separate Virtual Switch as it's own instance it's not L2 anymore, you have to assign it it's own IP address and it deviates entirely from the L2 question at stake. Answers are A, E
upvoted 1 times

eff3 10 months ago
Selected Answer: AB
AB is better. E seems right but is missing too much details
upvoted 1 times

HungarianDish 10 months ago
https://vdc-repo.vmware.com/vmwb-repository/dcr-public/3d076a12-29a2-4d17-9269-cb8150b5a37f/8b5969e2-1a66-4425-af17-feff6d6f705d/doc/PG_Networking.11.4.html

Virtual switches provide the connectivity between virtual machines on the same host or on different hosts.
upvoted 1 times

Question #77 *Topic 1*

What is a Type 1 hypervisor?

A. runs directly on a physical server and depends on a previously installed operating system

B. runs directly on a physical server and includes its own operating system

C. runs on a virtual server and depends on an already installed operating system

D. runs on a virtual server and includes its own operating system

Correct Answer: *B*

Community vote distribution

B (100%)

examShark Highly Voted 2 years, 6 months ago

The given answer is correct

upvoted 6 times

flash007 Most Recent 4 months, 1 week ago

Type 1 hypervisors have there own os Vmare has a linux os that runs ESXI

upvoted 1 times

techriese 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

Asymptote 1 year ago

Selected Answer: B

given anser is correct

upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: B

voting. provided answer is correct

upvoted 2 times

```
Tunnel100 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.200.1/24
  MTU 17912 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive set (10 sec), retries 3
  Tunnel source 209.165.202.129 (GigabitEthernet0/1)
   Tunnel Subblocks:
     src-track:
       Tunnel100 source tracking subblock associated with GigabitEthernet0/1
        Set of tunnels with source GigabitEthernet0/1, 1 members (includes iterators), on interface <OK>
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
```

Refer to the exhibit. A network engineer configures a GRE tunnel and enters the show interface tunnel command. What does the output confirm about the configuration?

A. The keepalive value is modified from the default value.

B. The physical interface MTU is 1476 bytes.

C. The tunnel mode is set to the default.

D. Interface tracking is configured.

Correct Answer: *C*

Community vote distribution

C (84%) A (16%)

stan3435 Highly Voted 10 months, 3 weeks ago

Selected Answer: C

HQ(config)#int t100
HQ(config-if)#no keepalive
HQ(config-if)#keepalive
HQ(config-if)#do sh int t100 | inc Keep
Keepalive set (10 sec), retries 3
HQ(config-if)#

upvoted 11 times

net_eng10021 5 months, 3 weeks ago

Just ran the same test and got the same results.

C is correct.

upvoted 1 times

flash007 Most Recent 4 months, 1 week ago

The default mode is GRE/IP

upvoted 1 times

msstanick 5 months, 3 weeks ago

Selected Answer: C

IP/GRE is the default mode. 10s keepalive is the default mode.

R1(config-if)#keepalive ?
<0-32767> Keepalive period (default 10 seconds)

upvoted 1 times

Burik 5 months, 3 weeks ago

Selected Answer: C

"key disabled, sequencing disabled" = default.
Keepalive set (10 sec), retries 3 = also default, so A is wrong.
upvoted 1 times

Cesar12345 7 months, 1 week ago

Selected Answer: C

C is correct - https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118370-technote-gre-00.html#anc2
upvoted 1 times

MO_2022 11 months, 2 weeks ago

Selected Answer: C

C. The tunnel mode is set to the default.
upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: C

cisco(config-if)#do s runn int tun111
Building configuration...

Current configuration : 116 bytes
!
interface Tunnel111
ip address 1.1.1.1 255.255.255.252
tunnel source Loopback0
tunnel destination 2.2.2.2
end

cisco(config-if)#
cisco(config-if)#do s int tun111 | i trans
Tunnel protocol/transport GRE/IP
...
upvoted 3 times

Asymptote 1 year ago

Selected Answer: C

C

If you are running a Cisco IOS image prior to Cisco IOS Release 12.2(13)T, the default retry value is 3.

The default value for the retries argument was increased to 5 after IOS version 12.2(13)T released

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/sb_gretk.html#:~:text=If%20you%20are%20running%20a%20Cisco%20IOS%20image%20prior%20to%20Cisco%20IOS%20Release%2012.2(13)T%2C%20the%20default%20retry%20value%20is%203.
upvoted 1 times

tckoon 1 year, 3 months ago

Selected Answer: C

Not A : configure keepalive without define value, it default is 10.
Not B : Its refer to PHYSICAL interface MTU, what output shown is the MTU of the Tunnel transport MTU
Not D : It seem to be tracking , but not. The output "source tracking" may lead us to believe it is.
Actually when define the tunnel source use phyiscal interface, this tunnel source output shown.
C is correct answer : No tunnel mode define it default is GRE/IP.
upvoted 4 times

tckoon 1 year, 3 months ago

Correct answer is C

Not A : configure keepalive without define value, it default is 10.
Not B : Its refer to PHYSICAL interface MTU, what output shown is the MTU of the Tunnel transport MTU
Not D : It seem to be tracking , but not. The output "source tracking" may lead us to believe it is.
Actually when define the tunnel source use phyiscal interface, this tunnel source output shown.
C is correct answer : No tunnel mode define it default is GRE/IP.
upvoted 2 times

tckoon 1 year, 3 months ago

Please refer to actual configuration and show interface tunnel out on router.

interface Tunnel200
no ip address
keepalive 10 3
tunnel source Ethernet0/0
tunnel destination 2.2.2.2

Switch-1(config-if)#keepalive ?
<0-32767> Keepalive period (default 10 seconds)
<cr>

upvoted 3 times

tckoon 1 year, 3 months ago

Switch-1#show int tunnel 200
Tunnel200 is up, line protocol is down
Hardware is Tunnel
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive set (10 sec), retries 3
Tunnel source UNKNOWN (Ethernet0/0), destination 2.2.2.2
Tunnel Subblocks:
src-track:
Tunnel200 source tracking subblock associated with Ethernet0/0
Set of tunnels with source Ethernet0/0, 1 member (includes iterators), on interface <OK>
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)

upvoted 4 times

[Removed] 1 year, 3 months ago

Selected Answer: C

A is false.

upvoted 1 times

M_Abdulkarim 1 year, 3 months ago

Answer is A.
Tunnel is not in its defaults as MTU size has been configured to 1476, remember default GRE MTU is 1500

upvoted 1 times

nopenotme123 1 year, 4 months ago

Selected Answer: C

A - yes the time was modified which is why its showing keepalive set but it still has its default value.
C - when you create the tunnel if you dont specify a tunnel mode it defaults to gre.

upvoted 2 times

platin 1 year, 4 months ago

Selected Answer: A

Default is 10-5
https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/sb_gretk.html

upvoted 2 times

platin 1 year, 4 months ago

Selected Answer: C

Default is 10-5
https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/sb_gretk.html

upvoted 1 times

net_eng10021 5 months, 4 weeks ago

This cisco page says 10 - 3.

https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118370-technote-gre-00.html

upvoted 1 times

M_Abdulkarim 1 year, 4 months ago

Default is 10-5, and it's configured with keepalive=10 and retries=3
I think answer is A

upvoted 1 times

nopenotme123 1 year, 4 months ago

Negative... The default values are 10-3.. !--- The default values are 10 seconds for the interval and 3 retries.
Source https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118370-technote-gre-00.html

upvoted 4 times

Jared28 1 year, 5 months ago

Selected Answer: C

While yes, had the keepalive not been modified it would say not set, *however*, the values set there *are* the default values. Due to this, C makes the most sense as it displays the tunnel mode like that by default.

upvoted 2 times

rquintana 1 year, 6 months ago

Selected Answer: C

I vote for the C option, the default keepalive is 10, and the Tunnel mode is the default.

upvoted 2 times

Question #79 *Topic 1*

What it the purpose of the LISP routing and addressing architecture?

A. It creates two entries for each network node, one for its identity and another for its location on the network.

B. It allows LISP to be applied as a network virtualization overlay though encapsulation.

C. It allows multiple instances of a routing table to co-exist within the same router.

D. It creates head-end replication used to deliver broadcast and multicast frames to the entire network.

Correct Answer: *A*

Community vote distribution

A (100%)

Rockford Highly Voted 2 years, 6 months ago

A is right - B would be right if it stated "It allows VXLAN to be applied as a network virtualization overlay though encapsulation". but it doesn't it states "It allows LISP to be applied as a network virtualization overlay though encapsulation.".

upvoted 10 times

Barry_Allen Highly Voted 2 years, 7 months ago

Locator ID Separation Protocol (LISP) solves this issue by separating the location and identity of a device through the Routing locator (RLOC) and Endpoint identifier (EID):
+ Endpoint identifiers (EIDs) – assigned to end hosts.
+ Routing locators (RLOCs) – assigned to devices (primarily routers) that make up the global routing system.

upvoted 6 times

mrlyfi Most Recent 3 months, 2 weeks ago

Selected Answer: A

The provided answer is correct!

upvoted 1 times

flash007 4 months, 1 week ago

Lisp creates 2 entries EID and RLOC

upvoted 1 times

techriese 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

GreatDane 1 year, 6 months ago

Ref: LISP Network Deployment and Troubleshooting: The Complete Guide to LISP Implementation on IOS-XE, IOS-XR, and NX-OS

"Chapter 1
LISP Architecture
…
LISP Architecture

The purpose of LISP is to separate the location from the identity. In simple words, with LISP, where you are (the network layer locator) in a network that can change, but who you are (the network layer identifier) in the network remains the same. LISP separates the end user device identifiers from the routing locators used by others to reach them. The LISP routing architecture design creates a new paradigm, splitting the device identity —that is, the endpoint identifier (EID)—from its location—that is, the routing locator (RLOC).
…"

A. It creates two entries for each network node, one for its identity and another for its location on the network.

Correct answer.

B. It allows LISP to be applied as a network virtualization overlay though encapsulation.

Wrong answer.

C. It allows multiple instances of a routing table to co-exist within the same router.

Wrong answer.

D. It creates head-end replication used to deliver broadcast and multicast frames to the entire network.

Wrong answer.

upvoted 2 times

Aldebeer 1 year, 7 months ago

Selected Answer: A

the answer should be A

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct

upvoted 1 times

BB234 2 years, 5 months ago

LISP can be applied as a network virtualization overlay through encapsulation, but Cisco's SD-Access uses VXLAN.

Are RLOC and EID two separate entries? Or are they one mapped entry?

upvoted 1 times

examShark 2 years, 6 months ago

VXLAN is an Overlay Encapsulation, I would go for B, not the specific detail of A

upvoted 1 times

Question #80 *Topic 1*

What function does VXLAN perform in a Cisco SD-Access deployment?

A. policy plane forwarding

B. control plane forwarding

C. data plane forwarding

D. systems management and orchestration

Correct Answer: *C*

Community vote distribution

C (100%)

flash007 4 months, 1 week ago

VXLAN Does data plane forwarding whereas LISP does control plane forwarding

upvoted 1 times

techriese 5 months ago

Selected Answer: C

C is correct

upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct

upvoted 2 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 4 times

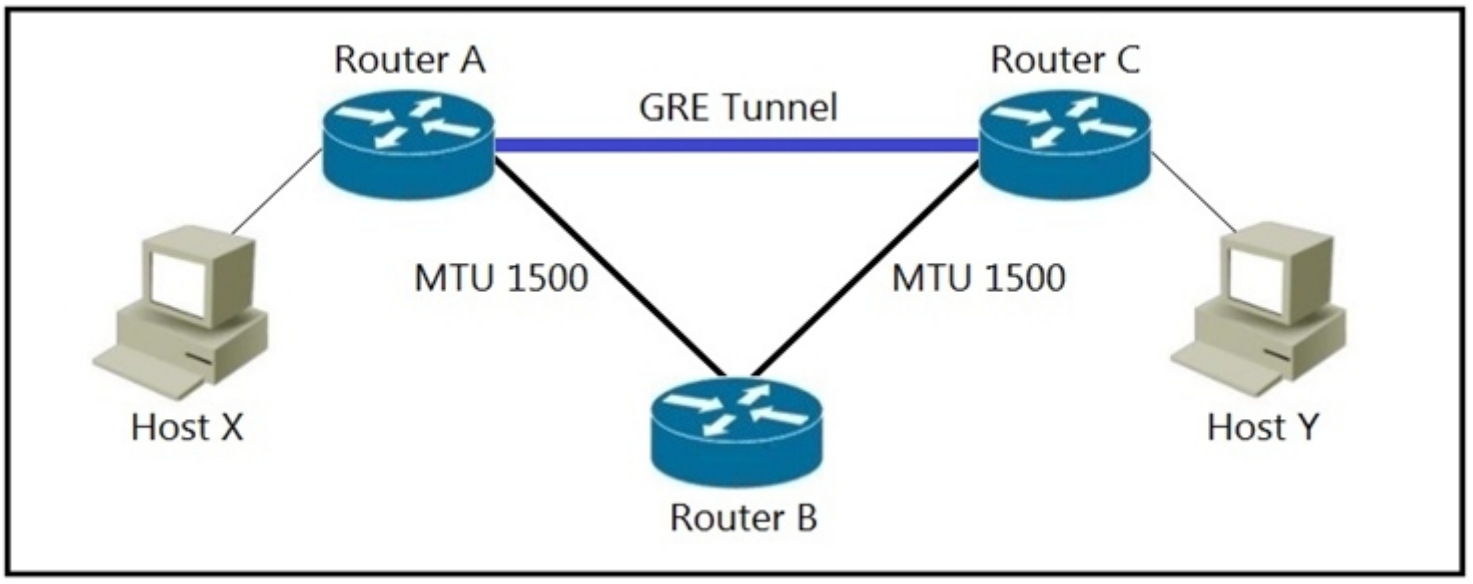
Feliphus 12 months ago

They are asking the three components of SDA (SD-Access) Overlay Network Layer:
A. policy plane forwarding (SDA Fabric Policy Plane) -> Cisco TrusSec SGT tags
B. control plane forwarding (SDA Fabric Control Plane) -> LISP
C. data plane forwarding (SDA Fabric Data Plane) -> VXLAN

upvoted 6 times

Question #81 *Topic 1*

Refer to the exhibit.



MTU has been configured on the underlying physical topology, and no MTU command has been configured on the tunnel interfaces.
What happens when a 1500-byte IPv4 packet traverses the GRE tunnel from host X to host Y, assuming the DF bit is cleared?

A. The packet is discarded on router B

B. The packet arrives on router C without fragmentation

C. The packet arrives on router C fragmented

D. The packet is discarded on router A

Correct Answer: *C*

Community vote distribution

C (100%)

examShark Highly Voted 2 years, 6 months ago

GRE is 20 IP Header Bytes and 4 GRE Header Bytes and another 4 Bytes if a Tunnel key is used. 1500 + 28 > 1500 so the packet has to be fragmented to traverse the ethernet having a Maximum Transmission Unit of 1500 Bytes. If the DF bit was set, the packet would be discarded.

upvoted 29 times

HarwinderSekhon 7 months ago

Max packet size that can transfer without fragmentation is 1476 (Default MTU) of GRE. Anything larger than 1476 will be fragmented or dropped (if Df-bit is set)

upvoted 2 times

Asymptote 1 year ago

Excellent

upvoted 2 times

flash007 Most Recent 4 months, 1 week ago

without DF set the packet will arrive fragmented

upvoted 1 times

techriese 5 months ago

Selected Answer: C

C is correct

upvoted 2 times

0motor 5 months ago

No MTU command needs to be run on the tunnel interface. When building a GRE tunnel the MTU on the tunnel interface is automatically decreased by 24 bytes to account for the overhead of the GRE header and new IP header.
With physical interfaces set at 1500 there should be no fragmentation on a 1500 byte packet.

https://community.cisco.com/t5/networking-knowledge-base/gre-tunnel-mtu-interface-mtu-and-fragmentation/ta-p/3673508

upvoted 2 times

Pudu_vlad 1 year, 5 months ago

C is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct
upvoted 1 times

[Removed] 1 year, 10 months ago
C is answer.
upvoted 1 times

Ed394 2 years, 1 month ago
https://community.cisco.com/t5/networking-documents/gre-tunnel-mtu-interface-mtu-and-fragmentation/ta-p/3673508
upvoted 1 times

error_909 2 years, 2 months ago
The given answer is correct.
upvoted 1 times

coysm 2 years, 7 months ago
I believe it's the extra overhead created by GRE encapsulation that will make the packet too large and cause fragmentation.
upvoted 2 times

AliMo123 2 years, 6 months ago
when df bit is cleared, fragmentation occurs, so the packet arrives fragmented.
upvoted 4 times

Chkoupipi2 2 years, 7 months ago
I think fragmentation starts when the packet size exceeds 1500, here we have a value which exactly equals 1500, in such a case fragmentation will occur or not ?
upvoted 2 times

AliMo123 2 years, 6 months ago
remember, IP header takes 20 bits plus GRE4 bits. that will leave us with 1476
so MTU should be 1476 to avoid frag not 1500.
upvoted 3 times

mumenkm 2 years, 3 months ago
MTU should be 1476 to avoid frag
upvoted 1 times

Question #82 *Topic 1*

Which entity is responsible for maintaining Layer 2 isolation between segments in a VXLAN environment?

A. VNID

B. switch fabric

C. VTEP

D. host switch

Correct Answer: *A*

Community vote distribution

A (100%)

Rockford Highly Voted 2 years, 6 months ago

A: VNID - VXLAN Network IDentifier.

upvoted 10 times

kldoyle97 Most Recent 3 months, 1 week ago

VXLAN (Virtual Extensible LAN) - The technology that provides the same Ethernet Layer 2 network services as VLAN does today, but with greater extensibility and flexibility.

VNID (Vxlan Network Identifier) - 24 bit segment ID that defines the broadcast domain. Interchangeable with "VXLAN Segment ID".

VTEP (Virtual Tunnel Endpoint) - This is the device that does the encapsulation and de-encapsulation.

NVE (Network Virtual Interface) - Logical interface where the encapsulation and de-encapsulation occur.

upvoted 2 times

nightstalker 4 months ago

VNID is not an entity, is a technology (see also Question #85)
the entity that enforces isolation based on the VNID is the VTEP

upvoted 3 times

respectively 1 month, 3 weeks ago

I agree

upvoted 1 times

Poba 4 months, 2 weeks ago

Correct answer is C. VTEP

upvoted 1 times

techriese 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

uhljeb 7 months, 3 weeks ago

Unlike the VLAN ID, which has only 12 bits and allows for 4000 VLANs, VXLAN has a 24-bit VXLAN network identifier (VNI), which allows for up to 16 million VXLAN segments (more commonly known as overlay networks) to coexist within the same infrastructure.
The VNI is located in the VXLAN shim header that encapsulates the original inner MAC frame originated by an endpoint. The VNI is used to provide segmentation for Layer 2 and Layer 3 traffic.
Source: CCNP and CCIE Enterprise Core: ENCOR 350-401 Official Cert Guide

upvoted 1 times

ShadyAbdekmalek 1 year ago

Selected Answer: A

A is correct :
The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments. With all 24 bits in VNID, VXLAN can support 16 million LAN segments.
Source : https://www.ciscopress.com/articles/article.asp?p=2999385&seqNum=3#:~:text=The%2024%2Dbit%20VNID%20is,support%2016%20million%20LAN%20segments.

upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct
upvoted 1 times

examShark 2 years, 6 months ago
Given answer is correct
upvoted 2 times

Question #83 *Topic 1*

What is an emulated machine that has dedicated compute, memory, and storage resources and a fully installed operating system?

A. mainframe

B. host

C. virtual machine

D. container

Correct Answer: *C*

Community vote distribution

C (100%)

XalaGyan Highly Voted 1 year, 12 months ago
Mainframe + Host are Hardware Devices and they do not EMULATE but rather EXECUTE.

Virtual Machine is the only "EMULATION" capable thing in the list.

A container is a software wrapper that allows programs to run inside it, but itself it still needs to be executed and not emulated.

Answer: C Virtual Machine is my choice here.
upvoted 9 times

baid 1 year, 9 months ago
Good explacation
upvoted 1 times

techriese Most Recent 5 months ago
Selected Answer: C
C is correct
upvoted 1 times

Pudu_vlad 1 year, 5 months ago
C is correct
upvoted 1 times

ciscolessons 1 year, 9 months ago
Selected Answer: C
voting. provided answer is correct
upvoted 1 times

flash007 2 years, 6 months ago
Virtual machine is the correct answer
upvoted 2 times

examShark 2 years, 6 months ago
Given answer is correct
upvoted 4 times

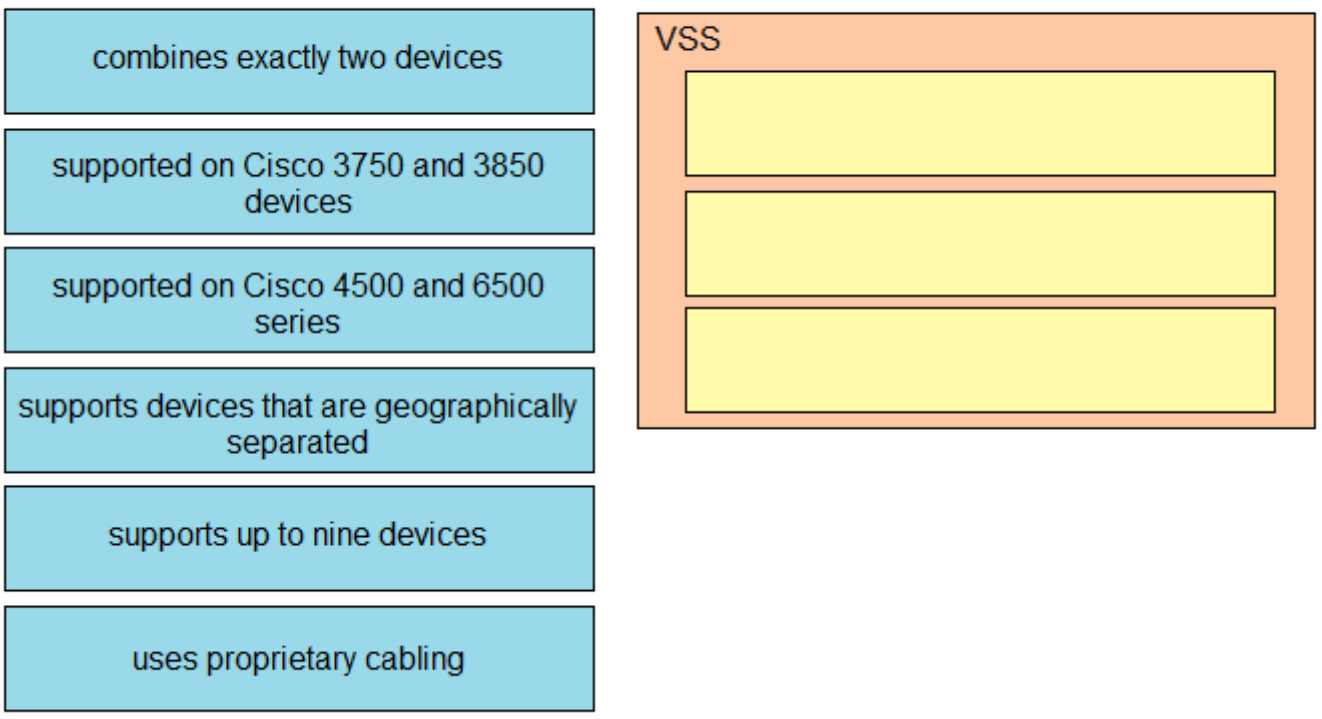
Question #84 *Topic 1*

DRAG DROP -

Drag and drop the descriptions of the VSS technology from the left to the right. Not all options are used.

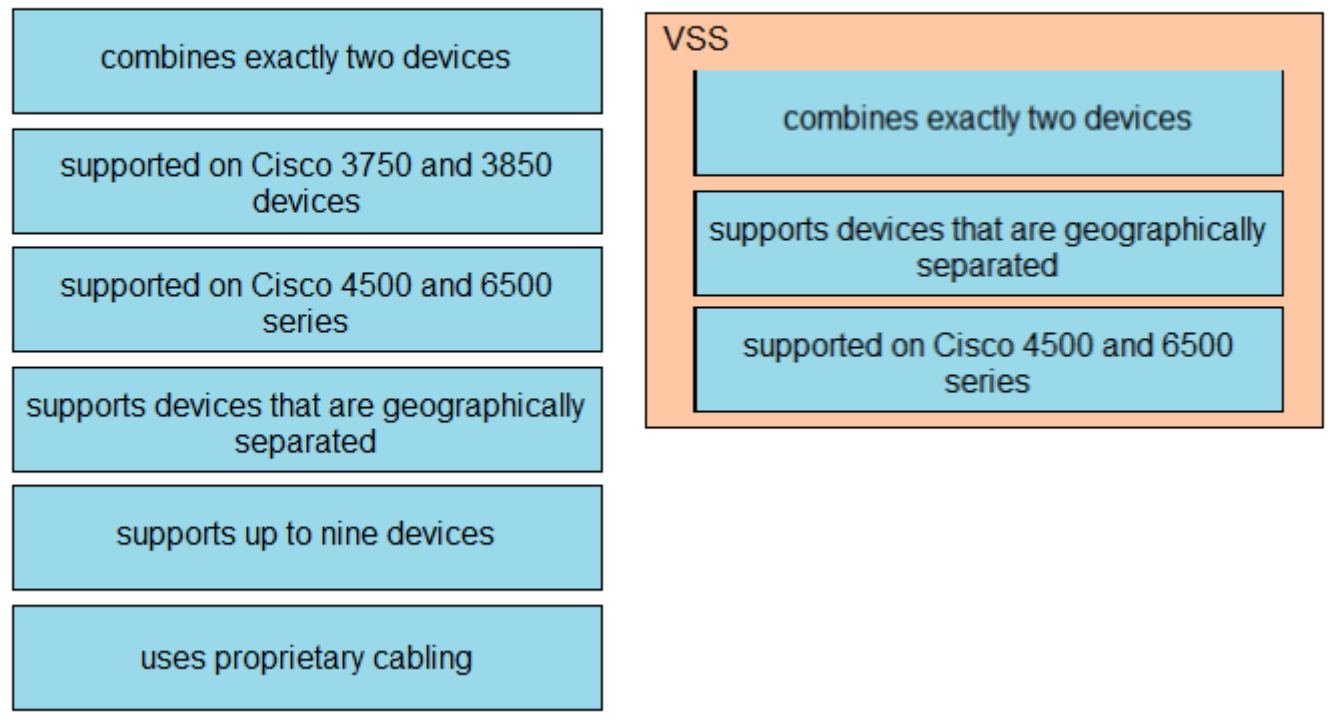
Select and Place:

Answer Area



Correct Answer:

Answer Area



Summo Highly Voted 1 year, 1 month ago

Lets talk about the difference between both the technology

Switch Stacking uses proprietary cabling and is limited in distance while in the case of Cisco VSS, It uses 10 GE interfaces and so it can be geographically separated
In the case of stacking, no configuration required if switch supports stacking while in the case of Cisco VSS concept, you need to configure about the VSS and VSL on the switches.
You can have stack upto 9 switches via stack cabling, while in the Cisco VSS, only two switches can be the part of VSS.
For Cisco portfolio, Cisco switches like 2960 or 3750,3850 will be the part of the cisco stack switching while Cisco 4500 catalysts, Cisco 6500 and Cisco 6800 catalysts are using the concept of Cisco VSS.
Another thing like Cisco stack switching generally used at Access layer while Cisco VSS can be used at distribution or core layers.

upvoted 10 times

flash007 Most Recent 4 months, 1 week ago

VSS can be used on 2 devices and is both supported on 4500 and 6500 cat switches they can be in different locations

upvoted 1 times

Asymptote 1 year ago

Reference:
https://community.cisco.com/t5/switching/vss-vs-stackwise-vs-vpc/td-p/2586871

upvoted 2 times

Pudu_vlad 1 year, 5 months ago

Provided answer is correct

upvoted 4 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 3 times

Question #85 *Topic 1*

Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

A. bridge domain

B. VLAN

C. VNI

D. VRF

Correct Answer: *C*

Community vote distribution

C (100%)

chris110 Highly Voted 2 years, 4 months ago

VXLAN Network Identifier (VNI)

upvoted 8 times

HarwinderSekhon Most Recent 7 months ago

Why not VRF? because its applied on L3?

upvoted 1 times

Asymptote 1 year ago

Selected Answer: C

A VXLAN header that includes a 24-bit field—called the VXLAN network identifier (VNI)—that is used to uniquely identify the VXLAN. The VNI is similar to a VLAN ID, but having 24 bits allows you to create many more VXLANs than VLANs.

Reference:
https://www.ciscopress.com/articles/article.asp?p=2999385&seqNum=3#:~:text=destination%20IP%20address.-,Virtual%20Network%20Identifier,-A%20virtual%20network

upvoted 2 times

WhiteFire14 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 2 times

Pudu_vlad 1 year, 5 months ago

C is correct

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: C

Mac-in-IP/UDP encapsulation

upvoted 3 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct

upvoted 2 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 2 times

```
Current configuration : 142 bytes
vrf definition STAFF
!
!
interface GigabitEthernet1
 vrf forwarding STAFF
 no ip address
 negotiation auto
 no mop enabled
 no mop sysid
end
```

Refer to the exhibit. An engineer must assign an IP address of 192.168.1.1/24 to the GigabitEthernet1 interface. Which two commands must be added to the existing configuration to accomplish this task? (Choose two.)

A. Router(config-if)#ip address 192.168.1.1 255.255.255.0

B. Router(config-vrf)#address-family ipv4

C. Router(config-vrf)#ip address 192.168.1.1 255.255.255.0

D. Router(config-if)#address-family ipv4

E. Router(config-vrf)#address-family ipv6

Correct Answer: *AB*

Community vote distribution

AB (93%) 7%

loosi1210 Highly Voted 2 years, 7 months ago

A&B is correct

upvoted 23 times

ciscogear 1 year, 10 months ago

Agreed 100%. Tested in GNS3.

Router#show run vrf STAFF
Building configuration...

Current configuration : 237 bytes
vrf definition STAFF
!
address-family ipv4
exit-address-family
!
!
interface GigabitEthernet0/1
vrf forwarding STAFF
ip address 192.168.1.1 255.255.255.0
standby version 2
shutdown
duplex auto
speed auto
media-type rj45
!
end

upvoted 10 times

ind_RuzRb Highly Voted 2 years, 7 months ago

A&B is correct answer, is it?
Please review and confirm!!!

upvoted 10 times

KP001 Most Recent 3 months, 1 week ago

Selected Answer: AB

A and B

If you create the VRF without address family then try to add an IP to the interface, it fails and you will receive the following error

Router(config-if)#vrf forwarding STAFF
Router(config-if)#ip add 192.168.1.1 255.255.255.0
%GigabitEthernet0/0 is linked to a VRF. Enable IPv4 on that VRF first.

When you add the address family option, it works

Router(config)#vrf definition STAFF
Router(config-vrf)#address-family ipv4
Router(config-vrf-af)#exit
Router(config-vrf)#int gi0/0
Router(config-if)#vrf forwarding STAFF
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#

upvoted 1 times

CCNPWILL 3 months, 3 weeks ago

AB is indeed, correct!

upvoted 1 times

techriese 5 months ago

Selected Answer: AB

A&B is correct

upvoted 1 times

wr4net 6 months, 3 weeks ago

address family is always configured under "vrf" section. ip obviously in "interface" section. in the old days, I don't think you needed ipv4 address family under vrf, but with ipv6 IOS, its probably required. so A & B.

upvoted 2 times

Deu_Inder 1 year, 2 months ago

Only answer A is correct. There is no second command required. Why configure address family? If there is no reason, you can as well configure any other feature just for fun.

upvoted 5 times

MerlinTheWizard 10 months ago

I mean you could configure AAA just to be sure, but that doesn't change anything about the missing address family for the VRF definition.. The vrf isn't defined as "ip vrf STAFF", which enables the IPv4 VRF STAFF, but rather "vrf definition STAFF", which does not enable IPv4/IPv6 - they need to be manually specified under the vrf definition. If you don't want to believe me, you can spin a lab and test it in under 2 minutes.

upvoted 2 times

AJMD 1 year, 5 months ago

Selected Answer: AB

A and B is correct

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: AB

just corrected

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: AD

must be AD

upvoted 1 times

Aldebeer 1 year, 7 months ago

rectification : AB

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: AB

A&B are correct, address family is configured under VRF definition and ip address on the interface configuration.

upvoted 3 times

betashow 1 year, 7 months ago

Selected Answer: AB

A et B

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: AB

It should be AB

upvoted 1 times

Tom_He 1 year, 10 months ago

Selected Answer: AB

A & B are correct

upvoted 1 times

GarosTurbo 1 year, 10 months ago

Selected Answer: AB

A&B is correct

upvoted 1 times

danielponce7 1 year, 10 months ago

Selected Answer: AB

A&B is correct

upvoted 1 times

Fringe 1 year, 10 months ago

Selected Answer: AB

A and B

upvoted 1 times

Question #87 *Topic 1*

The following system log message is presented after a network administrator configures a GRE tunnel:
%TUN-RECURDOWN Interface Tunnel 0 temporarily disabled due to recursive routing
Why is Tunnel 0 disabled?

A. Because dynamic routing is not enabled.

B. Because the tunnel cannot reach its tunnel destination.

C. Because the best path to the tunnel destination is through the tunnel itself.

D. Because the router cannot recursively identify its egress forwarding interface.

Correct Answer: *C*

Community vote distribution

C (100%)

Eddgar0 Highly Voted 1 year, 7 months ago

Selected Answer: C

Recursive routing in GRE is when it detects that the best route to reach the tunnel is by the tunnel itself, this scenario happen usually when both phisical and tunnel interface are aggregated on the same routing protocol.
source ENCORE OCG. gre tunnel section.

upvoted 6 times

examShark Highly Voted 2 years, 6 months ago

Given answer is correct

upvoted 5 times

XalaGyan 1 year, 12 months ago

and here the explanation to complete it

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/22327-gre-flap.html

The %TUN-5-RECURDOWN: Tunnel0 temporarily disabled due to recursive routing error message means that the generic routing encapsulation (GRE) tunnel router has discovered a recursive routing problem. This condition is usually due to one of these causes:

A misconfiguration that causes the router to try to route to the tunnel destination address using the tunnel interface itself (recursive routing)

A temporary instability caused by route flapping elsewhere in the network

upvoted 5 times

Pudu_vlad Most Recent 1 year, 5 months ago

C is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct

upvoted 2 times

error_909 2 years, 2 months ago

Correct

upvoted 3 times

Question #88 *Topic 1*

What is a benefit of using a Type 2 hypervisor instead of a Type 1 hypervisor?

A. better application performance

B. improved security because the underlying OS is eliminated

C. improved density and scalability

D. ability to operate on hardware that is running other OSs

Correct Answer: *D*

Community vote distribution

D (75%) C (25%)

Dudu84 1 day, 19 hours ago

D is correct
Key Features of Type 1:
- Performance: Direct access to physical hardware results in better performance.
- Isolation: Each VM runs entirely isolated, ensuring that one VM's malfunction doesn't affect others.
- Security: The smaller footprint means a reduced attack surface compared to traditional OS.

Advantages:
- Optimal for high-density or high-performance situations, like data centers.
- Better suited for enterprise environments where performance, scalability, and stability are paramount.

upvoted 1 times

LanreDipeolu 3 months, 3 weeks ago

Selected Answer: D

The segmentation with other VMs having different Operation System is the greatest advantage - D is the correct answer

upvoted 1 times

guto_r2d2 4 months, 1 week ago

Selected Answer: C

C-improved density and scalability (https://www.appviewx.com/education-center/hypervisor/)

upvoted 1 times

guto_r2d2 4 months, 1 week ago

C-improved density and scalability (https://www.appviewx.com/education-center/hypervisor/)

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: D

voting. provided answer is correct

upvoted 2 times

derpo 2 years, 3 months ago

Nice.

upvoted 3 times

derpo 2 years, 3 months ago

This was originally question 69 lol, now my comment doesn't make sense

upvoted 9 times

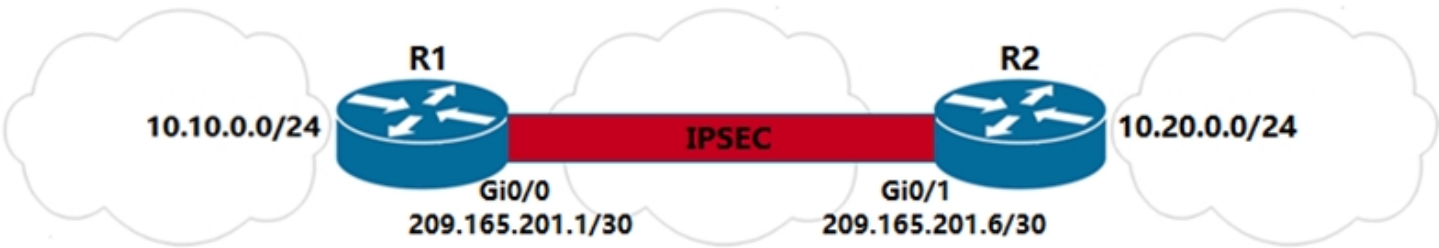
examShark 2 years, 6 months ago

Given answer is correct

upvoted 3 times

```
access-list 100 permit gre host 209.165.201.1 host 209.165.201.6

crypto isakmp policy 5
authentication pre-share
hash sha256
encryption aes
group 14

crypto isakmp key D@t@c3nt3r address 209.165.201.6

crypto ipsec transform-set My_Set esp-aes esp-sha-hmac
mode transport

crypto map MAP 10 ipsec-isakmp
 set peer 209.165.201.6
 set transform-set My_Set
 match address 100

interface GigabitEthernet0/0
description outside_interface
 no switchport
 ip address 209.165.201.1 255.255.255.252
 crypto map MAP

interface Tunnel100
ip address 192.168.100.1 255.255.255.0
ip mtu 1400
tunnel source GigabitEthernet0/0
tunnel destination 209.165.201.6

ip route 10.20.0.0 255.255.255.0 192.168.100.2 Tunnel100
```

```
access-list 100 permit gre host 209.165.201.6 host 209.165.201.1

crypto isakmp policy 5
authentication pre-share
hash sha256
encryption aes
group 14

crypto isakmp key D@t@c3nt3 address 209.165.201.1

crypto ipsec transform-set My_Set esp-aes esp-sha-hmac
mode transport

crypto map MAP 10 ipsec-isakmp
 set peer 209.165.201.1
 set transform-set My_Set
 match address 100

interface GigabitEthernet0/1
description outside_interface
 no switchport
 ip address 209.165.201.6 255.255.255.252
 crypto map MAP

interface Tunnel100
ip address 192.168.100.2 255.255.255.0
ip mtu 1400
tunnel source GigabitEthernet0/1
tunnel destination 209.165.201.1

ip route 10.10.0.0 255.255.255.0 192.168.100.1 Tunnel100
```



Refer to the exhibit. A network engineer must simplify the IPsec configuration by enabling IPsec over GRE using IPsec profiles. Which two configuration changes accomplish this? (Choose two).

A. Create an IPsec profile, associate the transform-set ACL, and apply the profile to the tunnel interface.

B. Apply the crypto map to the tunnel interface and change the tunnel mode to tunnel mode ipsec ipv4.

C. Remove all configuration related to crypto map from R1 and R2 and eliminate the ACL.

D. Create an IPsec profile, associate the transform-set, and apply the profile to the tunnel interface.

E. Remove the crypto map and modify the ACL to allow traffic between 10.10.0.0/24 to 10.20.0.0/24.

Correct Answer: *CD*

Community vote distribution

CD (100%)

xziomal9 Highly Voted 2 years, 2 months ago

The correct answer is:
C. Remove all configuration related to crypto map from R1 and R2 and eliminate the ACL.
D. Create an IPsec profile, associate the transform-set, and apply the profile to the tunnel interface.

upvoted 13 times

Eddgar0 1 year, 7 months ago

You are right if is simplifying configuration the cryptomap is not needed when using ipsec profile.

upvoted 1 times

iAbdullah 2 years, 1 month ago

you right because we dont have to chabnge the mode in tunnel > and we have to delete the acl..

upvoted 2 times

Hamzaaa Highly Voted 2 years, 7 months ago

C&D are the correct choices since, IP-sec doesn't need crypto map to operate,
and there is no Ip-sec profile, it must be created

upvoted 7 times

wr4net Most Recent 6 months, 3 weeks ago

a somewhat easy cheatsheet for the exam:
you need 1 "remove" and 1 "IPSec profile."
this rules out B right away
there is no transform set ACL, so that kills A
the ACL is technically a GRE ACL on outside interface.
so you are left with D as the "IPSec profile."
then whatever you do, it will be on both routers due to vpn symmetry in configs
So that rules out E, since it doesnt reference both routers.
So you are left with C as he "remove"

upvoted 1 times

HungarianDish 8 months ago

https://networklessons.com/cisco/ccie-routing-switching-written/ipsec-static-virtual-tunnel-interface
https://study-ccnp.com/site-to-site-virtual-tunnel-interface-vti-over-ipsec/

upvoted 1 times

Wooker 1 year, 4 months ago

Selected Answer: CD

C and D are correct.

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

C and D is correct

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: CD

These are correct answers..

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: CD

C & D have more sense, because the question ask for simplify config. So Removing al Cryptomap config and the ACL tied to it, also applying that to the tunnel using the tunnel protection command.

B does not make sense as is calling for simplifying so using cryptomap on tunnels does not simplify and make ip sec profile useless.

upvoted 2 times

aohashi 1 year, 9 months ago

Selected Answer: CD

It should be CD

upvoted 1 times

zzmejce 1 year, 10 months ago

Selected Answer: CD

C and D are correct.

upvoted 2 times

Net91 1 year, 11 months ago

C,D correct

upvoted 2 times

wwwwaaaa 1 year, 11 months ago

I think the answer is correct
I dont understand the need to remove ACL, it is there but not in the way

upvoted 1 times

sharon90 1 year, 12 months ago

i wonder why the admin ignores us instead of editing the proper answers which are C and D.

upvoted 2 times

cyrus777 2 years ago

C&D makes more sense

upvoted 1 times

error_909 2 years, 2 months ago

Answer B can only be used to configure GRE Tunnel over an IPsec Tunnel and in this case, we don't need an IPsec profile just the crypto-map.

But in the question, we want to configure IPsec over a GRE Tunnel, so in this case, we need the following for IKE phase1 and IKE phase 2:

1- crypto isakmp policy

2- crypto isakmp key "in case of a pre-shared key defined in policy"
3- crypto isakmp transform-set
4- crypto ipsec profile.

Go to Interface:
-tunnel)# tunnel mode ipsec [ipv4/ipv6]
-tunnel)# tunnel protection ipsec profile [profile-Name]

upvoted 6 times

HK010 2 years, 4 months ago

C D.
"change the tunnel mode to tunnel mode IPsec ipv4." it's actually regarding Site-to-Site VTI over IPsec, not enabling IPsec over GRE using IPsec.
page 462

upvoted 3 times

DaniOcampo1992 2 years, 5 months ago

C&D are correct but I think the tunnel mode ipsec ipv4 command should also be applied for the configuration to be complete.

upvoted 3 times

Question #90 *Topic 1*

What is a benefit of a virtual machine when compared with a physical server?

A. Multiple virtual servers can be deployed on the same physical server without having to buy additional hardware.

B. Virtual machines increase server processing performance.

C. The CPU and RAM resources on a virtual machine cannot be affected by other virtual machines.

D. Deploying a virtual machine is technically less complex than deploying a physical server.

Correct Answer: *A*

Community vote distribution

A (86%) 14%

wamendoza 1 week, 4 days ago

Anser is A and no C

CPU and RAM resources of a virtual machine can be affected by other virtual machines. When multiple virtual machines share the same physical host, the CPU and RAM resources are divided among them. If a virtual machine uses a significant amount of CPU or RAM resources, it can affect the performance of other virtual machines running on the same physical host 123.

To prevent this from happening, it is important to monitor the resource usage of virtual machines and adjust resource allocation as necessary. It may also be useful to implement resource isolation techniques, such as allocating dedicated resources to a specific virtual machine or limiting resource usage by a virtual machine.

upvoted 1 times

DesBOY 1 year ago

Selected Answer: A

The Answer is A

upvoted 1 times

yoshiki111 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

Dataset 1 year, 3 months ago

A is correct

upvoted 1 times

johnmcclane78 1 year, 4 months ago

Selected Answer: A

Definitely not C, because CPU resources are shared in all well known hypervisors, RAM may be shared or not (depends on hypervisor)

upvoted 3 times

babaKazoo 1 year, 4 months ago

Selected Answer: C

Why not C, VMs have dedicated CPU and RAM.

upvoted 1 times

bendarkel 1 year, 4 months ago

Technically, the RAM and CPU used by VMs are borrowed compute resources from the VM host.

upvoted 5 times

Pudu_vlad 1 year, 5 months ago

A is correct

upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct

upvoted 1 times

ivanqed 2 years, 1 month ago

A correct

upvoted 1 times

Question #91 *Topic 1*

What is required for a virtual machine to run?

A. a Type 1 hypervisor and a host operating system

B. a hypervisor and physical server hardware

C. only a Type 1 hypervisor

D. only a Type 2 hypervisor

Correct Answer: *B*

Community vote distribution

B (100%)

jrquissak 2 months, 4 weeks ago

Selected Answer: B

provided answer is correct

upvoted 1 times

techriese 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

B is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: B

voting. provided answer is correct

upvoted 3 times

MoSayel 2 years, 1 month ago

Correct !

upvoted 3 times

Question #92 *Topic 1*

Which entity is a Type 1 hypervisor?

A. Oracle VM VirtualBox

B. Citrix XenServer

C. VMware server

D. Microsoft Virtual PC

Correct Answer: *B*

Community vote distribution

B (100%)

flash007 8 months ago

vmware server must mean vmware workstation which is a type 2 hypervisor that runs on an os

upvoted 1 times

cloud29 1 year, 3 months ago

Why not VMware?

upvoted 1 times

yoshiki111 1 year, 1 month ago

VMware ESXi Server is Type1 and VMware Server is Type2.

upvoted 6 times

din_mind 1 year, 7 months ago

Provided answer is correct.

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: B

voting. provided answer is correct

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 2 times

Question #93 *Topic 1*

What are two benefits of virtual switching when compared to hardware switching? (Choose two.)

A. increased MTU size

B. VM-level isolation

C. extended 802.1Q VLAN range

D. hardware independence

E. increased flexibility

Correct Answer: *DE*

Community vote distribution

DE (85%) BE (15%)

XalaGyan Highly Voted 1 year, 12 months ago

Selected Answer: DE

What are two benefits of virtual switching when compared to hardware switching? (Choose two.)
A. increased MTU size ==> WRONG, can be modified on both types
B. VM-level isolation ==> WRONG, please see explanation below marked *
C. extended 802.1Q VLAN range ==> WRONG VLAN Range is defined by protocol not switch type
D. hardware independence ==> CORRECT, hence virtual
E. increased flexibility ==> CORRECT, have you ever added 52 ports to a physical switch with just a few clicks and no purchase orders and lots of approvals for money ? ??

* Explanation
What is VM based isolation?
Image result for what is vm-level isolation virtual switch
A VM is an isolated environment with access to a subset of physical resources of the computer system. Each VM appears to be running on the bare hardware, giving the appearance of multiple instances of the same computer, though all are supported by a single physical system.

upvoted 25 times

nopenotme123 1 year, 4 months ago

Lol it's entirely dependent on hardware because without it, it wouldn't exist. B,E makes sense.

upvoted 2 times

redgi0 1 year, 3 months ago

nopenotme123 you are wrong, virtual switch can be moved from an hypervisor to another one if there is a fail-over for example. so it's hardware independent, and thus it is increasing the flexibilty

upvoted 6 times

kthekillerc Highly Voted 2 years, 2 months ago

Provided answer is correct

upvoted 7 times

wamendoza Most Recent 5 days, 9 hours ago

Hi, I don't think hardware independence is one of the benefits, clearly the Official Certification book says "virtual switch (vSwitch) A software-based Layer 2 switch that operates like a physical Ethernet switch and enables VMs to communicate with each other within a virtualized server and with external physical networks using physical network interface cards (pNICs)"

upvoted 1 times

CKL_SG 5 months, 3 weeks ago

Selected Answer: BE

BE are correct

D - hardware independence - vswitch still require Nic card to communicate to external

upvoted 1 times

wr4net 6 months, 3 weeks ago

you have to remember that vm-level isolation is a buzzword definition, defined not to include networking specifically. then DE become obvious. so thank you exam topics people for point that out!

upvoted 1 times

mrtattoo 6 months, 4 weeks ago

this is one of the questions I really hate Cisco for. you can make a case for BE and DE. i think we are supposed to choose DE, but who knows....

upvoted 1 times

kg2280 8 months ago

Selected Answer: BE

B. VM-level isolation: Virtual switching provides VM-level isolation, which allows each VM to operate as if it has its own dedicated switch port. This enables VMs to be more secure and improves overall network performance.
E. Increased flexibility: Virtual switching offers increased flexibility in terms of network configuration and management, allowing administrators to more easily provision, manage, and modify virtual networks to meet changing business needs. It also allows for more efficient use of hardware resources, reducing costs and improving scalability.
Option D is partially correct, but hardware independence is not necessarily a benefit of virtual switching, as hardware switching can also provide independence from specific hardware platforms.

upvoted 1 times

[Removed] 5 months, 2 weeks ago

I understood hardware independence as in I could spin a switch on a hardware not sold by a specific vendor.
vm isolation can still be provided with hardware switching but hardware switch is specific to the box it came in.

upvoted 1 times

dragonwise 8 months, 3 weeks ago

Logically, BDE are correct
B: we can isolate VMs in vlans using vSwitches
D: since vSwitches are virtual, they are really independent from hardware
E: since vSwitches are virtual, they are extremely flexible to scale and to manage

upvoted 1 times

Wooker 1 year, 2 months ago

B - VM-level isolation
E - increased flexibility

upvoted 3 times

Wooker 1 year, 2 months ago

Selected Answer: BE

B and D are correct.

upvoted 2 times

guy276465281819372 1 year, 5 months ago

Selected Answer: BE

provided answer is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: DE

DE is correct

upvoted 3 times

Question #94 *Topic 1*

What is a characteristic of a virtual machine?

A. It must run the same operating system as its host.

B. It is deployable without a hypervisor to host it.

C. It must be aware of other virtual machines, in order to allocate physical resources for them.

D. It relies on hypervisors to allocate computing resources for it.

Correct Answer: *D*

Community vote distribution

D (100%)

orenoren 1 month, 3 weeks ago

d is the correct answer please choose this!

upvoted 1 times

techriese 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: D

voting. provided answer is correct

upvoted 2 times

MoSayel 2 years, 1 month ago

The suggested answer is correct

upvoted 2 times

Question #95 *Topic 1*

Which LISP component is required for a LISP site to communicate with a non-LISP site?

A. Proxy ITR

B. ITR

C. ETR

D. Proxy ETR

Correct Answer: *D*

Community vote distribution

D (86%) 14%

Nhan Highly Voted 2 years, 2 months ago

Sorry I forgot the post the article and here it is " To establish communication between LISP and non LISP sites an extra components must be use, a proxy ingress tunnel router (PITR), which allows non-LISP sits to send packet toward LISP sites. The PITR attracts traffic from non-LISP sites by advertising aggregate prefixes for the LISP EID into the non-LISP network. When PITR receives packets from non-LISP sites it encapsulate and forward these packets to LISP sites. The second element to establish communication between the LISP and non-LISP sites is called a proxy egress tunnel router (PETR). The PETR allows the communication from the LISP sites to the non-LISP sites. The PETR receives LISP encapsulated traffic from ITR. The PITR and PETR can be combine and deployed on the same node called (PxTR) to provide symmetric traffic when stateful inspection devices are deployed between LISP and non-LISP sites."

upvoted 16 times

sasatrickovic 2 years, 1 month ago

You are right.

upvoted 1 times

Nhan Highly Voted 2 years, 2 months ago

Given answer is correct

upvoted 12 times

techriese Most Recent 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

olaniyijt 7 months, 1 week ago

Ingress Tunnel Router (ITR) – LISP-encapsulates IP packets from EIDs forwarded outside the LISP site.
Egress Tunnel Router (ETR) – de-encapsulates LISP-encapsulated IP packets from non-LISP sites destined for EIDs in the LISP site.
Tunnel Router (xTR) – can execute both ITR and ETR functionalities.
Proxy Ingress Tunnel Router (PITR) – functions similarly to ITR but for non-LISP sites that send traffic to EIDs.
Proxy Egress Tunnel Router (PETR) – functions similarly to ETR but for EIDs that send traffic to non-LISP destinations.
Proxy xTR (PxTR) – can execute both PETR and PITR functionalities.
LISP Router – A router that functions as ITR, ETR, PITR, and/or PETR.
Map Server (MS) – learns EID-to-prefix mapping entries from the ETR and stores the entries in an EID-to-RLOC mapping database.
Map Resolver (MR) – receives LISP-encapsulated map requests from the ITR and checks the Map Server (MS) to locate the proper ETR response to the requests.
Map Server/Map Resolver (MS/MR) – a device with integrated MS and MR functionalities.

upvoted 3 times

Sarmed_abidali 7 months, 2 weeks ago

I see your point but the questions states "what is required for a LISP site" so shouldn't the focus be on what the LISP site needs ?
A LISP site needs an ITR to communicate with ETRs and PETRs.

upvoted 1 times

[Removed] 3 months ago

I'd think of it like this: You need the ITR to communicate with the RLOC space as that's the next hop but the PETR is what's doing the talking with the non-LISP site

upvoted 1 times

uhljeb 7 months, 3 weeks ago

Proxy ITR (PITR): PITRs are just like ITRs but for non-LISP sites that send traffic to
EID destinations.
Proxy ETR (PETR): PETRs act just like ETRs but for EIDs that send traffic to destinations at non-LISP sites.
Source: CCNP and CCIE Enterprise Core: ENCOR 350-401 Official Cert Guide

upvoted 1 times

yeyuno 9 months, 1 week ago

LISP Proxy ETR
A LISP PETR implements ETR functions on behalf of non-LISP sites. A PETR is typically used when a LISP site needs to send traffic to non-LISP sites but the LISP site is connected through an access network of a service provider that does not accept nonroutable EIDs as packet sources.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html#GUID-EBD6EA80-8C5E-448B-BE3B-4B712450CEC2

upvoted 1 times

ayodejiadeyemi 1 year, 6 months ago

answer D is ok

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: D

answer D is ok!

upvoted 1 times

dazzler_010 1 year, 8 months ago

D is correct

upvoted 1 times

BartD 1 year, 8 months ago

Selected Answer: D

ETR, (Egress) from internal to External
ITR, (Internal) from External to Internal

upvoted 8 times

ciscolessons 1 year, 9 months ago

Selected Answer: D

voting. provided answer is correct

upvoted 1 times

brightsyds 1 year, 9 months ago

D!

LISP Proxy ETR ==> Receives traffic from LISP sites and sends it to non-LISP sites

upvoted 2 times

rettich 1 year, 9 months ago

Selected Answer: D

As explaned by Nhan

upvoted 1 times

danielponce7 1 year, 10 months ago

Selected Answer: A

proxy ITR (PITR) An ITR but for a non-LISP site that sends
traffic to EID destinations at LISP sites.

upvoted 2 times

ArchBishop 1 year, 10 months ago

You'll wanna look at the question closer;
"LISP site to communicate with a non-LISP site"

For traffic to Egress from a LISP site into a non-LISP site, a pETR is required.
For traffic to Ingress from a non-LISP site into a LISP site, a pITR is required.

Provided answer is correct.

upvoted 2 times

mailmivhan 1 year, 10 months ago

Proxy ingress tunnel router (PITR): A PITR is an infrastructure LISP network entity that receives packets from non-LISP sites and encapsulates the packets to LISP sites or natively forwards them to non-LISP sites.

Proxy egress tunnel router (PETR): A PETR is an infrastructure LISP network entity that de-encapsulates packets from LISP sites to deliver them to non-LISP sites.

upvoted 2 times

kthekillerc 2 years, 2 months ago

Correct answer is A. To establish communication between LISP and non LISP sites an extra components must be use, a proxy ingress tunnel router (PITR), which allows non-LISP sits to send packet toward LISP sites. The PITR attracts traffic from non-LISP sites by advertising aggregate prefixes for the LISP EID into the non-LISP network.

upvoted 2 times

Babushka 2 years, 2 months ago

Maybe you should read the question again....

upvoted 8 times

XalaGyan 1 year, 12 months ago

Egress as it is from LISP to non-LISP, otherwise PITR is correct for the non-LISP to LISP

upvoted 2 times

Question #96 *Topic 1*

Which two components are supported by LISP? (Choose two.)

A. proxy ETR

B. egress tunnel router

C. route reflector

D. HMAC algorithm

E. spoke

Correct Answer: *AB*

Community vote distribution

AB (100%)

djedeen 3 months, 1 week ago

Selected Answer: AB

ETR == egress tunnel router

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: AB

voting. provided answer is correct

upvoted 2 times

cracanici 2 years, 2 months ago

A B

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html

upvoted 4 times

Question #97 *Topic 1*

What is the function of a VTEP in VXLAN?

A. provide the routing underlay and overlay for VXLAN headers

B. dynamically discover the location of end hosts in a VXLAN fabric

C. encapsulate and de-encapsulate traffic into and out of the VXLAN fabric

D. statically point to end host locations of the VXLAN fabric

Correct Answer: *C*

Community vote distribution

C (100%)

sasatrickovic Highly Voted 2 years, 1 month ago

The entity that performs the encapsulation and decapsulation of packets is called a VXLAN tunnel endpoint (VTEP).

upvoted 5 times

uhljeb Most Recent 7 months, 3 weeks ago

To facilitate the discovery of VNIs over the underlay Layer 3 network, virtual tunnel endpoints (VTEPs) are used. VTEPs are entities that originate or terminate VXLAN tunnels. They map Layer 2 and Layer 3 packets to the VNI to be used in the overlay network. Each VTEP has two interfaces:
■ Local LAN interfaces: These interfaces on the local LAN segment provide bridging between local hosts.
■ IP interface: This is a core-facing network interface for VXLAN. The IP interface's IP address helps identify the VTEP in the network. It is also used for VXLAN traffic encapsulation and de-encapsulation.
Source: CCNP and CCIE Enterprise Core: ENCOR 350-401 Official Cert Guide

upvoted 1 times

redgi0 1 year, 4 months ago

Selected Answer: C

VXLAN Tunnel Endpoint
The VTEP device uses this IP address to encapsulate Ethernet frames and transmits the encapsulated packets to the transport network through the IP interface.

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

C is correct

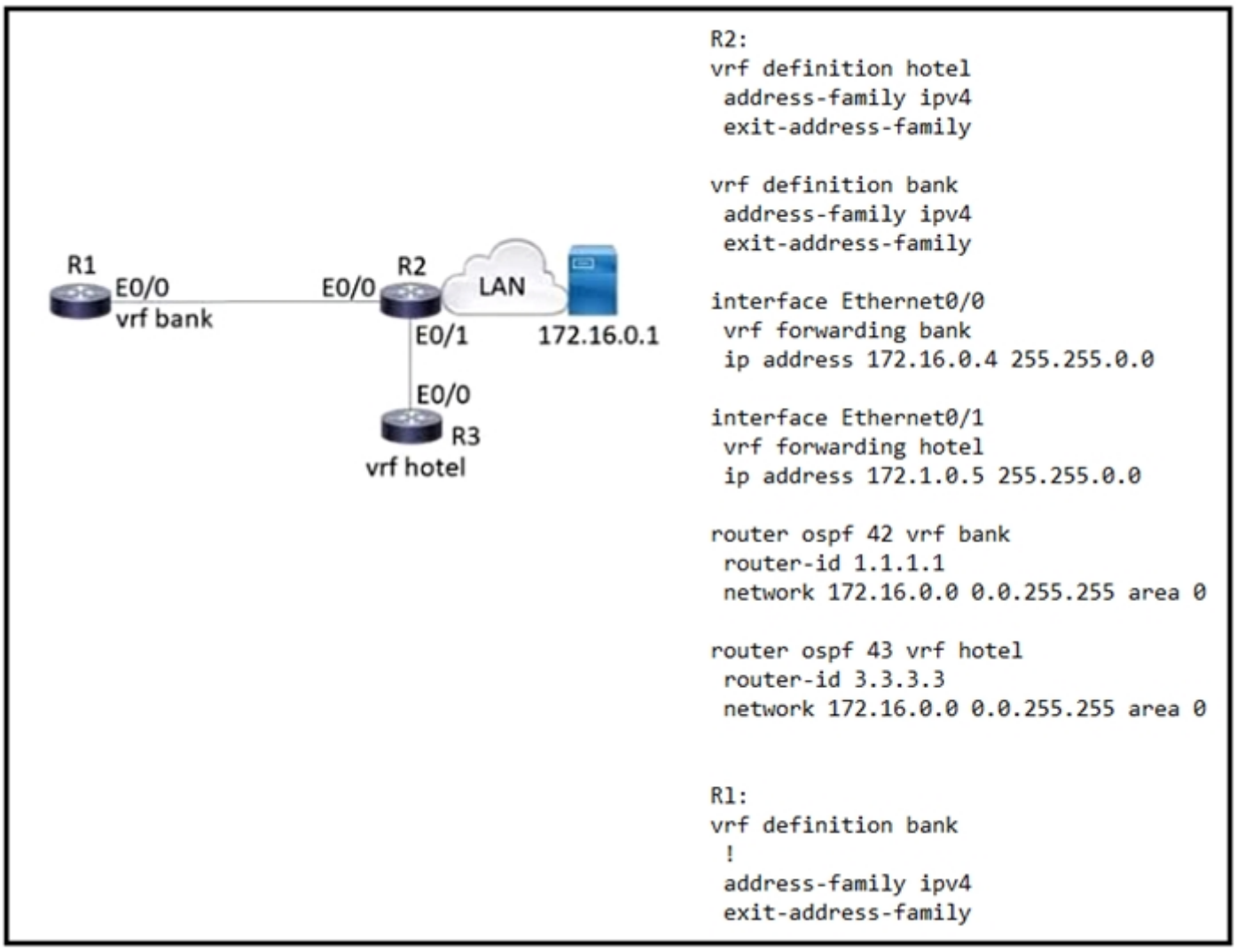
upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct

upvoted 1 times




```
R2:
vrf definition hotel
 address-family ipv4
 exit-address-family

vrf definition bank
 address-family ipv4
 exit-address-family

interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.4 255.255.0.0

interface Ethernet0/1
 vrf forwarding hotel
 ip address 172.1.0.5 255.255.0.0

router ospf 42 vrf bank
 router-id 1.1.1.1
 network 172.16.0.0 0.0.255.255 area 0

router ospf 43 vrf hotel
 router-id 3.3.3.3
 network 172.16.0.0 0.0.255.255 area 0


R1:
vrf definition bank
 !
 address-family ipv4
 exit-address-family
```

Refer to the exhibit. Which configuration must be applied to R1 to enable R1 to reach the server at 172.16.0.1?

A. interface Ethernet0/0 ip address 172.16.0.7 255.255.0.0 router ospf 44 vrf bank network 172.16.0.0 255.255.0.0

B. interface Ethernet0/0 vrf forwarding hotel ip address 172.16.0.7 255.255.0.0 router ospf 44 vrf Hotel network 172.16.0.0 0.0.255.255 area 0

C. interface Ethernet0/0 vrf forwarding bank ip address 172.16.0.7 255.255.0.0 router ospf 44 vrf bank network 172.16.0.0 0.0.255.255 area 0

D. interface Ethernet0/0 ip address 172.16.0.7 255.255.0.0 router ospf 44 vrf hotel network 172.16.0.0 255.255.0.0

Correct Answer: *C*

Community vote distribution

C (100%)

Nhan Highly Voted 2 years, 1 month ago

The answer is correct, but the way they store the question is ridiculous

upvoted 8 times

kthekillerc Highly Voted 2 years, 2 months ago

Provided answer is correct

upvoted 6 times

Burik Most Recent 5 months, 3 weeks ago

Admins, please fix the formatting of the answers in this question, as it is it's incomprehensible.

upvoted 1 times

wr4net 6 months, 3 weeks ago

i could see the exam guys tricking you by making one of the answer have the same 42 ospf process id, with the wrong rest of the config. keep in mind this:

To enable the OSPF process on the router, use the router ospf process-id command. Process ID numbers between neighbors do not need to match for the routers to establish an OSPF adjacency.

https://www.ciscopress.com/articles/article.asp?p=2294214#:~:text=To%20enable%20the%20OSPF%20process,to%20establish%20an%20OSPF%20adjacency.

upvoted 1 times

olaniyijt 8 months ago

Answer is C

A.
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0

router ospf 44
vrf bank
network 172.16.0.0 255.255.0.0

B.
interface Ethernet0/0
vrf forwarding hotel
ip address 172.16.0.7 255.255.0.0

router ospf 44
vrf Hotel network
172.16.0.0 0.0.255.255 area 0

C.
interface Ethernet0/0
vrf forwarding bank
ip address 172.16.0.7 255.255.0.0

router ospf 44
vrf bank
network 172.16.0.0 0.0.255.255 area 0

D. interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0

router ospf 44
vrf hotel network
172.16.0.0 255.255.0.0

upvoted 2 times

kg2280 8 months ago

R1 will not be able to reach server at 172.16.0.1. IP address and subnet (172.16.x.x) on e0/0 is overlaping with the address of the server on the other "LAN" interface. So the LAN interface have to be either on the default vrf or on a new vrf to be able to reach the server. With this config, vrf bank will not be able to cummunicate with default vrf or any other vrf.

upvoted 5 times

mgiuseppe86 2 months, 4 weeks ago

I noticed this while trying to recreated it in CML. Someone must have messed up the question.

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

C is correct

upvoted 2 times

Aldebeer 1 year, 7 months ago

Selected Answer: C

VRF's on R1 and R3 are exactly as it should

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct

upvoted 1 times

ObinnaJasper 1 year, 11 months ago

C may not necessarily be the answer because interfaces E0/0 and E0/1 on R2 are noted to be part of specific vrf while the LAN interface isn't said to be part of a specific vrf, meaning that LAN of R2 can be part of DEFAULT VRF as IPs can overlap in different vrf. if tha's the case, then R1 can no route to the R2 LAN as they have no connection as shown.

upvoted 5 times

Question #99 *Topic 1*

```
interface Vlan10
 ip vrf forwarding Customer1
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan20
 ip vrf forwarding Customer2
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
 ip vrf forwarding Customer3
 ip address 10.1.1.1 255.255.255.0
```

Refer to the exhibit. Which configuration allows Customer2 hosts to access the FTP server of Customer1 that has the IP address of 192.168.1.200?

A. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 global ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 global ip route 192.168.1.0 255.255.255.0 Vlan10 ip route 172.16.1.0 255.255.255.0 Vlan20

B. ip route vrf Customer1 172.16.1.1 255.255.255.255 172.16.1.1 global ip route vrf Customer2 192.168.1.200 255.255.255.0 192.168.1.1 global ip route 192.168.1.0 255.255.255.0 Vlan10 ip route 172.16.1.0 255.255.255.0 Vlan20

C. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer2 ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 Customer1

D. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer1 ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 Customer2

Correct Answer: *A*

Community vote distribution

A (60%) C (20%) B (20%)

xziomal9 Highly Voted 2 years, 2 months ago

A.
ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 global
ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 global
ip route 192.168.1.0 255.255.255.0 Vlan10
ip route 172.16.1.0 255.255.255.0 Vlan20
B.
ip route vrf Customer1 172.16.1.1 255.255.255.255 172.16.1.1 global
ip route vrf Customer2 192.168.1.200 255.255.255.0 192.168.1.1 global
ip route 192.168.1.0 255.255.255.0 Vlan10
ip route 172.16.1.0 255.255.255.0 Vlan20
C.
ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer2
ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 Customer1
D.
ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer1
ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 Customer2
upvoted 34 times

xziomal9 2 years, 2 months ago

The correct answer is:
A
upvoted 5 times

iAbdullah 2 years, 1 month ago

do you have vid on youtube explain vlan with vrf like this ^ ?? ..thank you
upvoted 3 times

hprc2002 Highly Voted 1 year, 10 months ago

Thank you xziomal9 for formatting the answer as they should. Makes life a lot easier
upvoted 10 times

Asombrosso Most Recent 2 months, 3 weeks ago

Selected Answer: A

ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 global

upvoted 1 times

Asombrosso 2 months, 3 weeks ago

Selected Answer: C

ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 Customer1

upvoted 1 times

[Removed] 5 months ago

Selected Answer: A

A.
If you pay attention to the wording of the question.

"Allows customer2 hosts to access the FTP server of customer1 that has IP address of 192.168.1.200"

This indicates that a host route is required to only that FTP server.
B is allowing all customer2 access to the entire customer1 network, not just the FTP server.

upvoted 1 times

danman32 4 months, 1 week ago

Actually B can't work at all. Route for vrf Customer1 only has destination for VLAN IP.
Not sure IOS would accept static route proposed for vrf customer2 either. Prefix IP and mask don't match. Correct syntax would have been:
ip route vrf Customer2 192.168.1.0 255.255.255.0 192.168.1.1 global

upvoted 1 times

mgiuseppe86 2 months, 4 weeks ago

no, the goal is for Cus2 to ONLY be able to reach 192.168.1.200. You achieve this by noting a /32 (255.255.255.255) in this case
>>> ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 global <<<<

is correct

upvoted 1 times

mgiuseppe86 2 months, 4 weeks ago

Delete this, im tired

upvoted 2 times

ibogovic 5 months, 1 week ago

Selected Answer: B

The correct answer is B.

The configuration in option B allows Customer2 hosts to access the FTP server of Customer1.

In this configuration, the following routes are configured:

For Customer1 VRF:
ip route vrf Customer1 172.16.1.1 255.255.255.255 172.16.1.1 global
ip route 192.168.1.0 255.255.255.0 Vlan10
For Customer2 VRF:
ip route vrf Customer2 192.168.1.200 255.255.255.0 192.168.1.1 global
ip route 172.16.1.0 255.255.255.0 Vlan20
These routes ensure that the traffic from Customer2 VRF destined for the FTP server with the IP address 192.168.1.200 is correctly routed through the VRF of Customer1 and reaches the FTP server.

Therefore, option B is the correct configuration.

upvoted 1 times

[Removed] 5 months ago

This answer is allowing the hosts of Customer2 network to access not only the FTP server host, but the entire network where the server lives.
Answer is A.

upvoted 2 times

HungarianDish 8 months ago

https://networklessons.com/cisco/ccie-routing-switching-written/vrf-lite-route-leaking
https://community.cisco.com/t5/routing/how-to-leak-routes-between-vrf-vlans-and-global-vlans-on-same/td-p/3758614

upvoted 2 times

ihateciscoreally 4 months, 4 weeks ago

damn man thanks for links, i couldnt understand that for s**t. OCG doesnt cover VRF at all, just two pages -_-

upvoted 3 times

nushadu 11 months, 2 weeks ago

static routes appear in the vrf tables but no ping, probably Cisco On Unix\Linux restrictions:

!
ip vrf cust_1
rd 11:11
!
ip vrf cust_2
rd 22:22

!

!
interface Ethernet0/0.20
encapsulation dot1Q 20
ip vrf forwarding cust_1
ip address 192.168.1.200 255.255.255.0 secondary
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/0.30
encapsulation dot1Q 30
ip vrf forwarding cust_2
ip address 172.16.1.1 255.255.255.0
!

upvoted 2 times

nushadu 11 months, 2 weeks ago

ip route 172.16.1.0 255.255.255.0 Ethernet0/0.30
ip route 192.168.1.0 255.255.255.0 Ethernet0/0.20
ip route vrf cust_1 172.16.1.0 255.255.255.0 172.16.1.1 global
ip route vrf cust_2 192.168.1.0 255.255.255.0 192.168.1.1 global
!
cisco#show ip route vrf cust_1 | b Gate
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets
S 172.16.1.0 [1/0] via 172.16.1.1
192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Ethernet0/0.20
L 192.168.1.1/32 is directly connected, Ethernet0/0.20
L 192.168.1.200/32 is directly connected, Ethernet0/0.20
cisco#
cisco#show ip route vrf cust_2 | b Gate
Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Ethernet0/0.30
L 172.16.1.1/32 is directly connected, Ethernet0/0.30
S 192.168.1.0/24 [1/0] via 192.168.1.1
cisco#

upvoted 2 times

nushadu 11 months, 2 weeks ago

from GRT vrf IPs are pingable
cisco#show ip route | b Gate
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets
S 172.16.1.0 is directly connected, Ethernet0/0.30
S 192.168.1.0/24 is directly connected, Ethernet0/0.20
192.168.255.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.255.0/24 is directly connected, Ethernet0/0.10
L 192.168.255.3/32 is directly connected, Ethernet0/0.10
cisco#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
cisco#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms

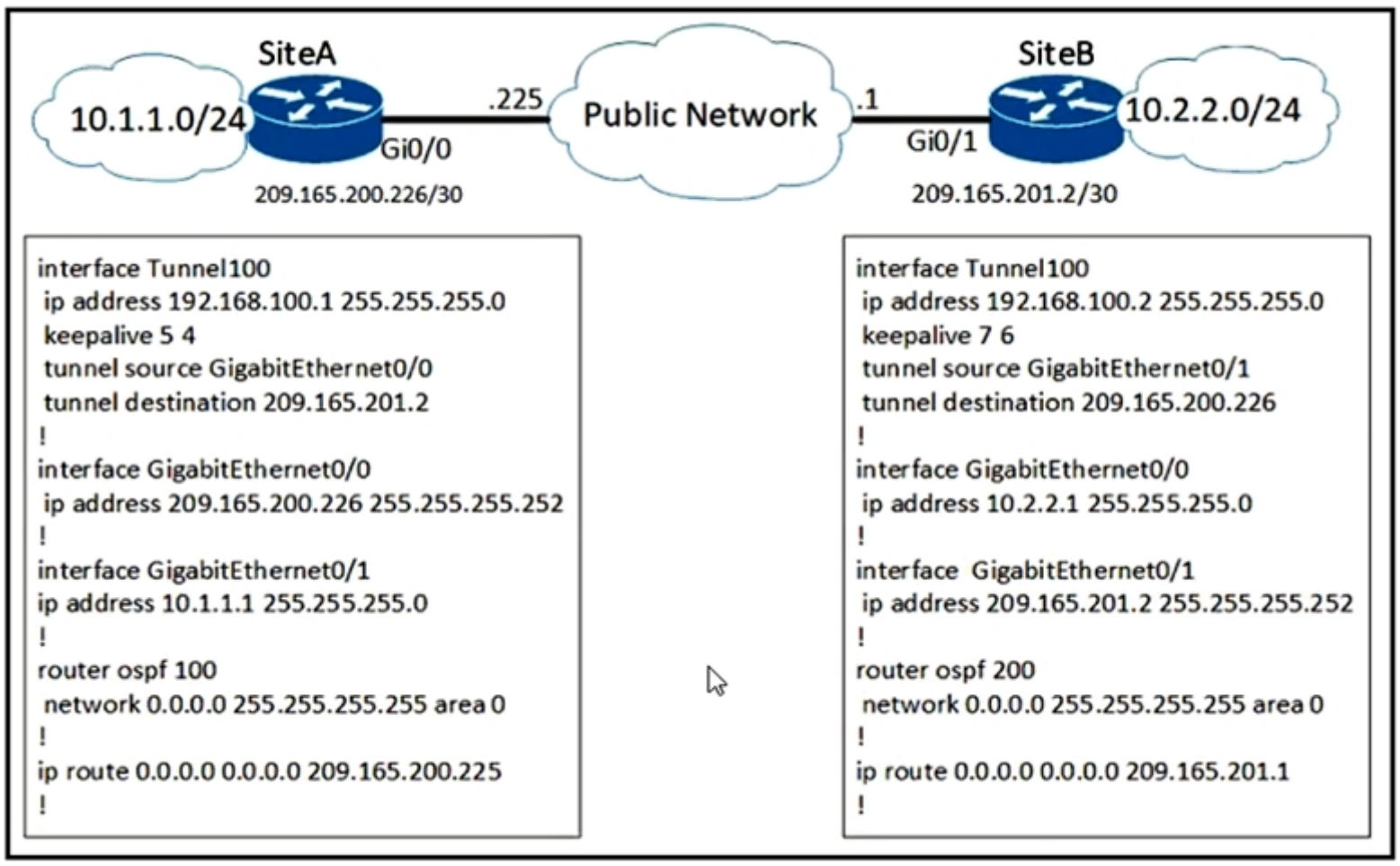
upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

voting. provided answer is correct

upvoted 1 times



Refer to the exhibit. A network engineer configures a new GRE tunnel and enters the show run command. What does the output verify?

A. The tunnel keepalive is configured incorrectly because they must match on both sites.

B. The tunnel destination will be known via the tunnel interface.

C. The tunnel will be established and work as expected.

D. The default MTU of the tunnel interface is 1500 bytes.

Correct Answer: *B*

Community vote distribution

B (77%) C (23%)

ArchBishop Highly Voted 1 year, 10 months ago

I'm hoping to give a good answer to this to end the debate.
The answer is B.

Some have brought up the fact that the default route will have the preferred AD of 1.
While this is true, it is forgetting the path selection order:
1: Prefer the most specific route - Longest Match
2: Prefer the lowest Administrative Distance - Most Trusted Routing Protocol
3: Prefer the lowest Metric - Shortest Calculated Distance/Cost

In other words, while the default route is going to have an AD of 1, the more specific destination address is going to be learned from OSPF through the Tunnel. The Source Router is going to learn the more specific route and prefer it over the default route, causing the recursive routing error.

upvoted 22 times

Danny_Xu 1 year ago

But it is not mentioned Internet is running OSPF, doesn't make sure that the route can be learnt via OSPF.

upvoted 3 times

Kapoduster Highly Voted 1 year, 11 months ago

Correct answer is B. Tested in CML.
Tunnel destination will be known via tunnel interface.
Look at network command in router ospf configuration and their wildcard. It include also default route.

*Dec 16 15:19:48.624: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel100, changed state to up
*Dec 16 15:19:49.576: %OSPF-5-ADJCHG: Process 100, Nbr 209.165.201.2 on Tunnel100 from LOADING to FULL, Loading Done
Router(config)#
Router(config)#exit
Router#
*Dec 16 15:19:54.146: %ADJ-5-PARENT: Midchain parent maintenance for IP midchain out of Tunnel100 - looped chain attempting to stacksh i
*Dec 16 15:19:55.527: %SYS-5-CONFIG_I: Configured from console by console
*Dec 16 15:19:58.624: %TUN-5-RECURDOWN: Tunnel100 temporarily disabled due to recursive routing

*Dec 16 15:19:58.624: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel100, changed state to down
*Dec 16 15:19:58.624: %OSPF-5-ADJCHG: Process 100, Nbr 209.165.201.2 on Tunnel100 from FULL to DOWN, Neighbor Down: Interface down or detached

upvoted 9 times

leetingo 1 year, 8 months ago

this makes sense. Initially the tunnel is up. After the tunnel is up, the tunnel interface is included into OSPF. The router learns all interface networks from the other router, which also include the tunnel destination address. Then causes a loop, and then bring down the tunnel

upvoted 5 times

msstanick Most Recent 5 months, 3 weeks ago

Selected Answer: B

Labed it up

*Jun 7 16:19:04.544: %TUN-5-RECURDOWN: Tunnel100 temporarily disabled due to recursive routing
*Jun 7 16:19:04.545: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel100, changed state to down

upvoted 2 times

6dd4aa0 8 months, 3 weeks ago

The network 0.0.0.0 255.255.255.255 area in the section ospf section is going to introduce a recursive looping.

I did a simulation with the given configuration. The interface tunnel ip address 192,168.100.2 was automatically disable to prevent a looping. Hence, it route from 10.1.1.0 to 10,2,2,0 does not work.

upvoted 2 times

kewokil120 11 months ago

Selected Answer: B

the network statement enables ospf on all interfaces and the /30 links will be in ospf.

upvoted 2 times

poy4242 11 months, 1 week ago

Selected Answer: B

as soon as tunnel will be up, the ospf process will run between the two router. This is per configuration all network participate in OSPF. Since they will exchange the route, the internet subnet will be exchanged and learned through the tunnel.

upvoted 2 times

Wooker 1 year, 2 months ago

Selected Answer: B

The answer is B

upvoted 2 times

Japsurd 1 year, 2 months ago

Selected Answer: B

Answer is B. To stop the flapping, we can use route filtering, increasing the ospf cost on the tunnel interface, or make the tunnel an ospf passive interface.

upvoted 4 times

[Removed] 1 year, 3 months ago

Selected Answer: C

Since when does OSPF runs freely on the internet?
Since when does OSPF routes have precendence over Static routes?

upvoted 2 times

MerlinTheWizard 10 months ago

Since when does OSPF run freely on the internet? You know the answer to that I pressume.. But from a purely networking perspective, all of this is valid.
OSPF has precedence over static routes in case of a more-specific match (or longer match), or in case the distance of the static route was adjusted - you need to think outside of the box..

upvoted 1 times

Feliphus 1 year ago

But, they are default routes, any other routes learned by OSPF as 209.165.200.226/30 and 209.155.201.2/30 are more specific than:
ip route 0.0.0.0 0.0.0.0 209.165.200.225
ip route 0.0.0.0 0.0.0.0 209.165.201.1
About the first comment, I understand the OSPF is propagating encapsulated inside the tunnel
It's complicated to sure but I select B

upvoted 1 times

pajonk22 1 year, 4 months ago

Correct answer is C - I recreated the topology in Lab. Keep in my you are advertising all subnets via OSPF and default route IP's are incorrect

upvoted 1 times

Neil101 1 year, 4 months ago

It will work temporarily until the tunnel destination is known via the tunnel itself as it will be advertised via OSPF once the tunnel is up, and you end up with recursive routing = bad. Correct answer = B

upvoted 2 times

Edwinmolinab 1 year, 4 months ago

Selected Answer: B

B can be a better answer because ospf will announce network the routers' network interfaces through the tunnel interface

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: C

C. Verifying the scenario The correct answer is the provided

A. No matter if the tunnnel keep aliver are differente the tunnel will be up (Wrong)

B. (MOS TRICKY ONE) even the ospf process are active for all interface including the tunnel, remember that the outgoing interface is on the internet (not running OSPF or maybe BGP) and also a static route pointing to the public is configured to take precedence in case of you are configured internet with BGP. So the tunnel destination wont be learned by the tunnel thus(WRONG)
C. is correct beacuse any configuration show will cause problem to the tunnel (CORRECT)

D. The default MTU (1476) was not changed on the configuration so (WRONG)

upvoted 3 times

Claudiu1 3 weeks ago

You are very wrong.
The best part here is that the 'internet' doesn't even need OSPF. The learning of the networks representing the ends of the GRE tunnel via the tunnel interfaces themselves, is not done by OSPF between the sites and the internet; it is done by OSPF between the sites directly via the GRE tunnel.

To verify this, just make a lab and configure static routing all across the 'internet'. Then, on the sites routers, just add all interfaces to ospf and see what happens

upvoted 1 times

MerlinTheWizard 10 months ago

You are presented with a full configuration that is relevant to the question. If you see OSPF enabled on an interface with public IP address, that is correct and still the same principles apply. Just because it probably wouldn't be configured this way ever in real life, it does test your understanding of the technology. B is correct - play it through in your head or test it in a lab.

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: B

It should be B

upvoted 2 times

zzmejce 1 year, 10 months ago

Selected Answer: B

B is correct

upvoted 2 times

LaughingGor 1 year, 10 months ago

I think it is B ,this lab will cause"GRE tunnel Flapping "problem.....

upvoted 2 times

wwwwaaaa 1 year, 11 months ago

Answer is correct

upvoted 2 times

molinux 1 year, 11 months ago

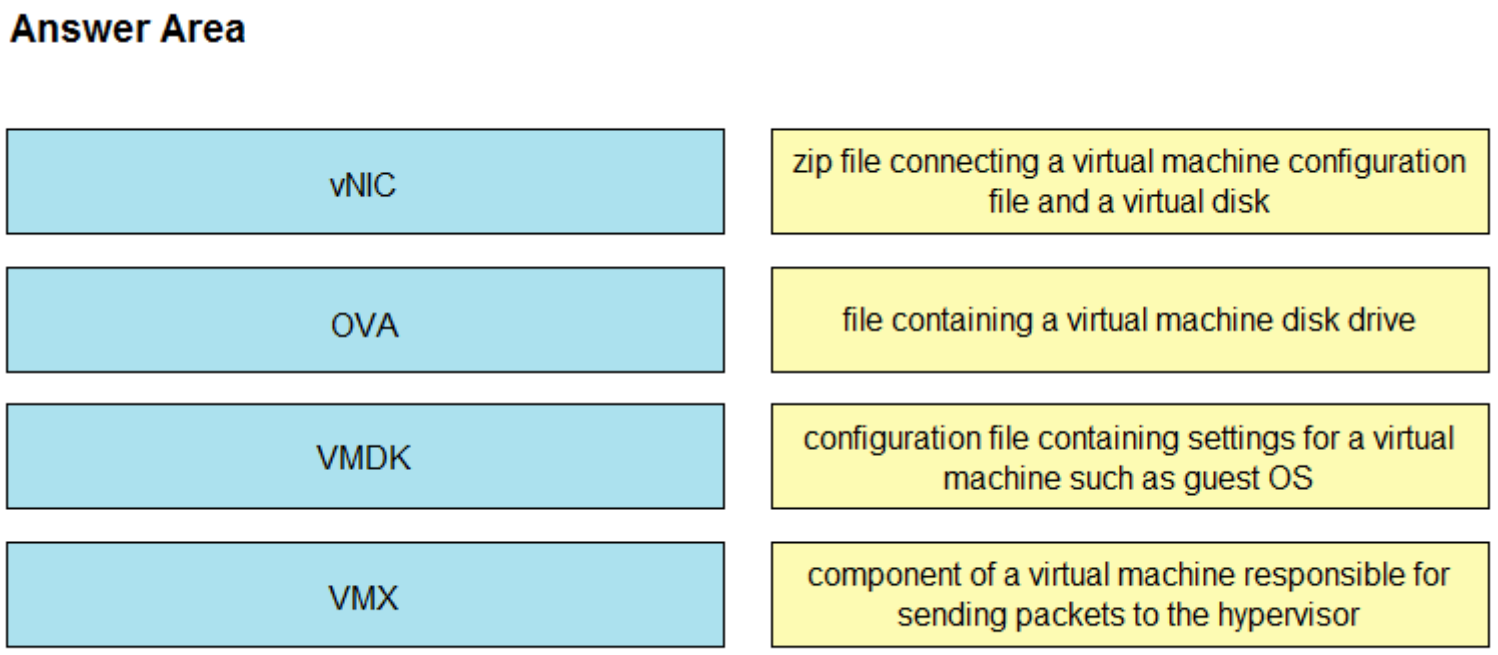
The given answer is correct. The tunnels source Site-A can never form adjacency with tunnel destination Site-B.

upvoted 4 times

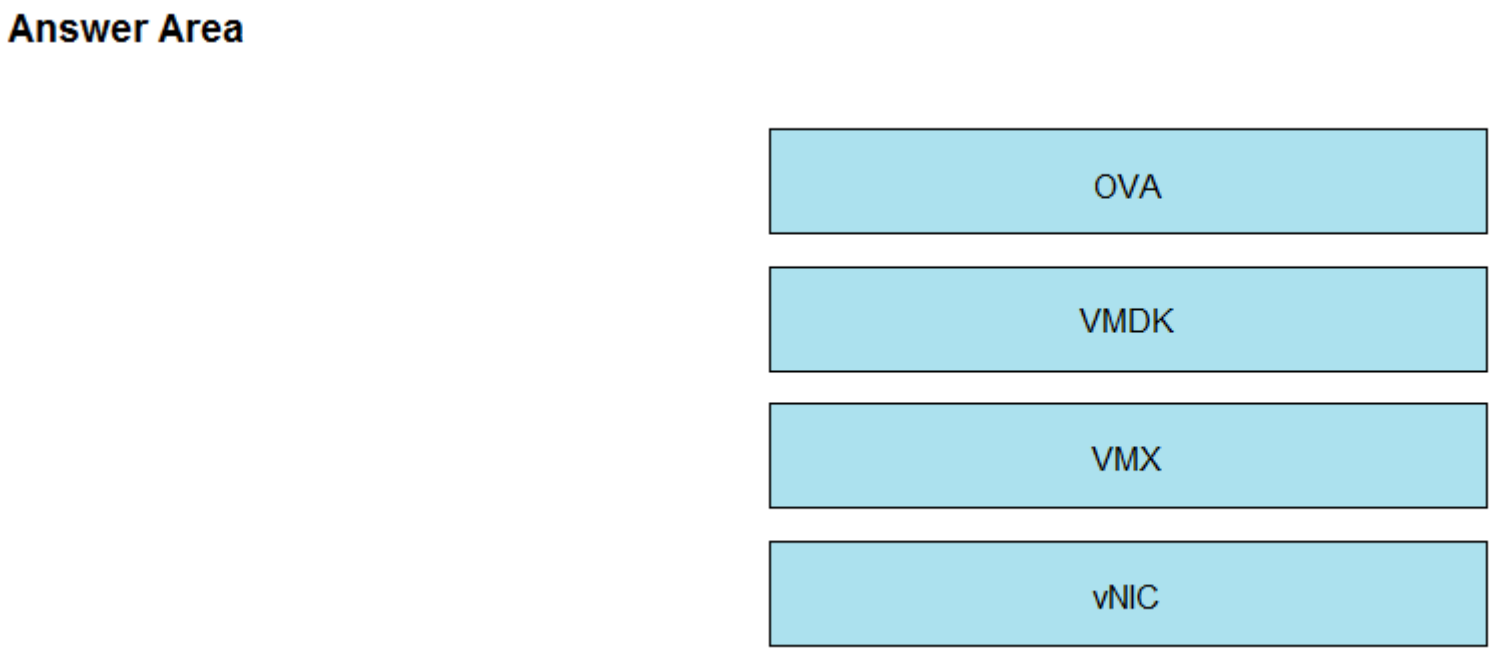
DRAG DROP -

Drag and drop the virtual components from the left onto their descriptions on the right.

Select and Place:



Correct Answer:



cracanici Highly Voted 2 years, 3 months ago

ova
vmdk
vmx
vnic

upvoted 47 times

kthekillerc Highly Voted 2 years, 2 months ago

ova-zip
vmdk- file containig
vmx-config file
Vnic- component

upvoted 12 times

kaupz Most Recent 4 weeks, 1 day ago

so this is a vmware exam now?

upvoted 1 times

[Removed] 5 months ago

I'm not sure how old these comments are, but it looks like the answer was corrected.
ova
vmdk
vmx
vnic

upvoted 3 times

Burik 5 months, 3 weeks ago

"zip file CONTAINING a virtual machine configuration file and a virtual disk", admins please fix this.

upvoted 1 times

AngelPAlonso 1 year, 6 months ago

ova
vmdk
vmx
vnic

upvoted 1 times

danny_f 1 year, 7 months ago

How do they get the simplest questions wrong. MODERATORS, FIX THIS PLEASE

upvoted 3 times

fascool 1 year, 7 months ago

Provided answer is wrong, correct answers are below.

upvoted 1 times

rafailsharifov 2 years ago

Please correct answers
Ova
VMDK
VMX
Vnic

upvoted 4 times

xziomal9 2 years, 2 months ago

The correct answer is:
OVA
VMDK
VMX
VNIC

upvoted 7 times

Question #102 *Topic 1*

Which element enables communication between guest VMs within a virtualized environment?

A. hypervisor

B. virtual router

C. vSwitch

D. pNIC

Correct Answer: *C*

Each VM is provided with a virtual NIC (vNIC) that is connected to the virtual switch. Multiple vNICs can connect to a single vSwitch, allowing VMs on a physical host to communicate with one another at layer 2 without having to go out to a physical switch.

Community vote distribution

C (75%) A (25%)

Brand 9 months, 1 week ago

Selected Answer: C

Guys, there is no way two VMs communicate without a virtual switch. Of course, without a hypervisor, you can't have VMs or anything at all but the key to VM communication is a virtual switch. No other way around it. At least not for this exam.

upvoted 3 times

Ayman_B 11 months ago

Selected Answer: C

Hypervisor provide the hole enviroment, but witch element provides communication between guest VMs within a virtualized environment is the vSwitch

upvoted 2 times

Dataset 12 months ago

Selected Answer: A

Its A for me
Regards

upvoted 1 times

hyjaker 1 year, 4 months ago

Selected Answer: C

vSwitch is required according to the manual.

upvoted 1 times

BigMouthDog 1 year, 5 months ago

Answer should be 'C'. "Hypervisor' is a more generic terminology rather the specific one, vSwitch

upvoted 2 times

Jared28 1 year, 5 months ago

Selected Answer: C

Backing up flash007 here. From the official cert guide:
"A vSwitch enables VMs to communicate with each other within a virtualized server and with external physical networks through the physical network interface cards (pNICs)."

upvoted 1 times

Wheelnet 1 year, 5 months ago

Selected Answer: A

In the official guide estudy appears:

"A hypervisor performs several tasks:

Provides resources to individual operating systems or VMs by partitioning the resources of the physical server or host on which it is installed.

Provides connectivity between VMs and between the VMs and external network resources.

Ensures separation between individual VMs."

upvoted 1 times

mrtattoo 6 months, 4 weeks ago

You are correct that the hypervisor provides connectivity between virtual machines and external network resources. However, the vSwitch is the specific element that enables communication between guest VMs within a virtualized environment.

When a virtual machine sends network traffic to another virtual machine on the same host, the traffic is sent to the vSwitch. The vSwitch then forwards the traffic to the destination virtual machine. The vSwitch can also be configured to provide network connectivity between virtual machines on different hosts in a cluster.

The hypervisor, on the other hand, is responsible for managing the virtual machines and providing access to physical resources such as CPU, memory, storage, and networking. It provides a layer of abstraction between the virtual machines and the physical hardware, and allows multiple virtual machines to share the same physical resources.

So, while the hypervisor plays a critical role in enabling communication between virtual machines and external network resources, the vSwitch is the specific element that enables communication between guest VMs within a virtualized environment.

upvoted 1 times

ciscolessons 1 year, 9 months ago

Selected Answer: C

voting. provided answer is correct

upvoted 1 times

Tsewaman 1 year, 10 months ago

vSwitch is correct

upvoted 1 times

diegodavid82 2 years, 3 months ago

the provided answer is correct

upvoted 2 times

flash007 2 years, 4 months ago

the hypervisor is the software that runs the virtual environment. the Pnic is a physical nic but in order to comunicate virtually you need a Vswitch which is a virtual switch

upvoted 2 times

examShark 2 years, 6 months ago

Could be either A, B or C, most likely the Switch

upvoted 3 times

Question #103 *Topic 1*

Which two methods are used to reduce the AP coverage area? (Choose two.)

A. Reduce channel width from 40 MHz to 20 MHz.

B. Reduce AP transmit power.

C. Enable Fastlane.

D. Increase minimum mandatory data rate.

E. Disable 2.4 GHz and use only 5 GHz.

Correct Answer: *BD*

Community vote distribution

BD (60%) BE (40%)

Hamzaaa Highly Voted 2 years, 7 months ago

B&D are the correct answers !!

upvoted 26 times

mhizha Highly Voted 2 years, 7 months ago

5Ghz has a lower coverage area as compared to 2.4Ghz. not sure what would be the best answer to go with B in this case.

upvoted 16 times

PureInertiaCopy 3 months, 2 weeks ago

This confused me but then I realised.
If you're using the 2.4GHz then it has a different coverage area to 5GHz anyways. Meaning that if the question is about reducing the coverage area, then this applies to the two WiFi bands SEPARATELY.

So the answer is B and D.

upvoted 1 times

amgue 2 years, 6 months ago

B & E are the correct answers

upvoted 9 times

jacop 2 years, 5 months ago

B,D and E are right answers, it suppose to chosse 3 not 2 only

upvoted 8 times

TTTTTT 2 years, 3 months ago

The transmit power of an AP affects the wireless coverage area and the maximum achievable signal-to-noise ratio. Proper configuration of transmit power is important for ensuring a wireless network is operating at its highest capacity.

Reference: https://documentation.meraki.com/MR/Radio_Settings/Transmit_Power_and_Antenna_Configuration

AP coverage area or the cell size, according to this Cisco link, there are two ways to reduce the AP coverage area:
+ Tuning Cell Size with Transmit Power
+ Tuning Cell Size with Data Rates

Setting the transmit power level is a simplistic approach to defining the cell size, but that is not the only variable involved. The cell size of an AP is actually a compromise between its transmit power and the data rates that it offers.

To design a wireless LAN for best performance, you would most likely need to disable some of the lower data rates. For example, you could disable the 1, 2, and 5.5 Mbps rates to force clients to use higher rates and better modulation and coding schemes. That would improve throughput for individual clients and would also benefit the BSS as a whole by eliminating the slower rates that use more time on a channel.

upvoted 12 times

TTTTTT 2 years, 3 months ago

ANs is B&D

upvoted 1 times

Eddgar0 1 year, 7 months ago

As E could be seem correct, the key point is to reduce the coverage area (reducing the coverage area may apply to both 2.4 GHz and 5 GHz so i think wont be suitable for this question

upvoted 5 times

Romrom99 Most Recent 3 months, 3 weeks ago

A. Reduce channel width from 40 MHz to 20 MHz: This option is correct. Reducing the channel width limits the frequency range used for communication, which in turn reduces the coverage area of the AP.

B. Reduce AP transmit power: This option is correct. Lowering the transmit power of the AP decreases the signal strength and, consequently, reduces the coverage area.

C. Enable Fastlane: Enabling Fastlane prioritizes certain types of traffic but doesn't directly impact the coverage area of the AP.

D. Increase minimum mandatory data rate: While this can encourage devices to use higher data rates, it doesn't directly reduce the coverage area of the AP.

E. Disable 2.4 GHz and use only 5 GHz: This can affect the frequency bands used, but it doesn't inherently reduce the coverage area.

upvoted 1 times

djedeen 3 months, 3 weeks ago

Selected Answer: BD

per other comments here:
https://www.ciscopress.com/articles/article.asp?p=2186207&seqNum=2
AP coverage area or the cell size, according to this Cisco link, there are two ways to reduce the AP coverage area:
+ Tuning Cell Size with Transmit Power
+ Tuning Cell Size with Data Rates

upvoted 1 times

forrestwanderer 3 months, 3 weeks ago

B and E are the only logically correct answer. Any high frequency wave will penetrate objects better (think gamma rays) but they have low wavelength and travel very less distance. If you have 5ghz high frequency, they will do well penetrating cardboard walls but don't expect it to penetrate and cross thick concrete walls.

Low frequency waves have high wavelength and travel farther and bounce off objects very well thats why you have AM and FM radio waves that is low frequency.

40mhz or 20mhz channel band has no affect on the range, its simply dividing the window into multiple channels.

upvoted 2 times

Asher 4 months ago

If I disabled 5ghz or 2.4ghz in production I would be shot 😂

upvoted 2 times

teikitiz 5 months, 1 week ago

I'm going with B&D. Higher minimum data rates means less range, and technically you can increase 5GHz radio power and get the same coverage as 2.4

upvoted 1 times

ermanzan 5 months, 2 weeks ago

Selected Answer: BD

B & D are the correct answers, 5Ghz could be valid because at the same transmit power and antenna gain the coverage is lower than a 2.4Ghz radio, but seems to be more accurate B and D

upvoted 1 times

Burik 5 months, 3 weeks ago

Selected Answer: BD

According to Cisco there are two ways to reduce the AP coverage area:

- Tuning Cell Size with Transmit Power
- Tuning Cell Size with Data Rates

https://www.ciscopress.com/articles/article.asp?p=2186207&seqNum=2

Regardless of what other sources say, to answer this question we have to rely on the Cisco guidelines.

upvoted 3 times

JackyChon 6 months, 2 weeks ago

Selected Answer: BD

B&D are the correct answers !!

upvoted 1 times

HungarianDish 7 months, 3 weeks ago

Selected Answer: BD

Controversial topic, cisco documents seem to go more in the direction of data rates and of course transmit power, so probably BD.

cisco says to change data rates:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_wireless_high_client_density_design_guide.html#concept_5B38A134200E42858DBDF3DC650ED74C

https://www.ciscopress.com/articles/article.asp?p=2186207&seqNum=2

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_wireless_high_client_density_design_guide.html

https://community.cisco.com/t5/wireless/wlc-data-rates/td-p/4400887

Blog about Ruckus says to do not change data rates:
https://todsfromds.com/2019/08/13/the-three-best-ways-to-control-ap-cell-size-and-two-you-shouldnt-use/
upvoted 1 times

JackDRipper 7 months, 3 weeks ago

Selected Answer: BD

Answer B is a no-brainer.
Answer D makes it possible to drop devices that are at the edge of the coverage area. You see, to maintain a stable connection, WiFi devices will automatically reduce the data rate when the RSSI and/or SNR starts compromising the transmission. This option allows the AP to drop the connection to the client if the data rate goes below the set minimum, effectively reducing the size of the AP's coverage.
Answer E will just cripple the AP and waste a whole band of WiFi hat can be used for 2.4GHz-only devices (ie. IoTs).
upvoted 2 times

Nickplayany 8 months, 1 week ago

Selected Answer: BE

B and E.

Why D is not correct for me:

Increase minimum mandatory data rate: Increasing the minimum mandatory data rate can improve network performance by encouraging devices to use higher data rates, but it does not reduce the coverage area of the AP.
upvoted 5 times

rami_mma 8 months, 1 week ago

B and E is correct
upvoted 1 times

rami_mma 8 months, 1 week ago

B and D
upvoted 1 times

dragonwise 8 months, 3 weeks ago

Selected Answer: BE

B&E are correct
B: by reducing power, signal is reduced
E: 5GHz has a higher bit rate but lower coverage

Increase minimum data rate does not affect coverage area, so D is WRONG
upvoted 2 times

cjk3 1 year ago

E is tricky, but not the correct answer. You could have the 5GHz (say 17dbm) radio running hotter than the 2.4Ghz (say 8dbm) radio. Turning off the 2.4 radio wouldn't decrease the cell size in this scenario.
upvoted 3 times

Question #104 *Topic 1*

Which antenna type should be used for a site-to-site wireless connection?

A. patch

B. dipole

C. omnidirectional

D. Yagi

Correct Answer: *D*

Community vote distribution

D (100%)

dansecu 2 months, 3 weeks ago

Correct answer is patch antenna.
Patch anttena have more gain and more directional radiation pattern.
Check Cisco Aironet 14-dBi Patch Antenna (AIR-ANT5114P-N):
https://www.cisco.com/c/en/us/td/docs/wireless/antenna/installation/guide/ant5114P.html
vs Cisco WPAN Yagi Antenna (ANT-WPAN-Y-OUT-N)
https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/antennas/installing-combined/b-cisco-industrial-routers-and-industrial-wireless-access-points-antenna-guide/m-ant-wpan-y-out-n.html

upvoted 1 times

ihateciscoreally 3 months, 1 week ago

Selected Answer: D

yagi and patch are correct answers, but yagi is definitely more directional than patch. thus correct answer is D.

upvoted 2 times

Colmenarez 4 months ago

I'd would use a Dish, but ok Cisco.

upvoted 3 times

techriese 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

Dataset 7 months, 3 weeks ago

what is the difference with PATCH ?

upvoted 1 times

C4l4v3r4 1 year, 2 months ago

Selected Answer: D

Yagi has the greatest directivity of the given answers.

D is correct.

upvoted 1 times

jordik 1 year, 9 months ago

Selected Answer: D

D is correct. A Yagi antenna contains a dipole but also has reflectors and directors.

upvoted 3 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 1 times

Question #105 *Topic 1*

In a wireless network environment, what is calculated using the numerical values of the transmitter power level, cable loss, and antenna gain?

A. SNR

B. RSSI

C. EIRP

D. dBi

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/23231-powervalues-23231.html

Community vote distribution
C (100%)

alexzs27 Highly Voted 1 year, 10 months ago
Effective Isotropic Radiated Power

The radiated (transmitted) power is rated in either dBm or W. Power that comes off an antenna is measured as effective isotropic radiated power (EIRP). EIRP is the value that regulatory agencies, such as the FCC or European Telecommunications Standards Institute (ETSI), use to determine and measure power limits in applications such as 2.4-GHz or 5-GHz wireless equipment. In order to calculate EIRP, add the transmitter power (in dBm) to the antenna gain (in dBi) and subtract any cable losses (in dB).
upvoted 10 times

techriese Most Recent 5 months ago
Selected Answer: C
C is correct
upvoted 1 times

Dataset 7 months, 3 weeks ago
Selected Answer: C
hi!
C is correct
Regards
upvoted 1 times

Shrishai 1 year, 1 month ago
C is correct
upvoted 1 times

cracanici 2 years, 2 months ago
Effective Isotropic Radiated Power
upvoted 3 times

examShark 2 years, 6 months ago
Given answer is correct
upvoted 3 times

Question #106 *Topic 1*

What does the LAP send when multiple WLCs respond to the CISCO-CAPWAP-CONTROLLER.localdomain hostname during the CAPWAP discovery and join process?

A. unicast discovery request to the first WLC that resolves the domain name

B. broadcast discovery request

C. join request to all the WLCs

D. unicast discovery request to each WLC

Correct Answer: *D*

Community vote distribution

tonght Highly Voted 2 years, 9 months ago

Answer should be D; let's look: https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107606-dns-wlc-config.html#anc5

upvoted 33 times

P1Z7C Highly Voted 2 years, 8 months ago

A is ok

The Lightweight AP (LAP) can discover controllers through your domain name server (DNS). For the access point (AP) to do so, you must configure your DNS to return controller IP addresses in response to CISCO-LWAPP-CONTROLLER.localdomain, where localdomain is the AP domain name. When an AP receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the AP sends discovery requests to the controllers.

The AP will attempt to resolve the DNS name CISCO-CAPWAP-CONTROLLER.localdomain. When the AP is able to resolve this name to one or more IP addresses, the AP sends a unicast CAPWAP Discovery Message to the resolved IP address(es). Each WLC that receives the CAPWAP Discovery Request Message replies with a unicast CAPWAP Discovery Response to the AP.

Reference: https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107606-dns-wlc-config.html

upvoted 11 times

Mahmoudragab94 2 years, 4 months ago

the AP sends discovery requests to the controllers. D is okay also

upvoted 1 times

Vlad_Is_Love_ua Most Recent 9 months, 1 week ago

Selected Answer: D

When multiple WLCs respond to the CISCO-CAPWAP-CONTROLLER.localdomain hostname during the CAPWAP discovery and join process, the LAP sends a unicast discovery request to each WLC that responded. This process is called the discovery response mechanism.

In this mechanism, each WLC that receives a discovery request from the LAP sends a discovery response to the LAP with its IP address. If multiple WLCs respond with the same hostname, the LAP sends a discovery request to each of them.

The LAP then selects the first WLC that responded to the discovery request and sends a join request to that WLC. If the first WLC does not respond, the LAP sends a join request to the next WLC in the list that responded to the discovery request, and so on.

upvoted 6 times

Ayman_B 11 months ago

Selected Answer: D

Once the DNS name has been resolved a unicast Discovery Request will be sent to the WLC IP/s.

upvoted 1 times

iGlitch 1 year ago

Selected Answer: D

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107606-dns-wlc-config.html#anc5

upvoted 2 times

Redzero07 1 year ago

Selected Answer: D

Answer is D

upvoted 1 times

PedroPicapiedra 1 year ago

Selected Answer: D

I Think is D too

D is correct
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107606-dns-wlc-config.html#anc5
upvoted 1 times

Ciscopass 1 year ago

Selected Answer: C

From the K Wallace cert guide: "When an AP has finished the discovery process, it should have built a list of live candidate controllers. Now it must begin a separate process to select one WLC and attempt to join it. "

So, I vote for C.
upvoted 1 times

Rose66 10 months, 4 weeks ago

The problem is, that the answer provided is "join request to all the WLCs" and not "join request to the selected WLC"....
upvoted 1 times

Typovy 1 year, 1 month ago

Selected Answer: C

C is correct
upvoted 1 times

Rumbrum 1 year, 1 month ago

Selected Answer: C

After WLCs reply AP will try to join them starting from the primary
upvoted 1 times

Rumbrum 1 year, 1 month ago

Wrong answer, can't delete. Right one is A
upvoted 1 times

nopenotme123 1 year, 3 months ago

Selected Answer: C

C is the only one that makes any sense. Why would the AP send out another discovery request if the WLC is responding?
upvoted 1 times

Heim_Ox 1 year, 5 months ago

C. If it receives a response to the CISCO-CAPWAP-CONTROLLER.localdomain the discovery process is already complete. The next is the join request and C is the only one that has that
upvoted 2 times

Ondskan 1 year, 6 months ago

Selected Answer: D

DNS

The AP will attempt to resolve the DNS name "CISCO-CAPWAP-CONTROLLER.localdomain". When the AP is able to resolve this name to one or more IP addresses, the AP sends a unicast CAPWAP Discovery Request to the resolved IP address(es). The DNS entries can be either an A (address) or CNAME (alias) records.
upvoted 2 times

nopenotme123 1 year, 3 months ago

The WLC is already responding meaning the AP has already sent out a discovery request.
upvoted 1 times

DLLLLLLLL 1 year, 6 months ago

Selected Answer: D

Answer should be D
upvoted 1 times

dazzler_010 1 year, 8 months ago

Answer should b D - each WLC, and then form a list of available WLCs to choose from.
upvoted 1 times

rettich 1 year, 9 months ago

Selected Answer: D

The AP will attempt to resolve the DNS name CISCO-CAPWAP-CONTROLLER.localdomain. When the AP is able to resolve this name to one or more IP addresses, the AP sends a unicast CAPWAP Discovery Message to the resolved IP address(es). Each WLC that receives the CAPWAP Discovery Request Message replies with a unicast CAPWAP Discovery Response to the AP.

Reference: https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107606-dns-wlc-config.html
upvoted 1 times

ciscogear 1 year, 10 months ago

A. Final answer. The unicast is sent to whatever DNS resolves to. It can be a single address or multiple. It does not send to all WLCs, only what is configured in DNS.

The AP will attempt to resolve the DNS name CISCO-CAPWAP-CONTROLLER.localdomain. When the AP is able to resolve this name to one or more IP addresses, the AP sends a unicast CAPWAP Discovery Message to the resolved IP address(es). Each WLC that receives the CAPWAP Discovery Request Message replies with a unicast CAPWAP Discovery Response to the AP.

upvoted 1 times

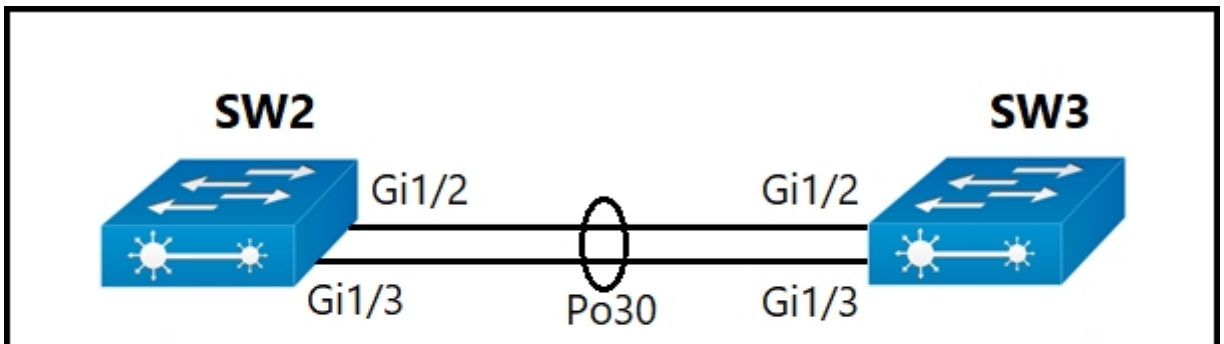
ciscogear 1 year, 10 months ago

Sorry, I meant D.
Each WLC.

upvoted 2 times

Question #107 *Topic 1*

Refer to the exhibit.




```
Interface gi1/2
Channel-group 30 mode desirable
Port-channel load-balance src-ip

Interface gi1/3
Channel-group 30 mode desirable
Port-channel load-balance src-ip

Interface PortChannel 30
Switchport mode trunk
Switchport encapsulation dot1q
Switchport trunk allowed vlan 10-100
```

A port channel is configured between SW2 and SW3. SW2 is not running a Cisco operating system. When all physical connections are made, the port channel does not establish.
Based on the configuration excerpt of SW3, what is the cause of the problem?

A. The port-channel mode should be set to auto.

B. The port channel on SW2 is using an incompatible protocol.

C. The port-channel trunk is not allowing the native VLAN.

D. The port-channel interface load balance should be set to src-mac.

Correct Answer: *B*

Community vote distribution

B (100%)

Reavr Highly Voted 2 years, 1 month ago

Answer is B.

The question states that SW2 is not running Cisco. Therefore it cannot run PaGP (which according to the snippet, SW3 is configured as). So it has to be changed to either channel-group active or passive to do LACP.

upvoted 9 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: B

>SW2 is not running a Cisco operating system.
PaGP is Cisco proprietary technology ...

upvoted 2 times

PedroPicapiedra 1 year ago

Selected Answer: B

The correct is B

*** PaGP - Cisco Propietary protocol
Config modes:
- Desirable
- Auto
- On

*** LACP - Open Standard Protocol
Config modes:
- Active
- Passive
- On

upvoted 4 times

Parot 1 year, 1 month ago

Answer is B. Desirable mode means PAGP - cisco proprietary protocol. LACP should be use to setup the link between Cisco and non -Cisco devices.

upvoted 1 times

KZM 1 year, 2 months ago

PAGP is Cisco proprietary and LACP is an IEEE 802.3ad open standard protocol. Between Cisco IOS and non-Cisco devices, just support LACP for Link Aggregation.
The command "Channel-group xx mode desirable" is used in PAGP. For the LACP configuration, the command should be "Active or Passive" in channel-group mode.

upvoted 1 times

Multicast01005e 2 years, 1 month ago

B is absolutely correct

upvoted 3 times

kthekillerc 2 years, 5 months ago

B is the correct answer

upvoted 3 times

ABC123 2 years, 8 months ago

B is wrong. Answer should be A, as desirable is for Cisco Proprietary PAgP.
S1(config)# interface range f0/13 -15
S1(config-if-range)# channel-group 1 mode ?
active Enable LACP unconditionally
auto Enable PAgP only if a PAgP device is detected
desirable Enable PAgP unconditionally
on Enable Etherchannel only
passive Enable LACP only if a LACP device is detected
From:
https://packetlife.net/blog/2010/jan/18/etherchannel-considerations/

upvoted 1 times

mustache 2 years, 8 months ago

kindly check the exhibit and read the question carefully before answering!
B is correct, wrong Protocol is being used, PAgP is cisco proprietary. LACP is open Standard

upvoted 11 times

muska04 2 years, 4 months ago

B is the Correct answer. Auto => PAgP, not supported on non-cisco equipment.

upvoted 4 times

amgue 2 years, 6 months ago

The question asks for the source of the problem, A gives the solution not the source, the correct answer is B

upvoted 7 times

ArchBishop 1 year, 10 months ago

A is not a solution...
Desirable/Auto => PAgP
Active/Passive => LACP

upvoted 2 times

Question #108 *Topic 1*

What is a fact about Cisco EAP-FAST?

A. It requires a client certificate.

B. It is an IETF standard.

C. It does not require a RADIUS server certificate.

D. It operates in transparent mode.

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/99791-eapfast-wlc-rad-config.html

Community vote distribution
C (100%)

XalaGyan Highly Voted 1 year, 12 months ago

Selected Answer: C
What is a fact about Cisco EAP-FAST?
A. It requires a client certificate. ==> WRONG. it uses PAC (Protected Access Credentials)
B. It is an IETF standard. ==> WRONG, please watch the question. it says CISCO FAST not IEEE
C. It does not require a RADIUS server certificate. ==> CORRECT or lets say best answer from given ones
D. It operates in transparent mode.==> WRONG. I got no clue what is there to be transparent

Answer: C
upvoted 10 times

nead Highly Voted 2 years, 7 months ago

C is Correct.
EAP-FACT uses a PAC. Creates its own certificate. No AAA needed.
upvoted 8 times

testbench007 Most Recent 1 year, 10 months ago

C is correct. There is no client or server certificates used in EAP-FAST.
upvoted 3 times

Nhan 2 years, 1 month ago

The EAP-FAST protocol is a publicly accessible IEEE 802.1X EAP type that Cisco developed to support customers that cannot enforce a strong password policy and want to deploy an 802.1X EAP type that does not require digital certificates.
upvoted 5 times

Nhan 2 years, 2 months ago

The given answer is correct
upvoted 2 times

cracanici 2 years, 3 months ago

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/eap-fast/200322-Understanding-EAP-FAST-and-Chaining-imp.html
upvoted 2 times

mustache 2 years, 8 months ago

A: should be the right answer.
upvoted 1 times

mustache 2 years, 8 months ago

C seams to be worng...
EAP-FAST (Flexible Authentication via Secure Tunneling) was developed by Cisco*. Instead of using a certificate to achieve mutual authentication. EAP-FAST authenticates by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution.
https://www.intel.com/content/www/us/en/support/articles/000006999/wireless.html
upvoted 1 times

mustache 2 years, 7 months ago

Correction: C is right answer.
EAP-FAST is a flexible EAP method which allows mutual authentication of a supplicant and a server. It is similar to EAP-PEAP, but typically does not require the use of client or even server certificates.
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/eap-fast/200322-Understanding-EAP-FAST-and-Chaining-imp.html#anc2
upvoted 6 times

Barry_Allen 2 years, 7 months ago

okay ill choose C thanks.

upvoted 3 times

Question #109 *Topic 1*

Which DNS lookup does an access point perform when attempting CAPWAP discovery?

A. CISCO-CONTROLLER.local

B. CAPWAP-CONTROLLER.local

C. CISCO-CAPWAP-CONTROLLER.local

D. CISCO-DNA-CONTROLLER.local

Correct Answer: *C*

Reference:

http://www.revolutionwifi.net/revolutionwifi/2010/11/capwap-controller-discovery-process_23.html

Community vote distribution

C (100%)

techriese 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: C

its right

upvoted 2 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

Question #110 *Topic 1*

Refer to the exhibit.

```
access-list 1 permit 10.1.1.0 0.0.0.31
ip nat pool CISCO 209.165.201.1  209.165.201.30 netmask 255.255.255.224
ip nat inside source list 1 pool CISCO
```

What are two effects of this configuration? (Choose two.)

A. It establishes a one-to-one NAT translation.

B. The 209.165.201.0/27 subnet is assigned as the outside local address range.

C. The 10.1.1.0/27 subnet is assigned as the inside local addresses.

D. Inside source addresses are translated to the 209.165.201.0/27 subnet.

E. The 10.1.1.0/27 subnet is assigned as the inside global address range.

Correct Answer: *CD*

Community vote distribution

AC (50%) CD (50%)

[Removed] Highly Voted 2 years, 10 months ago

it cant be A because this is not a static one to one NAT.
it cant be B because outside local is the private address of the destination, it has nothing to do with the network that we are configuring.
it cant be E because 1) its a private IP address 2) we specify the inside global pool in the 2nd command

it has to be C) because we "assign" (aka permit with the ACL) the 10.1.1.0/27 block to be NATed
it has to be D) for the same obvious reason, we state this block to be the inside global pool in the command

upvoted 32 times

Feliphus 1 year ago

About A, the option says "It establishes a one-to-one NAT translations", accoding to the official guide at page 418, there are three types of NAT:
- a static one-to-one mapping
- a dynamic one-to-one mapping
- a dyanmic many-to-one mapping
I understand you can not affirm that A is not correct, and suppose the static word was omitted in the answer. You can only be completly sure the third kind of NAT is not correct. In my opinion A and C are the correct answers.
By the way, I think D is not correct because the address 209.165.201.0 and 209.165.201.31 are not included inside the pool CISCO to be the same than 209.165.201.0/27 as the source-list 1 does with 10.1.1.0/27 which included the net IP (.0) and broadcast IP (.31)

upvoted 3 times

cyrus777 Highly Voted 2 years ago

it's not A because it is many to many
it's not B because 209.165.201.0/27 is inside global not outside local
it's not E because 10.1.1.0/27 is inside local
then C and D are correct

upvoted 6 times

Mahnazyh 2 months ago

Dynamic and static are one2one but pat aka nat overload is one to many

upvoted 1 times

djedeen Most Recent 3 weeks, 4 days ago

Selected Answer: CD

C&D: not 1:1; 209.165.201.0/27 == inside global; 10.1.1.0/27 == inside local
Good explanation:https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/4606-8.html

upvoted 1 times

KZM 1 month, 3 weeks ago

Selected Answer: AC

It is Dynamic NAT Binding. Dynamic binding guarantees a one-to-one mapping between the local address and the global address. D. is incorrect. Because 209.165.201.0/27 subnet including the address from 209.165.201.0 through 209.165.201.31 (Remember you are not assigning IP address to an interface with /27 subnet. So, forget the Network Address and Broadcast address blah blah... Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/nat-xe-3s-book/nat-xe-3s-book_chapter_011011.pdf

upvoted 1 times

mahnazmohamz 1 month, 3 weeks ago

Selected Answer: AC

one to one is dynamic
upvoted 1 times

teikitiz 5 months ago

Selected Answer: AC

I'll stick with A and C, focusing on NAT terminology.

A- OK, this is a 1to1 mapping, although dynamic. B- NOK, those are inside global. C- OK. D- most controversial one. if it were "inside local" instead of "inside source", then it would be OK, but it isn't. Conceptually we know this is how it behaves, but NAT terms don't match. E- These are inside local, so NOK
upvoted 1 times

ibogovic 5 months, 1 week ago

Selected Answer: CD

C. The 10.1.1.0/27 subnet is assigned as the inside local addresses.
D. Inside source addresses are translated to the 209.165.201.0/27 subnet.

Explanation:
The access list "access-list 1 permit 10.1.1.0 0.0.0.31" defines the inside local addresses (source addresses) that will be translated. It permits the 10.1.1.0/27 subnet.

The NAT configuration "ip nat inside source list 1 pool CISCO" specifies that the inside local addresses (10.1.1.0/27 subnet) will be translated to the addresses in the NAT pool named "CISCO" (209.165.201.1 to 209.165.201.30).

Therefore, the inside source addresses (10.1.1.0/27 subnet) will be translated to the 209.165.201.0/27 subnet, and the 10.1.1.0/27 subnet is assigned as the inside local address range.
upvoted 1 times

teikitiz 5 months ago

but A is correct too, as it is a one-to-one mapping (dynamic, not static, but still 1to1)
upvoted 1 times

mhizha 7 months ago

The answer is A & C
The reason I rule out D is that in the NAT world, there is nothing called an inside local address. If this question was not about NAT maybe the term "inside local" would be acceptable.
upvoted 1 times

Burik 5 months, 3 weeks ago

The term "Inside local" is a proper term in the NAT world.

R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 192.0.2.10:23 192.168.0.10:23 10.0.0.2:32978 10.0.0.2:32978
upvoted 1 times

bk989 6 months, 2 weeks ago

in the OCG on NAT they mention "inside local" about half a dozen times
upvoted 2 times

Cesar12345 7 months ago

Selected Answer: CD

A similar example is described in the official certification guide on page 661.
upvoted 1 times

FerroForce 7 months ago

Selected Answer: CD

It is C and D
upvoted 1 times

HungarianDish 7 months, 3 weeks ago

"Dynamic NAT is useful when fewer addresses are available than the actual number of hosts to be translated. It creates an entry in the NAT table when the host initiates a connection and establishes a one-to-one mapping between the addresses. But, the mapping can vary and it depends upon the registered address available in the pool at the time of the communication. Dynamic NAT allows sessions to be initiated only from inside or outside networks for which it is configured. Dynamic NAT entries are removed from the translation table if the host does not communicate for a specific period of time which is configurable. The address is then returned to the pool for use by another host."

Static NAT is one-to-one, and it creates a permanent entry in the NAT table.
Dynamic NAT is also one-to-one, but the NAT entry is only present for a specific period of time. => A is OK.
C is more obvious.

https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html
upvoted 1 times

rami_mma 8 months, 1 week ago

A and D is correct.
upvoted 1 times

albertie 8 months, 1 week ago

Static Nat - This is the actual one to one NAT
Dynamic NAT - This is the type of NAT on question. don't confuse with static and dynamic NAT
PAT (Overloading NAT)

upvoted 1 times

HungarianDish 8 months, 3 weeks ago

Selected Answer: AC

https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html

upvoted 1 times

cerf 9 months, 2 weeks ago

A and C are the correct!

upvoted 1 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: AC

A and C
I have not found any official cisco document which is using the declaration "many-to-many" for this scenario. There is always the wording "one-to-one", accompanied by dynamic or static. "A" describes a dynamic one-to-one NAT and is therefore correct.
In addition, in this official guide they use the wording one-to-one clearly together with network ranges. Reference:
https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb4154-configure-one-to-one-network-address-translation-nat-on-rv32.html
D. is also just not true. The NAT happens not into the /27 range, it only happens into a subset of this /27 range. The .0 and .31 are missing in the pool.

upvoted 2 times

ciscokoolaid 11 months ago

Selected Answer: CD

A is wrong because the configuration shown is for dynamic NAT which is a many-to-many IP translation - not one-to-one.

upvoted 1 times

Question #111 *Topic 1*

An engineer configures a WLAN with fast transition enabled. Some legacy clients fail to connect to this WLAN.
Which feature allows the legacy clients to connect while still allowing other clients to use fast transition based on their OUIs?

A. over the DS

B. 802.11k

C. adaptive R

D. 802.11v

Correct Answer: *C*

Community vote distribution

C (100%)

Tommy133 Highly Voted 2 years, 1 month ago

Cisco 802.11r supports three modes:
+ Pure mode: only allows 802.11r client to connect
+ Mixed mode: allows both clients that do and do not support FT to connect
+ Adaptive mode: does not advertise the FT AKM at all, but will use FT when supported clients connect
Therefore “Adaptive mode” is the best answer here

upvoted 10 times

39first Highly Voted 2 years, 10 months ago

C. Adaptive 802.11r

See below:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html

upvoted 7 times

XalaGyan 1 year, 12 months ago

Bro here is another documentation that gives also a good explanation.

http://giantsnerdwifi.blogspot.com/2017/11/ciscos-adaptive-11r.html

upvoted 4 times

Burik Most Recent 5 months, 3 weeks ago

Selected Answer: C

What "Adaptive R" is even supposed to mean anyway? It's Adaptive 802.11r, I've never heard of "Adaptive R", not even as a colloquial term.

upvoted 2 times

ciscolessons 1 year, 8 months ago

Selected Answer: C

provided answer is correct

upvoted 2 times

Wesgo 2 years, 9 months ago

Adaptive 802.11rTheconfiguration is to all devices, but the adaptive 11r feature will only be applied to supporting iOS devices running iOS 10 or later. All other devices will be able to associate using standard WPA2(including Mac clients)

https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-6/Enterprise_Best_Practices_for_iOS_devices_and_Mac_computers_on_Cisco_Wireless_LAN.pdf

upvoted 3 times

skh 3 years ago

I think C

https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html

upvoted 2 times

Question #112 *Topic 1*

What are two common sources of interference for Wi-Fi networks? (Choose two.)

A. LED lights

B. radar

C. fire alarm

D. conventional oven

E. rogue AP

Correct Answer: *BE*

Community vote distribution

BE (80%) AE (20%)

Saqib79 Highly Voted 3 years, 6 months ago

Correct Options are B & E.

upvoted 42 times

CBlu Highly Voted 3 years, 6 months ago

B&E, LED has no impact on wifi

upvoted 16 times

Mimimimimi 1 year, 12 months ago

LED can have impact on Wi-Fi, but it is not common. It's usually low quality LED when it happens.
But you are correct, B&E are the 'common sources'.

upvoted 3 times

tarres44 Most Recent 6 months, 2 weeks ago

Selected Answer: BE

Correct Options are B & E.

upvoted 2 times

Pilgrim5 7 months, 3 weeks ago

Selected Answer: BE

BE are correct

D might have been right if they stated microwave oven as these ovens operate on the 2.4GHz band. However conventional ovens don't produce microwave radiations so D is wrong.

upvoted 2 times

DLLLLLLLL 1 year, 6 months ago

Selected Answer: BE

B & E correct!

upvoted 2 times

Aldebeer 1 year, 7 months ago

Selected Answer: BE

How LED light impact Wifi ?

upvoted 2 times

proxmox 1 year, 8 months ago

Selected Answer: BE

Radar uses the same radio band as 5gHz wifi

upvoted 3 times

ciscolessons 1 year, 8 months ago

Selected Answer: BE

provided answer is correct

upvoted 2 times

aohashi 1 year, 9 months ago

Selected Answer: BE

It should be BE

upvoted 2 times

jordik 1 year, 9 months ago

Selected Answer: AE

A, B, and E can all be correct. A is less likely with modern LED lights but can occur with budget lights. B is very unlikely to occur unless you live near an airfield or military installation. E is obvious.
Given most setups are not near an airfield, the answer is A and E.

upvoted 4 times

AndreasThornus 1 year ago

There are other RADAR sources - weather radars for example.

upvoted 2 times

GarosTurbo 1 year, 10 months ago

Selected Answer: BE

B,E a re the correct answers

upvoted 1 times

cyrus777 2 years ago

B & E
https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Common_Sources_of_Wireless_Interference

upvoted 4 times

Nhan 2 years, 1 month ago

The microwave can cause some interference but not the oven, the led light interference is way too small that doesn't effect anything at all, the humidity density can cause some Interface, humans body, water, tree, rain, snow... can cause good a substantial amount of radio lost but for this question and given answer the radar and rogue AP is the correct answer, remember the submarine can not transmit the signal from while floating under the water, so they float the antenna to the surface when they want to communicate with the central command.

upvoted 4 times

xziomal9 2 years, 2 months ago

The correct answer is:
B. radar
E. rogue AP

upvoted 2 times

jerryguo1019 2 years, 3 months ago

common sources of interference for Wi-Fi networks:
1. florescent lights; not LED lights
2. Radar is source of WiFi interference
3. Security motion detectors; not fire alarm
4. Microwave oven; not conventional oven
5. Rogue AP
so B & E are correct!!!

upvoted 6 times

HK010 2 years, 4 months ago

A E. I have read that in Network+ before.
Radar is a valid answer, but you probably won't have a radar i nearby your WLAN, which means it's not a common reason.

upvoted 1 times

Glass17 2 years, 4 months ago

Fluorescent lights can indeed cause interference.
Haven't heard of LEDs.

upvoted 1 times

Hamzaaa 2 years, 7 months ago

Radar & Rog AP, B&E are correct

upvoted 1 times

Question #113 *Topic 1*

Which two pieces of information are necessary to compute SNR? (Choose two.)

A. transmit power

B. noise floor

C. EIRP

D. RSSI

E. antenna gain

Correct Answer: *BD*
Reference:
https://community.cisco.com/t5/wireless-mobility-documents/snr-rssi-eirp-and-free-space-path-loss/ta-p/3128478

Community vote distribution

BD (100%)

Saqib79 Highly Voted 3 years, 6 months ago

Correct Options are B & D.

upvoted 58 times

mdsabbir 2 years, 1 month ago

Correct ans is A & B. SNR = 20 log 10 (S / N). S = Signal , N = Noise.

upvoted 5 times

mdsabbir 2 years, 1 month ago

Sorry - its is B & D. S = receiver Signal strength, N = Noise Floor

upvoted 3 times

skh Highly Voted 3 years ago

B & D.
Study Guide book
signal-to-noise ratio (SNR) A measure of received signal quality, calculated as the difference between the signal's RSSI and the noise floor. A higher SNR is preferred.

upvoted 17 times

Networkfate Most Recent 4 months, 1 week ago

SNR (dB) = P received_signal (dBm) - P noise (dBm)

upvoted 1 times

ibogovic 5 months, 1 week ago

Selected Answer: BD

The correct answers are B. noise floor and D. RSSI.

Signal-to-Noise Ratio (SNR) is a measure of the signal strength relative to the background noise level in a wireless communication system. To compute SNR, the following two pieces of information are necessary:

Noise floor: The noise floor is the level of background noise present in the wireless environment. It represents the total power of all interfering signals, thermal noise, and other sources of noise. The noise floor is typically measured in decibels (dB) and is an important factor in determining the SNR.
Received Signal Strength Indicator (RSSI): RSSI is a measurement of the power level of the received signal at the receiver. It represents the strength of the signal as perceived by the receiver and is typically measured in dBm (decibels relative to milliwatts). RSSI provides information about the received signal power, which is necessary to calculate the SNR.

upvoted 1 times

nopenotme123 1 year, 3 months ago

Selected Answer: BD

The graph in the book clearly shows RSSI and Noise floor for snr calculations..

upvoted 1 times

GreatDane 1 year, 5 months ago

Ref: Signal-to-noise ratio – Wikipedia

"...
Definition

Signal-to-noise ratio is defined as the ratio of the power of a signal (meaningful input) to the power of background noise (meaningless or

unwanted input):
..."

A. transmit power

Correct answer.

B. noise floor

Correct answer.

C. EIRP

Wrong answer.

D. RSSI

Wrong answer.

E. antenna gain

Wrong answer.
upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: BD

The RSSI value focuses on the expected signal alone, without regard to any other signals that may also be received, like noise!
upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: BD

Transmit power is not taken into account to calculate SNR, B and D are the correct ones.
upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: BD

It should be BD
upvoted 2 times

rettich 1 year, 9 months ago

Selected Answer: BD

RSSI is significant in calculating SNR as explained many times here, just wanted to place a vote
upvoted 1 times

xziomal9 2 years, 2 months ago

The correct answer is:
B. noise floor
D. RSSI
upvoted 1 times

Darcy42 2 years, 5 months ago

B and D are correct.
upvoted 1 times

tonyx182 2 years, 6 months ago

B&D is the correct answer!!
upvoted 1 times

AliMo123 2 years, 6 months ago

B&D
simply, antenna gain and transmit power are measurement of EIRP, so noise floor and RSSI are correct ones
upvoted 1 times

khaganiabbasov 2 years, 7 months ago

noise floor and RSSI...
upvoted 1 times

Hamzaaa 2 years, 7 months ago

B & D, equation is: SNR = RSSI - N
N: Noise floor
upvoted 2 times

ind_RuzRb 2 years, 7 months ago

Correct Answers are B & D.
upvoted 1 times

Question #114 *Topic 1*

Which OSPF network types are compatible and allow communication through the two peering devices?

A. point-to-multipoint to nonbroadcast

B. broadcast to nonbroadcast

C. point-to-multipoint to broadcast

D. broadcast to point-to-point

Correct Answer: *B*
Reference:
https://www.freeccnaworkbook.com/workbooks/ccna/configuring-ospf-network-types

Community vote distribution

B (100%)

XalaGyan Highly Voted 3 years, 2 months ago

According to the document the following is supported.

Here is a quick list of which combinations will work:
Broadcast to Broadcast
Non-Broadcast to Non-Broadcast
Point-to-Point to Point-to-Point
Point-to-Multipoint to Point-to-Multipoint
Broadcast to Non-Broadcast (adjust hello/dead timers)
Point-to-Point to Point-to-Multipoint (adjust hello/dead timers)

https://anetworkartist.blogspot.com/2010/02/mixing-matching-different-ospf-network.html

upvoted 31 times

rami_mma Most Recent 8 months, 1 week ago

Point-to-point and point-to-multipoint do not use DR/BDR so you can use them with BC and Non-Bc since the BCor Non-BC use the DR/BDR.
The correct answer BC with Non-BC

upvoted 1 times

HungarianDish 8 months, 3 weeks ago

Selected Answer: B

https://learningnetwork.cisco.com/s/question/0D53i00000Kt4FfCAJ/ospf-network-types

Some adjustments are necessary however (timers, plus static neighbour configuration on one end)

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: B

tested:
router ospf 1
passive-interface default
no passive-interface Vlan10
network 0.0.0.0 255.255.255.255 area 0
neighbor 192.168.255.3
sw1#
sw1#
sw1#s runn int vlan 10
Building configuration...

Current configuration : 142 bytes
!
interface Vlan10
description "MGMT"
ip address 192.168.255.2 255.255.255.0
ip ospf network non-broadcast
ip ospf hello-interval 10
end

sw1#sh ip ospf nei

Neighbor ID Pri State Dead Time Address Interface
10.0.0.1 1 FULL/BDR 00:00:31 192.168.255.3 Vlan10
sw1#

upvoted 2 times

nushadu 11 months, 2 weeks ago

far-end:

cisco#show runn int e0/0.10
Building configuration...

Current configuration : 116 bytes
!
interface Ethernet0/0.10
description to_sw1
encapsulation dot1Q 10
ip address 192.168.255.3 255.255.255.0
end

cisco#show runn | s router ospf
router ospf 1
passive-interface default
no passive-interface Ethernet0/0.10
network 0.0.0.0 255.255.255.255 area 0
cisco#sh ip ospf nei

Neighbor ID Pri State Dead Time Address Interface
192.168.255.2 1 FULL/DR 00:00:38 192.168.255.2 Ethernet0/0.10
cisco#

upvoted 1 times

Jothi 1 year, 3 months ago

Provided answer is correct - B
Compatible Network types:
Broadcast to Broadcast
Non-broadcast to Non-broadcast
Point-to-Point to Point-to-Point
Broadcast to Non-broadcast (adjust hello/dead timers)
Point-to-Point to Point-to-Multipoint (adjust hello/head timers)

upvoted 4 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 2 times

BigMomma4752 2 years, 8 months ago

The correct answer is B.

upvoted 3 times

Helloory 3 years ago

B is correct

upvoted 1 times

rezavage 3 years ago

A is the only option that both side have the same timers

upvoted 2 times

rezavage 3 years ago

I'll go for A because broadcast network cant form adjacencies with non-broadcast netwoeks

upvoted 2 times

TheNetworkStudent 3 years, 2 months ago

checked it in GNS3, D doesn't work. Neighborship builds but routes don't get exchanged, routing table remains empty. It's because the method of exchanging routes is different hence it isn't compatible.

R4#show ip ospf neigh

Neighbor ID Pri State Dead Time Address Interface
3.3.3.3 1 FULL/BDR 00:00:35 10.0.1.1 GigabitEthernet0/0

R3#show ip ospf neigh

Neighbor ID Pri State Dead Time Address Interface
4.4.4.4 0 FULL/ - 00:00:37 10.0.1.2 GigabitEthernet0/0

upvoted 2 times

TheNetworkStudent 3 years, 2 months ago

When you do broadcast and non-broadcast, you need to edit the hello and dead intervals but it will build full adjacencies and will exchanges routes. It must be B.

upvoted 3 times

Os_ 3 years, 2 months ago

from Pearsontestprep's ENARSI test explanation Question24:

"Although it is highly recommended that network types match, it is not a requirement as long as the network types are compatible. Since the network types Broadcast and Point-to-Point use the same timers (Hello 10 and Dead 40), by default they will be able to form a neighbor adjacency with each other. Although Broadcast uses a DR/BDR and Point-to-Point does not, that difference will not prevent them from forming a full neighbor adjacency and synchronizing their LSDBs."

Means adjust timers and all combis should be compatible imho.

upvoted 2 times

DJOHNR 3 years, 3 months ago

I think it is A.... go to your router and try this...

Hub(config)#interface serial 0/0
Hub(config-if)#ip address 192.168.123.1 255.255.255.0
Hub(config-if)#encapsulation frame-relay
Hub(config-if)#ip ospf network point-to-multipoint non-broadcast
Hub(config-if)#exit
Hub(config)#router ospf 1
Hub(config-router)#network 192.168.123.0 0.0.0.255 area 0
Hub(config-router)#neighbor 192.168.123.2
Hub(config-router)#neighbor 192.168.123.3

upvoted 1 times

jzjs 3 years, 3 months ago

i think it depends on whether choose DR/BDR
instead of hello dead time cause it can be changed
so I agree on B

upvoted 4 times

rezareza 3 years, 5 months ago

A and D
Broadcast
Hello: 10 Wait: 40 Dead: 40
Point-to-point
Hello: 10 Wait: 40 Dead: 40

Non-broadcast
Hello: 30 Wait: 120 Dead: 120
Point-to- multipoint
Hello: 30 Wait: 120 Dead: 120

upvoted 1 times

MaxMoon 3 years, 5 months ago

A and B

upvoted 1 times

Question #115 *Topic 1*

Refer to the exhibit.

```
R1#debug ip ospf hello
R1#debug condition interface Fa0/1
        Condition 1 Set
```

Which statement about the OSPF debug output is true?

A. The output displays OSPF hello messages which router R1 has sent or received on interface Fa0/1.

B. The output displays all OSPF messages which router R1 has sent or received on all interfaces.

C. The output displays all OSPF messages which router R1 has sent or received on interface Fa0/1.

D. The output displays OSPF hello and LSACK messages which router R1 has sent or received.

Correct Answer: *A*

Community vote distribution

A (100%)

nushadu 11 months, 2 weeks ago

Selected Answer: A

cisco#show debugging

OSPF:
OSPF hello debugging is on

Condition 1: interface Et0/0.10 (1 flags triggered)
Flags: Et0/0.10

cisco#
*Dec 16 21:16:19.138: OSPF-1 HELLO Et0/0.10: Send hello to 224.0.0.5 area 0 from 192.168.255.3
cisco#
*Dec 16 21:16:20.677: OSPF-1 HELLO Et0/0.10: Rcv hello from 192.168.255.2 area 0 192.168.255.2
cisco#
*Dec 16 21:16:28.785: OSPF-1 HELLO Et0/0.10: Send hello to 224.0.0.5 area 0 from 192.168.255.3
cisco#
*Dec 16 21:16:30.568: OSPF-1 HELLO Et0/0.10: Rcv hello from 192.168.255.2 area 0 192.168.255.2
cisco#

upvoted 1 times

Pudu_vlad 1 year, 5 months ago

A is correct

upvoted 3 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 4 times

P1Z7C 2 years, 8 months ago

debug condition interface

Limits output for some debugging commands based on the interfaces.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/debug/command/a1/db-a1-cr-book/db-c1.html

upvoted 1 times

ezer 3 years, 1 month ago

f0\1 is wrong

upvoted 2 times

Question #116 *Topic 1*

Which statement about multicast RPs is true?

A. RPs are required only when using protocol independent multicast dense mode.

B. RPs are required for protocol independent multicast sparse mode and dense mode.

C. By default, the RP is needed periodically to maintain sessions with sources and receivers.

D. By default, the RP is needed only to start new sessions with sources and receivers.

Correct Answer: *D*

Reference:

https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

Community vote distribution

D (100%)

spittin_venom Highly Voted 3 years, 3 months ago

Answer is D from the linked doc.

n most cases, the placement of the RP in the network is not a complex decision. By default, the RP is needed only to start new sessions with sources and receivers. Consequently, the RP experiences little overhead from traffic flow or processing. In PIM-SM version 2, the RP requires less processing than in PIM-SM version 1 because sources must only periodically register with the RP to create state.

upvoted 11 times

Eddgar0 Most Recent 1 year, 7 months ago

Selected Answer: D

From the link is correct the provided answer

upvoted 2 times

Question #117 *Topic 1*

To increase total throughput and redundancy on the links between the wireless controller and switch, the customer enabled LAG on the wireless controller.
Which EtherChannel mode must be configured on the switch to allow the WLC to connect?

A. Active

B. Passive

C. On

D. Auto

Correct Answer: *C*
Reference:
https://community.cisco.com/t5/wireless-mobility-documents/lag-link-aggregation/ta-p/3128669

Community vote distribution

C (100%)

skh Highly Voted 3 years ago

C
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010100001.html
LAG requires the EtherChannel to be configured for 'mode on' on both the controller and the Catalyst switch.
upvoted 9 times

djedeen Most Recent 3 months, 3 weeks ago

Controller only supports the on mode of the LAG
LACP and PAgP are not supported on the controller
upvoted 2 times

Pudu_vlad 1 year, 2 months ago

C is correct
upvoted 2 times

GreatDane 1 year, 5 months ago

Ref: LAG - Link Aggregation - Cisco Community

Post by Rajan Parmar

"...
Controller only supports the on mode of the LAG
...
"Make sure the port-channel on the switch is configured for the IEEE standard Link Aggregation Control Protocol (LACP), not the Cisco proprietary Port Aggregation Protocol (PAgP)."Controller only supports the on mode of the LAG.
..."

A. Active

Wrong answer.

B. Passive

Wrong answer.

C. On

Correct answer.

D. Auto

Wrong answer.
upvoted 3 times

riccardorossi 1 year, 5 months ago

Selected Answer: C
C is the correct answer for AirOS WLC. With the new 9800 IOS-XE WLC it is possible all the solution.
upvoted 2 times

Eddgar0 1 year, 7 months ago

Selected Answer: C

Given anser are correct

upvoted 1 times

Question #118 *Topic 1*

Based on this interface configuration, what is the expected state of OSPF adjacency?

R1:
```
interface GigabitEthernet0/1
  ip address 192.0.2.1 255.255.255.252
  ip ospf 1 area 0
  ip ospf hello-interval 2
  ip ospf cost 1
end
```

R2:
```
interface GigabitEthernet0/1
  ip address 192.0.2.2 255.255.255.252
  ip ospf 1 area 0
  ip ospf cost 500
end
```

A. 2WAY/DROTHER on both routers

B. not established

C. FULL on both routers

D. FULL/BDR on R1 and FULL/BDR on R2

Correct Answer: *B*

Community vote distribution

B (100%)

TheNetworkStudent Highly Voted 3 years, 2 months ago

No source given, when the config is applied between 2 routers:

*Sep 25 13:36:55.438: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on GigabitEthernet0/0 from FULL to DOWN, Neighbor Down: Dead timer expired

When you set the hello the dead is automatically changed to 4x the hello:

Timer intervals configured, Hello 2, Dead 8

The other side is default (Hello of 10s) hence sends it too late every time. B is correct

upvoted 34 times

SandyIndia 2 years, 3 months ago

- Hallo & Dead timer must match - Router ID must not match
- Area id must match
- Auth type & Auth Data must match
- Subnet mask must match
- MTU Size must match
- Stub Flag must match

upvoted 21 times

ArShuRaZ 2 years, 10 months ago

Thank you for the knowledge.

upvoted 6 times

danman32 Most Recent 4 months, 4 weeks ago

I was considering the scenario if the hello timer was left at default for R1.
I almost considered answer D: but then I noticed it shows both routers as BDR. Based on the subnet, only these two routers could exist on the segment, so one would have to be a DR, the other a BDR. Answer D says both are BDRs, but one has to be a DR. Even if there were more routers on a segment, you still would only have one BDR so if another router were DR, then either R1 or R2 would be 2WAY/DROTHER, or both.
Then I saw answer C. Indeed both would be full, though one would be DR, the other BDR, if it weren't for the hello timer change.
But then we don't have enough information to determine the election results. Need priority, router ID, loopback IPs and all other IPs on the routers.

upvoted 1 times

CKL_SG 5 months ago

Selected Answer: B

Test in GNS3 it was due to different timer set
OSPF was form after R2 set the same timer

ip ospf hello-interval 2
upvoted 1 times

turbosteam888 1 year, 1 month ago

so if the hello set to 3 it will be established?
upvoted 1 times

StefanOT2 10 months, 2 weeks ago

10 Seconds. It is a Ethernet Interface = Broadcast by default. Reference: https://www.freeccnaworkbook.com/workbooks/ccna/configuring-ospf-network-types
upvoted 2 times

Pudu_vlad 1 year, 2 months ago

B is the correct ans
upvoted 1 times

Eddgar0 1 year, 7 months ago

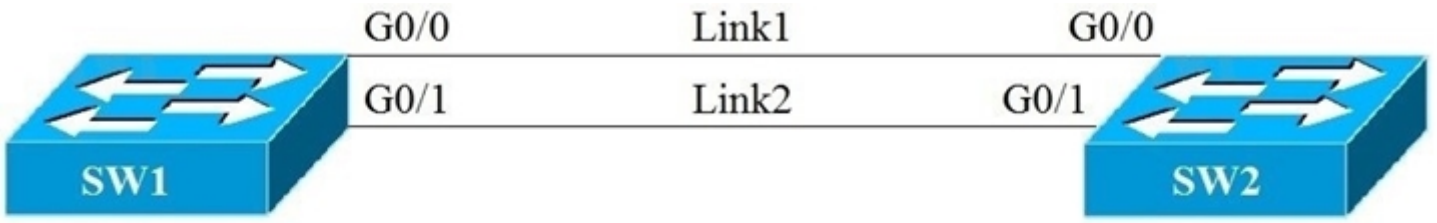
Selected Answer: B

Timers must match between 2 ospf router to be neighbors
upvoted 4 times

Ansari0071 3 years, 5 months ago

B is correct answer
upvoted 4 times

Refer to the exhibit.




```
SW2#show spanning-tree

 VLAN0001

   Spanning tree enabled protocol ieee

   Root ID     Priority    32769
               Address     5000.0005.0000
               Cost        4
               Port        1 (GigabitEthernet0/0)
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

   Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
               Address     5000.0006.0000
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
               Aging Time  300 sec

Interface           Role  Sts  Cost  Prio.Nbr   Type
---------------     ----  ---  ----  --------  --------------------
Gi0/0               Root  FWD   4    128.1      P2p
Gi0/1               Altn  BLK   4    32.2       P2p
```

Link1 is a copper connection and Link2 is a fiber connection. The fiber port must be the primary port for all forwarding. The output of the show spanning-tree command on SW2 shows that the fiber port is blocked by spanning tree. An engineer enters the spanning-tree port-priority 32 command on G0/1 on SW2, but the port remains blocked.
Which command should be entered on the ports that are connected to Link2 to resolve the issue?

A. Enter spanning-tree port-priority 4 on SW2.

B. Enter spanning-tree port-priority 32 on SW1.

C. Enter spanning-tree port-priority 224 on SW1.

D. Enter spanning-tree port-priority 64 on SW2.

Correct Answer: *B*

Community vote distribution

rezavage Highly Voted 3 years ago

B is correct. whenever a tie happens on two ports that receiving the same advertised cost and want to choose the RP , the port that is receiving the bpdu from the upstream switch port with lower priority will win the race and will becom the root port. so, in order to change the root port on SW2 you have to lower the port priority on switch 1.

upvoted 20 times

jmaroto Highly Voted 2 years, 8 months ago

B is correct. Check in lab, when the switch 2 receive the bpdu with port priority it change the Altn Blocked port to root port.

Mar 8 23:24:09.971: RSTP(2): updt roles, received superior bpdu on Et0/1
*Mar 8 23:24:09.971: RSTP(2): Et0/1 is now root port
*Mar 8 23:24:09.971: RSTP(2): Et0/0 blocked by re-root
*Mar 8 23:24:09.971: RSTP(2): Et0/0 is now alternate
*Mar 8 23:24:09.971: RSTP[2]: Et0/0 state change completed. New state is [blocking]
*Mar 8 23:24:09.971: RSTP[2]: Et0/1 state change completed. New state is [forwarding]
*Mar 8 23:24:09.971: RSTP(2): starting topology change timer for 35 seconds
*Mar 8 23:24:09.971: STP[2]: Generating TC trap for port Ethernet0/1

upvoted 6 times

djedeen Most Recent 3 months ago

Selected Answer: B

Lower port priority on upstream (bpdu sender) will be selected, default value is 128.

upvoted 1 times

teikitiz 5 months ago

Selected Answer: B

This link really helped refreshing this topic.
https://www.omnisecu.com/cisco-certified-network-associate-ccna/how-spanning-tree-protocol-stp-select-root-port.php

upvoted 1 times

NTGuru 7 months, 2 weeks ago

Correct Answer B
Order of precedence
1. A lower Root Bridge ID
2. A lower path cost to the Root
3. A lower Sending Bridge ID
4. A lower Sending Port ID

upvoted 1 times

HungarianDish 8 months, 2 weeks ago

Selected Answer: B

root port election: configure "port priority" on upstream switches on designated ports or modify "port cost" on downstream switches on root ports

https://community.cisco.com/t5/routing/spanning-tree-with-port-priority/td-p/1815059

upvoted 2 times

x3rox 9 months, 3 weeks ago

There is a problem with this question. The Root Switch is SW1 so SW2 needs to find the closest port to the root. Since we have a tie in cost SW2 will select the port receiving the lowest priority from the upstream switch. In the output we see that G0/1 (Fiber) is ALREADY the lowest priority on SW1 (32.2). So it should've been elected as RP NOT G0/0. WHY IS G0/1 IN BLOCKING STATE???

upvoted 2 times

x3rox 9 months, 3 weeks ago

Forget it. I misunderstood the output. The column PrioNbr is local. ok -So.... SW needs to W2 will select the port receiving the lowest priority from the upstream switch. Asumming that it has the default values SW2 will receive BPDUs indicating Priorities as follows: 128.1 for G0/0 and 128.2 for G0/1. SW will elect the lowest between the two which is G0/0 as a Root Port (Link 1 - Cooper). So, in order to change this selection the admin will need to go ahead the change the port priority on SW1 to a lower value for G0/1 so that SW2 will elected as it's Root Port. Answer B is correct as it will change the default 128.2 to 32.2 for G0/1. Now SW2 will see that 32.2 on G0/1 is lower than the receiving priority of 128.1 that G0/0 has and will make G0/1 it's Root Port (Link 2 - Fiber) - DO NOT LOOK at the column Prio.Nbr, these are local values that don't do anything in this scenario.

upvoted 2 times

x3rox 9 months, 3 weeks ago

Switch(config-if)#spanning-tree port-priority ?
<0-224> port priority in increments of 32

upvoted 1 times

x3rox 9 months, 3 weeks ago

from GNS3
vios_l2-ADVENTERPRISEK9-M
Experimental Version 15.2(20170321:233949)

upvoted 1 times

nushadu 11 months, 2 weeks ago

In my current lab, I could not find 32 value, only 64, root sw:

sw2(config-if)#spanning-tree port-priority ?
<0-192> port priority in increments of 64

sw2(config-if)#spanning-tree port-priority 32
% Port Priority in increments of 64 is required

sw2(config-if)#spanning-tree port-priority 64
sw2(config-if)#do s runn interface port-channel 2
Building configuration...

Current configuration : 136 bytes
!
interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
spanning-tree port-priority 64
end

sw2(config-if)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

far-end before changing priority (see Po2 port):
sw1#
sw1#show spanning-tree vlan 1 | i Po2|Et0/3
Et0/3 Root FWD 100 128.4 Shr

Po2 Altn BLK 100 128.66 Shr
sw1#
!!! after
sw1#
sw1#show spanning-tree vlan 1 | i Po2|Et0/3
Et0/3 Altn BLK 100 128.4 Shr
Po2 Root FWD 100 128.66 Shr
sw1#

upvoted 1 times

nushadu 11 months, 2 weeks ago

I would say "B" but I did not have this option in my lab 32 (only 64), maybe in the newest version IOS ...

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: B

B is correct because in this scenario sw2 will select the root port of the lowest port priority of the advertising switch (switch that send the bpdu) in this case the SW1.

upvoted 5 times

youtri 2 years ago

notice that Ethernet port priority by default is 128

tested by eve ng

Switch(config-if)#spanning-tree port-priority 32
% Port Priority in increments of 64 is required

upvoted 4 times

Hugh_Jazz 2 years, 3 months ago

B is absolutely correct. Change PP on upstream switch.

upvoted 1 times

msz_battle 2 years, 5 months ago

DSW1(config-if)#spanning-tree port-priority 32
% Port Priority in increments of 64 is required
:)

upvoted 3 times

vdsdrs 2 years, 3 months ago

Platform depended, lowest increment can be 16.

upvoted 5 times

TimHon 2 years, 7 months ago

https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/spanning-tree-port-priority.html

upvoted 1 times

Tuborger 3 years ago

D. Enter spanning-tree port-priority 64 on SW2.

upvoted 2 times

AliMo123 2 years, 6 months ago

you have to try on both SWs before increment the port priority to 64, so try 32 on SW1 and it works just perfectly fine. If that did not work, then definitely 64 on SW2 will be the correct one.

upvoted 3 times

XalaGyan 1 year, 11 months ago

Port Priority is local to the switch. it wont matter what you do on the remote end as it is significant to the remote switch itself and wont be advertised.

upvoted 2 times

youtri 2 years ago

even you change the priority in SW2 it doesn t change the blk port, i tested in eve ng,you should change priority in SW1

upvoted 2 times

Question #120 *Topic 1*

Which behavior can be expected when the HSRP version is changed from 1 to 2?

A. No changes occur because the standby router is upgraded before the active router.

B. No changes occur because version 1 and 2 use the same virtual MAC OUI.

C. Each HSRP group reinitializes because the virtual MAC address has changed.

D. Each HSRP group reinitializes because the multicast address has changed.

Correct Answer: *C*

Community vote distribution

C (100%)

Sparks026 Highly Voted 3 years, 6 months ago

Option C is correct - Even though HSRP version 2 uses the new IP multicast address 224.0.0.102 to send hello packets instead of the multicast address of 224.0.0.2, used by HSRP version 1; when the HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.

upvoted 33 times

Quick_X 3 years, 4 months ago

Correct, from cisco directly; "When the HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.?"

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-hsrp-v2.html#:~:text=Version%201%20is%20the%20default,the%20multicast%20address%20of%20224.0.&text=HSRP%20version%202%20permits%20an,MAC%20address%20range%200000.0C9F.

upvoted 7 times

[Removed] Highly Voted 1 year, 7 months ago

Selected Answer: C

HSRP version 1, virtual router's MAC address is 0000.0c07.ACxx , where xx is the HSRP group.
HSRP version 2, virtual MAC address is 0000.0C9F.Fxxx, where xxx is the HSRP group.
Note: HSRP for IPv6, MAC address range from 0005.73A0.0000 through 0005.73A0.0FFF.

upvoted 5 times

Pudu_vlad Most Recent 1 year, 2 months ago

C is correct

upvoted 1 times

GreatDane 1 year, 5 months ago

Ref: First Hop Redundancy Protocols Configuration Guide, Cisco IOS Release 15M&T

"...
Information About HSRP Version 2
HSRP Version 2 Design
...
When the HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.
..."

A. No changes occur because the standby router is upgraded before the active router.

Wrong answer.

B. No changes occur because version 1 and 2 use the same virtual MAC OUI.

Wrong answer.

C. Each HSRP group reinitializes because the virtual MAC address has changed.

Correct answer.

D. Each HSRP group reinitializes because the multicast address has changed.

Wrong answer.

upvoted 1 times

rpidcock 2 years, 3 months ago

Agree with all that C is the correct answer. When changed the group reinitializes because it has a new virtual MAC address.

upvoted 1 times

edg 3 years, 3 months ago

Confirm that the correct option is C, following the next text:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-hsrp-v2.html

"When the HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address."

upvoted 4 times

Jack1188 3 years, 4 months ago

The correct answer is C

upvoted 4 times

AndresV 3 years, 4 months ago

C is Correct

upvoted 4 times

Saqib79 3 years, 6 months ago

Correct Option is D.

upvoted 2 times

Refer to the exhibit.

```
R1#show ip bgp
BGP table version is 32, local router ID is 192.168.101.5
Status codes: S suppressed, d damped, h history, *valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
     Network          Next Hop            Metric     LocPrf     Weight    Path
*    192.168.102.0    192.168.101.18          80                    0    64517i
*                     192.168.101.14          80         80         0    64516i
*                     192.168.101.10                                0    64515 64515i
*>                    192.168.101.2                                 32768    64513i
*                     192.168.101.6                         80      0    64514 64514i
```

Which IP address becomes the active next hop for 192.168.102.0/24 when 192.168.101.2 fails?

A. 192.168.101.10

B. 192.168.101.14

C. 192.168.101.6

D. 192.168.101.18

Correct Answer: *D*

Community vote distribution

D (100%)

DJOHNR Highly Voted 3 years, 3 months ago

An empty LocPrf is set at 100, the highest number wins for next hop selection.

So the two values of 80 for LocPrf can be ignored.

That means you can thow away .6 and .14. This leaves .18 and .10

Next look at the Path. Shortest path wins! Between .18 and .10, .18 has a shorter path, 64517i vs 64515 64515i
The right answer is D

upvoted 64 times

CBlu Highly Voted 3 years, 5 months ago

Just to clarify:
The empty "local preference" implies it's a local preference of 100. And the highest local preference wins, hence the 2 entries with local pref. 80 can be ignored.

upvoted 47 times

Caradum Most Recent 1 year ago

Selected Answer: D

D is correct, as many explained it correctly here.

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: D

AS have higer loca preferences and shorter ASPATH

upvoted 1 times

Violator 1 year, 9 months ago

This question is still asked. Passed today.

upvoted 1 times

gomezdiazfm 1 year, 10 months ago

B. 192.168.101.14 si the correct answer. LocalPref is 100 when is a iBGP peer, but in the exhibit we have a eBGP peer.

upvoted 1 times

youtri 1 year, 12 months ago

the order of the attributes is: W-L-A-M

1-Weight (the hightest wins)

2-Local preference (default value =100) (the hightest wins)

-3As path (the lowest AS path wins)

4-Metric (the lowest wins)

upvoted 8 times

Hack4 2 years, 5 months ago

right answer

upvoted 2 times

davdtech 2 years, 8 months ago

Weight, local prf, Originate,AS , Origin MED
it's very useful to use

D is correct

upvoted 3 times

networker 3 years, 3 months ago

ok thanks

upvoted 1 times

mbustani 3 years, 3 months ago

D is correct.
lower metric wins. default 100
higher local preference wins. default 100
so, by elimination, it remains only .14 and .18.
first comparison is metric and after that local preference. both .14 and .18 have the same metric. So, let's compare local preference: .14 = 80 and .18 = 100 (default).
.18 is the correct. letter D.

upvoted 6 times

Burik 5 months, 3 weeks ago

No. Your answer is correct, but your reasoning is wrong. BGP Metric [MED] defaults to 0 and it's checked after Weight, Local Preference, and AS path length, in that order.

upvoted 1 times

chalosca 3 years, 4 months ago

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
18 and 10 has 100 (loc_pref) / they are both 'i' / shortest AS_PATH wins

upvoted 2 times

Question #122 *Topic 1*

Which PAgP mode combination prevents an EtherChannel from forming?

A. auto/desirable

B. desirable/desirable

C. desirable/auto

D. auto/auto

Correct Answer: *D*
Reference:
https://www.omnisecu.com/cisco-certified-network-associate-ccna/etherchannel-pagp-and-lacp-modes.php

Community vote distribution

D (100%)

skh Highly Voted 3 years ago

Auto just listens for PAgP and never tries to initiate an EtherChannel negotiation, and thats why you can't have both sides as Auto.

Correct D auto/auto no forming

upvoted 20 times

XalaGyan 1 year, 12 months ago

wonderful explanation

upvoted 2 times

[Removed] Most Recent 5 months ago

Selected Answer: D

corect

upvoted 1 times

KZM 1 year, 2 months ago

Auto/Desirable and Desirable/Desirable configuration in 2 routers will form PAgP. Auto/Auto in two sides will never negotiate from any side and never form EtherChannel.

upvoted 2 times

brightsyds 1 year, 9 months ago

D for sure!

upvoted 1 times

Question #123 *Topic 1*

If a VRRP master router fails, which router is selected as the new master router?

A. router with the lowest priority

B. router with the highest priority

C. router with the highest loopback address

D. router with the lowest loopback address

Correct Answer: *B*

Community vote distribution

B (100%)

edg Highly Voted 3 years, 3 months ago

https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/350_550/index.html#page/tesla_350_550_olh/ts_vrrp_18_09.html

In the "Basic VRRP Topology" figure, if Router A, the virtual router master, fails, a selection process takes place to determine if virtual router backups B or C must take over. If Routers B and C are configured with the priorities of 101 and 100, respectively, Router B is elected to become virtual router master because it has the higher priority. If both have the same priority, the one with the higher IP address value is selected to become the virtual router master.

upvoted 10 times

[Removed] Most Recent 5 months ago

Selected Answer: B

correct

upvoted 1 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 1 times

Question #124 *Topic 1*

Which two mechanisms are available to secure NTP? (Choose two.)

A. IPsec

B. IP prefix list-based

C. encrypted authentication

D. TACACS-based authentication

E. IP access list-based

Correct Answer: *CE*
Reference:
https://www.cisco.com/c/dam/en/us/td/docs/ios-xml/ios/bsm/configuration/xe-3se/3650/bsm-xe-3se-3650-book.html

Community vote distribution

CE (100%)

AndresV Highly Voted 3 years, 4 months ago

From the reference Link:
Cisco strongly recommends that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

upvoted 21 times

supershysherlock Highly Voted 3 years ago

"The two security features available are an access list-based restriction scheme and an encrypted authentication mechanism"

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html

upvoted 9 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: CE

cisco(config)#ntp ?
access-group Control NTP access
allow Allow processing of packets
authenticate Authenticate time sources
authentication-key Authentication key for trusted time sources

upvoted 2 times

Pudu_vlad 1 year, 2 months ago

answer c and e

upvoted 1 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 2 times

Question #125 *Topic 1*

In OSPF, which LSA type is responsible for pointing to the ASBR router?

A. type 1

B. type 2

C. type 3

D. type 4

Correct Answer: *D*

DJOHNR Highly Voted 3 years, 3 months ago

LSA Type 1: Router LSA
LSA Type 2: Network LSA
LSA Type 3: Summary LSA
LSA Type 4: Summary ASBR LSA
LSA Type 5: Autonomous system external LSA
LSA Type 6: Multicast OSPF LSA
LSA Type 7: Not-so-stubby area LSA
LSA Type 8: External attribute LSA for BGP

https://networklessons.com/ospf/ospf-lsa-types-explained

D. Type 4

upvoted 32 times

flash007 Most Recent 4 months, 1 week ago

Type 3 is the ABR and Type 4 is the ASBR

upvoted 1 times

Nadalex 1 year, 1 month ago

Type 1 - Router LSA - by all routers within the area Within the area
Type 2 - Network LSA - DR (Designated router) - Within the area
Type 3 - Summary LSA - ABR (Area Border Router) - Within the network
Type 4 - ASBR Summary - ABR (Area Border Router) - Within the network
Type 5 - AS-external LSA - ASBR (Autonomous System Boundary Router) - Within the network
Type 6 - Group Membership LSA -
Type 7 - NSSA External LSA - ASBR (Autonomous System Boundary Router) - Intra-area
Type 8 - Link-local LSA (OSPFv3) - by all routers - within the area Link
Type 9 - Link-local opaque (OSPFv2) - Link-local -
Type 9 - Intra-Area-Prefix (OSPFv3) - Link-local
Type 10 - Area-local opaque - Area-local
Type 11 - Autonomous System opaque - Within the network

upvoted 3 times

brightsyds 1 year, 9 months ago

D for sure!

LSA 4 ==> These are LSA's that announces the presence of an ASBR to other areas

upvoted 1 times

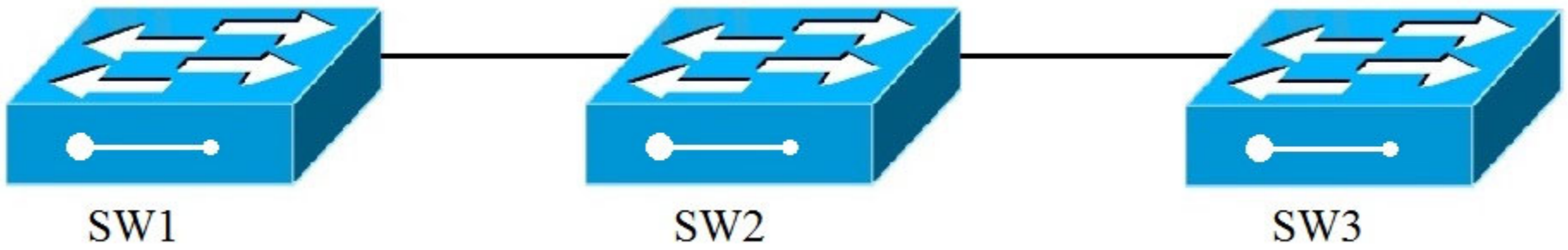
TimHon 2 years, 7 months ago

https://www.router-switch.com/faq/6-types-of-ospf-lsa.html

upvoted 1 times

Question #126 *Topic 1*

Refer to the exhibit.



VLANs 50 and 60 exist on the trunk links between all switches. All access ports on SW3 are configured for VLAN 50 and SW1 is the VTP server. Which command ensures that SW3 receives frames only from VLAN 50?

A. SW1(config)#vtp mode transparent

B. SW3(config)#vtp mode transparent

C. SW2(config)#vtp pruning

D. SW1(config)#vtp pruning

Correct Answer: *D*

Reference:

https://www.orbit-computer-solutions.com/vtp-pruning/

Community vote distribution

D (90%) 10%

P1Z7C Highly Voted 2 years, 8 months ago

VTP pruning should only be enabled on VTP servers, all the clients in the VTP domain will automatically enable VTP pruning.
D is correct, since SW1 is the VTP server

upvoted 37 times

XDR Highly Voted 8 months ago

Selected Answer: D

Answer is D. Verified applying the configuration in production environment.

upvoted 6 times

Degen6969 7 months ago

I too like to live dangerously

upvoted 3 times

flash007 Most Recent 4 months, 1 week ago

the vtp server is switch1 and that is where the pruning needs applying to

upvoted 1 times

mrtattoo 6 months, 4 weeks ago

Another question I hate Cisco for. C and D are both valid options. It depends. To really answer that question we would need more information. Knowing Cisco they probably want us to got with D, because Cisco likes enterprise business.....

upvoted 1 times

Rose66 10 months, 4 weeks ago

Selected Answer: D

as described in provided link.....
"VTP pruning should only be enabled on VTP servers, all the clients in the VTP domain will automatically enable VTP pruning. By default, VLANs 2 – 1001 are pruning eligible, but VLAN 1 can’t be pruned because it’s an administrative VLAN. Both VTP versions 1 and 2 support pruning."

upvoted 2 times

Ayman_B 11 months ago

Selected Answer: D
pruning is only ever done on servers

upvoted 1 times

mansaf 11 months, 1 week ago

pruning is only ever done on servers -> d

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: D

far-end has vlan30 allowed on trunk:
sw1(config)#do s int tru

Port Mode Encapsulation Status Native vlan
Et0/0 on 802.1q trunking 1
Et0/3 desirable n-isl trunking 1
Po2 on 802.1q trunking 1

Port Vlans allowed on trunk
Et0/0 1-4094
Et0/3 1-4094
Po2 1-4094

Port Vlans allowed and active in management domain
Et0/0 1,10,30,40,50
Et0/3 1,10,30,40,50
Po2 1,10,30,40,50

Port Vlans in spanning tree forwarding state and not pruned
Et0/0 1,10,30,40,50
Et0/3 1,30 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Po2 1
sw1(config)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

far-end adding vlan50 in trunk:
sw2(config-if)#do s runn int e0/0
Building configuration...

Current configuration : 161 bytes
!
interface Ethernet0/0
description to_e0/0_r2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 30
switchport mode trunk
duplex auto
end

sw2(config-if)# switchport trunk allowed vlan add 50
sw2(config-if)#do s runn int e0/0
Building configuration...

Current configuration : 164 bytes
!
interface Ethernet0/0
description to_e0/0_r2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 30,50
switchport mode trunk
duplex auto
end

sw2(config-if)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

pruning feature allows\add this vlan50 to the forwarding on the trunk on the upstream sw1:
sw1(config)#do s int tru
... omitted...
Port Vlans allowed and active in management domain
Et0/0 1,10,30,40,50
Et0/3 1,10,30,40,50
Po2 1,10,30,40,50

Port Vlans in spanning tree forwarding state and not pruned
Et0/0 1,10,30,40,50
Et0/3 1,30,50 <<<<<<<<<<<<<<<<<<<< + vlan 50
Po2 1
sw1(config)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw1(config)#do s vtp sta
VTP Version capable : 1 to 3
VTP version running : 1
VTP Domain Name : ccnp
VTP Pruning Mode : Enabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.1000
Configuration last modified by 192.168.255.2 at 12-17-22 16:36:18

Local updater ID is 192.168.255.2 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN:

VTP Operating Mode : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 9
Configuration Revision : 4
MD5 digest : 0xF4 0x8E 0xFF 0xAD 0x30 0xDF 0x35 0x92
0x61 0xAE 0x50 0x47 0xB2 0x07 0xA0 0xF1
sw1(config)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw2#sh vtp status
VTP Version capable : 1 to 3
VTP version running : 1
VTP Domain Name : ccnp
VTP Pruning Mode : Enabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.4000
Configuration last modified by 192.168.255.2 at 12-17-22 16:36:18

Feature VLAN:

VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 9
Configuration Revision : 4
MD5 digest : 0xF4 0x8E 0xFF 0xAD 0x30 0xDF 0x35 0x92
0x61 0xAE 0x50 0x47 0xB2 0x07 0xA0 0xF1
sw2#

upvoted 1 times

bora4motion 1 year ago

Selected Answer: C

I'm going with C

upvoted 1 times

IceFireSoul 1 year, 8 months ago

If you prune vlan on SW1, than vlan 60 traffic will not propagate to SW2 either , so D is definitely wrong. Correct answer is C.

upvoted 2 times

Burik 5 months, 3 weeks ago

What? That's not how pruning works. VLAN 60 will be propagated to SW2, if SW2 has access ports in VLAN 60.

upvoted 1 times

timtgh 1 year, 6 months ago

Doesn't pruning only suppress traffic where it's not needed? The only reason SW3 won't get VLAN 60 traffic is because it doesn't need it. If SW2 has ports in VLAN 60, it will receive the VLAN 60 frames, even with pruning applied everywhere.

upvoted 3 times

Nhan 2 years, 1 month ago

Sorry, my previous statement is wrong, bro pruning can only happen on then to server therefore the given answer is correct D

upvoted 3 times

Nhan 2 years, 2 months ago

Vlan pruning can happen on switch 2 as well, the main reason to apply then to pruning in this case and this is the best practice. Applying the pruning at the source rather than wait for the vlan traffic travel to the sw2 then pruning it there. The same concept apply to access-list.

upvoted 1 times

Nirob 2 years, 8 months ago

According to the reference link, shouldn't it pruned on SW2 connecting SW3?

upvoted 1 times

AliMo123 2 years, 6 months ago

only SW1 is VTP server, and since prune vtp is configured only on vtp server mode, then SW1 is correct.

upvoted 5 times

Patrick1234 2 years, 6 months ago

Any documentation on that? I have some doubts here because you can configure pruning on vtp clients as well..

upvoted 6 times

Question #127 *Topic 1*

Which First Hop Redundancy Protocol maximizes uplink utilization and minimizes the amount of configuration that is necessary?

A. GLBP

B. HSRP v2

C. VRRP

D. HSRP v1

Correct Answer: *A*

examShark 2 years, 6 months ago

Given answer is correct

upvoted 4 times

XalaGyan 1 year, 12 months ago

only GLBP can maximize utilzation of links by being ACTIVE/ACTIVE while all others are ACTIVE/STANDBY/LISTENING

NOTE!!!! there is NO MHSRP only HSRP v1 and 2.

upvoted 7 times

Pilgrim5 8 months ago

Thanks so much XalaGyan!

I checked online and saw that MHSRP exists..
https://ipwithease.com/multiple-hsrp-mhsrp-load-sharing-fhrp/

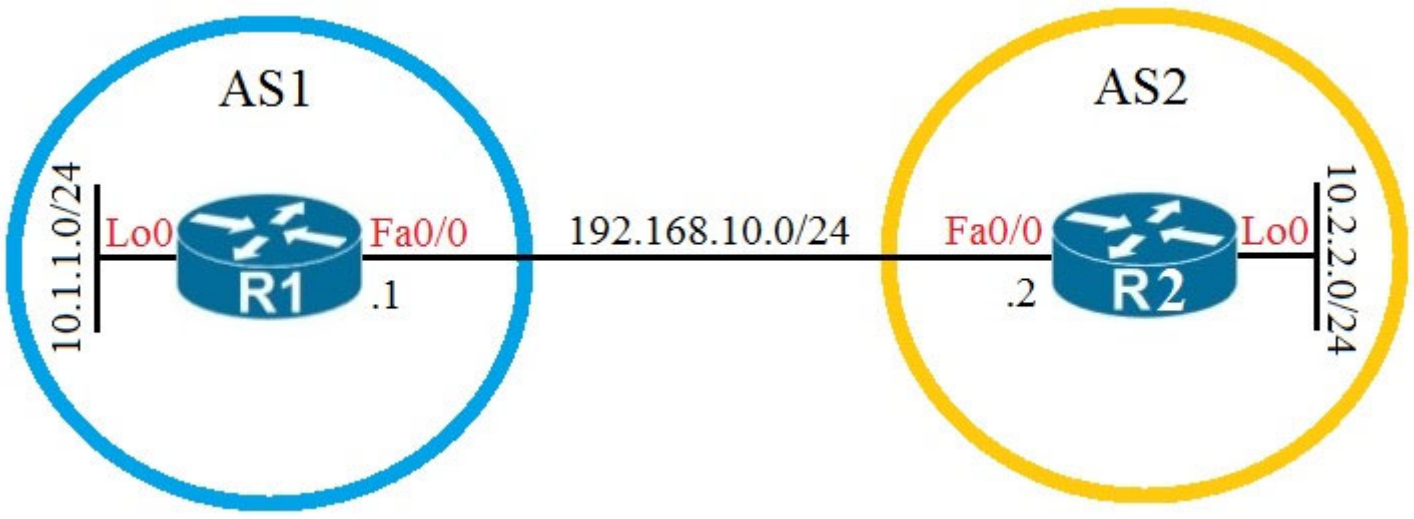
upvoted 3 times

danman32 4 months, 4 weeks ago

Right, because all MHSRP is is having multiple groups, and any FHRP can do that.
The difference is that you leverage one group to be active for one VIP, and the other groups for other VIPs.
Even so, question states minimal amount of configuration. For MHSRP you'd need multiple groups, one group for each uplink you want utilized.

upvoted 1 times

Refer to the exhibit.



Which configuration establishes EBGP neighborship between these two directly connected neighbors and exchanges the loopback network of the two routers through BGP?

A. R1(config)#router bgp 1 R1(config-router)#neighbor 192.168.10.2 remote-as 2 R1(config-router)#network 10.1.1.0 mask 255.255.255.0 R2(config)#router bgp 2 R2(config-router)#neighbor 192.168.10.1 remote-as 1 R2(config-router)#network 10.2.2.0 mask 255.255.255.0

B. R1(config)#router bgp 1 R1(config-router)#neighbor 10.2.2.2 remote-as 2 R1(config-router)#network 10.1.1.0 mask 255.255.255.0 R2(config)#router bgp 2 R2(config-router)#neighbor 10.1.1.1 remote-as 1 R2(config-router)#network 10.2.2.0 mask 255.255.255.0

C. R1(config)#router bgp 1 R1(config-router)#neighbor 192.168.10.2 remote-as 2 R1(config-router)#network 10.0.0.0 mask 255.0.0.0 R2(config)#router bgp 2 R2(config-router)#neighbor 192.168.10.1 remote-as 1 R2(config-router)#network 10.0.0.0 mask 255.0.0.0

D. R1(config)#router bgp 1 R1(config-router)#neighbor 10.2.2.2 remote-as 2 R1(config-router)#neighbor 10.2.2.2 update-source lo0 R1(config-router)#network 10.1.1.0 mask 255.255.255.0 R2(config)#router bgp 2 R2(config-router)#neighbor 10.1.1.1 remote-as 1 R2(config-router)#neighbor 10.1.1.1 update-source lo0 R2(config-router)#network 10.2.2.0 mask 255.255.255.0

Correct Answer: *A*

Community vote distribution

A (100%)

xzioma19 Highly Voted 2 years, 2 months ago

A.
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0
R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
B.
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0
R2(config)#router bgp 2
R2(config-router)#neighbor 10.1.1.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
C.
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.0.0.0 mask 255.0.0.0
R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.0.0.0 mask 255.0.0.0
D.
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#neighbor 10.2.2.2 update-source lo0
R1(config-router)#network 10.1.1.0 mask 255.255.255.0
R2(config)#router bgp 2
R2(config-router)#neighbor 10.1.1.1 remote-as 1
R2(config-router)#neighbor 10.1.1.1 update-source lo0
R2(config-router)#network 10.2.2.0 mask 255.255.255.0

The correct answer is:
A

upvoted 21 times

maurom Highly Voted 3 years, 4 months ago

A is the correct because we are dont use igp

upvoted 14 times

diegodavid82 2 years, 1 month ago

Well, to establish an EBGP neighbor you don't need an IGP.
Answer A is correct because is the right configuration.

upvoted 3 times

techriese Most Recent 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

bora4motion 1 year ago

Selected Answer: A

A is correct.

upvoted 1 times

Pudu_vlad 1 year, 2 months ago

A is the correct

upvoted 1 times

Dataset 1 year, 3 months ago

A is correct

upvoted 1 times

brightsyds 1 year, 9 months ago

A for sure!

upvoted 1 times

pj_machado 2 years, 4 months ago

D is not correct because it does not have the bgp multi-hop configuration command

upvoted 1 times

ArchBishop 1 year, 10 months ago

The routers are essentially directly connected, so they are not required to have 'multi-hop' configured.
For D to be the correct answer, each router would need to have a valid entry in their RIB to reach the destination neighbor's loopback network (more specifically, the neighbors loopback interface). This, at a minimum, could be accomplished with a static route on each router to their neighbor's loopback network, whether a /32 to the interface, or a /24 that covers the entire subnet.
Otherwise, the router will HAVE the neighbor entry, but have no clue how to reach the remote IP.

upvoted 2 times

ArchBishop 1 year, 10 months ago

I am wrong about 'multi-hop.'
eBGP ttl default is 1 hop before discard occurs.
When using loopback as a source, the hop from the loop network to the exit interface's network counts as 1 hop, meaning discard will occur. Multi-hop, update-source, AND valid route, are all required in order to use loopbacks in a neighbor statement.

upvoted 2 times

patrickni 3 years, 2 months ago

chalosca is correct. Answer is A.

upvoted 1 times

akbntc 3 years, 3 months ago

Question has clearly asked "Which configuration establishes EBGP neighborship between these two directly connected neighbors", so option A is correct.

upvoted 1 times

nead 3 years, 3 months ago

A is correct.
D is close but there is no information of the Loopback addresses, so they cannot be used in the neighbor statement

upvoted 1 times

Jack1188 3 years, 4 months ago

The answer is A

upvoted 3 times

imed 3 years, 4 months ago

answer D is correct

upvoted 1 times

bluemoon0817 3 years, 4 months ago

No, D is IBGP's configuration.

upvoted 1 times

nep1019 3 years, 5 months ago

Answer is D. In order to exchange the Loopback addresses you must have the update-source statement added to the neighbor statement.

upvoted 2 times

bluemoon0817 3 years, 4 months ago

D is IBGP's configuration.

upvoted 1 times

chalosca 3 years, 4 months ago

This would require "ebgp-multihop 2"
Answer is A

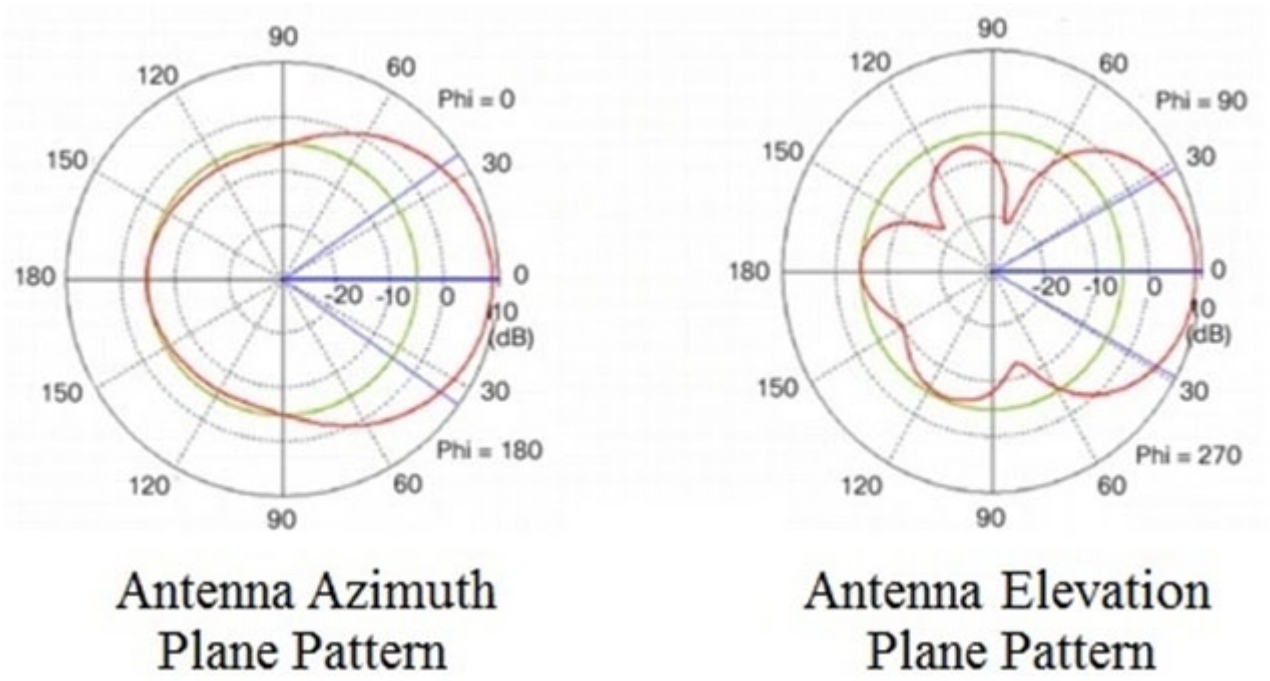
upvoted 6 times

AleGll 2 years, 11 months ago

A is the correct one. D is another right way to configure BGP peers (using loopback addresses), but it's not the requested mode.

upvoted 1 times

Refer to the exhibit.



Which type of antenna do the radiation patterns present?

A. Yagi

B. patch

C. omnidirectional

D. dipole

Correct Answer: *B*

Reference:

https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html

TimHon Highly Voted 2 years, 7 months ago

Patch Antenna, the same diagram from Cisco Whitepaper. (Figure 7. Single Patch Antenna with 3D Radiation Pattern, Azimuth Plane Pattern and Elevation Plane Pattern)
https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html

upvoted 9 times

danman32 4 months, 4 weeks ago

Link doesn't seem to be helpful anymore.

upvoted 1 times

TheNetworkStudent Most Recent 3 years, 2 months ago

According to the whitepaper in the reference, B is correct.

Fun fact is that according to the official exam guide it should be a Yagi, but apparantly they mixed up the pictures in the guide which makes it confusing.

upvoted 4 times

MerlinTheWizard 10 months ago

Nothing seems to be mixed up in my encor book.. Page 535 mentions Figure 18-23 which is on page 536. You can compare it to the patch antenna patterns from Figure 18-20 (535)

upvoted 2 times

danman32 4 months, 4 weeks ago

Book shows nearly same pattern style in azimuth and elevation for patch and yagi, with patch being more oval with minimal tail.
In this test question, they seem to be mixing pattern style. Yagi also seemed plausible
Then again, Yagi pattern seems more narrow focused.

upvoted 1 times

danny_f 1 year, 7 months ago

Classic Cisco...the "offical" study books are trash.

upvoted 3 times

Question #130 *Topic 1*

Which reason could cause an OSPF neighborship to be in the EXSTART/EXCHANGE state?

A. mismatched OSPF link costs

B. mismatched OSPF network type

C. mismatched areas

D. mismatched MTU size

Correct Answer: *D*
Reference:
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13684-12.html#neighbors

LM77 Highly Voted 1 year, 10 months ago
Answer D

"Neighbors Stuck in Exstart/Exchange State
The problem occurs most frequently when attempting to run OSPF between a Cisco router and another vendor's router. The problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces don't match. If the router with the higher MTU sends a packet larger that the MTU set on the neighboring router, the neighboring router ignores the packet."

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13684-12.html
upvoted 6 times

nushadu Most Recent 11 months, 2 weeks ago
use ISIS instead))
D. is right anyway ...
upvoted 2 times

XalaGyan 1 year, 12 months ago
In this example, there is a mismatch in MTU values between two OSPF neighbors. This router has MTU 1600:

OSPF: Rcv DBD from 10.100.1.2 on GigabitEthernet0/1 seq 0x2124 opt 0x52 flag 0x2
len 1452 mtu 2000 state EXSTART
OSPF: Nbr 10.100.1.2 has larger interface MTU
The other OSPF router has interface MTU 2000:

OSPF: Rcv DBD from 10.100.100.1 on GigabitEthernet0/1 seq 0x89E opt 0x52 flag 0x7
len 32 mtu 1600 state EXCHANGE
OSPF: Nbr 10.100.100.1 has smaller interface MTU

MTU mismatch causes that exact state
upvoted 3 times

examShark 2 years, 6 months ago
The given answer is correct
upvoted 3 times

Question #131 *Topic 1*

When configuring WPA2 Enterprise on a WLAN, which additional security component configuration is required?

A. PKI server

B. NTP server

C. RADIUS server

D. TACACS server

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/100708-wpa-uwn-config.html#conf

Community vote distribution

C (100%)

edg Highly Voted 3 years, 3 months ago

Reference:
https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified/#:~:text=the%20authentication%20process.-,WPA2%2DEnterprise,several%20different%20systems%20labelled%20EAP.

WPA2-Enterprise
Deploying WPA2-Enterprise requires a RADIUS server, which handles the task of authenticating network users access. The actual authentication process is based on the 802.1x policy and comes in several different systems labelled EAP.

upvoted 13 times

Vale86 Most Recent 5 months, 2 weeks ago

why only Radius and not Tacacs ? You can do it with both, no?

upvoted 1 times

ihateciscoreally 3 months, 2 weeks ago

RADIUS supports EAP which is obligatory when running Enterprise mode (802.1X). TACACS doesnt support EAP, so you cant use this for Enterprise mode.

upvoted 1 times

dudalykai 3 months, 4 weeks ago

true, tacacs is the same as radius but with more flexibility

upvoted 1 times

bora4motion 1 year ago

Selected Answer: C

Radius is correct - C

upvoted 1 times

Dataset 1 year, 3 months ago

RADIUS is ok

upvoted 1 times

hku68 2 years, 10 months ago

Radius !!!!

upvoted 4 times

Question #132 *Topic 1*

A customer has several small branches and wants to deploy a Wi-Fi solution with local management using CAPWAP.
Which deployment model meets this requirement?

A. local mode

B. autonomous

C. SD-Access wireless

D. Mobility Express

Correct Answer: *D*

Community vote distribution

D (100%)

Saqib79 Highly Voted 3 years, 6 months ago

Correct Option is D.

upvoted 31 times

StasStryukov Highly Voted 3 years, 2 months ago

Correct answer is Mobility Express. From Encor Cert guide: "As you might have guessed, it is also possible to move the WLC even below the access layer and into an AP. Figure 18-7 illustrates the Mobility Express topology, where a fully functional Cisco AP also runs software that acts as a WLC. This can be useful in small scale environments,such as small, midsize, or multi-site branch locations, where you might not want to invest in dedicated WLCs at all. The AP that hosts the WLC forms a CAPWAP tunnel with the WLC, as do any other APs at the same location. A Mobility Express WLC can support
up to 100 APs."

upvoted 19 times

danman32 Most Recent 4 months, 4 weeks ago

A does seem plausible, but requires an extra component: a dedicated WLC which would have to be at the branch office in order for the management to be local.
But we're dealing with small branch offices here, so we want lower cost.
With Mobility Express, the difference between CAPWAP image and ME image is whether the WLC function is included or not. For CAPWAP image, ME based WLC is not included so it can't act as a WLC. With ME image, it can act as a WLC.
But in an ME environment, the APs not operating as the WLC still communicate to the designated/elected WLC by CAPWAP.

upvoted 1 times

techriese 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

bora4motion 1 year ago

D - Mobility Express - available on many WAPs such as 3802s etc.

upvoted 2 times

Pudu_vlad 1 year, 2 months ago

Option D is correct

upvoted 1 times

Rockford 2 years, 6 months ago

Correct answer; Local Management and yes ME does use CAPWAP.

upvoted 2 times

numan_ahmed 2 years, 10 months ago

D is the correct one

upvoted 1 times

Sajj_gabi 2 years, 10 months ago

I believe is D as well as the book does say if the AP is acting as a WLC it forms a capwap tunnel at the same location

upvoted 2 times

[Removed] 2 years, 10 months ago

As far as i can tell Mobility Express does not use CapWap. the question saying "local management" is confusing.

upvoted 2 times

HK010 2 years, 4 months ago

it actually uses CAPWAP, CertGuide p,520

upvoted 1 times

CiscoSystems 2 years, 11 months ago

Correct answer is in fact A. Mobility express is controller-less thus does not create a CAPWAP tunnel.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-2/b_Mobility_Express_Deployment_guide/b_Mobility_Express_Deployment_guide_chapter_01100.html
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/mobility-express/solution-overview-c22-741355.pdf

upvoted 1 times

danman32 4 months, 4 weeks ago

The links you provided do not say that CAPWAP isn't used if you are using an ME image.
In fact, point 2b in the URL effectively says you'd use the CAPWAP image if you don't want the 1800 series AP to be able to be a WLC in an ME environment.
CAPWAP is still used between the ME AP elected to be the WLC and all other APs, whether non-elected APs have ME or CAPWAP image.

Local mode is plausible, but would require the extra cost and configuration of an actual WLC, but D is best answer for a branch office that wants local configuration. For a small branch office, you'd want lowest cost.

upvoted 1 times

cruzarcos 2 years, 10 months ago

According to: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide - Page 520, the AP does create a CAPWAP tunnel:

"Figure 18-7 illustrates the Mobility Express topology, where a fully functional
Cisco AP also runs software that acts as a WLC. This can be useful in small scale environments,
such as small, midsize, or multi-site branch locations, where you might not want to
invest in dedicated WLCs at all. The AP that hosts the WLC forms a CAPWAP tunnel with
the WLC, as do any other APs at the same location."

So D would be correct

upvoted 5 times

Helloory 3 years ago

Correct answer is D

upvoted 1 times

skh 3 years ago

I think D is the correct
Study Guide book
Figure 18-7 WLC Location in a Mobility Express Wireless Network
Topology see in Mobility Express use management CAPWAP
The AP that hosts the WLC forms a CAPWAP tunnel with the WLC, as do any other APs at the same location. A Mobility Express WLC

Cisco AP Modes Local mode: The default lightweight mode that offers one or more
functioning BSSs on a specific channel. During times when it is not
transmitting, the AP scans the other channels to measure the level of
noise, measure interference, discover rogue devices, and match against
intrusion detection system (IDS) events.

upvoted 2 times

Happiman 3 years, 1 month ago

Answer is A: ME and CAPWAP are two different modes.

upvoted 1 times

lexlexlex 3 years, 2 months ago

A.

Determining the image on the Access Point
The Cisco 1830, 1850, 2800 and 3800 series access points can either have CAPWAP image or the Cisco Mobility Express image which is capable of running the virtual Wireless LAN controller function on the Access Point.

It is either or situation

upvoted 1 times

james4231 3 years, 2 months ago

should be A

upvoted 1 times

akbntc 3 years, 3 months ago

Option D: Mobility Express.

upvoted 1 times

Refer to the exhibit.

Clients > Detail

< Back | Apply | Link Test | Remove

Client Properties

MAC Address	00:09:ef:0G:07:bd
IP Address	192.100.101.100
Client Type	Regular
User Name	
Port Number	29
Interface	Staff
VLAN ID	3602
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Anchor
Mobility Peer IP Address	172.22.253.20.
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	3710
Power Save Mode	OFF
Current TxRateSet	
Data RateSet	5.5,11.0,6.0,9.0,12.0,19.0,24.0,36.0,40.0,54.0

AP Properties

AP Address	3c:ce:73:1b:33:39
AP Name	172.22.253.20
AP Type	Mobile
WLAN Profile	Staff
Status	Associated
Association ID	0
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Enable

The WLC administrator sees that the controller to which a roaming client associates has Mobility Role Anchor configured under Clients > Detail.

Which type of roaming is supported?

A. indirect

B. Layer 3 intercontroller

C. intracontroller

D. Layer 2 intercontroller

Correct Answer: *B*

Community vote distribution

B (100%)

Saqib79 Highly Voted 3 years, 6 months ago

Correct Option is B.

upvoted 40 times

Sparks026 Highly Voted 3 years, 6 months ago

Layer 3 intercontroller is correct because the mobility peer IP address is in different subnet from the client IP address

upvoted 29 times

Eddgar0 Most Recent 1 year, 7 months ago

Selected Answer: B

I Think B is correct because only on l3 roaming is the achoring feature used, and also seen the mobility ip address is different than local address

upvoted 5 times

PixelRunner 1 year, 7 months ago

Selected Answer: B

B: Layer 3 is correct

upvoted 2 times

diegodavid82 1 year, 9 months ago

Selected Answer: B

100% L3 Inter controller. You can review this post:
https://mrncciew.com/2013/03/17/l3-inter-controller-roaming/

The client in Anchor WLC is seen with "mobility role" = Anchor and "AP type" Mobile

upvoted 2 times

ArchBishop 1 year, 10 months ago

Many people are saying L3 Roaming capable, which I agree... but they are saying it because the Mobility Role is set to Anchor....
If it was L2 capable or not capable at all, what would the other entries look like? I cannot seem to find much documentation about the mobility roles.

Also, "because the mobility peer IP is in a different subnet from the client IP."
What does this mean? Why would the mobility peer ip have anything to do with the client IP.
I'll keep reading until I find an answer, but I have not found anything yet.
Comments appreciated until then.

upvoted 3 times

danny_f 1 year, 7 months ago

THe primary WLC and anchor WLC have different addresses so L3 comes into place. This is a good read.
https://www.lookingpoint.com/blog/wireless-mobility-anchoring#:~:text=Cisco%20defines%20mobility%20anchoring%20as,Anchor%20for%20that%20specific%20WLAN.

upvoted 2 times

diegodavid82 1 year, 9 months ago

I found the reason why B is the correct answer, you can review this post:
https://mrncciew.com/2013/03/17/l3-inter-controller-roaming/
:)

upvoted 2 times

Nhan 2 years, 1 month ago

B is correct answer, tin this case client roaming to a different eco on a different subnet, the new capwap tunnel will be built between the eco and the client, the client up address won't change, and the original wcl
is the anchor wcl

upvoted 2 times

xziomal9 2 years, 2 months ago

The correct answer is:
B. Layer 3 intercontroller

upvoted 3 times

wts 2 years, 3 months ago

The client cannot have an anchor role. Perhaps this is the role of this controller from the point of view of the client, which means that he has not moved anywhere.
The client's settings are shown. How can you figure out which roaming the controller supports?
For this you do not need topology and configuration of controller interfaces?

upvoted 2 times

HK010 2 years, 4 months ago

D for sure, Guys! The client still connect to the Anchor, it doesn't roam to the foreign, so no roaming happens here. It's just a tricky question. They just throw the word Anchor to make you think about L3.

upvoted 2 times

HK010 2 years, 4 months ago

So the client basically roamed from A x-wlc to a WLC that has the role Anchor which you can assign it to the WLC you want.

upvoted 1 times

tonyx182 2 years, 5 months ago

B is the correct answer

upvoted 1 times

kthekillerc 2 years, 5 months ago

correct Option is D intercontroller layer 2

upvoted 1 times

LeGrosMatou 2 years, 6 months ago

If the clients roam between APs registered to different controllers and the client WLAN on the two controllers is on different subnet, then it is called inter-controller L3 roam.
In this situation as well controllers exchange mobility messages. Client database entry change is completely different that to L2 roam(instead of move, it will copy). In this situation the original controller marks the client entry as "Anchor" where as new controller marks the client entry as "Foreign".The two controllers now referred to as "Anchor controller" & "Foreign Controller" respectively. Client will keep the original IP address & that is the real advantage.
Note: Inter-Controller (normally layer 2) roaming occurs when a client roam between two APs registered to two different controllers, where each controller has an interface in the client subnet.

upvoted 3 times

davdtech 2 years, 8 months ago

If its marked as an Anchor the other will be marked as Foreign. This is only used when you have 2 WLCs in different vlans so its L3 intra roaming

upvoted 4 times

Wesgo 2 years, 9 months ago

B, it is so clear... "Layer 3 roaming is similar to Layer 2 roaming in that the controllers exchange mobility messages on the client roam. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains transparent to the wireless client, and the client maintains its original IP address. "
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/overview.html

upvoted 6 times

Summa 2 years, 10 months ago

Answer should be B
https://www.youtube.com/watch?v=N5jAStIozQw

upvoted 4 times

[Removed] 2 years, 10 months ago

It has to be B, right?
Layer 3 roaming is similar to Layer 2 roaming in that the controllers exchange mobility messages on the client roam. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains transparent to the wireless client, and the client maintains its original IP address.

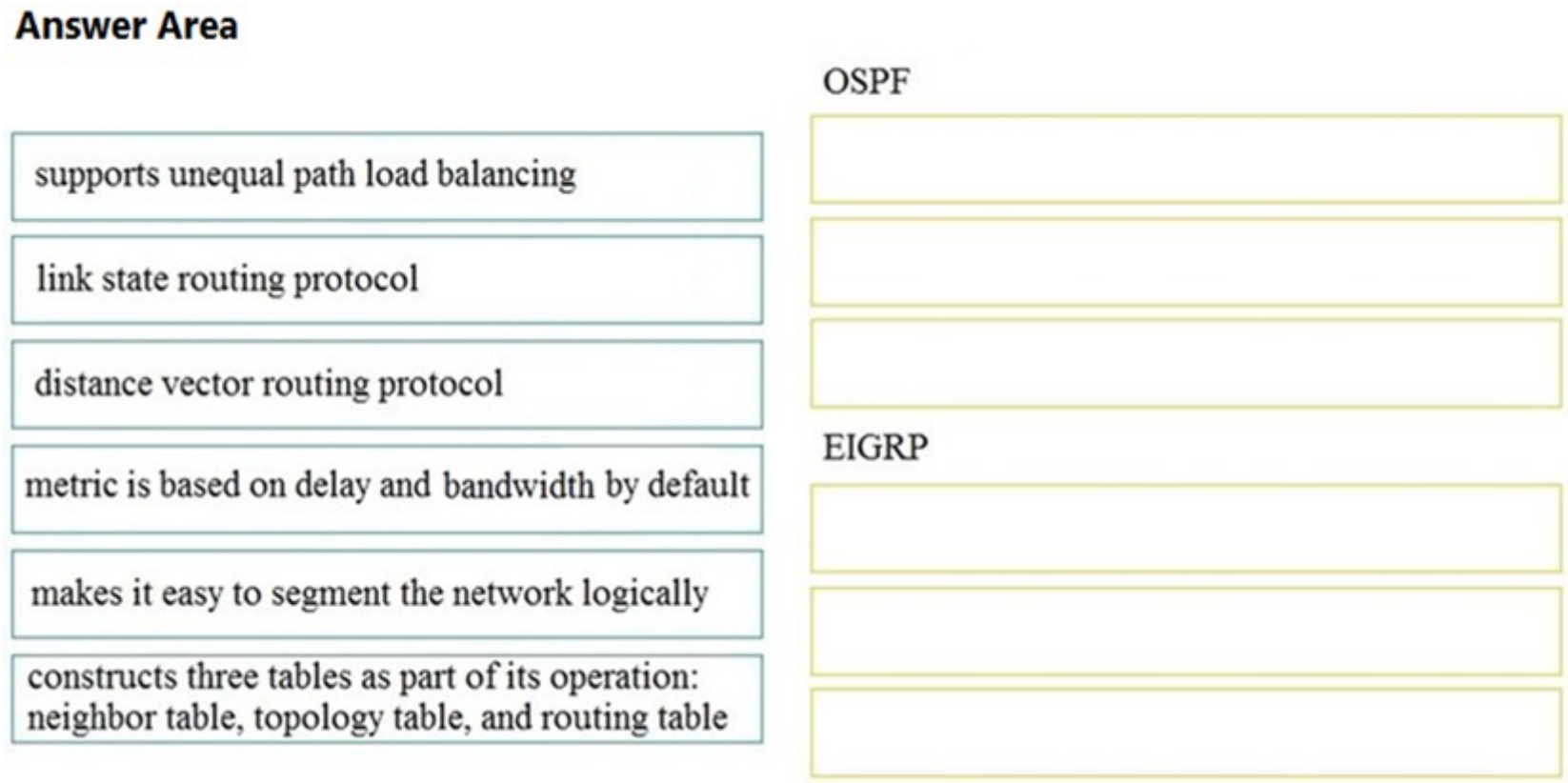
upvoted 1 times

Question #134 *Topic 1*

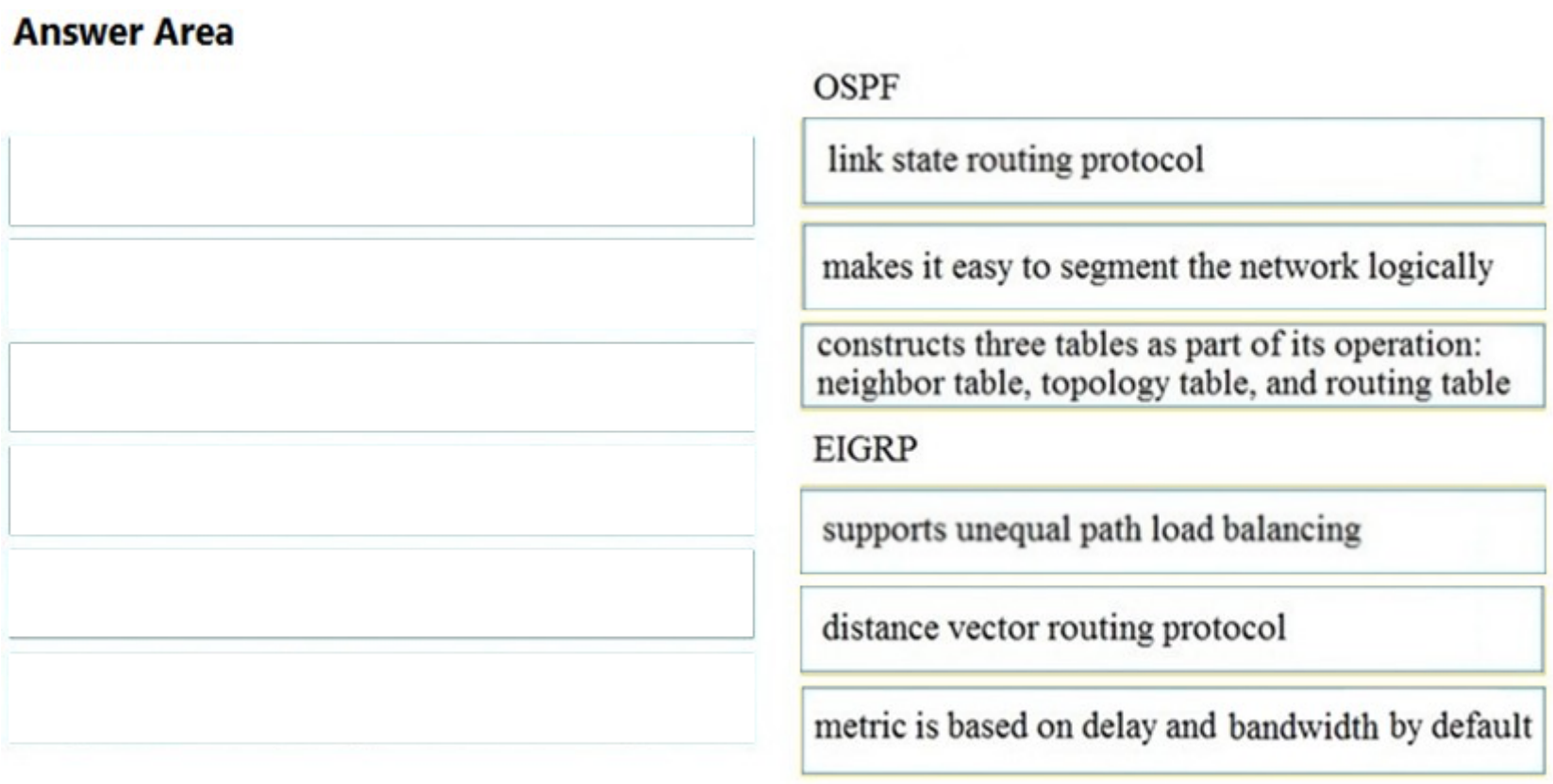
DRAG DROP -

Drag and drop the characteristics from the left onto the correct routing protocol types on the right.

Select and Place:



Correct Answer:



carlovalle 1 year, 2 months ago

EIGRP build 3 types of tables
https://www.networkurge.com/2020/07/eigrp-tables.html

upvoted 1 times

danman32 4 months, 4 weeks ago

The three table types do exist for both EIGRP and OSPF, and initially I had put the 3 tables under EIGRP.
However you only have 3 slots under EIGRP, and there's already 3 items that can ONLY be EIGRP: unequal path LB, Distance Vector (OSPF is link-state), and metric based on BW and Delay (OSPF is only cost based on BW)

upvoted 2 times

HungarianDish 10 months ago

It is true, however, ospf also builds these three tables: neighbor, topology, routing.
https://study-ccna.com/ospf-overview/

upvoted 2 times

MerlinTheWizard 10 months ago

not exactly q clear question, but after considering the other options, this can belong to ospf only.. But yeah, the term topology is bit confusing since you're building OSPF database, unlike EIGRP topology table

upvoted 1 times

bendarkel 1 year, 3 months ago

OSPF

Link state routing protocol.
Makes it easy to segment the network logically.
Constructs three tables as part of its operation: Neighbor, Topology, and routing.

EIGRP

Supports unequal path load balancing.
Distance vector routing protocol.
Metric is based on delay and bandwidth by default.
upvoted 3 times

Question #135 *Topic 1*

Which feature is supported by EIGRP but is not supported by OSPF?

A. route filtering

B. unequal-cost load balancing

C. route summarization

D. equal-cost load balancing

Correct Answer: *B*

hku68 Highly Voted 2 years, 10 months ago
%100 B
upvoted 6 times

wabenzy Most Recent 5 months ago
B is absolutely the correct answer
upvoted 1 times

kthekillerc 2 years, 5 months ago
B is the correct answer
upvoted 2 times

Question #136 *Topic 1*

What is the correct EBGP path attribute list, ordered from most preferred to least preferred, that the BGP best-path algorithm uses?

A. local preference, weight, AS path, MED

B. weight, local preference, AS path, MED

C. weight, AS path, local preference, MED

D. local preference, weight, MED, AS path

Correct Answer: *B*

Community vote distribution

B (100%)

youtri Highly Voted 1 year, 12 months ago

remember WLAM

upvoted 24 times

ermanzan 5 months, 2 weeks ago

Very good trick to remember it!!! Thanks mate.

upvoted 1 times

GeorgeFortiGate 1 year ago

Nice way to remember ;)

upvoted 3 times

skh Highly Voted 3 years ago

Path Selection Attributes: Weight > Local Preference > Originate > AS Path > Origin > MED > External > IGP Cost > eBGP Peering > Router ID

upvoted 12 times

wabenzy Most Recent 5 months ago

This pneumonic will help you memorize how BGP selects best route.
"We Love Oranges AS Oranges Mean Pure Refreshment!"
We === Weight (Highest)
Love === LOCAL_PREF (Highest)
Oranges === Originate (local)
AS === AS_PATH (shortest)
Oranges === ORIGIN Code (IGP > EGP > Incomplete)
Mean === MED (lowest)
Pure === Paths (External > Internal)
Refreshments === RID (lowest)

upvoted 5 times

[Removed] 5 months ago

Selected Answer: B

We Love Oranges As Oranges Mean Pure Refreshment

upvoted 3 times

Vlad_Is_Love_ua 8 months, 4 weeks ago

Selected Answer: B

Routing policy is based on the following attributes:
Prefer the highest weight attribute (local to router)
Prefer the highest local preference attribute (global with AS)
Prefer route originated by the local router (next hop = 0.0.0.0)
Prefer the shortest AS path (least number of autonomous systems in AS-path attribute)
Prefer the lowest origin attribute (IGP < EGP < incomplete)
Prefer the lowest MED attribute (exchanged between autonomous systems)

upvoted 1 times

packetsniffer007 1 year, 2 months ago

Selected Answer: B

We Love Oranges As Oranges Mean Pure Refreshment
Easy acronym to remember order

upvoted 4 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 2 times

woody_ 3 years, 2 months ago

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html#anc2

upvoted 1 times

Question #137 *Topic 1*

A local router shows an EBGP neighbor in the Active state.

Which statement is true about the local router?

A. The local router is attempting to open a TCP session with the neighboring router.

B. The local router is receiving prefixes from the neighboring router and adding them in RIB-IN.

C. The local router has active prefixes in the forwarding table from the neighboring router.

D. The local router has BGP passive mode configured for the neighboring router.

Correct Answer: *A*

Community vote distribution

A (100%)

hku68 Highly Voted 2 years, 10 months ago

A is correct

https://community.cisco.com/t5/routing/confirm-quot-active-quot-meaning-in-bgp/td-p/1391629

upvoted 10 times

kebkim Highly Voted 1 year, 2 months ago

BGP CONNECT session : BGP waits for a TCP connection with the remote peer. If successful, an OPEN message is sent. If unsuccessful, the session is placed in an Active state.

upvoted 5 times

jackr76 5 months, 4 weeks ago

IF SUCCESFUL, thus not yet. How come already active?

upvoted 1 times

CCNPWILL 1 month, 1 week ago

That is the name of the state that it is in. As in, actively trying to attempt to establish connection.

upvoted 1 times

[Removed] Most Recent 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

Refer to the exhibit.

```
SwitchC#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally       : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Transparent
VTP Domain Name                 : cisco.com
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MDS digest                      : 0xE5 0x28 0x5D 0x3E 0x2F 0xE5 0xAD 0x2B
Configuration last modified by 0.0.0.0 at 1-10-19 09:01:38

SwitchC#show vlan brief

VLAN  Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1     default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6,
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10,
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14,
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18,
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22,
                                                 Fa0/23, Fa0/24, Po1
110 Finance                          active
210 HR                               active    Fa0/1
310 Sales                            active    Fa0/2
[...output omitted...]

SwitchC#show int trunk
Port        Mode         Encapsulation      Status        Native vlan
Gig1/1      on           802.1q             trunking      1
Gig1/2      on           802.1q             trunking      1

Port        Vlans allowed on trunk
Gig1/1      1-1005
Gig1/2      1-1005

Port        Vlans allowed and active in management domain
Gig1/1      1, 110, 210, 310
Gig1/2      1, 110, 210, 310

Port        Vlans in spanning tree forwarding state and not pruned
Gig1/1      1, 110, 210, 310
Gig1/2      1, 110, 210, 310

SwitchC#show run interface port-channel 1
interface Port-channel 1
 description Uplink_to_Core
 switchport mode trunk
```

SwitchC connects HR and Sales to the Core switch. However, business needs require that no traffic from the Finance VLAN traverse this switch.

Which command meets this requirement?

A. SwitchC(config)#vtp pruning vlan 110

B. SwitchC(config)#vtp pruning

C. SwitchC(config)#interface port-channel 1 SwitchC(config-if)#switchport trunk allowed vlan add 210,310

D. SwitchC(config)#interface port-channel 1 SwitchC(config-if)#switchport trunk allowed vlan remove 110

Correct Answer: *D*

Community vote distribution

D (91%) 9%

last7 Highly Voted 3 years, 1 month ago

Answer is D. B would prune vlan 110 because there are no ports in that vlan, except that vtp mode is transparent, so pruning mode is Disabled.

upvoted 15 times

OhBee 1 year, 10 months ago

Also, B is not correct since this switch is not even participating in the VTP domain :)

upvoted 2 times

ABC123 Highly Voted 2 years, 5 months ago

Option C would be correct also if the keyword "add" was not there

upvoted 9 times

[Removed] 5 months, 2 weeks ago

so... its wrong then

upvoted 3 times

danman32 4 months, 4 weeks ago

Actually no, because then you'd be eliminating default VLAN 1, which is not what the question wants.

upvoted 1 times

djedeen Most Recent 3 months, 1 week ago

Selected Answer: D

Trunk already allows all VLANs, hence adding 2 VLANs changes nothing (e.g. option C).

upvoted 1 times

PureInertiaCopy 3 months, 2 weeks ago

But.... Po1 is in VLAN 1...It's not even a trunk...

upvoted 1 times

FD_M 3 months, 2 weeks ago

Selected Answer: D

we cannot enable vtp pruning on this switch b/c this switch is in transparent mode

upvoted 1 times

khaganiabbasov 3 months, 3 weeks ago

D is correct

You can use vtp pruning command in server mode - switch in transparent mode.

upvoted 1 times

LanreDipeolu 3 months, 3 weeks ago

Selected Answer: D

pruning statement can only come from server domain, so the only option is to remove the unwanted vlan with switchport trunk allowed vlan remove 110 statement. "D" is correct

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: D

before removing vlan10:
sw1#show int tru

Port Mode Encapsulation Status Native vlan
Et0/0 on 802.1q trunking 1
Et0/3 desirable n-isl trunking 1
Po2 on 802.1q trunking 1

Port Vlans allowed on trunk
Et0/0 1-4094
Et0/3 1-4094
Po2 1-4094 <<<<<<<<<<<<<<<<<<<<

Port Vlans allowed and active in management domain
Et0/0 1,10,30,40,50,110
Et0/3 1,10,30,40,50,110
Po2 1,10,30,40,50,110 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Port Vlans in spanning tree forwarding state and not pruned
Et0/0 1,10,30,40,50,110
Et0/3 1
Po2 1,30,50
sw1#

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw1(config-if)#switchport trunk allowed vlan remove 110
sw1(config-if)#
sw1(config-if)#do s runn int po2
Building configuration...

Current configuration : 182 bytes
!
interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1-109,111-4094
switchport mode trunk
spanning-tree port-priority 64
end

sw1(config-if)#
upvoted 2 times

nushadu 11 months, 2 weeks ago

sw1(config-if)#do s int tr

Port Mode Encapsulation Status Native vlan
Et0/0 on 802.1q trunking 1
Et0/3 desirable n-isl trunking 1
Po2 on 802.1q trunking 1

Port Vlans allowed on trunk
Et0/0 1-4094
Et0/3 1-4094
Po2 1-109,111-4094 <<<<<<<<<<<<<<<<<<

Port Vlans allowed and active in management domain
Et0/0 1,10,30,40,50,110
Et0/3 1,10,30,40,50,110
Po2 1,10,30,40,50 <<<<<<<<<<<<<<<<<<<<<<<<

Port Vlans in spanning tree forwarding state and not pruned
Et0/0 1,10,30,40,50,110
Et0/3 1
Po2 1,30,50
sw1(config-if)#
upvoted 1 times

forccnp 11 months, 3 weeks ago

Selected Answer: D

D is correct answer 100%
upvoted 1 times

bora4motion 1 year ago

Selected Answer: D

going with D
upvoted 1 times

forccnp 1 year ago

Selected Answer: D

D) is correct answer
upvoted 1 times

prietito 1 year, 6 months ago

Selected Answer: C

ABC123 is correct. By omitting finance vlan allow to trunk. This traffic will not traverse the switch
upvoted 1 times

redgi0 1 year, 4 months ago

Incorrect.
You have a trunk allowing ALL VLAN.
if you ADD 2 VLANs, you will still have a trunk allowing ALL VLAN

D is correct answer
upvoted 6 times

danman32 4 months, 4 weeks ago

And if there wasn't an ADD clause, you'd then be blocking VLAN 1 which is clearly not desired.
upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: D

D is correct, as switch is transparent mode that means vtp prunning can not be enable also not participating on the VTP. the option C is adding vlan but in the image all vlans are already allowed in the trunk, The only option is D as is blocking the undesired vlan from the trunk.
upvoted 3 times

Nhan 2 years, 2 months ago

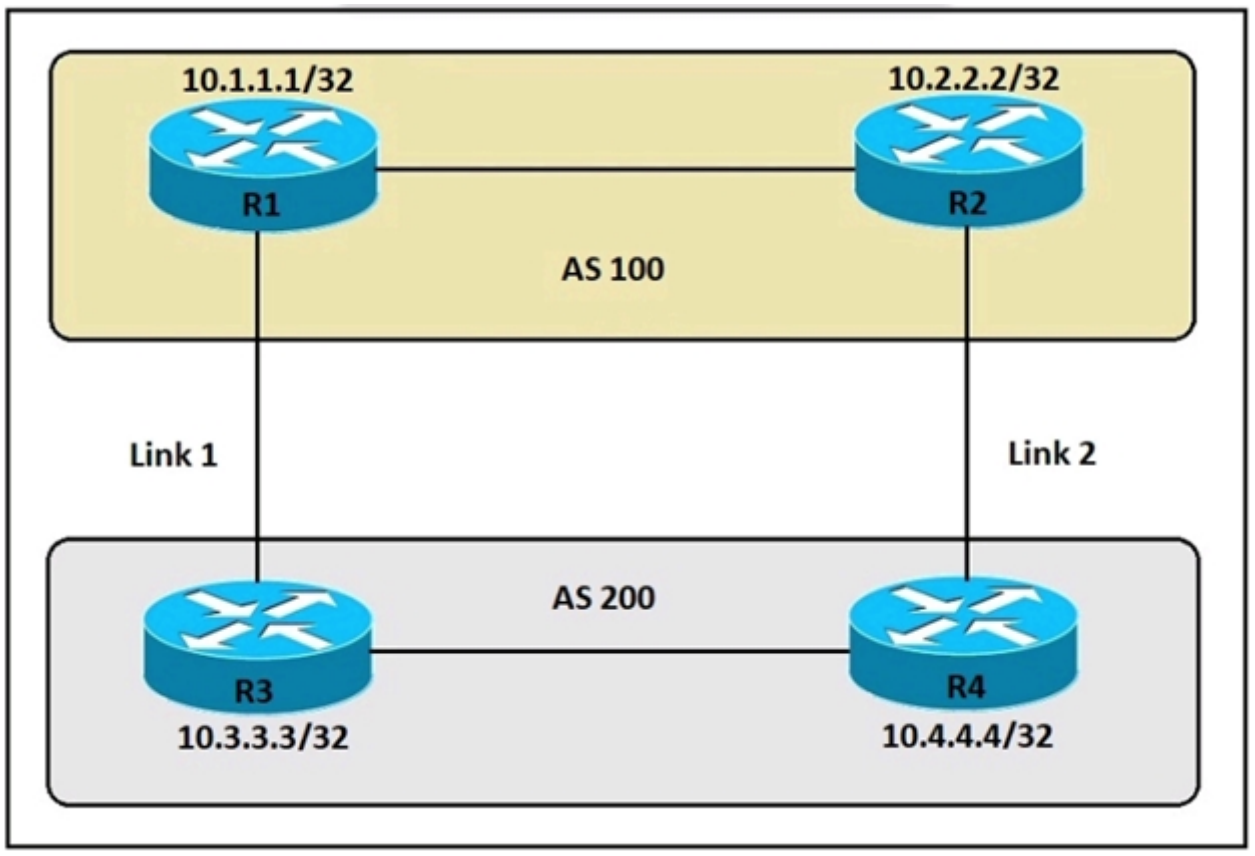
Basically the vlan 110 need to be block from the trunk port which is po1 in this case
upvoted 3 times

AliMo123 2 years, 7 months ago

Also, prune mode is configured only on VTP server mode , so option D is 100% correct
upvoted 3 times

Question #139 *Topic 1*

Refer to the exhibit.



An engineer must ensure that all traffic leaving AS 200 will choose Link 2 as the exit point.
Assuming that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers, which configuration accomplishes this task?

A. R4(config-router)bgp default local-preference 200

B. R3(config-router)bgp default local-preference 200

C. R4(config-router)neighbor 10.2.2.2 weight 200

D. R3(config-router)neighbor 10.1.1.1 weight 200

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html#:~:text=Border%20Gateway%20Protocol%20(BGP)%20routers,to%20use%20for%20traffic%20forwarding.

Community vote distribution

A (100%)

Commando1664 Highly Voted 2 years, 6 months ago
Weight only applies to the Router it is applied to, Local preference will apply to the whole AS group.
upvoted 36 times

bendarkel 1 year, 3 months ago
In this case, yes. Weight only applies to the router where it's configured, but not in all cases. In the cases where route reflectors are involved, weight can impact all routers in an AS if the weighted route/path is being advertised to the route reflector.
upvoted 5 times

ihateciscoreally 3 months, 1 week ago
Reflectors are beyond scope of ENCOR.
upvoted 3 times

examShark Highly Voted 2 years, 6 months ago
The given answer is correct
upvoted 9 times

Ahmad98ali Most Recent 3 months ago
Selected Answer: A
The given answer is correct
upvoted 1 times

djedeen 3 months, 1 week ago

Selected Answer: A

Local preference defaults to 100, and highest value wins so setting to 200 is the solution.

upvoted 2 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

generally speaking it is EXIT point FROM AS:
cisco(config-router)#bgp default ?
inter-as-hybrid Configure Inter-AS Hybrid peer defaults
ipv4-unicast Activate ipv4-unicast for a peer by default
ipv6-nexthop Default IPv6 nexthop format
local-preference local preference (higher=more preferred)
route-target Control behavior based on Route-Target attributes

cisco(config-router)#bgp default lo
cisco(config-router)#bgp default local-preference ?
<0-4294967295> Configure default local preference value

cisco(config-router)#bgp default local-preference 200
cisco(config-router)#

upvoted 3 times

bora4motion 1 year ago

Selected Answer: A

Weight is Cisco proprietary and it is locally significant to the router and does not apply to the entire AS. Use Local Pref insteadl - A

upvoted 4 times

bendarkel 1 year, 3 months ago

This appears to be a tricky one. Both R3 and R4 have their local preference values defaulted to 200. They're both weighing their external neighbors at 200. That means this comes down to which AS 200 edge router BGP external peering and configs are applied first to determine through which edge router AS 200 egress to AS 100.

upvoted 2 times

youtri 1 year, 12 months ago

A correct
weight i think when you have a edge router bgp with 2 link toward a diferent ISP router edge
lpease someonde confirm me if it correct

upvoted 1 times

Eddgar0 1 year, 7 months ago

Is correct that you say, local preference only is significant locally on the router to preferer an exit point.

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

cracanici 2 years, 3 months ago

A
https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html

upvoted 2 times

Broekie 2 years, 6 months ago

I go for answer C
BGP assigns the first valid path as the current best path. BGP then compares the best path with the next path in the list, until BGP reaches the end of the list of valid paths. This list provides the rules that are used to determine the best path:
1. Prefer the path with the highest WEIGHT.
Note: WEIGHT is a Cisco-specific parameter. It is local to the router on which it is configured.
2. Prefer the path with the highest LOCAL_PREF.
Note: A path without LOCAL_PREF is considered to have had the value set with the bgp default local-preferencecommand, or to have a value of 100 by default.

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html

upvoted 3 times

ABC123 2 years, 8 months ago

It seems Weight option (C) would be applicable if both exit peering links were on the same router, because Weight has local significance, also it requires peering routers to be Cisco, though weight attribute is supported in some other BGP implementation like VMware NSX-V.

upvoted 3 times

Question #140 *Topic 1*

Which feature of EIGRP is not supported in OSPF?

A. load balancing of unequal-cost paths

B. load balance over four equal-cost paths

C. uses interface bandwidth to determine best path

D. per-packet load balancing over multiple paths

Correct Answer: *A*

Community vote distribution

A (100%)

bora4motion 1 year ago

Selected Answer: A

A is correct

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 3 times

hku68 2 years, 10 months ago

A is correct

upvoted 3 times

Question #141 *Topic 1*

Which NTP Stratum level is a server that is connected directly to an authoritative time source?

A. Stratum 0

B. Stratum 1

C. Stratum 14

D. Stratum 15

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/bsm/16-6-1/b-bsm-xe-16-6-1-asr920/bsm-time-calendar-set.html

Community vote distribution

B (86%) 14%

DUGGIEFRESH Highly Voted 1 year, 6 months ago

ENCORE 350-401, Chapter 15, Pg 396, section "Network Time Protocol", paragraph 2:
"NTP servers that are directly attached to an authoritative time source are stratum 1 servers"
Answer is B, quote taken directly from the book

upvoted 12 times

danman32 Most Recent 4 months, 4 weeks ago

Although in real-world you wouldn't find a stratum 0 NTP server you could connect to, you could specify any server as stratum 0 which would make it authoritative (no server better than me).
Question though asks what the stratum would be for a server CONNECTED to an Authoritative server, where we can assume the authoritative server was configured as stratum 0, whether that's realistic or not.

upvoted 3 times

Nickplayany 8 months, 3 weeks ago

Selected Answer: B

It is B guys...

upvoted 1 times

Wooker 1 year, 2 months ago

Selected Answer: B

Answer is B

upvoted 1 times

Dataset 1 year, 3 months ago

Stratum 0 is an atomic clock, cannot be a time server.
B is correct

upvoted 1 times

prietito 1 year, 6 months ago

Selected Answer: B

rlilewis is correct.
Stratum 0
A reference clock source that relays Coordinated Universal Time (UTC) and has little or no delay is known as a Stratum 0 device. Stratum 0 servers cannot be used on the network. Instead, they are directly connected to computers that then operate as primary time servers.

upvoted 2 times

rlilewis 1 year, 6 months ago

Selected Answer: B

i think stratum 0 is an atomic clock.

It's B.

upvoted 2 times

pierresadou 1 year, 7 months ago

Selected Answer: A

Should be A

upvoted 1 times

danman32 4 months, 4 weeks ago

A would be correct if the server IS the authoritative server.
But here the question asks about the server that is CONNECTED to the authoritative server, so stratum can't be 0, has to be 1 or higher, higher if the authoritative server was set as a stratum level of 13 or 14.

upvoted 2 times

tempaccount00001 4 months, 4 weeks ago

stratum 0 is the clock, if you connect to it you are stratum 1, answer is B

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 3 times

mumenkm 2 years, 2 months ago

B is correct.
NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server typically has an authoritative time source (such as a radio or atomic clock, or a Global Positioning System (GPS) time source) directly attached, a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on.

upvoted 4 times

Summa 3 years ago

should be A: 0

The NTP Stratum Model
The NTP Stratum model is a representation of the hierarchy of time servers in an NTP network, where the Stratum level (0-15) indicates the device's distance to the reference clock.

Stratum 0 means a device is directly connected to e.g., a GPS antenna. Stratum 0 devices cannot distribute time over a network directly, though, hence they must be linked to a Stratum 1 time server that will distribute time to Stratum 2 servers or clients, and so on. The higher the Stratum number, the more the timing accuracy and stability degrades.

The NTP protocol does not allow clients to accept time from a Stratum 15 device, hence Stratum 15 is the lowest NTP Stratum.

http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/NTP_Stratums.htm#:~:text=The%20NTP%20Stratum%20model%20is,to%20e.g.%2C%20a%20GPS%20antenna.

upvoted 1 times

Dataset 1 year, 2 months ago

Hi ! stratum 0 is an atomic watch and connot be a time server
Regards

upvoted 1 times

Jem_1919193 3 years ago

NTP servers that are directly attached to an
authoritative time source are stratum 1 servers.-FROM OFFICIAL CERT GUIDE.FYI

upvoted 7 times

rezavage 3 years ago

stratum level 0 cannot be a time server so the answer is level 1 which is B

upvoted 6 times

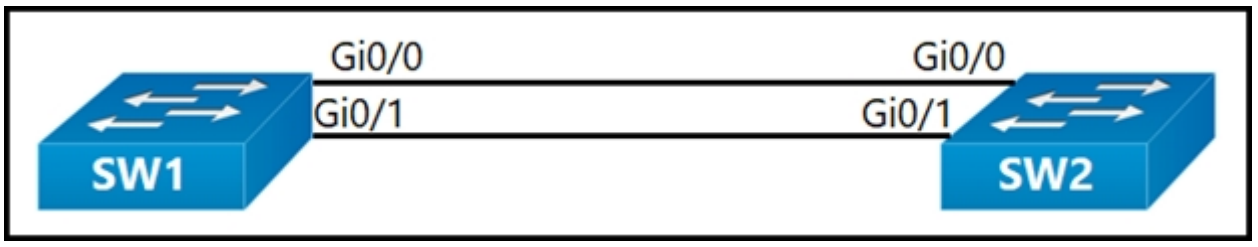
hku68 2 years, 10 months ago

B is correct.
https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/bsm/16-6-1/b-bsm-xe-16-6-1-asr920/bsm-time-calendar-set.html

upvoted 3 times

Question #142 *Topic 1*

Refer to the exhibit.



An engineer reconfigures the port-channel between SW1 and SW2 from an access port to a trunk and immediately notices this error in SW1's log:

*Mar 1 09:47:22.245: %PM-4-ERR_DISABLE: bpduguard error detected on Gi0/0, putting Gi0/0 in err-disable state

Which command set resolves this error?

A. SW1(config-if)#interface Gi0/0 SW1(config-if)#no spanning-tree bpdufilter SW1(config-if)#shut SW1(config-if)#no shut

B. SW1(config-if)#interface Gi0/0 SW1(config-if)#no spanning-tree bpduguard enable SW1(config-if)#shut SW1(config-if)#no shut

C. SW1(config-if)#interface Gi0/0 SW1(config-if)#spanning-tree bpduguard enable SW1(config-if)#shut SW1(config-if)#no shut

D. SW1(config-if)#interface Gi0/1 SW1(config-if)#spanning-tree bpduguard enable SW1(config-if)#shut SW1(config-if)#no shut

Correct Answer: *B*

Community vote distribution

B (100%)

xziomal9 Highly Voted 2 years, 2 months ago

A.
SW1(config-if)#interface Gi0/0
SW1(config-if)#no spanning-tree bpdufilter
SW1(config-if)#shut
SW1(config-if)#no shut
B.
SW1(config-if)#interface Gi0/0
SW1(config-if)#no spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
C.
SW1(config-if)#interface Gi0/0
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
D.
SW1(config-if)#interface Gi0/1
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut

The correct answer is:
B

upvoted 11 times

habibmangal Most Recent 7 months, 2 weeks ago

the port has been connected to an unauthorized device or misconfigured. To resolve the error, BPDU Guard needs to be disabled on the interface and the interface needs to be brought out of the err-disable state.

Option C is the correct set of commands to resolve this error as it enables BPDU Guard on the interface, which will prevent any unauthorized BPDU frames from being received on the interface, and then the interface is shut down and then brought back up.
Option B is not the correct set of commands to resolve the error. This is because the "no" keyword is used with the "spanning-tree bpduguard enable" command, which would disable BPDU Guard on the interface. Instead, the "spanning-tree bpduguard enable" command needs to be omitted, and the "spanning-tree portfast disable" command needs to be used to prevent BPDU Guard from being triggered again on this interface

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: B

tested:
sw2(config-if)#spanning-tree bpduguard enable
sw2(config-if)#
*Dec 17 17:23:04.850: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Et0/3 with BPDU Guard enabled. Disabling port.
sw2(config-if)#
*Dec 17 17:23:04.850: %PM-4-ERR_DISABLE: bpduguard error detected on Et0/3, putting Et0/3 in err-disable state

*Dec 17 17:23:05.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
sw2(config-if)#
*Dec 17 17:23:06.853: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to down
sw2(config-if)#

sw2#show interfaces status | i /3|Stat
Port Name Status Vlan Duplex Speed Type
Et0/3 err-disabled 1 auto auto unknown
sw2#

upvoted 2 times

nushadu 11 months, 2 weeks ago

sw2(config-if)#do s runn interface e0/3
Building configuration...

Current configuration : 74 bytes
!
interface Ethernet0/3
duplex auto
spanning-tree bpduguard enable
end

sw2(config-if)#no spanning-tree bpduguard enable
sw2(config-if)#shutdown
sw2(config-if)#no shutdown
*Dec 17 17:30:52.608: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to administratively down
sw2(config-if)#no shutdown
sw2(config-if)#
*Dec 17 17:30:55.776: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to up
*Dec 17 17:30:56.777: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to up
sw2(config-if)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw2#show interfaces status | i /3|Stat
Port Name Status Vlan Duplex Speed Type
Et0/3 connected trunk auto auto unknown
sw2#

upvoted 1 times

timtgh 1 year, 6 months ago

Answer is correct, but this is a bad switch config because that port has portfast enabled and it shouldn't.

upvoted 3 times

timtgh 1 year, 6 months ago

The real proper solution would be disable portfast from all of those trunk ports. But that's not an option, so B is the best choice.

upvoted 2 times

error_909 2 years, 2 months ago

Correct

upvoted 1 times

SandyIndia 2 years, 3 months ago

Warning: Spantree port fast start should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches, bridges, etc. to
a fast start port can cause temporary spanning tree loops.
(config-if)#spanning-tree portfast disable
https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html

upvoted 2 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 1 times

Question #143 *Topic 1*

When a wireless client roams between two different wireless controllers, a network connectivity outage is experienced for a period of time. Which configuration issue would cause this problem?

A. Not all of the controllers in the mobility group are using the same mobility group name.

B. Not all of the controllers within the mobility group are using the same virtual interface IP address.

C. All of the controllers within the mobility group are using the same virtual interface IP address.

D. All of the controllers in the mobility group are using the same mobility group name.

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107188-mobility-groups-faq.html

Community vote distribution

B (100%)

aki290 Highly Voted 3 years, 3 months ago

B is the correct answer.
If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time.

upvoted 37 times

BB234 2 years, 5 months ago

The correct answer is B.
If the mobility group name is different, then the controllers are in different mobility groups.

upvoted 8 times

akbntc Highly Voted 3 years, 3 months ago

"All controllers must be configured with the same mobility group name. All controllers must be configured with the same virtual interface IP address. If necessary, you can change the virtual interface IP address by editing the virtual interface name on the Controller > Interfaces page.

If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time."

upvoted 15 times

ihateciscoreally Most Recent 3 months, 1 week ago

answer A is also correct so why B?

upvoted 1 times

[Removed] 5 months ago

Selected Answer: B

The virtual interface IP address is a logical interface on the wireless controller that is used for mobility management, DHCP relay, and web authentication2. The virtual interface IP address must be configured on each controller in the network, and it must be the same on all controllers that are part of the same mobility group2.
When a wireless client roams between two different controllers, the client's IP address and subnet remain unchanged, and the client's data traffic is tunneled from the foreign controller (the controller to which the client roams) to the anchor controller (the controller from which the client roams) using the virtual interface IP address as the tunnel endpoint2.
If not all of the controllers within the mobility group are using the same virtual interface IP address, the mobility tunnel between them may not be established or maintained correctly, and the client may experience a network connectivity outage during roaming2.
To avoid this problem, we need to ensure that all of the controllers within the mobility group are using the same virtual interface IP address, and that this IP address is routable and reachable across the network2.

upvoted 1 times

Cesar12345 7 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_virtual_interfaces.pdf

upvoted 1 times

fourfour 1 year, 7 months ago

Selected Answer: B

how can wlcs with different mobility group names can belong to the same mobility group?

upvoted 2 times

dazzler_010 1 year, 8 months ago

A looks to be a legitimate answer. Since not all controllers in the mobility group using the same mobility group name, network outage may happen if client roams out to a controller with different mobility group

upvoted 1 times

dazzler_010 1 year, 8 months ago

i mean different mobility group name

upvoted 1 times

Fringe 1 year, 10 months ago

Selected Answer: B

B is the correct answer

upvoted 3 times

Net91 1 year, 11 months ago

B is the correct answer, admin ?

upvoted 2 times

GATUNO 2 years ago

B Response / A prerequisite for configuring Mobility Groups is "All controllers must be configured with the same virtual interface IP address". If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time. -> Answer B is correct.
Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/configguide/b_cg85/mobility_groups.html

upvoted 3 times

GATUNO 2 years, 1 month ago

according cisco link, there is no virtual ip concept, triky question

upvoted 1 times

jjfromoverhere 1 year, 8 months ago

see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/mobility_groups.html
There very clearly is a virtual IP

upvoted 1 times

xziomal9 2 years, 2 months ago

The correct answer is:
B. Not all of the controllers within the mobility group are using the same virtual interface IP address.

upvoted 1 times

nariman93 2 years, 2 months ago

http://what-when-how.com/deploying-and-troubleshooting-cisco-wireless-lan-controllers/configuring-mobility-groups-cisco-wireless-lan-controllers/
Same virtual interface IP address: If the virtual IPs are not the same between the controllers, the handoff of the client database entry will not take place and the client will be disconnected for a short period. -------
I think B is correct

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

ahmedox 2 years, 2 months ago

- different (Name) Mobility Groups ==> the client need to reauthenticate (unless the new controller in the new Mobility Group is in the Mobility List of the Last Controler, in this case the roamin will be seamless)
- Different Virtual Ip adresses for the controllers on the same Mobility Group, the Client will experience a network outage.
so i think the more adequate answer is B.

upvoted 2 times

theunnameddemon 2 years, 6 months ago

Can the APs Join a WLC That Belongs to a Mobility Group That is Different From the Currently Associated Mobility Group?
Yes. By default , when a WLC goes down, the APs registered to this WLC failovers to another WLC of the same Mobility Group, if the LAP is configured for failover. However, if a backup Controller Support is configured, then it can be any WLC even outside the Mobility Group and the access points failovers to controllers even outside the Mobility Group. Refer toN+1 High Availability Deployment Guide for more information.

upvoted 1 times

AliMo123 2 years, 6 months ago

there is no such a concept "same virtual IP" in mobility group. what if the controllers have different IP addresses (intercontroller L3)? A is 100% correct.

upvoted 2 times

jjfromoverhere 1 year, 8 months ago

see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/mobility_groups.html
There very clearly is a virtual IP

upvoted 1 times

Question #144 *Topic 1*

What is the role of the RP in PIM sparse mode?

A. The RP maintains default aging timeouts for all multicast streams requested by the receivers.

B. The RP acts as a control-plane node only and does not receive or forward multicast packets.

C. The RP is the multicast router that is the root of the PIM-SM shared multicast distribution tree.

D. The RP responds to the PIM join messages with the source of a requested multicast group.

Correct Answer: *C*

Community vote distribution

C (100%)

TheNetworkStudent Highly Voted 3 years, 2 months ago

Exam guide: "In essence, two trees are created: an SPT from the FHR to the RP (S,G) and a shared tree from the RP to the LHR (*,G)". The RP is the root of the shared tree in PIM sparse mode, C is correct.

upvoted 24 times

gtddrf 2 years, 3 months ago

Answer is C.
Multicast Distribution Shared Tree - Unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called a rendezvous point (RP).
Source: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/ip_mcast_rtng/b_165_ip_mcast_rtng_9300_cg/b_165_ip_mcast_rtng_9300_9500_cg_chapter_0100.html

upvoted 6 times

Hugh_Jazz 2 years, 1 month ago

When hosts join a multicast group, the directly connected routers send PIM Join messages toward the RP. The RP keeps track of multicast groups. Hosts that send multicast packets are registered with the RP by the first hop router of that host. The RP then sends Join messages toward the source. At this point, packets are forwarded on a shared distribution tree.

upvoted 2 times

Hugh_Jazz 2 years, 1 month ago

Concur with C. D has just enough info that is incorrect in verbiage.

upvoted 2 times

Askhat Highly Voted 3 years, 2 months ago

Correct ans D

upvoted 8 times

Glass17 2 years, 4 months ago

My English i not good enough to understand tricky nuances of Cisco questions, but IMHO:
The RP will not responds to the PIM join messages with "THE SOURCE" of a requested multicast group, but rather will start forwarding multicast traffic in direction of requester.
So "C" would be a better answer.

upvoted 4 times

Ittcainfo Most Recent 8 months, 2 weeks ago

ITTCA.org NO UFRONT PAYMENT!!

GET CERTIFIED IN 2 DAYS.100%PASS GUARANTEED.PAY AFTER RESULTS!!
For the Below certificates

1. AWS Certification
2. Sales force
3. Scrum Master
4. Oracle Certification: OCA, OCP
5. Cisco Certification: CCNA, CCNP
6. ITIL Foundation & Intermediate
7. Prince 2 Foundation and Practitioner
8. VMWARE Certification
9. Check Point Certification (CISA,CISM)
10. EC-COUNCIL Certification (CEH V-9)CCISO
11. Cloud Certification
12. IBM Certification
13. HP Certification
14. Citrix Certification
15. Juniper certification
16. Azure

17.Skype 70-333/34
18.PMI (PMP/CAPM/ACP/PBA ,RMP)
19.ISTQB. Book for online proctor exam and we'll remotely take the exam for you. Pay us after confirmation of results
WhatsApp +1(409)223 7790
upvoted 1 times

pulseberg 8 months, 2 weeks ago

D. The RP responds to the PIM join messages with the source of a requested multicast group.

In PIM (Protocol Independent Multicast) Sparse Mode, the RP (Rendezvous Point) plays a crucial role in facilitating the multicast traffic delivery to the receivers. The RP is responsible for keeping track of the multicast groups and their associated sources in the network. It receives the join messages from the routers and forwards them to the appropriate source(s) of the group. The RP also maintains a mapping between the multicast group address and the source(s) associated with it. When the RP receives the multicast traffic from the source(s), it forwards it to all the routers in the network that have requested to join the group.
upvoted 1 times

dazzler_010 1 year, 8 months ago

RP is root of the PIM-SM SPT. So answer is C.
upvoted 1 times

rettich 1 year, 9 months ago

Selected Answer: C

Answer is 100% C;
D is incorrect because RP does not respond to a Join message, it simply forwards the multicast stream to the reciever . (See also answer from "RTE" and "lukaszr")
upvoted 1 times

testbench007 1 year, 10 months ago

C is the correct answer.
upvoted 1 times

xziomal9 2 years, 2 months ago

The correct answer is:
C. The RP is the multicast router that is the root of the PIM-SM shared multicast distribution tree.
upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct
upvoted 1 times

vdsdrs 2 years, 3 months ago

Rather than guessing based on 3 sentence long paragraph, I encourage you to spend 5 min to read RFC 4609, section 3.3.1.
RP doesn't respond to any join messages.
Correct answer is C.
upvoted 2 times

cracanici 2 years, 3 months ago

D
https://www.juniper.net/documentation/en_US/junos-space-apps/connectivity-services-director4.0/topics/concept/pim-sparse-mode-overview.html
upvoted 1 times

vdsdrs 2 years, 3 months ago

Thanks for the Juniper article - it conforms that correct answer is C.
upvoted 1 times

RTE 2 years, 4 months ago

may be D better
In sparse mode, a router assumes that other routers do not want to forward multicast packets for a group, unless there is an explicit request for the traffic. When hosts join a multicast group, the directly connected routers send PIM Join messages toward the RP. The RP keeps track of multicast groups. Hosts that send multicast packets are registered with the RP by the first hop router of that host. The RP then sends Join messages toward the source. At this point, packets are forwarded on a shared distribution tree. If the multicast traffic from a specific source is sufficient, the first hop router of the host may send Join messages toward the source to build a source-based distribution tree.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16-5/imc-pim-xe-16-5-book/imc-tech-oview.html#GUID-8168D184-0F45-4EAA-B9C0-68403809DE77
upvoted 1 times

vdsdrs 2 years, 3 months ago

Where do you see in the quoted paragraph any info about RESPONDING to any Join messages? RP doesn't respond to join message. It sends its own Join messages towards sources.
C is the only correct answer.
upvoted 1 times

lukaszr 2 years, 4 months ago

C
From Guide: "Figure 13-17 illustrates a multicast source sending multicast traffic to the FHR. The FHR
then sends this multicast traffic to the RP, which makes the multicast source known to the
RP. It also illustrates a receiver sending an IGMP join to the LHR to join the multicast group.

The LHR then sends a PIM join (*,G) to the RP, and this forms a shared tree from the RP to
the LHR. The RP then sends a PIM join (S,G) to the FHR, forming a source tree between the source and the RP. <!>In essence, two trees are created: an SPT from the FHR to the RP (S,G) and a shared tree from the RP to the LHR (*,G)." <!>

upvoted 2 times

v_ermak 2 years, 4 months ago

Sparse Mode
Sparse mode operation centers around a single unidirectional shared tree whose root node is called the rendezvous point (RP). Sources must register with the RP to get their multicast traffic to flow down the shared tree by way of the RP. This registration process actually triggers a shortest path tree (SPT) Join by the RP toward the source when there are active receivers for the group in the network.

A sparse mode group uses the explicit join model of interaction. Receiver hosts join a group at a rendezvous point (RP). Different groups can have different RPs.

Multicast traffic packets flow down the shared tree to only those receivers that have explicitly asked to receive the traffic.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16-5/imc-pim-xe-16-5-book/imc-tech-oview.html

upvoted 1 times

hasanozdemirrr 2 years, 5 months ago

An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree.
C is correct.

upvoted 2 times

AliMo123 2 years, 6 months ago

In PIM-SM, source sends traffic to RP then fwd it towards the reciver. when the receiving router gets the traffic, it will send join message directly to the source creating a source-based distribution tree from the source to the receiver. This mesg does not include RP that's why RP is only needed at the start of the session. C is correct and RP is the root of out tree.

upvoted 2 times

J2DFW 2 years, 7 months ago

C is correct

https://netcraftsmen.com/pim-sparse-mode/

upvoted 1 times

Question #145 *Topic 1*

Why is an AP joining a different WLC than the one specified through option 43?

A. The AP is joining a primed WLC

B. The APs broadcast traffic is unable to reach the WLC through Layer 2

C. The AP multicast traffic is unable to reach the WLC through Layer 3

D. The WLC is running a different software version

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html#:~:text=on%20document%20conventions.-,Overview%20of%20the%20Wireless%20LAN%20Controller%20(WLC)%20Discovery%20and%20Join%20Process,-In%20a%20Cisco

Community vote distribution

A (100%)

Skliffi Highly Voted 3 years, 3 months ago

I think it's A - Primed WLC

Locally stored controller IPv4 or IPv6 address discovery—If the access point was previously associated to a controller, the IPv4 or IPv6 addresses of the primary, secondary, and tertiary controllers are stored in the access point's nonvolatile memory. This process of storing controller IPv4 or IPv6 addresses on an access point for later deployment is called priming the access point.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-6/config-guide/b_cg86/ap_connectivity_to_cisco_wlc.html

upvoted 30 times

Alliam 3 years, 2 months ago

Skliffi, We have to look at it as existing an existing access point not new. If the AP was already primed with the primary, secondary or tertiary controller, so it will join whatever the controller the access point was primed which is the primary controller.

upvoted 2 times

TheNetworkStudent Highly Voted 3 years, 2 months ago

The order of selecting a WLC according to the exam guide:

1: If the AP has previously joined a controller and has been configured or "primed" with a primary, secondary, and tertiary controller, it tries to join those controllers in succession.

2. If the AP does not know of any candidate controller, it tries to discover one (which includes the use of option 43).

Priming an AP directly overrules option 43, so A should be the correct answer.

upvoted 23 times

KZM Most Recent 1 year, 1 month ago

Intra-Controller Roaming: client roaming across access points managed by the same controller.
Inter-Controller Roaming: client roaming across access points in managed by different controllers in the same mobility group and on the same subnet.
Inter-Subnet Roaming: client roaming across access points managed by different controllers in the same mobility group on different subnets.

upvoted 1 times

Pudu_vlad 1 year, 2 months ago

A is correct

upvoted 1 times

GreatDane 1 year, 5 months ago

Ref: How to configure the Lightweight AP in order to join the respective WLAN Controller - Cisco Community

Post by TCC_2

"...
Overview of the Wireless LAN Controller (WLC) Discovery and Join Process
...
In addition to these methods, the LAP does automatically look on the local subnet for controllers with a 255.255.255.255 local broadcast. Also, the LAP remembers the management IP address of any controller it joins across reboots. Therefore, if you put the LAP first on the local subnet of the management interface, it will find the controller's management interface and remember the address. This is called priming. This does not help find the controller if you replace a LAP later on. Therefore, Cisco recommends using the DHCP option 43 or DNS methods.
..."

A. The AP is joining a primed WLC

Correct answer.

B. The APs broadcast traffic is unable to reach the WLC through Layer 2

Wrong answer.

C. The AP multicast traffic is unable to reach the WLC through Layer 3

Wrong answer.

D. The WLC is running a different software version

Wrong answer.

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: A

A is the correct answer. Primed.

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: A

Only if is a primed wlc the controller will have this behavior.

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: A

It should be A

upvoted 3 times

rettich 1 year, 9 months ago

Selected Answer: A

Even if you don't know the right anser you can rule out b, c,d
Why should the AP user boadcast or multicast to communicat with the WLC, when he gets the IP Adresse in option 43. Communication between WLC and AP is always unicast!
D is Wrong becaus if the Software does not match the AP always loads the correct version from the WLC.
So only Anser A ist left

upvoted 5 times

xziomal9 2 years, 2 months ago

The correct answer is:
A. The AP is joining a primed WLC

upvoted 2 times

Hamzaaa 2 years, 7 months ago

Only if a Prime WLC exists, we see this behaviour
A is correct

upvoted 3 times

netpeer 2 years, 8 months ago

Option 43 talks about a LIST of WLCs NOT a single one. It's A.

upvoted 1 times

Jclemente 2 years, 8 months ago

Should be A the correct answer..

upvoted 2 times

numan_ahmed 2 years, 10 months ago

its A, the AP is already primed to another WLC

upvoted 3 times

tonght 2 years, 10 months ago

Correct Answer: A

upvoted 5 times

hku68 2 years, 10 months ago

A is correct.
AP try to join primed controller first. If it has no primed controller, goes option 43.

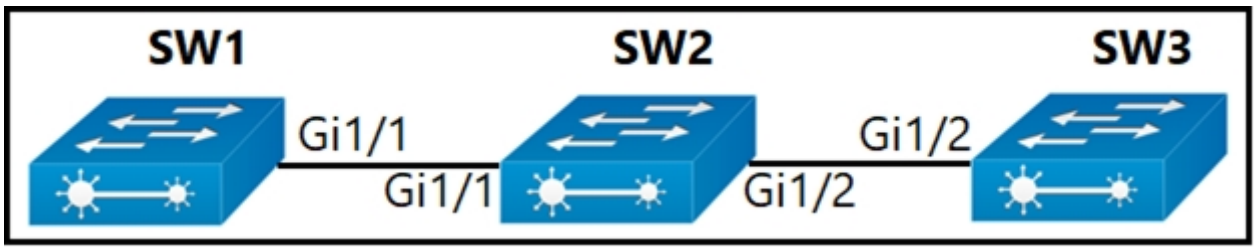
upvoted 4 times

MrBishop 2 years, 11 months ago

Okay, the answer could be different depending on the way the alphabetized your answers, but the correct answer is: The AP is joining a primed WLC
source: https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html Section: Problem 5

upvoted 3 times

Question #146 *Topic 1*



Company policy restricts VLAN 10 to be allowed only on SW1 and SW2. All other VLANs can be on all three switches. An administrator has noticed that VLAN 10 has propagated to SW3.
Which configuration corrects the issue?

A. SW1(config)#int gi1/1 SW1(config)#switchport trunk allowed vlan 1-9,11-4094

B. SW2(config)#int gi1/2 SW2(config)#switchport trunk allowed vlan 10

C. SW2(config)#int gi1/2 SW2(config)#switchport trunk allowed vlan 1-9,11-4094

D. SW1(config)#int gi1/1 SW1(config)#switchport trunk allowed vlan 10

Correct Answer: *C*

Community vote distribution

C (100%)

jmaroto Highly Voted 2 years, 8 months ago

C is the correct answer. A is wrong because we need the vlan 10 in sw1-sw2 trunk.

upvoted 9 times

Viraj007 Highly Voted 2 years, 8 months ago

c is answer

upvoted 5 times

Colmenarez Most Recent 3 months, 4 weeks ago

Selected Answer: C

Awful, I'd issue swi trunk allo vlan remove 10

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: C

tested:
sw1(config-if)#switchport trunk allowed vlan 1-9,11-4094
sw1(config-if)#do s runn interface Port-channel2
Building configuration...

Current configuration : 179 bytes
!
interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1-9,11-4094
switchport mode trunk
spanning-tree port-priority 64
end

sw1(config-if)#do s int tr | i Po2
Po2 on 802.1q trunking 1
Po2 1-9,11-4094
Po2 1,30,40,50,110
Po2 1
sw1(config-if)#

upvoted 1 times

bora4motion 1 year ago

Selected Answer: C

easy one, C

upvoted 1 times

Asymptote 1 year ago

Selected Answer: C

B wipeout all VLANs and only allowed VLAN 10.

upvoted 1 times

Pudu_vlad 1 year, 2 months ago

C is correct

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: C

The provided answer is correct

upvoted 2 times

Nhan 2 years, 2 months ago

I love you guys all are genius the future of the country are here .... Lol just kidding, release some stress :)

upvoted 2 times

bora4motion 1 year ago

and your english is awesome.

upvoted 1 times

rpidcock 2 years, 3 months ago

Agree with all. C is the correct answer as the "switchport trunk allowed vlan 1-9,11-4094" statement when executed on interface Gi1/2, interface config mode of SW2 will limit VLAN 10 from being allowed to SW3.

upvoted 1 times

noov 2 years, 8 months ago

i think that the correct answer is C

upvoted 2 times

Metro 2 years, 8 months ago

C is absolutely right.

upvoted 4 times

Jclemente 2 years, 8 months ago

The correct answer is C...

upvoted 3 times

Question #147 *Topic 1*

Which First Hop Redundancy Protocol should be used to meet a design requirement for more efficient default gateway bandwidth usage across multiple devices?

A. GLBP

B. LACP

C. HSRP

D. VRRP

Correct Answer: *A*

Community vote distribution

A (100%)

[Removed] Highly Voted 2 years, 10 months ago

glbp: cisco prop, load balancing per request/per host
lacp: not a fhrp
hsrp: cisco prop, no load balancing, active/passive, useful in DC with VPC
vrrp: ietf, for saving an ip address

upvoted 17 times

bora4motion Most Recent 1 year ago

Selected Answer: A

A is correct.

upvoted 2 times

Pudu_vlad 1 year, 2 months ago

A is correct

upvoted 2 times

Nhan 2 years, 1 month ago

Stupid autocorrect I mean GLBP = use all router in the group (up to 4 routers)

upvoted 3 times

Nhan 2 years, 1 month ago

Bascially, with flap you can ultilize all router in the group using round robin, for load balancing, in other word, all router in the group are active.

upvoted 3 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 2 times

Question #148 *Topic 1*

A client device roams between access points located on different floors in an atrium. The access points are joined to the same controller and configured in local mode. The access points are in different AP groups and have different IP addresses, but the client VLAN in the groups is the same.
Which type of roam occurs?

A. inter-controller

B. inter-subnet

C. intra-VLAN

D. intra-controller

Correct Answer: *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-3/config-guide/b_cg83/b_cg83_chapter_010011.html

Community vote distribution

D (100%)

AliMo123 Highly Voted 2 years, 7 months ago
Intar means within while inter means between, so as long as the APs are on the same WLC, then it is a intra-controller
upvoted 15 times

Eddgar0 Most Recent 1 year, 7 months ago
Selected Answer: D
Same controllers, means intracontroller so D is correct
upvoted 1 times

XalaGyan 1 year, 12 months ago
given answer is correct
upvoted 1 times

examShark 2 years, 6 months ago
Given answer is correct
upvoted 2 times

Question #149 *Topic 1*

Which DHCP option helps lightweight APs find the IP address of a wireless LAN controller?

A. Option 43

B. Option 60

C. Option 67

D. Option 150

Correct Answer: *A*

Community vote distribution

A (100%)

bora4motion 1 year ago

Selected Answer: A

A is correct

upvoted 2 times

Eddgar0 1 year, 7 months ago

Selected Answer: A

Given answer is correct

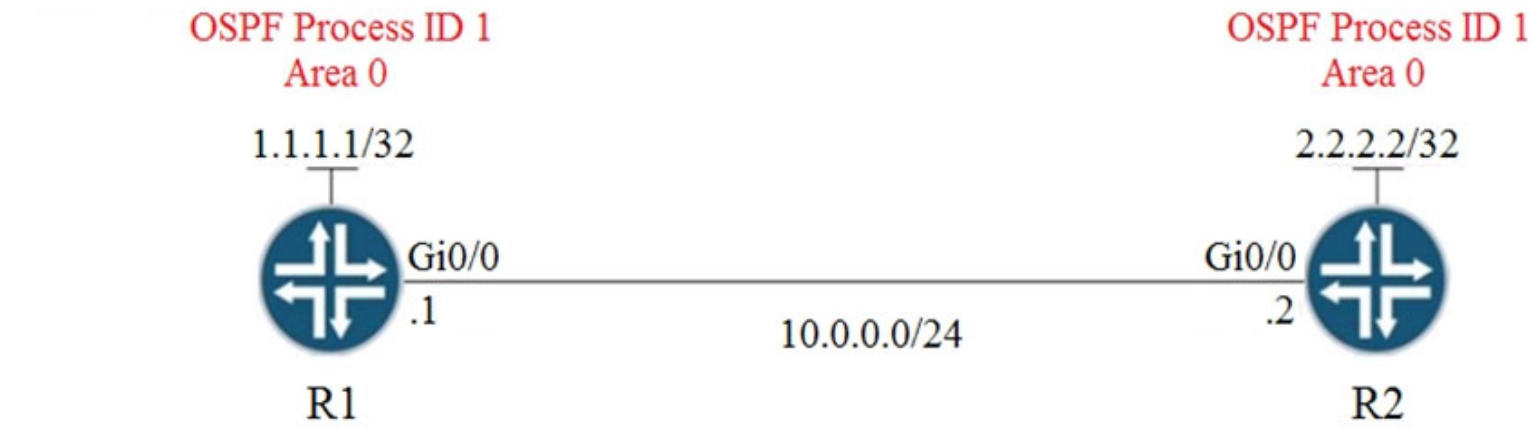
upvoted 2 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 4 times

Refer to the exhibit.




```
Router R1
router ospf 1
   router-id 1.1.1.1
   network 1.1.1.1 0.0.0.0 area 0
   network 10.0.0.0 0.0.0.255 area 0
```

```
Router R2
router ospf 1
   router-id 2.2.2.2
   network 2.2.2.2 0.0.0.0 area 0
   network 10.0.0.0 0.0.0.255 area 0
```

A network engineer is configuring OSPF between router R1 and router R2. The engineer must ensure that a DR/BDR election does not occur on the Gigabit
Ethernet interfaces in area 0.
Which configuration set accomplishes this goal?

A. R1(config-if)interface Gi0/0 R1(config-if)ip ospf network point-to-point R2(config-if)interface Gi0/0 R2(config-if)ip ospf network point-to-point

B. R1(config-if)interface Gi0/0 R1(config-if)ip ospf network broadcast R2(config-if)interface Gi0/0 R2(config-if)ip ospf network broadcast

C. R1(config-if)interface Gi0/0 R1(config-if)ip ospf database-filter all out R2(config-if)interface Gi0/0 R2(config-if)ip ospf database-filter all out

D. R1(config-if)interface Gi0/0 R1(config-if)ip ospf priority 1 R2(config-if)interface Gi0/0 R2(config-if)ip ospf priority 1

Correct Answer: *A*

Community vote distribution

A (100%)

xziomal9 Highly Voted 2 years, 2 months ago

A.
R1(config-if)interface Gi0/0
R1(config-if)ip ospf network point-to-point
R2(config-if)interface Gi0/0
R2(config-if)ip ospf network point-to-point
B.
R1(config-if)interface Gi0/0
R1(config-if)ip ospf network broadcast
R2(config-if)interface Gi0/0
R2(config-if)ip ospf network broadcast
C.
R1(config-if)interface Gi0/0
R1(config-if)ip ospf database-filter all out
R2(config-if)interface Gi0/0
R2(config-if)ip ospf database-filter all out
D.
R1(config-if)interface Gi0/0
R1(config-if)ip ospf priority 1
R2(config-if)interface Gi0/0
R2(config-if)ip ospf priority 1

The correct answer is:
A

upvoted 10 times

Asymptote Most Recent 1 year ago

Selected Answer: A

OSPF interfaces with P2P connection type no DR and BDR election is required.

Reference:
https://learningnetwork.cisco.com/s/question/0D53i00000Kt70lCAB/why-no-dr-or-bdr-in-ospf-with-point-to-point-link

upvoted 2 times

Pudu_vlad 1 year, 2 months ago

A is correct

upvoted 1 times

Nhan 2 years, 2 months ago

The ospf will use the loop back int to form the adjacency after the configuration is done. A is correct answer

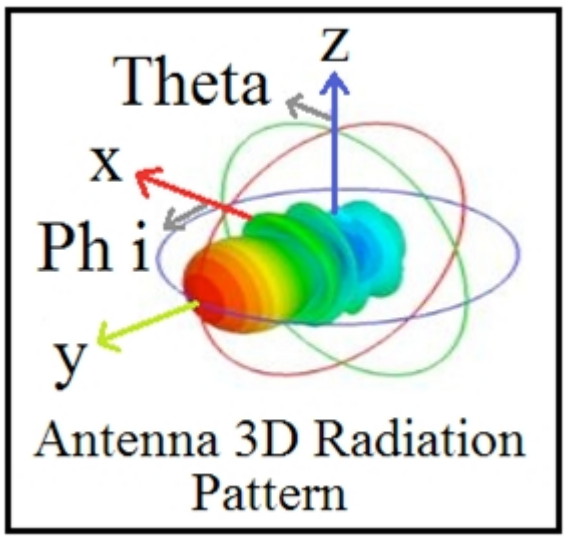
upvoted 4 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 1 times

Refer to the exhibit.



Which type of antenna does the radiation pattern represent?

A. multidirectional

B. directional patch

C. omnidirectional

D. Yagi

Correct Answer: *D*

Reference:

https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html

Community vote distribution

D (100%)

Dataset 3 months, 1 week ago

hi!
what is the difference with directional?
thanks

upvoted 1 times

LanreDipeolu 3 months, 3 weeks ago

Selected Answer: D

It resembles patch radiation but the correct answer is yagi "D" because of the enhanced curvature at the E-plane

upvoted 1 times

Pudu_vlad 1 year, 2 months ago

D is correct

upvoted 2 times

pierresadou 1 year, 7 months ago

Selected Answer: D

D is correct

upvoted 3 times

examShark 2 years, 6 months ago

Given solution is correct

upvoted 4 times

Question #152 *Topic 1*

Wireless users report frequent disconnections from the wireless network. While troubleshooting, a network engineer finds that after the user is disconnected, the connection re-establishes automatically without any input required. The engineer also notices these message logs:
AP 'AP2' is down. Reason: Radio channel set. 6:54:04 PM
AP 'AP4' is down. Reason: Radio channel set. 6:44:49 PM
AP 'AP7' is down. Reason: Radio channel set. 6:34:32 PM
Which action reduces the user impact?

A. enable coverage hole detection

B. increase the AP heartbeat timeout

C. enable BandSelect

D. increase the dynamic channel assignment interval

Correct Answer: *D*

Community vote distribution

D (71%) A (29%)

AliMo123 Highly Voted 2 years, 7 months ago

when a radio changes from one channel to another, the user gets disconnected shortly, so increase DCA to more than 10 mins(default DCA) to reduce the number of times users are disconnceted .

upvoted 14 times

Rose66 Highly Voted 10 months, 4 weeks ago

Selected Answer: D

These message logs inform that the radio channel has been reset (and the AP must be down briefly). With dynamic channel assignment (DCA), the radios can frequently switch from one channel to another but it also makes disruption. The default DCA interval is 10 minutes, which is matched with the time of the message logs. By increasing the DCA interval, we can reduce the number of times our users are disconnected for changing radio channels.

upvoted 5 times

Asher Most Recent 4 months ago

The RRMcoverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.
Don't think this meets the criteria

upvoted 1 times

ibogovic 5 months, 1 week ago

Selected Answer: A

A. Enable coverage hole detection.

The symptoms described in the scenario, where wireless users experience frequent disconnections from the network but the connection re-establishes automatically without any input, can be indicative of coverage holes in the wireless network. Coverage holes are areas where the wireless signal strength is insufficient, leading to connectivity issues for users within those areas.

By enabling coverage hole detection, the wireless network can identify and mitigate these coverage holes more effectively. Coverage hole detection allows the access points (APs) to monitor the signal strength and quality within their coverage areas. If a coverage hole is detected, the AP can take proactive measures to address the issue, such as adjusting transmit power, optimizing channel selection, or triggering alarms for further investigation.

Enabling coverage hole detection helps in identifying and resolving areas with poor coverage, improving the overall user experience by reducing the frequency of disconnections.

upvoted 1 times

JCSantana20 1 month, 3 weeks ago

That would be a good answer if we didn't have the logs. The access points are readjusting their radio channels within the frequency and are coming down very briefly because of that.

upvoted 1 times

MaxwellJK 4 months, 1 week ago

Great argument but is not correct. the reason is "radio channel set". So option D is the correct one.

upvoted 1 times

habibmangal 7 months, 2 weeks ago

Selected Answer: A

Of the options provided, the most relevant action that can help with this issue is to enable coverage hole detection. Coverage hole detection allows access points to detect when client devices are unable to connect or stay connected to the wireless network due to a weak signal or other

issues, and take appropriate action to mitigate the issue, such as increasing transmit power or changing channels. Therefore, the correct answer is A. enable coverage hole detection.

upvoted 1 times

Dimitryvld 1 year ago

read carefully: reduces, so not solves completely..

upvoted 1 times

danielponce7 1 year, 10 months ago

What the wright answer

upvoted 1 times

youtri 1 year, 11 months ago

https://packet6.com/configuring-cisco-rrm-dca-dynamic-channel-assignment/

upvoted 1 times

Refer to the exhibit.

```
access-list 1 permit 172.16.1.0 0.0.0.255
ip nat inside source list 1 interface gigabitethernet0/0 overload
```

The inside and outside interfaces in the NAT configuration of this device have been correctly identified.

What is the effect of this configuration?

A. NAT64

B. dynamic NAT

C. static NAT

D. PAT

Correct Answer: *D*

Pudu_vlad 1 year, 2 months ago

D is correct

upvoted 1 times

Nhan 2 years, 2 months ago

DDDDDDDDDDDDDDDDD JUST KIDDING

upvoted 1 times

kthekillerc 2 years, 5 months ago

D is the correct answer

upvoted 3 times

harbaksh 2 years, 7 months ago

Should be B
No ports involved

upvoted 1 times

Rockford 2 years, 6 months ago

I think your thinking of the wrong kind of port, PAT is NAT overload: Port Address Translation (PAT) is also called as NAT Overloading. Port Address Translation (PAT/NAT Overload) is the NAT technology which prevents IPv4 Address depletion. Port Address Translation (PAT/NAT Overload) can map multiple Private IPv4 addresses to a single public IP address by using different source ports.

upvoted 9 times

AliMo123 2 years, 6 months ago

D is correct
overload means more than one port in NAT process

upvoted 7 times

timtgh 1 year, 6 months ago

Actually "overload" means you are overloading fewer inside global addresses (in this case, the single gig0/0 address), with more than one local addresses (to support multiple devices).

upvoted 4 times

timtgh 1 year, 6 months ago

And yes, D is correct.

upvoted 3 times

Akam 2 years, 3 months ago

If you have no enough knowledge please do not write any comment, even a beginner knows the keyword (overload) means your are using PAT, so what port you are talking about?

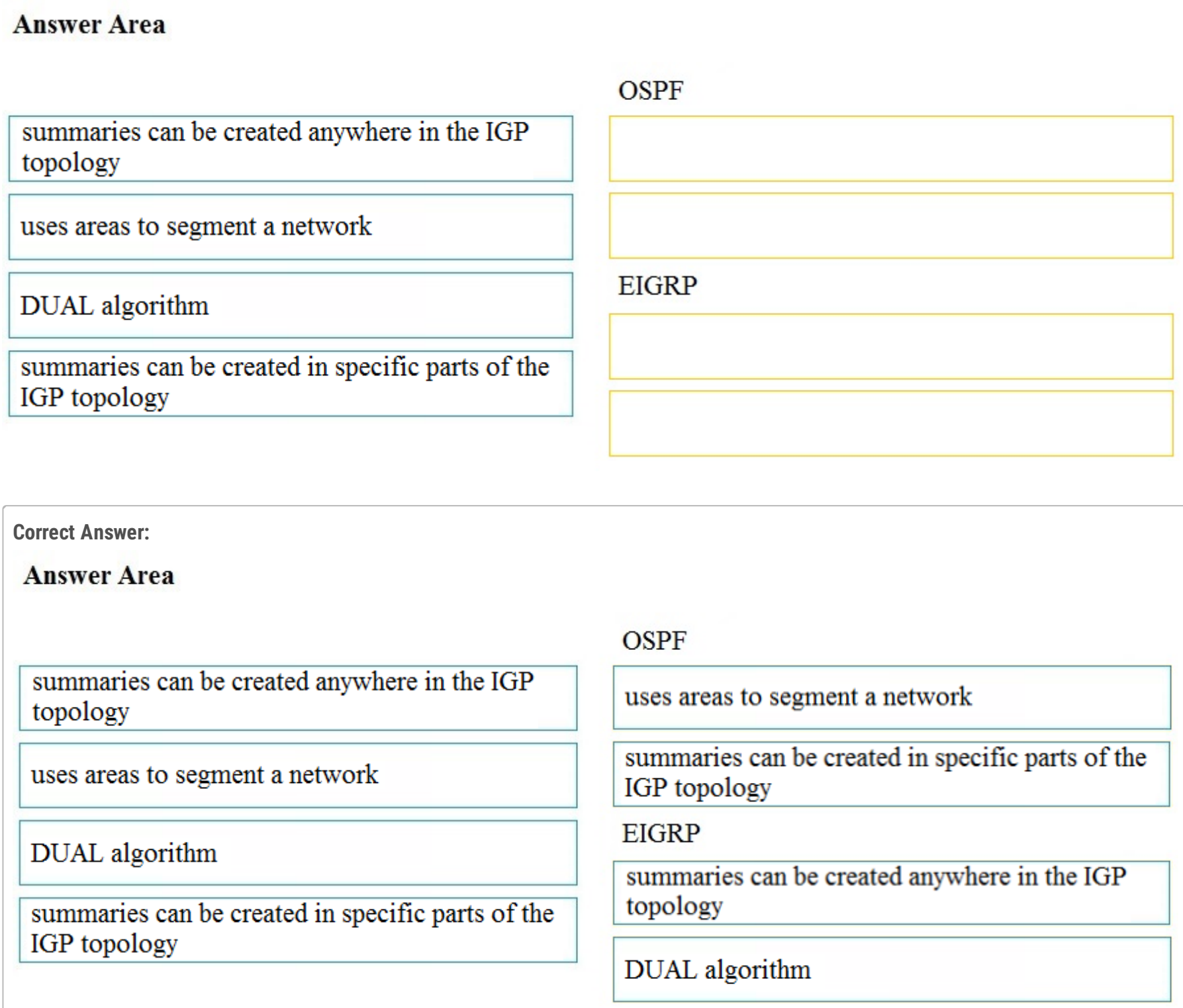
upvoted 13 times

Question #154 *Topic 1*

DRAG DROP -

Drag and drop the descriptions from the left onto the routing protocol they describe on the right.

Select and Place:



Correct Answer:

examShark Highly Voted 2 years, 6 months ago

The given answer is correct.

upvoted 8 times

CCNPWILL Most Recent 1 month, 1 week ago

Provided answer is correct. I approve!

upvoted 1 times

[Removed] 4 months, 3 weeks ago

Answer is correct

upvoted 1 times

[Removed] 4 months, 3 weeks ago

OSPF
-uses areas to segment a network
summaries can be created in specific parts of the IGP topology

EIGRP
-DUAL algorithm
-summaries can be created anywhere in the IGP topology

upvoted 1 times

Asymptote 1 year ago

Answer is correct

upvoted 2 times

Question #155 *Topic 1*

What is the purpose of an RP in PIM?

A. send join messages toward a multicast source SPT

B. ensure the shortest path from the multicast source to the receiver

C. receive IGMP joins from multicast receivers

D. secure the communication channel between the multicast sender and receiver

Correct Answer: *A*

Community vote distribution

A (95%) 5%

examShark Highly Voted 2 years, 6 months ago

The given answer is correct

upvoted 10 times

ABC123 2 years, 4 months ago

So what is the role of FHR then? as per official Cert guide page 348 paragraph "PIM Shared and Source Path Trees", PIM SPT joins sent from RP to FHR not to the source..?

upvoted 2 times

vdsdrs 2 years, 3 months ago

Look closely at the answer.
'Send join messages TOWARD a multicast source' - not '[...] TO multicast source'
You are right that RP join message will be send TO FHR but it is also correct that the join messages are sent TOWARDS source.

A is correct answer.

upvoted 9 times

Violator Highly Voted 1 year, 9 months ago

This question is still asked. Passed today.

upvoted 9 times

baid 1 year, 8 months ago

Congratulations on your passing.

upvoted 2 times

[Removed] Most Recent 5 months, 2 weeks ago

Selected Answer: A

Correct Answer: A
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-pim-allowrp.html#:~:text=.%20In%20a%20PIM,source%20and%20receiver.

upvoted 1 times

NTGuru 7 months, 2 weeks ago

A is the correct answer .
The RP receives PIM join from the LHR
The LHR receives IGMP join from the receiver
The RP receives PIM register from the FHR
https://docs.nvidia.com/networking-ethernet-software/knowledge-base/Configuration-and-Usage/Network-Configuration/Pim-Overview/#:~:text=First%20Hop%20Router%20(FHR),to%20an%20interested%20multicast%20receiver.

upvoted 2 times

Ayman_B 11 months ago

Selected Answer: A

(RP) is used to establish communication between a source and the receivers in a multicast group using PIM protocols, so it sends join messages toward a multicast source using Protocol (PIM) to build the distribution tree for the multicast group SPT

upvoted 5 times

endy023 11 months ago

Answer is B
An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree

upvoted 1 times

captainjee 1 year, 2 months ago

but what is a multicast source shortest path tree?
multicast source is the source of the traffic. SPT is describing the specific route/tree through the multicast network - there is no such thing as a multicast source SPT...
upvoted 1 times

timtgh 1 year, 6 months ago

Selected Answer: A

The answer is A because an RP does send a join message towards the source.
Note: The comments saying that IGMP operates at L2 are incorrect. IGMP and PIM are both L3 protocols and are carried in IP packets. Only IGMP Snooping, a switch feature, operates at L2.
upvoted 3 times

Aldebeer 1 year, 7 months ago

Selected Answer: A

An LHR receives an IGMP join from a receiver. Then, It sends a PIM join toward the RP :
upvoted 3 times

Eddgar0 1 year, 7 months ago

Selected Answer: A

The A is correct, the is tricky but clearly RP does no receive IGMP Join messages so making C. incorrect
upvoted 2 times

ciscolessons 1 year, 9 months ago

Selected Answer: A

Given answer is correct.
upvoted 1 times

bogd 1 year, 9 months ago

Selected Answer: A

Answer is A.

C is misleading, because it mentions IGMP joins (not PIM joins!)
upvoted 3 times

ciscolessons 1 year, 9 months ago

You are correct I believe!
upvoted 2 times

rettich 1 year, 9 months ago

Selected Answer: C

A. incorrect because RP uses a shared tree and not SPT (shortes path tree)
B. incorrect because a shared tree is not always the shortest path between source and reciever
C. correct
D.incorrect because RP does not add any security
upvoted 1 times

Eddgar0 1 year, 7 months ago

Disagree, RP uses SPT toward th FHR. and shared tree toward to receivers. find on Multicast on OCG. so A is CORRECT
C: NOT CORRECT because RP does not receive IGMP JOIN messages, that funcion is for LHR.
upvoted 2 times

Nhan 2 years, 1 month ago

The given answer is correct also STP = shortest path tree
upvoted 1 times

xziomal9 2 years, 2 months ago

The correct answer is:
C. receive IGMP joins from multicast receivers
upvoted 2 times

Eddgar0 1 year, 7 months ago

FALSE, RP does not receive IGMP join messages that funciont is for LHR's
upvoted 1 times

AliMo123 2 years, 6 months ago

is not A because
An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree. By default, when the first hop router of the receiver learns about the source, it will send a join message directly to the source, creating a source-based distribution tree from the source to the receiver. This source tree does not include the RP unless the RP is located within the shortest path between the source and receiver.
https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html
upvoted 1 times

AliMo123 2 years, 6 months ago

correction:
I have checked this question and A is correct and here is why:
IGMP happens at layer 2 between a receiver and a local router, so IGMP is received by a router which is close to a receiver.
PIM is occurring at layer 3 where all the local routers send their requests to RP and then RP sends join mesgs towards multicast source. so IGMP is received by local routers where they send requests to RP(close to multicast source) to find the response for these requests.

upvoted 7 times

amgue 2 years, 6 months ago

I am a little bit confused about this question, the JOIN message will be sent frome receiver to RP and frome RP to the source

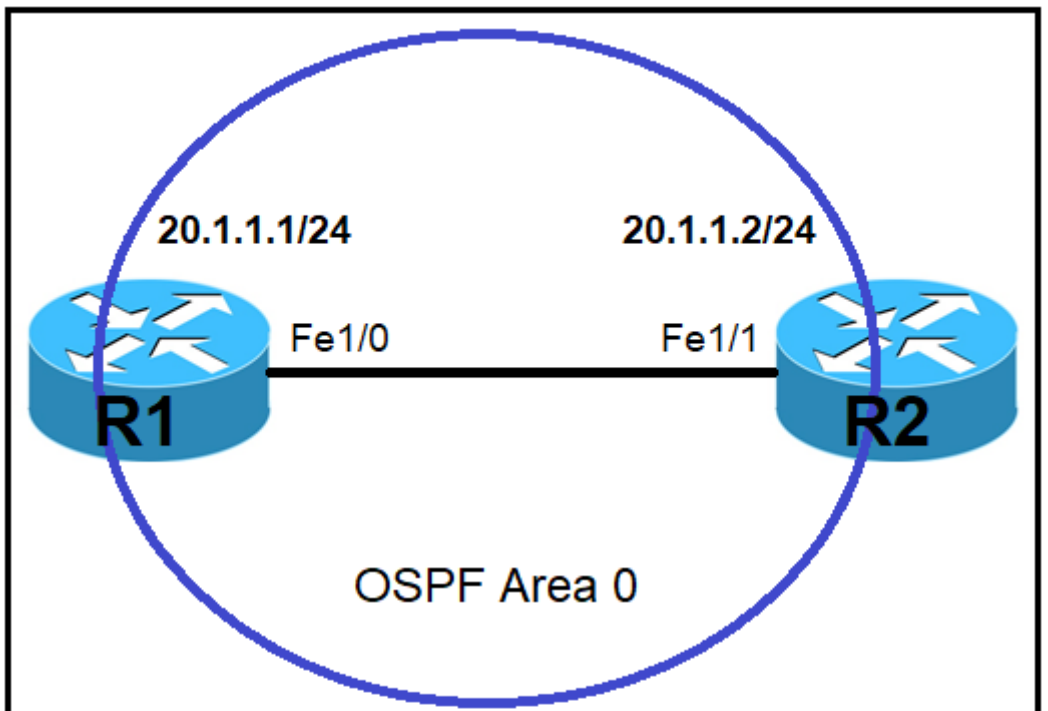
upvoted 1 times

amgue 2 years, 6 months ago

The correct answer is A, I just saw IGMP in answer C which is wrong because RP don't receive IGMP messages

upvoted 2 times

Question #156 *Topic 1*




```
hostname R1
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
auto-cost reference-bandwidth 1000
!
hostname R2
router ospf 2
network 20.0.0.0 0.0.0.255 area 0
```

Refer to the exhibit. Which command must be applied to R2 for an OSPF neighborship to form?

A. network 20.1.1.2 255.255.0.0 area 0

B. network 20.1.1.2 0.0.0.0 area 0

C. network 20.1.1.2 255.255.255.255 area 0

D. network 20.1.1.2 0.0.255.255 area 0

Correct Answer: *B*

Community vote distribution

B (100%)

pyrokar Highly Voted 1 year, 4 months ago

This question is stupid.
B, C and D all work. Tested on two 1941 routers running on IOS 15.1.
This is due to the fact the network command just specifies interfaces that run OSPF and due to the wildcards all three options have 20.1.1.2 inside their range.
B is a /32 and simpoly the IP
C will be automaticly converted to 0.0.0.0 255.255.255.255
D will be automaticly converted to 20.1.0.0 0.0.255.255

upvoted 14 times

[Removed] Most Recent 5 months ago

Selected Answer: B

As stated by others, B, C, and D all work, but the question is asking to just form a neighborship. B is The one that specifically targets that directive and no more.

upvoted 1 times

Asymptote 1 year ago

Selected Answer: B

From the security prospective,
advertising just enough network is a good practise.
B definitely the best among.

upvoted 4 times

Pudu_vlad 1 year, 2 months ago

B is correct
upvoted 2 times

KZM 1 year, 3 months ago
"B", "C", and "D" will work, I think. But "B" is more specific and best practice.
upvoted 1 times

tara38 1 year, 7 months ago
Selected Answer: B
Tested in GNS3 as seen below
R2(config)#router ospf 2
R2(config-router)#network 20.1.1.2 0.0.0.0 area 0
R2(config-router)#
*Mar 1 00:10:02.131: %OSPF-5-ADJCHG: Process 2, Nbr 1.1.1.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
R2(config-router)#end
*Mar 1 00:10:07.555: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
1.1.1.1 1 FULL/DR 00:00:38 20.1.1.1 FastEthernet0/0
R2#
So B is correct!
upvoted 3 times

Eddgar0 1 year, 7 months ago
Selected Answer: B
Given answer is corrrect
upvoted 1 times

Mdorgham 1 year, 8 months ago
Answer should be C.
Regardless on using Wildcard mask or not ,the subnets should match for neighbors to come up
upvoted 1 times

timtgh 1 year, 6 months ago
No. The network command has nothing to do with the subnet matching. The IP addresses are both on the same subnet (20.1.0.0/24), so that requirement is met. Wildcard masks are a separate topic and have no effect on that rule. The wildcard masks on two routers don't have to match, as long as the result of the mask causes the correct interfaces to be included (on both sides).
upvoted 4 times

timtgh 1 year, 6 months ago
Typo correction: the subnet is 20.1.1.0/24.
upvoted 1 times

maymaythar 1 year, 10 months ago
Selected Answer: B
Due to wildcard masks that OSPF use to be more specific which allow having OSPF hello packet to be synchronised between two routers
upvoted 2 times

Carl1999 2 years ago
C.
The network mask must exactly match the neighbor router in order to establish an OSPF neighbor.
upvoted 2 times

OhBee 1 year, 10 months ago
But OSPF uses wildcard masks, so 0.0.0.0 is more specific than 255.255.255.255. So B is the answer :)
upvoted 3 times

timtgh 1 year, 6 months ago
No. The IP subnet (of the interface IP address) is what has to match. That has nothing to do with the wildcard mask in the "network" command. The routers don't see each other's wildcard mask, and they are not compared, and there is absolutely no rule saying they have to match.
upvoted 1 times

kthekillerc 2 years, 2 months ago
Provided answer is correct
upvoted 2 times

rpidcock 2 years, 3 months ago
I agree the B is correct. Because 20.1.1.2 is an individual IP vs. a /24 subnet like 21.1.1.0, then it would be appropriate to have an exact match wildcard mask (i.e. 0.0.0.0).
upvoted 3 times

examShark 2 years, 6 months ago
The given answer is correct
upvoted 2 times

Chkoupipi2 2 years, 7 months ago

I think it's more D isn't it ?

upvoted 1 times

AliMo123 2 years, 6 months ago

0.0.0.0 is more specific than 0.0.255.255

upvoted 2 times

AliMo123 2 years, 6 months ago

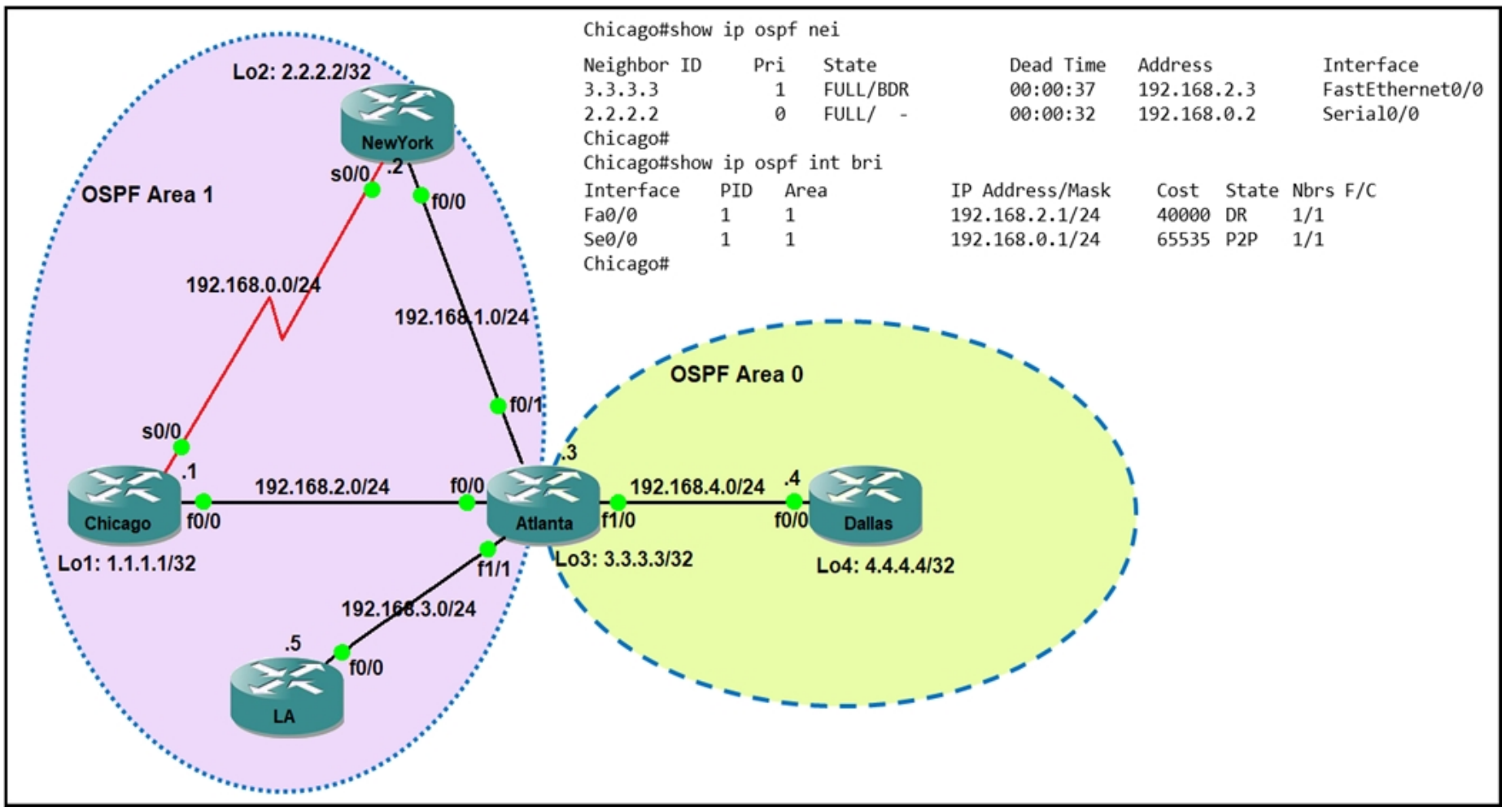
The network 20.0.0.0 0.0.0.255 area (" command on R2 did not cover the IP address of Fal/1 interface of R2 so OSPF did not run on this interface. Therefore we have to use the command "network 20.1.1.2 0.0.255.255 area 0" to turn on OSPF on this interface.
Note: The command "network 20.1.1.2 0.0.255.255 area 0" can be used too so this answer is also correct but answer B is the best answer here.

upvoted 4 times

timtgh 1 year, 6 months ago

If you use 0.0.255.255 for the mask, that is /16, so you would just put 20.1.0.0 for the address. Putting 20.1.1.2 with a /16 mask doesn't make sense. But it's harmless, and most Cisco routers will automatically zero out the unneeded bits, and change it to 20.1.0.0 in the running config.

upvoted 3 times



Refer to the exhibit. Which router is the designated router on the segment 192.168.0.0/24?

A. This segment has no designated router because it is a p2p network type.

B. Router Chicago because it has a lower router ID.

C. Router NewYork because it has a higher router ID.

D. This segment has no designated router because it is a nonbroadcast network type.

Correct Answer: *A*

Community vote distribution

A (100%)

Violator Highly Voted 1 year, 9 months ago

This question is still asked. Passed today.

upvoted 7 times

danman32 Most Recent 4 months, 4 weeks ago

All this mess of a topology in the exhibit, and all we're needing to be interested in is the link between NY and Chicago.
Even just the Show information is sufficient, but the topology diagram homes it in. I didn't even look at the Show information and had the answer, though it confirms the network type.

upvoted 1 times

wabenzy 5 months ago

Selected Answer: A

A is the correct answer.
Whenever you see "point-to" in and SOPF network type know that there is no DR and BDR election.

upvoted 1 times

[Removed] 5 months ago

Selected Answer: A

correct

upvoted 1 times

JMAN78 5 months ago

Why is answer A correct?
why is answer A correct?

upvoted 1 times

danman32 4 months, 4 weeks ago

Because the connection between NY and Chicago is a P2P. P2P network types do not have DR/BDR.

upvoted 2 times

danielponce7 1 year, 10 months ago

Selected Answer: A

A is correct

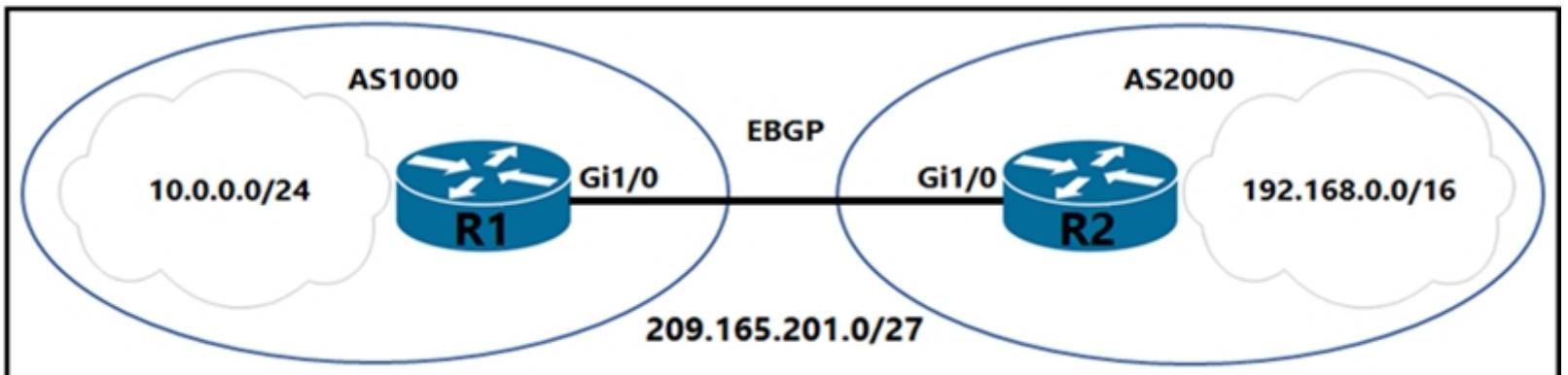
upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 4 times

Question #158 *Topic 1*




```
R1
router bgp 1000
address-family ipv4 unicast
neighbor 209.165.201.2 remote-as 2000
network 10.0.0.0 mask 255.255.255.0
description Peer Router B

R2
router bgp 2000
address-family ipv4 unicast
neighbor 209.165.201.1 remote-as 1000
network 10.0.0.0 mask 255.255.255.0
description Peer Router A
```

Refer to the exhibit. Which two commands are needed to allow for full reachability between AS 1000 and AS 2000? (Choose two.)

A. R2#no network 10.0.0.0 255.255.255.0

B. R2#network 209.165.201.0 mask 255.255.192.0

C. R2#network 192.168.0.0 mask 255.255.0.0

D. R1#no network 10.0.0.0 255.255.255.0

E. R1#network 192.168.0.0 mask 255.255.0.0

Correct Answer: *AC*

Community vote distribution

AC (100%)

rpidcock Highly Voted 2 years, 3 months ago

A & C are correct. Need to negate the 10.0.0.0 /24 network on R2 and then add the 192.168.0.0 /16 network on R2. Hence, A & C, although I think to be exact the answer on A should be "no network 10.0.0.0 mask 255.255.255.0" vs. the "no network 10.0.0.0 255.255.255.0".

upvoted 11 times

Nhan Highly Voted 2 years, 2 months ago

Basically R2 need to advertise the network 182.168.... Not 10.0....

upvoted 8 times

myhdtv6 Most Recent 4 months, 2 weeks ago

R1 do not need anything to be changed and all correct, so D & E not the answer straight.

between A,B,C , B is the network interface running on its onw, its not the neighbor, so B removed as well

left over A & C is the answer

upvoted 1 times

[Removed] 5 months ago

Selected Answer: AC

correct

upvoted 1 times

iGlitch 1 year ago

The answers are correct but I think there is a typo in A.

upvoted 2 times

danman32 4 months, 4 weeks ago

What's the typo?
If you are referring to being in the proper configuration mode, then C also has a typo.
Otherwise A has correct syntax: the network being removed is a /24 or 255.255.255.0 subnet mask.

upvoted 1 times

Ebsa 2 years ago

given answer is correct

upvoted 1 times

cracanici 2 years, 3 months ago

A C seems to me

upvoted 1 times

joffrea 2 years, 3 months ago

A & D are the correct answer.

upvoted 1 times

danman32 4 months, 4 weeks ago

You need what D is removing, so that R1 advertises the 10.0.0.0/24 network

upvoted 1 times

joffrea 2 years, 3 months ago

the given answer is correct

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

```
interface Vlan10
 ip vrf forwarding Clients
 ip address 192.168.1.1. 255.255.255.0
!
interface Vlan20
 ip vrf forwarding Servers
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
 ip vrf forwarding Printers
 ip address 10.1.1.1 255.255.255.0
-- output omitted for brevity --
 router eigrp 1
 10.0.0.0
 172.16.0.0
 192.168.1.0
```

Refer to the exhibit. An engineer attempts to configure a router on a stick to route packets between Clients, Servers, and Printers; however, initial tests show that this configuration is not working. Which command set resolves this issue?

A. interface Vlan10 no ip vrf forwarding Clients ! interface Vlan20 no ip vrf forwarding Servers ! interface Vlan30 no ip vrf forwarding Printers

B. router eigrp 1 network 10.0.0.0 255.255.255.0 network 172.16.0.0 255.255.255.0 network 192.168.1.0 255.255.255.0

C. interface Vlan10 no ip vrf forwarding Clients ip address 192.168.1.1. 255.255.255.0 ! interface Vlan20 no ip vrf forwarding Servers ip address 172.16.1.1 255.255.255.0 ! interface Vlan30 no ip vrf forwarding Printers ip address 10.1.1.1 255.255.255.0

D. router eigrp 1 network 10.0.0.0 255.0.0.0 network 172.16.0.0 255.255.0.0 network 192.168.1.0 255.255.0.0

Correct Answer: *C*

Community vote distribution

C (95%) 5%

BB234 Highly Voted 2 years, 4 months ago

Removing the VRF also removes the configured IP address

upvoted 16 times

cracanici 2 years, 2 months ago

not like this, it does not

interface Vlan20
no ip vrf forwarding Servers
ip address 172.16.1.2 255.255.255.0

upvoted 3 times

iAbdullah 2 years, 1 month ago

You right thank you

upvoted 1 times

FrameRelay Highly Voted 1 year, 1 month ago

Selected Answer: C

Correct Answer is C.
Just to add my vote to help clarify, once you remove the VRF from the interface, this also strips the IP address configuration previously configured, therefore remove the VRF and then configure the interface IP.

upvoted 15 times

yellowswan Most Recent 3 months, 2 weeks ago

hahaha, I thought it would configure a route leak between different VRFs, the answer told me just to delete the vrf directly!!

upvoted 1 times

goomisch 6 months, 4 weeks ago

C ofcourse. - to be honest I like answer like this, "good feature, turn it off" :)

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: C

as I understood it the idea of the question to migrate all IPs to the global routing table (GRT) if so "C" scenario should work

upvoted 2 times

Zikosheka 1 year, 2 months ago

C
IPs will be removed, and we need to re-configure the IPs for each interface

upvoted 2 times

tckoon 1 year, 3 months ago

Only correct answer is C. Remove VRF from interface definately remove interface IP address.
Trick of this answer C is it add back interface IP address with other than .1 which trigger panic to us. By right it will not work as clients GW IP is pointing to .1. (likely mistake in the question preparation)

upvoted 1 times

tckoon 1 year, 1 month ago

type in answer C had been corrected by admin. the GW IP is .1

upvoted 1 times

redgi0 1 year, 3 months ago

Selected Answer: C

I choose C IP is removed. and it does make sense too.
too dangerous to keep the IP, what do we do if that IP is duplicated ?

IOU7(config)#int vlan10
IOU7(config-if)#do sh run int vlan10
Building configuration...

Current configuration : 88 bytes
!
interface Vlan10
vrf forwarding Customer1
ip address 192.168.1.1 255.255.255.0
end

IOU7(config-if)#no vrf forwarding Customer1
% Interface Vlan10 IPv4 disabled and address(es) removed due to enabling VRF

IOU7(config-if)#do sh run int vlan10
Building configuration...

Current configuration : 39 bytes
!
interface Vlan10
no ip address
end

upvoted 2 times

kelapasawit 1 year, 4 months ago

Selected Answer: A

Removing VRF doesn't remove ip address.
It required the router to reboot in order remove the configuration from the show run.

upvoted 1 times

aurthur 1 year, 10 months ago

A.
interface Vlan10 no ip vrf forwarding Clients
!
interface Vlan20 no ip vrf forwarding Servers
!
interface Vlan30 no ip vrf forwarding Printers

B.
router eigrp 1
network 10.0.0.0 255.255.255.0
network 172.16.0.0 255.255.255.0
network 192.168.1.0 255.255.255.0

C.
interface Vlan10
no ip vrf forwarding Clients ip address 192.168.1.2. 255.255.255.0
!
interface Vlan20
no ip vrf forwarding Servers ip address 172.16.1.2 255.255.255.0
!
interface Vlan30
no ip vrf forwarding Printers ip address 10.1.1.2 255.255.255.0

D.
router eigrp 1

network 10.0.0.0 255.0.0.0
network 172.16.0.0 255.255.0.0
network 192.168.1.0 255.255.0.0

upvoted 7 times

diegodavid82 2 years, 1 month ago

Provided Answer is correct. C

upvoted 2 times

Nhan 2 years, 2 months ago

VRF is creating virtual router, there for there is no routing among those subnet, router on a stick is all subnet are creating in one router using sub interface or physical int but all int must be in one router

upvoted 3 times

cracanici 2 years, 2 months ago

not like this, it does not

interface Vlan20
no ip vrf forwarding Servers
ip address 172.16.1.2 255.255.255.0

upvoted 3 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 2 times

Question #160 *Topic 1*

How does SSO work with HSRP to minimize network disruptions?

A. It enables HSRP to elect another switch in the group as the active HSRP switch.

B. It ensures fast failover in the case of link failure.

C. It enables data forwarding along known routes following a switchover, while the routing protocol reconverges.

D. It enables HSRP to failover to the standby RP on the same device.

Correct Answer: *D*

Community vote distribution

D (78%) B (22%)

MohamedRashed10290 Highly Voted 2 years, 9 months ago

D is correct

upvoted 27 times

TTTTTT 2 years, 3 months ago

SSO HSRP alters the behavior of HSRP when a device with redundant Route Processors (RPs) is configured for stateful switchover (SSO) redundancy mode. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails.

The SSO HSRP feature enables the Cisco IOS HSRP subsystem software to detect that a standby RP is installed and the system is configured in SSO redundancy mode. Further, if the active RP fails, no change occurs to the HSRP group itself and traffic continues to be forwarded through the current active gateway device.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-s/fhp-15-s-book/fhp-hsrp-sso.html

upvoted 10 times

BB234 2 years, 5 months ago

D is the correct answer.

C is referring to NSF Non-Stop Forwarding which can be implemented in addition to SSO

upvoted 3 times

Alondrix Most Recent 2 months, 1 week ago

This question is worded terrible. Is this accurate for D? "on the same device"? Isn't HSRP between two DIFFERENT devices, one active and the other standby? Failover occurs to the standby RP on a DIFFERENT device and then that device becomes active.

upvoted 1 times

habibmangal 7 months, 2 weeks ago

Selected Answer: B

When SSO is enabled on a Cisco router, the active and standby routers exchange state information periodically. In the event of a failure, the standby router assumes the role of the active router and begins forwarding traffic. This process is transparent to the network, and there is no interruption in service.

Specifically, when SSO is enabled with HSRP, the standby router maintains a synchronized copy of the active router's HSRP state information, including the virtual IP address and MAC address. If the active router fails, the standby router can immediately take over as the active HSRP router and continue forwarding traffic using the same virtual IP and MAC addresses.

Therefore, the correct answer is B. It ensures fast failover in the case of link failure.

upvoted 2 times

Burik 5 months, 3 weeks ago

"SSO HSRP alters the behavior of HSRP when a device with redundant Route Processors (RPs) is configured for stateful switchover (SSO) redundancy mode. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails."

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-sy/fhp-15-sy-book/fhp-hsrp-sso.pdf

The answer is D.

upvoted 1 times

Pudu_vlad 1 year, 2 months ago

D is correct

upvoted 1 times

pierresadou 1 year, 7 months ago

Selected Answer: D

D is correct

upvoted 1 times

[Removed] 1 year, 7 months ago

Selected Answer: D

D is correct. C is for Cisco Nonstop Forwarding (NSF) with
Stateful Switchover. Note: Do not use HSRP with Cisco Nonstop Forwarding with Stateful Switchover.

upvoted 2 times

Aldebeer 1 year, 7 months ago

D is the answer

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: D

C is nonsense. D is the right answer.

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: D

It should be D

upvoted 1 times

rettich 1 year, 9 months ago

Selected Answer: D

just wanted to place a vote; See other posts why D is corrcet

upvoted 2 times

Amansoor79 2 years ago

D is the correct answer

upvoted 1 times

Hack4 2 years, 5 months ago

D is the correct answer

upvoted 1 times

bolbolskanes 2 years, 6 months ago

D is correct this is a link about SSO HSRP https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-s/fhp-15-s-book/fhp-hsrp-sso.html

upvoted 1 times

bolbolskanes 2 years, 6 months ago

D is correct Link for more information about SSO HSRP

upvoted 1 times

BigMomma4752 2 years, 8 months ago

The correct answer is D.

upvoted 1 times

Jclemente 2 years, 8 months ago

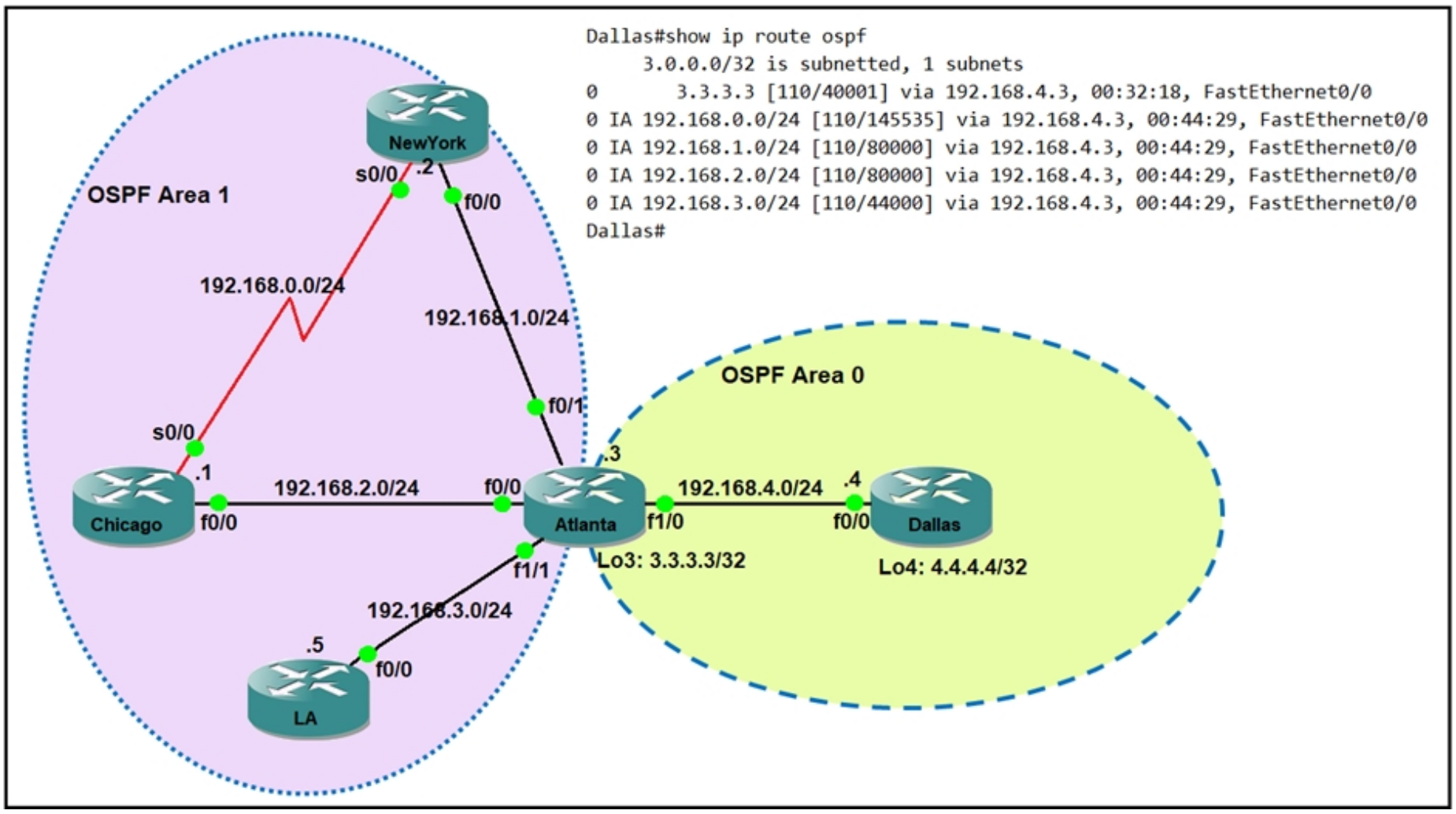
D is the correct answer....

upvoted 1 times

Jclemente 2 years, 8 months ago

D is correct for sure..

upvoted 1 times



Refer to the exhibit. Which command when applied to the Atlanta router reduces type 3 LSA flooding into the backbone area and summarizes the inter-area routes on the Dallas router?

A. Atlanta(config-router)#area 0 range 192.168.0.0 255.255.252.0

B. Atlanta(config-router)#area 1 range 192.168.0.0 255.255.248.0

C. Atlanta(config-router)#area 0 range 192.168.0.0 255.255.248.0

D. Atlanta(config-router)#area 1 range 192.168.0.0 255.255.252.0

Correct Answer: *D*

Community vote distribution

D (100%)

P1Z7C Highly Voted 2 years, 8 months ago

OSPF is link state routing protocol that works on the concept of areas. All areas must have same LSDB (link state database); hence OSPF summarization can only done on the border routers i.e. on ABR (Area border router) and ASBR (Autonomous system boundary router).In this document we discussed about route summarization between the areas.

Background:
Summarization between areas can be done on ABR by using single command under OSPF process:

area [area-id] range [ip-address] [mask] [advertise | not-advertise |cost {cost}]

A) area-id= Identifier of the area about which routes are to be summarized

B) [ip-address] [mask]= Summary route to be advertise in areas

https://community.cisco.com/t5/networking-documents/ospf-inter-area-route-summarization/ta-p/3145113

upvoted 9 times

timtgh Highly Voted 1 year, 6 months ago

B and D would both do the job. But D is more of an exact match for those subnets, while B would allow those four subnets plus an additional four. I assume they're looking for answer D because it matches the subnet list exactly.

upvoted 6 times

cjk3 11 months, 3 weeks ago

B would break Area 0

upvoted 1 times

MerlinTheWizard 10 months ago

i'm not really sure that it would since you'd have a more specific match as a connected route.. but that is specific to this particular topology

upvoted 1 times

danman32 4 months, 1 week ago

It might not break area 0, but the summarization would include the subnet that's in area 0: 192.168.4.0/24 (255.255.248.0 would include 192.168.0-7.0), so at the very least, bad practice.

upvoted 1 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: D

#area 1 range 192.168.0.0 255.255.252.0
it means advertise summary route FROM area 1 TO -> area 0
on the Dallas router, it will look like -> 192.168.0.0/22 (one instead four routes/24)

upvoted 2 times

nushadu 11 months, 1 week ago

+ this command adds summary route to GRT next-hop NULL0:

cisco_R3#show ip route ospf | b Gate
Gateway of last resort is 2.2.2.2 to network 0.0.0.0

55.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O 55.0.0.0/18 is a summary, 00:31:04, Null0 <<<<<<<<<<<<<<<<<<<<
O 55.0.0.0/24 [110/101] via 10.111.10.2, 00:31:04, Ethernet0/0.50
cisco_R3#show runn | s ospf
router ospf 1
router-id 3.3.3.3
auto-cost reference-bandwidth 1000
area 22 range 55.0.0.0 255.255.192.0 <<<<<<<<<<<<<<<<<<<<<<
area 22 filter-list prefix PL_3 in
passive-interface default
no passive-interface Ethernet0/0.10
no passive-interface Ethernet0/0.50
network 0.0.0.0 255.255.255.255 area 0
bfd all-interfaces
cisco_R3#

upvoted 1 times

brightsyds 1 year, 9 months ago

D!

192.168.0.0/24
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24

128
64
32
16
8
4
2
1
=255

192.168.0.0 11000000 10101000 00000-000 00000000
192.168.1.0 11000000 10101000 00000-001 00000000
192.168.2.0 11000000 10101000 00000-010 00000000
192.168.3.0 11000000 10101000 00000-011 00000000

192.168.0.0 11000000 10101000 000000-11 00000000
192.168.0.0/22

upvoted 5 times

brightsyds 1 year, 9 months ago

192.168.0.0/24
192.168.1.0/24
192.168.2.0/24
192.168.3.0/24

128
64
32
16
8
4
2
1
=255

192.168.0.0 11000000 10101000 00000-000 00000000
192.168.1.0 11000000 10101000 00000-001 00000000
192.168.2.0 11000000 10101000 00000-010 00000000
192.168.3.0 11000000 10101000 00000-011 00000000

192.168.0.0 11000000 10101000 000000-11 00000000
192.168.0.0/22

upvoted 1 times

Nhan 2 years, 1 month ago

This is route summarization the given answer is correct

upvoted 2 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

netpeer 2 years, 8 months ago

D is good as it summarizes the best those 4 subnets 192.168.0/1/2/3.X

upvoted 2 times

BigMomma4752 2 years, 8 months ago

The correct answer is D.

upvoted 1 times

Question #162 *Topic 1*

An engineer must configure interface GigabitEthernet0/0 for VRRP group 10. When the router has the highest priority in the group, it must assume the master role.
Which command set must be added to the initial configuration to accomplish this task?

Initial Configuration -
interface GigabitEthernet0/0
description To IDF A 38-24-044.40
ip address 172.16.13.2 255.255.255.0

A. standby 10 ip 172.16.13.254 255.255.255.0 standby 10 preempt

B. vrrp group 10 ip 172.16.13.254 255.255.255.0 vrrp group 10 priority

C. standby 10 ip 172.16.13.254 standy 10 priority 120

D. vrrp 10 ip 172.16.13.254 vrrp 10 preempt

Correct Answer: *D*

Community vote distribution

D (100%)

Pb1805 Highly Voted 2 years, 10 months ago
I think the correct answer is D
upvoted 14 times

diegodavid82 2 years, 1 month ago
Standby command is for HSRP
Standby "group" Word incorrect ----> Standby # ....
upvoted 3 times

diegodavid82 2 years, 1 month ago
For VRRP the commands always star with "VRRP"
upvoted 1 times

Aldebeer Highly Voted 1 year, 7 months ago
Selected Answer: D
Hi, VRRP enables preemption by default. So, i would put instead : vrrp 10 priority ..
upvoted 6 times

timtgh 1 year, 6 months ago
The question doesn't say the router must have highest priority. It just says *when* it does, it must become master. That can only mean it needs the preempt command. Also the priority command in Option B is wrong because it doesn't have a priority number.
upvoted 2 times

uzbin 1 year, 2 months ago
Missing priority is probably a typo.
Preemption is default for VRRP so no need to add it.
upvoted 3 times

Splashisthegreatestmovie Most Recent 5 months, 2 weeks ago
There has got to be something wrong with this question because preempt is enabled by default on VRRP and there's no value listed for the priority which means everything is set to defaults. none of it makes any sense
upvoted 3 times

Burik 5 months, 3 weeks ago
Admins, please, these badly formatted questions needs to be fixed.
upvoted 3 times

nushadu 11 months, 2 weeks ago
Selected Answer: D
tested:
cisco(config-subif)#do s runn interface Ethernet0/0.40
Building configuration...

Current configuration : 155 bytes
!

interface Ethernet0/0.40
description To IDF A 38-24-044.40
encapsulation dot1Q 40
ip address 172.16.13.2 255.255.255.0
vrrp 10 ip 172.16.13.254
end

cisco(config-subif)#do s vrrp
Ethernet0/0.40 - Group 10
State is Master
Virtual IP address is 172.16.13.254
Virtual MAC address is 0000.5e00.010a
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Master Router is 172.16.13.2 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec

cisco(config-subif)#

upvoted 2 times

KOJJY 11 months, 2 weeks ago

Selected Answer: D

correct 100%

upvoted 1 times

Pudu_vlad 1 year, 2 months ago

D is correct

upvoted 1 times

Deu_Inder 1 year, 2 months ago

D is the answer only because the other three answers are totally incorrect. But D is also only half correct.

upvoted 1 times

Jonathan_Perez 1 year, 11 months ago

D.- vrrp 10 ip 172.16.13.254
vrrp 10 preempt

upvoted 2 times

Vianney 1 year, 11 months ago

There is no standby command used for vrrp. D is the correct answer

upvoted 1 times

netpeer 2 years, 8 months ago

D is correct, there is no standby cmd used for vrrp.

upvoted 1 times

noov 2 years, 8 months ago

the correct one is D

upvoted 1 times

BigMomma4752 2 years, 8 months ago

The correct answer is D.

upvoted 1 times

AOA 2 years, 8 months ago

I totally agreed with Ramona88. D is correct because Standby command isn't used in VRRP.

upvoted 2 times

RHK0783 2 years, 9 months ago

A. standby 10 ip 172.16.13.254 255.255.255.0 standby 10 preempt (WRONG - Standby is HSRP syntax)
B. vrrp group 10 ip 172.16.13.254 255.255.255.0 vrrp group 10 priority (WRONG - word "group" is command in VRRP)
C. standby 10 ip 172.16.13.254 standy 10 priority 120 (WRONG - Standby is HSRP syntax)
D. vrrp 10 ip 172.16.13.254 vrrp 10 preempt (Correct)

upvoted 4 times

Kanenas 2 years, 9 months ago

Preemp in vrrp is enabled by default,so the correct answer is D,standby is used in HSRP

upvoted 3 times

netplwiz 2 years, 9 months ago

standby is used for for HSRP:

https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/13780-6.html

D is correct

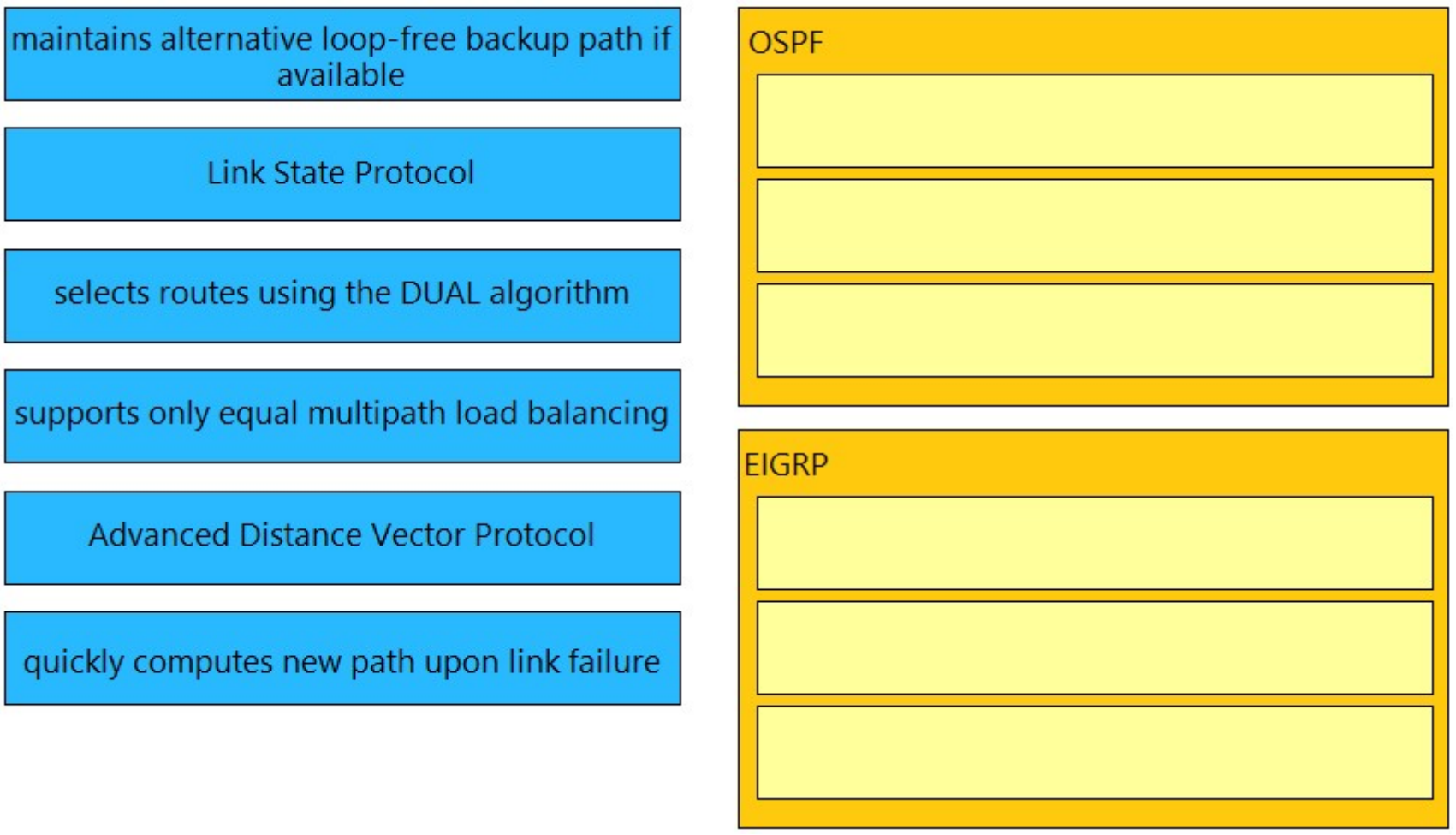
upvoted 3 times

Question #163 *Topic 1*

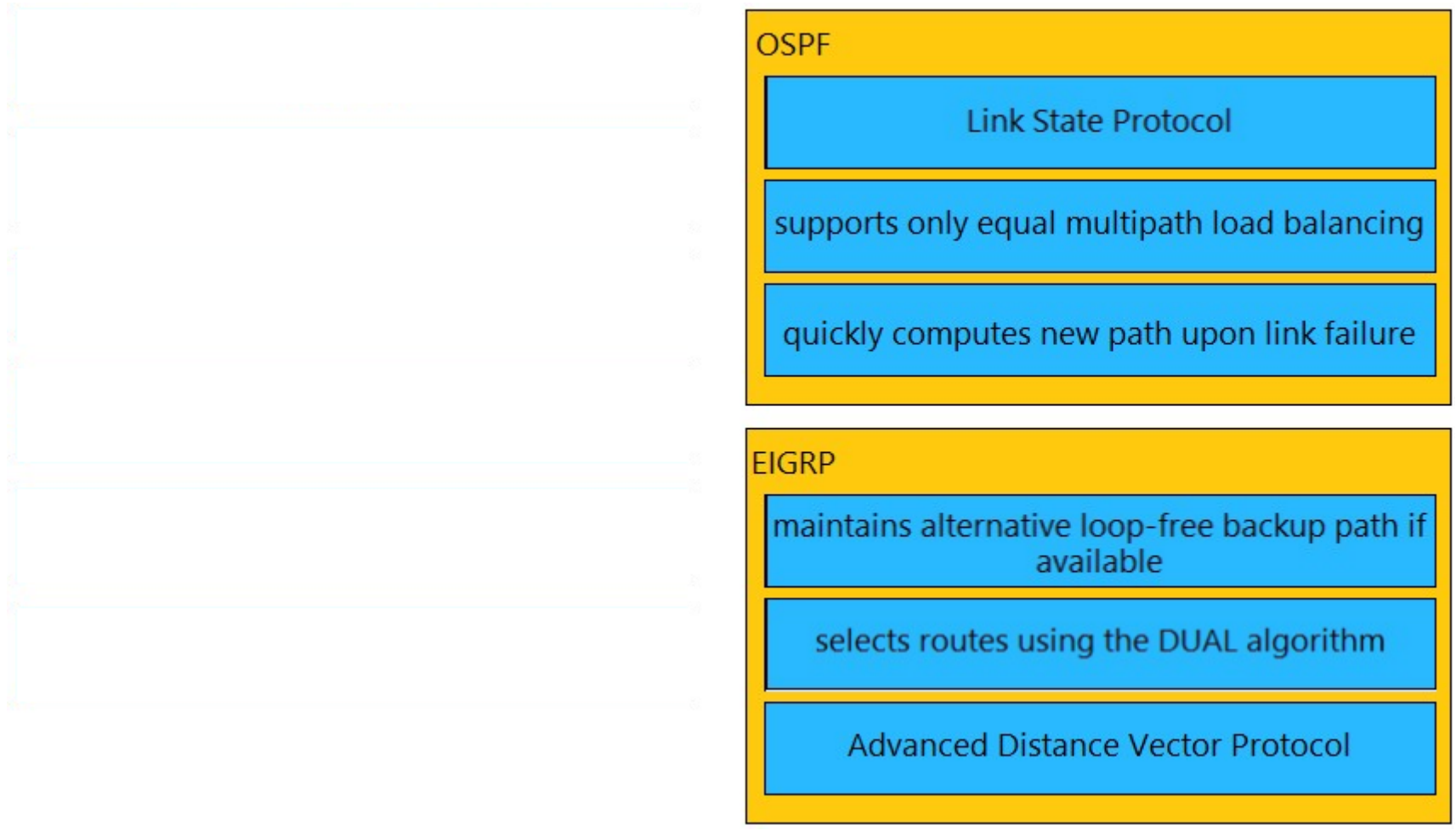
DRAG DROP -

Drag and drop the characteristics from the left onto the routing protocols they describe on the right.

Select and Place:



Correct Answer:



examShark Highly Voted 2 years, 6 months ago

The given answer is correct

upvoted 5 times

CCNPWILL Most Recent 1 month, 1 week ago

given answers are right.

upvoted 1 times

VLAN4461 4 months, 1 week ago

OSPF has a loop-free-alternate feature to maintain a backup path:
https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200225-Configure-Loop-Free-Alternate-path-with.html
EIGRP quickly computes a new route via the feasible successor, whereas OSPF may have to run the Dijkstra algorithm.

upvoted 3 times

```
DSW1#sh spanning-tree
MST1
  Spanning tree enabled protocol mstp
  Root ID    Priority    32769
             Address     0018.7363.4300
             Cost        2
             Port        13 (FastEthernet1/0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     001b.0d8e.e080
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa1/0/7             Desg FWD 2         128.9    P2p Bound (PVST)
Fa1/0/10            Desg FWD 2         128.12   P2p Bound (PVST)
Fa1/0/11            Root FWD 2         128.13   P2p
Fa1/0/12            Altn BLK 2         128.14   P2p
```

```
DSW1#sh spanning-tree mst

##### MST1    vlans mapped:   10,20
Bridge        address 001b.0d8e.e080 priority     32769 (32768 sysid 1)
Root          address 0018.7363.4300 priority     32769 (32768 sysid 1)
              port    Fa1/0/11       cost         2          rem hops 19
!
... output omitted
!
```

Refer to the exhibit. Which two commands ensure that DSW1 becomes the root bridge for VLAN 10 and 20? (Choose two.)

A. spanning-tree mst 1 priority 4096

B. spanning-tree mst 1 root primary

C. spanning-tree mst vlan 10,20 priority root

D. spanning-tree mst 1 priority 1

E. spanning-tree mstp vlan 10,20 root primary

Correct Answer: *AB*

Community vote distribution

AB (89%) 11%

kldoyle97 3 months ago

in Global config
(c)# spanning-tree instanceID# root {primary | secondary}
(c)# spanning-tree instanceID# priority {increment of 4096} default is 32768

Only time "vlan" is used is when you are configuring an instance in mst configuration
making choice E incorrect

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: AB

!
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name region_1
revision 2
instance 1 vlan 1-30
instance 2 vlan 31-110
!
!

sw2(config)#do s spann mst
MST1 vlans mapped: 1-30

Bridge address aabb.cc00.4000 priority 32769 (32768 sysid 1)
Root address aabb.cc00.1000 priority 32769 (32768 sysid 1)
port Po2 cost 2000000 rem hops 19

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 2000000 128.1 Shr Edge
Et0/2 Desg FWD 2000000 128.3 Shr
Et0/3 Altn BLK 2000000 128.4 Shr
Po2 Root FWD 2000000 128.65 Shr
MST2

upvoted 4 times

nushadu 11 months, 2 weeks ago

sw2(config)#spanning-tree mst 1 root ?
primary Configure this switch as primary root for this spanning tree
secondary Configure switch as secondary root

sw2(config)#spanning-tree mst 1 root primary

MST1 vlans mapped: 1-30
Bridge address aabb.cc00.4000 priority 24577 (24576 sysid 1)
Root this switch for MST1

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 2000000 128.1 Shr Edge
Et0/2 Desg FWD 2000000 128.3 Shr
Et0/3 Desg FWD 2000000 128.4 Shr
Po2 Desg FWD 2000000 128.65 Shr

MST2

upvoted 2 times

nushadu 11 months, 2 weeks ago

sw2(config)#spanning-tree mst 1 priority 4096
sw2(config)#do s spann mst
MST1 vlans mapped: 1-30
Bridge address aabb.cc00.4000 priority 4097 (4096 sysid 1)
Root this switch for MST1

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 2000000 128.1 Shr Edge
Et0/2 Desg FWD 2000000 128.3 Shr
Et0/3 Desg FWD 2000000 128.4 Shr
Po2 Desg FWD 2000000 128.65 Shr

MST2

upvoted 2 times

KOJJY 11 months, 2 weeks ago

Selected Answer: AB

correct 100%

upvoted 2 times

forccnp 1 year ago

Selected Answer: DE

why not D and E?

upvoted 1 times

RinorAvdyli 12 months ago

Option D can't be because the priority should be increments of 4096 even though 0 can still apply, but not 1.
Option E can't be correct, because with MST the idea is to configure instances of VLANs, not VLANs individually and the command mstp doesn't seem to be a correct IOS command at all.

upvoted 4 times

gcata 1 year, 3 months ago

Selected Answer: AB

The 2 ways to manipulate the configuration of the root bridge is by using the
“spanning-tree mst instance-id priority value” command manually or the
“spanning-tree mst instance-id root (primary | secondary)” command.
If using the priority command you must set the ID in multiples of 4096.

upvoted 2 times

youtri 2 years ago

always we have to put a number after mst
priority should be increment of 4096

upvoted 2 times

youtri 2 years ago

always we have to put a number after mst , priority should be incrent 4096

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 4 times

cracanici 2 years, 2 months ago

A E ? maybe

upvoted 1 times

cracanici 2 years, 2 months ago

No, not E

upvoted 2 times

Babushka 2 years, 2 months ago

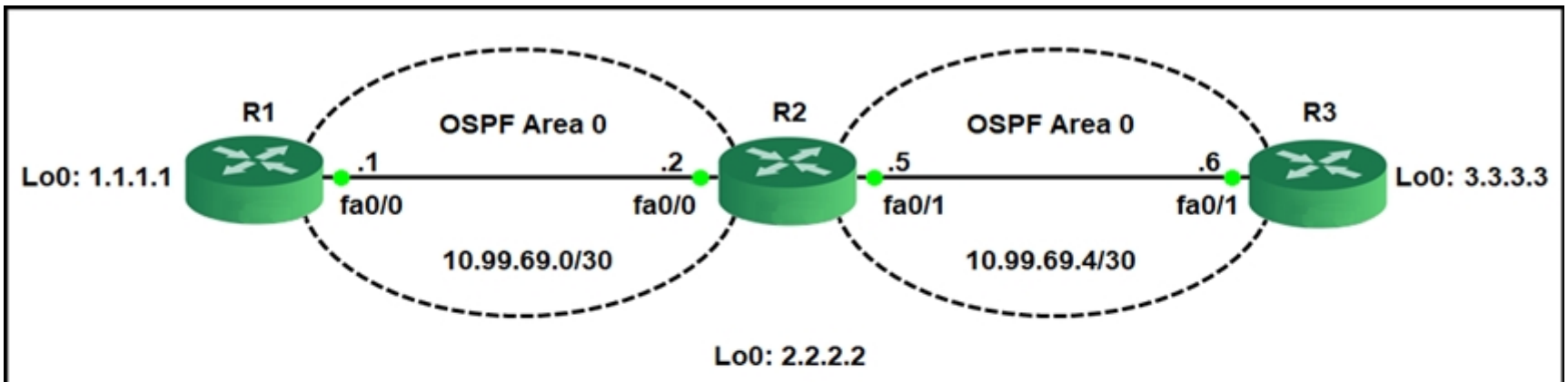
mstp? Definitely not E.

upvoted 3 times

examShark 2 years, 6 months ago

Given answer is corect

upvoted 2 times




```
R1#ping
Protocol [ip]:
Target IP address: 3.3.3.3
Repeat count [5]: 3
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]: yes
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
Packet sent with the DF bit set
Packet has IP options: Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)


Unreachable from 10.99.69.2, maximum MTU 1492. Received packet has options
 Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)

 [output omitted]
```

Refer to the exhibit. R1 is able to ping the R3 fa0/1 interface. Why do the extended pings fail?

A. The maximum packet size accepted by the command is 1476 bytes.

B. The DF bit has been set.

C. R3 is missing a return route to 10.99.69.0/30.

D. R2 and R3 do not have an OSPF adjacency.

Correct Answer: *B*

youtri Highly Voted 1 year, 7 months ago

DF=1 dont fragment
DF=0 fragment

upvoted 7 times

Caradum Most Recent 1 year ago

B ist correct.

R1 sends the ping with a packet size of 1500 and the DF bit set (=R1 is not allowed to fragment the ping). R2 only accepts packets with the size of 1492. Therefor the ping gets discarded from R2.

To solve this, dont set the DF bit or lower the packet size.

upvoted 3 times

brightsyds 1 year, 9 months ago

B!

Because the do-not-fragment (DF) bit was set, the packet would be discarded

upvoted 2 times

SandyIndia 2 years, 2 months ago

Don't Fragment (DF) Bit is set.

upvoted 4 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 2 times

Question #166 *Topic 1*

```
!
interface FastEthernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
!
interface FastEthernet0/2
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
access-list 10 permit 10.10.10.0 0.0.0.255
!
```

Refer to the exhibit. Which command allows hosts that are connected to FastEthernet0/2 to access the Internet?

A. ip nat inside source list 10 interface FastEthernet0/2 overload

B. ip nat inside source list 10 interface FastEthernet0/1 overload

C. ip nat outside source static 209.165.200.225 10.10.10.0 overload

D. ip nat outside source list 10 interface FastEthernet0/2 overload

Correct Answer: *B*

Community vote distribution

B (100%)

[Removed] 5 months ago

Selected Answer: B

correct

upvoted 1 times

brightsyds 1 year, 9 months ago

B for sure!

upvoted 3 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 4 times

```
R1
interface GigabitEthernet0/0
ip address 192.168.250.2 255.255.255.0
standby 20 ip 192.168.250.1
standby 20 priority 120

R2
interface GigabitEthernet0/0
ip address 192.168.250.3 255.255.255.0
standby 20 ip 192.168.250.1
standby 20 priority 110
```

Refer to the exhibit. What are two effects of this configuration? (Choose two.)

A. If R1 goes down, R2 becomes active but reverts to standby when R1 comes back online.

B. If R2 goes down, R1 becomes active but reverts to standby when R2 comes back online.

C. R1 becomes the active router.

D. R1 becomes the standby router.

E. If R1 goes down, R2 becomes active and remains the active device when R1 comes back online.

Correct Answer: *CE*

Community vote distribution

CE (90%) 10%

samk87 Highly Voted 2 years, 8 months ago

its C & E. Please refer to the link below
https://community.cisco.com/t5/switching/understanding-standby-preempt/td-p/1870591

upvoted 16 times

diegodavid82 2 years, 1 month ago

E is correct because HSRP is Non-Preempt by default.

upvoted 4 times

mgiuseppe86 Most Recent 2 months, 3 weeks ago

C is only the active router if it was booted first, or configured first. D can also be correct if R2 was booted or configured before R1. It's a dumb question, probably not correct, but I wouldnt put it past Cisco to ask us these asinine questions. We have to assume R1 was booted and configured first. BeCaUsE 1 CoMeS BeFoRe 2...

However, none of the other answers (A,B) are correct because regardless there is no preempt command. So the router to stay online will retain as Active. The routers will not revert to standby unless the active router goes down or the pre-empt command is put on the standby router.

I am going with C, because of logic, and E because that is actually the only other true answer.

upvoted 1 times

Pilgrim5 7 months, 3 weeks ago

Selected Answer: CE

R1 becomes the active router because the router with highest priority becomes the active router. This makes C correct,

There is no Standby preempt statement on R1 so if it goes down, R2 takes over and R1 never becomes active even if it comes up again till R2 goes down.

upvoted 2 times

Leoveil 8 months ago

Selected Answer: CE

C because R1 will be in active state (priority 120) after applying the configurations and while R1 is still up . however, E is the effect of the configurations after R1 goes down R2 will be active and remain active due to no preempt con both routers.

upvoted 1 times

RShrestha 9 months ago

Agree with answer E but so not agree with C how can R1 be active if it went down and recovered but there is no preepmt command to make it active again. So in my opinion only E

upvoted 1 times

markymark874 11 months ago

Selected Answer: CE

No preempt vommand configured

upvoted 1 times

bora4motion 1 year ago

Selected Answer: CE

C + E is correct

upvoted 1 times

forccnp 1 year ago

C and E are correct

upvoted 1 times

H3kerman 1 year, 1 month ago

Selected Answer: CE

router with higher priority will become active, without preempt r1 will not become active after come online. preempt is not a default command with hsrp

upvoted 1 times

carlovalle 1 year, 2 months ago

Selected Answer: CE

Preempt is not enabled

upvoted 1 times

siteoforigin 1 year, 2 months ago

Selected Answer: CE

Preempt is not enabled, if R1 goes down it will not become active again.

upvoted 1 times

greencafe24 1 year, 2 months ago

Selected Answer: CE

Correct answers: CE
Preempt is not configured on R1 hence R2 will remain as the active Router.

upvoted 1 times

jaz600 1 year, 3 months ago

Selected Answer: AC

Preempt is not configured on R1 hence R2 will remain as the active Router.
https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/13780-6.html

upvoted 1 times

nopenotme123 1 year, 3 months ago

Exactly... Since preempt isnt enabled R1 will not resume active router once it comes back online.. CE

upvoted 2 times

brightsyds 1 year, 9 months ago

CE for sure!

Because the preempt keyword is not used, R1 will not become Active if it goes down and comes back online

upvoted 3 times

rettich 1 year, 9 months ago

to be honest you can't tell if C or D is correct with the given information. The Router that comes up fist will be the active. Keep that in mind if the answers or question varies slightly!
A and B are incorrect and E is correct.
But if i had to choose two answers to this question i would pick C & E although i dont totally agree

upvoted 2 times

Nhan 2 years, 2 months ago

The given answer is correct, the reason that R2 is still active even r1 comeback on line is the preempt command wasn't set

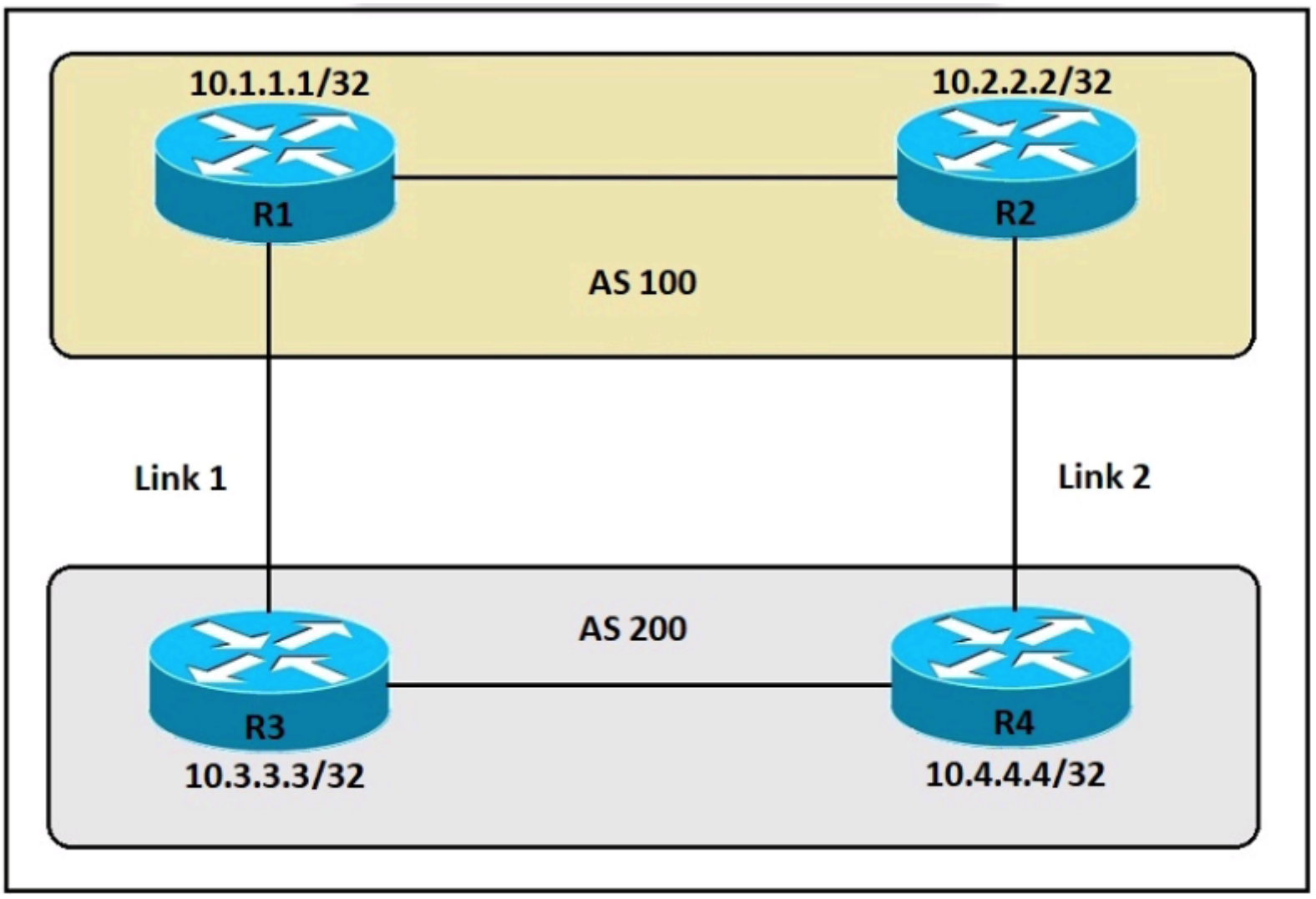
upvoted 1 times

Hack4 2 years, 5 months ago

C & E are the right answer..

upvoted 1 times

Question #168 *Topic 1*



Refer to the exhibit. An engineer must ensure that all traffic entering AS 200 from AS 100 chooses Link 2 as an entry point. Assume that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers. Which configuration accomplishes this task?

A. R3(config)#route-map PREPEND permit 10 R3(config-route-map)#set as-path prepend 200 200 200 R3(config)#router bgp 200 R3#(config-router)#neighbor 10.1.1.1 route-map PREPEND out

B. R4(config)#route-map PREPEND permit 10 R4(config-route-map)#set as-path prepend 100 100 100 R4(config)#router bgp 200 R4(config-router)#neighbor 10.2.2.2 route-map PREPEND in

C. R4(config)#route-map PREPEND permit 10 R4(config-route-map)#set as-path prepend 200 200 200 R4(config)#router bgp 200 R4(config-router)#neighbor 10.2.2.2 route-map PREPEND out

D. R3(config)#route-map PREPEND permit 10 R3(config-route-map)#set as-path prepend 100 100 100 R3(config)#router bgp 200 R3(config-router)#neighbor 10.1.1.1 route-map PREPEND in

Correct Answer: *A*

Community vote distribution

A (100%)

xziomal9 Highly Voted 2 years, 2 months ago

A.
R3(config)#route-map PREPEND permit 10
R3(config-route-map)#set as-path prepend 200 200 200
R3(config)#router bgp 200
R3#(config-router)#neighbor 10.1.1.1 route-map PREPEND out
B.
R4(config)#route-map PREPEND permit 10
R4(config-route-map)#set as-path prepend 100 100 100
R4(config)#router bgp 200
R4(config-router)#neighbor 10.2.2.2 route-map PREPEND in
C.
R4(config)#route-map PREPEND permit 10
R4(config-route-map)#set as-path prepend 200 200 200
R4(config)#router bgp 200
R4(config-router)#neighbor 10.2.2.2 route-map PREPEND out
D.
R3(config)#route-map PREPEND permit 10
R3(config-route-map)#set as-path prepend 100 100 100
R3(config)#router bgp 200
R3(config-router)#neighbor 10.1.1.1 route-map PREPEND in

upvoted 26 times

XalaGyan 1 year, 11 months ago

thx a lot bro for taking the time and writing this down. your answer is correct.

upvoted 3 times

brightsyds Highly Voted 1 year, 9 months ago

A for sure!

R3 prepends its AS and sends it outbound to R1 in AS 100. Because R1 and R2 are in one iBGP domain (AS 100), all traffic from AS 100 will prefer to use a shorter AS path to AS 200 which is R4's link.

upvoted 10 times

timtgh 1 year, 6 months ago

Thanks. But why is it prepending it three times?

upvoted 3 times

bora4motion 1 year ago

That's what you do when you want to "make a route look bad" you add your own AS to the AS-Path and make it longer. BGP is routing through AS numbers.

upvoted 7 times

alawi2 1 year, 6 months ago

to make longer, imagine 200 + 200 + 200
it is basically telling BGP the equivalent of having to cross 3 AS with cost 200 each

upvoted 9 times

jason2626 1 year, 4 months ago

Makes sense! Thanks for the explanation.

upvoted 3 times

danman32 Most Recent 4 months, 1 week ago

I got this one wrong and selected D because I remembered similar Q139 and misread this question that we want AS100 to choose link 2, and not AS 200 choose link 2.
But now that I read these discussions, realized I had the traffic direction backwards, in which case answer is definitely A.

upvoted 1 times

charafDZ 9 months, 1 week ago

What is AS path Prepending?
In the Border Gateway Protocol (BGP), prepending is a technique used to deprioritize a route by artificially increasing the length of the AS-PATH attribute by repeating an autonomous system number (ASN). Route selection in BGP prefers the shorter AS path length, assuming all other criteria are equal

upvoted 1 times

Dataset 9 months, 2 weeks ago

hi!
why is the route map PREPEND applied on R3 , out ?
Thanks
Regards

upvoted 1 times

danman32 4 months, 1 week ago

Because you want to influence AS100's traffic pattern to AS200, unlike Q139 which had you influence traffic from AS200 to AS100.
Therefore you want link1 to appear to AS200 as the longer route.

upvoted 2 times

bora4motion 1 year ago

Selected Answer: A

A is the correct option, you add your own AS in the AS Path to make it "look bad".

upvoted 1 times

WINDSON 1 year ago

what is the meaning of permit 10 ?

upvoted 1 times

Pudu_vlad 1 year, 2 months ago

A is correct

upvoted 1 times

Raju255 1 year, 8 months ago

Correct Answer is A
A.
R3(config)#route-map PREPEND permit 10
R3(config-route-map)#set as-path prepend 200 200 200
R3(config)#router bgp 200
R3#(config-router)#neighbor 10.1.1.1 route-map PREPEND out
B.

R4(config)#route-map PREPEND permit 10
R4(config-route-map)#set as-path prepend 100 100 100
R4(config)#router bgp 200
R4(config-router)#neighbor 10.2.2.2 route-map PREPEND in
C.
R4(config)#route-map PREPEND permit 10
R4(config-route-map)#set as-path prepend 200 200 200
R4(config)#router bgp 200
R4(config-router)#neighbor 10.2.2.2 route-map PREPEND out
D.
R3(config)#route-map PREPEND permit 10
R3(config-route-map)#set as-path prepend 100 100 100
R3(config)#router bgp 200
R3(config-router)#neighbor 10.1.1.1 route-map PREPEND in

upvoted 3 times

hprc2002 1 year, 10 months ago

XZIOMAL9, thank you for the formatting; the original presentation of the potential answers is abysmal!

upvoted 1 times

heaven2021 2 years, 1 month ago

>>xziomal9
thank you very much!!

upvoted 2 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 2 times

Question #169 *Topic 1*

Which DHCP option provides the CAPWAP APs with the address of the wireless controller(s)?

A. 43

B. 66

C. 69

D. 150

Correct Answer: *A*

Community vote distribution

A (100%)

pierresadou 1 year, 7 months ago

Selected Answer: A

A is correct

upvoted 2 times

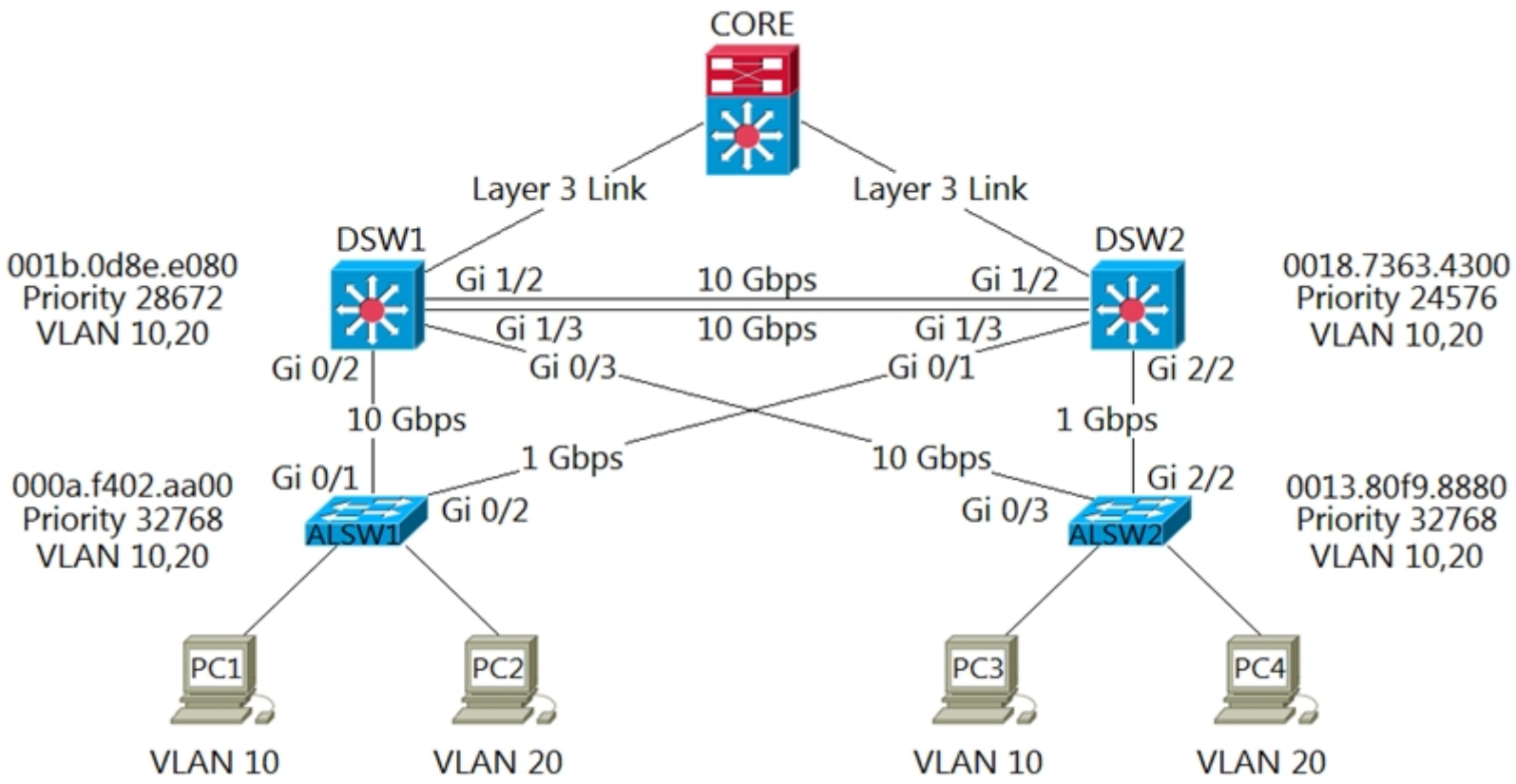
examShark 2 years, 6 months ago

Given answer is correct

upvoted 1 times

Question #170 *Topic 1*

Refer to the exhibit.



Which two commands ensure that DSW1 becomes root bridge for VLAN 10? (Choose two.)

A. DSW1(config)#spanning-tree vlan 10 priority 4096

B. DSW1(config)#spanning-tree vlan 10 priority root

C. DSW2(config)#spanning-tree vlan 10 priority 61440

D. DSW1(config)#spanning-tree vlan 10 port-priority 0

E. DSW2(config)#spanning-tree vlan 20 priority 0

Correct Answer: *AB*

Community vote distribution

AC (100%)

J2DFW Highly Voted 2 years, 7 months ago

The answers should be
DSW1(config)#spanning-tree vlan 10 priority 4096 < -- This is listed
DSW1(config)#spanning-tree vlan 10 priority root < -- this is not valid
DSW1(config)#spanning-tree vlan 10 root primary < -- This is not listed, but should be the correct command

upvoted 19 times

ciscogear 1 year, 10 months ago

In that case B is incorrect. You must select best answers, not best config.

upvoted 1 times

Furiel Highly Voted 2 years, 6 months ago

A and C

upvoted 17 times

raizer 2 years, 2 months ago

Yes. A&C
61440 is a valid (and "low/bad") priority

SW1(config)#spanning-tree vlan 10 priority 32767
% Bridge Priority must be in increments of 4096.
% Allowed values are:
0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440

Option B is not correct. it is just simmilar to:
spanning-tree vlan 10 root primary

upvoted 10 times

Hugh_Jazz 2 years, 1 month ago

Concur, A & C

upvoted 3 times

MaxwellJK Most Recent 4 months, 1 week ago

Selected Answer: AC

B is no correct.

DSW1(config)#spanning-tree vlan 10 priority ?
<0-61440> bridge priority in increments of 4096

DSW1(config)#spanning-tree vlan 10 priority root
^
% Invalid input detected at '^' marker.

upvoted 1 times

techriese 4 months, 4 weeks ago

Selected Answer: AC

A & C is correct

upvoted 1 times

floodhound 6 months, 3 weeks ago

Selected Answer: AC

B is an invalid command only A & C are valid here

upvoted 1 times

Cesar12345 7 months ago

Selected Answer: AC

Switch(config)#spanning-tree vlan 10 priority ?
<0-61440> bridge priority in increments of 4096
0 Is the lowest possible so the best available priority for the STP root bridge election.

upvoted 1 times

rami_mma 8 months, 1 week ago

Sorry A and B is correct

upvoted 1 times

rami_mma 8 months, 1 week ago

A and D is correct.

upvoted 2 times

Chiaretta 9 months, 1 week ago

Selected Answer: AC

Concur, A & C

upvoted 1 times

FelipePadilha 10 months ago

Selected Answer: AC

A and C are the correct answers.

For B to be valid, the command should be: spanning-tree vlan 10 root primary

upvoted 1 times

Ayman_B 11 months ago

Selected Answer: AC

choosing A and C give two values to vlan 10 in DSW1(4096) and DSW2(61440) The root bridge is chosen based on the lowest bridge priority value, with the switch having the lowest priority becoming the root bridge and in this case DSW1 (496)

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: AC

sw1(config)#do s spann vla 10

VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 24586
Address aabb.cc00.4000
Cost 100
Port 4 (Ethernet0/3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address aabb.cc00.1000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 100 128.1 Shr
Et0/2 Desg FWD 100 128.3 Shr

Et0/3 Root FWD 100 128.4 Shr

sw1(config)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw2(config)#spanning-tree vlan 10 priority 4096
sw2(config)#do s spann vla 10

VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 4106
Address aabb.cc00.4000
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4106 (priority 4096 sys-id-ext 10)
Address aabb.cc00.4000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/3 Desg FWD 100 128.4 Shr
Po2 Desg FWD 100 128.65 Shr

sw2(config)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw1(config)#spanning-tree vlan 10 priority 61440
sw1(config)#do s spann vla 10

VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 4106
Address aabb.cc00.4000
Cost 100
Port 4 (Ethernet0/3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 61450 (priority 61440 sys-id-ext 10)
Address aabb.cc00.1000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 100 128.1 Shr
Et0/2 Desg FWD 100 128.3 Shr
Et0/3 Root FWD 100 128.4 Shr

sw1(config)#

upvoted 1 times

bora4motion 1 year ago

Selected Answer: AC

A + C is correct.

upvoted 1 times

forccnp 1 year ago

Selected Answer: AC

A and C

upvoted 1 times

GeorgeFortiGate 1 year ago

Selected Answer: AC

Either we should modify DSW1 to be have better priority or DSW2 to have worse priority ;)

upvoted 1 times

HBL_203 1 year, 2 months ago

A & C
B is not correct, the command "B. DSW1(config)#spanning-tree vlan 10 priority root
" is not correct.
the correct onr is "#spanning-tree vla 1 root primary"

upvoted 3 times

cnasidney 1 year, 4 months ago

A and C
4096 best that 28672
SW1 increment 0 4096 8192 12288 ...

And the output of Sw1 28672, best that 61440
SW2 write spanning-tree vlan 10 priority 61440, high priority of on vlan 10

upvoted 1 times

Question #171 *Topic 1*

What mechanism does PIM use to forward multicast traffic?

A. PIM sparse mode uses a pull model to deliver multicast traffic.

B. PIM dense mode uses a pull model to deliver multicast traffic.

C. PIM sparse mode uses receivers to register with the RP.

D. PIM sparse mode uses a flood and prune model to deliver multicast traffic.

Correct Answer: *A*

Community vote distribution

A (100%)

ABC123 Highly Voted 2 years, 7 months ago

It seems C is trick question because Receivers use join messages or membership reports, while Register messages are for Sources...

upvoted 11 times

Hamzaaa 2 years, 7 months ago

true, so A is correct answer

upvoted 5 times

mrlyfi Most Recent 3 months, 2 weeks ago

Selected Answer: A

Provided answer is correct!

upvoted 1 times

ihateciscoreally 4 months, 2 weeks ago

of course this wasnt mentioned in the OCG :D no single word "push" or "pull" through 30 pages.

however solution is:
PIM sparse mode: this is a “pull” model where we only forward multicast traffic when requested.

PIM dense mode: this is a “push” model where we flood multicast traffic everywhere and then prune it when it’s not needed.

upvoted 2 times

GreatDane 1 year, 5 months ago

Ref: IP Multicast: PIM Configuration Guide - IP Multicast Technology Overview [Cisco IOS XE 16] – Cisco

“...
Protocol Independent Multicast
...
PIM Dense Mode

PIM dense mode (PIM-DM) uses a push model to flood multicast traffic to every corner of the network.
...
PIM Sparse Mode

PIM sparse mode (PIM-SM) uses a pull model to deliver multicast traffic.
...”

A. PIM sparse mode uses a pull model to deliver multicast traffic.

Correct answer.

B. PIM dense mode uses a pull model to deliver multicast traffic.

Wrong answer.

C. PIM sparse mode uses receivers to register with the RP.

Wrong answer.

D. PIM sparse mode uses a flood and prune model to deliver multicast traffic.

Wrong answer.

upvoted 2 times

Nhan 2 years, 1 month ago

The given answer is correct
https://networklessons.com/cisco/ccie-routing-switching-written/multicast-pim-sparse-dense-mode

upvoted 2 times

BB234 2 years, 5 months ago

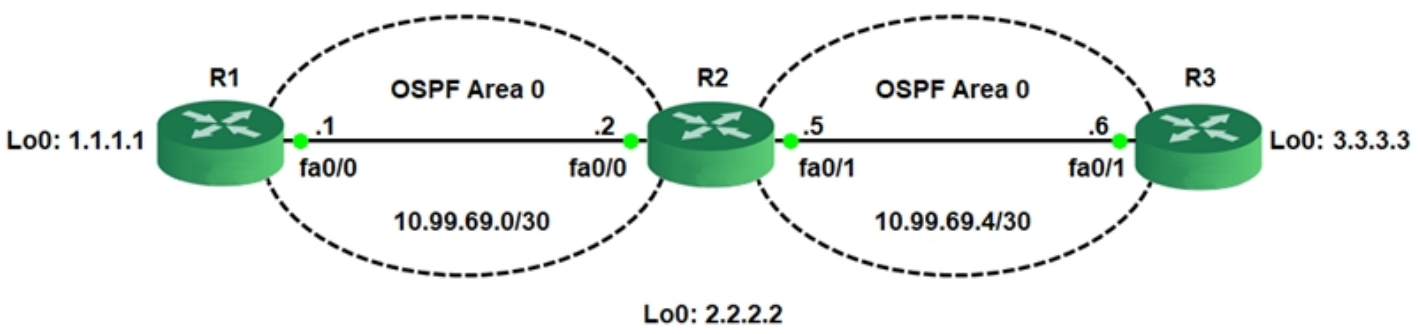
"PIM sparse mode (PIM-SM) uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data will receive the traffic."

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16-5/imc-pim-xe-16-5-book/imc-tech-oview.html

upvoted 4 times

Question #172 *Topic 1*

Refer to the exhibit.




```
R1#traceroute
Protocol [ip]:
Target IP address: 3.3.3.3
Source address: 1.1.1.1
Numeric display [n]:
Timeout in seconds: [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Tine to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose [none]: Record
Number of hops [9]:
Loose, Strict, Record, Timestamp, Verbose [RV]:
Type escape sequence to abort.

Continued --->
```

```
Tracing the route to 3.3.3.3

  1 10.99.69.2 36 msec
Received packet has options
Total option bytes = 40, padded length = 40
  Record route:
    (10.99.69.1) <*>
    (0.0.0.0)
    (0.0.0.0)
   End of list

----output omitted--

  2 10.99.69.6 !A
Received packet has options
Total option bytes = 40, padded length = 40
  Record route:
    (10.99.69.1)
    (10.99.69.5) <*>
    (0.0.0.0)
    (0.0.0.0)
  End of list
  !A
----output omitted---
```

The traceroute fails from R1 to R3.

What is the cause of the failure?

A. An ACL applied inbound on loopback0 of R2 is dropping the traffic.

B. The loopback on R3 is in a shutdown state.

C. Redistribution of connected routes into OSPF is not configured.

D. An ACL applied inbound on fa0/1 of R3 is dropping the traffic.

Correct Answer: *D*

Community vote distribution

D (100%)

RhJ72 Highly Voted 2 years, 3 months ago

D is correct, but for this reason. Note the !A in the output. This means that the response was administratively prohibited by an ACL. This limits the answer to either A or D. Given we see the !A at fa0/1 of R3, the D is the answer.

upvoted 25 times

nopenotme123 Highly Voted 1 year, 3 months ago

Selected Answer: D

Its clearly D and !A gives it away. The ! indicates that .6 did reply and the A means it was administratively prohibited.. Hence ACL...
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html

upvoted 8 times

[Removed] Most Recent 5 months ago

D is correct

upvoted 1 times

Dataset 7 months, 2 weeks ago

Selected Answer: D

!A ...
means rejected by an ACL
Regards

upvoted 1 times

rami_mma 8 months, 1 week ago

D is corrent

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

Put the ACL to the loopback interface will not work
The loopback interface is a control-plane interface so because is a logical interface the ACL will not block the traffic.

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

R3#show access-lists
Standard IP access list 1
10 deny 1.1.1.1
20 permit any
R3#

R3#show running-config interface lo0
Building configuration...

Current configuration : 85 bytes
!
interface Loopback0
ip address 3.3.3.3 255.255.255.255
ip access-group 1 in
end

R1#ping 3.3.3.3 source 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
R1#

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

The only way in this scenario is to apply the ACL in the physical interface facing R2 to the R3 router:

R3#show running-config interface ethernet 0/1
Building configuration...

Current configuration : 103 bytes
!
interface Ethernet0/1
ip address 10.99.69.6 255.255.255.252
ip access-group 1 in
duplex auto
end

R1#traceroute
Protocol [ip]: ip
Target IP address: 3.3.3.3
Ingress traceroute [n]: n
Source address: 1.1.1.1
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 3.3.3.3
VRF info: (vrf in name/id, vrf out name/id)
1 10.99.69.2 1 msec 1 msec 0 msec
2 10.99.69.6 !A !A *

As you can see the traffic is now blocked

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

What you can do instead is doing some policing to the control plane instead? Why? Because the loopback interface is a logical interface so is an interface controlled by the Control Plane (The control plane is generally considered to be where a router or switch makes its decisions. This is software based, and uses the CPU rather than specialised hardware, such as an ASIC).

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

Here the config:

class-map match-all DENY-TRAFFIC-TO-LOOPBACK
match access-group 1

policy-map DENY-TRAFFIC-TO-LOOPBACK
class DENY-TRAFFIC-TO-LOOPBACK
police 8000 conform-action transmit exceed-action drop

control-plane
service-policy input DENY-TRAFFIC-TO-LOOPBACK

In this case in the ACL we don't use the deny statement but the permit statement because we permit to the traffic sourced by the host 1.1.1.1 to be policed.

R3#show access-lists 1
Standard IP access list 1
10 permit 1.1.1.1 (5234 matches)
20 permit any (77 matches)

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

R3#show policy-map control-plane
Control Plane

Service-policy input: DENY-TRAFFIC-TO-LOOPBACK

Class-map: DENY-TRAFFIC-TO-LOOPBACK (match-all)
5942 packets, 675000 bytes
5 minute offered rate 6000 bps, drop rate 0000 bps
Match: access-group 1
police:
cir 8000 bps, bc 1500 bytes
conformed 5523 packets, 627294 bytes; actions:
transmit
exceeded 419 packets, 47706 bytes; actions:
drop
conformed 6000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
57669 packets, 6579474 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any

The QoS done to the Control Plane is doing his job...

SO THE ANSWER IS????? OF COURSE IS THE D ONE!

upvoted 2 times

John13121 11 months ago

D - is the answer take a look at the end "!A" which means filtered by an Access List - Administratively prohibited !

upvoted 4 times

GreatDane 1 year, 5 months ago

Ref: what !A in traceroute output - Cisco Community

Post by glen.grant

"...
Administratively unreachable. Usually, this output indicates that an access list is blocking traffic."

A. An ACL applied inbound on loopback0 of R2 is dropping the traffic.

Wrong answer.

B. The loopback on R3 is in a shutdown state.

Wrong answer.

C. Redistribution of connected routes into OSPF is not configured.

Wrong answer.

D. An ACL applied inbound on fa0/1 of R3 is dropping the traffic.

Correct answer.

upvoted 2 times

AltimusOn 1 year, 8 months ago

"D" is the correct answer.

upvoted 1 times

kierownikk0 2 years, 1 month ago

A is the correct answer and there is why:
B - if loopback on R3 would be in shutdown state then 3.3.3.3 would not be in the routing table of R1. OSPF does not propagate networks configured on shutdown interfaces. In the result there would not be any hops in the output.
C - from perspective of R3, network configured on loopback interface is in "Connected" state, so if redistribution of connected routes would not be configured then 3.3.3.3 would not be propagated to R1. The result would be the same as in B
D - if ACL would drop inbound traffic of Fa0/1 then in the output would not be adress 10.99.69.6 (second hop). Remember, if router decrement TTL to 0 then it have to send respond to the source of the packet. In the header of the response is an IP address of the router which hit TTL = 0.
Sorry for any mistakes, English is not my native language :/

upvoted 2 times

kierownikk0 2 years, 1 month ago

My bad, answer A is about R2 not R3... In this case I think there is no correct answer.

upvoted 1 times

examShark 2 years, 6 months ago

Given answer is correct.
(Traceroute would not leave R1 if 3.3.3.3 was not in R1's routing table)

upvoted 4 times

amgue 2 years, 6 months ago

I would say that the loopback int in R3 is in a shutdown state (answer B), because if answer D is true as supposed (All traffic entering fa0/1 in R3 is droped) than we should not see the ip 10.99.69.6 in our traceroute result

upvoted 1 times

AliMo123 2 years, 6 months ago

D is correct. The reason we see 10.99.69.6 in the output is that we ping the Lo 3.3.3.3 of R3 with his add, so off course we will see the connected add of the Lo 3.3.3.3

upvoted 3 times

AliMo123 2 years, 6 months ago

look at the output: record route 10.99.69.1 to 10.99.69.5 which is the add of fa0/1 of router, so the Lo is up.

upvoted 2 times

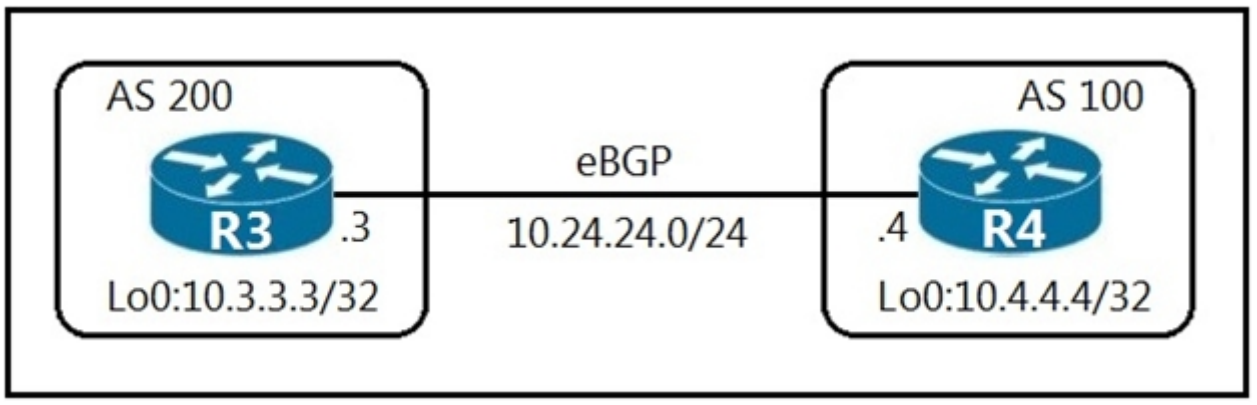
baid 1 year, 9 months ago

yes, you are right.

upvoted 1 times

Question #173 *Topic 1*

Refer to the exhibit.



An engineer must establish eBGP peering between router R3 and router R4. Both routers should use their loopback interfaces as the BGP router ID.
Which configuration set accomplishes this task?

A. R3(config)#router bgp 200 R3(config-router)#neighbor 10.4.4.4 remote-as 100 R3(config-router)# neighbor 10.4.4.4 update-source Loopback0 R4(config)#router bgp 100 R4(config-router)#neighbor 10.3.3.3 remote-as 200 R4(config-router)#network 10.3.3.3 update-source Loopback0

B. R3(config)#router bgp 200 R3(config-router)#neighbor 10.24.24.4 remote-as 100 R3(config-router)#neighbor 10.24.24.4 update-source Loopback0 R4(config)#router bgp 100 R4(config-router)#neighbor 10.24.24.3 remote-as 200 R4(config-router)#neighbor 10.24.24.3 update-source Loopback0

C. R3(config)#router bgp 200 R3(config-router)#neighbor 10.4.4.4 remote-as 100 R3(config-router)#bgp router-id 10.3.3.3 R4(config)#router bgp 100 R4(config-router)#neighbor 10.3.3.3 remote-as 200 R4(config-router)#bgp router-id 10.4.4.4

D. R3(config)#router bgp 200 R3(config-router)#neighbor 10.24.24.4 remote-as 100 R3(config-router)#bgp router-id 10.3.3.3 R4(config)#router bgp 100 R4(config-router)#neighbor 10.24.24.3 remote-as 200 R4(config-router)#bgp router-id 10.4.4.4

Correct Answer: *A*

Community vote distribution

D (100%)

LimRS Highly Voted 2 years, 8 months ago
Answer is D, verified with GNS3.
Answer A won't establish BGP link.
upvoted 42 times

XalaGyan 1 year, 11 months ago
you are totally correct. BGP would not know how to connect to the peer because the IGP does not know how to get to the peer. (Answer A)

Answer D delivers exactly what was asked for a ROUTER ID or RID.

thanks bro for sharing
upvoted 7 times

M_Abdulkarim 1 year, 4 months ago
True, because when loopback interfaces used as update source in ebgp, then ebgp-multihop [1-255] command must be used to establish peering between routers besides we're asked to use loopback interfaces as Router IDs.
upvoted 2 times

MarioSo3 Highly Voted 2 years, 4 months ago
Correct answer is D, because the question is asking for use the loopback as the router-id, not forming the adjacency with it. If you need to use the loopback address as the neighbor ip address in BGP you need to add multihop command.
upvoted 19 times

diegodavid82 2 years, 1 month ago
Totally agree.
upvoted 1 times

ArchBishop 1 year, 10 months ago
BGP multi-hop is only required if the eBGP peers are more that 1 hop away from each other.
In this segment, they are essentially directly attached, within the same subnet. Multi-hop, in this segment, is not needed.

For loopback-based adjacencies you need 2 things:
1: update-source loopback0 to overwrite the exit interface with the loopback's address
2: a valid route to the peer's loopback on each router so that the router can reach the peer's loopback interface to establish an adjacency.

upvoted 1 times

ArchBishop 1 year, 10 months ago

I am wrong... multi-hop is required even if they are directly attached.

upvoted 2 times

ArchBishop 1 year, 10 months ago

The answer is still D, otherwise.

upvoted 1 times

Manicardi Most Recent 1 month, 4 weeks ago

Selected Answer: D

Answer A won't establish BGP link.
Answer is D

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

Answer is D.

Those of you saying 'A'. How? How does 10.3.3.3/32 form a relationship with 10.4.4.4/32? We have no info in this diagram except a known layer 2 link. There is no known static routes linking 10.3.3.3/32 from 10.24.24.3 and vice versa. The solution also suggests we want to use loopback0 as an update-source. The question doesnt ask for this. This eliminates A.

B is not correct because the question states nothing about using loopback as update sources. It's asking for BGP Router ID

C is not correct because we are trying to form a BGP relationship between 2 routers that lack vital routing information. However, the rotuer-id portion is correct...

Which brings us to D.
We are forming a BGP relationship between a layer 2 link between 2 routers, and defining the RID as the loopback0 interface.

upvoted 1 times

ihateciscoreally 3 months ago

A.
R3(config)#router bgp 200
R3(config-router)#neighbor 10.4.4.4 remote-as 100
R3(config-router)# neighbor 10.4.4.4 update-source Loopback0
R4(config)#router bgp 100
R4(config-router)#neighbor 10.3.3.3 remote-as 200
R4(config-router)#network 10.3.3.3 update-source Loopback0

B.
R3(config)#router bgp 200
R3(config-router)#neighbor 10.24.24.4 remote-as 100
R3(config-router)#neighbor 10.24.24.4 update-source Loopback0
R4(config)#router bgp 100
R4(config-router)#neighbor 10.24.24.3 remote-as 200
R4(config-router)#neighbor 10.24.24.3 update-source Loopback0

C.
R3(config)#router bgp 200
R3(config-router)#neighbor 10.4.4.4 remote-as 100
R3(config-router)#bgp router-id 10.3.3.3
R4(config)#router bgp 100
R4(config-router)#neighbor 10.3.3.3 remote-as 200
R4(config-router)#bgp router-id 10.4.4.4

D.
R3(config)#router bgp 200
R3(config-router)#neighbor 10.24.24.4 remote-as 100
R3(config-router)#bgp router-id 10.3.3.3
R4(config)#router bgp 100
R4(config-router)#neighbor 10.24.24.3 remote-as 200
R4(config-router)#bgp router-id 10.4.4.4

upvoted 4 times

LanreDipeolu 3 months, 1 week ago

Selected Answer: D

The key to the answer is "use their loopback interfaces as the BGP router ID" Hence the correct answer is D

upvoted 1 times

djedeen 3 months, 2 weeks ago

Selected Answer: D

Only C and D set the BGP router ID correctly (A & B wrong), and C is using the loopbacks as neighbor IPs (wrong).

upvoted 1 times

Networkfate 4 months ago

Answer A is right .
Bcz by default follow below steps

Use the address configured by the bgp router-id command
Use the Loopback interface address with the highest IP address
Use the highest IP address of the interface

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

Those of you saying 'A'. How? How does 10.3.3.3/32 form a relationship with 10.4.4.4/32? We have no info in this diagram except a known layer 2 link between another network. There is no known static routes linking 10.3.3.3/32 from 10.24.24.3 and vice versa. Basically, we have no IGP info. The solution also suggests we want to use loopback0 as an update-source. The question doesn't ask for this. This eliminates A.

The question wants you to establish a BGP link between routers. D accomplishes this via the l2 link 1024.24.3 and .4 respectively.

Then the question asks you to use the loopback interface as the BGP router ID. So you set your RID via the bgp router-id command to match that of the loopback.

It's common Cisco word question trickery, i dont expect many people with English as their second language to understand this one.

The answer is D.

upvoted 1 times

Networkfate 4 months ago

See here we are forming neighborship with loopback address so BGP going to choose RID by default Loopback address then why do we require to manually configure RID ??

upvoted 1 times

Networkfate 4 months ago

router bgp 100
bgp log-neighbor-changes
no synchronization
neighbor 10.24.24.3 remote-as 200
network 0.0.0.0

Router# sh ip bgp sum
BGP router identifier 10.4.4.4, local AS number 100
BGP table version is 3, main routing table version 6
0 network entries using 0 bytes of memory
0 path entries using 0 bytes of memory
0/0 BGP path/bestpath attribute entries using 0 bytes of memory
0 BGP AS-PATH entries using 0 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 32 total bytes of memory
BGP activity 0/0 prefixes, 0/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.24.24.3 4 200 12 14 3 0 0 00:02:02 4

upvoted 1 times

LanreDipeolu 3 months, 3 weeks ago

Your post "Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.24.24.3 4 200 12 14 3 0 0 00:02:02 4" shows neighborhood failure. Hence "A" is not correct, "D: is the answer.

upvoted 1 times

[Removed] 4 months, 3 weeks ago

Selected Answer: D

Correct answer is D

upvoted 1 times

techriese 4 months, 4 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

[Removed] 5 months ago

Selected Answer: D

Correct answer is D,

upvoted 1 times

adrian0792 5 months, 3 weeks ago

option a is not valid because it does not accept the command network 10.3.3.3 update-source Loopback0

upvoted 1 times

Giza 5 months, 3 weeks ago

Answer is D.
Both routers should use their loopback interfaces as the "BGP router ID"
Just router ID.

upvoted 1 times

Blue_Water 7 months ago

Selected Answer: D

Answer is D

upvoted 1 times

Chiaretta 7 months, 2 weeks ago

Selected Answer: D

answer is D

upvoted 2 times

XDR 7 months, 3 weeks ago

A.
R3(config)#router bgp 200
R3(config-router)#neighbor 10.4.4.4 remote-as 100
R3(config-router)# neighbor 10.4.4.4 update-source Loopback0
R4(config)#router bgp 100
R4(config-router)#neighbor 10.3.3.3 remote-as 200
R4(config-router)#network 10.3.3.3 update-source Loopback0
B.
R3(config)#router bgp 200
R3(config-router)#neighbor 10.24.24.4 remote-as 100
R3(config-router)#neighbor 10.24.24.4 update-source Loopback0
R4(config)#router bgp 100
R4(config-router)#neighbor 10.24.24.3 remote-as 200
R4(config-router)#neighbor 10.24.24.3 update-source Loopback0
C.
R3(config)#router bgp 200
R3(config-router)#neighbor 10.4.4.4 remote-as 100
R3(config-router)#bgp router-id 10.3.3.3
R4(config)#router bgp 100
R4(config-router)#neighbor 10.3.3.3 remote-as 200
R4(config-router)#bgp router-id 10.4.4.4
D.
R3(config)#router bgp 200
R3(config-router)#neighbor 10.24.24.4 remote-as 100
R3(config-router)#bgp router-id 10.3.3.3
R4(config)#router bgp 100
R4(config-router)#neighbor 10.24.24.3 remote-as 200
R4(config-router)#bgp router-id 10.4.4.4

upvoted 4 times

MMaris018 7 months, 3 weeks ago

Selected Answer: D

It just specify to use Loopback as a router id

upvoted 1 times

Question #174 *Topic 1*

An engineer is configuring GigabitEthernet1/0/0 for VRRP. When the router has the highest priority in group 5, it must assume the master role. Which command set should the engineer add to the configuration to accomplish this task? interface GigabitEthernet1/0/0 description To IDF A 38-70-774-10 ip address 172.16.13.2 255.255.255.0

A. standby 5 ip 172.16.13.254 standby 5 priority 100 standby 5 track 1 decrement 10

B. standby 5 ip 172.16.13.254 standby 5 priority 100 standby 5 preempt

C. vrrp 5 ip 172.16.13.254 vrrp 5 priority 100

D. vrrp 5 ip 172.16.13.254 255.255.255.0 vrrp 5 track 1 decrement 10 vrrp 5 preempt

Correct Answer: *C*

Community vote distribution

C (100%)

examShark Highly Voted 2 years, 6 months ago

Given answer is correct
(You don't use a subnet mask in vrrp)

upvoted 24 times

Nhan Highly Voted 2 years, 1 month ago

The given answer is correct VRRP preemption is enable buy default, that why the command doesn't need preempt
https://community.cisco.com/t5/switching/vrrp-the-preempt-is-enabled-by-default/td-p/2776994

upvoted 12 times

Mimimimimi 2 years ago

This is the only correct explanation.

upvoted 2 times

timtgh 1 year, 6 months ago

But C is definitely wrong. Even if preempt is on by default, it's still the best answer, since all other answers are completely out of the question. C does not provide the needed result. D does, even if we know it's already on by default.

upvoted 1 times

timtgh 1 year, 6 months ago

Actually D is also wrong because it has a subnet mask in the syntax. C doesn't do anything because priority 100 is the default. There is no right answer. Maybe C is the best wrong answer, because it has no syntax errors and D does. But C does not ensure that the router will become master when it has high priority. Also, it does not ensure high priority, since 100 is just the default and may be also on the other routers.

upvoted 7 times

mgiuseppe86 Most Recent 2 months, 3 weeks ago

Selected Answer: C

Preempt is enabled by default in VRRP. However, default priority in VRRP is 100. Setting the priority of 100 will not matter, anything higher than 100 assuming the rest of the participating group members are default, will take priority.

C is really the only possible answer. A and B are for HSRP and D tracking is really for layering VRRP inside an SD-WAN VPN or SIG.

upvoted 1 times

danman32 4 months, 1 week ago

Though it is true that VRRP default priority is 100, question states WHEN the router has the highest priority. We don't know what the priority is of the other router. For all we know the other router may have a track or has priority set lower than 100 which would make this router have the highest priority.
So answer C is viable since preempt is default, even if setting priority to 100 is redundant.
The other answers are flat out wrong because either are for HSRP, or bad syntax.

upvoted 2 times

[Removed] 5 months ago

Selected Answer: C

Given answer is correct

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: C

!
interface Ethernet0/0
ip address 172.16.113.2 255.255.255.0

vrrp 5 ip 172.16.113.254
!
cisco(config-if)#do s vrrp
Ethernet0/0 - Group 5
State is Master
Virtual IP address is 172.16.113.254
Virtual MAC address is 0000.5e00.0105
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Master Router is 172.16.113.2 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec

cisco(config-if)#
upvoted 1 times

KZM 11 months, 3 weeks ago

Virtual Router Redundancy Protocol (VRRP)
Ans"A and B"->Standby command is used in HSRP configuration.
preemption is already enable by default and no needed in VRRP
Ans"D" subnet mask is no needed to configure in Virtual IP address (So Ans "D" is wrong)
Ans"C" is more suitable. But it is not sure if the router will become Master or not. Because the priority was stetted as the default value 100. To become Master or not is also depends on another Router's configuration.
upvoted 2 times

ShadyAbdekmalek 1 year ago

I think the question is not accurate,
Review Q#162 and make a comparison
upvoted 1 times

Parot 1 year, 1 month ago

Options ate bit strange. A & B definitely wrong. VRRP states are: master and backup and not active and standby. In D preempt is enabled, but its default for VVRP. Only C is left as the correct one...
upvoted 1 times

H3kerman 1 year, 1 month ago

Selected Answer: C

C is only relevant answer here
upvoted 1 times

GreatDane 1 year, 5 months ago

Ref: Implementing VRRP – Cisco

"...
VRRP Router Priority
...
Priority also determines if a VRRP router functions as a backup virtual router and determines the order of ascendancy to becoming a master virtual router if the master virtual router fails. You can configure the priority of each backup virtual router with a value of 1 through 254, using the vrrp priority command.
..."

A. standby 5 ip 172.16.13.254 standby 5 priority 100 standby 5 track 1 decrement 10

Wrong answer.

B. standby 5 ip 172.16.13.254 standby 5 priority 100 standby 5 preempt

Wrong answer.

C. vrrp 5 ip 172.16.13.254 vrrp 5 priority 100

Correct answer.

D. vrrp 5 ip 172.16.13.254 255.255.255.0 vrrp 5 track 1 decrement 10 vrrp 5 preempt

Correct answer.
upvoted 1 times

GreatDane 1 year, 5 months ago

Sorry,

D. vrrp 5 ip 172.16.13.254 255.255.255.0 vrrp 5 track 1 decrement 10 vrrp 5 preempt

Wrong answer.
upvoted 1 times

pierresadou 1 year, 6 months ago

Selected Answer: C

The Answer is C because Preemption is enable by default and they don't use subnet mask in VRRP

upvoted 3 times

Nhan 2 years, 1 month ago

It's ok to set the priority to 100 which is default. There is nothing wrong with that

upvoted 2 times

Babushka 2 years, 2 months ago

Isn't C incomplete command since it's missing mask? Why would you set priority 100 when that's default?

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

Why would you set a subnet mask for a vIP? you are basing the subnet mask of the vIP on the actual configured IP of the interface that will partake in group membership.

> ip address 172.16.13.2 255.255.255.0

in any failover protocol onfig, a subnet mask is never defined for the vIP

upvoted 1 times

Nickelkeep 2 years, 3 months ago

The question is incomplete.

upvoted 2 times

J2DFW 2 years, 7 months ago

Answer B refers to HSRP and the question is requiring VRRP. A and B are not correct answers.

upvoted 2 times

netpeer 2 years, 8 months ago

It is B. C and D cannot be because theer is no such command as vrrp 5 ip addres, only vrrp 5 address-family ...And A cannot be because that it decreases the router priority, which makes no sense.

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

I think you need to do more reading. The question calls for VRRP. So off the bat A and B are incorrect because that is for HSRP config.

upvoted 1 times

derpo 2 years, 3 months ago

There is a vrrp <group> ip <ip address> command. C is correct. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-vrrp.html

upvoted 2 times

alawi2 1 year, 6 months ago

A&B starts with "standby" which is the command to configure HSRP, so they are wrong without doubt

upvoted 1 times

Question #175 *Topic 1*

Which two security features are available when implementing NTP? (Choose two.)

A. encrypted authentication mechanism

B. symmetric server passwords

C. clock offset authentication

D. broadcast association mode

E. access list-based restriction scheme

Correct Answer: *AE*

Community vote distribution

AE (100%)

GreatDane Highly Voted 1 year, 5 months ago

Ref: Network Time Protocol: Best Practices White Paper – Cisco

"…
NTP Overview
…
The time kept on a machine is a critical resource and it is strongly recommend that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. The two security features available are an access list-based restriction scheme and an encrypted authentication mechanism.
…"

A. encrypted authentication mechanism

Correct answer.

B. symmetric server passwords

Wrong answer.

C. clock offset authentication

Wrong answer.

D. broadcast association mode

Wrong answer.

E. access list-based restriction scheme

Correct answer.

upvoted 6 times

CCNPWILL Most Recent 1 month, 1 week ago

Given answers are 100% correct.

upvoted 1 times

[Removed] 5 months ago

Selected Answer: AE

correct

upvoted 1 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 3 times

Question #176 *Topic 1*

How does the EIGRP metric differ from the OSPF metric?

A. The EIGRP metric is calculated based on bandwidth only. The OSPF metric is calculated on delay only.

B. The EIGRP metric is calculated based on delay only. The OSPF metric is calculated on bandwidth and delay.

C. The EIGRP metric is calculated based on bandwidth and delay. The OSPF metric is calculated on bandwidth only.

D. The EIGRP metric is calculated based on hop count and bandwidth. The OSPF metric is calculated on bandwidth and delay.

Correct Answer: *C*
By default, EIGRP metric is calculated:
metric = bandwidth + delay
While OSPF is calculated by:
OSPF metric = Reference bandwidth / Interface bandwidth in bps

Community vote distribution

C (100%)

GreatDane 1 year, 5 months ago

Ref: EIGRP Metrics used with Redistribution

Post by dmcneil330

"OSPF uses a cost value as a metric. This cost is derived from the interface bandwidth by default. EIGRP uses a composite metric comprised of bandwidth, delay, reliability, and load.
..."

A. The EIGRP metric is calculated based on bandwidth only. The OSPF metric is calculated on delay only.

Wrong answer.

B. The EIGRP metric is calculated based on delay only. The OSPF metric is calculated on bandwidth and delay.

Wrong answer.

C. The EIGRP metric is calculated based on bandwidth and delay. The OSPF metric is calculated on bandwidth only.

Correct answer.

D. The EIGRP metric is calculated based on hop count and bandwidth. The OSPF metric is calculated on bandwidth and delay.

Wrong answer.

upvoted 2 times

pierresadou 1 year, 6 months ago

Selected Answer: C

By default, EIGRP is : bandwidth + delay while OSFP is only bandwidth

upvoted 2 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 3 times

Question #177 *Topic 1*

Refer to the exhibit.

R1	R2
key chain cisco123 key 1 key-string Cisco123!	key chain cisco123 key 1 key-string Cisco123!
Ethernet0/0 - Group 10 State is Active 8 state changes, last state change 00:02:49 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a	Ethernet0/0 - Group 10 State is Active 17 state changes, last state change 00:02:17 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a

An engineer is installing a new pair of routers in a redundant configuration.

Which protocol ensures that traffic is not disrupted in the event of a hardware failure?

A. HSRPv1

B. GLBP

C. VRRP

D. HSRPv2

Correct Answer: *A*

The ג€virtual MAC addressג€ is 0000.0c07.acXX (XX is the hexadecimal group number) so it is using HSRPv1. HSRP Version 2 uses a new MAC address which ranges from 0000.0C9F.F000 to 0000.0C9F.FFFF.

Community vote distribution

A (100%)

AliMo123 Highly Voted 2 years, 6 months ago

MAC add is 0c which is hsrp v1
HSRPv2 is 0c9f
VRRP is 5e00

upvoted 21 times

baid 1 year, 9 months ago

Yes, 00000c is the OUI code of cisco, the 00005e is the OUI code of ICANN, IANA Department, the VRRP is pubic protocol, so it use the OUI code of ICANN, IANA Department.

upvoted 1 times

alawi2 1 year, 6 months ago

well you are part right mate, MAC 0c07 is for HSRP v1, but both routers are in active state which can only be achieved with GLBP, so the question is definitely wrong.

upvoted 1 times

Jared28 1 year, 5 months ago

Agreed, for no disruption GLBP would be best and HSRP can't have 2 active, so I'm sure the information is not correct.

upvoted 2 times

H3kerman 1 year, 1 month ago

you can have 2 Active in HSRP, but you need to have ACL between them filtering HSRP multicasts. Anyway I would say GLBP should be the answer but according to MAC that's clear HSRPv1. In every angle this is pretty tricky question

upvoted 1 times

someguy8921 Highly Voted 2 years ago

The way the question is phrased I would think GLBP is the right answer. This question feels like it was written by an ASL individual as it isn't clear if they're asking what the current configuration IS or what the configuration SHOULD be based on the given requirement.

upvoted 10 times

eww_cybr Most Recent 5 months ago

The engineer is installing hence the configuration and setup is still work in progress. This would mean it's possible for both routers to be active at the same time e.g., cabling not yet done.

upvoted 1 times

[Removed] 5 months, 1 week ago

Selected Answer: A

The question is so bad.
The exhibit shows an HSRPv1 configuration, but the question is asking which protocol ensures traffic is not disrupted in the event of a hardware failure. The way its worded makes the exhibit IRRELEVANT!

To answer the question directly! GLBP is the only protocol that uses Active/Active FHRP

To answer the question based on the exhibit! the answer is HSRPv1.

upvoted 3 times

pmmg 8 months, 2 weeks ago

The question is poor. The MAC address is for HSRP1. So none of the others are active. The question should read 'Which protocol 'is' ensuring that...' Without the MAC, I would think B

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

cisco(config-if)#do s runn int e0/0
Building configuration...

Current configuration : 98 bytes
!
interface Ethernet0/0
ip address 172.16.113.2 255.255.255.0
standby 10 ip 172.16.113.254
end

cisco(config-if)#do s stand
Ethernet0/0 - Group 10
State is Active
2 state changes, last state change 00:00:25
Virtual IP address is 172.16.113.254
Active virtual MAC address is 0000.0c07.ac0a
Local virtual MAC address is 0000.0c07.ac0a (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.424 secs
Preemption disabled
Active router is local
Standby router is unknown
Priority 100 (default 100)
Group name is "hsrp-Et0/0-10" (default)
cisco(config-if)#

upvoted 1 times

JCV13 1 year, 1 month ago

The answer is all of them. If the question said "Which protocol is used in the exhibit" then it would be HSRPv1.

upvoted 3 times

Pudu_vlad 1 year, 2 months ago

A is correct

upvoted 1 times

GreatDane 1 year, 5 months ago

Ref: Hot Standby Router Protocol Features and Functionality – Cisco

"...
HSRP Addressing
...
HSRP uses the following MAC address on all media except Token Ring:

0000.0c07.ac** (where ** is the HSRP group number)
..."

A. HSRPv1

Correct answer.

B. GLBP

Wrong answer.

C. VRRP

Wrong answer.

D. HSRPv2

Wrong answer.

upvoted 2 times

[Removed] 1 year, 5 months ago

Question is not very well written
upvoted 3 times

Nhan 2 years, 1 month ago

This is a trick question, the only one protocol in this question that allow continues traffic without interruption is GLBP because all routers are in the group are active and load balancing using round robin, other protocol in this question are using standby and active, there are small amount of packet lost while the standby is taking over the active role.
upvoted 3 times

nopenotme123 1 year, 3 months ago

Its not a trick question, it a badly written question.
upvoted 1 times

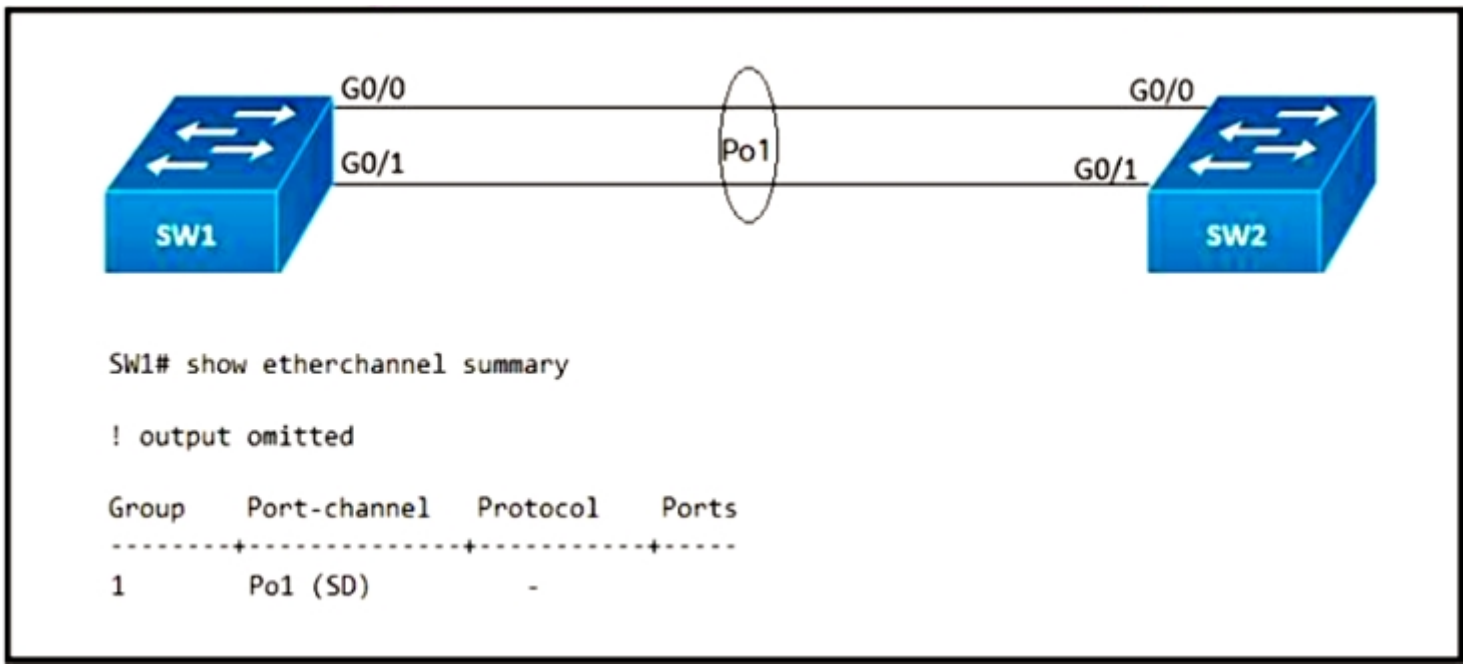
Nhan 2 years, 1 month ago

Correct answer is Glbp. The given answer is not correct
upvoted 1 times

examShark 2 years, 6 months ago

Given answer is correct
upvoted 2 times

Question #178 *Topic 1*



Refer to the exhibit. After an engineer configures an EtherChannel between switch SW1 and switch SW2, this error message is logged on switch SW2:

SW2#

09:45:32: %PM-4-ERR_DISABLE: channel-misconfig error detected on Gi0/0, putting Gi0/0 in err-disable state

09:45:32: %PM-4-ERR_DISABLE: channel-misconfig error detected on Gi0/1, putting Gi0/1 in err-disable state

Based on the output from switch SW1 and the log message received on switch SW2, what action should the engineer take to resolve this issue?

A. Configure the same protocol on the EtherChannel on switch SW1 and SW2.

B. Define the correct port members on the EtherChannel on switch SW1.

C. Correct the configuration error on Interface Gi0/0 on switch SW1.

D. Correct the configuration error on Interface Gi0/1 on switch SW1.

Correct Answer: *A*

Community vote distribution

B (62%) A (38%)

HK010 Highly Voted 2 years, 4 months ago

B because even if it's a wrong protocol, you will get to see the ports that are configured with the command SHOW..... like this
SW1#show etherchannel summary | begin Group
Group Port-channel Protocol Ports
------+------------+-----------+---
1 Po1(SD) LACP Fa0/13(I) Fa0/14(I)

SW2#show etherchannel summary | begin Group
Group Port-channel Protocol Ports
------+------------+-----------+---
1 Po1(SD) PAgP Fa0/13(I) Fa0/14(I)

upvoted 31 times

bendarkel 11 months ago

Are the ports expected to show up in the "show etherchannel summary" output even with a wrong/mismatched channel negotiation protocol?

upvoted 2 times

echipbk 10 months, 3 weeks ago

According to the output from SW1, there are no port configured yet. It means only the below command was configured:
int port-channel 1
exit

So, essentially, the port-channel exists without any members inside it, then whatever configurations are done on either side won't affect each other, which means there won't be such message displayed on the console in the first place.

upvoted 3 times

echipbk 10 months, 3 weeks ago

Which means the correct answer is A

upvoted 2 times

echipbk 10 months, 3 weeks ago

Sorry, my bad. Forget what I said. But I think the correct answer is A
upvoted 1 times

kg2280 8 months ago
The correct answer is B. Just like you said po1 on sw1 have no members. This why sw2 had the port putted in errdisable. sw2 is already in mode on, just like sw1. The only that is missing, is the port on sw1. After this, you shut / no shut the port on sw2 and it should be good. With lacp or pagp, the port-channel wneed to negotiate to come up. Until the port-channel come up, all the ports are in stand-alone
upvoted 4 times

ABC123 Highly Voted 2 years, 7 months ago
Should be B, there's no ports in show output
upvoted 17 times

bendarkel 11 months ago
Are the ports expected to show up in the "show etherchannel summary" output even with a wrong/mismatched channel negotiation protocol?
upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago
Yes

SW12(config-if)#do show etherchannel summary
Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+---
1 Po1(SU) - Gi0/0(P) Gi0/1(P)
upvoted 1 times

NewLife77 Most Recent 3 months ago
Selected Answer: A
This question is about etherchannels. Answer is A
upvoted 1 times

Manvek 3 months, 3 weeks ago
Selected Answer: A
Configuring the protocol means adding the channel. If no channel is added to the ercherchannel, then no protocol is configured.
upvoted 1 times

Networkfate 3 months, 3 weeks ago
see the output log there is no port is shut or up state ,So its clearly saying that , it just cresated port chaneel on global config , not yet interface configuration has started So answer would be define correct port member on sw1
upvoted 1 times

JochenStacker 3 months, 4 weeks ago
Selected Answer: B
There are no ports in the ehterchannel summary
upvoted 1 times

teikitiz 4 months, 2 weeks ago
Selected Answer: A
the exhibit will be valid only if the Po1 interface is set and no protocol nor members defined on interface view. B says "Define the correct port members on the EtherChannel on switch SW1", which would assume some ports had already been set, and would result on a different exhibit. Choosing A will both set the adequate protocol and port members. My 1 cent.
upvoted 1 times

[Removed] 4 months, 3 weeks ago
Selected Answer: B
Answer is B
Exhibit shows that the port-channel 1 does not have members configured.
upvoted 1 times

[Removed] 5 months ago
Selected Answer: B
B.

The show command shows that there is no interfaces as members of the port-channel
upvoted 1 times

KevA_Kev 5 months, 1 week ago
A is the correct answer. What is not be shown in the screenshot is the other has only channel-protocol pagp command configured under the interfaces while sw2 interfaces have channel-group 1 mode on configured so no protocol is configured on sw2 while sw1 is saying we use pagp. I tested in lab and got exact same outputs in the question ...err-disable message and ether channel shows no ports configured on. If try adding the channel-group 1 mode on the interfaces on sw1 then will get an error stating “channel protocol mismatch for interface gi0/0…. Would need to remove the the channel-protocol command first

upvoted 1 times

Burik 5 months, 3 weeks ago

Selected Answer: B

It's B, lab it.

If you just create a Po1 interface without defining any ports, they won't show up in the output:

SW1#show etherchannel summary
[..]
Group Port-channel Protocol Ports
------+-------------+-----------+-----
1 Po1(SD) -

Once SW2 starts receiveing BPDU on its Po1 it will err-disable the ports:

*Jun 10 14:24:33.017: %PM-4-ERR_DISABLE: channel-misconfig (STP) error detected on Po1, putting Et0/0 in err-disable state
*Jun 10 14:24:33.017: %PM-4-ERR_DISABLE: channel-misconfig (STP) error detected on Po1, putting Et0/1 in err-disable state
*Jun 10 14:24:33.018: %PM-4-ERR_DISABLE: channel-misconfig (STP) error detected on Po1, putting Po1 in err-disable state

upvoted 3 times

HungarianDish 7 months, 3 weeks ago

Please do not spam us with chat gpt answers. This is not a valid source for CCNP context.

upvoted 1 times

HungarianDish 7 months, 3 weeks ago

Selected Answer: B

I labbed it up, and following configuration modeled the issue successfully:
SW1:
-int ra fa0/0 - 1 => only trunk configuration
-int port-channel 1 (to create Po1 without members)
SW2:
-int ra fa0/0 - 1 => trunk configuration + channel group 1 mode on

show etherchannel summary on SW1=> shows Group 1, Port-channel Po1 (number 1), Protocol - (which is mode on), but nothing under Ports

This is because channel-group members were not configured. Everything else is configured, and SW1 picked up on the protocol configuration of mode on from SW2.

upvoted 2 times

diamant 9 months, 1 week ago

chat gpt :
Check the interface configuration: Verify the configuration settings for the EtherChannel interface on the switch. Make sure that the settings on both ends of the link match.

Check the EtherChannel protocol: Verify the EtherChannel protocol that is being used on the switch. Make sure that the protocol is the same on both ends of the link.

Check the port channel interface: Check the Port-Channel interface configuration to make sure that it is correctly configured. Verify that the Port-Channel interface is enabled and that the correct number of member interfaces are assigned to it.

Check the cables and connections: Verify the physical connections between the switch and the other devices. Check that the cables are properly seated and that there are no loose connections. Replace the cables if necessary.

Clear the error: Clear the error message by issuing the "shutdown" and "no shutdown" commands on the interface configuration mode.

upvoted 1 times

nightstalker 3 months, 4 weeks ago

do you really rely on chatgpt to study for an exam? *double-facepalm*

upvoted 1 times

echipbk 10 months, 3 weeks ago

Selected Answer: A

A is the correct answer. Please read my explanation by searching for "echipbk"

upvoted 1 times

Ayman_B 11 months ago

Selected Answer: B

the error messages indicates that an error has been detected on interface Gi0/0 and Gi0/1, and the interface has been disabled as a result.
In this case, it means that there is a problem with the configuration of the channel group on interfaces . This could be caused by:
1. an incorrect channel group configuration,
2. an incorrect configuration of the link aggregation protocol
3. a mismatch between the channel group configuration and the physical cabling of the
interface.
so the answer of defining the correct port members on the Etherchannel on switch SW1 seems more logic.

upvoted 2 times

Fadhelben 11 months, 1 week ago

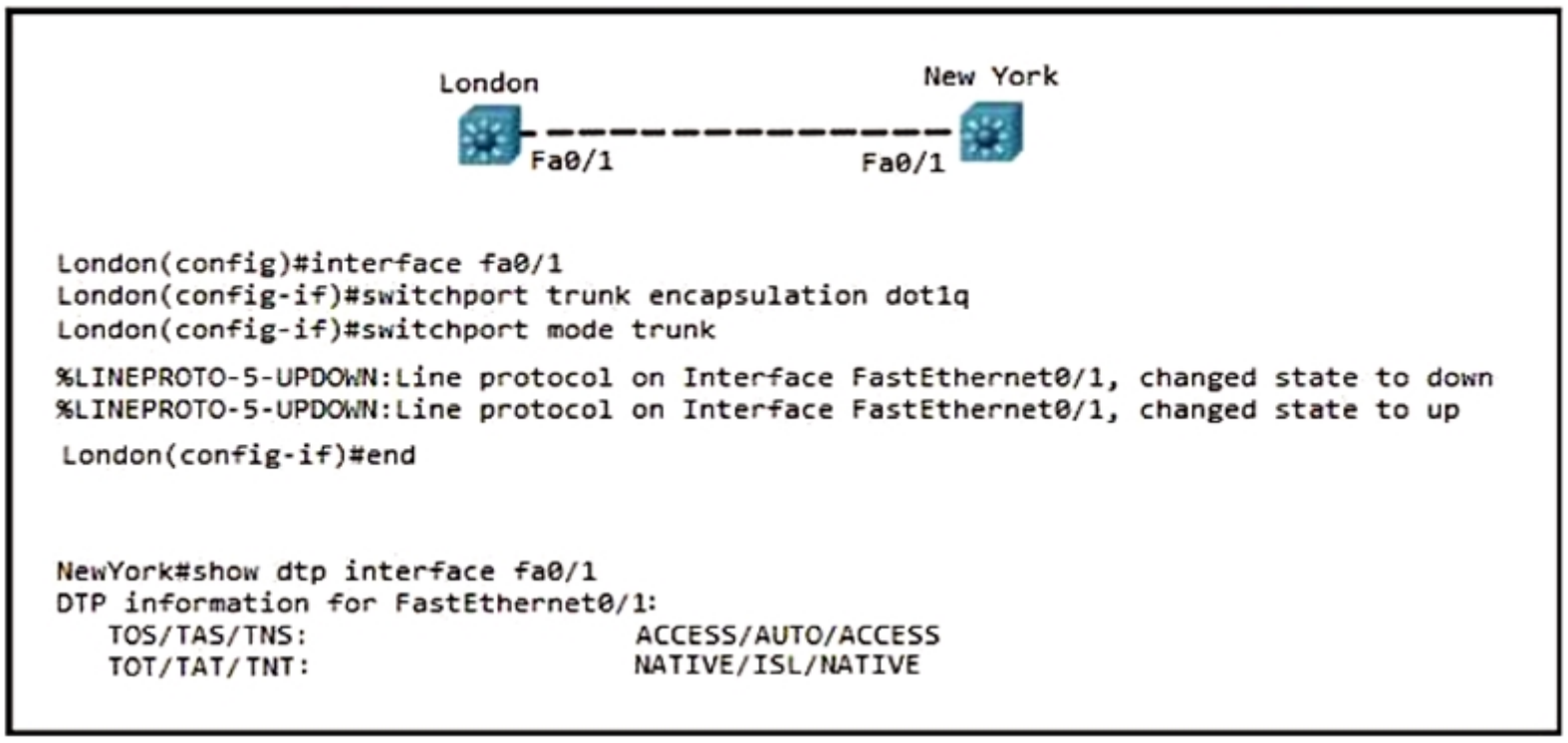
Selected Answer: A

I test it, the err-disable is generated from a protocol mismatch between the two switches. When there are no ports, it will just show PO(SD) without causing "err-disable".

Also you can have some explanation from this link:
https://community.cisco.com/t5/switching/spanning-tree-problem/td-p/2519524

upvoted 4 times

Question #179 *Topic 1*



Refer to the exhibit. Communication between London and New York is down. Which command set must be applied to resolve this issue?

A. NewYork(config)#int f0/1 NewYork(config)#switchport nonegotiate NewYork(config)#end NewYork#

B. NewYork(config)#int f0/1 NewYork(config)#switchport mode trunk NewYork(config)#end NewYork#

C. NewYork(config)#int f0/1 NewYork(config)#switchport trunk encap dot1q NewYork(config)#end NewYork#

D. NewYork(config)#int f0/1 NewYork(config)#switchport mode dynamic desirable NewYork(config)#end NewYork#

Correct Answer: *B*

Community vote distribution

C (69%) D (31%)

Babushka Highly Voted 2 years, 2 months ago

Has to be C.
TOS = Trunk Operational Status
TAS = Trunk Administrative Status
TNS = Trunk Negotiated Status
TOT = Trunk Operational Trunk-Encapsulation
TAT = Trunk Administrative Trunk-Encapsulation
TNT = Trunk Negotiated Trunk-Encapsulation

Operational = What we are doing at this moment
Administrative = How we configured it
Negotiated = What we asked for during the negotiation

TAS is configured as Auto, so if other side is trunk and this side is auto then it will form trunk. There is no need for B.

If we look for trunk-encapsulation TAT, it's set for ISL. It will not work for .1q.

I think you need to change encapsulation to .1q, so answer should be C.
upvoted 55 times

alawi2 1 year, 6 months ago

when i come upon comments like yours, it renews my faith in humanity XOXO
upvoted 10 times

raizer 2 years, 2 months ago

agree.
perfectly explained
upvoted 2 times

baid 1 year, 9 months ago

Thanks for your explanation
upvoted 1 times

Hamzaaa Highly Voted 2 years, 7 months ago

C is the correct the answer because:
1. the port is auto, so it tends to be access but if it detects the other side to be trunk, it will change automatically to mode trunk,

2. The problem is the protocol is Cisco ISL, it must be changed to .1q
and that's what C config does

upvoted 21 times

bendarkel 1 year, 3 months ago

Depends on how old the platform is. Newer platforms no longer use ISL, and defaults to dot1q.

upvoted 2 times

examShark 2 years, 6 months ago

Agreed C, more info to back this up:
https://learningnetwork.cisco.com/s/question/0D53i00000Ksyty/tostastns-tottattnt

upvoted 5 times

bier132 Most Recent 4 months, 1 week ago

Selected Answer: C

If Cisco switches are using Dynamic Trunking Protocol (DTP) between two ports, and one port is configured with the Inter-Switch Link (ISL) encapsulation, while the other port is configured with the IEEE 802.1Q (dot1q) encapsulation, the two ports will not negotiate a trunk.

DTP will not be able to establish a trunk link between these two ports because ISL and dot1q are incompatible trunking encapsulation protocols. ISL is a Cisco-proprietary protocol for trunking, while dot1q is an industry-standard protocol widely used for trunking. Since they are different protocols, they cannot negotiate a trunk link using DTP.

In this scenario, if you want to create a trunk between the two switches, you should configure both ports with the same trunking encapsulation protocol. If one switch is using ISL, the other switch should also use ISL. If one switch is using dot1q, the other switch should use dot1q as well. This way, they can successfully negotiate a trunk link and pass VLAN traffic between them.

upvoted 2 times

mp777 4 months, 2 weeks ago

Selected Answer: D

I would select D, because:
A: other side has DTP enabled, so cannot disable DTP
B: mode trunk, but missing encapsulation, which will be ISL vs dot1q
C: encapsulation dot1q, but missing mode trunk, it will not make the switch port trunk
D: CORRECT, because both, mode trunk and encapsulation will be negotiated by DTP

upvoted 1 times

mp777 4 months, 2 weeks ago

CORRECTION:
although London has DTP enabled but has mode trunk configured, mode trunk negotiates trunking with NewYork which is set to auto. Last thing to configure then is the encapsulation, so C is correct.

upvoted 1 times

rami_mma 8 months, 1 week ago

C is the correct answer.
The remote side configured with (switchport trunk enc isl) you only need to change it to dotq.

upvoted 1 times

Clauster 8 months, 2 weeks ago

Selected Answer: D

A is incorrect because you are setting the trunk to nonegotiate and that's not what we want
B is incorrect because it's missing Switchport mode trunk encapsulation dot1Q.
C is incorrect because it's missing switchport mode trunk
D is the correct answer, setting a trunk port to Dynamic Desirable will send negotiations to the other end and it will Trunk 100% of the time. Set up the Packet tracer and test it yourself, It's gonna work.

upvoted 3 times

Ayman_B 10 months, 4 weeks ago

Selected Answer: C

for NewYork switch the DTP interface fa0/1 :
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/ISL/NATIVE
it shows that it is currently operating as an Access Port, in Dynamic Auto mode, and its negotiated to be an Access Port.
The second line NATIVE/ISL/NATIVE. shows it is not forming or negotiating a Trunk with SW1.

So to make it truly dynamic, it should put Fa1/0/1 on SW2 encapsulation type back into negotiate :
NewYork(config)#int f0/1
NewYork(config)#switchport trunk encap dot1q
NewYork(config)#end

It can take 10 or 15 seconds for DTP to bring interfaces back up due to that 30 second time, but the interface did eventually bounce, and when it came back it is now showing :
TOS/TAS/TNS: TRUNK/AUTO/TRUNK
TOT/TAT/TNT: 802.1Q/NEGOTIATE/802.1Q

for more details :
https://loopedback.com/2017/08/26/dtp-dynamic-trunking-protocol-the-exam-information-and-a-lot-of-live-cli-output-to-demonstrate-behaviors-of-dtp/

upvoted 1 times

Parot 1 year, 1 month ago

NY site configured with ISL(cisco), but London use dot1.q. For me answer is C.

upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: C

Its C, admin please change the answer.

upvoted 1 times

dougj 1 year, 1 month ago

Selected Answer: C

You need the correct encapsulaton. Answer must be C

upvoted 1 times

bendarkel 1 year, 3 months ago

On newer platforms and codes, ISL is no longer a trunk negotiation protocol. Dot1q is now the default. On such platforms, you only need to configure the interface as switchport mode trunk.

upvoted 2 times

danman32 4 months, 3 weeks ago

That may be true but in this exhibit, clearly NY isn't one of those newer platforms as it has ISL configured.

upvoted 1 times

thinqtanklearningDOTcom 1 year, 4 months ago

Trunk ports run DTP automatically unless the command nonegotiate is issued. Setting the other side to dynamic desirable means that encapsulation mode and trunk status is negotiated.

upvoted 1 times

Edwinmolinab 1 year, 5 months ago

B is not possible because encapsulation is mandatory before the command switchport mode trunk

upvoted 2 times

ChristinaA 1 year, 5 months ago

Selected Answer: C

NY port is using ISL instead of dot1q tagging. London is set to Trunk, NY is set to auto, trunk w/ auto will negotiate as trunk.

Answer has to be C.

upvoted 1 times

BartD 1 year, 8 months ago

Selected Answer: C

Need to set the same protocol on both sides

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: C

It should be C

upvoted 1 times

mailmivhan 1 year, 9 months ago

Selected Answer: C

Should be C

upvoted 1 times

Question #180 *Topic 1*

Which encryption hashing algorithm does NTP use for authentication?

A. SSL

B. MD5

C. AES128

D. AES256

Correct Answer: *B*

Community vote distribution

B (100%)

nushadu 11 months, 2 weeks ago

Selected Answer: B

sw2(config)#ntp authenticat?
authenticate authentication-key

sw2(config)#ntp authenticati
sw2(config)#ntp authentication-key ?
<1-4294967295> Key number

sw2(config)#ntp authentication-key 1 ?
md5 MD5 authentication

sw2(config)#ntp authentication-key 1 md
sw2(config)#ntp authentication-key 1 md5 ?
WORD Authentication key

sw2(config)#ntp authentication-key 1 md5

upvoted 2 times

Parot 1 year, 1 month ago

The only one hash algorithm here is MD5. So answer is B!

upvoted 1 times

H3kerman 1 year, 1 month ago

Selected Answer: B

NTP version 4 includes no cryptography (from the viewpoint of government regulations) and introduces MD5 keys
MD5 is anyway only hashing algorithm from options. Rest of them do encryption not hashing.

upvoted 2 times

Encor 1 year, 4 months ago

Resposta dada correta

upvoted 1 times

GreatDane 1 year, 5 months ago

Ref: Configuring NTP – Cisco

"…
Configuring Authentication in Client Mode
…
Step 1…Configure an authentication key pair for NTP and specify whether the key will be trusted or untrusted…set ntp key public_key [trusted | untrusted] md5 secret_key
…"

A. SSL

Wrong answer.

B. MD5

Correct answer.

C. AES128

Wrong answer.

D. AES256

Wrong answer.
upvoted 1 times

pierresadou 1 year, 6 months ago

Selected Answer: B

Provided response is correct
upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct
upvoted 1 times

```
SW1# show interfaces trunk

! Output omitted for brevity

Port      Mode      Encapsulation      Status         Native

Gi1/0/1   auto      802.1q             trunking       1

Port      Vlans allowed on trunk

Gi1/0/1   1-4094

SW2# show interfaces trunk

! Output omitted for brevity

Port      Mode      Encapsulation      Status         Native

Gi1/0/1   auto      802.1q             trunking       1

Port      Vlans allowed on trunk

Gi1/0/1   1-4094
```

Refer to the exhibit. The trunk between Gig1/0/1 of switch SW2 and Gig1/0/1 of switch SW1 is not operational. Which action resolves this issue?

A. Configure both interfaces to nonegotiate and ensure that the switches are in different VTP domains.

B. Configure both interfaces in dynamic auto DTP mode and ensure that the switches are in the same VTP domain.

C. Configure both interfaces in dynamic auto DTP mode and ensure that the switches are in different VTP domains.

D. Configure both interfaces in dynamic desirable DTP mode and ensure that the switches are in the same VTP domain.

Correct Answer: *D*

Community vote distribution

D (100%)

RhJ72 Highly Voted 2 years, 3 months ago

The DTP questions are awful. When DTP is in auto it wont be able to negotiate a trunk, therefore, the show int trunk command will produce no output. I still agree, the answer should still be D. DTP needs to be removed from IOS! Utter rubbish and more effort should be put into creating the questions on the subject.

upvoted 10 times

jonas4ccie 2 years, 1 month ago

I agree, how so does the output show the status is "trunking" when the trunk is not working?

upvoted 2 times

elp213 2 years, 1 month ago

I think is because you configure the interface in mode trunk, it's not because the trunk link is working

upvoted 1 times

Aldebeer 1 year, 7 months ago

Actually both sides are trunking in the "wait" mode, until a partner on the other side is found(!)

upvoted 2 times

Hamzaaa Highly Voted 2 years, 7 months ago

when both are on Auto, they become access mode, when both are desirable, they become trunk mode, so D is correct

upvoted 6 times

XalaGyan 1 year, 11 months ago

remember

Auto Auto => all lazy and no one forms a trunk (like saying after you, no after you sir)
Auto desirable => Trunk because of after you, of thanks i will

Desirable Auto => Trunk because of the same
Desirable Desirable => Trunk there will be a fight about who goes first

upvoted 8 times

Dataset 1 year ago

jajajaja good example!
Regards

upvoted 1 times

Parot Most Recent 1 year, 1 month ago

D is correct.

upvoted 1 times

pierresadou 1 year, 6 months ago

Selected Answer: D

The response is D

upvoted 1 times

TS78 1 year, 10 months ago

D is right answer!

upvoted 1 times

```
Vlan503 - Group 1
   State is Active
      1 state change, last state change 32w6d
   Virtual IP address is 10.0.3.241
   Active virtual MAC address is 0000.0c07.ac01
      Local virtual MAC address is 0000.0c07.ac01 (v1 default)
   Hello time 3 sec, hold time 10 sec
      Next hello sent in 0.064 secs
   Preemption enabled
   Active router is local
   Standby router is 10.0.3.242, priority 100 (expires in 10.624 sec)
   Priority 110 (configured 110)
   Group name is "hsrp-V1503-1" (default)
```

Refer to the exhibit. Which two facts does the device output confirm? (Choose two.)

A. The device's HSRP group uses the virtual IP address 10.0.3.242.

B. The device is configured with the default HSRP priority.

C. The device sends unicast messages to its peers.

D. The standby device is configured with the default HSRP priority.

E. The device is using the default HSRP hello timer.

Correct Answer: *DE*

Community vote distribution

DE (69%) BE (31%)

chris110 Highly Voted 2 years, 4 months ago

D & E is correct! The default priority value is 100. The router in the HSRP group with the highest priority value becomes the active router. The default hold time is 10 seconds for both versions of HSRP (v1 and v2), which is roughly three times the default hello time.

upvoted 13 times

mgiuseppe86 Most Recent 2 months, 3 weeks ago

Selected Answer: DE

People saying B are not actually researching HSRP. Default priority is 100, same with VRRP.

The current device in the example is the ACTIVE router and it says Priority 110.

Question D states the STANDBY router is configured with default (100), which is correct.

> Standby router is 10.0.3.242, priority 100

100 is indeed, the default hsrp priority so its D.

upvoted 1 times

[Removed] 5 months ago

Selected Answer: DE

I see a lot of answers confusing the following lines of the command "show standby"

!
Active router is local
Standby router is 10.0.3.242, priority 100 (expires in 10.624 sec)
Priority 110 (configured 110)
!

The first line describes the local router, the one for which we are seeing the show command.
The second line describes who the standby router, its ip address, and its configured priority
The third line goes back to describe local router settings, and w e see that Priority is 110 and it even goes further and tells us the priority has been configured, otherwsie it would have said "default 100"

upvoted 2 times

ibogovic 5 months, 1 week ago

Selected Answer: BE

B. The device is configured with the default HSRP priority. The output shows that the configured priority is 110, which matches the default priority value.

E. The device is using the default HSRP hello timer. The output states that the hello time is 3 seconds, which is the default hello timer value for HSRP.

upvoted 1 times

arjun_prs 5 months ago

Wrong. 100 is the default priority, not 110.

upvoted 1 times

massimp 6 months, 2 weeks ago

Selected Answer: DE

D & E Correct! Standby has default priority value.

upvoted 2 times

uhljeb 7 months, 2 weeks ago

D and E are 100% correct.

upvoted 1 times

HungarianDish 8 months ago

Selected Answer: DE

Example: https://www.packetswitch.co.uk/cisco-hsrp-configuration-example/

upvoted 1 times

Wissammawas 8 months, 2 weeks ago

Selected Answer: BE

for me its B&E

upvoted 1 times

Dataset 9 months, 2 weeks ago

Selected Answer: BE

The standby device priority is 110 (default value is 100)
So for me are correct B and E
Regards

upvoted 2 times

HungarianDish 8 months, 2 weeks ago

You are right! Standby device priority has 110. It's B,E.

upvoted 1 times

HungarianDish 8 months ago

Sorry, bad eyes for this. Standby is default (100), active is 110. So, D&E.

upvoted 2 times

MPERERWE256 5 months, 4 weeks ago

This is true because there are two priorities 100 for standby and 110 for active . the qn requires the priority of the standby not that of active

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: DE

cisco#show standby
Ethernet0/0 - Group 10
State is Active
2 state changes, last state change 00:40:46
Virtual IP address is 172.16.113.254
Active virtual MAC address is 0000.0c07.ac0a
Local virtual MAC address is 0000.0c07.ac0a (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.568 secs
Preemption disabled
Active router is local
Standby router is unknown
Priority 100 (default 100)
Group name is "hsrp-Et0/0-10" (default)

cisco#show running-config interface Ethernet0/0
Building configuration...

Current configuration : 98 bytes
!
interface Ethernet0/0
ip address 172.16.113.2 255.255.255.0
standby 10 ip 172.16.113.254
end

cisco#

upvoted 1 times

[Removed] 1 year, 7 months ago

Selected Answer: DE

hsrp uses multicast: 224.0.0.2 v1, 224.0.0.102 v2, 224.0.0.18 vrrp. default hsrp hello time is 3 sec, hold timer is 10 sec

upvoted 2 times

Nhan 2 years, 1 month ago

Standby router priority is 100, which is default

upvoted 1 times

hasanozdemirrr 2 years, 5 months ago

B-E true.

upvoted 2 times

ABC123 2 years, 4 months ago

110 is not default HSRP priority

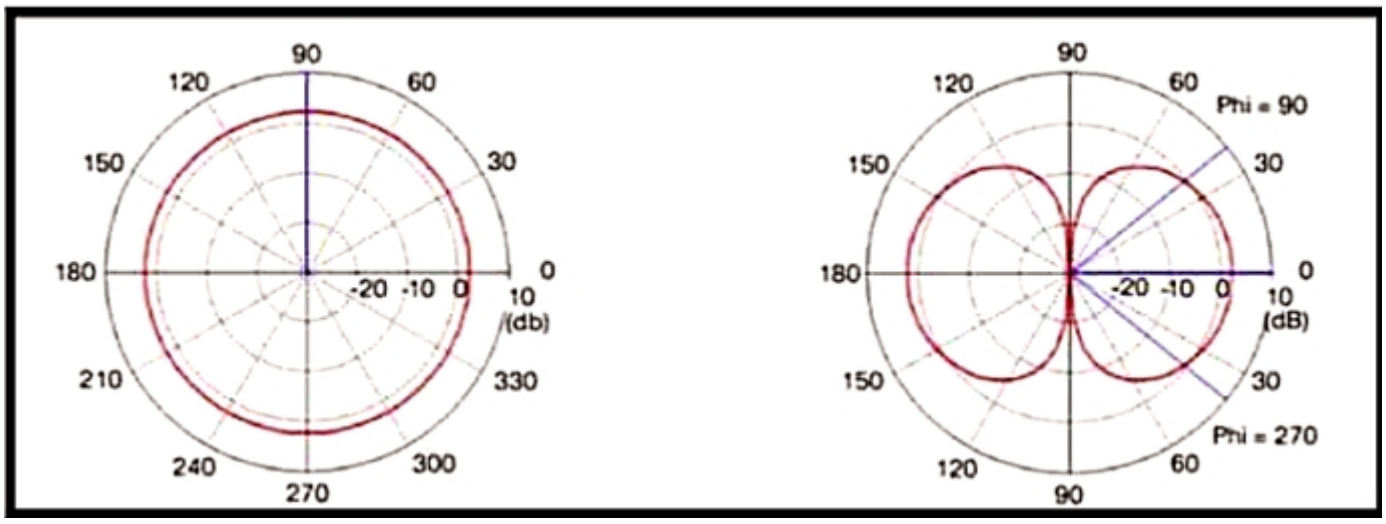
upvoted 3 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 4 times

Question #183 *Topic 1*



Refer to the exhibit. Which type of antenna is shown on the radiation patterns?

A. patch

B. dipole

C. omnidirectional

D. Yagi

Correct Answer: *B*

Community vote distribution

B (100%)

dazzler_010 Highly Voted 1 year, 8 months ago

Answer is B. Diagram coming off from
https://www.industrialnetworking.com/pdf/Antenna-Patterns.pdf

upvoted 9 times

mansaf Highly Voted 11 months, 1 week ago

he thicc boi

upvoted 8 times

Eddgar0 Most Recent 1 year, 7 months ago

Selected Answer: B

Answer is B. Even the pattern shown is a patter of a omnidirectional antena, that pattern is specific of dipole antenas, so making most correct between two

upvoted 4 times

frosty17 1 year, 11 months ago

I agree with XalaGyan. Question refers to the type of antenna. Dipole is an example of an Omnidirectional Antenna.
https://www.ccexpert.us/wireless-networks/common-antenna-types.html

upvoted 3 times

Eddgar0 1 year, 7 months ago

I do understand and the question is vague, dipole is also a type of omnidirectional antenna, but omnidirectional antennas have varying patterns, in this case the most specific and extact match of the pattern is the dipole antena. for that reason i keep on B as the correct answer.

upvoted 4 times

XalaGyan 1 year, 11 months ago

I am sorry to say but that looks to me eexactly like a omni antenna pattern.
Answer D is more correct for me

upvoted 1 times

MerlinTheWizard 10 months ago

Cisco encor guide: "There are two basic types of antennas, omnidirectional and directional." ... "A common type of omnidirectional antenna is the dipole."
Yes, picture displays A SPECIFIC kind of omnidirectional antenna - a dipole one.
Dipole antenna is omnidirectional..

upvoted 1 times

XalaGyan 1 year, 11 months ago

Answer C: Omni (sorry)

upvoted 2 times

d3d4r 1 year, 11 months ago

Omni looks like a Donat
upvoted 1 times

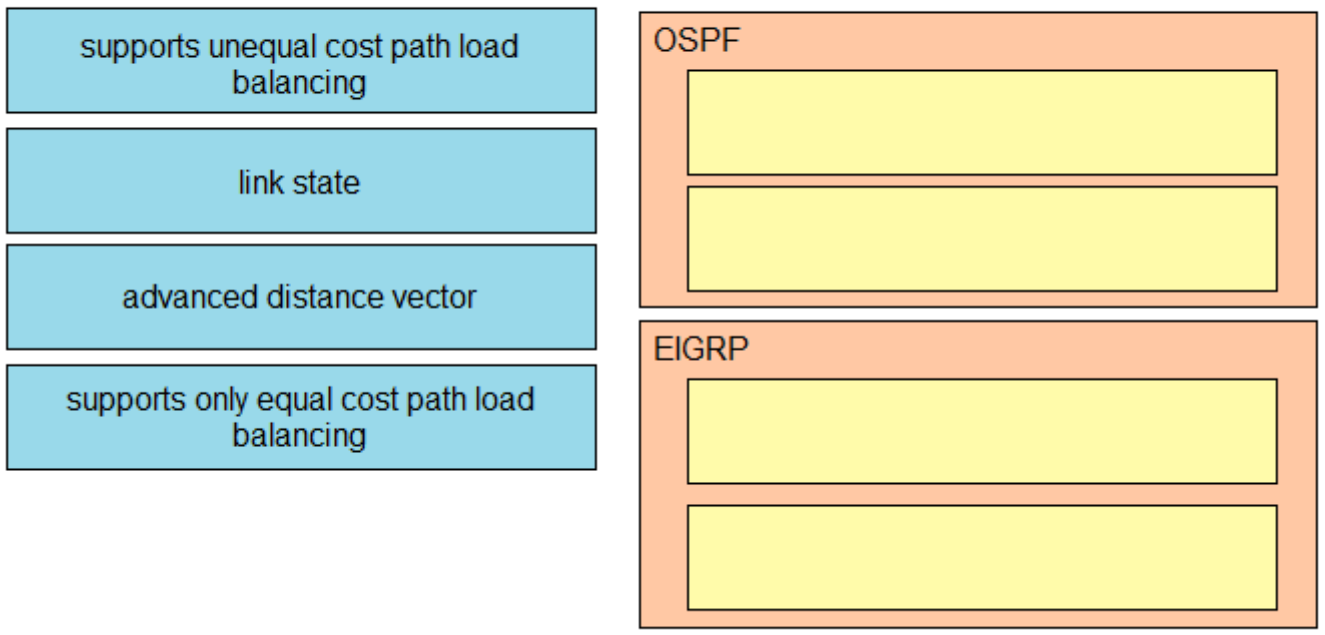
Broekie 2 years, 5 months ago
It's a Dipole Antenna
https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html
upvoted 3 times

examShark 2 years, 6 months ago
The given answer is correct
upvoted 2 times

Question #184 *Topic 1*

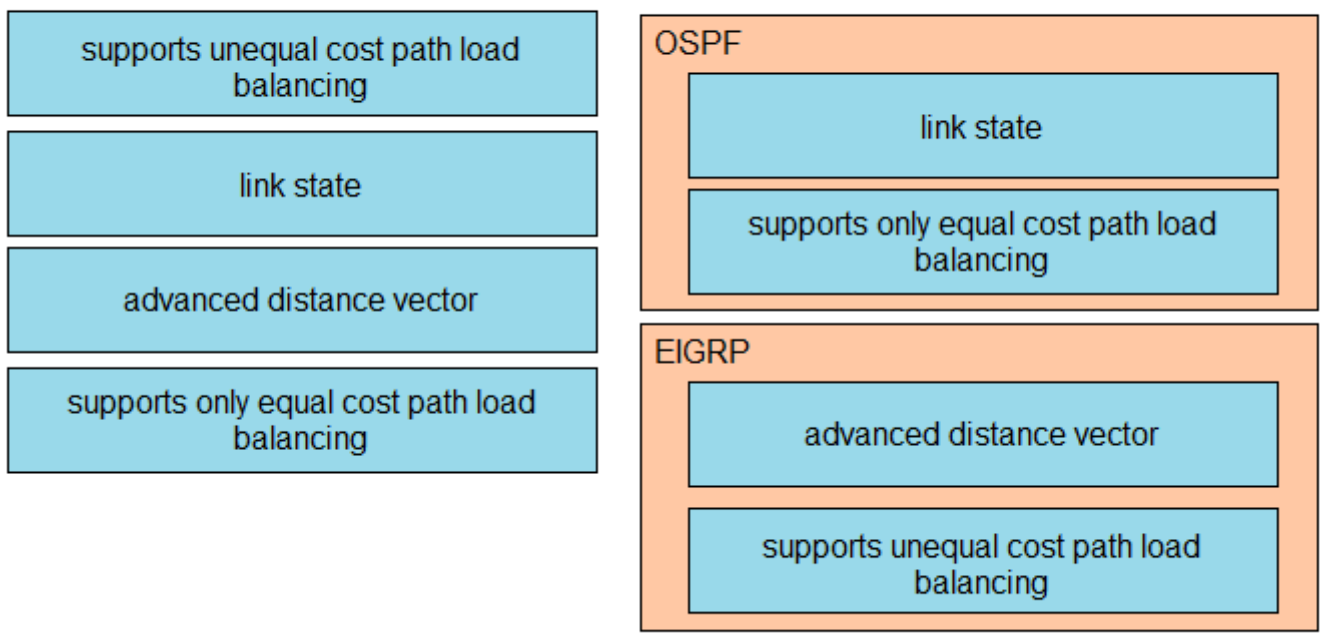
DRAG DROP -
Drag and drop the descriptions from the left onto the routing protocol they describe on the right.
Select and Place:

Answer Area



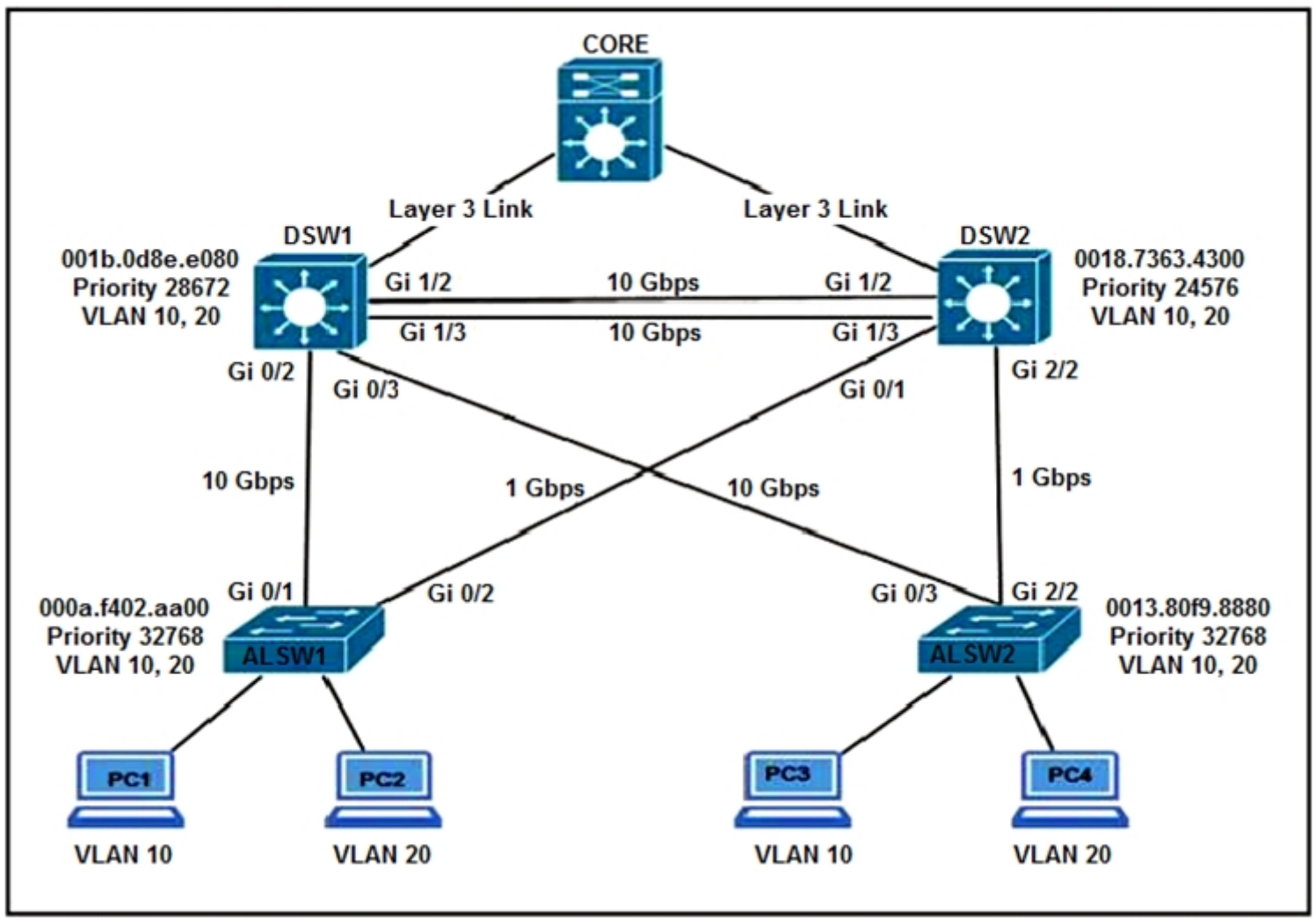
Answer Area

Correct Answer:



CCNPWILL 1 month, 1 week ago
Given answer is indeed correct.
upvoted 1 times

examShark 2 years, 6 months ago
The given answer is correct
upvoted 2 times



Refer to the exhibit. All switches are configured with the default port priority value. Which two commands ensure that traffic from PC1 is forwarded over the Gi1/3 trunk port between DSW1 and DSW2? (Choose two.)

A. DSW2(config)#interface gi1/3

B. DSW1(config-if)#spanning-tree port-priority 0

C. DSW2(config-if)#spanning-tree port-priority 128

D. DSW1(config)#interface gi1/3

E. DSW2(config-if)#spanning-tree port-priority 16

Correct Answer: *DE*

Community vote distribution

AE (92%) 8%

Mac13 Highly Voted 2 years, 7 months ago

The correct answers would look to be A & E.

Priority is chosen based on the upstream port, therefore we need to make this change on DSW2. This means answers B and D are out.

Port priority is set in increments of 16:

Switch(config-if)#spanning-tree port-priority ?
<0-240> port priority in increments of 16

This leaves us with C or E. C is the default, so won't change the behaviour here, so it's out too.

The only two still standing are A & E.

upvoted 66 times

mgiuseppe86 2 months, 3 weeks ago

"Priority is chosen based on the upstream port, therefore we need to make this change on DSW2. This means answers B and D are out."

Why would B be out based on that statement? you even showed the command can be set between 0 and 240 meaning 0 is a valid command.

upvoted 1 times

rogi2023 4 months ago

Just to clarify for all of us. DSW2 is RootBridge, Frames goes PC1->ASW1->directly Root Bridge DSW2 !!! If we agree on this; Than the task is: how to make on DSW1 root port int g1/03 instead of G1/02 ? answer is clear A&E. HTH

upvoted 3 times

youtri 2 years ago

you are right, i was using an IOS switch en eve ng and the incremnt is 64

upvoted 3 times

Mimimimimi 2 years, 1 month ago

I trust the answer from Mac13.

If you change port-priority, you do it on designated ports/upstream devices. (i.e. DSW2)
If you would change DSW1, you would have to work with port costs on root ports/downstream devices.
Source: https://community.cisco.com/t5/routing/spanning-tree-with-port-priority/td-p/1815059

upvoted 1 times

Broekie Highly Voted 2 years, 5 months ago

Correct Answer here is B, D
DSW2 will be elected as root bridge. So all the ports of a root bridge are in forwarding mode. DSW1 has to make the decision to block redundant ports. Default port priority is 128, so interface number breaks the tie. In this case Gi1/3 on DSW1 will be blocked. To prefer Gi1/3 over Gi1/2 the port priority has to be lower than 128. the most appropriate answer is DSW1(config-if)#spanning-tree port-priority 0. Before applying this command you need to apply DSW1(config)#interface gi1/3
The priority values are 0, 32, 64, 96, 128, 160, 192, and 224. All other values are rejected.
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/spanning-tree-port-priority.html#:~:text=The%20priority%20values%20are%200,is%20the%20default%20STP%20mode.

upvoted 18 times

albertie 8 months, 1 week ago

You need to change the priority on the Designated port side , Not from the Root/blocking port side. so you need to do the changes on DSW2 not on
DSW1

upvoted 2 times

Adrenalina73 2 years, 2 months ago

I confirm B,D tested on GNS3 lab

upvoted 3 times

ABC123 2 years, 4 months ago

Make sense

upvoted 1 times

chris110 2 years, 4 months ago

Yes u r right

upvoted 1 times

mgiuseppe86 Most Recent 2 months, 3 weeks ago

I am having a tough time with this one.

The answer can be B or E. (but definitely A)

DSW2(config-if)#spanning-tree port-priority ?
<0-240> port priority in increments of 16

you can actually set it to 0 or 16 and DSW1 will see it as a root port.

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Gi1/2 Altn BLK 4 128.1 P2p
Gi1/3 Root FWD 4 128.2 P2p

So im not too sure what the right answer is.

upvoted 1 times

LanreDipeolu 3 months, 3 weeks ago

Selected Answer: AE

You should open the interface you want to configure. "A" opens the correct interface and "E" configures it. AE are the correct answers

upvoted 1 times

JochenStacker 3 months, 4 weeks ago

Selected Answer: AE

Is the only answer I can see that makes sense

upvoted 1 times

danman32 4 months, 3 weeks ago

One thing we can all agree on, can't be DE as given answer says.
D is starting configuration on SW1, E continues the interface configuration on SW2. Mismatched pairs.
Only choice pairs that can be chosen are AE or BD. Choice C is default port priority so that's out if you think you should configure SW2, not relevant if you think you should configfure SW1.

I misread the text saying all PORT priorities are at defaults, thinking it said all switch priorities are defaults, though the exhibit shows the two distribution switches have different priorities. Either way, switch priorities same or as exhibited, bridge MAC makes SW2 root.
That makes all its ports designated, so it is SW1 that needs to decide whether either of the ports between then are RP or blocked. Only way to do

this is by setting port priority.
But SW1 will be going by the port priority it sees reported by SW2, NOT by what SW1 ports are set to.
So must make configuration change at SW2.
Answer therefore must be AE

upvoted 2 times

Splashisthegreatestmovie 5 months, 2 weeks ago

Selected Answer: BD

You're all mistaken. To change the port priority on a switch you have to change the adjacent port on the upstream switch. It's B&D. It's page 64 of the OCG.

upvoted 1 times

danman32 4 months, 3 weeks ago

Upstream from root bridge, not upstream from packet stream. Direction of frames has no bearing on what STP blocks or doesn't blocks.

upvoted 2 times

MaxwellJK 4 months, 1 week ago

Read it again. You will figure it out. it is A & E. "Both the port priority and port number are controlled by the upstream switch" in this case DSW2.

upvoted 2 times

Chiaretta 7 months, 2 weeks ago

Selected Answer: AE

A and E

upvoted 1 times

KinLeung0413 10 months ago

Lab with EVE-NG, I attempt to change the port priority on DSW1 Gi1/3 the port-priority to 0 but it didn't work. While change the port-priority on DSW2 Gi1/3, it took effect. So the Answer should be A,E.

upvoted 2 times

Ayman_B 10 months, 4 weeks ago

Selected Answer: AE

DSW2(config)#interface gi1/3
DSW2(config-if)#spanning-tree port-priority 16

upvoted 2 times

nushadu 11 months, 2 weeks ago

Selected Answer: AE

UPSTREAM (root) switch interface towards DOWNSTREAM switch configured with prior 64:
sw1#show running-config interface Po2
Building configuration...

Current configuration : 179 bytes
!
interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1-9,11-4094
switchport mode trunk
spanning-tree port-priority 64
end

sw1#

upvoted 1 times

nushadu 11 months, 2 weeks ago

this is ROOT port from DOWNSTREAM switch perspective (see Po2 int):
sw2#show spanning-tree vlan 30

VLAN0030
Spanning tree enabled protocol rstp
Root ID Priority 32798
Address aabb.cc00.1000
Cost 100
Port 65 (Port-channel2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32798 (priority 32768 sys-id-ext 30)
Address aabb.cc00.4000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 100 128.1 Shr Edge
Et0/3 Altn BLK 100 128.4 Shr
Po2 Root FWD 100 128.65 Shr

sw2#
upvoted 1 times

nushadu 11 months, 2 weeks ago

remove priority from UPSTREAM swith:
sw1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
sw1(config)#interface Port-channel2
sw1(config-if)#no spanning-tree port-priority 64
sw1(config-if)#
sw1(config-if)#do show spanning-tree vlan 30

VLAN0030
Spanning tree enabled protocol rstp
Root ID Priority 32798
Address aabb.cc00.1000
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32798 (priority 32768 sys-id-ext 30)
Address aabb.cc00.1000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 100 128.1 Shr
Et0/3 Desg FWD 100 128.4 Shr
Po2 Desg FWD 100 128.66 Shr

sw1(config-if)#
upvoted 1 times

nushadu 11 months, 2 weeks ago

root port has been changed on DOWNSTREAM switch from Po2 -> E0/3:
sw2#show spanning-tree vlan 30

VLAN0030
Spanning tree enabled protocol rstp
Root ID Priority 32798
Address aabb.cc00.1000
Cost 100
Port 4 (Ethernet0/3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32798 (priority 32768 sys-id-ext 30)
Address aabb.cc00.4000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 100 128.1 Shr Edge
Et0/3 Root FWD 100 128.4 Shr <<<<<<<<<<<<<<<<<<< root port
Po2 Altn BLK 100 128.65 Shr

sw2#
upvoted 1 times

Asymptote 1 year ago

Selected Answer: AE

AE

Topology explination:
DSW2 is the root bridge as it has lowest BID in the topology.

The topology must be using 802.1D-2004 version of cost.
Pre-802.1D-1998
1Gbps cost =1
10Gbps cost = 1

802.1D-1998
1Gbps cost = 4
10Gbps cost =2

802.1D-2004
1Gbps cost = 20000

10Gbps cost = 2000

ALSW1 > DSW1 > RB cost = 4000
ALSW1 > RB cost = 20000
Gi 0/1 of ALSW1 become root port,
Gi 0/2 become blocking port as DSW1 has better BID.

If PC1 want to talk to PC3,
the path should be PC1 > ALSW1 > DSW1 > RB > ALSW2 > PC3.

DSW1 Gi1/2 become root port as both Gi1/2 and Gi1/3 of RB has the same root path cost and the same BID, also the same port priority, it use the lowest port number.
DSW1 Gi1/3 become blocking state.

If we want PC1 traffic goes through Gi1/3 between,
we have to make Gi1/3 of RB which is DSW2 lowest port priority, the only option is AE.

root port and blocking port role switch on DSW1.
upvoted 1 times

cloud29 1 year, 1 month ago

Selected Answer: AE

A and E are correct
upvoted 1 times

Tannhaus 1 year, 4 months ago

Selected Answer: AE

Only DSW2 can influence this. Correct answer A&E.
upvoted 2 times

Hermin 1 year ago

DS1 switch when there is tie breaking event:
1. Lowest Sending Bridge ID
2. Lowest Port Priority (of sender)
3. Lowest Interface number (of sender)
upvoted 1 times

DiscardedPacket 1 year, 5 months ago

Correct answer is B, D. DSW1 will become the root bridge, so no ports are in a blocking state.

Port-priority configured locally affects what is ADVERTISED to the connected switch. So by changing port-priority to lowest value on DSW1 g1/3, this will be advertised across to DSW2 and cause that port on DSW2 to be forwarding state.
upvoted 1 times

DiscardedPacket 1 year, 5 months ago

Actually, i'm wrong. Its AE.
DSW2 is the root bridge, therefore the config change needs to be made on DSW2 to advertise the port priority across to DSW1 and have the port change its value.
upvoted 1 times

[Removed] 1 year, 7 months ago

Selected Answer: AE

selection process

- the lowest accumulated Spanning Tree Path Cost to the Root Bridge (Root Switch) as the Root Port, when a Non-Root Switch has multiple paths to reach the Root Switch.

10 Gbps - 2
1 Gbps - 4
100 Mbps - 19
10 Mbps - 100

- if same accumulated Spanning Tree Path Cost in a Non-Root Switch, select the port connected to the neighbor switch which has the lowest Switch ID value as the Root Port.
- If all the multiple paths go through the same neighboring switch to reach the Root Bridge (Root Switch), select the local port which receives the lowest port Spanning Tree Port Priority
- If the received Spanning Tree Port Priority value values are the same between the connecting ports to reach the Root Bridge (Root Switch), select the port which receives the lowest physical port number from neighbor Switch as the Root Port.
upvoted 2 times

Aldebeer 1 year, 7 months ago

Selected Answer: AE

The answers are A and E. SW1 can not have impact in this case!
upvoted 1 times

Question #186 *Topic 1*

A company has an existing Cisco 5520 HA cluster using SSO. An engineer deploys a new single Cisco Catalyst 9800 WLC to test new features. The engineer successfully configures a mobility tunnel between the 5520 cluster and 9800 WLC. Clients connected to the corporate WLAN roam seamlessly between access points on the 5520 and 9800 WLC. After a failure on the primary 5520 WLC, all WLAN services remain functional; however, clients cannot roam between the 5520 and 9800 controllers without dropping their connection. Which feature must be configured to remedy the issue?

A. mobility MAC on the 5520 cluster

B. mobility MAC on the 9800 WLC

C. new mobility on the 5520 cluster

D. new mobility on the 9800 WLC

Correct Answer: *B*

Community vote distribution

B (66%) A (34%)

HungarianDish Highly Voted 10 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/High_Availability_DG.html#pgfId-44041

"When the HA pair is set up, by default, the Primary WLC's MAC address is synced as the Mobility MAC address on the Standby WLC"

-> Devices in 5520 HA cluster already have the mobility mac.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html

"Ensure that you configure the mobility MAC address using the wireless mobility mac-address command for High-Availability to work"

-> Mobility MAC needs to be set manually on new Catalyst 9800.

upvoted 8 times

rlilewis Highly Voted 1 year, 6 months ago

Selected Answer: A

No, A is correct.

The question was quite clear that it was working fine until the 5520 failed over to the secondary node in its cluster. Why would configuring a mobility MAC on the standalone 9800 solve anything?

High Availability (SSO) Deployment Guide:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/High_Availability_DG.html

"The Primary units MAC should be used as Mobility MAC in the HA setup in order to form a mobility peer with another HA setup or **independent controller**"

upvoted 5 times

alejaandrocd 1 year, 6 months ago

"In order to keep the mobility network stable without any manual intervention and in the event of failure or switchover, the back-and-forth concept of Mobility MAC has been introduced. When the HA pair is set up, by default, the Primary WLC's MAC address is synced as the Mobility MAC address on the Standby WLC which can be seen via the show redundancy summary command on both the controllers"

Therefore, 100% should be configured on Cat98k

upvoted 2 times

[Removed] Most Recent 5 months ago

Selected Answer: B

The mobility MAC address is a unique identifier for a wireless controller in a mobility group2. A mobility group is a set of controllers that can share information and support seamless roaming for wireless clients1.

upvoted 2 times

[Removed] 5 months ago

When using SSO (Stateful Switchover), the mobility MAC address of the active controller is used by both controllers in the HA pair2. This ensures that the mobility peers can communicate with the same MAC address regardless of which controller is active.
In this scenario, the 5520 HA cluster already has a mobility MAC address configured, which is shared by both controllers in the cluster. However, the 9800 WLC does not have a mobility MAC address configured, which means it uses its own physical MAC address as the mobility identifier2.

upvoted 1 times

[Removed] 5 months ago

When the primary 5520 WLC fails, the standby 5520 WLC takes over as the active controller and uses the same mobility MAC address as before. However, the 9800 WLC does not recognize this MAC address as its mobility peer, because it was expecting the physical MAC address of the primary 5520 WLC. Therefore, the mobility tunnel between the 5520 cluster and 9800 WLC breaks, and clients cannot roam without dropping their connection.
To remedy this issue, we need to configure a mobility MAC address on the 9800 WLC using the wireless mobility mac-address command2. This will allow the 9800 WLC to use a consistent MAC address as its mobility identifier, and to recognize the mobility MAC address of the 5520 cluster as its peer. This way, the mobility tunnel will remain intact even after a failure on the primary 5520 WLC.

upvoted 1 times

Ayman_B 10 months, 4 weeks ago

Selected Answer: B

this allows the 9800 WLC to act as a "anchor" for client roaming, allowing clients to maintain their connection as they roam between access points that are controlled by different controllers and that will to remedy the issue

upvoted 5 times

Gedson 11 months, 3 weeks ago

Selected Answer: A

Must be B

upvoted 2 times

KOJJY 11 months, 3 weeks ago

Selected Answer: B

B CORRECT ANSWER

upvoted 1 times

Stylar 1 year ago

Selected Answer: B

To me B is correct.

You have 2 5k devices with SSO, and a 1 9k device.
If cluster and primary works fine, then everything is fine.
However when Primary 5k device fails, secondary should take over. Now Secondary with 9k doesnt talk to each other as it should.

Ensure that you configure the mobility MAC address using the wireless mobility mac-address command for HighAvailability to work.

Therefore you should enable this on the 9k device so it knows about the other devices.

Doing it on the cluster with already established SSO wont do anything. Given answer (B) should be the correct one.

upvoted 3 times

fenilp1 1 year ago

Selected Answer: A

A is correct. Things failed after Active 5520 went down and Standby took the Active role

upvoted 2 times

zpacket 1 year, 1 month ago

Selected Answer: B

Provided answer is correct

"Once the HA pair is formed, the Mobility MAC cannot be changed or edited".
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/High_Availability_DG.html#pgfId-44041

That means that other mobility group members (in our case the newly added 9800 WLC) would have to make sure they are configured with the appropriate mobility mac of the existing 5520 cluster. There is NO possibility to change the HA MAC without breaking the HA and re-configure it. Seems there was a misconfiguration by the engineer who configured the new 9800 "to test new features".

upvoted 4 times

Deu_Inder 1 year, 2 months ago

Correct me please if I am wrong here. The given answer is correct. Why? After stateful switchover, the standby 5520 will be active. As 'rlilewis' has quoted already, "The Primary units MAC should be used as Mobility MAC in the HA setup in order to form a mobility peer with another HA setup or **independent controller**"
So, because after the switchover, the configured MAC address of the primary is no more valid, you need to change the MAC address on the 9800 controller to point it to the MAc address of the secondary.

upvoted 3 times

Heim_Ox 1 year, 5 months ago

if mobility MAC wasn't already configured on the 9800, roaming wouldn't have worked. We are told it was working. I think the standby 5520 must have been the one that was forgotten to be configured. I would choose A.

upvoted 2 times

winder 1 year, 5 months ago

Selected Answer: A

It is the roaming service between the new 5520 and the one 9800 not working (dropping). Seems to me that the new controller not forming a mobility peer with 9800 due to the new mac address of the device. that means there was no mac address sync on HA group of 5520. so A

upvoted 3 times

RhJ72 2 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html

"Ensure that you configure the mobility MAC address using the wireless mobility mac-address command for High-Availability to work."

upvoted 2 times

timtgh 1 year, 6 months ago

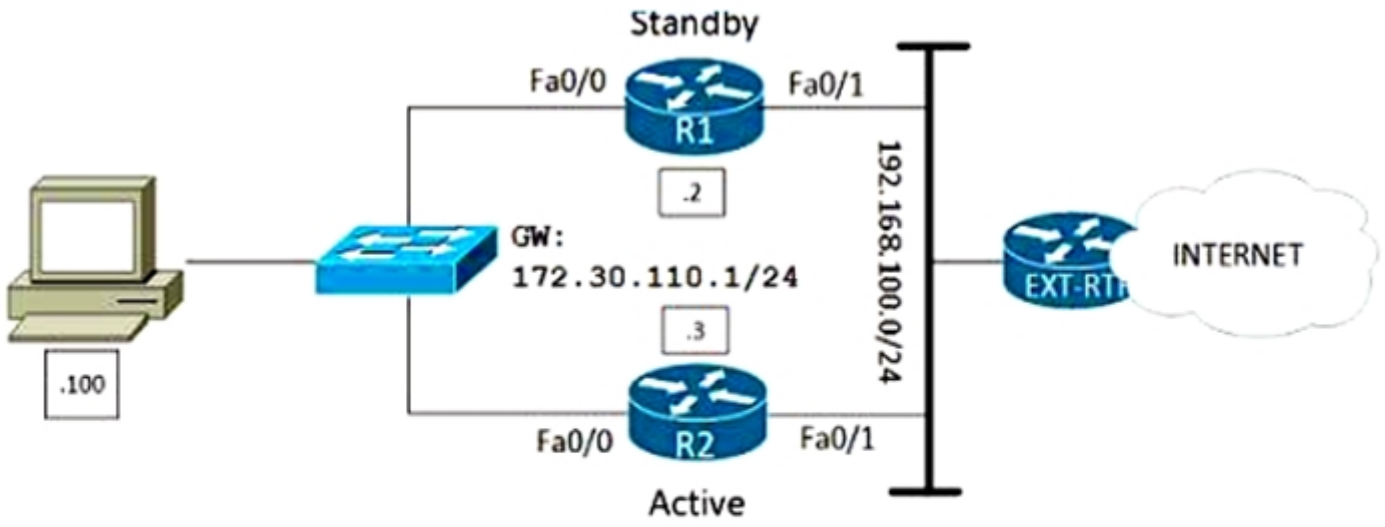
But it's a SINGLE 98000, so it's not using HA. The 5520 side is the side with an HA cluster and needs the command.

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 2 times



Refer to the exhibit. Which configuration change ensures that R1 is the active gateway whenever it is in a functional state for the 172.30.110.0/24 network?

A. R2 standby 1 priority 90 standby 1 preempt

B. R2 standby 1 priority 100 standby 1 preempt

C. R1 standby 1 preempt R2 standby 1 priority 90

D. R1 standby 1 preempt R2 standby 1 priority 100

Correct Answer: *C*

Community vote distribution

C (100%)

Njavwa 3 months ago

Selected Answer: C

default priority is 100 and its in preempt will be chosen as the active gateway, standby configured is 100, it will give back rights(if so to say) when R1 comes online

upvoted 1 times

adrian0792 3 months, 2 weeks ago

it could also be the a

upvoted 1 times

uhljeb 7 months, 2 weeks ago

C is 100% correct

upvoted 1 times

pmmg 8 months, 2 weeks ago

Selected Answer: C

Setting R1 to preempt means take over the role when online, setting R2 to 90 means it will lose to a higher value in an election. 100 is default.

upvoted 2 times

nushadu 11 months, 2 weeks ago

Selected Answer: C

cisco#show standby
Ethernet0/0 - Group 10
State is Active
2 state changes, last state change 00:57:43
Virtual IP address is 172.16.113.254
Active virtual MAC address is 0000.0c07.ac0a
Local virtual MAC address is 0000.0c07.ac0a (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.824 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 100 (default 100)

Group name is "hsrp-Et0/0-10" (default)
cisco#
*Dec 17 22:41:45.948: %HA_EM-6-LOG: CONF_CHANGE: Configuration changed
cisco#
cisco#sh run int Ethernet0/0
Building configuration...

Current configuration : 118 bytes
!
interface Ethernet0/0
ip address 172.16.113.2 255.255.255.0
standby 10 ip 172.16.113.254
standby 10 preempt
end

cisco#

upvoted 1 times

Asymptote 1 year ago

Selected Answer: C

Given answer is correct

upvoted 1 times

timtgh 1 year, 6 months ago

No, A is correct. For R1 to be active, it must have higher priority. The default is 100, and setting a router to 90 will cause it to lose. Set R2 to 90, not R1.

upvoted 2 times

timtgh 1 year, 6 months ago

Please disregard, I misread. Option C does set R2 to 90.

upvoted 3 times

pierresadou 1 year, 6 months ago

Selected Answer: C

The given answer is correct

upvoted 2 times

Violator 1 year, 9 months ago

This question is still asked. Passed today.

upvoted 2 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

Question #188 *Topic 1*

A customer has completed the installation of a Wi-Fi 6 greenfield deployment at their new campus. They want to leverage Wi-Fi 6 enhanced speeds on the trusted employee WLAN. To configure the employee WLAN, which two Layer 2 security policies should be used? (Choose two.)

A. WPA2 (AES)

B. 802.1X

C. OPEN

D. WEP

E. WPA (AES)

Correct Answer: *AB*

Community vote distribution

AB (63%) BC (38%)

examShark Highly Voted 2 years, 6 months ago

The given answer is correct

upvoted 16 times

uhljeb 7 months, 2 weeks ago

No, it's not.

upvoted 2 times

xziomal9 Highly Voted 2 years, 2 months ago

The correct answer is:
B. 802.1X
C. OPEN

upvoted 10 times

mgiuseppe86 Most Recent 2 months, 3 weeks ago

Selected Answer: BC

802.1x without a doubt is an answer. Regarding the A/C Debate, you would not secure a wifi 6 environment with WPA2, and it is a trusted employee WLAN. I currently do this where I am eployed now and the trusted OPEN Network with 802.1x allows for enhanced security.

upvoted 1 times

tsamoko 2 months, 3 weeks ago

yeah , they are right WPA2 is not supported so B & C

https://www.extremenetworks.com/resources/blogs/wireless-security-in-a-6-ghz-wi-fi-6e-world#:~:text=The%20Wi%2DFi%20Alliance%20requires,(OWE)%20in%206%20GHz.

upvoted 2 times

mrlyfi 3 months, 2 weeks ago

The correct answer is B and C (802.1X and Open) !

upvoted 1 times

teikitiz 5 months, 1 week ago

WPA 2 is supported on WiFi 6. It is not supported on WiFi6E (on 6GHz band; it is supposed to be "legacy free")

upvoted 1 times

uhljeb 7 months, 2 weeks ago

B and C

upvoted 2 times

uhljeb 7 months, 2 weeks ago

WPA2 is not supported on WI-FI6, and WEP is out of the discussion, so the correct answers are 802.1x and OPEN.

upvoted 4 times

jaz600 8 months, 1 week ago

Selected Answer: BC

B&C
WPA2 is not supported on wifi6

upvoted 3 times

HungarianDish 8 months, 2 weeks ago

Is this about wifi 6E? Do they mean OWE or Open SSID?
Anyway, WPA2 seems to be out of support on wifi 6/6E. 802.1x and Open (OWE?) seem to be working.
Could someone check this please?

A couple of good sources:
https://www.cisco.com/c/en/us/products/collateral/wireless/nb-06-preparing-for-wifi-6-ebook-cte-en.html
"WPA3 is a mandatory requirement for the Wi-Fi 6E network"
https://blogs.cisco.com/networking/wlan-ssid-security-migration-into-6ghz-networks
"any new device supporting 6GHz, will be required to "only" support the following security standards while in the new band: WPA3..., OWE..., SAE..."
https://www.cisco.com/c/en/us/products/wireless/what-is-wifi-6-vs-wifi-6e.html#~benefits
"Wi-Fi Protected Access 3 (WPA3) mandatory for all Wi-Fi 6E devices, without backward compatibility for WPA2"
upvoted 2 times

x3rox 9 months, 2 weeks ago

Similar question on older exam when referring ro 802.11ac - the answer was OPEN:
https://www.examtopics.com/discussions/cisco/view/5831-exam-200-355-topic-1-question-36-discussion/
upvoted 1 times

x3rox 9 months, 2 weeks ago

When Cisco is describing Wi-fi 6, they state this about OPEN:
Wifi6…It offers enhanced security for open Wi-Fi networks with encryption of unauthenticated traffic, robust password protection against brute-force dictionary attacks, and superior data reliability for sensitive information with 192-bit encryption.

Also, they state this about 802.1X, in the context of wifi6:
Cisco Network Essentials and Network Advantage licenses enable wireless fundamentals such as 802.1X authentication, QoS, Plug and Play (PnP), telemetry and visibility, Single Sign-On (SSO), and security controls. These licenses are perpetual.
Source: https://www.cisco.com/c/en/us/products/collateral/wireless/nb-06-preparing-for-wifi-6-ebook-cte-en.html
upvoted 2 times

x3rox 9 months, 2 weeks ago

More on 802.1X:
Supported WPA3 modes
[….] WPA3-Enterprise, for 802.1X security networks. This leverages IEEE 802.1X with SHA-256 as the Authentication and Key Management (AKM).

[…] while the WPA2-capable clients can use WPA2-Enterprise's 802.1X SHA1 or 802.1X-SHA256
Note: This mode should be used only when necessary. For maximum security, the recommended mode is to use only WPA3 and not a mix of WPA3 and WPA2.

Source: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/wpa3-dep-guide-og.html

WPA2(AES) is not a wifi6 Security Enhancement, which is the question concern. - wifi6 enhancement.

Looks to me the BC we would be a better choice. What do you think?
upvoted 2 times

x3rox 9 months, 2 weeks ago

Chapter: Configuring Layer2 Security:
The available Layer 2 security policies are as follows:

None (open WLAN)

Static WEP or 802.1X

source: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01010000.html
upvoted 2 times

x3rox 9 months, 2 weeks ago

Moreover:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01010000.html
upvoted 1 times

x3rox 9 months, 2 weeks ago

The default security setting for new WLANs is 802.1X with dynamic keys enabled. To maintain robust Layer 2 security, leave 802.1X configured on your WLANs.
upvoted 1 times

eff3 10 months ago

Selected Answer: AB

I think the question is confusing.. They want you to use .1x (instead of a PSK) with! wpa2. Open is not a standard that is discussed
upvoted 3 times

StefanOT2 10 months, 3 weeks ago

Selected Answer: AB

A and B. Both are supported and working for Wifi6. For sure not OPEN (C).
upvoted 2 times

Fadhelben 10 months, 4 weeks ago

Selected Answer: BC

Wi-Fi 6 supports only WPA3.
- Security: WPA3 is a mandatory requirement for the Wi-Fi 6E network, and this secures the network more than ever. Not only that, but since only Wi-Fi 6 products will be using this network, there are no legacy security issues to deal with here.
https://www.cisco.com/c/en/us/products/collateral/wireless/nb-06-preparing-for-wifi-6-ebook-cte-en.html#WhatisWiFi6

upvoted 2 times

StefanOT2 10 months, 3 weeks ago

WPA3 is for sure not mandatory for Wifi6. I have it running in our environment with WPA2. It is only true that WPA3 must be supported by Wifi6 products, but this does not mean WPA2 is not working any more.

upvoted 3 times

poy4242 11 months, 1 week ago

Am I the only one to think dot1x is not a L2 security but a AAA security ?

upvoted 2 times

x3rox 9 months, 2 weeks ago

The default security setting for new WLANs is 802.1X with dynamic keys enabled. To maintain robust Layer 2 security, leave 802.1X configured on your WLANs.
source: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_01001100.html.xml

upvoted 1 times

x3rox 9 months, 2 weeks ago

Chapter: Configuring Layer2 Security:
The available Layer 2 security policies are as follows:

None (open WLAN)

Static WEP or 802.1X

source: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01010000.html

upvoted 1 times

Nickplayany 1 year ago

Selected Answer: AB

Tricky question. A and B
It says trusted not guest (so C is off)

upvoted 5 times

Question #189 *Topic 1*

Which two actions, when applied in the LAN network segment, will facilitate Layer 3 CAPWAP discovery for lightweight AP? (Choose two.)

A. Utilize DHCP option 43.

B. Utilize DHCP option 17.

C. Configure an ip helper-address on the router interface.

D. Enable port security on the switch port.

E. Configure WLC IP address on LAN switch

Correct Answer: *AC*

Community vote distribution

AC (100%)

Raipen24 1 year ago

given answer is correct

upvoted 1 times

pierresadou 1 year, 6 months ago

Selected Answer: AC

The given answer is correct

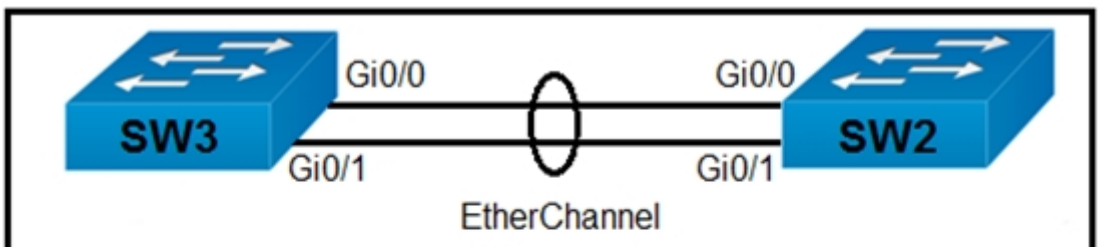
upvoted 2 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

Question #190 *Topic 1*




```
SW2# show ip interface brief | include Port
Port-channel1 unassigned YES unset down down
SW2# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+---------------
-------
1 Po1(S D ) PAgP Gi0/0(I) Gi0/1(I)

SW3# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
```

Refer to the exhibit. Which action resolves the EtherChannel issue between SW2 and SW3?

A. Configure switchport mode trunk on SW2.

B. Configure switchport nonegotiate on SW3.

C. Configure channel-group 1 mode desirable on both interfaces.

D. Configure channel-group 1 mode active on both interfaces.

Correct Answer: *D*

Community vote distribution

C (93%) 7%

rggod Highly Voted 2 years, 7 months ago

Shouldn't this be C? SW2 is using PAgP

upvoted 19 times

Deepak_k 2 years, 7 months ago

May be SW3 is not a Cisco Switch? LACP Works on both CISCO and Non CISCO

upvoted 3 times

noov 2 years, 7 months ago

exactly

upvoted 2 times

reh 2 years, 1 month ago

Both r cisco sw pls check sw symbol.

upvoted 2 times

gtddrf 2 years, 4 months ago

The answer is C because SW2 is running PAgP (Cisco Proprietary). "channel-group 1 mode desirable" enables PAgP. "channel-group 1 mode active on" enables LACP. This also concludes that both switches are Cisco switches.

upvoted 9 times

Miguex125 Highly Voted 2 years, 6 months ago

For me the answer is C, this is a cisco exam, however at least one of those switches should be cisco, and according with the picture, both outcomes are the same, so both are cisco.

upvoted 8 times

Haidary Most Recent 3 weeks, 2 days ago

The provided answer should be correct I, when you change the mode to on both interfaces then you will have LACP instead of PAGP.

upvoted 1 times

Haidary 3 weeks, 2 days ago

Active mode

upvoted 1 times

LanreDipeolu 3 months, 3 weeks ago

Selected Answer: D

The simple fact that the etherchannel bundle is showing PagP and the interfaces are showing standalone, even when connect suggest that the SW might be a different protocol. You are better off changing the channel protocol to active. I support D as the final answer.

upvoted 1 times

danman32 4 months, 3 weeks ago

A problem with this question is that it does not specify what switch the proposed configuration should be on for answers C and D. Also answers C and D says both INTERFACES, not both switches.
C would be correct if we're changing both interfaces on SW3 so that we match PagP on SW2.
But answer D could be correct if we change both interfaces on SW2, since with the complete configuration shown for SW3 on other sites for this question, it is configured for LACP.

upvoted 1 times

uhljeb 7 months, 2 weeks ago

I can't see the entire output, so I don't know the deal with SW3. But if we have PAgP configured on the SW2, then on the SW3, we must configure auto or desirable to bring etherchannel up.

upvoted 1 times

Clauster 8 months, 3 weeks ago

Selected Answer: C

SW2 It's already configured with Port Aggregation Protocol as shown on the output of Show Etherchannel Summary.
The question also does not specify which switch to make the configuration we are to assume it's on SW3, if we configure Active on both interfaces the Etherchannel will not bundle due to incompatible protocols
Active/Passive are both configuration for LACP.
Active/Passive = Bundle
Active/Active = Bundle
Passive/Passive = No bundle

Auto/Desirable are both configurations for PAGP
Auto/Desirable = Bundle
Desirable/Desirable = Bundle
Auto/Auto = No bundle

Hope this helps.

upvoted 1 times

Dataset 9 months, 2 weeks ago

Selected Answer: C

C is correct
one side (sw2) shows PAgP, so for the etherchannel works properly both sw must run the same protocol, so teh option is "desirable"
Regards!

upvoted 1 times

stan3435 10 months, 3 weeks ago

Selected Answer: C

mode desirable for PaGp, mode active for LACP

upvoted 2 times

XBfoundX 10 months, 3 weeks ago

This question is ridiculous.
Both solutions can work, it depends if I have multivendor on my enviroment or not.
Of course as the other says because both are Cisco switches Cisco prefer to use their own protocols....

upvoted 3 times

Rose66 10 months, 3 weeks ago

Selected Answer: C

It's a cisco exam.... the question doesn't say anything about non Cisco-Switches it's C

upvoted 1 times

KOJJY 11 months, 3 weeks ago

Selected Answer: C

for me is 100% C
because from the picture the switches are cisco platform

upvoted 2 times

Asymptote 1 year ago

Selected Answer: C

SW2 is using PAgP and both members interface Gi0/0 and Gi0/1 are in state(I),
it means they are not receiving any activity.

configure channel-group 1 mode desirable on SW3.

upvoted 1 times

H3kerman 1 year, 1 month ago

Selected Answer: C

mode desirable for PaGp, mode active for LACP

upvoted 1 times

iGlitch 1 year, 2 months ago

Both C and D are correct answers, but D has a typo and the original one states group 5 instead of 1. and knowing that the answer is C.

upvoted 3 times

tckoon 1 year, 2 months ago

This question the image of the SW3 "show etherchannel summary" truncated (refer to url link) SW3 etherchannel protocol is LACP. This mean SW2 is Cisco and SW3 is non-Cisco.

Also answer D there is typo , it is port-channel 5 not 1, please refer to url below. So its definately wrong answer.

So final answer definately is C.

https://www.bestciscodumps.com/questions/resolves-the-etherchannel-issue-between-sw2-and-sw3

upvoted 3 times

juantron 1 year, 4 months ago

I think it should be D. C and D are possible solutions, but we don't know if one of the two is not a Cisco switch.

upvoted 1 times

juantron 1 year, 4 months ago

Both are Cisco switches (show etherchannel summary is cisco command). So C is the best answer. Excuse me.

upvoted 2 times

```
Router#show ip ospf interface
GigabitEthernet0/1.40 is up, line protocol is up
  Internet Address 10.3.5.254/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
        0         1       no        no        Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 10.3.5.254
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 172.16.30.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
        0         1       no        no        Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 172.16.30.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 172.16.11.29/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
        0         1       no        no        Base
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 172.16.11.27, Interface address 172.16.11.27
  Backup Designated router (ID) 172.16.11.30, Interface address 172.16.11.30
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
```

Refer to the exhibit. A network engineer configures OSPF and reviews the router configuration. Which interface or interfaces are able to establish OSPF adjacency?

A. GigabitEthernet0/0 and GigabitEthernet0/1

B. only GigabitEthernet0/1

C. only GigabitEthernet0/0

D. GigabitEthernet0/1 and GigabitEthernet0/1.40

Correct Answer: *D*

Community vote distribution

C (96%) 4%

netpeer Highly Voted 2 years, 8 months ago

C the others are in passive mode

upvoted 56 times

Pilgrim5 7 months, 3 weeks ago

Well said.. Short and sweet answer

upvoted 1 times

SandyIndia 2 years, 2 months ago

"No Hellos (Passive Interface)". If you configure passive interface then the network on the interface will still be advertised but it won't send any OSPF hello packets. This way it's impossible to form an OSPF neighbor adjacency.

upvoted 12 times

diegodavid82 2 years, 1 month ago

Exactly, in this way the correct answer is C.

upvoted 5 times

soloo 2 years, 6 months ago

correct

upvoted 3 times

DrGn06 Highly Voted 2 years, 8 months ago

Correct answer C. GigabitEthernet0/1 and GigabitEthernet0/1.40 are in passive mode

upvoted 10 times

mgiuseppe86 Most Recent 2 months, 3 weeks ago

Selected Answer: C

The second I saw (Passive Interface) on G0/1.40 and G0/1 right away the answer was "C" Only G0/0.

There is nothing else to debate about this question.

upvoted 1 times

kldoyle97 3 months ago

"No backup designated router" for GigabitEthernet0/1 and GigabitEthernet0/1.40.
both interfaces have 'broadcast' configured for their network types, meaning there should be a BDR if any adjacency has been formed.
option C makes most sense.

upvoted 1 times

LanreDipeolu 3 months, 3 weeks ago

Selected Answer: D

The state on the interfaces are clearly shown. Two of them are DR while one is DBROTHER. One of the DR interface is a sub-interface of the other. I will therefore eliminate DBROTHER and pick the interface and sub-interface - "D" is the correct answer

upvoted 1 times

uhljeb 7 months, 2 weeks ago

GigabitEthernet0/1 and GigabitEthernet0/1.40 are passive interfaces.

upvoted 1 times

Chiaretta 7 months, 2 weeks ago

Selected Answer: C

Only C the others are passive interfacec

upvoted 1 times

Clauster 8 months, 2 weeks ago

Selected Answer: C

Other Interfaces are in Passive Mode

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

The right answer is C.
When an interface is a passive-interface do not receive and send hello messages, so they cannot establish an ospf neighborship without these messages.

The only interface that is not passive is the G0/0 so the answer is C.

upvoted 2 times

Ayman_B 10 months, 4 weeks ago

Selected Answer: C

GigabitEthernet0/0 is not in a passive mode , the two others are in passive mode.

upvoted 1 times

eb87v 10 months, 4 weeks ago

Selected Answer: C

C. only GigabitEthernet0/0 others are in passive mode.

upvoted 1 times

GeorgeFortiGate 1 year ago

Selected Answer: C

C is the correct answer. Admins please correct this answer.

upvoted 1 times

Dataset 1 year ago

Selected Answer: C

C is correct , other are passived...so they cant send HELLO messages...connot form OSPF Adjayencies.

upvoted 1 times

cloud29 1 year, 1 month ago

Answer is C

upvoted 1 times

Ondskan 1 year, 6 months ago

Selected Answer: C

C - correct others in passive mode

upvoted 2 times

pierresadou 1 year, 6 months ago

Selected Answer: C

C is the correct answer

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: C

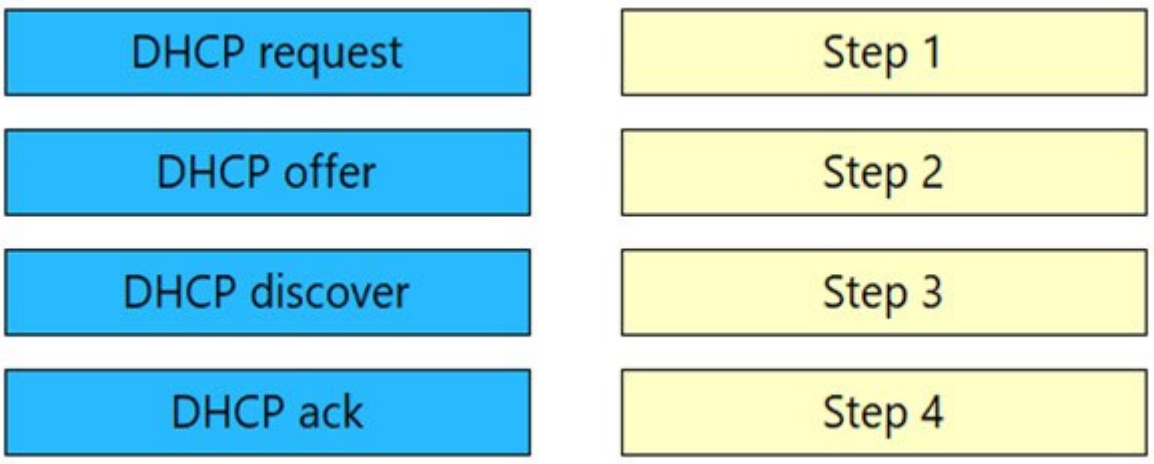
yes, answer C only Gb0/0

upvoted 1 times

DRAG DROP -

Drag and drop the DHCP messages that are exchanged between a client and an AP into the order they are exchanged on the right.

Select and Place:



Correct Answer:

Hack4 Highly Voted 2 years, 5 months ago

DORA => Discover , Offer, Request and Acknowledgement

upvoted 41 times

danman32 Highly Voted 4 months, 3 weeks ago

I like DORA, she's a nice person, always giving me an IP.

upvoted 5 times

ihateciscoreally Most Recent 3 months, 1 week ago

its more like CCNA question but ok.

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

Question #193 *Topic 1*

Which two methods are used by an AP that is trying to discover a wireless LAN controller? (Choose two.)

A. Cisco Discovery Protocol neighbor

B. querying other APs

C. DHCP Option 43

D. broadcasting on the local subnet

E. DNS lookup CISCO-DNA-PRIMARY.localdomain

Correct Answer: *CD*
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html#backinfo

Community vote distribution
CD (100%)

nead Highly Voted 3 years, 3 months ago
It is C & D
E has the wrong name to be resolved, the correct names is cisco-capwap-controller.domainname
upvoted 25 times

alawi2 1 year, 5 months ago
i was suckered by not paying attention to the exact wording in the DNS record
upvoted 5 times

YTAKE 2 years, 2 months ago
The AP goes through this process on startup:

The LAP boots and DHCPs an IP address if it was not previously assigned a static IP address.

The LAP sends discovery requests to controllers through the various discovery algorithms and builds a controller list. Essentially, the LAP learns as many management interface addresses for the controller list as possible via:

DHCP option 43 (good for global companies where offices and controllers are on different continents)

DNS entry for cisco-capwap-controller (good for local businesses - can also be used to find where brand new APs join)

Note: If you use CAPWAP, make sure that there is a DNS entry for cisco-capwap-controller.

Management IP addresses of controllers the LAP remembers previously

A Layer 3 broadcast on the subnet

Statically configured information

Controllers present in the mobility group of the WLC the AP last joined
upvoted 2 times

SandyIndia 2 years, 2 months ago
1) LAP does automatically look on the local subnet for controllers with a 255.255.255.255 local broadcast.
2) Management IP addresses of controllers the LAP remembers previously. Therefore, if you put the LAP first on the local subnet of the management interface, it will find the controller's management interface and remember the address. This is called priming.
3) DHCP option 43 (good for global companies where offices and controllers are on different continents).
4) DNS resolution of "Cisco-capwap-controller.local_domain", (good for local businesses - can also be used to find where brand new APs join)
https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html
upvoted 4 times

Ondskan Most Recent 1 year, 6 months ago
Selected Answer: CD
answer correct, wrong DNS name.
upvoted 1 times

kthekillerc 2 years, 2 months ago
Provided answer is correct
upvoted 1 times

skh 3 years ago
https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html#backinfo

upvoted 1 times

damilola1987 3 years, 4 months ago

C & E ; Therefore, Cisco recommends using the DHCP option 43 or DNS methods {culled from the link)

upvoted 2 times

Jem_1919193 3 years ago

E is wrong. kindly analyze first before commenting. thanks. correct domain name is cisco-capwap-controller.localdomain

upvoted 14 times

Question #194 *Topic 1*

What is the responsibility of a secondary WLC?

A. It enables Layer 2 and Layer 3 roaming between itself and the primary controller.

B. It registers the LAPs if the primary controller fails.

C. It avoids congestion on the primary controller by sharing the registration load on the LAPs.

D. It shares the traffic load of the LAPs with the primary controller.

Correct Answer: *B*

Community vote distribution

B (100%)

Jclemente Highly Voted 2 years, 8 months ago

I think the correct answer is B

upvoted 31 times

hasanozdemirrr Highly Voted 2 years, 5 months ago

guys B could true if the primary WLC down, but the question says WLC operates, so the correct answer is A.

upvoted 5 times

Tannhaus 1 year, 4 months ago

Read answer B: "if primary fails". Correct answer is B.

upvoted 1 times

techplus Most Recent 1 year, 4 months ago

Selected Answer: B

Secondary controller not Anchor controller

upvoted 2 times

danny_f 1 year, 7 months ago

MODERATORS FIX THIS PLEASE. It's B, it's a standby backup device.

upvoted 1 times

AlbertoStu 1 year, 7 months ago

Selected Answer: B

Definitely B.

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: B

It should be B

upvoted 1 times

jordik 1 year, 9 months ago

Selected Answer: B

Correct answer is B. A is not true for all secondary controllers. C and D are only valid in a cluster/load balancing configuration.

upvoted 2 times

ArchBishop 1 year, 9 months ago

A: A secondary, or tertiary controller does not allow roaming functionality by default. They MUST be in the same mobility group for this functionality.
B: Yes
C: A secondary, or tertiary controller does not load-share registration of LAPs by default. They MUST be in the same mobility group for this functionality.
D: No; neither secondary/tertiary, nor mobility grouped controllers have this functionality. While mobility grouped controllers can share LAP registration and context-state information (including client-state) the actual traffic itself is NOT load-balanced (shared) across controllers within the mobility group.

upvoted 2 times

ArchBishop 1 year, 9 months ago

Much of this question relies on your understanding of the benefits, limitations, and differences between Mobility Groups, and Primary/Secondary/Tertiary controllers.

A LAP can be configured to have a secondary/tertiary controller for backup registration purposes; where none of the controllers are in the same mobility groups, if in mobility groups at all. The reverse is true; where controllers that are all in the same mobility group can be assigned as primary, secondary, and tertiary on an LAP.. of which, enables roaming seamlessly, and several other benefits.

upvoted 2 times

GATUNO 2 years ago

When the primary controller (WLC-1) goes down, the APs automatically get registered with the secondary controller (WLC-2). The APs register back to the primary controller when the primary controller comes back on line.
Reference: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/69639-wlcfailover.html

upvoted 1 times

Carl1999 2 years ago

It is A.
L2/L3 roaming needs a secondary WLC.

upvoted 2 times

Nhan 2 years, 1 month ago

Logically the Vice President will replace the president when he is unable to serve the country for some reason and the same in networking the secondary will take over the primary when the primary is down. This is matter of common sense to have a secondary for backup purposes

upvoted 4 times

Nhan 2 years, 2 months ago

Correct answer is B

upvoted 1 times

xziomal9 2 years, 2 months ago

The correct answer is:
B. It registers the LAPs if the primary controller fails.

upvoted 1 times

kthekillerc 2 years, 5 months ago

It is A

upvoted 2 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 3 times

AliMo123 2 years, 7 months ago

The question is very tricky here. It does not say when the primary WLC fails, but it says while the primary WLC operates. so the role of secondary WLC while the primary functions is to enable L2. L3 roaming btw itself and the primary WLC.

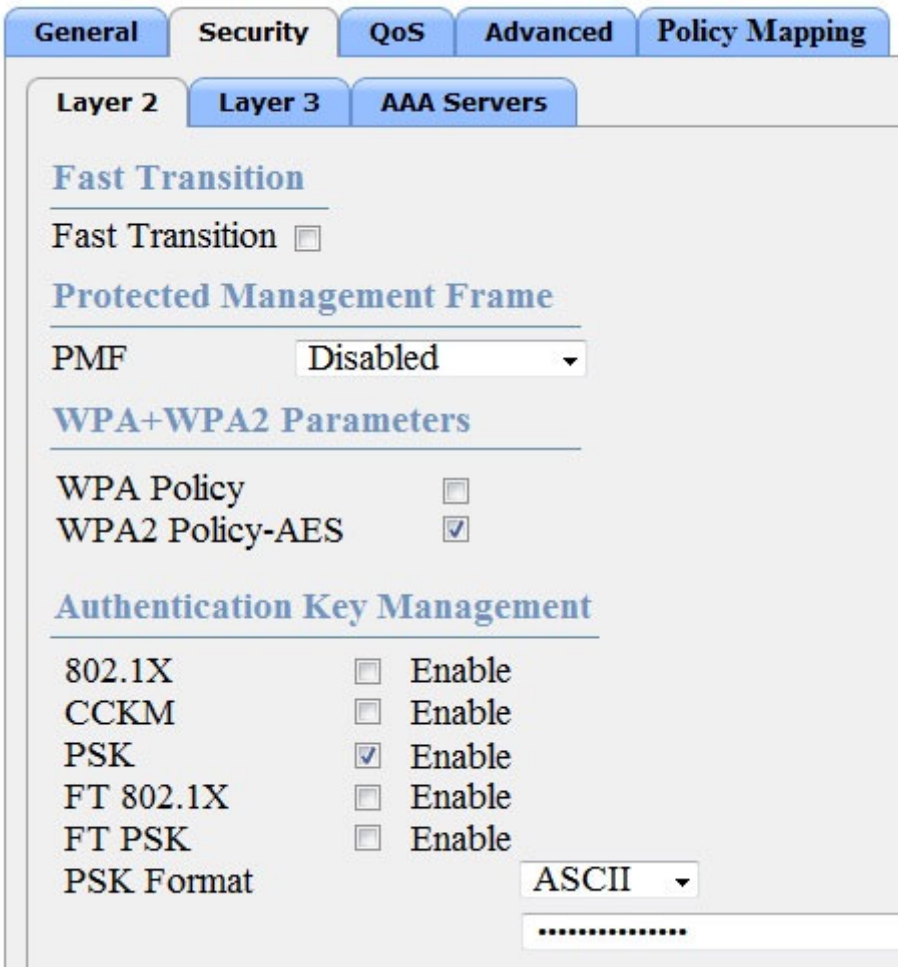
upvoted 3 times

Hamzaaa 2 years, 7 months ago

B is correct

upvoted 1 times

Refer to the exhibit.



Based on the configuration in this WLAN security setting, which method can a client use to authenticate to the network?

A. text string

B. username and password

C. RADIUS token

D. certificate

Correct Answer: *A*

Community vote distribution

A (100%)

edg Highly Voted 3 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01010000.html

"Select or unselect the PMF PSK check box to configure the preshared keys for PMF. Choose the PSK format as either ASCII or Hexadecimal and enter the PSK."

upvoted 5 times

danny_f Most Recent 1 year, 7 months ago

Selected Answer: A

PSK aka text

upvoted 1 times

Nhan 2 years, 1 month ago

PSK = preshare key = a text string > the given answer is correct

upvoted 4 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

Question #196 *Topic 1*

A client device fails to see the enterprise SSID, but other client devices are connected to it.
What is the cause of this issue?

A. The client has incorrect credentials stored for the configured broadcast SSID.

B. The hidden SSID was not manually configured on the client.

C. The broadcast SSID was not manually configured on the client.

D. The client has incorrect credentials stored for the configured hidden SSID.

Correct Answer: *B*

Community vote distribution

B (100%)

edg Highly Voted 3 years, 3 months ago

The answer is "B".
https://en.wikipedia.org/wiki/Network_cloaking
upvoted 10 times

Aldebeer Most Recent 1 year, 7 months ago

Selected Answer: B

the hidden SSID is the issue of not seen.
upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct
upvoted 3 times

Question #197 *Topic 1*

Which two descriptions of FlexConnect mode for Cisco APs are true? (Choose two.)

A. APs that operate in FlexConnect mode cannot detect rogue APs.

B. When connected to the controller, FlexConnect APs can tunnel traffic back to the controller.

C. FlexConnect mode is used when the APs are set up in a mesh environment and used to bridge between each other.

D. FlexConnect mode is a feature that is designed to allow specified CAPWAP-enabled APs to exclude themselves from managing data traffic between clients and infrastructure.

E. FlexConnect mode is a wireless solution for branch office and remote office deployments.

Correct Answer: *BE*
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html

Community vote distribution
BE (80%) DE (20%)

uhljeb 7 months, 2 weeks ago
FlexConnect is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points (AP) in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. In the connected mode, the FlexConnect access point can also perform local authentication.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html
upvoted 4 times

HungarianDish 8 months ago
Selected Answer: BE
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html

"FlexConnect is a wireless solution for branch office and remote office deployments."
"A FlexConnect AP can, on a per-WLAN basis, either tunnel client data in CAPWAP to the controller (called Central Switching)"
upvoted 1 times

bimyo 5 months ago
I agree as D. describes "Central Switched mode" and not "FlexConnect mode"
upvoted 1 times

JohnSmithZhao 9 months ago
Chat GPT said the correct answer is BD
upvoted 2 times

JohnSmithZhao 9 months ago
"D. FlexConnect mode is a feature that is designed to allow specified CAPWAP-enabled APs to exclude themselves from managing data traffic between clients and infrastructure: FlexConnect mode allows APs to process and forward client traffic locally, without sending it to the controller for processing. This can reduce network latency and bandwidth utilization, especially in remote or branch offices."
upvoted 1 times

JohnSmithZhao 9 months ago
"Option E is incorrect because while FlexConnect mode can be used in branch or remote offices, it is not limited to those environments and can be used in any deployment scenario where the features of FlexConnect mode are applicable."
upvoted 1 times

JohnSmithZhao 9 months ago
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html
upvoted 1 times

JohnSmithZhao 9 months ago
From above link, E should be good too...
upvoted 1 times

dnjJ56 11 months, 2 weeks ago
Selected Answer: BE
Flexconnect has two modes
1. Centrally switched - Primarily, tunnels traffic to WLC, if lost connectivity, starts to switch locally. When recovers starts tunneling back. (This is what Answer B is referring to)

2. Locally switched - always switched locally.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html
upvoted 1 times

bora4motion 1 year ago

Selected Answer: BE

b+e is correct. I use FlexConnect at work with 5520s and at home with 2504 - though I don't need it.
upvoted 1 times

H3kerman 1 year, 1 month ago

Selected Answer: DE

A FlexConnect AP can, on a per-WLAN basis, either tunnel client data in CAPWAP to the controller (called Central Switching), or have client data egress at the AP's LAN port (called Local Switching). With Locally Switched WLANs, the AP can tag client traffic in separate VLANs, to segregate the traffic from its management interface.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html#flexconnect-overview

I would chose DE
upvoted 1 times

jra777 1 year, 1 month ago

Selected Answer: BE

B & E are correct.
upvoted 1 times

M_Abdulkarim 1 year, 3 months ago

Selected Answer: BE

Given answer is correct, answer B confirms that AP is connected to WLC(Reachable)
Operation Modes

There are two modes of operation for the FlexConnect AP.

1- Connected mode: The WLC is reachable. In this mode the FlexConnect AP has CAPWAP connectivity with its WLC.

2- Standalone mode: The WLC is unreachable. The FlexConnect has lost or failed to establish CAPWAP connectivity with its WLC. A WAN-link outage between a branch and its central site is a example of such a mode of operation.
upvoted 1 times

pepsifreak 1 year, 5 months ago

Selected Answer: BE

Look at the referenc link. Given answers are correct.
upvoted 2 times

ChristinaA 1 year, 5 months ago

Selected Answer: DE

I think it's D & E. In flex connect mode, the APs don't have to send DATA traffic back to the WLC, that traffic can be sent locally on the switch. Only control plane traffic goes back to the WLC.
FLEX CONNECT MODE -
-- Ideal for branch network locations
-- Traffic is switched locally at branch (instead of via the CAPWAP tunnel on the WLC)
-- Can find rogue access points

Darude 1 year ago

At work we have configured AP in flexconnect mode for users(localy switched) and for Guest vlan we have centraly switched on the same AP (goes to the wlc) it works very well. So BE is correct answer
upvoted 1 times

ChristinaA 1 year, 5 months ago

or maybe i just don't understand what D is trying to say, I read it as though it's trying to say no need to send data back to the WLC. I wish Cisco would make some of the wording of their questions better! ughh. so frustrating.
upvoted 2 times

Aldebeer 1 year, 7 months ago

BE correct
upvoted 2 times

AshPat 1 year, 9 months ago

Selected Answer: BE

Answers are correct.
upvoted 1 times

diegodavid82 2 years, 1 month ago

Provided answers are correct. B.E
upvoted 1 times

Question #198 *Topic 1*

```
DSW1#sh spanning-tree int fa1/0/7

Vlan                 Role Sts Cost      Prio.Nbr Type
-------------------- ---- --- --------- -------- --------------------------
VLAN0001             Desg FWD 2         128.9    P2p Edge
VLAN0010             Desg FWD 2         128.9    P2p Edge
VLAN0020             Desg FWD 2         128.9    P2p Edge
VLAN0030             Desg FWD 2         128.9    P2p Edge
VLAN0040             Desg FWD 2         128.9    P2p Edge
```

Refer to the exhibit. How was spanning-tree configured on this interface?

A. By entering the command spanning-tree portfast trunk in the interface configuration mode.

B. By entering the command spanning-tree mst1 vlan 10,20,30,40 in the global configuration mode.

C. By entering the command spanning-tree portfast in the interface configuration mode.

D. By entering the command spanning-tree vlan 10,20,30,40 root primary in the interface configuration mode.

Correct Answer: *A*

Community vote distribution

A (87%) 10%

zzmejce Highly Voted 1 year, 10 months ago

Selected Answer: A

Provided answer is correct.
Since there are multiple VLANs on the port, the port is in trunk mode. If you leave the trunk keyword (answer C), the following message is shown:
%Portfast has been configured on GigabitEthernet0/10 but will only
have effect when the interface is in a non-trunking mode.

upvoted 12 times

Mimimimimi Highly Voted 2 years, 1 month ago

Answer is C.
All ports have a p2p edge status. Edge indicates that they are connected to a host, not a switch.
If the status would be p2p, they would be a trunkport. In which case, spanning-tree portfast trunk could be used.
Quote from Ciscopress ENCOR 350-401 book, page 66:
"The portfast feature is enabled on a specific access port with the command spanning-tree portfast or globally on all access ports with the command spanning-tree portfast default."

upvoted 9 times

Neil101 1 year, 4 months ago

I'm saying answer is A. Reason is a trunk port can go to a client and doesn't have to go to a switch. As it's a trunk, the word 'trunk' needs to be included in the spanning-tree portfast command, otherwise its not a trunk port by definition. Graphic shows the port is carrying multiple VLANs to an end client, hence 'trunk' is required.

upvoted 2 times

bendarkel 1 year, 3 months ago

Perfect case is a hypervisor.

upvoted 1 times

mgiuseppe86 Most Recent 2 months, 3 weeks ago

Selected Answer: A

"spanning-tree portfast trunk"is a hidden Cisco command. Because they dont want you to use it. This question is stupid

Sw1(config-if)#spanning-tree portfas ?
disable Disable portfast for this interface
edge Enable portfast edge on the interface
network Enable portfast network on the interface

Sw1(config-if)#spanning-tree portfast trunk
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

Sw1(config-if)#spanning-tree portfast?
portfast

upvoted 1 times

HungarianDish 8 months, 2 weeks ago

Trunk port:
sw1#sh span int g0/0

Vlan Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
VLAN0001 Root FWD 4 128.1 P2p Edge
VLAN0002 Root FWD 4 128.1 P2p Edge
VLAN0003 Root FWD 4 128.1 P2p Edge
VLAN0004 Root FWD 4 128.1 P2p Edge
VLAN0005 Root FWD 4 128.1 P2p Edge
sw1#
sw1#sh run
****
interface GigabitEthernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
negotiation auto
spanning-tree portfast edge trunk

P.S.: "spanning-tree portfast trunk" is not available in CML in IOSvL2

upvoted 2 times

HungarianDish 8 months, 2 weeks ago

Access port (could have used spanning-tree link-type point-to-point, but it was not needed thanks to the duplex link to the server):
sw1#sh span int g0/1

Vlan Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
VLAN0001 Desg FWD 4 128.2 P2p Edge
sw1#
sw1#sh run
****
interface GigabitEthernet0/1
switchport mode access
switchport nonegotiate
negotiation auto
spanning-tree portfast edge

upvoted 2 times

HungarianDish 8 months, 2 weeks ago

Selected Answer: A

You can get P2p Edge displayed under "show spanning-tree interface ..." in many ways, but only a trunk port is going to show more than one vlan.
Thus, we need to use " spanning-tree portfast edge trunk" or " spanning-tree portfast trunk" depending on the IOS version.
I labbed it up in CML to confirm the result.

upvoted 3 times

rogi2023 4 months, 1 week ago

perfectly explained, thx.

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

sw2#show runn int e0/0
Building configuration...

Current configuration : 194 bytes
!
interface Ethernet0/0
description to_e0/0_r2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 30,50
switchport mode trunk
duplex auto
spanning-tree portfast trunk
end

sw2#
sw2#
sw2#show spanning-tree vlan 50 | i Edge
Et0/0 Desg FWD 100 128.1 Shr Edge
sw2#

upvoted 2 times

nushadu 11 months, 2 weeks ago

sw2#show spanning-tree int e0/0

Vlan Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
VLAN0030 Desg FWD 100 128.1 Shr Edge

VLAN0050 Desg FWD 100 128.1 Shr Edge
sw2#
upvoted 2 times

forccnp 11 months, 3 weeks ago

Selected Answer: D

D is correct answer
upvoted 1 times

danman32 4 months, 3 weeks ago

That can't be correct. You don't designate bridge (switch) priority in interface configuration mode, you'd do so in global configuration mode.
upvoted 1 times

M_Abdulkarim 1 year, 4 months ago

Selected Answer: A

Provided answer is correct, however the command should include edge if it's required to have the exact same output like this:
spanning-tree portfast edge trunk on the interface
upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: A

look at the .. "Edge" port display.. The command is true. Ans: A
upvoted 3 times

Eddgar0 1 year, 7 months ago

Selected Answer: A

Is a trunk port because Multiple VLANs are in the same port and are edge type that means that the "spanning-tree portfast trunk" command has been issued. without the trunk option porfast command does not work on trunk ports
upvoted 5 times

Marving 1 year, 10 months ago

Selected Answer: C

the commands used with answer A,B and D are invalid commands. run a test on all of the in CML. the correct answer is C.
upvoted 3 times

iGlitch 1 year ago

I abslotly agree with you, it has the same output in the question with addition to a warning msg.
but cisco mentioned this in the OCG, and they want to confuse us with this, although both A and C are aplicable and have the same output, but most ppl chose to go with A.
upvoted 1 times

hybl2467 1 year, 8 months ago

From ENCORE book, STP Portfast section: Portfast can be enabled on trunk links with the command spanning-tree portfast trunk. However, this command should be used only with ports that are connecting to a single host (such as a server with only one NIC that is running a hypervisor with VMs on different VLANs). Running this command on interfaces
connected to other switches, bridges, and so on can result in a bridging loop.
upvoted 4 times

hybl2467 1 year, 10 months ago

There are more than 1 VLAN configured on the Edge port and that tell us that the port is a trunk, the correct answer is A
upvoted 3 times

diegodavid82 2 years, 1 month ago

Well They are two reasons for a port will state in DESG role:
1. When is a root bridge for a VLAN, the ports for this specific VLAN will be DESG ports.
2. After SPT calc the port result in DESG.

Now, the output shows a specific port that has many VLANs, in this way is a trunk port but at the same time have "p2p EDGE" under column Type.

So, the correct answer is "A", for sure.
upvoted 2 times

Hugh_Jazz 2 years, 1 month ago

Answer is A. This is a valid switch IF config:

sw2(config-if)#spanning-tree portfast trunk
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
sw2(config-if)#

Now look at output based on my config:

sw2#sh spanning-tree int G0/1
Vlan Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- -------------------------------
VLAN0001 Altn FWD 4 128.25 P2p
VLAN0010 Altn LRN 4 128.25 P2p
VLAN0020 Altn LRN 4 128.25 P2p
VLAN0030 Altn LSN 4 128.25 P2p
VLAN0040 Altn LSN 4 128.25 P2p
sw2#

upvoted 3 times

Nhan 2 years, 1 month ago

D is correct answer

upvoted 1 times

error_909 2 years, 2 months ago

The given answer is incorrect.
There is no command under the interface called "spanning-tree portfast trunk "
The right answer is C

upvoted 3 times

Telecommunications 1 year, 11 months ago

On most of switch port fast trunk existe
So answer is A

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

on CML, code 15 and above, there is no such command as spanning-tree portfast trunk

Sw1(config-if)#spanning-tree portfast ?
disable Disable portfast for this interface
edge Enable portfast edge on the interface
network Enable portfast network on the interface

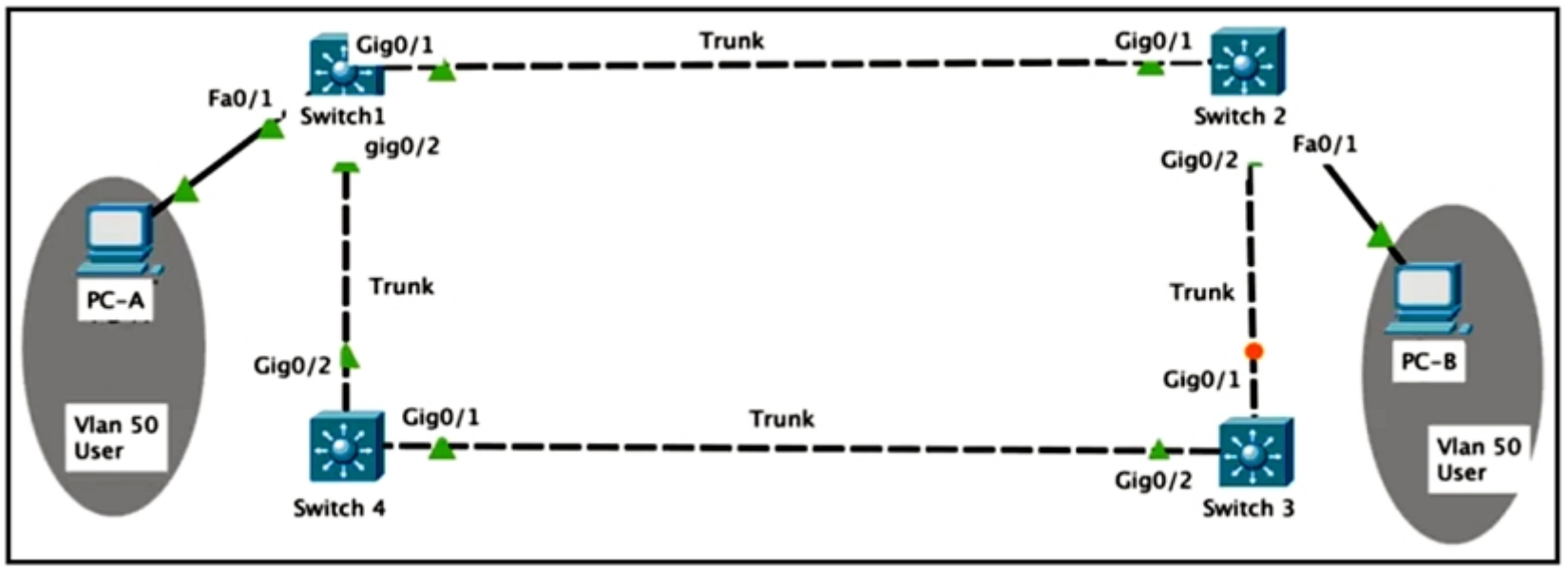
upvoted 1 times

SandyIndia 2 years, 2 months ago

Given ans is correct A. can enable portfast with router on stick case.where you have switch with trunk configured with router interface.
https://www.cisco.com/c/en/us/td/docs/switches/connectedgrid/cg-switch-sw-master/software/configuration/guide/layer2/CGS_1000_L2/l2_stpopt.pdf

upvoted 3 times

Question #199 *Topic 1*



Refer to the exhibit. Rapid PVST+ is enabled on all switches. Which command set must be configured on Switch1 to achieve the following results on port fa0/1?

☞ When a device is connected, the port transitions immediately to a forwarding state.

☞ The interface should not send or receive BPDUs.

☞ If a BPDU is received, it continues operating normally.

A. Switch1(config)# spanning-tree portfast bpdufilter default Switch1(config)# interface f0/1 Switch1(config-if)# spanning-tree portfast

B. Switch1(config)# spanning-tree portfast bpduguard default Switch 1 (config)# interface f0/1 Switch1 (config-if)# spanning-tree portfast

C. Switch1(config)# interface f0/1 Switch1(config-if)# spanning-tree portfast

D. Switch1(config)# interface f0/1 Switch1(config-if)# spanning-tree portfast Switch1 (config-if)# spanning-tree bpduguard enable

Correct Answer: *A*

Community vote distribution

A (78%) 13% 9%

Darude Highly Voted 1 year ago

Selected Answer: A

BPDU filtering allows you to avoid transmitting BPDUs on PortFast-enabled ports that are connected to an end system. When you enable PortFast on the switch, spanning tree places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states.

By default, spanning tree sends BPDUs from all ports regardless of whether PortFast is enabled. BDPU filtering is on a per-switch basis; after you enable BPDU filtering, it applies to all PortFast-enabled ports on the switch.

upvoted 8 times

djedeen Most Recent 3 weeks, 4 days ago

Selected Answer: A

bpduguard will put ports into err-disabled if bpdu received.

upvoted 1 times

ibogovic 5 months, 1 week ago

Selected Answer: A

A. Switch1(config)# spanning-tree portfast bpdufilter default
Switch1(config)# interface f0/1
Switch1(config-if)# spanning-tree portfast

Explanation:

The command "spanning-tree portfast bpdufilter default" enables PortFast on all access ports and applies the BPDU filter. This allows the port to immediately transition to the forwarding state and prevents the interface from sending or receiving BPDUs.
The command "interface f0/1" enters the interface configuration mode for fa0/1.
The command "spanning-tree portfast" enables PortFast on the interface.

upvoted 2 times

jubrilak 5 months, 3 weeks ago

Guys, C is the ANSWER
1) If you enable BPDU Filter globally on the router, it will send 11 BPDUs out when the port first comes up, but if it receives no BPDU it will stop and maintain a portfast state, however, if it receives a BPDU it will lose its portfast state.
See Page 191 of the Official Study Guide

upvoted 1 times

danman32 4 months, 3 weeks ago

But then answer C isn't correct either based on your logic, BPDUs would be sent out of interface, and could receive them too.

upvoted 1 times

Burik 5 months, 3 weeks ago

No. It's A. Lab it.

upvoted 1 times

uhljeb 7 months, 2 weeks ago

The ideal configuration would look like this:
!
interface Ethernet0/2
spanning-tree portfast edge
spanning-tree bpdufilter enable
!
When configuring spanning-tree portfast edge bpdufilter default globally, the port still receives and sends BPDUs.

Switch#show spanning-tree interface e0/2 detail
Port 3 (Ethernet0/2) of VLAN0020 is broken (Port Type Inconsistent)
--Output Ommited--
The port is in the portfast edge mode
Link type is point-to-point by default
Bpdu filter is enabled by default
BPDU: sent 7, received 6

Maybe this is a bug related to EVE-NG, but only when I configure the BPDU filter on the interface it works as explained in the question.

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

Selected Answer: A

The A one is the correct answer because is asking this two things:
- 1) port going immediately to forwarding state
- 2) The interface should not send or receive bpdus (by def in all intefaces bpdus are sent)

https://community.cisco.com/t5/switching/why-stp-rstp-sends-bpdu-on-access-ports/td-p/4190130

- 3) If a bpdu is received the port needs to be up and running anyways

Even if the command spanning-tree portfast is configured later whit the command spanning-tree portfast bpdufilter default when a port is on portfast state the bpdufilter option will be activated on that port:

Switch#show running-config | sec spanning
spanning-tree mode rapid-pvst
spanning-tree portfast edge bpdufilter default

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

Switch#show spanning-tree interface ethernet 0/0 det
Port 1 (Ethernet0/0) of VLAN0001 is designated forwarding
Port path cost 100, Port priority 128, Port Identifier 128.1.
Designated root has priority 32769, address aabb.cc00.4000
Designated bridge has priority 32769, address aabb.cc00.4000
Designated port id is 128.1, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 208, received 1

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

SORRY THIS IS THE RIGHT PORT!

Switch#show spanning-tree interface ethernet 0/1 det
Port 2 (Ethernet0/1) of VLAN0001 is designated forwarding
Port path cost 100, Port priority 128, Port Identifier 128.2.
Designated root has priority 32769, address aabb.cc00.4000
Designated bridge has priority 32769, address aabb.cc00.4000
Designated port id is 128.2, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 60, received 0

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

After portfast:

Switch(config)#interface ethernet 0/1
Switch(config-if)#spanning-tree portfast

Switch(config-if)#do sh spanning int eth0/1 det
Port 2 (Ethernet0/1) of VLAN0001 is designated forwarding
Port path cost 100, Port priority 128, Port Identifier 128.2.
Designated root has priority 32769, address aabb.cc00.4000
Designated bridge has priority 32769, address aabb.cc00.4000
Designated port id is 128.2, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
The port is in the portfast edge mode
Link type is point-to-point by default
Bpdu filter is enabled by default ==> you can see that is activated
BPDU: sent 40, received 0

upvoted 1 times

XBfoundX 10 months, 3 weeks ago

Notice also that when you activate the bpdufilter on the port the counters about sending a bpdu on that port will stop cause of it:

Switch#show spanning-tree interface ethernet 0/1 det
Link type is point-to-point by default
BPDU: sent 147, received 0

Switch#show spanning-tree interface ethernet 0/1 det
Link type is point-to-point by default
BPDU: sent 154, received 0

After porfast command enabled:

Switch#show spanning-tree interface ethernet 0/1 det
Bpdu filter is enabled by default
BPDU: sent 170, received 0

Switch#show spanning-tree interface ethernet 0/1 det
Bpdu filter is enabled by default
BPDU: sent 170, received 0

upvoted 1 times

bendarkel 10 months, 4 weeks ago

Selected Answer: D

The question is specific to SW1 interface fa0/1, not all interfaces on SW1. spanning-tree portfast bpdufilter default is global, it impacts all interfaces on SW1.

upvoted 1 times

bendarkel 10 months, 4 weeks ago

Correction. Best answer is A. Answer D has bpduguard, which if/when BPDUs are received, places the interface an err-disabled state (shutdown), which the question is saying should not be the case.

upvoted 2 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

A. but I am not sure, there are no these commands in my IOU\L2 switch from available choices, config looks like this:

sw2#show spanning-tree vlan 30 detail

Port 1 (Ethernet0/0) of VLAN0030 is designated forwarding
Port path cost 100, Port priority 128, Port Identifier 128.1.
Designated root has priority 32798, address aabb.cc00.1000
Designated bridge has priority 32798, address aabb.cc00.4000
Designated port id is 128.1, designated path cost 100
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 6
The port is in the portfast mode by portfast trunk configuration <<<<<<<<<<<<
Link type is shared by default
Bpdu filter is enabled <<<<<<<<<<<<<<<<<<
BPDU: sent 0, received 0 <<<<<<<< no increase counters after the clearing

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw2#show runn int e0/0
Building configuration...

Current configuration : 227 bytes
!
interface Ethernet0/0
description to_e0/0_r2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 30,50
switchport mode trunk
duplex auto

spanning-tree portfast trunk
spanning-tree bpdufilter enable
end

sw2#

upvoted 1 times

bora4motion 12 months ago

Selected Answer: A

a is correct

upvoted 1 times

Asymptote 1 year ago

Selected Answer: D

Configure global bpdufilter will still send out around 10 or 12 BPDUs at the very begining,
while manually configure on the interface will not send any.

Bpdu filter will prevent inbound and outbound bpdu but will remove portfast state on a port if a bpdu is received. Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

upvoted 2 times

Parot 1 year, 1 month ago

The answer is C!

upvoted 1 times

Parot 1 year, 1 month ago

I had to dig bit deeper and correct myself. Answer is A.

upvoted 1 times

FrameRelay 1 year, 1 month ago

Selected Answer: C

The question is specific to port fa0/1, therefore global commands are ruled out, thats answers A and B off the table. Answer C is specific to port fa0/1 as requested, and portfast mode ensures all bpdu packets are ignored and maintains the port operational. Answer D has the option of BPDU guard which puts the port in err-disable upon receiving BPDU packets advertising better routes, therefore not the answer.
The correct answer is C.

upvoted 1 times

MerlinTheWizard 10 months ago

Global commands are not ruled out, they still achieve the desired outcome on a specific interface. You'd rule them out if they would cause some other inconsistency or problems on the rest of the ports. Besides, there is only one option that meets the BPDU requirement (although, as stated in the comments, it would be better if it was per-interface bpdufilter since you're still sending around 10 bpdus initially)

upvoted 1 times

Lalane 1 year, 1 month ago

When you use spanning tree portfast command under interface sub mode interface is still able to send and recieve bpdus , portfast is specifically used for change interface state to forwarding

upvoted 1 times

santiagofarinas 1 year, 4 months ago

A
At the global level, you can enable BPDU filtering on Port Fast-enabled STP ports by using the spanning-tree portfast bpdufilter default global configuration command. This command prevents interfaces that are in a Port Fast-operational state from sending or receiving BPDUs.
I would say A but would configure the portfast first on the interface

upvoted 1 times

BigMouthDog 1 year, 4 months ago

The second condition is "not send or receive BPDUs" ==> we must use bpdufilter , therefore answer b and d will be eliminated. Since answer c does not have configuration part of bpdufilter, it can be taken away as well.

upvoted 1 times

BigMouthDog 1 year, 4 months ago

Also it has to be noticed that the bdpufilter is global configuration mode

upvoted 1 times

Lalane 1 year, 1 month ago

Is global config but only for int with portfast activated

upvoted 1 times

sanalainen 1 year, 4 months ago

Selected Answer: C

Portfast on fa0/1 would make it to transition immediately to a forwarding state. BPDU guard is not enabled by default, so receiving BPDUs would not make it to go errdisable state.

upvoted 1 times

answerx 1 year, 6 months ago

Selected Answer: A

"At the global level, you can enable BPDU filtering on Port Fast-enabled STP ports by using the spanning-tree portfast bpdufilter default global configuration command."

https://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/trash/swstpopt.html#:~:text=The%20BPDU%20filtering%20feature%20can,bpdufilter%20default%20global%20configuration%20command.

upvoted 2 times

Aldebeer 1 year, 7 months ago

The question is why bpdufilter set globally ? it is only needed on port fa0/1 (?!)

upvoted 3 times

timtgh 1 year, 6 months ago

True, but this is the only answer that meets the requirements for fa0/1, even though doing the whole switch isn't needed.

upvoted 3 times

pierresadou 1 year, 6 months ago

That was my question too !!!!

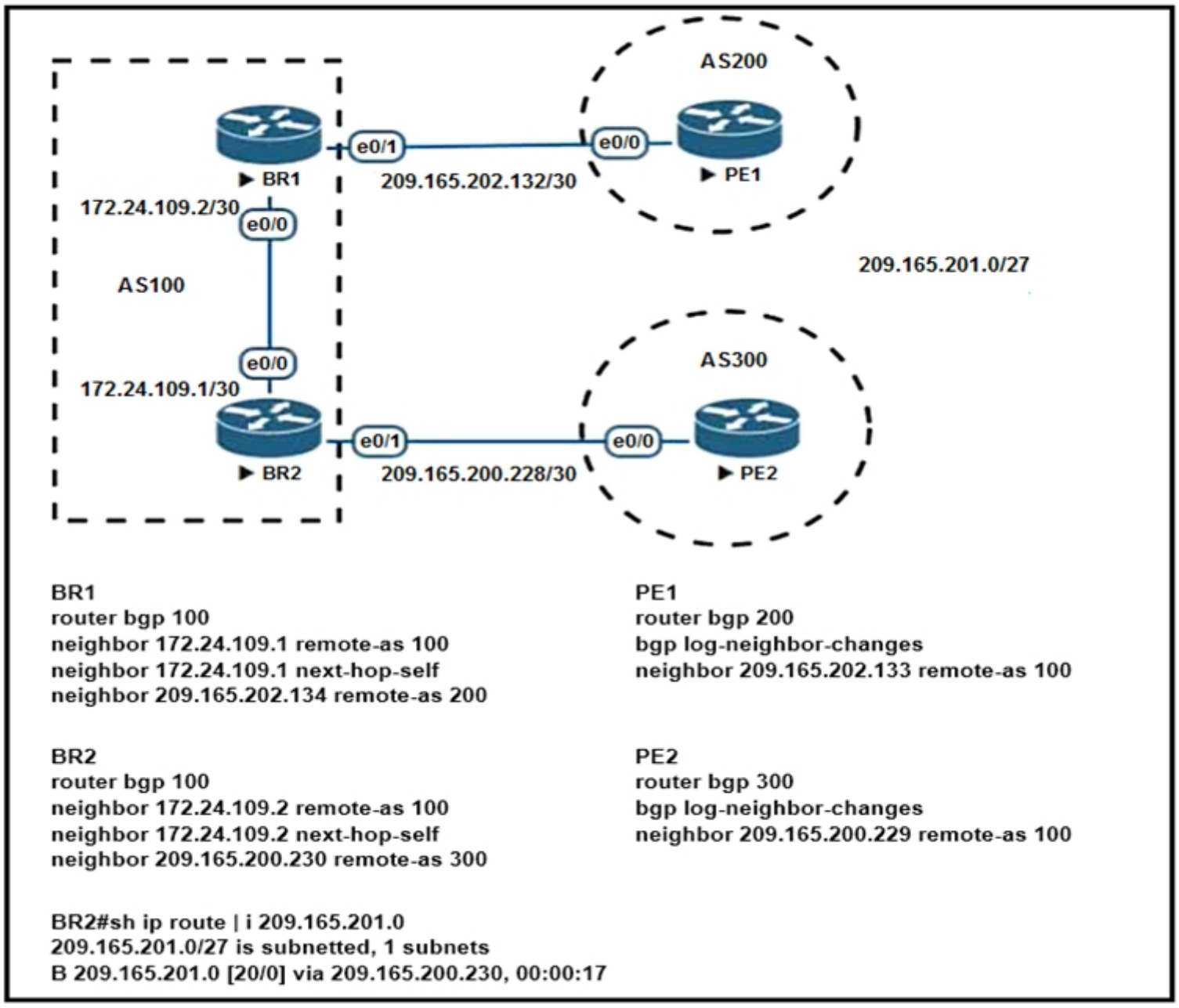
upvoted 1 times

KUM_WENG 1 year, 6 months ago

agree it asking on fa0/1 only

upvoted 1 times

Question #200 *Topic 1*



Refer to the exhibit. Which configuration change will force BR2 to reach 209.165.201.0/27 via BR1?

A. Set the MED to 1 on PE2 toward BR2 outbound.

B. Set the origin to igp on BR2 toward PE2 inbound.

C. Set the weight attribute to 65,535 on BR1 toward PE1.

D. Set the local preference to 150 on PE1 toward BR1 outbound.

Correct Answer: *B*

Community vote distribution

A (65%) B (30%) 4%

Nickelkeep Highly Voted 2 years, 3 months ago

The correct answer is A.

upvoted 24 times

rettich Highly Voted 1 year, 9 months ago

No Answer is correct
A) Med is not compered if As-Path is not the same or Always-compare-med is configured (nor is)
B) would prefer the path BR2 -PE2 which is not the goal
C) prefers the path only on BR1 local, does not change decision on BR2
D) you cant configure Local pref outbound to another AS

upvoted 17 times

Lalane 1 year, 1 month ago

Lower MED is prefer you can see route from PE2 on BR2 has a AD of 20 because EBGP and metric 0. When you put MED(MED=IGP metric) to 1 on PE2 to BR2 as BR1 is anouncing his best route to PE2 with a MED of 0 PE2 will prefer PE1 path

upvoted 3 times

rlilewis 1 year, 6 months ago

The path IS the same because its IBGP on the left side. So the answer is A.

upvoted 2 times

AceRhino 1 year, 7 months ago

Agree (also tested for my peace of mind).

upvoted 2 times

djedeen Most Recent 3 weeks, 4 days ago

Selected Answer: A

A. D is incorrect because the ASes are different on the PE2 so this rules out MED.

upvoted 1 times

msstanick 5 months, 3 weeks ago

Selected Answer: A

I can confirm A worked for me. After changing the metric for the route on PE2, BR2 changed its ip route to go via BR1.

BR2#sh bgp ipv4 uni

Network Next Hop Metric LocPrf Weight Path
* 209.165.201.0/27 209.165.200.230 1 0 200 i
*>i 172.24.109.2 0 100 0 200 i

BR2#sh ip route 209.165.201.0
Routing entry for 209.165.201.0/27, 1 known subnets
B 209.165.201.0 [200/0] via 172.24.109.2, 00:08:00

upvoted 2 times

siyamak 5 months, 3 weeks ago

A is the correct answer only if the comment bgp Always-compare-med is configured.

Synopsis
bgp always-compare-med
no bgp always-compare-med
Configures
BGP route selection

Default
Disabled

Description
This command allows the comparison of the multi-exit discriminator (MED) for paths, regardless of which autonomous system the path comes from.

upvoted 1 times

HarwinderSekhon 6 months, 2 weeks ago

MED is only applicable and useful when we are entering same AS. but here we have two different AS 200, 300 so none of the options are correct. FU$@ this question and person who made it.

upvoted 7 times

CBlu 9 months, 3 weeks ago

A is not correct as for some people it may work who try in the lab and for others it might not.

always compare MED is needed as other have said.

B seems... correct, but weird

C only on local router
D local pref is only for the local AS...

Pretty silly question, imo.

upvoted 2 times

XBfoundX 9 months, 3 weeks ago

The answer in this case is A ONLY if you put the bgp always-compare-med command in BR2.

A: RIGHT ONE
B: nope... remember that the origin code means this:
e: Exterior Gateway Protocol, you will never see this one 'cause it was the protocol before BGP.
i: network announced via the network command
?: network redistributed in BGP

So you they are saying that you need to put the origin code i for a BGP announce that for sure you are receiving via the network command,,,,
Sounds bad right? It will not change nothing at all.

C: Nope the weight attribute is only for the local router, so not good.

D: Nope again, the local preference value can be propagated only to the local AS, so if they were saying to set the BGP local preference to 150 on BR1 in inbound direction it will be right but is not the case. (REMEBER: the LP is ONLY set in INBOUND DIRECTION!)

upvoted 1 times

straightAnswers 8 months ago

XBFoundX,
to adding your information.
LP can influence Inbound direction from any BGP Peer and also Outbound for iBGP peers only.

upvoted 1 times

XBfoundX 9 months, 3 weeks ago

Let's try the B one in lab:

The configuration is the same as shown but of course i used the network command to announce the network 209.165.201.0/27, the topolgy is also the same.

BGP TABLE OF R2

BR2#show ip bgp
Network Next Hop Metric LocPrf Weight Path
*> 172.24.109.0/30 0.0.0.0 0 32768 i
* i 172.24.109.2 0 100 0 i
*> 209.165.201.0/27 209.165.200.230 0 0 300 i
* i 172.24.109.2 0 100 0 200 i

You see that the igp origin is set already..... BUT... let's try....

upvoted 1 times

XBfoundX 9 months, 3 weeks ago

CONFIGURATION THAT YOU NEED TO APPLY TO BR2:

conf t
access-list 1 permit 209.165.201.0 0.0.0.31
route-map Oi2BR2
match ip address 1
set origin igp
route-map Oi2BR2 permit 20
end

conf t
router bgp 100
neighbor 209.165.200.230 route-map Oi2BR2 in
end
clear ip bgp * (in production will reset the TCP session so be careful! use "clear ip bgp * soft in" instead)

BR2#show ip bgp
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 172.24.109.0/30 0.0.0.0 0 32768 i
* i 172.24.109.2 0 100 0 i
*> 209.165.201.0/27 209.165.200.230 0 0 300 i
* i 172.24.109.2 0 100 0 200 i

AMAZING!!! absolutely nothing has changed...

upvoted 1 times

XBfoundX 9 months, 3 weeks ago

Let's try with the right one (A):

Remember that the MED is an attribute that you can ONLY apply in outgoing direction so... We need to apply this config in PE2 in out direction.

CONFIG:

conf t
access-list 1 permit 209.165.201.0 0.0.0.31

route-map MEDchange2BR2 permit 10
match ip address 1
set metric 1
route-map MEDchange2BR2 permit 20

router bgp 300
neighbor 209.165.200.229 route-map MEDchange2BR2 out

upvoted 2 times

XBfoundX 9 months, 3 weeks ago

For refresh the updates coming from PE2 in BR2 do the command clear ip bgp * soft in.
BR2#show ip bgp
Network Next Hop Metric LocPrf Weight Path
*> 172.24.109.0/30 0.0.0.0 0 32768 i
* i 172.24.109.2 0 100 0 i
*> 209.165.201.0/27 209.165.200.230 1 0 300 i
* i 172.24.109.2 0 100 0 200 i
You see that we still prefer the announce via PE2 because in this case the other AS IS NOT THE SAME!!! DO NOT GET CONFUSED!!!!
Remember that the other announce is done by another AS!

upvoted 1 times

XBfoundX 9 months, 3 weeks ago

Our next hop for sure is our ibgp neighbor, but the as that we need to reach is another so for let this happen we need to use this command in BR2 because he will compare the he is the one who compares all the bgp announcements:

BR2:
conf t
router bgp 100
bgp always-compare-med

BR2#show ip bgp
Network Next Hop Metric LocPrf Weight Path
*> 172.24.109.0/30 0.0.0.0 0 32768 i
* i 172.24.109.2 0 100 0 i
* 209.165.201.0/27 209.165.200.230 1 0 300 i
*>i 172.24.109.2 0 100 0 200 i
BR2#

Finally you see that we are installing in routing table the route via PE1 using BR1 as the next-hop.

I hope I was clear and that the examples helped.
See yaa

upvoted 4 times

StefanOT2 10 months, 1 week ago

Selected Answer: B

Answer B
A is wrong. MED is only used when the first hop on the AS Path is identical. In this case, this is not true.

upvoted 1 times

nushadu 10 months, 4 weeks ago

Selected Answer: B

actually, this case is described here, see sec. #5

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html

and why MED "solution" is the wrong answer in this scenario (first AS nums are different) see next sec. #6

upvoted 1 times

Ayman_B 10 months, 4 weeks ago

Selected Answer: A

4) D wrong .. Local preference is the second BGP attribute and is used to choose the exit path for an autonomous system. The BGP preference has to be set inbound on routes being received to influence the outbound routing behaviour.
3) C wrong .. weight used locally on the router.
2) B when set the origin to igp on BR2 toward PE2 inbound. The ORIGIN would prefer the path BR2 -PE2 which is not the goal.
1) A correct answer

upvoted 1 times

ciscokoolaid 11 months ago

This question should be thrown out completely. I believe the correct answer is A BUT in order for that be the case - the following command needs to be added to the BR1 BGP routing process "bgp always-compare-med". The reason for this is that the 209.165.201.0/27 route is being advertised by two different ASs. If both PE1 and PE2 were part of the same AS, then answer A will be correct as it is.

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: B

I've played a lot with this question, set metric (MED) does not work in this case, when I restarted BGP peering\neighbour the BEST route become an older one (it does not matter what MED is) according to BGP Best Path Selection Algorithm #10:
When both paths are external, prefer the path that was received first (the oldest one).

cisco_R3(config-router)#do s runn | s router bgp 3
router bgp 3
bgp router-id 3.3.3.3
bgp log-neighbor-changes
redistribute connected
neighbor 192.168.255.22 remote-as 2
neighbor 192.168.255.22 soft-reconfiguration inbound
neighbor 192.168.255.55 remote-as 5
neighbor 192.168.255.55 soft-reconfiguration inbound
cisco_R3(config-router)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

pay attention to netw 200.200.200.0/24 ,
currently it is BEST via next-hop 192.168.255.55 (5.5.5.5)
and yes, the MED is lower as you see:

cisco_R3(config-router)#do s ip bgp 200.200.200.0
BGP routing table entry for 200.200.200.0/24, version 8
Paths: (2 available, best #2, table default)

Advertised to update-groups:
4
Refresh Epoch 1
2, (received & used)
192.168.255.22 from 192.168.255.22 (2.2.2.2)
Origin incomplete, metric 200, localpref 100, valid, external
rx pathid: 0, tx pathid: 0
Refresh Epoch 1
5, (received & used)
192.168.255.55 from 192.168.255.55 (5.5.5.5)
Origin incomplete, metric 100, localpref 100, valid, external, best
rx pathid: 0, tx pathid: 0x0
cisco_R3(config-router)#do s ip bgp | b 200
* 200.200.200.0 192.168.255.22 200 0 2 ?
*> 192.168.255.55 100 0 5 ?
cisco_R3(config-router)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

reset bgp peering AS5 + debug ip rou:
cisco_R3(config-router)#do clear ip bgp 5
cisco_R3(config-router)#
*Dec 18 17:55:25.080: %BGP-3-NOTIFICATION: sent to neighbor 192.168.255.55 6/4 (Administrative Reset) 0 bytes
*Dec 18 17:55:25.085: %BGP-5-ADJCHANGE: neighbor 192.168.255.55 Down User reset
...
*Dec 18 17:55:25.086: RT: updating bgp 200.200.200.0/24 (0x0) :
via 192.168.255.22 0 1048577

*Dec 18 17:55:25.086: RT: closer admin distance for 200.200.200.0, flushing 1 routes
*Dec 18 17:55:25.086: RT: add 200.200.200.0/24 via 192.168.255.22, bgp metric [20/200]
*Dec 18 17:55:25.905: %BGP-5-ADJCHANGE: neighbor 192.168.255.55 Up
cisco_R3(config-router)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

as you can see the BEST via 2.2.2.2 even with worse MED (200);

cisco_R3(config-router)#do s ip bgp 200.200.200.0
BGP routing table entry for 200.200.200.0/24, version 10
Paths: (2 available, best #2, table default)
Advertised to update-groups:
4
Refresh Epoch 1
5, (received & used)
192.168.255.55 from 192.168.255.55 (5.5.5.5)
Origin incomplete, metric 100, localpref 100, valid, external
rx pathid: 0, tx pathid: 0
Refresh Epoch 1
2, (received & used)
192.168.255.22 from 192.168.255.22 (2.2.2.2)
Origin incomplete, metric 200, localpref 100, valid, external, best
rx pathid: 0, tx pathid: 0x0
cisco_R3(config-router)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

applying route-map with IGP towards 2.2.2.2:
!
ip prefix-list PL_1 seq 10 permit 200.200.200.0/24
ip prefix-list PL_2 seq 10 permit 0.0.0.0/0
!
route-map to_R2 permit 10
match ip address prefix-list PL_1
set origin igp
!
route-map to_R2 permit 20
match ip address prefix-list PL_2
!

upvoted 1 times

nushadu 11 months, 2 weeks ago

sorry, applying to 5.5.5.5, curr conf:
cisco_R3(config-router)#do s runn | s router bgp 3
router bgp 3
bgp router-id 3.3.3.3
bgp log-neighbor-changes
redistribute connected
neighbor 192.168.255.22 remote-as 2
neighbor 192.168.255.22 soft-reconfiguration inbound
neighbor 192.168.255.55 remote-as 5
neighbor 192.168.255.55 soft-reconfiguration inbound
neighbor 192.168.255.55 route-map to_R2 in

cisco_R3(config-router)#do s ip bgp 200.200.200.0
BGP routing table entry for 200.200.200.0/24, version 10
Paths: (2 available, best #2, table default)
Advertised to update-groups:
4
Refresh Epoch 1
5, (received & used)
192.168.255.55 from 192.168.255.55 (5.5.5.5)
Origin incomplete, metric 100, localpref 100, valid, external
rx pathid: 0, tx pathid: 0
Refresh Epoch 1
2, (received & used)
192.168.255.22 from 192.168.255.22 (2.2.2.2)
Origin incomplete, metric 200, localpref 100, valid, external, best
rx pathid: 0, tx pathid: 0x0
cisco_R3(config-router)#

upvoted 1 times

RREVECO 1 year, 2 months ago

Selected Answer: A

The correct answer is A.
(laboratory validated)
BR2#show ip bgp
Network Next Hop Metric LocPrf Weight Path
* i209.165.201.0/27 172.24.109.2 0 100 0 200 i
*> 209.165.200.230 0 0 300 i

upvoted 3 times

Deu_Inder 1 year, 2 months ago

B: by setting the origin to igp on BR2 toward PE2 inbound we are making the route to 209.165.201.0/27 even better.
Consider: O Origin Code (IGP bettern than EGP better than Incomplete)

C: Setting the weight attribute to 65,535 on BR1 toward PE1 wont help as weight will be only local to BR1.

D: Setting the local preference to 150 on PE1 toward BR1 outbound: I have not yet heard of setting local preference outbound.

A: correct answer.

upvoted 1 times

bendarkel 1 year, 3 months ago

Selected Answer: B

The given answer (B) appears to be correct. The Origin BGP attribute is a mandatory BGP attribute like Next-Hop and AS Path. Setting the Origin attribute to IGP on BR2 toward PE2, forces BR2 to choose the path to 209.165.201.0/27 via BR1, which is advertising the prefix with an Origin of EGP which is prefered (EGP over IGP, over ? (Redistribution).

Answer A is wrong because PE1 and PE2 are in different AS.

Answer C is wrong because using the Weight attribute on BR1 toward PE1 is a decision local to BR1, unless BR1 is configured as a route-reflector and BR2 a route-relector client. In such case, Weight can be used to influence the routing decision of all devices in an AS.

Answer D is wrong because Local Preference is not transitive, unless in the case of using Communities to signal devices in another AS. Also, Local Preference is used as an inbound policy to influence outbound routing.

upvoted 4 times

Edwinmolinab 1 year, 4 months ago

Selected Answer: A

We cannot set the local preference on PE1 because local preference is only sent to iBGP neighbors so this attribute cannot reach BR1 -> Answer is not correct.

Weight attribute is only used locally in a router (not be exchanged between BGP neighbors) so we cannot affect BR2 from BR1 with this attribute -> Answer is not correct.

We cannot affect BR2 routing decision by modifying BGP advertisements from BR2 toward PE2 (inbound) -> is not correct. Also if network 209.165.201.0/27 is advertised with “network” statement in BGP, BR2 will match it with origin “IGP”. Please check the example in the link below.

By default, the MED attribute is set to 0 so by increasing the MED on PE2 toward BR2, BR2 would think the metric of its direct link to PE2 is higher than the path advertised by BR1 -> BR2 would use BR1 to reach 209.165.201.0/27.

Good lab example and reference: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13759-37.html

upvoted 4 times

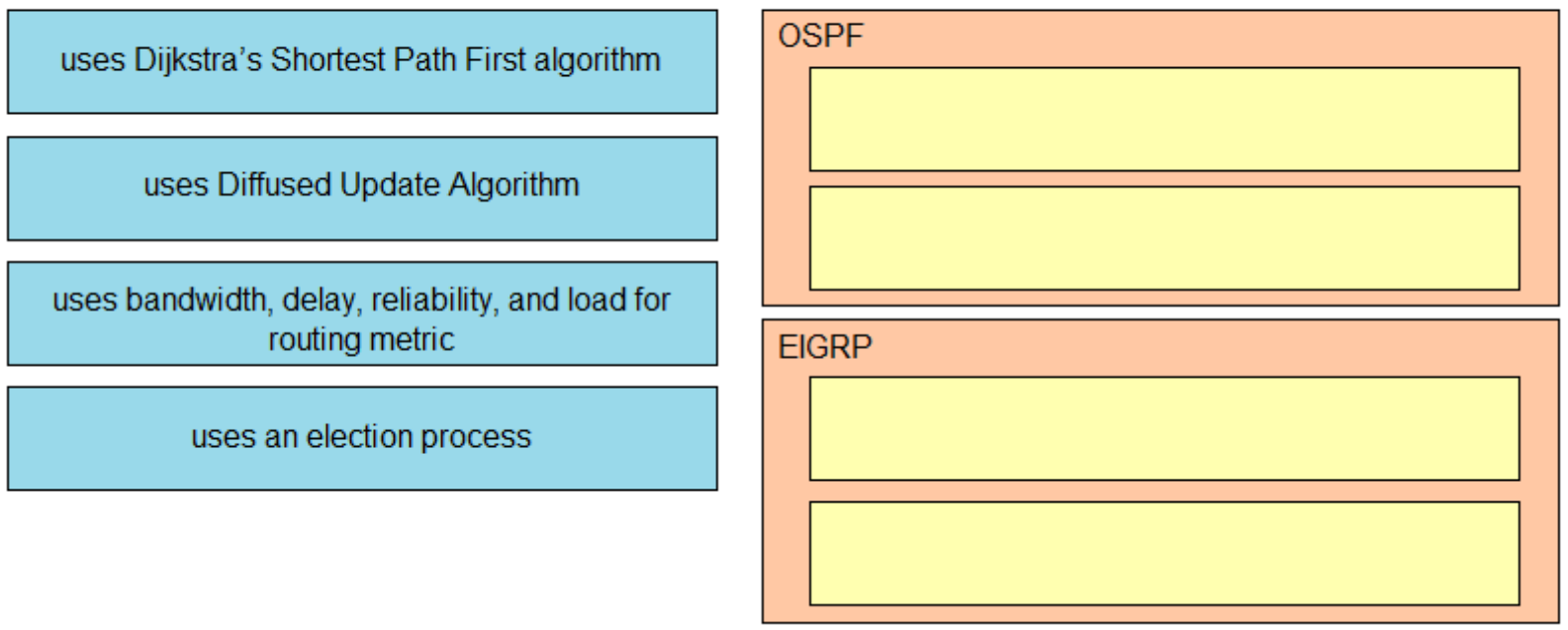
Question #201 *Topic 1*

DRAG DROP -

Drag and drop the characteristics from the left onto the protocols they apply to on the right.

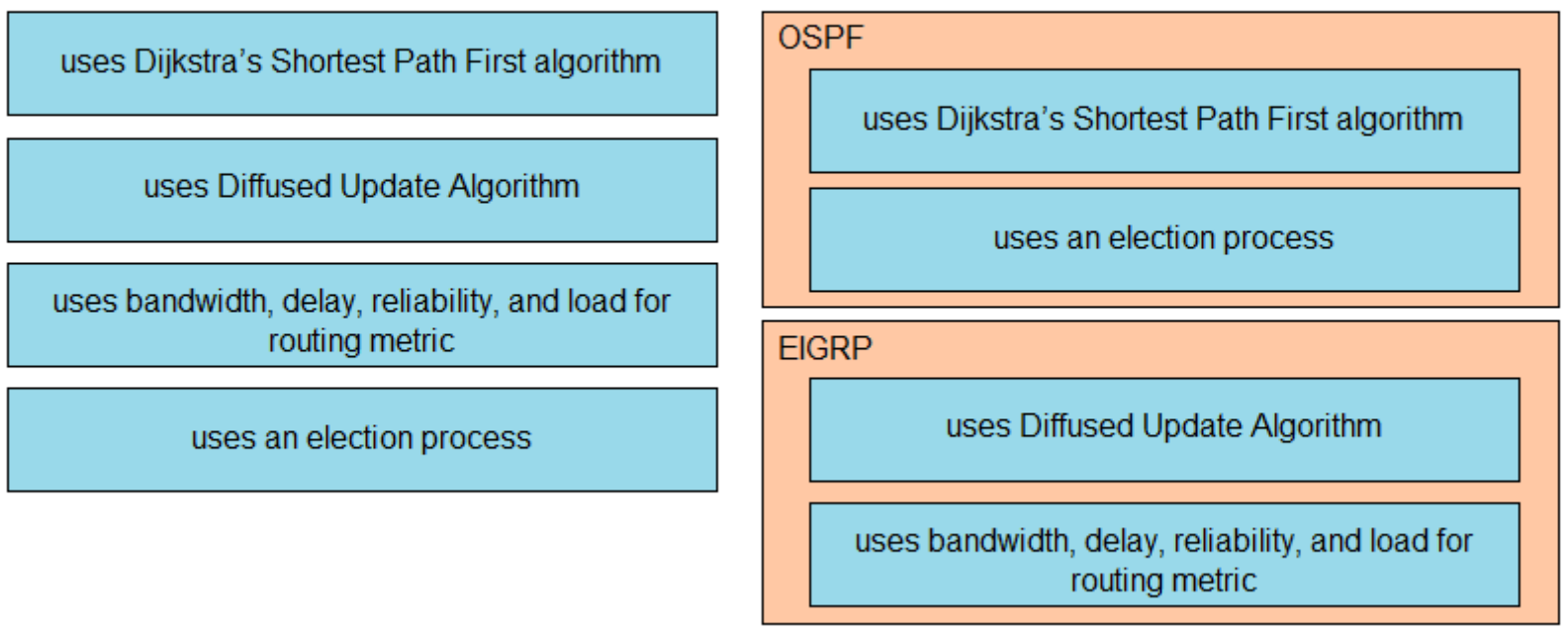
Select and Place:

Answer Area



Correct Answer:

Answer Area

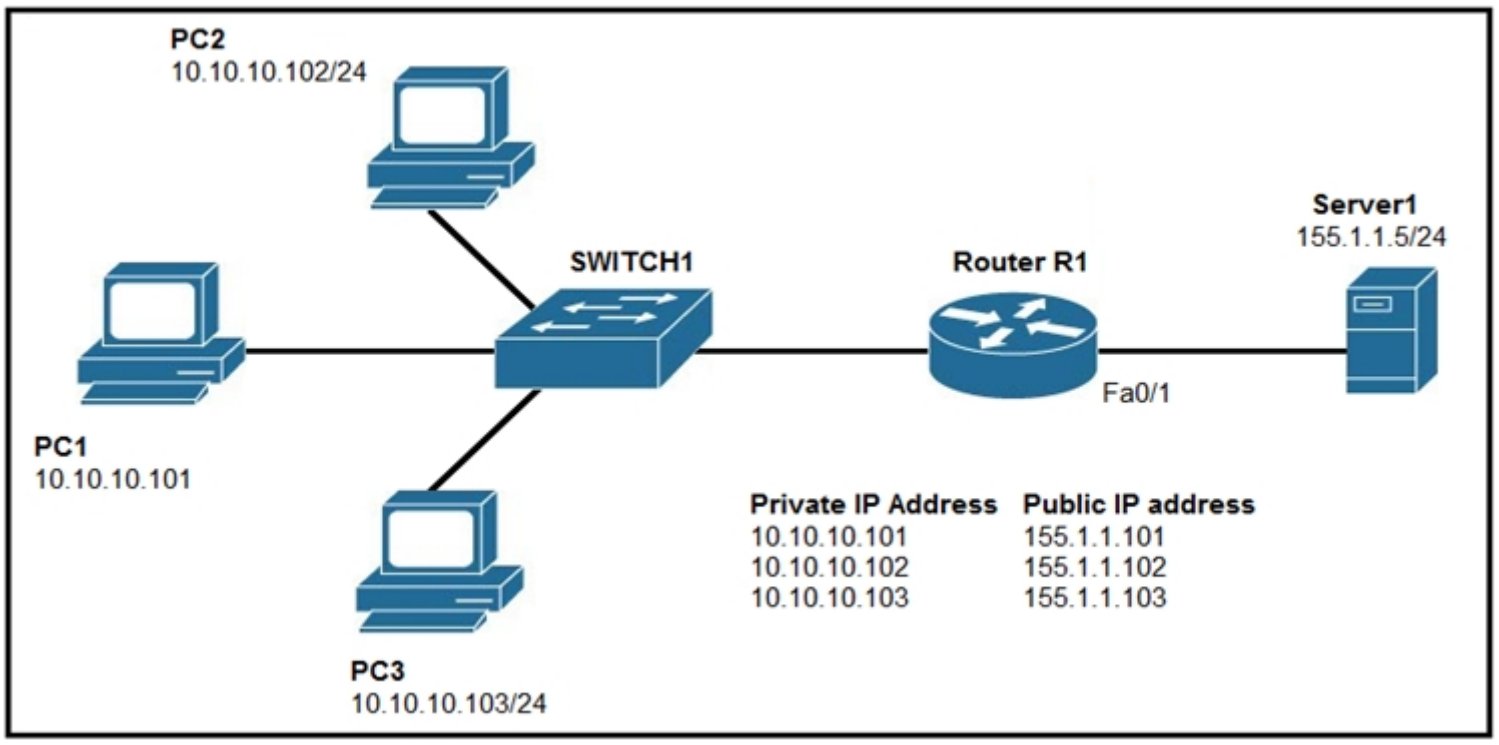


diegodavid82 2 years, 1 month ago

The provided answer is correct.

upvoted 2 times

Question #202 *Topic 1*



Refer to the exhibit. Which set of commands on router R1 allow deterministic translation of private hosts PC1, PC2, and PC3 to addresses in the public space?

A. RouterR1(config)#int f0/0 RouterR1(config)#ip nat inside RouterR1(config)#exit RouterR1(config)#int f0/1 RouterR1(config)#ip nat outside RouterR1(config)#exit RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255 RouterR1(config)#ip nat inside source list 1 interface f0/1 overload

B. RouterR1(config)#int f0/0 RouterR1(config)#ip nat inside RouterR1(config)#exit RouterR1(config)#int f0/1 RouterR1(config)#ip nat outside RouterR1(config)#exit RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255 RouterR1(config)#ip nat pool POOL 155.1.1.101 155.1.1.103 netmask 255.255.255.0 RouterR1(config)#ip nat inside source list 1 pool POOL

C. RouterR1(config)#int f0/0 RouterR1(config)#ip nat inside RouterR1(config)#exit RouterR1(config)#int f0/1 RouterR1(config)#ip nat outside RouterR1(config)#exit RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101 RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102 RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103

D. RouterR1(config)#int f0/0 RouterR1(config)#ip nat outside RouterR1(config)#exit RouterR1(config)#int f0/1 RouterR1(config)#ip nat inside RouterR1(config)#exit RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101 RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102 RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103

Correct Answer: *C*

Community vote distribution

C (100%)

GATUNO Highly Voted 2 years ago

deterministic means static , tricky question

upvoted 8 times

xziomal9 Highly Voted 2 years, 2 months ago

C.
RouterR1(config)#int f0/0
RouterR1(config)#ip nat inside
RouterR1(config)#exit
RouterR1(config)#int f0/1
RouterR1(config)#ip nat outside
RouterR1(config)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102
RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103
D.
RouterR1(config)#int f0/0
RouterR1(config)#ip nat outside
RouterR1(config)#exit
RouterR1(config)#int f0/1
RouterR1(config)#ip nat inside
RouterR1(config)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102
RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103

upvoted 6 times

Manicardi Most Recent 1 month, 4 weeks ago

Selected Answer: C

deterministic means static

upvoted 1 times

Dataset 6 months ago

"deterministic" is the magic word
C is correct
Regards

upvoted 2 times

bk989 7 months, 2 weeks ago

It is C. D will do the translations in the opposite direction. The NAT pool works for B, however doesn't guarantee a deterministic translation.

upvoted 1 times

bora4motion 1 year ago

Selected Answer: C

C is correct

upvoted 2 times

iGlitch 1 year, 1 month ago

Although it has typos and is poorly written, the keyword here is "Deterministic" so it should be a static translation, Answer C is correct.

upvoted 2 times

Bruno305 1 year, 9 months ago

Selected Answer: C

Provided answer is correct

upvoted 2 times

brightsyds 1 year, 9 months ago

C for sure!

RouterR1(config)#int f0/0
RouterR1(config)#ip nat inside
RouterR1(config)#exit
RouterR1(config)#int f0/1
RouterR1(config)#ip nat outside
RouterR1(config)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102
RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103

upvoted 5 times

Jaaason 1 year, 11 months ago

Provided answer is correct

upvoted 1 times

xziomal9 2 years, 2 months ago

A.
RouterR1(config)#int f0/0
RouterR1(config)#ip nat inside
RouterR1(config)#exit
RouterR1(config)#int f0/1
RouterR1(config)#ip nat outside
RouterR1(config)#exit
RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255
RouterR1(config)#ip nat inside source list 1 interface f0/1 overload
B.
RouterR1(config)#int f0/0
RouterR1(config)#ip nat inside
RouterR1(config)#exit
RouterR1(config)#int f0/1
RouterR1(config)#ip nat outside
RouterR1(config)#exit
RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255
RouterR1(config)#ip nat pool POOL 155.1.1.101 155.1.1.103 netmask 255.255.255.0
RouterR1(config)#ip nat inside source list 1 pool POOL

upvoted 5 times

Babushka 2 years, 2 months ago

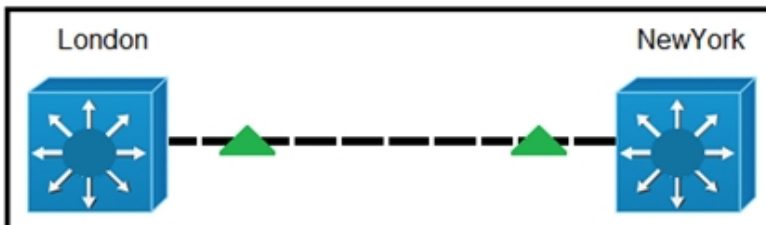
Provided answer is correct, A is for overload, B has syntax error on ACL, and D has wrong NAT zone. FA0/1 is outside not inside.

upvoted 3 times

diegodavid82 2 years, 1 month ago

I agree, the correct answer is C.
When telling us "deterministic translation" is like a static translation.

upvoted 1 times




```
London(config)#interface range fa0/1-2
London(config-if-range)#switchp trunk encapsulation dot1q
London(config-if-range)#switchp mode trunk
London(config-if-range)#channel-group 1 mode active
London(config-if-range)#end
London#
```

```
NewYork#show etherchannel summary
Flags:  D - down         P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group Port-channel   Protocol    Ports
------------------------------------------------------------------------
1     Po1(SD)            PAgP   Fa0/1(I) Fa0/2(D)
NewYork#
NewYork#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------
Port-channel: Po1
------------
Age of the Port-channel   = 00d:00h:14m:20s
Logical slot/port   = 2/1       Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel |
Protocol            =   PAGP
Port Security       = Disabled
```

Refer to the exhibit. Communication between London and New York is down. Which command set must be applied to the NewYork switch to resolve the issue?

A. NewYork(config)#no interface po1 NewYork(config)#interface range fa0/1-2 NewYork(config-if)#channel-group 1 mode negotiate NewYork(config-if)#end NewYork#

B. NewYork(config)#no interface po1 NewYork(config)#interface range fa0/1-2 NewYork(config-if)#channel-group 1 mode on NewYork(config-if)#end NewYork#

C. NewYork(config)#no interface po1 NewYork(config)#interface range fa0/1-2 NewYork(config-if)#channel-group 1 mode passive NewYork(config-if)#end NewYork#

D. NewYork(config)#no interface po1 NewYork(config)#interface range fa0/1-2 NewYork(config-if)#channel-group 1 mode auto NewYork(config-if)#end NewYork#

Correct Answer: *C*

Community vote distribution

C (75%) D (25%)

SandyIndia Highly Voted 2 years, 2 months ago

LACP Port Negotiation
1) Active - Passive
2) Active - Active
3) ON - ON

upvoted 12 times

Haidary Most Recent 3 weeks, 2 days ago

C is correct
As we have LACP on the London side. Then we have to remove the PAgp on the NY side and configure it as passive for LACP. Active and Passive are forming etherchannel for LACP.

upvoted 1 times

bk989 7 months, 2 weeks ago

Answer is C. New York is currently in PAgp mode, and London has been configured as LACP. So we need to change NewYork to LACP, which makes the answer C.

upvoted 2 times

Pilgrim5 7 months, 2 weeks ago

Selected Answer: D

I think the ans should be D.

LACP - Active/Passive.
PAGP - Desirable/auto.

upvoted 1 times

danman32 4 months, 3 weeks ago

Right, so answer D won't work, since for D, you're setting it back to PaGp which has been the problem all along. London is Active (LACP) so NY also has to be LACP

upvoted 2 times

RShrestha 8 months, 4 weeks ago

both switch has to have the same protocol one is on LACP and other one in PaGP how can they form a ether channel?

upvoted 2 times

felix_simon 10 months, 2 weeks ago

London is LACP Protocol, NewYork is PAgP Protocol. None of the answers are correct.

upvoted 3 times

danman32 4 months, 3 weeks ago

Right, so that's why for NY, which all answers have you reconfigure, you want to set as LACP, which answer C does.
Granted C has it set to passive, but London is active so that's OK.

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: C

!
interface Ethernet0/1
description to_e0/1_SW2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1-9,11-4094
switchport mode trunk
duplex auto
channel-group 2 mode passive
!

upvoted 2 times

nushadu 11 months, 2 weeks ago

peer:
sw2(config-if)#do s runn interface Ethernet0/1
Building configuration...

Current configuration : 157 bytes
!
interface Ethernet0/1
description to_e0/1_SW1
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
channel-group 2 mode active
end

sw2(config-if)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw2#show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+---
2 Po2(SU) LACP Et0/1(P)

sw2#

upvoted 1 times

bora4motion 1 year ago

Selected Answer: C

C is correct
upvoted 1 times

Jaaason 1 year, 11 months ago
Provided answer is correct
upvoted 1 times

Kayyye 2 years ago
Provided answer is correct
upvoted 1 times

Nhan 2 years, 2 months ago
The given answer is correct, also we can set the mode to active, active-active , also can form po1
upvoted 3 times

kthekillerc 2 years, 2 months ago
Provided answer is correct
upvoted 1 times

Scav20 2 years, 2 months ago
I´ve finally found the correct answer for this question
upvoted 1 times

TTTTTT 2 years, 3 months ago
Active/Pasive will work... provided ans is correct
upvoted 1 times

```
Switch2#
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/23, putting Fa0/23 in err-disable
state
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/24, putting Fa0/24 in err-disable
state
Switch2#

Switch1#show etherchannel summary

!output omitted

Group  Port-channel  Protocol    Ports
------------------------------------------
1      Po2(SD)          LACP      Fa1/0/23(D)


Switch2#show etherchannel summary

!output omitted

Group  Port-channel  Protocol    Ports
------------------------------------------------------------
1      Po1(SD)          -         Fa0/23(D)     Fa0/24(D)
```

Refer to the exhibit. An engineer is configuring an EtherChannel between Switch1 and Switch2 and notices the console message on Switch2. Based on the output, which action resolves this issue?

A. Configure more member ports on Switch1.

B. Configure less member ports on Switch2.

C. Configure the same port channel interface number on both switches.

D. Configure the same EtherChannel protocol on both switches.

Correct Answer: *D*

Community vote distribution

D (100%)

ChristinaA Highly Voted 1 year, 6 months ago

Selected Answer: D

Protocol on Switch 2 is "-" which means it's been set to use "on", i.e. not LACP (active/passive) or PAgP (desirable/auto). In other words, it's not using the same etherchannel protocol.

upvoted 8 times

charafDZ Most Recent 9 months ago

1/ The Etherchannel group numbers are locally significant to the appliance and they do not need to match.

2/ EtherChannel modes :
PAgP Mode
LACP Mode
ON Mode

upvoted 2 times

nushadu 11 months, 2 weeks ago

Selected Answer: D

sw2(config-if)#do s runn interface Ethernet0/1
Building configuration...

Current configuration : 153 bytes
!
interface Ethernet0/1
description to_e0/1_SW1
switchport trunk encapsulation dot1q
switchport mode trunk

duplex auto
channel-group 2 mode on
end

sw2(config-if)#do s etherch su | b Proto
Group Port-channel Protocol Ports
------+------------+-----------+---
2 Po2(SU) - Et0/1(P)

sw2(config-if)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

far-end in DOWN state:
sw1#sh int po2 | i proto
Port-channel2 is down, line protocol is down (notconnect)
0 unknown protocol drops
sw1#sh int status | i PO2
sw1#sh int status | i Po2
Po2 notconnect trunk auto auto
sw1#show etherchannel summary | b Proto
Group Port-channel Protocol Ports
------+------------+-----------+---
1 Po1(SD) -
2 Po2(SD) LACP Et0/1(s)

sw1#

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw1# sh run int e0/1
Building configuration...

Current configuration : 201 bytes
!
interface Ethernet0/1
description to_e0/1_SW2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1-9,11-4094
switchport mode trunk
duplex auto
channel-group 2 mode passive
end

sw1#

upvoted 1 times

nushadu 11 months, 2 weeks ago

solution:
sw2(config-if)#do s runn interface Ethernet0/1
Building configuration...

Current configuration : 153 bytes
!
interface Ethernet0/1
description to_e0/1_SW1
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
channel-group 2 mode on
end

sw2(config-if)#no channel-group 2 mode on
sw2(config-if)#
sw2(config-if)#channel-group 2 mode active
sw2(config-if)#
*Dec 18 19:36:51.084: %LINK-3-UPDOWN: Interface Port-channel2, changed state to up
*Dec 18 19:36:52.087: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to up
sw2(config-if)#

upvoted 1 times

bora4motion 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

kimo1234 1 year, 4 months ago

What about number of ports configured on each side?

upvoted 2 times

Neil101 1 year, 3 months ago

Port channel will still come up using the same etherchannel protocol on both switches - even if the number of ports on each side doesn't match. i.e. Number of ports doesn't need to match.

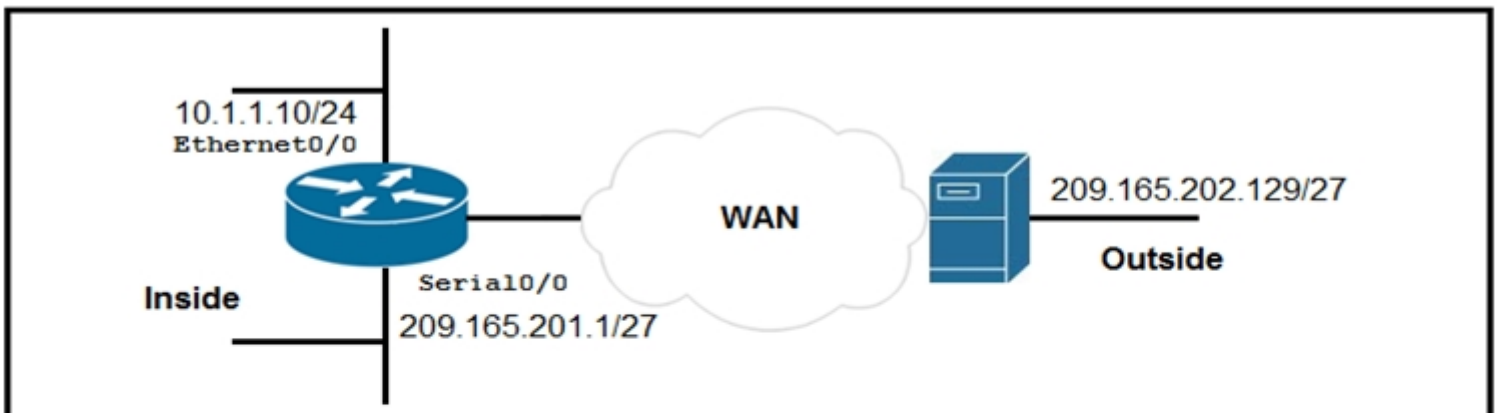
upvoted 4 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

Question #205 *Topic 1*




```
R1
interface Ethernet0/0
ip address 10.1.1.10 255.255.255.0
ip nat inside
!
interface Serial0/0
ip address 209.165.201.1 255.255.255.224
ip nat outside
!
ip nat pool Busi 209.165.201.1 209.165.201.2 netmask 255.255.255.252
ip nat inside source list 1 pool Busi
!
access-list 1 permit 10.1.1.0 0.0.0.255
!

R1# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 0 extended)
Outside interface:
Serial0/0
Inside interfaces:
Ethernet0/0
Hits: 119 Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool Busi refcount 1
pool fred: netmask 255.255.255.252
start 209.165.201.1 end 209.165.201.2
type generic, total addresses 2, allocated 1 (50%), misses 0
!
```

Refer to the exhibit. A network engineer configures NAT on R1 and enters the show command to verify the configuration. What does the output confirm?

A. The first packet triggered NAT to add an entry to the NAT table.

B. R1 is configured with NAT overload parameters.

C. A Telnet session from 160.1.1.1 to 10.1.1.10 has been initiated.

D. R1 is configured with PAT overload parameters.

Correct Answer: *A*

Community vote distribution

A (100%)

Pilgrim5 7 months, 3 weeks ago

Selected Answer: A

B - Wrong as the configuration is not that of NAT overload.

D - Wrong as the configuration is not that of port access translation (PAT).
Note that PAT is the same as NAT Overload.

C - The output provided doesn't show evidence of a TCP connection.

A- Right as the last line of the output shows that one of the outside global addresses is in use.

upvoted 3 times

Zikosheka 1 year, 2 months ago

Selected Answer: A

The answer is A.

upvoted 1 times

diegodavid82 2 years, 1 month ago

The provided answer is fine. The answer is A.

upvoted 1 times

Question #206 *Topic 1*

```
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.2 on FastEthernet0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
%OSPF-6-AREACHG: 10.0.0.1/32 changed from area 0 to area 1
%OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from
backbone area must be virtual-link but not found from 10.0.0.2,
FastEthernet0/0
```

Refer to the exhibit. What is the cause of the log messages?

A. OSPF area change

B. MTU mismatch

C. IP address mismatch

D. hello packet mismatch

Correct Answer: *A*

Community vote distribution

A (91%) 9%

Jared28 Highly Voted 1 year, 5 months ago

Selected Answer: A

Due to the conflicting opinions here I tested it in GNS3. I tried altering the MTU, hello timers and the area. The only one that produced this problem is the area change.

upvoted 12 times

Brand 9 months, 1 week ago

dear sir, you just won the internet.

upvoted 2 times

CCNPWILL Most Recent 1 month, 1 week ago

OBVIO...

upvoted 1 times

flash007 4 months, 1 week ago

the error mentions area many times so this is the big clue here

upvoted 1 times

kewokil120 11 months ago

Selected Answer: A

Area mismatch. Should not even have to lab this for a ccnp test. Area need to be same for neighborship

upvoted 2 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

cisco_R3(config-router)#network 192.168.255.3 0.0.0.0 area 1
cisco_R3(config-router)#
*Dec 18 19:46:09.590: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.255.2 on Ethernet0/0.10 from FULL to DOWN, Neighbor Down: Interface down or detached
cisco_R3(config-router)#
*Dec 18 19:46:09.590: %OSPF-6-AREACHG: 192.168.255.3/32 changed from area 0 to area 1
cisco_R3(config-router)#
*Dec 18 19:46:14.061: %OSPF-4-ERRRCV: Received invalid packet: mismatched area ID from backbone area from 192.168.255.2, Ethernet0/0.10
cisco_R3(config-router)#
*Dec 18 19:46:23.896: %OSPF-4-ERRRCV: Received invalid packet: mismatched area ID from backbone area from 192.168.255.2, Ethernet0/0.10
cisco_R3(config-router)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

cisco_R3(config-router)#do s runn | s ospf
router ospf 1
passive-interface default
no passive-interface Ethernet0/0.10
network 192.168.255.3 0.0.0.0 area 1
network 0.0.0.0 255.255.255.255 area 0
cisco_R3(config-router)#

upvoted 1 times

nushadu 11 months, 2 weeks ago

cisco_R3(config-router)#no network 192.168.255.3 0.0.0.0 area 1
cisco_R3(config-router)#
*Dec 18 19:48:21.676: %OSPF-6-AREACHG: 192.168.255.3/32 changed from area 1 to area 0
cisco_R3(config-router)#
*Dec 18 19:48:21.752: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.255.2 on Ethernet0/0.10 from LOADING to FULL, Loading Done
cisco_R3(config-router)#

upvoted 1 times

bora4motion 1 year ago

Selected Answer: A

MTU can take down an OSPF adjacency but you won't see that in the log. It's A.

upvoted 1 times

YTAKE 1 year, 5 months ago

Wow,

Yes, the root cause is area change. And this log message is not generated because of area change configuration. It is because of the reception of the Hello Packet.

I was tricked too, so I believe the answer is D.

But this message is

upvoted 1 times

YTAKE 1 year, 5 months ago

Looking more closely again:

---- there are three facilities that generated, particullarly:
1 --- AREACHG: for configuration change of the area
2 --- ERRRCV: for the hello packet

It is confusing, take your chance

upvoted 1 times

YTAKE 1 year, 5 months ago

A and B

this is one of the BS questions

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: A

with hello packets the information is arrived!

upvoted 1 times

Eddgar0 1 year, 7 months ago

Selected Answer: A

I think A is correct and not D, because is asking for the "cause" of the log, and the cause of the log was triggered by an area change, the consecuence of the event cause a drop of adjacency.

upvoted 2 times

Opimon007 1 year, 7 months ago

Selected Answer: A

area change

upvoted 1 times

diegodavid82 1 year, 9 months ago

Selected Answer: D

Into the hello packet is the area ID, the area ID must be matched between peers to establish a relationship. In this way, a mismatch of the hello packet is the correct answer for me.

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 3 times

Question #207 *Topic 1*

A network engineer configures BGP between R1 and R2. Both routers use BGP peer group CORP and are set up to use MD5 authentication. This message is logged to the console of router R1:
`May 5 39:85:55.469: %TCP-6-BADAUTH` Invalid MD5 digest from 10.10.10.1 (29832) to 10.120.10.1 (179) tebleid -0
Which two configurations allow a peering session to form between R1 and R2? (Choose two.)

A. R1(config-router)#neighbor 10.10.10.1 peer-group CORP R1(config-router)#neighbor CORP password Cisco

B. R2(config-router)#neighbor 10.120.10.1 peer-group CORP R2(config-router)#neighbor CORP password Cisco

C. R2(config-router)#neighbor 10.10.10.1 peer-group CORP R2(config-router)#neighbor PEER password Cisco

D. R1(config-router)#neighbor 10.120.10.1 peer-group CORP R1(config-router)#neighbor CORP password Cisco

E. R2(config-router)#neighbor 10.10.10.1 peer-group CORP R2(config-router)#neighbor CORP password Cisco

Correct Answer: *AB*

Community vote distribution

AB (83%) DE (17%)

hex2 Highly Voted 1 year, 10 months ago

Answer is correct, AB. The question states the console output is from R1, which means that R1 is 10.120.10.1, and R2 is 10.10.10.1. If you missed that you may have assumed the reverse and picked DE.

upvoted 17 times

LanreDipeolu 3 months, 2 weeks ago

I think ED choice is more appropriate; all because the syslog message was obtained from R1 that indicated R1 is 10.10.0.1

upvoted 3 times

bk989 6 months, 2 weeks ago

because R1 is 10.120.10.1, according to the error message which states TCP port 179, which is DESTINATION port for BGP, hence A, B are the only possible answers in this case. The destination port 179 is referring to the incoming router 10.120.1.x

upvoted 5 times

SandyIndia Highly Voted 2 years, 1 month ago

if the two routers have different passwords configured, a message such as this is displayed:
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:179
https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/112188-configure-md5-bgp-00.html

upvoted 7 times

LanreDipeolu Most Recent 3 months, 2 weeks ago

Selected Answer: DE

I think ED choice is more appropriate; all because the syslog message was obtained from R1 that indicated R1 is 10.10.0.1

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

R1 is configured with the IP 10.10.10.1 while R2 is configured with 10.120.10.1. This is noticeable because BGP speaks over port 179. So the destination port is attached to the destination IP as noted in the error log. This way we can determine the destination IP is accurate (B).

upvoted 1 times

due 4 months, 2 weeks ago

i think alarm TCP-6-BADAUTH` Invalid MD5 digest.
the local router in inspector and found that Invalid.
Local router should be destination (port 179).
So, local router R1 is 10.120

upvoted 1 times

Leoveil 4 months, 4 weeks ago

Selected Answer: AB

(29832) random port number represent source.
(179) BGP default port number represent destination.

upvoted 2 times

nushadu 11 months, 2 weeks ago

Selected Answer: AB

cisco_R2#show running-config | section bgp
router bgp 2
bgp router-id 2.2.2.2
bgp log-neighbor-changes

neighbor GR_AS3 peer-group
neighbor GR_AS3 remote-as 3
neighbor GR_AS3 password cisco
neighbor 192.168.255.3 peer-group GR_AS3
!
address-family ipv4
redistribute connected
neighbor 192.168.255.3 activate
neighbor 192.168.255.3 soft-reconfiguration inbound
exit-address-family
cisco_R2#

upvoted 1 times

nushadu 11 months, 2 weeks ago

cisco_R3#show running-config | section bgp
router bgp 3
bgp router-id 3.3.3.3
bgp log-neighbor-changes
neighbor GR_AS2 peer-group
neighbor GR_AS2 remote-as 2
neighbor GR_AS2 password 7 1511021F0725
neighbor 192.168.255.22 peer-group GR_AS2
neighbor 192.168.255.55 remote-as 5
!
address-family ipv4
redistribute connected
neighbor GR_AS2 soft-reconfiguration inbound
neighbor 192.168.255.22 activate
neighbor 192.168.255.55 activate
neighbor 192.168.255.55 soft-reconfiguration inbound
neighbor 192.168.255.55 route-map to_R5 in
exit-address-family
cisco_R3#

upvoted 1 times

nushadu 11 months, 2 weeks ago

cisco_R3#show ip bgp summary | b Nei
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
192.168.255.22 4 2 9 14 44 0 0 00:04:14 3
192.168.255.55 4 5 42 59 44 0 0 00:32:39 3
cisco_R3#

upvoted 1 times

bora4motion 1 year ago

Selected Answer: AB

A,B is correct. The log is on R1.

upvoted 2 times

Qiaopuyun 1 year ago

I confused, the TCP destination port is 179 and source port is dynamic. so the ip address for R1 is 10.10.10.1

upvoted 2 times

Japsurd 1 year ago

Answer is correct. The port number used (179) also gives it away. But Cisco asking so many questions that are not in the OCG is breaking my spirit.

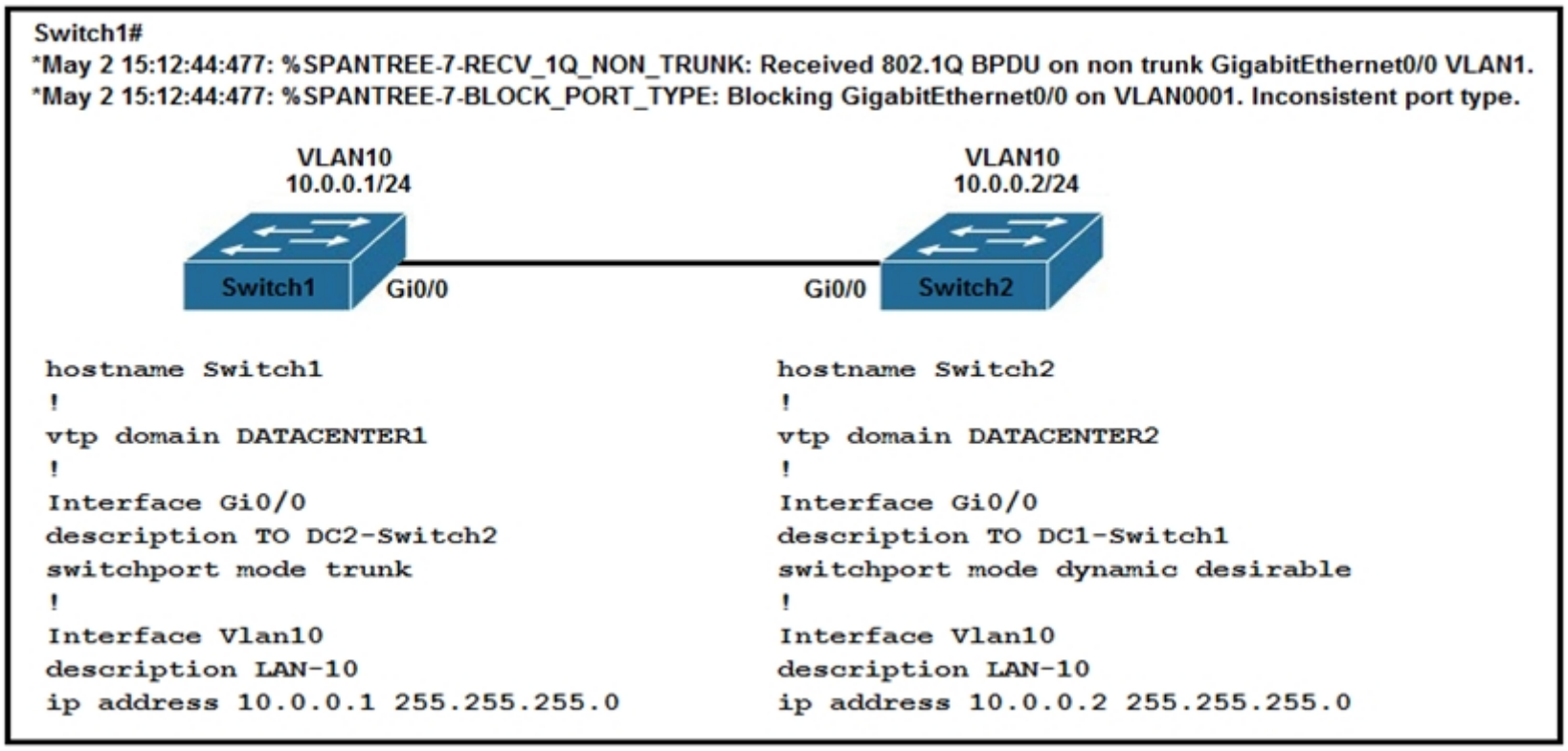
upvoted 2 times

rpidcock 2 years, 2 months ago

Given answer is correct. Verified in GNS3 lab.

upvoted 4 times

Question #208 *Topic 1*



Refer to the exhibit. An engineer implemented several configuration changes and receives the logging message on Switch1. Which action should the engineer take to resolve this issue?

A. Change Switch2 to switch port mode dynamic auto.

B. Change the VTP domain to match on both switches.

C. Change Switch1 to switch port mode dynamic auto.

D. Change Switch1 to switch port mode dynamic desirable.

Correct Answer: *B*

Community vote distribution

B (75%) D (25%)

error_909 Highly Voted 2 years, 2 months ago

Data Traffic Blocked between VTP Domains
Sometimes it is required to connect to switches that belong to two different VTP domains. For example, there are two switches called Switch1 and Switch2. Switch1 belongs to VTP domain cisco1 and Switch2 belongs to VTP domain cisco2. When you configure trunk between these two switches with the Dynamic Trunk Negotiation (DTP), the trunk negotiation fails and the trunk between the switches does not form, because the DTP sends the VTP domain name in a DTP packet. Because of this, the data traffic does not pass between the switches.

https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98155-tshoot-vlan.html#topic5

upvoted 21 times

mgiuseppe86 Highly Voted 2 months, 3 weeks ago

Cisco needs to pretend VTP Never existed. No one.. NO ONE uses VTP. It's career suicide

upvoted 5 times

myhdtv6 Most Recent 4 months, 2 weeks ago

Selected Answer : B

Look at the answers
Trunk <--> Dynamic Desirable = Trunk (always)

so the negotiation mode has nothing to do with Trunk is not getting formed, it is something else.

and something else is the VTP domain.

upvoted 1 times

danman32 4 months, 3 weeks ago

This is what bothers me:
Error is reported on SW1 saying that G0/0 is not a trunk but received trunk BPDU from SW2.
That would make sense if SW1 G0/0 were dynamic but it is static Trunk, it doesn't need DTP from SW2 to make it trunk.
Now if the error was shown on SW2, that would make sense if VTP is required for DTP to be received. Without a valid DTP from the other side (from SW1), it would go to access mode.

upvoted 1 times

rami_mma 8 months, 1 week ago

If you are expecting trunk negotiation then both switch should belong to the same domain.
All proposed option offer dynamic mode and this will not work if both side do not belong to the same vtp domain.
upvoted 2 times

Clauster 8 months, 3 weeks ago

Dynamic Desirable and Trunk manual will always trunk, you don't need to add dynamic desirable to the other switch.
upvoted 2 times

Opreis 9 months ago

Selected Answer: B

Answer is correct, vtp domain needs to match
upvoted 1 times

bendarkel 10 months, 4 weeks ago

Selected Answer: B

B is correct. A VTP domain mismatch will break trunking.
upvoted 1 times

kewokil120 11 months ago

Selected Answer: B

https://www.google.com/url?sa=i&url=https%3A%2F%2Fnetworkjutsu.com%2Fdynamic-trunking-protocol%2F&psig=AOvVaw1FZqtzUJIajw02NTajqcuM&ust=1672506569079000&source=images&cd=vfe&ved=0CA8QjRxqFwoTCNDd7dDqofwCFQAAAAAdAAAAABAE
upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: D

unfortunately, I do not have this feature in my lab:

sw1(config-if)#switchport mode ?
access Set trunking mode to ACCESS unconditionally
dot1q-tunnel set trunking mode to TUNNEL unconditionally
trunk Set trunking mode to TRUNK unconditionally

sw1(config-if)#switchport mode

but I've played with changing the VTP domain name and this did not trigger an error from the question, I think this is a TRUNK issue, so we need to establish trunk here first ...
upvoted 2 times

Aldebeer 1 year, 7 months ago

Selected Answer: B

DTP requires that the VTP domain match between the two switches.
upvoted 3 times

rpidcock 2 years, 2 months ago

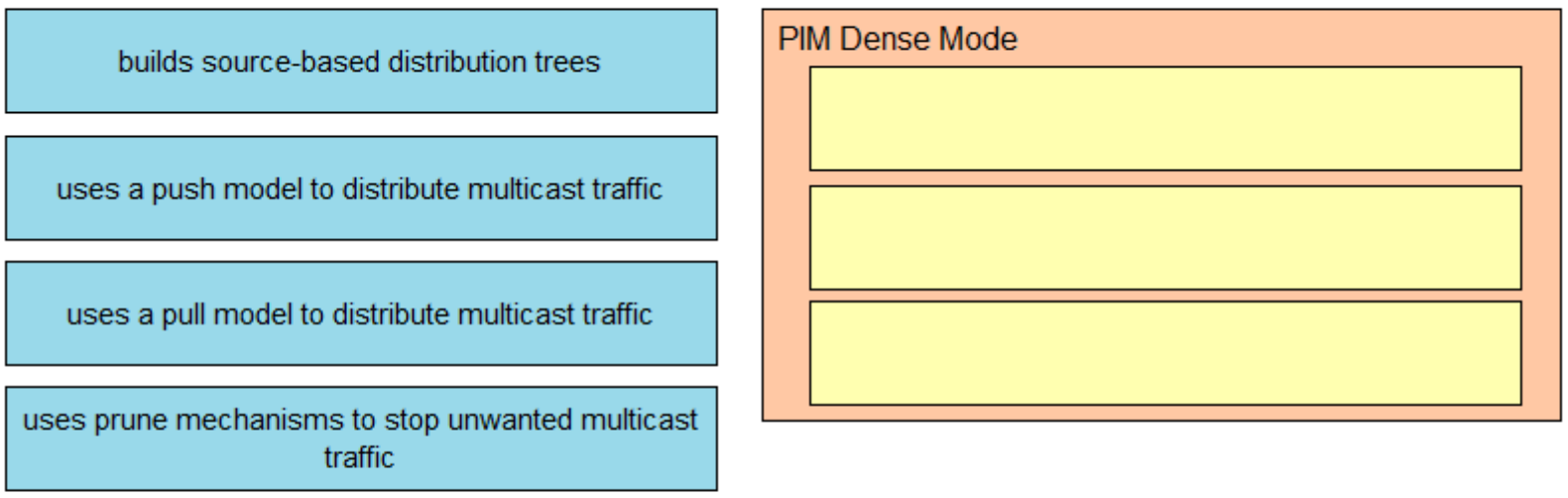
Given answer is correct. Verified in GNS3 lab.
upvoted 4 times

DRAG DROP -

Drag and drop the characteristics of PIM Dense Mode from the left to the right. Not all options are used.

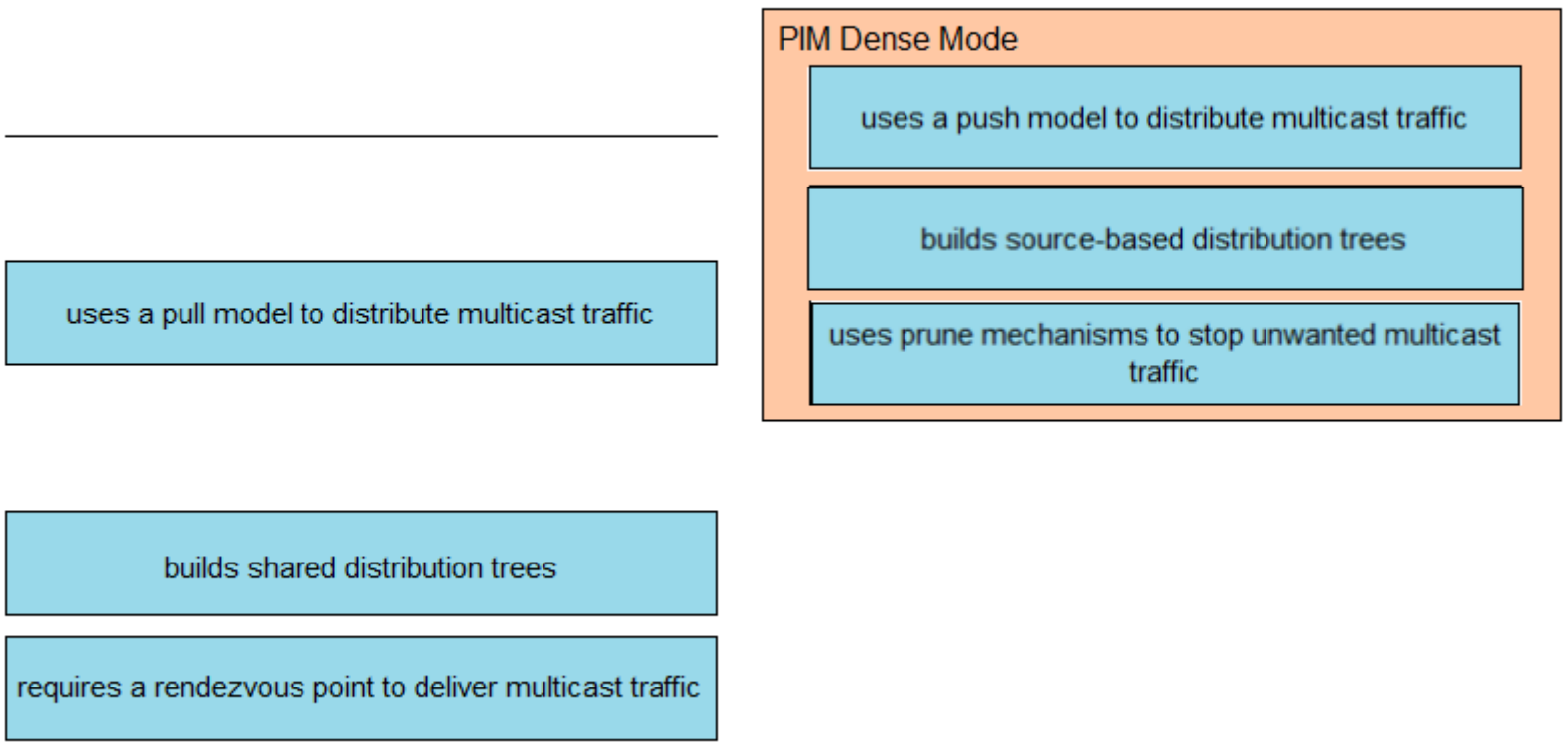
Select and Place:

Answer Area



Correct Answer:

Answer Area



kthekillerc Highly Voted 2 years, 2 months ago

Provided answer is correct

upvoted 7 times

DRAG DROP -

Drag and drop the wireless elements on the left to their definitions on the right.

Select and Place:

Answer Area

beamwidth	a graph that shows the relative intensity of the signal strength of an antenna within its space
polarization	the relative increase in signal strength of an antenna in a given direction
radiation patterns	measures the angle of an antenna pattern in which the relative signal strength is half-power below the maximum value
gain	radiated electromagnetic waves that influence the orientation of an antenna within its electromagnetic field

Correct Answer:

Answer Area

radiation patterns

gain

beamwidth

polarization

kthekillerc Highly Voted 2 years, 2 months ago

Provided answer is correct

upvoted 5 times

[Removed] Most Recent 5 months ago

correct

upvoted 1 times

Jared28 1 year, 5 months ago

Wouldn't be this (excerpts from the official guide, #2 and #4 I'm not as sure on):
1. Gain - In other words, the gain of an antenna is a measure of how effectively it can focus RF energy in a certain direction.

2. Radiation Patterns: Between 2 and 4 I was unsure for this one but the fact they spend a lot of time talking about graphing it, this felt best in #2.

3. Beamwidth: The beamwidth is determined by finding the strongest point on the plot, which is usually somewhere on the outer circle. Next, the plot is followed in either direction until the value decreases by 3 dB, indicating the point where the signal is one-half the strongest power.

4. Polarization: The electrical field wave's orientation, with respect to the horizon, is called the antenna polarization.

upvoted 2 times

Jared28 1 year, 5 months ago

NM given answer correct, I mixed up #1 and 2 when I wrote the. The excerpts still fit though, just first radiation, gain, beam, polar

upvoted 2 times

Question #211 *Topic 1*

How are the different versions of IGMP compatible?

A. IGMPv2 is compatible only with IGMPv2.

B. IGMPv3 is compatible only with IGMPv3.

C. IGMPv2 is compatible only with IGMPv1.

D. IGMPv3 is compatible only with IGMPv1

Correct Answer: *C*

Community vote distribution

C (100%)

Claudiu1 2 weeks, 1 day ago

this question is downright idiotic

upvoted 1 times

wr4net 6 months, 2 weeks ago

if v3 is compatible with v2, then doesn't this imply that v2 is in some way able to work with v3, so it's too compatible with v3? seems like a stupid question. the only good answer is C though, so i agree with that.

upvoted 2 times

danman32 4 months, 3 weeks ago

I was thinking the same thing.

upvoted 1 times

HeinThu 11 months, 2 weeks ago

Selected Answer: C

Compatible with other Versions of IGMP?
IGMPv1 : No
IGMPv2 : Yes, only with IGMP v1
IGMPv3 : Yes, with both IGMP v1 and v2

upvoted 4 times

danman32 4 months, 3 weeks ago

But if v3 is compatible with v2, wouldn't that make v2 also compatible with v3?
If that's so then v2 is not ONLY compatible with v1.

upvoted 1 times

ihateciscoreally 3 months, 2 weeks ago

no man, another example is programming:

C++ is compatible with C (C++ understands C syntax)
C is not compatible with C++ (C doesnt understand C++ syntax).

upvoted 1 times

diegodavid82 1 year, 9 months ago

It's not exact but is the best answer because other options are false. IGMP V3 is compatible with V1 and V2 (and obvious V3), likewise, IGMP V2 is compatible with V1 (and obvious with V3). Finally, IGMP V1 is only compatible with V1.

upvoted 4 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

Question #212 *Topic 1*

Which measurement is used from a post wireless survey to depict the cell edge of the access points?

A. SNR

B. Noise

C. RSSI

D. CCI

Correct Answer: *A*

Community vote distribution

C (74%) A (26%)

hex2 Highly Voted 1 year, 10 months ago

Selected Answer: C

https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html says BOTH answers:

"Heat map that displays RF coverage for all 'in-scope' areas with coverage set at the target RSSI for cell edge with a signal legend."

"The edge of the coverage for an AP is based on the signal strength and SNR measured as the client device moves away from the AP. "

It also says stuff like "For voice deployments, it is recommended that the cell edge should be at -67 dBm with 20 percent overlap." and -67 dBm is more of an RSSI value than a SNR value so I'm going with C. RSSI but really..... its a roll of the dice isn't it?

upvoted 6 times

rlilewis 1 year, 6 months ago

I think this is correct. I can't find any other info on "cell edge".

I'm going with RSSI.

upvoted 2 times

LanreDipeolu Most Recent 3 months, 1 week ago

Selected Answer: A

I just re-checked. A is the correct answer - The edge of the coverage for an AP is based on the signal strength and SNR measured as the client device moves away from the AP.

upvoted 2 times

HungarianDish 8 months ago

Selected Answer: C

Picturing the edge of the cells seems to be working based on RSSI.
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/en/us/td/docs/wireless/technology/7920/site_survey/guide/7920ssg/survwipt.html.xml
https://learningnetwork.cisco.com/s/question/0D53i00000KsodRCAR/how-to-determine-the-cell-edge

upvoted 4 times

Clauster 8 months, 4 weeks ago

Selected Answer: A

The Answer is not C here's why
RSSI is Received Signal Strength, this is an acronim used and it is very useful to determine the location of a Device by using Location Services or it is also used to check the signal strength that a device actually has, this is not a Graph that SHOWS, the word "depict" means show/graph/drawing, and this can be done with Single Noise Ratio, the graph will show you what you need post Wireless Survey. I am going with A

upvoted 4 times

kewokil120 11 months ago

Selected Answer: C

RSSI is the answer

upvoted 1 times

AngelPAlonso 1 year, 6 months ago

Selected Answer: C

Analyze and define the cell edge: This requires the use of AirMagnet Survey, although there are simple tools like Omnipeek or Wireshark that can be used to measure wireless traffic as a client roams from one AP to another. According to design best practices that revolve around the Cell Edge Design, a wireless handset should roam before the RSSI reaches -67 dBm. You can analyze signal strength and determine the approximate cell edge by measuring the signal strength in a beacon frame as you move from the center of one cell towards the edge of that cell.
https://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan_troubleshoot/8_Site_Survey_RF_Design_Valid.html

upvoted 4 times

Eddgar0 1 year, 7 months ago

Selected Answer: C

I agree that RSSI should be the answer

upvoted 1 times

hybl2467 1 year, 8 months ago

SNR needed to support performance requirements

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: C

It should be C

upvoted 1 times

Jcob 2 years ago

You have a next question 210 asking you for value of SNR
So RSSI is measurement that you receive. But in order to calculate SNR you need to calculate also Floor noise right? And that is POST-analysis. So It should be SNR.
But yes the question is heavily confusing because even in manual post survey is not properly defined if it is after measuring RSSI or SNR

upvoted 3 times

staman 2 years, 1 month ago

Ans is C

upvoted 1 times

xziomal9 2 years, 2 months ago

The correct answer is:
C. RSSI

upvoted 2 times

kthekillerc 2 years, 2 months ago

Coverage defines the ability of wireless clients to connect to a wireless AP with a signal strength and quality high enough to overcome the effects of RF interference. The edge of the coverage for an AP is based on the signal strength and SNR measured as the client device moves away from the AP.

The signal strength required for good coverage varies dependent on the specific type of client devices and applications on the network.

To accommodate the requirement to support wireless Voice over IP (VoIP), refer to the RF guidelines specified in the Cisco 7925G Wireless IP Phone Deployment Guide. The minimum recommended wireless signal strength for voice applications is -67 dBm and the minimum SNR is 25 dB.

The first step in the analysis of a post site survey is to verify the 'Signal Coverage'. The signal coverage is measured in dBm. You can adjust the color-coded signal gauge to your minimum-allowed signal level to view areas where there are sufficient and insufficient coverage. The example in Figure 8 shows blue, green, and yellow areas in the map have signal coverage at -67 dBm or better. The areas in grey on the coverage maps have deficient coverage. Source from Cisco

upvoted 2 times

diegodavid82 2 years, 1 month ago

I Agree, the correct answer is C.

upvoted 1 times

Adrenalina73 2 years, 2 months ago

RSSI is correct so C. :
https://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan_troubleshoot/8_Site_Survey_RF_Design_Valid.html

upvoted 2 times

rpidcock 2 years, 2 months ago

I believe that C (RSSI) is the correct answer.
https://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan_troubleshoot/8_Site_Survey_RF_Design_Valid.html
Environment Characteristics, Section 7.

upvoted 2 times

cracanici 2 years, 2 months ago

I think is A
https://community.cisco.com/t5/wireless/snr-and-rssi-values/td-p/1445589

upvoted 2 times

kthekillerc 2 years, 3 months ago

A is the correct answer for a post wireless survey.

upvoted 2 times

Question #213 *Topic 1*

If a client's radio device receives a signal strength of -67 dBm and the noise floor is -85 dBm, what is the SNR value?

A. 15 dB

B. 16 dB

C. 18 dB

D. 20 dB

Correct Answer: *C*

Community vote distribution

C (100%)

youtri Highly Voted 1 year, 10 months ago

-67 - (-85)=18

upvoted 9 times

flash007 Most Recent 4 months, 1 week ago

85-67 is 18 simple deduction so -18

upvoted 1 times

bora4motion 1 year ago

Selected Answer: C

easy one, C

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 4 times

Question #214 *Topic 1*

Which AP mode allows an engineer to scan configured channels for rogue access points?

A. monitor

B. bridge

C. local

D. sniffer

Correct Answer: *A*

Community vote distribution

A (100%)

Hamo1 2 months, 4 weeks ago

I think it's D....The controller enables you to configure an access point as a network "sniffer", which captures and forwards all the packets on a particular channel to a remote machine that runs packet analyzer software. These packets contain information on time stamps, signal strength, packet sizes, and so on.

Sniffers allow you to monitor and record network activity, and detect problems.

upvoted 1 times

Gtekzzz 10 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 2 times

bora4motion 1 year ago

Selected Answer: A

A is correct

upvoted 2 times

Asymptote 1 year ago

Selected Answer: A

The local and FlexConnect mode access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to perform high rogue detection, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point continues to spend about 50 milliseconds on each channel.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010111000.html#:~:text=The%20local%20and%20FlexConnect%20mode%20access%20points,spend%20about%2050%20milliseconds%20on%20each%20channel.

upvoted 4 times

rpidcock 2 years, 2 months ago

Monitor—This is radio receive only mode, and allows the AP to scan all configured channels every 12 seconds. Only de-authentication packets are sent in the air with an AP configured this way. A monitor mode AP can detect rogues, but it cannot connect to a suspicious rogue as a client in order to send the RLDP packets.

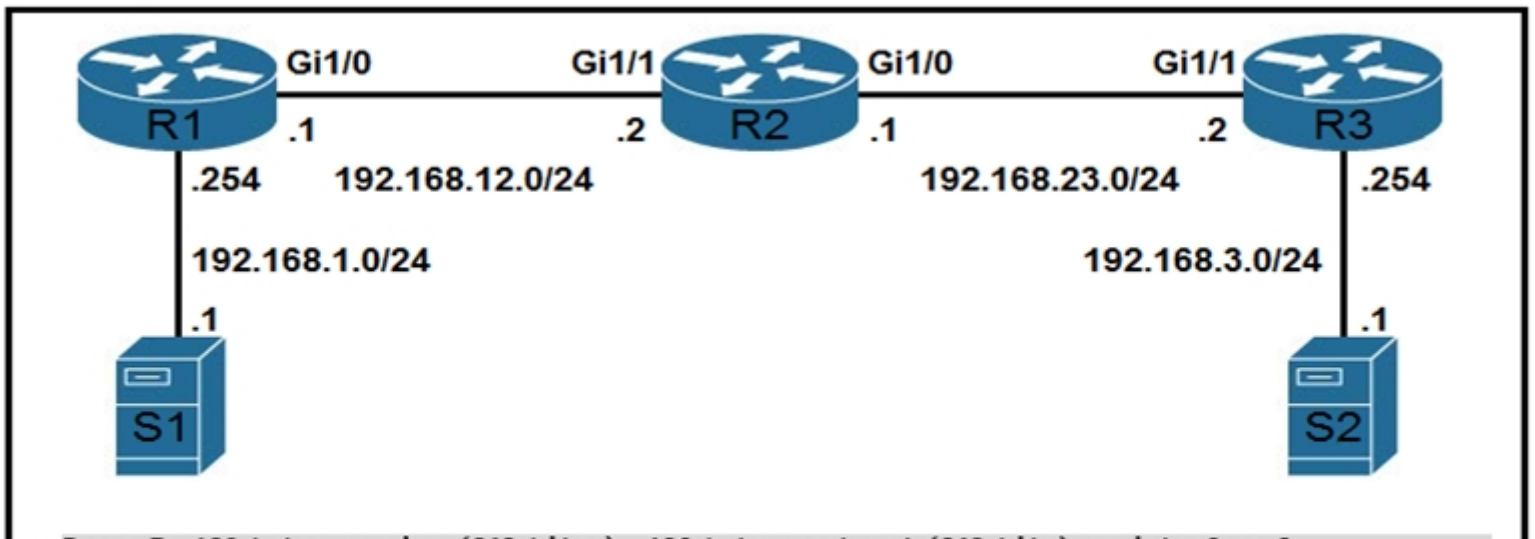
upvoted 3 times

kthekillerc 2 years, 3 months ago

A is the correct answer

upvoted 2 times

Question #215 *Topic 1*



Refer to the exhibit. While troubleshooting a routing issue, an engineer issues a ping from S1 to S2. Which two actions result from the initial value of the TTL?
(Choose two.)

A. The packet reaches R2, and the TTL expires.

B. R1 replies with a TTL exceeded message.

C. The packet reaches R3, and the TTL expires.

D. R2 replies with a TTL exceeded message.

E. R3 replies with a TTL exceeded message.

F. The packet reaches R1, and the TTL expires.

Correct Answer: *CE*

Community vote distribution

AD (75%) CE (22%)

Hugh_Jazz Highly Voted 2 years, 1 month ago

It is A & D. Source MAC in the capture is VMWare, Dest MAC is Cisco. Routers first check the TTL before any further process, subtact 1 at R1. Send to R2, subtract and you have ZERO. Discard packet and reply with ICMP Time Exceeded message from that point, don't even bother checking the Route table for futher processing.

If Packet was sourced from R1, then R3 would be the last hop and TTL would expire.

upvoted 35 times

Pilgrim5 7 months, 3 weeks ago

But it's R1 that sets the TTL of 2 so shouldn't the TTL expire at R3..?

upvoted 1 times

mp777 4 months, 2 weeks ago

TTL=2 is set on initial echo request as the packet is captured before entering R1 - note the vmware ethernet mac header. if it was on any other routing segment, src mac address would be the one of cisco's.

upvoted 3 times

mellohello 9 months ago

When a router in the path finds that the TTL is 1, it responds to the source with an ICMP “time exceeded” message. This lets the source know that the packet traversed that particular router as a hop.

I will go for A and D as well.

upvoted 1 times

catdotwell 1 year, 5 months ago

From the CCNP book: "The TTL is a Layer 3 loop prevention mechanism that reduces a packet’s TTL field by 1 for every Layer 3 hop. If a router receives a packet with a TTL of 0, the packet is discarded."

When it reaches R1, it has a TTL of 2 , it only has a TTL of 1 when it exits R1.

"If Packet was sourced from R1, then R3 would be the last hop and TTL would expire" - exactly, last hop is R3, so R3 will reply with a TTL exceeded messages, therefore C and E are correct.

upvoted 11 times

Feliphus 12 months ago

But, you suppose the IP packet with TTL=0 travels from R2 to R3, What sense will have that action if you know R3 will drope it just after receive it ? It's more logic R2 inmediately drop it

upvoted 1 times

Kapoduster Highly Voted 1 year, 11 months ago

Selected Answer: CE

I think, the given answer is correct.
When packet is arrived to R1 TTL is 2. It decrease TTL to 1 and send packet to R2. R2 decrease TTL to 0 and send packet with TTL 0 to R3. R3 receive packet with TTL 0 so reply with "Time to live exceeded in transit”. Or am I wrong ?

upvoted 11 times

dragonwise 8 months, 2 weeks ago

I have simulated the exact scenario, and the answer is AD

upvoted 2 times

catdotwell 1 year, 5 months ago

you are correct, the CCNP book says "The TTL is a Layer 3 loop prevention mechanism that reduces a packet’s TTL field by 1 for every Layer 3 hop. If a router receives a packet with a TTL of 0, the packet is discarded."

R2 sees the packet with a TTL of 1, it only has a TTL of 0 when exits R2 towards R3, but in that instance R2 is not taking care of the packet anymore.

upvoted 3 times

kiyaye1 Most Recent 6 days, 23 hours ago

its A&D , R1(TTL-1=1) sends to R2(TTL-1=0) , a router won't send out a packet with ttl 0 rather will respond with TTL expired , Every time a router receives a packet, it subtracts one from the TTL count and then passes it onto the next location in the network. If at any point the TTL count is equal to zero after the subtraction, the router will discard the packet and send an ICMP message back to the originating host.

upvoted 1 times

KZM 2 weeks, 1 day ago

Selected Answer: AD

As per the showing exhibit, the packet was captured in the R1's interface that connected to S1(Consider based on showing Scr and Dst MAC address).
S1 will send the packet with TTL value 2 origin. R1 will reduce the TTL value to 1 before sending it to R2. So the packet will reach R2 with the TTL value 1. R2 will reduce the TTL value to 0 before sending and no longer forwards the packet to R3, and then drops it.

upvoted 1 times

KZM 2 weeks, 1 day ago

Edit: The packet may be captured on the output of the S1 interface. The answer: A, D.

upvoted 1 times

KZM 2 weeks, 1 day ago

I have already tested in my Lab and no packet was reached to the R2 exit interface and R3. And R2 reply as TTL expired.
VPCS> ping 192.168.3.1 -T 2

*192.168.12.2 icmp_seq=1 ttl=254 time=0.692 ms (ICMP type:11, code:0, TTL expired in transit)
*192.168.12.2 icmp_seq=2 ttl=254 time=0.604 ms (ICMP type:11, code:0, TTL expired in transit)
*192.168.12.2 icmp_seq=3 ttl=254 time=0.721 ms (ICMP type:11, code:0, TTL expired in transit)
*192.168.12.2 icmp_seq=4 ttl=254 time=1.126 ms (ICMP type:11, code:0, TTL expired in transit)
*192.168.12.2 icmp_seq=5 ttl=254 time=0.499 ms (ICMP type:11, code:0, TTL expired in transit)

VPCS>

upvoted 1 times

Claudiu1 2 weeks, 1 day ago

Selected Answer: AD

The correct answers are A and D
I just checked in EVE-NG and the TTL exceeded answer is sent from 192.168.12.2 to 192.168.1.1. It seems that:
- R1 receives the packet, decreases the TTL to 1 and forwards it towards R2.
- R2 receives the packet, decreases the TTL to 0, discards it and sends a TTL Exceeded message to S1

upvoted 1 times

Jasper 1 month, 3 weeks ago

When a packet is by a router, the router subtracts 1 from the TTL count. Then, the packet travels to the next destination on the network. When the TTL count is 0, after the final subtraction, the packet is discarded by the router. This triggers an Internet Control Message Protocol (ICMP) message that's sent back to the originating host.

upvoted 1 times

darcone23 2 months, 3 weeks ago

Selected Answer: AD

So the packet reaches R2 and TTL expires, R2 discars this packet and sends TTL expired message...

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

Selected Answer: AD

Tested in CML

Each router decrements the TTL by 1. The packet's first hop being the gateway of the Device will now have a TTL of 1, the second hop being R2 now has a TTL of 0, meaning the packet has reached R2 but expired, never actually making it to R3.

R2 then replies with a TTL exceeded message back to the client.

S1@linux:~$ ping -t 2 192.168.3.1
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
From 192.168.12.2 icmp_seq=1 Time to live exceeded
--- 192.168.3.1 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1002ms

When I change the TTL to 3

S1@linux:~$ ping -t 3 192.168.3.1
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=1 ttl=253 time=65.2 ms
--- 192.168.3.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 50.672/57.919/65.166/7.247 ms

upvoted 2 times

kldoyle97 3 months ago

Selected Answer: AC

When a router receives a packet with TTL = 1
if the destination of the packet is not itself it will drop the packet.
In this question, R2 will drop the packet and reply with an ICMP type 11 (time exceeded) message
https://www.youtube.com/watch?v=zesTvBZCESk&list=PLxbwE86jKRgOb2uny1CYEzyRy_mc-lE39&index=21&ab_channel=Jeremy%27sITLab

upvoted 1 times

djedeen 3 months, 1 week ago

Selected Answer: AD

A & D
Routers always decrement the TTL by 1 and forward the packet if the new TTL is greater than zero. If it is zero, some routers issue a ICMP time exceeded in transit packet as you've noticed, but some don't (mostly for security reasons).

upvoted 1 times

Asher 4 months ago

Think of it like traceroute. It starts with a TTL of 1 hits the first hop decrements to 0 and drops and replays with ICMP time exceeded. Then sends out a packet with two TTL, goes an extra hop then drops. Rinse and repeat.

upvoted 1 times

Poba 4 months, 2 weeks ago

When a router receives a packet with a Time-to-Live (TTL) value of 1, it performs the following actions:

Decrement TTL: The router decreases the TTL value in the IP header of the packet by 1.

Check TTL Value: After decrementing the TTL, the router checks the new TTL value. If the TTL becomes zero or less after the decrement, the router considers the TTL expired.

Generate Time Exceeded Message: If the TTL becomes zero or less, the router generates an ICMP (Internet Control Message Protocol) Time Exceeded message. This message informs the original source of the packet that the TTL has expired, indicating that the packet has been discarded. The Time Exceeded message includes the IP header of the original packet and is sent back to the source IP address.

Discard the Packet: After generating the Time Exceeded message, the router discards the original packet. It does not forward the packet any further.

upvoted 1 times

Adnan5252 4 months, 2 weeks ago

A and D because ping is send from s1 r1 is count as 1 and r2 ttL value become 0 ...

upvoted 1 times

ibogovic 5 months ago

Selected Answer: AB

In the given exhibit, the Time to Live (TTL) value is 2. The TTL field is used to limit the number of hops a packet can take through a network. Each router decrements the TTL value by 1 when forwarding the packet. If the TTL value becomes 0, the router drops the packet and sends an ICMP Time Exceeded message back to the source.

Let's analyze the possible scenarios:

The packet reaches R2, and the TTL expires. (Possible)
R1 replies with a TTL exceeded message. (Possible)
The packet reaches R3, and the TTL expires. (Not possible, as the TTL is already 2, and there are only two routers shown in the exhibit.)
R2 replies with a TTL exceeded message. (Possible)
R3 replies with a TTL exceeded message. (Not possible, as the TTL is already 2, and there are only two routers shown in the exhibit.)
The packet reaches R1, and the TTL expires. (Not possible, as R1 is the source of the packet, and it does not decrement its own TTL.)
Based on the given information, the two possible actions that result from the initial value of the TTL (2) are:

A. The packet reaches R2, and the TTL expires.
B. R1 replies with a TTL exceeded message.

upvoted 1 times

jakeydsnakey 5 months ago

Selected Answer: AD

Answer is A & D.

I tested in lab (EVE-NG) and tried to ping from vPC-1(192.168.1.1) with modified TTL of 2 going to vPC-2 (192.168.3.1). Below is the result.

VPCS> ping 192.168.3.1 -T 2

*192.168.12.2 icmp_seq=1 ttl=254 time=2.470 ms (ICMP type:11, code:0, TTL expired in transit)
*192.168.12.2 icmp_seq=2 ttl=254 time=2.929 ms (ICMP type:11, code:0, TTL expired in transit)
*192.168.12.2 icmp_seq=3 ttl=254 time=3.719 ms (ICMP type:11, code:0, TTL expired in transit)
*192.168.12.2 icmp_seq=4 ttl=254 time=2.944 ms (ICMP type:11, code:0, TTL expired in transit)
*192.168.12.2 icmp_seq=5 ttl=254 time=2.533 ms (ICMP type:11, code:0, TTL expired in transit)

- 192.168.12.2 is R2 physical interface facing R1 (answer A) and replied with a TTL expired in transit message (answer D). The icmp packet didn't reach R3 anymore (verified with wireshark in EVE-NG) which makes answer C & E wrong/invalid.

Regards.

upvoted 2 times

CKL_SG 5 months, 1 week ago

Selected Answer: AD

testing using gns3
ICMP drop at R2 with Time to live Exceeded

upvoted 3 times

msstanick 5 months, 3 weeks ago

Selected Answer: AD

Labed it up to be sure - AD. The packet never reaches R3 as R2 sends the icmp request back to the source with a message that the TTL is only 1 and packet is not going to be forwarded.

upvoted 2 times

Question #216 *Topic 1*

What is the wireless Received Signal Strength Indicator?

A. the value given to the strength of the wireless signal received compared to the noise level

B. the value of how strong the wireless signal is leaving the antenna using transmit power, cable loss, and antenna gain

C. the value of how much wireless signal is lost over a defined amount of distance

D. the value of how strong a wireless signal is received, measured in dBm

Correct Answer: *D*

Community vote distribution

D (100%)

thinqtanklearningDOTcom Highly Voted 1 year, 4 months ago

A - Signal to Noise Ratio
B - Effective Isotropic Radio Power
C - Attenuation
D - RSSI <<< Correct

upvoted 7 times

Pilgrim5 Most Recent 7 months, 3 weeks ago

Selected Answer: D

Given answer is correct 100

upvoted 1 times

alawi2 1 year, 5 months ago

actually, both A & D are technically sound, hope i dont see it in the exams

upvoted 1 times

thinqtanklearningDOTcom 1 year, 4 months ago

Negative. A is SIGNAL TO NOISE RATIO

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

Question #217 *Topic 1*

Which two operational modes enable an AP to scan one or more wireless channels for rogue access points and at the same time provide wireless services to clients? (Choose two.)

A. monitor

B. rogue detector

C. FlexConnect

D. sniffer

E. local

Correct Answer: *CE*

Community vote distribution

CE (100%)

sasatrickovic Highly Voted 2 years, 1 month ago

C and E are correct.

Rogue Detection is performed by Local and Flex-Connect (in connected mode) mode APs and utilizes a time-slicing technique which allows client service and channel scanning with the usage of the same radio. With the move to off channel for a period of 50ms every 16 seconds, the AP, by default, only spends a small percentage of its time to not serve clients.

Monitor mode serves only to scan, not to serve clients.

Monitor mode APs are also far superior at the detection of rogue clients as they have a more comprehensive view of the activity that occurs in each channel.

Just as @YTAKE, @Adrenalina73, @xziomal9, @wifishark and others say.

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html#anc8

upvoted 20 times

pacman64 Highly Voted 2 years, 3 months ago

Shouldn't it be C & E?

upvoted 7 times

SandyIndia 2 years, 2 months ago

C & E correct.
Monitor mode, sniffer mode, and rogue detector mode do not provide client connectivity.

upvoted 3 times

nopenotme123 1 year, 3 months ago

Rogue does provide client connectivity.. It'll just deem it rogue aha..

upvoted 1 times

techplus Most Recent 1 year, 4 months ago

Selected Answer: CE

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html

Local Mode APs
Serves clients with time-slicing off-channel scan
Monitor Mode APs
Dedicated Scan

Flex-Connect Facts

A FlexConnect AP (with rogue detection enabled) in the connected mode takes the containment list from the controller. If auto-contain SSID and auto contain adhoc are set in the controller, then these configurations are set to all FlexConnect APs in the connected mode and the AP stores it in its memory.

upvoted 1 times

BigMouthDog 1 year, 5 months ago

Answer is C & E, because "Monitor" mode is not used for client serving, none of them is except "Local" and "FlexConnect"

upvoted 1 times

timtgh 1 year, 6 months ago

B,C, and E are all correct. But they only want two answers so probably C and E.

upvoted 1 times

sayywhat 1 year, 6 months ago

CE
+In a dense RF environment, where maximum rogue access points are suspected, the chances of detecting rogue access points by a local mode access point and FlexConnect mode access point in channel 157 or channel 161 are less when compared to other channels. To mitigate this problem, we
recommend that you use dedicated monitor mode access points.

+The local and FlexConnect mode access points are designed to serve associated clients. These access points spend relatively less time performing
off-channel scanning: about 50 milliseconds on each channel. If you want to perform high rogue detection, a monitor mode access point must be used.
Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes offchannel more frequently, which improves the chances of rogue detection. However, the access point continues to spend about 50 milliseconds on each
channel.

upvoted 2 times

hyjaker 1 year, 7 months ago

Selected Answer: CE

I agree with the others. Monitor mode does not transmit. Therefore, it cannot serve client's.

upvoted 1 times

Aldebeer 1 year, 7 months ago

Selected Answer: CE

it say; ..one or more wireless channels for rogue ap.. so, the ans. = C&E

upvoted 1 times

hybl2467 1 year, 8 months ago

• Local: The default lightweight mode that offers one or more functioning BSSs on a specific channel. During times when it is not transmitting, the AP scans the other channels to measure the level of noise, measure interference, discover rogue devices, and match against intrusion detection system (IDS) events.
Monitor: The AP does not transmit at all, but its receiver is enabled to act as a dedicated sensor. The AP checks for IDS events, detects rogue access points, and determines the position of stations through location-based services.

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: CE

It should be CE

upvoted 2 times

donjime 1 year, 10 months ago

Selected Answer: CE

CE because only both bring services of BSS to clients and scans the channel when there is no traffic

upvoted 4 times

Alizadeh 1 year, 11 months ago

Selected Answer: CE

correct CE

upvoted 4 times

xziomal9 2 years, 2 months ago

The correct answer is:
C. FlexConnect
E. local

upvoted 2 times

Adrenalina73 2 years, 2 months ago

Hello I suppose is C and E ... look there about FlexConnect architecture:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73/ch7_HREA.pdf

upvoted 4 times

YTAKE 2 years, 2 months ago

Exactly: C and E

the trick here is that "while serving clients"

Monitor mode does 100% scanning. It does not serve clients:

See Scanning modes in this doc:

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html

Rogue Management in an Unified Wireless Network

upvoted 2 times

error_909 2 years, 2 months ago

C ^& E 100%

upvoted 2 times

kthekillerc 2 years, 3 months ago

C and E are the only two modes able to provide wireless service to clients. https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html#anc8

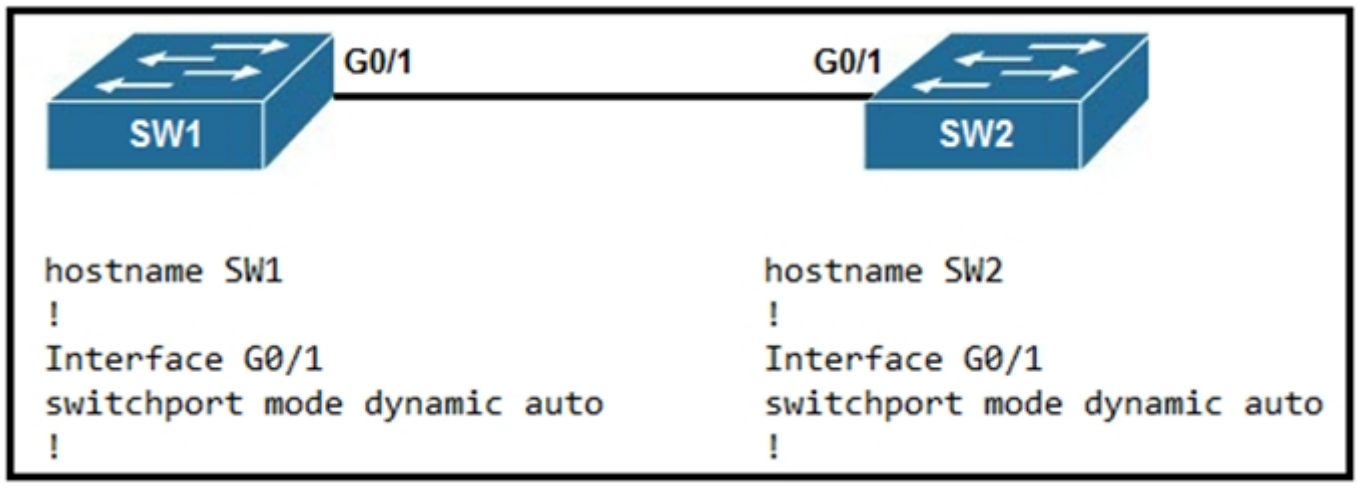
upvoted 2 times

wifishark 2 years, 3 months ago

C & E are the right answer (Local and FlexConnect)

upvoted 3 times

Question #218 *Topic 1*



Refer to the exhibit. An engineer attempts to configure a trunk between switch SW1 and switch SW2 using DTP, but the trunk does not form. Which command should the engineer apply to switch SW2 to resolve this issue?

A. switchport nonegotiate

B. no switchport

C. switchport mode dynamic desirable

D. switchport mode access

Correct Answer: *C*

sasatrickovic Highly Voted 2 years, 1 month ago

DESIRABLE must be paired with AUTO on other side to form.
The answer is correct.

upvoted 5 times

CCNPWILL Most Recent 1 month, 1 week ago

Even without seeing the exhibit.... the answer proposed is correct since its the only one that would form a trunk.

upvoted 1 times

Question #219 *Topic 1*

An engineer is troubleshooting the AP join process using DNS. Which FQDN must be resolvable on the network for the access points to successfully register to the WLC?

A. wlchostname.domain.com

B. cisco-capwap-controller.domain.com

C. ap-manager.domain.com

D. primary-wlc.domain.com

Correct Answer: *B*

[Removed] 4 months, 2 weeks ago
aceitcert.com is free
upvoted 1 times

kthekillerc 2 years, 2 months ago
Provided answer is correct
upvoted 1 times

Question #220 *Topic 1*

Which new enhancement was implemented in Wi-Fi 6?

A. Uplink and Downlink Orthogonal Frequency Division Multiple Access

B. Channel bonding

C. Wi-Fi Protected Access 3

D. 4096 Quadrature Amplitude Modulation Mode

Correct Answer: *A*
Reference:
https://ibwave.com/wi-fi-6-networks/#:~:text=1024%2DQAM%20(Quadrature%20Amplitude%20Modulation,speeds%20by%20up%20to%2025%25
.

LM77 Highly Voted 1 year, 10 months ago
Answer A is correct

"Perhaps the most important new capability introduced with Wi-Fi 6 is Orthogonal Frequency Division Multiple Access (OFDMA). This RF modulation technique allows multiple Wi-Fi 6 clients to simultaneously receive data during the same transmit opportunity. Allowing more information for multiple devices to be transmitted in parallel during a particular window of opportunity, all while reducing some of the traditional overhead of sending the same amount of information independently.

OFDMA divides a channel into further subcarriers compared to Orthogonal Frequency Division Multiplexing (OFDM)"

https://www.cisco.com/c/en/us/solutions/cisco-on-cisco/enterprise-wifi-6.html
upvoted 12 times

dudalykai Most Recent 3 months, 3 weeks ago
Also
Wi-Fi Protected Access 3 (WPA3) is available in Wi-Fi 6 and is mandatory for Wi-Fi 6E. WPA3 adds more robust 192-bit encryption, providing consistent cryptography and helping eliminate the "mixing and matching of security protocols"that are defined in the 802.11 standard. Additionally, WPA3 requires Protected Management Frames (PMF) negotiation. PMF provides an additional layer of protection from deauthentication and disassociation attacks.
So there should be two correct answers to this question
upvoted 2 times

Question #221 *Topic 1*

Which device makes the decision for a wireless client to roam?

A. wireless client

B. wireless LAN controller

C. access point

D. WCS location server

Correct Answer: *A*
Reference:
https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Client_roaming_and_connectivity_decisions_explained

Community vote distribution

A (100%)

miccamilla Highly Voted 1 year, 6 months ago

Roaming is a client side decision in 802.11 WiFi. Client devices listen for beacon frames or send probe requests to discover APs advertising the preferred SSID.

upvoted 7 times

Asymptote Most Recent 1 year ago

Selected Answer: A

The client device is in complete control of the roaming decision, based on its own roaming algorithm. It uses active scanning and probing to discover other candidate APs that it might roam to.

upvoted 2 times

Parot 1 year, 1 month ago

Answer is A.

upvoted 2 times

H3kerman 1 year, 1 month ago

Selected Answer: A

Roaming is a client side decision in 802.11 WiFi. Client devices listen for beacon frames or send probe requests to discover APs advertising the preferred SSID. The clients driver uses the received signal strength of beacons or probe responses to make decisions on whether to change APs or remain connected to the current AP. In terms of roaming,

upvoted 2 times

Dataset 1 year, 2 months ago

I think is B

upvoted 1 times

WINDSON 1 year ago

please study hard and don't post incorrect answer

upvoted 3 times

Dataset 7 months, 2 weeks ago

ohhh...sorry master,....jajjajajajajaja

upvoted 1 times

fefe411 1 year, 7 months ago

Should be B

upvoted 1 times

Question #222 *Topic 1*

An engineer configures GigabitEthernet 0/1 for VRRP group 115. The router must assume the primary role when it has the highest priority in the group.
Which command set is required to complete this task?
interface GigabitEthernet0/1
ip address 10.10.10.2 255.255.255.0
vrrp 115 ip 10.10.10.1
vrrp 115 authentication 407441579

A. Router(config if)# vrrp 115 track 1 decrement 100 Router(config-if)# vrrp 115 preempt

B. Router(config-if)# vrrp 115 priority 100

C. Router(config-if)# vrrp 115 track 1 decrement 10 Router(config-if)# vrrp 115 preempt

D. Router(config-if)# standby 115 priority 100 Router(config-if)# standby 115 preempt

Correct Answer: *B*

Reference:

https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/350_550/index.html#page/tesla_350_550_olh/ts_vrrp_18_09.html

Community vote distribution

B (55%) C (45%)

Splashisthegreatestmovie Highly Voted 5 months, 2 weeks ago

Something is missing from this question. In VRRP preempt is configured by default and the priority is set to the default. All in All this question is a disaster.

upvoted 8 times

prietito Highly Voted 1 year, 10 months ago

Default priority for VRRP = 100. Question is vague, not enough information. I think C is more of a valid answer.

upvoted 8 times

iGlitch 1 year, 1 month ago

What does C do? explain

upvoted 2 times

djedeen Most Recent 3 months, 2 weeks ago

Selected Answer: B

VRRP preemption on by default, so A, C, D are red herrings. 'When' it is highest priority, other router could be decrementing based on tracking or static config.

upvoted 1 times

Colmenarez 4 months ago

Selected Answer: B

La opcion B es la correcta, si configuras trach 10 para bajar la prioridad, entonces no siempre R1 sera el primario y es lo que esta pidiendo la pregunta.

upvoted 2 times

sonjad 4 months, 1 week ago

Looks like B is correct. It says "The router must assume the primary role WHEN it has the highest priority in the group." So the question is not how to make this router primary, but how to make it primary if it has the highest priority. So they are checking only the knowledge of default preemption behavior of vrrp.

upvoted 1 times

HarwinderSekhon 5 months ago

Selected Answer: B

preempt is configured by default

upvoted 2 times

Entivo 6 months, 1 week ago

Selected Answer: C

The answer is clearly C. You cannot decrement by 100 if the priority is 100 (try it in a lab) and we know the priority is 100 because no priority has been set in the config and therefore the default applies. The best answer is to decrement by 10, making the new priority 90 (we can only assume that the other router is also on the default priority as we haven't been told otherwise and if you've done any Cisco exams before you will know that they expect you to assume and know all the defaults for everything). Preempt is necessary otherwise the primary router won't take control of the VIP when its priority returns to 100.

upvoted 2 times

[Removed] 5 months, 2 weeks ago

VRRP, preempt is enabled by default. Here is my opinion, this question sucks, but:

A: decrement 100 is not valid
B: priority 100 is default
C: again, preempt is default
D: standby is HSRP

The excerpt must be missing something

upvoted 4 times

HungarianDish 8 months ago

Option A) with decrement by 100 is wrong for sure. It results in priority 0, and that is not a valid priority value for vrrp. If priority 0 is set, then vrrp gets stuck in "Init" state.
See example below:
DSW2(config-if)#do sh vrrp
Vlan0002 - Group 2
State is Init
Virtual IP address is 10.10.2.3
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 0
Track object 1 state Down decrement 100

upvoted 3 times

pmmg 8 months, 2 weeks ago

Selected Answer: B

I think the answer is B. There is no information given about the other router, but by inference it must be set with a higher priority than the one in the question. It would also be set to preempt (by default or by command). Our example is to be the standby. It should take over in the event of a failure of the active rtr, and be preempted when it comes back online.

Answer A, decrementing by 100 seems extreme.
Answer B, set it default, which should be lower than its partner, making it the standby.
Answer C, By decrementing 10, we make it priority 90, but there is no need to preempt, the active one has failed.
Answer D, by making it priority 100 and preempting, would make it active unless its partner had a higher priority.

If the partner has a higher priority already, preempting should be configured on it, not the standby.

Make sense?

upvoted 3 times

bk989 6 months, 2 weeks ago

you're right it is C. Especially since vrrp doesn't need pre-emption.

upvoted 1 times

Clauster 8 months, 4 weeks ago

Selected Answer: C

There's a lot of missing information however, in order for a router to assume it's highest role in this case "Master" it needs to enable Preemption.

upvoted 1 times

errepe_ 8 months, 1 week ago

vrrp has the preempt enabled by default

upvoted 5 times

charafDZ 9 months ago

If you wanna understand VRRP OBJECT TRACKING

https://community.cisco.com/t5/routing/the-decrement-of-vrrp-object-tracking/td-p/4498532

upvoted 2 times

SirJani 9 months, 3 weeks ago

Vrrp preempt is the default behaviour, does not need to be explicitly configured. So therefore both B and C should work. Which one is the better answer, don't know

upvoted 1 times

rafaelinho88 9 months, 3 weeks ago

TYPOSSSSSSSSSS

. Router(config-if)#vrrp 116 priority 100
B. Router(config-if)#standby 115 priority 100
Router(config-if)#standby 115 prompt
C. Router(config-if)#vrrp 116 track 1 decrement 10
Router(config-if)#vrrp 115 preempt
D. Router(config-if)#vrrp 115 track 1 decrement 100
Router(config-if)#vrrp 115 preempt

upvoted 2 times

danman32 4 months ago

None of these alternate answers would work.
Only A, C and D pertain to VRRP.
Only B and D use the correct group #.
D is invalid since you can't decrement down by 100 if default is 100.
B either has a typo (prompt vs preempt) or even if it was preempt, all defaults.
And we really need to know what the other router is set to. We can only assume defaults so if this router came down and back up, it would have same priority as other

upvoted 1 times

Gtekzzz 10 months, 2 weeks ago

Selected Answer: C

Default priority for VRRP = 100. Question is vague. I would suggest answer C is more valid.

upvoted 1 times

Rose66 10 months, 3 weeks ago

Selected Answer: B

I do not see any correct choice here, preemption is enabled by default as well as priority == 100. But for me Answer b is the best choice... Maybe in the test there will be a priority value > 100... so it will be B

upvoted 2 times

Ayman_B 10 months, 3 weeks ago

Selected Answer: C

The configuration that provided in the Question sets The router as the active router for the VRRP group ..
and the default priority is 100 .. so,I think B is not logical choise..

Now to complete this task we have to bay attention to the following :

If the uplink interface of a router in a VRRP group fails, usually the VRRP group cannot be aware of the uplink interface failure, and the hosts on the LAN are not able to access external networks because of the uplink failure. This problem can be solved by tracking , so addind the this command will complete the task :

C. Router(config-if)# vrrp 115 track 1 decrement 10 Router(config-if)# vrrp 115 preempt

now that means:

Monitor an uplink and change the priority of the router according to the state of the uplink. if it fails The priority of the VRRP group will be decreased by 10 and the router will not become more the master.

upvoted 2 times

Dataset 11 months, 1 week ago

Selected Answer: C

Because there is no need to enable preempt, in VRRP is default configuration.
Regards

upvoted 1 times

Dataset 9 months, 2 weeks ago

sorry, i mean B

upvoted 1 times

Question #223 *Topic 1*

How is MSDP used to interconnect multiple PIM-SM domains?

A. MSDP allows a rendezvous point to dynamically discover active sources outside of its domain.

B. MSDP SA request messages are used to request a list of active sources for a specific group.

C. MSDP depends on BGP or multiprotocol BGP for interdomain operation.

D. MSDP messages are used to advertise active sources in a domain.

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-msdp-im-pim-sim.html

Community vote distribution
A (61%) C (20%) Other

Daaid 3 months ago

Selected Answer: A

From Cisco Document, matches A exactly
https://www.cisco.com/c/en/us/td/docs/ios/12_4t/ip_mcast/configuration/guide/mctmsdp.html#wp1054452
Benefits of Using MSDP to Interconnect Multiple PIM-SM Domains
•Allows a rendezvous points (RP) to dynamically discover active sources outside of its domain.

upvoted 3 times

yellowswan 3 months, 1 week ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-msdp-im-pim-sim.html
according to the link, I paste somet content here:
1. Allows a rendezvous point (RP) to dynamically discover active sources outside of its domain. ==> matches option A
2. SA request messages are used to request a list of active sources for a specific group. ==> matches option B
3. MSDP depends on BGP or multiprotocol BGP (MBGP) for interdomain operation. We recommended that you run MSDP on RPs sending to global multicast groups. ==> matches option C
4. SA messages are used to advertise active sources in a domain. ==> it's SA message, not all 4 types of MSDP messages, so it's wrong

Is there any possibility that the question asked you to select an INCORRECT option?

upvoted 2 times

LanreDipeolu 3 months, 1 week ago

Selected Answer: C

Multicast Source Discovery Protocol- MSDP, If listeners exist, it triggers a PIM join into the source domain towards the data source. In a peering relationship, one MSDP peer listens for new TCP connections on the well-known port 639.

upvoted 1 times

djedeen 3 months, 1 week ago

Nope, C:
Prerequisites for Using MSDP to Interconnect Multiple PIM-SM Domains
Before you configure MSDP, the addresses of all MSDP peers must be known in Border Gateway Protocol (BGP).

upvoted 1 times

djedeen 3 months, 2 weeks ago

Selected Answer: A

MSDP provides inter-domain access to multicast sources in all domains by enabling all Rendezvous Points (RPs) to discover multicast sources outside of their domains

upvoted 1 times

Dv123456 4 months, 1 week ago

Is there MSDP in the Cert. Guide? Surely not in the blueprint

upvoted 1 times

HarwinderSekhon 5 months ago

Selected Answer: A

A is the answer.

The purpose of MSDP is to discover multicast sources in other PIM domains. The main advantage of MSDP is that it reduces the complexity of interconnecting multiple PIM-SM domains by allowing PIM-SM domains to use an interdomain source tree (rather than an common shared tree). When MSDP is configured in a network, RPs exchange source information with RPs in other domains. An RP can join the interdomain source tree for sources that are sending to groups for which it has receivers. The RP can do that because it is the root of the shared tree within its domain, which has branches to all points in the domain where there are active receivers. When a last-hop router learns of a new source outside the PIM-SM domain (through the arrival of a multicast packet from the source down the shared tree), it then can send a join toward the source and join the interdomain source tree.

https://www.cisco.com/c/en/us/td/docs/ios/12_4t/ip_mcast/configuration/guide/mctmsdp.html
upvoted 2 times

Splashisthegreatestmovie 5 months, 2 weeks ago
I'm struggling with this because you can't run MSDP between domains without BGP so C is completely valid. However A is an accurate description.
upvoted 1 times

michalcz 7 months ago
Prerequisites for Using MSDP to Interconnect Multiple PIM-SM Domains
Before you configure MSDP, the addresses of all MSDP peers must be known in Border Gateway Protocol (BGP).
upvoted 1 times

Chiaretta 7 months, 2 weeks ago
Selected Answer: A
The purpose of MSDP is to discover multicast sources in other PIM domains.
upvoted 1 times

Clauster 8 months, 1 week ago
Selected Answer: A
Answer is A
Straight from Cisco White Pages
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-msdp-im-pim-sim.html
upvoted 2 times

Uzzi1222 8 months, 2 weeks ago
Selected Answer: A
Allows a rendezvous point (RP) to dynamically discover active sources outside of its domain.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-msdp-im-pim-sim.html
upvoted 2 times

Jahsha 9 months ago
Selected Answer: A
I think it is a the question is how is it used not how it functions
upvoted 1 times

Cooldude89 9 months, 2 weeks ago
Selected Answer: B
B is correct
source from Cisco
upvoted 1 times

Cooldude89 9 months, 1 week ago
Correction , most suitable is Answer A
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-msdp-im-pim-sim.html
upvoted 1 times

HungarianDish 10 months ago
AC according to mentioned document:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-msdp-im-pim-sim.html

The question should state "choose two"!
upvoted 2 times

TSKARAN 10 months ago
Selected Answer: A
MSDP is a mechanism to connect multiple PIM-SM domains. The purpose of MSDP is to discover multicast sources in other PIM domains.
upvoted 2 times

rafaelinho88 10 months ago
Is that answer from ChatGPT lol
upvoted 2 times

ironbornson 9 months, 3 weeks ago
He is telling you the answer is A because even B and C are correct only A explains how is MSDP used
upvoted 2 times

rafaelinho88 9 months, 3 weeks ago
It is B bro.
https://www.cisco.com/c/en/us/td/docs/ios/12_4t/ip_mcast/configuration/guide/mctmsdp.html#wp1054387
upvoted 1 times

TSKARAN 10 months, 2 weeks ago

Selected Answer: A
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-msdp-im-pim-sim.html
upvoted 1 times

Question #224 *Topic 1*

If the noise floor is -90 dBm and the wireless client is receiving a signal of 75'ˆ‚ dBm, what is the SNR?

A. 15

B. 1.2

C. 165'ˆ‚

D. .83

Correct Answer: *A*

Signal Strength ‚ˆ' Noise floor = SNR

Community vote distribution

A (79%) C (21%)

Stylar Highly Voted 1 year ago

Selected Answer: A

There is obviously a typo here, you cant go to the + range.. Maximum achievable strength is -30dbm. The question should say -75, not 75.

upvoted 6 times

[Removed] 5 months, 2 weeks ago

This makes more sense.

upvoted 1 times

Evreni Most Recent 4 weeks, 1 day ago

Selected Answer: C

C: is correct
https://www.omnicalculator.com/physics/signal-to-noise-ratio

upvoted 1 times

Poba 4 months, 2 weeks ago

To calculate the Signal-to-Noise Ratio (SNR), we need to convert the signal and noise power from dBm to linear scale (watts) and then use the SNR equation:

SNR (dB) = 10 * log10(signal power / noise power)

Given:
Noise floor = -90 dBm
Signal strength = 75 dBm

First, let's convert the signal and noise power to watts:

Signal Power (W) = 10^((Signal Strength (dBm) - 30) / 10)
Signal Power (W) = 10^((75 - 30) / 10)
Signal Power (W) = 10^4.5
Signal Power (W) = 31,622.7766 W

Noise Power (W) = 10^((Noise Floor (dBm) - 30) / 10)
Noise Power (W) = 10^((-90 - 30) / 10)
Noise Power (W) = 10^-12
Noise Power (W) = 0.000000000001 W

Now, let's calculate the SNR in dB:

SNR (dB) = 10 * log10(signal power / noise power)
SNR (dB) = 10 * log10(31,622.7766 / 0.000000000001)
SNR (dB) = 10 * log10(31,622,776,600,000,000)
SNR (dB) = 10 * 16.5
SNR (dB) = 165

Therefore, the SNR is 165 dB. The correct answer is C.

upvoted 2 times

danman32 4 months, 3 weeks ago

What is ‚ˆ' supposed to mean?

upvoted 2 times

Amoksepp 4 months, 4 weeks ago

The correct answer is: E: run away because the radio waves reach your device with a power of 31622 W. :D

upvoted 4 times

HungarianDish 10 months ago

Selected Answer: A

The example might be taken from this site:

https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength

"For example, if a client device's radio receives a signal at -75 dBm, and the noise floor is -90 dBm, then the effective SNR is 15 dB. This would then reflect as a signal strength of 15 dB for this wireless connection. "

upvoted 3 times

NJENI 10 months, 2 weeks ago

There is typo coz the the answer shud be 165

upvoted 2 times

Typovy 1 year ago

Selected Answer: A

Asymptote is wrong, A is correct answer

upvoted 1 times

Asymptote 1 year ago

Selected Answer: C

C

SNR = signal strength in dBm - noise

75 - (-90) = 165

if a client device's radio receives a signal at -75 dBm, and the noise floor is -90 dBm, then the effective SNR is 15 dB. This would then reflect as a signal strength of 15 dB for this wireless connection.

Reference:
https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength#:~:text=if%20a%20client%20device%27s%20radio%20receives%20a%20signal%20at%20%2D75%20dBm%2C%20and%20the%20noise%20floor%20is%20%2D90%20dBm%2C%20then%20the%20effective%20SNR%20is%2015%20dB.%C2%A0This%20would%20then%20reflect%20as%20a%20signal%20strength%20of%2015%20dB%20for%20this%20wireless%20connection.%C2%A0

upvoted 2 times

dogdoglee 1 year ago

-75 -(-90) = 15

upvoted 7 times

H3kerman 1 year, 1 month ago

Selected Answer: A

90-75=15

upvoted 1 times

Question #225 *Topic 1*

Refer to the exhibit.

The EtherChannel between SW2 and SW3 is not operational. Which action resolves this issue?

A. Configure the channel-group mode on SW3 Gi0/0 and Gi0/1 to active.

B. Configure the mode on SW2 Gi0/0 to trunk.

C. Configure the channel-group mode on SW2 Gi0/0 and Gi0/1 to on.

D. Configure the mode on SW2 Gi0/1 to access.

Correct Answer: *B*

Community vote distribution

B (100%)

rettich Highly Voted 1 year, 9 months ago

Question and answers are wiered:
-according to config snippet SW2 G0/0 is not configured to participate in the channel
-according to show command none of the Interfaces is participating in the Channel But i can't find a mistake why G0/1 is not working.
The given answer is the best i can find, but it will not fix that all interfaces participate in teh channel afterwards

upvoted 11 times

Burik Highly Voted 5 months, 3 weeks ago

Wrong exhibit, missing channel-group 1 mode active under g0/0.
Fixed exhibit: https://ibb.co/BgC7K4H

upvoted 9 times

HarwinderSekhon 4 months, 4 weeks ago

Thank you sir

upvoted 2 times

CCNPWILL Most Recent 1 month, 1 week ago

Selected Answer: B

Sw2 Gi0/0... has switchport mode access... easy. Answer is B.

upvoted 1 times

sdmejia01 2 months, 1 week ago

Can someone explain why Gi0/1 is down if everything is matching correctly?

upvoted 1 times

danman32 4 months ago

Clearly the G0/0 link is the problem, but wondered why G0/1 would not come up.
Then realized not only is there a link state mismatch, but the Ethernet pair on the same switch is a mismatch so LACP throws the whole thing out, even though G0/1 between switches is a match

upvoted 1 times

Clauster 8 months, 3 weeks ago

2 configurations need to be done
#1 on SW2 need to set G0/0 to Trunk
#2 on SW2 need to set G0/0 to LACP Mode Active < If you don't set this up it will not bundle and it will be missing the config.

upvoted 2 times

danman32 4 months, 3 weeks ago

Apparently the exhibit given here has that cut off.
But it has to be implied it is there, since show eth summ shows that G0/0 is a candidate.

upvoted 1 times

Darude 1 year ago

Selected Answer: B

TCKOON is right the immage is missing the channel-group 1 mode active statement but if you google it you will find the right picture.

upvoted 1 times

bora4motion 1 year ago

Selected Answer: B

easy one, b is correct

upvoted 2 times

tckoon 1 year, 2 months ago

Answer B is correct.
Just the typo in SW2 Gi0/0 config snippet. Where ther is missing " channel-group 1 mode active".

SW2 Gi0/0 , switchport mode access need to chagne to trunk.

upvoted 4 times

Deu_Inder 1 year, 2 months ago

The answer B would not bring the etherchannel up. For the etherchannel to be up, we need 'channel-group 1 mode active on SW2 go0/0.' There are two issues in the config of Gi0/0 of SW2.

upvoted 2 times

nerdymarwa 8 months, 1 week ago

wasn't trunk mode known to be sending out DTP packets, despite being a static configuration? when we use 'swi mode trunk' by default dtp packets will be sent unless we issue 'switchport nonegotiate'

upvoted 1 times

danman32 4 months, 3 weeks ago

But switchport nonegotiate IS configured.

upvoted 1 times

casahit 1 year, 4 months ago

All the physical interfaces in the ether-channel must have the same config (access/trunk, allowed VLANs, duplex, speed) to form logical channel.
Correct answer is B

upvoted 2 times

Question #226 *Topic 1*

Refer to the exhibit.

```
ip nat pool Internet 10.10.10.1 10.10.10.100 netmask 255.255.255.0
ip nat inside source route-map Users pool Internet
!
ip access-list standard Users
  10 permit 192.168.1.0 0.0.0.255
!
route-map Users permit 10
  match ip address Users
```

Which action completes the configuration to achieve a dynamic continuous mapped NAT for all users?

A. Reconfigure the pool to use the 192.168.1.0 address range.

B. Configure a match-host type NAT pool.

C. Increase the NAT pool size to support 254 usable addresses.

D. Configure a one-to-one type NAT pool.

Correct Answer: *C*

Community vote distribution

C (56%) B (44%)

Edwinmolinab Highly Voted 1 year, 5 months ago

Selected Answer: B

B is more appropriate because the sentence says dynamic continuous mapped"

Match Host
The ability to configure NAT to assign the same Host portion of an IP Address and only translate the Network prefix portion of the IP Address. Useful where you are using the host portion as a means to identify or number users uniquely.
to me B is more appropriate. Because C could be aleatory

upvoted 7 times

Me_3e 1 year, 4 months ago

agree with you if focus on the wording "dynamic continuous mapped" but not all users can NAT except range 1-100.

upvoted 2 times

maddyr Most Recent 3 days, 7 hours ago

Selected Answer: C

Only C satisfies the complete statement : dynamic continuous mapped NAT for all users

upvoted 1 times

Brandonkiaora 3 weeks, 1 day ago

The answer is C, as continuous mapping means it has no 'insufficient ip pool' situation.

Why not B, match-host type means 192.168.1.x will be mapped to 10.10.10.x, host is exactly the same. Now the ip pool is not big enough to map all inside IPs.

upvoted 1 times

CCNPWILL 1 month, 1 week ago

C is correct. for ALL users. /24 ... need to increase pool size more than just the 100.

upvoted 1 times

Chuckzero 3 months, 1 week ago

The question is very correct in itself nothing missing or misleading.

The NAT Pool Internet is using a netmask of /24, however, the range configured for users is .1 to .100, barely 100 users out of 254 useable inside global address (10.10.10.0/24).

Again, the user subnet is also using a netmask of /24 (from the inverse of the Users' access-list.

The configuration as it is, is already performing a dynamic continuous mapped NAT for all users but will not be efficient if 254 users (192.168.1.0/24) want to access the internet at the same time.

So, it is expedient that we increase the NAT pool size to support 254 usable addresses, otherwise we might be wasting it and at the same not performing optimally.

upvoted 2 times

Chiaretta 7 months, 2 weeks ago

Selected Answer: C

C is the coorect answer for me

upvoted 1 times

Clauster 8 months, 3 weeks ago

We are missing the Output of the POOL configuration for NAT
That Pool Configuration must not have a range of 254 IP Address in the Public IP Pool it might be something like:
ip nat pool 209.0.5.0 209.0.5.128 netmask 255.255.255.128

If this was in the Output shown then yes 100% the answer would be C I am sure this won't be a problem in the exam and we will select the correct answer.

upvoted 1 times

Clauster 8 months, 4 weeks ago

Again i feel like we are missing more information on the question, if maybe at the top would of said there are less than 220 users in the environment then yea the obvious answer would of been C but we don't have enough info, these type of questions won't come out in the exam because of how lack of information it has.

upvoted 1 times

kewokil120 11 months ago

Selected Answer: C

i think it's the right answer

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: C

>NAT for all users
do you have any idea how many users are on the LAN? NO? me too ...
based on the provided ACL we can guess that about ~254,
so we need to increase NAT size if we need NAT FOR ALL users, right?
here is the description match-host feature probably together they would work better
https://ccie4all.wordpress.com/2013/01/12/nat-with-match-host-keyword/
I mean 1) increase pool 2) configure match-host
cisco_R2(config)#$ Internet 10.0.0.1 10.0.0.10 netmask 255.255.255.0 type ?
match-host Keep host numbers the same after translation
rotary Rotary address pool

cisco_R2(config)#

upvoted 1 times

KOJJY 11 months, 3 weeks ago

Selected Answer: C

i think it's the right answer

upvoted 1 times

MO_2022 11 months, 3 weeks ago

Selected Answer: C

C makes more sense

upvoted 1 times

bora4motion 1 year ago

C makes more sense, don't know why you'd pick B when you can't translate /24 with that.

upvoted 1 times

Tacolicious 1 year ago

Selected Answer: C

It is C

upvoted 1 times

Stylar 1 year ago

Selected Answer: C

Why would you want to chose match-host option? This is just to ensure that you're matching the host portion of the IP range given of the Inside local to the inside global, which is not very applicable here.
Go for C, this is much more applicable, if we assume we need to use the whole IP range of /24 and not just 1-100.

upvoted 1 times

PedroPicapiedra 1 year ago

Selected Answer: C

Clearly is C. It is neccesary more address

upvoted 1 times

Dataset 1 year ago

Selected Answer: C

if all the user must be "translated" ...so is C for me
Regards

upvoted 1 times

Question #227 *Topic 1*

How does EIGRP differ from OSPF?

A. EIGRP is more prone to routing loops than OSPF.

B. EIGRP uses more CPU and memory than OSPF.

C. EIGRP has a full map of the topology, and OSPF only knows directly connected neighbors.

D. EIGRP supports equal or unequal path cost, and OSPF supports only equal path cost.

Correct Answer: *D*

Reference:

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13677-19.html

Community vote distribution

D (100%)

charafDZ 9 months ago

Selected Answer: D

The provided answer is correct.

upvoted 2 times

Question #228 *Topic 1*

Which AP mode allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues?

A. client mode

B. SE-connect mode

C. sensor mode

D. sniffer mode

Correct Answer: *C*
Reference:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-5/b_Cisco_Aironet_Sensor_Deployment_Guide.html.xml

Community vote distribution

C (82%) Other

ChristinaA Highly Voted 1 year, 6 months ago

Selected Answer: C

Sensor mode: this is a special mode which is not listed in the books but you need to know. In this mode, the device can actually function much like a WLAN client would associating and identifying client connectivity issues within the network in real time without requiring an IT or technician to be on site.

upvoted 9 times

Just_little_me Most Recent 2 weeks, 5 days ago

Selected Answer: C

its C
check the cisco site..
Introduction to Sensor Mode

As these wireless networks grow especially in remote facilities where IT professionals may not always be on site, it becomes even more important to be able to quickly identify and resolve potential connectivity issues ideally before the users complain or notice connectivity degradation.

To address these issues, Cisco introduced a Wireless Service Assurance and a new AP mode called sensor mode. For more information, see Cisco Aironet Sensor Deployment Guide.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/b_wl_16_10_cg_chapter_01101110.html

upvoted 1 times

Saboo 4 months, 2 weeks ago

So which one is it? I don't think it is sensor mode because that isn't even a mode on the AP. And this is directly from the posted resources that people are so confidently posting, wondering if people even read the source they are posting:

The sensor is not an AP. It’s designed as a dedicated sensor, simulating wireless client behavior. The sensor does not join the wireless controller because it operates independently from the wireless controller. Instead, the sensor depends on Cisco DNA Center for provisioning, configuration, operation, monitoring, and upgrade.

https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/Cisco_1800S_Sensor_Deployment_Guide_133.pdf

upvoted 1 times

sonjad 4 months, 1 week ago

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/b_wl_16_10_cg_chapter_01101110.html

upvoted 1 times

eww_cybr 5 months ago

https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-active-sensor/guide-c07-744925.html

upvoted 2 times

habibmangal 7 months, 2 weeks ago

Selected Answer: A

The AP mode that allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues is "client mode" (option A). In client mode, the AP acts as a client to connect to another WLAN network and can identify connectivity issues from a client's perspective.

Option B, "SE-connect mode" is not a commonly used AP mode, and there is no standard definition for it.

Option C, "sensor mode," is a mode in which the AP monitors the wireless spectrum for intrusion detection and prevention purposes.

Option D, "sniffer mode," is a mode in which the AP captures and analyzes network traffic for troubleshooting and diagnostic purposes.
upvoted 1 times

LanreDipeolu 3 months, 2 weeks ago
I fully agree with you. "A" is more appropriate
upvoted 1 times

Badger_27 8 months, 2 weeks ago
Missing from the OCG and my online training.
upvoted 3 times

kk_learn 8 months, 3 weeks ago
Selected Answer: C
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/b_wl_16_10_cg_chapter_01101110.html

As these wireless networks grow especially in remote facilities where IT professionals may not always be on site, it becomes even more important to be able to quickly identify and resolve potential connectivity issues ideally before the users complain or notice connectivity degradation.
To address these issues, Cisco introduced a Wireless Service Assurance and a new AP mode called sensor mode.
upvoted 1 times

Clauster 8 months, 4 weeks ago
Selected Answer: C
The answer is 100% C
Here's Cisco's Whitepaper where it clearly states it:
https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/Cisco_1800S_Sensor_Deployment_Guide_133.pdf
upvoted 1 times

nushadu 11 months, 2 weeks ago
Selected Answer: C
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg/b_wl_16_12_cg_chapter_01111101.html
upvoted 1 times

bora4motion 1 year ago
Selected Answer: C
Answer is C - you can even buy a dedicate module which would act as a client. C is the answer.
upvoted 1 times

WINDSON 1 year ago
client mode for sure !
upvoted 2 times

Parot 1 year ago
Answer is Sniffer mode - D.
upvoted 1 times

dougj 1 year, 1 month ago
Selected Answer: D
No such mode as sensor mode now, must be sniffer mode
upvoted 1 times

bora4motion 1 year ago
dude, stop posting wrong stuff:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/b_wl_16_10_cg_chapter_01101110.pdf
upvoted 1 times

FrameRelay 1 year, 1 month ago
D, Sniffer Mode. Because these questions are based on the new Wireless solution, not the old. Previously we only had Monitor or Sensor mode on the 1800, 2800, 3800 etc... in the new Cat9k, cisco introduced Sniffer Mode that allows wireless clients to connect for tshoot purposes, and thats the one Cisco wants to hear, so don't fall for this one its a little tricky as I would have also voted Sensor mode but its not, its Sniffer Mode.
upvoted 1 times

bora4motion 1 year ago
On the 3702 and 3802s it was monitor mode, it wasnt monitor OR sensor. Sniffer is wrong.
You configure the AP in Client mode and pull data into DNA.
client is correct.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/b_wl_16_10_cg_chapter_01101110.pdf
upvoted 1 times

Rene79 1 year, 5 months ago
Sensor mode is new
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/b_wl_16_10_cg_chapter_01101110.html
upvoted 2 times

LeGloupier 1 year, 6 months ago

C seems correct:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-5/b_Cisco_Aironet_Sensor_Deployment_Guide.html.xml
"""
Using a supported AP or dedicated sensor the device can actually function much like a WLAN client would associating and identifying client connectivity issues within the network in real time without requiring an IT or technician to be on site.
"""

upvoted 3 times

GamecockIsland 1 year, 7 months ago

Selected Answer: D

There is no sensor mode. Sniffer makes the most sense

upvoted 1 times

Question #229 *Topic 1*

A client device roams between wireless LAN controllers that are mobility peers. Both controllers have dynamic interfaces on the same client VLAN. Which type of roam is described?

A. intra-VLAN

B. inter-controller

C. intra-controller

D. inter-subnet

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html

Community vote distribution
B (57%) C (43%)

msstanick 5 months, 3 weeks ago

Selected Answer: B
The WLC changes so it is an inter change. Page 437 of Cisco's 31 days before CCNP book.
upvoted 2 times

Keegom 7 months, 2 weeks ago

Selected Answer: B
inter-controller
upvoted 2 times

bk989 7 months, 2 weeks ago

It is inter-controler. Bottom of p.547 of OCG: "When a client roams from one AP to another and those AP's lie on two differenct controllers, the client makes an intercontroller roam." In the context of the question it is making a Layer 2 (same VLAN) inter-controller roam.
upvoted 2 times

Pilgrim5 7 months, 3 weeks ago

Selected Answer: C
C
This is because the 2 controllers are in the client's vlan. If either of the controllers was in other vlan, then the ans would be intercontroller - B
upvoted 3 times

Leoveil 7 months, 3 weeks ago

A client device roams between >>>wireless LAN controllers <<< that are mobility peers,
B. inter-controller : ==> when WLAN interfaces of the WLC are on the same IP subnets
C. intra-controller : ==> APs are both on he same WLC
D. inter-subnet : ==> when WLAN interfaces of the WLC are on different IP subnets
upvoted 3 times

Pilgrim5 7 months, 2 weeks ago

Oh right.. 💯
Thanks!
upvoted 1 times

rafaelinho88 10 months ago

The roam described is an "Intra-Controller Roam" or a "Layer 2 Roam". When a client device moves within the same VLAN and switches between mobility peers (which are wireless LAN controllers in this case), it is considered to be a layer 2 roam. The client device maintains the same IP address and retains its current association with the wireless network, and the roaming process occurs transparently to the client. The wireless LAN controllers exchange information and maintain consistency between themselves, ensuring that the client device is able to maintain its wireless connection as it moves between access points associated with the different controllers.
upvoted 2 times

myhdtv6 4 months, 2 weeks ago

Man, Itra-controller means within the same controller, isn't it ??? the question says, the "CLIENT ROAMS BTW THE CONTROLLERSSSSSSS", that means its btwn two controllers already, so "INTRA" is out of scope alrady
upvoted 2 times

kebkim 1 year, 2 months ago

Intercontroller Layer 2 roaming occurs when the wireless LAN interfaces of the controllers are on the same IP subnet.
upvoted 2 times

Question #230 *Topic 1*

Which component does Cisco Threat Defense use to measure bandwidth, application performance, and utilization?

A. TrustSec

B. Advanced Malware Protection for Endpoints

C. NetFlow

D. Cisco Umbrella

Correct Answer: *C*
Reference:
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/ctd-first-look-design-guide.pdf page 8

Community vote distribution

C (100%)

Asymptote 1 year ago

Selected Answer: C

Answer is correct
link provided expired, here is the valid.

NetFlow is a key element of the original version of the Cisco Cyber Threat Defense solution, and continues to play a vital role in this second-generation update.

NetFlow is a Cisco application that measures IP network traffic attributes of a traffic flow. A flow is identified as a unidirectional stream of packets between a given source and destination as it traverses the Cisco device. NetFlow was initially created to measure network traffic characteristics such as bandwidth, application performance, and utilization.

Reference:
https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

upvoted 3 times

H3kerman 1 year, 1 month ago

Selected Answer: C

NetFlow is an embedded instrumentation to characterize network operation. Visibility into the network is an indispensable tool for IT professionals. In response to new requirements and pressures, network operators are finding it critical to understand how the network is behaving including:

Application and network usage
Network productivity and utilization of network resources
The impact of changes to the network
Network anomaly and security vulnerabilities
Long term compliance issues

upvoted 3 times

Question #231 *Topic 1*

Which IP SLA operation requires the IP SLA responder to be configured on the remote end?

A. UDP jitter

B. ICMP jitter

C. TCP connect

D. ICMP echo

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/46sg/configuration/guide/Wrapper-46SG/swipsla.pdf

Community vote distribution

A (100%)

S_E_T Highly Voted 3 years, 6 months ago

A is the correct answer.
Note: Before you configure a UDP jitter operation on the source device, you must enable the IP SLAs responder on the target device (the operational target).

upvoted 16 times

Networkfate Most Recent 4 months, 1 week ago

) TCP Connect operation to measure the response time taken to perform a TCP Connect operation between a Cisco router and devices using IPv4 or IPv6. TCP Connect accuracy is enhanced by using the IP SLAs Responder at the destination Cisco router
Ans: Only TCP connect

upvoted 1 times

Cooldude89 9 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 2 times

rafaelinho88 10 months ago

Selected Answer: A

UDP Echo IP SLA operation requires the IP SLA responder to be configured on the remote end.

upvoted 2 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

cisco_R2#show runn | section ip sla
ip sla 1
udp-jitter 5.5.5.5 65000
frequency 5
ip sla schedule 1 life forever start-time now
cisco_R2#
cisco_R2#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID Type Destination Stats Return Last
(ms) Code Run
---
*1 udp-jitter 5.5.5.5 RTT=2 OK 19 seconds ago

cisco_R2#

upvoted 2 times

nushadu 11 months, 2 weeks ago

far-end:
cisco_R5#show ip sla responder
General IP SLA Responder on Control port 1967
General IP SLA Responder on Control V2 port 1167
General IP SLA Responder is: Enabled
Number of control message received: 15 Number of errors: 0
Recent sources:
192.168.255.22 [23:25:38.444 UTC Sun Dec 18 2022]
192.168.255.22 [23:25:23.446 UTC Sun Dec 18 2022]
192.168.255.22 [23:25:08.448 UTC Sun Dec 18 2022]
192.168.255.22 [23:24:48.456 UTC Sun Dec 18 2022]

192.168.255.22 [23:24:28.443 UTC Sun Dec 18 2022]
Recent error sources:

Number of control v2 message received: 0 Number of errors: 0
Recent sources:
Recent error sources:

Permanent Port IP SLA Responder
Permanent Port IP SLA Responder is: Enabled

udpEcho Responder:
IP Address Port
84215045 65000
cisco_R5#
cisco_R5#s runn | s ip sla
ip sla responder
ip sla responder udp-echo ipaddress 5.5.5.5 port 65000
cisco_R5#

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

gerilac 2 years, 9 months ago

Correct answere is A

From the document on the link below "...It includes several operations as examples, including configuring the responder, configuring UDP jitter operation, which requires a responder, and configuring ICMP echo operation, which does not require a responder."

https://www.cisco.com/c/en/us/td/docs/switches/metro/me3600x_3800x/software/release/15-5_1_S/configuration/guide/3800x3600xscg/swipsla.pdf

upvoted 3 times

saad_82 2 years, 9 months ago

I will go for C
ip sla responder {tcp-connect | udp-echo} ipaddress ip-address port port-number

upvoted 1 times

39first 2 years, 9 months ago

Definitely A.
There are no service like to send an UDP response back for an UDP echo request.
So UDP echo responder is required for an UDP echo, UDP jitter SLA.

upvoted 2 times

juniper 3 years ago

A is 100% Correct!

upvoted 1 times

BTK0311 3 years, 3 months ago

TCP is transport layer...the destination device can be ANY device using IP OR an IP SLA as a responder. Therefore TCP connect does not require a responder be configured in the remote end. Just that the remote end has an IP.

upvoted 2 times

Skliffi 3 years, 3 months ago

A is correct (UDP jitter)

"Before You Begin
Before configuring a UDP jitter operation on a source device, the IP SLAs Responder must be enabled on the target device (the operational target). The IP SLAs Responder is available only on Cisco IOS software-based devices. To enable the Responder, perform the task in the "Configuring the IP SLAs Responder on the Destination Device" section."
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/xe-16/sla-xe-16-book/sla-udp-jitter.html

"TCP Connect Operation
The IP SLAs TCP Connect operation measures the response time taken to perform a TCP Connect operation between a Cisco device and devices using IP. TCP is a transport layer (Layer 4) Internet protocol that provides reliable full-duplex data transmission. The destination device can be any device using IP or an IP SLAs Responder."
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/xe-16/sla-xe-16-book/sla-tcp-conn.html

upvoted 4 times

nead 3 years, 3 months ago

A is correct all the others can be terminated on an non Cisco device. But for jitter the destination has to understand the packet, so needs to be Cisco device.

upvoted 1 times

chris7411 3 years, 5 months ago

"configuring UDP jitter operation, which
requires a responder, and configuring ICMP echo operation, which does not require a responder. "

So answer A is right

upvoted 3 times

dave369 3 years, 6 months ago

A.
"This section does not include configuration information for all available operations as the configuration information details are included in the Cisco IOS IP SLAs Configuration Guide. It does include several operations as examples, including configuring the responder, configuring UDP jitter operation, which requires a responder, and configuring ICMP echo operation, which does not require a responder. "

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/46sg/configuration/guide/Wrapper-46SG/swipsla.pdf

upvoted 1 times

edlaffer 3 years, 6 months ago

ip sla responder {tcp-connect | udp-echo} ipaddress ip-address port port-number

Configure the switch as an IP SLAs responder.

The optional keywords have these meanings:

•tcp-connect—Enable the responder for TCP connect operations.

•udp-echo—Enable the responder for User Datagram Protocol (UDP) echo or jitter operations.

•ipaddress ip-address—Enter the destination IP address.

•port port-number—Enter the destination port number.

Note The IP address and port number must match those configured on the source device for the IP SLAs operation.

upvoted 3 times

Saqib79 3 years, 6 months ago

Correct Option is C.

upvoted 1 times

Question #232 *Topic 1*

```
<?xml version="1.0" encoding="utf-8"?>
        <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
```

Refer to the exhibit. What does the error message relay to the administrator who is trying to configure a Cisco IOS device?

A. The device received a valid NETCONF request and serviced it without error.

B. The NETCONF running datastore is currently locked.

C. A NETCONF request was made for a data model that does not exist.

D. A NETCONF message with valid content based on the YANG data models was made, but the request failed.

Correct Answer: *C*

Community vote distribution

C (100%)

AliMo123 Highly Voted 2 years, 6 months ago

If a request is made for a data model that doesn't exist on the Catalyst 3850 or a request is made for a leaf that is not implemented in a data model, the Server (Catalyst 3850) responds with an empty data response. This is expected behavior.
https://www.cisco.com/c/en/us/support/docs/storage-networking/management/200933-YANG-NETCONF-Configuration-Validation.html
upvoted 21 times

diegodavid82 2 years, 1 month ago

How, thanks for the link. Answer C is correct.
upvoted 1 times

flash007 Most Recent 4 months, 1 week ago

3. Missing Data Model RPC Error Reply Message

If a request is made for a data model that doesn't exist on the Catalyst 3850 or a request is made for a leaf that is not implemented in a data model, the Server (Catalyst 3850) responds with an empty data response. This is expected behavior.

Tip: Use the NETCONF capabilities functionality to determine which data models are supported by the Catalyst software. See section 2. of Configuring the Centralized Management Platform (Laptop).

<?xml version="1.0" encoding="utf-8"?>
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
upvoted 2 times

pmmg 8 months, 2 weeks ago

Selected Answer: C

From Cisco:

3. Missing Data Model RPC Error Reply Message

If a request is made for a data model that doesn't exist on the Catalyst 3850 or a request is made for a leaf that is not implemented in a data model, the Server (Catalyst 3850) responds with an empty data response. This is expected behavior.

Tip: Use the NETCONF capabilities functionality to determine which data models are supported by the Catalyst software. See section 2. of Configuring the Centralized Management Platform (Laptop).

<?xml version="1.0" encoding="utf-8"?>
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
upvoted 2 times

SheldonC 11 months ago

Correct:
https://www.cisco.com/c/en/us/support/docs/storage-networking/management/200933-YANG-NETCONF-Configuration-Validation.html
upvoted 1 times

WinterRat 2 years, 1 month ago

Where do you see Catalyst 3850 in the question or the error message ?
Is the exhibit correct ?
upvoted 3 times

AlbertoStu 1 year, 8 months ago

The example is taken directly from the linked document.
upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

Question #233 *Topic 1*

Which three methods does Cisco DNA Center use to discover devices? (Choose three.)

A. CDP

B. SNMP

C. LLDP

D. ping

E. NETCONF

F. a specified range of IP addresses

Correct Answer: *ACF*

Community vote distribution

ACF (100%)

v_ermak Highly Voted 2 years, 4 months ago

You can add devices to Cisco DNA Center by using.
● Cisco Discovery Protocol (CDP)
A Layer 2, media-independent, and network-independent device discovery protocol that runs on all Cisco network equipment
● Link Layer Discovery Protocol (LLDP)
A standardized method of adding network devices in multivendor networks
● IP address ranges (Range)
A process using ping sweep to determine device reachability, incrementing through the range sequentially

IP address ranges (Range) - ping

upvoted 9 times

flash007 Most Recent 4 months, 1 week ago

CDP is cisco discovery protocol LLDP is lnk layer discovery protocol which is used to discover many other vendors than cisco IP range will be used to discover devices

upvoted 1 times

forccnp 1 year ago

Selected Answer: ACF

provided answer is correct

upvoted 1 times

timtgh 1 year, 6 months ago

Another bad question. Docs list "IP address range" as one of the methods, but this method is actually ping.

upvoted 3 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

makis32 2 years, 6 months ago

A specified range of IP addresses? That is not a "method". Cisco DNA center uses ICMP to "scan" for devices on a specified subnet or range of IP addresses. Correct Answer is A,C,D.

upvoted 3 times

Broekie 2 years, 5 months ago

Answer A,C,F
Discovery provides the following methods to add devices:
Cisco Discovery Protocol (CDP)
Link Layer Discovery Protocol (LLDP)
IP address ranges

https://www.cisco.com/c/dam/en_us/training-events/product-training/dnac-13/DNAC13_AddingDevicesByUsingDiscovery.pdf

upvoted 9 times

Question #234 *Topic 1*

Which statement about TLS is accurate when using RESTCONF to write configurations on network devices?

A. It is used for HTTP and HTTPS requests.

B. It requires certificates for authentication.

C. It is provided using NGINX acting as a proxy web server.

D. It is not supported on Cisco devices.

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b_166_programmability_cg/b_166_programmability_cg_chapter_01011.html

Community vote distribution
C (55%) B (45%)

craaazymi Highly Voted 3 years, 6 months ago
Correct option is C: "NGINX is an internal webserver that acts as a proxy webserver. It provides Transport Layer Security (TLS)-based HTTPS. RESTCONF request sent via HTTPS is first received by the NGINX proxy web serve,r and the request is transferred to the confd web server for further syntax/semantics check."
upvoted 36 times

Saqib79 Highly Voted 3 years, 6 months ago
Correct Option is B.
upvoted 14 times

NikosTsironis Most Recent 1 month, 4 weeks ago
Selected Answer: C
If you would use Postman i would say B as it would require authehentication but if nginx has aleady preloaded the certs, answer is C
upvoted 1 times

DJ_Yahia 2 months ago
Selected Answer: B
The correct answer is B. It requires certificates for authentication.

TLS (Transport Layer Security) is a cryptographic protocol that provides secure communication over a computer network. It is used to protect data in transit from being intercepted, tampered with, or forged.

TLS is required for authentication when using RESTCONF to write configurations on network devices. This is because RESTCONF is a secure protocol that uses HTTPS. HTTPS is HTTP over TLS, so it uses TLS to encrypt the communication between the client and the server.

The other answer choices are incorrect:

A. It is used for HTTP and HTTPS requests. TLS can be used for both HTTP and HTTPS requests, but it is required for HTTPS requests.
C. It is provided using NGINX acting as a proxy web server. NGINX can be used as a proxy web server for RESTCONF, but it is not required.
D. It is not supported on Cisco devices. TLS is supported on Cisco devices.
upvoted 1 times

wr4net 6 months, 2 weeks ago
stupid question that is not covered at all in OCG. in fact, search of OCG shows no keyword reference to NGINX. However, process of elimination works:
A-no config tool is going to use http
B-certificates (assume client-based is what they are talking about) are typically optional
D-if it didnt apply to cisco, why is it on the test.

So it must be C. but still this is a stupid question. This link hints at nginx

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/168/b_168_programmability_cg/RESTCONF.html
upvoted 4 times

ihateciscoreally 3 months, 1 week ago
man, OCG barely covers NETCONF and RESTCONF :D 2 pages and they require configuration skills on the exam. i know that i can use various resources but then why i paid $70 for the book where things like VRF, NETCONF/RESTCONF, basic python and much more is not covered?
upvoted 1 times

danman32 4 months ago

That definitely is a shortcoming of the book, since configure and verify NETCONF and RESTCONF is a test topic. CBTNuggets covered how to enable both, and NGINX was a dependency.
upvoted 1 times

Raoul78 7 months, 1 week ago

Selected Answer: C

Agree with crasimi
upvoted 1 times

kg2280 8 months ago

Selected Answer: C

NGINX is an internal webserver that acts as a proxy webserver. It provides Transport Layer Security (TLS)-based HTTPS. RESTCONF request sent via HTTPS is first received by the NGINX proxy web serve,r and the request is transferred to the confd web server for further syntax/semantics check.
upvoted 2 times

Rose66 10 months, 3 weeks ago

Selected Answer: C

Look comment of craazymi....
upvoted 1 times

dougj 1 year, 1 month ago

Selected Answer: C

Correct answer is C. RESTCONF doesnt use TLS for authentication, it uses it for transport only.
upvoted 1 times

[Removed] 1 year, 6 months ago

Selected Answer: B

I don't see how it can be any other than B.
Look at RFC8040 (RESTCONF) section 2
https://datatracker.ietf.org/doc/html/rfc8040#section-2
upvoted 4 times

GATUNO 2 years ago

C--- NGINX is an internal webserver that acts as a proxy webserver. It provides Transport Layer Security (TLS)-based HTTPS. RESTCONF request sent via HTTPS is first received by the NGINX proxy web serve,r and the request is transferred to the confd web server for further syntax/semantics check.
upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct
upvoted 2 times

68250test 2 years, 6 months ago

For C : NGINX is an internal webserver that acts as a proxy webserver. It provides Transport Layer Security (TLS)-based HTTPS. RESTCONF request sent via HTTPS is first received by the NGINX proxy web server and the request is transferred to the confd web server for further syntax/semantics check.
For B : To authenticate a client, a RESTCONF server MUST use TLS based client certificates (Section 7.4.6 of [RFC5246]), or MUST use any HTTP authentication scheme defined in the HTTP Authentication Scheme Registry (Section 5.1 in [RFC7235]). A server MAY also support the combination of both client certificates and an HTTP client authentication scheme, with the determination of how to process this combination left as an implementation decision.
upvoted 1 times

netpeer 2 years, 8 months ago

Where is this info in the cert guide????
upvoted 6 times

iGlitch 1 year, 1 month ago

That's why we are here reading the dumps :D
upvoted 3 times

Paco_SP 2 years, 9 months ago

B isn't correct becuase the certificate isn't used to authenticate. "NETCONF and RESTCONF connections must be authenticated using authentication, authorization, and accounting (AAA). As a result, RADIUS or TACACS+ users defined with privilege level 15 access are allowed access into the system."
So the best option is C.
upvoted 1 times

68250test 2 years, 6 months ago

To authenticate a client, a RESTCONF server MUST use TLS based client certificates (Section 7.4.6 of [RFC5246]), or MUST use any HTTP authentication scheme defined in the HTTP Authentication Scheme Registry (Section 5.1 in [RFC7235]). A server MAY also support the combination of both client certificates and an HTTP client authentication scheme, with the determination of how to process this combination left as an implementation decision.
upvoted 3 times

[Removed] 2 years, 10 months ago

C is correct:

NGINX is an internal webserver that acts as a proxy webserver. It provides Transport Layer Security (TLS)-based HTTPS. RESTCONF request sent via HTTPS is first received by the NGINX proxy web serve,r and the request is transferred to the confd web server for further syntax/semantics check.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/168/b_168_programmability_cg/RESTCONF.html

The certificate seems to not be required, but optional

upvoted 3 times

patrickni 3 years, 2 months ago

C is not correct. A NGINX is an optional reverse proxy server for web server performance. The Cisco link just shows a scenario that such a NGINX proxy is used. B is correct. It is required by the RFC. -Dumb Lemon

upvoted 6 times

Question #235 *Topic 1*

What do Cisco DNA southbound APIs provide?

A. interface between the controller and the consumer

B. RESTful API interface for orchestrator communication

C. interface between the controller and the network devices

D. NETCONF API interface for orchestrator communication

Correct Answer: *C*

Community vote distribution

C (100%)

Benzzyy Highly Voted 3 years, 1 month ago

Answer is C

upvoted 7 times

[Removed] Highly Voted 2 years, 10 months ago

Southbound is primarily aimed at non-Cisco "thirdparty" devices!

Northbound: Discovery and management of the network over REST API
Southbound: SDK integration into the DNA Center via device packs to support multivendor environment
Eastbound: Event / Notification Handler
Westbound: Integration of reporting, analysis, service management

upvoted 6 times

Xerath Most Recent 11 months, 3 weeks ago

Selected Answer: C

Provided answer is correct.

upvoted 1 times

H3kerman 1 year, 1 month ago

Selected Answer: C

So, what's the big deal about the Intent API? Cisco DNAC exposes the Intent API to programs outside of the Cisco DNAC platform. Such APIs are commonly called northbound APIs, in contrast to the southbound APIs that the controller uses to communicate with managed devices. Third-party programs can send API calls to the NCP to do almost anything you can do using the Cisco DNA Center web interface! For example, you could write a script to get detailed device information on a switch. In fact, you're going to learn how to do that right now!

upvoted 1 times

Nhan 2 years, 2 months ago

The given answer is correct

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

Question #236 *Topic 1*

Which statement about an RSPAN session configuration is true?

A. Only one session can be configured at a time.

B. A special VLAN type must be used as the RSPAN destination.

C. A filter must be configured for RSPAN sessions.

D. Only incoming traffic can be monitored.

Correct Answer: *B*

Community vote distribution

B (100%)

Hamzaaa Highly Voted 2 years, 7 months ago

B is correct
RSPAN allows you to monitor traffic from source ports distributed over multiple switches, which means that you can centralize your network capture devices. RSPAN works by mirroring the traffic from the source ports of an RSPAN session onto a VLAN that is dedicated for the RSPAN session.

upvoted 8 times

danman32 Most Recent 4 months ago

I've often wondered why a regular VLAN couldn't be used for RSPAN transport and I could never find any info that clearly stated why. I've done it without configuring the VLAN transport for RSPAN.
I believe though is that an RSPAN VLAN has all the usual VLAN control frames suppressed such as BDUs, DTP, VTP, etc so that only the captures are sent through.

upvoted 1 times

H3kerman 1 year, 1 month ago

Selected Answer: B

Configuring RSPAN requires a few more steps. You have to configure a dedicated RSPAN VLAN on both the source and destination switches, like so:
vlan 3333 name RSPAN remote-span

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

hku68 2 years, 10 months ago

B is correct
https://community.cisco.com/t5/networking-documents/understanding-span-rspan-and-erspan/ta-p/3144951

upvoted 4 times

skh 3 years ago

in all participating switches -> This VLAN can be considered a special VLAN type
Answer is correct.

upvoted 1 times

Question #237 *Topic 1*

Which feature must be configured to allow packet capture over Layer 3 infrastructure?

A. RSPAN

B. ERSPAN

C. VSPAN

D. IPSPAN

Correct Answer: *B*
Reference:
https://community.cisco.com/t5/networking-documents/understanding-span-rspan-and-erspan/ta-p/3144951

Community vote distribution
B (100%)

ea8le Highly Voted 2 years, 11 months ago
Encapsulated remote SPAN (ERSPAN): encapsulated Remote SPAN (ERSPAN), as the name says, brings generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains.
upvoted 7 times

flash007 Most Recent 4 months, 1 week ago
ERSPAN is used for capturing in layer 3
upvoted 1 times

Vlad_Is_Love_ua 8 months, 4 weeks ago
Selected Answer: B
The Cisco ERSPAN mirrors traffic on one or more “source” ports and delivers the mirrored traffic to one or more “destination” ports on another switch. 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” switch. ERSPAN supports source ports, source VLANs, and destination ports on different switches, which provide Remote Monitoring of multiple switches across your network.
upvoted 1 times

H3kerman 1 year, 1 month ago
Selected Answer: B
Last up in the SPAN lineup is ERSPAN. The concept is similar to RSPAN, except because we're encapsulating frames in IP, we need to specify IP addresses and uniquely identify each monitoring session.
upvoted 3 times

LM77 1 year, 10 months ago
Answer B

https://community.cisco.com/t5/networking-documents/understanding-span-rspan-and-erspan/ta-p/3144951
upvoted 1 times

kthekillerc 2 years, 2 months ago
Provided answer is correct
upvoted 1 times

Refer to the exhibit.

```
vlan 222
 remote-span
!
vlan 223
 remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

What is the result when a technician adds the monitor session 1 destination remote vlan 223 command?

A. The RSPAN VLAN is replaced by VLAN 223.

B. RSPAN traffic is sent to VLANs 222 and 223.

C. An error is flagged for configuring two destinations.

D. RSPAN traffic is split between VLANs 222 and 223.

Correct Answer: *A*

Community vote distribution

A (100%)

jmaroto Highly Voted 2 years, 8 months ago

A is correct. This is the result in a lab.
switch-1(config)#do sh run | s monitor
monitor session 1 source interface Gi1/0/2 rx
monitor session 1 source interface Gi1/0/1 tx
monitor session 1 source interface Po14
monitor session 1 destination remote vlan 222

switch-1(config)#do sh monitor session 1
Session 1

Type : Remote Source Session
Source Ports :
RX Only : Gi1/0/2
TX Only : Gi1/0/1
Both : Po14
Dest RSPAN VLAN : 222

switch-1(config)#monitor session 1 destination remote vlan 223
switch-1(config)#do sh run | s monitor
monitor session 1 source interface Gi1/0/2 rx
monitor session 1 source interface Gi1/0/1 tx
monitor session 1 source interface Po14
monitor session 1 destination remote vlan 223
switch-1(config)#do sh monitor session 1
Session 1

Type : Remote Source Session
Source Ports :
RX Only : Gi1/0/2
TX Only : Gi1/0/1
Both : Po14
Dest RSPAN VLAN : 223

upvoted 20 times

rggod 2 years, 7 months ago

I'm missing that output. my pics never shows destination remote vlan change

upvoted 1 times

Hugh_Jazz 2 years, 1 month ago

Concur, just to be on the safe side, I just ran it through a switch config. Got the same result, answer is A.

upvoted 2 times

MaxwellJK Most Recent 4 months, 1 week ago

Selected Answer: A

DIST2(config)#monitor session 1 destination remote vlan 222
DIST2(config)#do sh run | sec remote
remote-span
remote-span
monitor session 1 destination remote vlan 222
DIST2(config)#monitor session 1 destination remote vlan 223
DIST2(config)#do sh run | sec remote
remote-span
remote-span
monitor session 1 destination remote vlan 223
DIST2(config)#

upvoted 1 times

youtri 1 year, 11 months ago

Selected Answer: A

overwriting,given answer is correct

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

Commando1664 2 years, 6 months ago

Just tried in a lab and got C

monitor session 1 source interface Gi0/1
monitor session 1 destination interface Gi0/2
Access_Sw01(config)#$sion 1 destination interface gigabitEthernet 0/1
% Interface(s) Gi0/1 already configured as monitor sources

upvoted 1 times

MerlinTheWizard 10 months ago

That is not a C option, you're trying to use source interface as destination.. duh

upvoted 2 times

Question #239 *Topic 1*

```
SW1#sh monitor session all
Session 1
------------

Type                     : Remote Destination Session
Source RSPAN VLAN        : 50

Session 2
------------

Type                     : Local Session
Source Ports             :
      Both               : Fa0/14
  Destination Ports      : Fa0/15
      Encapsulation      : Native
            Ingress      : Disables
```

Refer to the exhibit. An engineer configures monitoring on SW1 and enters the show command to verify operation. What does the output confirm?

A. RSPAN session 1 is incompletely configured for monitoring.

B. RSPAN session 1 monitors activity on VLAN 50 of a remote switch.

C. SPAN session 2 monitors all traffic entering and exiting port FastEthernet 0/15.

D. SPAN session 2 only monitors egress traffic exiting port FastEthernet 0/14.

Correct Answer: *A*

Community vote distribution

A (100%)

AliMo123 Highly Voted 2 years, 6 months ago

A is correct.
Session 1 is missing destination port
Session 2 is missing source port

upvoted 11 times

youtri 1 year, 11 months ago

session 2
src port is f0/14

upvoted 7 times

rafaelinho88 Most Recent 10 months ago

Selected Answer: A

SW1 has been configured with the following commands:
SW1(config)#monitor session 1 source remote vlan 50
SW1(config)#monitor session 2 source interface fa0/14
SW1(config)#monitor session 2 destination interface fa0/15
The session 1 on SW1 was configured for Remote SPAN (RSPAN) while session 2 was configured for local SPAN. For RSPAN we need to configure the destination port to complete the configuration.
Note: In fact we cannot create such a session like session 1 because if we only configure Source RSPAN VLAN 50 (with the command monitor session 1 source remote vlan 50) then we will receive a Type: Remote Source Session (not Remote Destination Session)

upvoted 2 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

Question #240 *Topic 1*

A network is being migrated from IPv4 to IPv6 using a dual-stack approach. Network management is already 100% IPv6 enabled.
In a dual-stack network with two dual-stack NetFlow collectors, how many flow exporters are needed per network device in the flexible NetFlow configuration?

A. 1

B. 2

C. 4

D. 8

Correct Answer: *B*

Community vote distribution

B (67%) A (33%)

DJOHNR Highly Voted 3 years, 3 months ago

The answer is B : 2, but not because of IPv4 and IPV6.

A dual-stack device is a device with network interfaces that can originate and understand both IPv4 and IPv6 packets.

It is because each flow collector can only send to a single destination. In this question there are two NetFlow collectors... thus two destination. Thus the need for 2 flow exporters.

Each flow exporter supports only one destination. If you want to export the data to multiple destinations, you must configure multiple flow exporters and assign them to the flow monitor.

You can export to a destination using either an IPv4 or IPv6 address.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/cfg-de-fnflow-exprts.html

Look under the section "Configuring the Flow Exporter"

upvoted 46 times

slopeza0270 Highly Voted 3 years, 5 months ago

Two flow exporters, one that matches ipv4 and one that matches ipv6

upvoted 5 times

Elmaestro Most Recent 1 week, 1 day ago

B is correct because TWO dual-stack NetFlow collectors = two exporters

upvoted 1 times

CCNPWILL 1 month, 1 week ago

Selected Answer: B

Answer B.

upvoted 1 times

orenoren 1 month, 3 weeks ago

Selected Answer: B

6-4=2 b is the correct answer

upvoted 1 times

ibogovic 5 months ago

Selected Answer: A

In a dual-stack network with two dual-stack NetFlow collectors, only one flow exporter is needed per network device in the flexible NetFlow configuration.

In the context of NetFlow, a flow exporter is responsible for sending NetFlow data (flow records) to the configured NetFlow collectors. In a dual-stack network, both IPv4 and IPv6 traffic is present, and since the network management is already 100% IPv6 enabled, the NetFlow data for both IPv4 and IPv6 flows will be sent to the two dual-stack NetFlow collectors.

So, regardless of whether the network device is handling both IPv4 and IPv6 traffic (dual-stack) or just one of them, a single flow exporter is sufficient to send flow records to the two dual-stack NetFlow collectors.

The correct answer is A. 1 flow exporter per network device.

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

spapi0390 3 years ago

@DJOHNR is right, two exporters for two dual stack collectors. Two dual stack collector have 4 IPs (two IPv4 and two IPv6), which doesn't mean that 4 exporters needed.

upvoted 3 times

TheNetworkStudent 3 years, 2 months ago

If you use the legacy "ip flow-export" way of configuring things you can set multiple destinations so the answer could be 1. But they ask specifically for the "Cisco" way because it states flexible netflow.

Using the Cisco way with the command "flow exporter <WORD>" you can set only 1 destination per flow exporter, so you'll need to configure 2 flow exporter. B is correct.

upvoted 2 times

micbosh 3 years, 3 months ago

one exporter but 2 monitorars ... so A

upvoted 1 times

Nirvana 3 years, 5 months ago

I think A is correct , It says per Network!

upvoted 1 times

CBlu 3 years, 5 months ago

"per network device", so it should be 2, I think. (for ipv4 & ipv6)

upvoted 2 times

Question #241 *Topic 1*

A network engineer is configuring Flexible NetFlow and enters these commands. sampler NetFlow1 mode random one-out-of 100 interface fastethernet 1/0 flow-sampler NetFlow1
What are two results of implementing this feature instead of traditional NetFlow? (Choose two.)

A. Only the flows of top 100 talkers are exported.

B. CPU and memory utilization are reduced.

C. The number of packets to be analyzed are reduced.

D. The data export flow is more secure.

E. The accuracy of the data to be analyzed is improved.

Correct Answer: *BC*

Community vote distribution

BC (100%)

examShark Highly Voted 2 years, 6 months ago

The given answer is correct

upvoted 7 times

SandyIndia Highly Voted 2 years, 2 months ago

Flow sampling reduces the CPU overhead of analyzing traffic with Flexible NetFlow by reducing the number of packets that are analyzed. Flow samplers are used to reduce the load on the device that is running by limiting the number of packets that are selected for analysis.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/use-fnflow-redce-cpu.pdf

upvoted 6 times

Raoul78 Most Recent 7 months, 1 week ago

Selected Answer: BC

Answers are correct

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answers are correct B,C

upvoted 2 times

Nickelkeep 2 years, 3 months ago

correct answer is B, E

upvoted 1 times

```
flow record Recorder
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
!
flow exporter Exporter
 destination 192.168.100.22
 transport udp 2055
!
flow monitor Monitor
 exporter Exporter
 record Recorder
!
et-analytics
 ip flow-export destination 192.168.100.22 2055
!
interface gi1
ip flow monitor Monitor input
ip flow monitor Monitor output
et-analytics enable
!
```

Refer to the exhibit. An engineer must add the SNMP interface table to the NetFlow protocol flow records. Where should the SNMP table option be added?

A. under the interface

B. under the flow record

C. under the flow monitor

D. under the flow exporter

Correct Answer: *D*

Community vote distribution

D (67%) B (33%)

Adrenalina73 Highly Voted 2 years, 2 months ago

D. is correct: https://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html
The following example causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option interface-table
upvoted 8 times

nushadu Highly Voted 11 months, 2 weeks ago

Selected Answer: D

cisco_R2(config)#flow exporter test
cisco_R2(config-flow-exporter)#option ?
application-attributes Application Attributes Table Option
application-table Application Table Option
c3pl-class-table C3PL class cce-id table
c3pl-policy-table C3PL policy cce-id table
exporter-stats Exporter Statistics Option
inspect-class-table Policy Firewall Class Table
inspect-ext-event-table Policy Firewall Extended Event Table
inspect-protocol-table Policy Firewall Protocol Table
inspect-zonepair-table Policy Firewall Zone-pair Table
interface-table Interface SNMP-index-to-name Table Option
metadata-version-table Metadata Version Table Option
sampler-table Export Sampler Option
sub-application-table Sub Application Table Option
vrf-table VRF ID-to-name Table Option

cisco_R2(config-flow-exporter)#option
upvoted 5 times

ibogovic Most Recent 5 months ago

Selected Answer: B

I would go with B:

The complete modified configuration would look like this:

flow record Recorder
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect interface input-snmp
collect interface output-snmp
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last

flow exporter Exporter
destination 192.168.100.22
transport udp 2055

flow monitor Monitor
exporter Exporter
record Recorder

ip flow-export destination 192.168.100.22 2055

interface GigabitEthernet0/1
ip flow monitor Monitor input
ip flow monitor Monitor output

et-analytics enable

In this modified configuration, the SNMP interface table option is included in the flow record configuration. The flow exporter, flow monitor, and interface configurations remain unchanged.

upvoted 3 times

nopenotme123 1 year, 4 months ago

Selected Answer: D

The following example causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option interface-table

upvoted 1 times

Edwinmolinab 1 year, 5 months ago

Given answer is correct
Examples
The following example causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:

Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option exporter-stats

The following example causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option interface-table

upvoted 2 times

rpidcock 2 years ago

Confusing question, but I agree with Adrenalina73, D is the correct answer.

upvoted 1 times

error_909 2 years, 2 months ago

Provided Answer is correct

https://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html

upvoted 3 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 2 times

spapi0390 2 years, 4 months ago

The following example causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

Router(config)# flow exporter FLOW-EXPORTER-1

Router(config-flow-exporter)# option interface-table

upvoted 3 times

HK010 2 years, 4 months ago

Actually it's A.
Step 6 collect counter {bytes [exported | long]
flows [exported] | packets} [exported |
long]
or
collect timestamp sys-uptime {first |
last}
or
collect interface {input | output} snmp
Page 3 states "collect interface {input | output} snmp" under "flow record".
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-0_1_se/configuration/guide/3750xcg/swmnetflow.pdf

upvoted 1 times

gtddrf 2 years, 4 months ago

The answer is B.
In the same document, steps 3 thru 6 are done under Step 2 "flow record record-name"

upvoted 1 times

sasatrickovic 2 years, 1 month ago

D.
The following example causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

Router(config)# flow exporter FLOW-EXPORTER-1

Router(config-flow-exporter)# option interface-table

upvoted 1 times

certcisco 2 years, 4 months ago

I would think B?
Page 3 states "collect interface {input | output} snmp" under "flow record".
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-0_1_se/configuration/guide/3750xcg/swmnetflow.pdf

upvoted 2 times

HK010 2 years, 4 months ago

It's A thanks for reference.
collect interface {input | output} snmp

upvoted 1 times

ABC123 2 years, 4 months ago

Isn't it B ?!

upvoted 3 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 2 times

Question #243 *Topic 1*

A network administrator is implementing a routing configuration change and enables routing debugs to track routing behavior during the change. The logging output on the terminal is interrupting the command typing process.
Which two actions can the network administrator take to minimize the possibility of typing commands incorrectly? (Choose two.)

A. Configure the logging synchronous global configuration command.

B. Configure the logging synchronous command under the vty.

C. Increase the number of lines on the screen using the terminal length command.

D. Configure the logging delimiter feature.

E. Press the TAB key to reprint the command in a new line.

Correct Answer: *BE*

Community vote distribution

BE (100%)

Saqib79 Highly Voted 3 years, 6 months ago

Correct Options are B & E.

upvoted 32 times

nep1019 Highly Voted 3 years, 5 months ago

Definitely B and E. B is correct according to the doc at
https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_l1.html

logging synchronous

To synchronize unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty, use the logging synchronous command in line configuration mode. To disable synchronization of unsolicited messages and debug output, use the no form of this command.

logging synchronous [level severity-level | all] [limit number-of-lines]

upvoted 14 times

mgiuseppe86 Most Recent 2 months, 3 weeks ago

Selected Answer: BE

I mean i have configured thousands of switches. its B and E. simply hitting tab, even if the command is wrong, will repeat what you have typed on a new line.

upvoted 1 times

kewokil120 10 months, 2 weeks ago

Selected Answer: BE

BE is right

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 3 times

BigMomma4752 2 years, 7 months ago

The correct answers are B&E.

upvoted 3 times

jmaroto 2 years, 8 months ago

A is wrong. There isn't a global command "logging synchronous".

R10(config)#logging synchronous
Translating "synchronous"
^
% Invalid input detected at '^' marker.

R10(config)#

upvoted 10 times

cvndani 1 year, 10 months ago

not a global command, under VTY exists, read the question again

upvoted 1 times

saad_82 2 years, 9 months ago

B and E is correct
A not possible as logging syn cant be enabled globally
C this is just to increate the output lines while issuing show command for example
D Append delimiter to syslog messages

upvoted 3 times

Wesgo 2 years, 9 months ago

"The logging synchronous GLOBAL CONFIGURATION command also affects the display of messages to the console. When this command is enabled, messages appear only after you press Return."
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swlog.html

upvoted 1 times

Wesgo 2 years, 9 months ago

It's A+B!
REQUIRED: conf t
OPTIONAL: line vty x y
REQUIRED: logging synchronous

E is wrong, as TAB will not repeat previous user input if had not been interrupted in the middle of a word.

upvoted 2 times

39first 2 years, 9 months ago

B and E. logging synch can be configured only in line configuration mode.

upvoted 1 times

thassan 2 years, 10 months ago

Correct options are B, E.

upvoted 1 times

Nenzo85 2 years, 11 months ago

Correct A & E:
"The logging synchronous global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press Return.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swlog.html"

upvoted 1 times

brface 2 years, 12 months ago

B&E is correct

upvoted 1 times

Helloory 3 years ago

Correct answers are B and E

upvoted 1 times

BTK0311 3 years, 3 months ago

The logging synchronous global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press Return. For more information, see the "Synchronizing Log Messages" section.

upvoted 1 times

Dcisco 3 years, 1 month ago

You cannot configure logging synchronous globally online in console and vty ine

upvoted 1 times

BTK0311 3 years, 3 months ago

Unless I'm missing something. When I use tab it's to complete out a command. Such as. Sh-TAB then I get show. The up arrow will reprint the last line.

upvoted 1 times

akbntc 3 years, 3 months ago

Correct answer: B & E.

upvoted 2 times

Question #244 *Topic 1*

When using TLS for syslog, which configuration allows for secure and reliable transportation of messages to its default port?

A. logging host 10.2.3.4 vrf mgmt transport tcp port 514

B. logging host 10.2.3.4 vrf mgmt transport udp port 514

C. logging host 10.2.3.4 vrf mgmt transport tcp port 6514

D. logging host 10.2.3.4 vrf mgmt transport udp port 6514

Correct Answer: *C*
Reference:
https://tools.ietf.org/html/rfc5425

Community vote distribution
C (100%)

H3kerman Highly Voted 1 year, 1 month ago

Selected Answer: C
TCP/514 - shell cmd
UDP/514 - syslog
TCP/6514 - syslog over TLS
UDP/6514 - syslog over DTLS
upvoted 14 times

YTAKE Highly Voted 2 years, 1 month ago
key to remember:

secure and reliable
upvoted 6 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: C
TCP port 6514 is the default port for syslog over TLS.
logging host 111.0.0.1 transport tcp port 6514
upvoted 1 times

kthekillerc 2 years, 2 months ago
Provided answer is correct
upvoted 1 times

Hamzaaa 2 years, 7 months ago
C is true
The TCP port 6514 has been allocated as the default port for syslog over TLS, as defined in this document.
upvoted 4 times

Question #245 *Topic 1*

Refer to this output.
R1# *Feb 14 37:09:53.129: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
What is the logging severity level?

A. notification

B. emergency

C. critical

D. alert

Correct Answer: *A*

Community vote distribution

A (100%)

Hamzaaa Highly Voted 2 years, 7 months ago

0 —emergency: System unusable.
1 —alert: Immediate action needed.
2 —critical: Critical condition—default level.
3 —error: Error condition.
4 —warning: Warning condition.
5 —notification: Normal but significant condition.
6 —informational: Informational message only.

upvoted 20 times

adamzet33 3 weeks, 4 days ago

EACEWNID

upvoted 1 times

youtri 1 year, 8 months ago

7 -debug
thanks

upvoted 5 times

WINDSON Highly Voted 1 year ago

Even awesome cisco engineer will need ice-cream daily

upvoted 18 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: A

cisco_R2(config)#logging buffered ?
<0-7> Logging severity level
<4096-2147483647> Logging buffer size
alerts Immediate action needed (severity=1)
critical Critical conditions (severity=2)
debugging Debugging messages (severity=7)
discriminator Establish MD-Buffer association
emergencies System is unusable (severity=0)
errors Error conditions (severity=3)
filtered Enable filtered logging
informational Informational messages (severity=6)
notifications Normal but significant conditions (severity=5)
warnings Warning conditions (severity=4)
xml Enable logging in XML to XML logging buffer
<cr>

cisco_R2(config)#logging buffered

upvoted 2 times

bitsandbytes 1 year ago

Selected Answer: A

Every Awesome Cisco Engineer Will Need Icecream Daily
0 1 2 3 4 5 6 7

upvoted 5 times

Dataset 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 3 times

gtddrf 2 years, 3 months ago

Answer is A (Protocol up/down status is a notification)
From https://community.cisco.com/t5/networking-documents/how-to-configure-logging-in-cisco-ios/ta-p/3132434
Router messages
0 Emergencies System shutting down due to missing fan tray
1 Alerts Temperature limit exceeded
2 Critical Memory allocation failures
3 Errors Interface Up/Down messages
4 Warnings Configuration file written to server, via SNMP request
5 Notifications Line protocol Up/Down
6 Information Access-list violation logging
7 Debugging Debug messages

upvoted 4 times

XalaGyan 1 year, 11 months ago

DinWec AE
thats how i remember them.

upvoted 2 times

netpeer 2 years, 8 months ago

Severity is 5 which is notification

upvoted 2 times

skh 3 years ago

A
(Level 5 – notification)
Based on Cisco information: "Interface up or down transitions and system restart messages, displayed at the notifications level. This message is only for information; switch functionality is not affected."
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sga/configuration/guide/config/log.html

upvoted 4 times

Question #246 *Topic 1*

An engineer reviews a router's logs and discovers the following entry. What is the event's logging severity level?
Router# *Jan 01 38:24:04.401: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up

A. error

B. warning

C. informational

D. notification

Correct Answer: *A*

Community vote distribution

A (100%)

RhJ72 Highly Voted 2 years, 3 months ago

Every Awesome Cisco Engineer Will Need Icecream Daily
upvoted 27 times

well123 9 months ago

hhhh this is cool, thanks...
upvoted 1 times

netplwiz Highly Voted 2 years, 9 months ago

A. Error is correct. The Number in %LINK-3-UPDOWN indicates this is logging level 3:

Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:
0 —emergency: System unusable
1 —alert: Immediate action needed
2 —critical: Critical condition—default level
3 —error: Error condition
4 —warning: Warning condition
5 —notification: Normal but significant condition
6 —informational: Informational message only
7 —debugging: Appears during debugging only

https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/sm/logging-level.html
upvoted 20 times

LanreDipeolu Most Recent 3 months, 2 weeks ago

Selected Answer: A

A is the correct answer. The acronym I use is Edwards, Always, Cries, Even, When, Nobody, Is, Dead
upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

cisco_R2(config)#logging buffered ?
<0-7> Logging severity level
<4096-2147483647> Logging buffer size
alerts Immediate action needed (severity=1)
critical Critical conditions (severity=2)
debugging Debugging messages (severity=7)
discriminator Establish MD-Buffer association
emergencies System is unusable (severity=0)
errors Error conditions (severity=3) <<<<<<<<<<<<<<<<<<<<<<<<
filtered Enable filtered logging
informational Informational messages (severity=6)
notifications Normal but significant conditions (severity=5)
warnings Warning conditions (severity=4)
xml Enable logging in XML to XML logging buffer
<cr>

cisco_R2(config)#logging buffered
upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct
upvoted 2 times

gtddrf 2 years, 3 months ago

Answer is A (Interfaces up/down status is an error)
From https://community.cisco.com/t5/networking-documents/how-to-configure-logging-in-cisco-ios/ta-p/3132434
Router messages
0 Emergencies System shutting down due to missing fan tray
1 Alerts Temperature limit exceeded
2 Critical Memory allocation failures
3 Errors Interface Up/Down messages
4 Warnings Configuration file written to server, via SNMP request
5 Notifications Line protocol Up/Down
6 Information Access-list violation logging
7 Debugging Debug messages

upvoted 1 times

Rockford 2 years, 6 months ago

Logging severity messages:
seq no:timestamp: %facility-severity-MNEMONIC:description
severity - Single-digit code from 0 to 7 that is the severity of the message
In this case it is 3 therefore error...

upvoted 2 times

Hamzaaa 2 years, 7 months ago

0 —emergency: System unusable.
1 —alert: Immediate action needed.
2 —critical: Critical condition—default level.
3 —error: Error condition.
4 —warning: Warning condition.
5 —notification: Normal but significant condition.
6 —informational: Informational message only.

upvoted 2 times

netpeer 2 years, 8 months ago

Severity is 3 which is error

upvoted 2 times

netpeer 2 years, 8 months ago

The previous question is for the same topic and was notification, now it's error???
Come on...

upvoted 1 times

hybl2467 1 year, 8 months ago

Read the question (R1# *Feb 14 37:09:53.129: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up)

upvoted 1 times

hybl2467 1 year, 8 months ago

%LINEPROTO-5-UPDOWN not %LINK-3-UPDOWN

upvoted 1 times

danman32 4 months ago

Yes but would a link going UP rather than DOWN really generate an error?
But even if not a typo, go by the severity level # in the syslog for the answer.

upvoted 1 times

sabaheta 2 years, 9 months ago

Yup its level 3 -error, I was looking at wrong output. Correct answer A.

upvoted 2 times

sabaheta 2 years, 9 months ago

I'm not sure about this one is it "D. notification", or the "C warning", since there is 401 ?

upvoted 2 times

sabaheta 2 years, 9 months ago

D. correct answer this is notification.

upvoted 3 times

Question #247 *Topic 1*

Refer to the exhibit.

```
monitor session 1 source vlan 10 - 12 rx
monitor session 1 destination interface gigabitethernet0/1
```

An engineer must configure a SPAN session.

What is the effect of the configuration?

A. Traffic received on VLANs 10, 11, and 12 is copied and sent to interface g0/1.

B. Traffic sent on VLANs 10 and 12 only is copied and sent to interface g0/1.

C. Traffic sent on VLANs 10, 11, and 12 is copied and sent to interface g0/1.

D. Traffic received on VLANs 10 and 12 only is copied and sent to interface g0/1.

Correct Answer: *A*

Community vote distribution

A (100%)

network_gig 1 year, 1 month ago

Selected Answer: A

It has Rx in it, which means only the receiving traffic will be monitored; hence, option C is wrong. The command has a range of VLANs and hence options B and D are incorrect. A is the correct answer.

upvoted 1 times

c4byp 1 year, 10 months ago

right, rx : received, tx: sent

upvoted 3 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

Refer to the exhibit.

```
vlan 222
 remote-span
!
vlan 223
 remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

These commands have been added to the configuration of a switch.

Which command flags an error if it is added to this configuration?

A. monitor session 1 source interface port-channel 6

B. monitor session 1 source vlan 10

C. monitor session 1 source interface FastEthemet0/1 rx

D. monitor session 1 source interface port-channel 7, port-channel 8

Correct Answer: *B*

Community vote distribution

B (88%) 13%

Hack4 Highly Voted 2 years, 5 months ago

B the monitor session can source interface or vlan not both at the same time

upvoted 18 times

Mac13 Highly Voted 2 years, 7 months ago

I labbed this on a switch, and it's answer B.

Switch#sh run | i moni
monitor session 1 source interface Gi0/2 rx
monitor session 1 source interface Gi0/1 tx
monitor session 1 source interface Po5
monitor session 1 destination remote vlan 222

Switch(config)#monitor session 1 source vlan 10
% Cannot add VLANs as sources for SPAN session 1

A range of addresses can be added (D), separated by a comma (,):

Switch(config)#monitor session 1 source interface port-channel 5 ?
, Specify another range of interfaces
both Monitor received and transmitted traffic
rx Monitor received traffic only
tx Monitor transmitted traffic only
<cr>

upvoted 11 times

[Removed] Most Recent 5 months ago

Selected Answer: B

a monitor session can have multiple source interface, or vlans, but not a mix of both.

upvoted 1 times

HungarianDish 10 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_40_se/configuration/guide/scg1/swspan.pdf

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_01101101.html
upvoted 1 times

TSKARAN 10 months ago

Selected Answer: B

I tried to add to the section ,
SW-1#show run | sec monitor
monitor session 1 source interface Gi0/3

SW-1(config)#monitor session 1 source vlan 30
% Cannot add VLANs as sources for SPAN session 1
SW-1(config)#
monitor session 1 destination remote vlan 110
upvoted 2 times

TSKARAN 10 months ago

{Retyping in the correct order & format}

I tried to add to the section ,
SW-1#show run | sec monitor
monitor session 1 source interface Gi0/3
monitor session 1 destination remote vlan 110

SW-1(config)#monitor session 1 source vlan 30
% Cannot add VLANs as sources for SPAN session 1
SW-1(config)#
upvoted 1 times

Rose66 10 months, 3 weeks ago

Selected Answer: B

B because Interfaces and VLAN aren't allowed together
upvoted 1 times

MO_2022 11 months, 2 weeks ago

Selected Answer: B

Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session
upvoted 2 times

WINDSON 1 year ago

crazy, only 1 people answer is correct in all comments!
onkel_andi, you are awesome !
upvoted 1 times

onkel_andi 1 year, 1 month ago

Selected Answer: C

Because of FastEthemet0/1
upvoted 1 times

Masashi_O 2 years, 6 months ago

Answer is B
https://community.cisco.com/t5/switching/span-configuration/td-p/939322
upvoted 1 times

Hamzaaa 2 years, 7 months ago

B is correct
A monitor session can source from interfaces or VLANs – not both at the same time.
upvoted 3 times

netpeer 2 years, 7 months ago

Correction: tried on a switch and it's possible, it's D
upvoted 3 times

netpeer 2 years, 8 months ago

B agree with audi87
upvoted 1 times

Audi87 2 years, 8 months ago

Answer is B

A monitor session can source from interfaces or VLANs – not both at the same time.

RSPAN consists of at least one RSPAN source session, an RSPAN VLAN, and at least one RSPAN destination session. You separately configure RSPAN source sessions and RSPAN destination sessions on different network devices. To configure an RSPAN source session on a device, you associate a set of source ports or source VLANs with an RSPAN VLAN.
Traffic monitoring in a SPAN session has these restrictions:
+ Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.

upvoted 4 times

micmic70 2 years, 8 months ago

It should be D

upvoted 1 times

Question #249 *Topic 1*

Which method does Cisco DNA Center use to allow management of non-Cisco devices through southbound protocols?

A. It creates device packs through the use of an SDK.

B. It uses an API call to interrogate the devices and register the returned data.

C. It obtains MIBs from each vendor that details the APIs available.

D. It imports available APIs for the non-Cisco device in a CSV format.

Correct Answer: *A*

Community vote distribution

A (100%)

Miguex125 Highly Voted 2 years, 6 months ago

Answer is correct, "Cisco DNA Center allows customers to manage their non-Cisco devices through the use of a Software Development Kit (SDK) that can be used to create Device Packages for third-party devices".

https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/multivendor-support-southbound

upvoted 11 times

shefo1 Most Recent 3 days, 20 hours ago

Selected Answer: A

from OCG , p.697

Cisco DNA Center integrates with many other tools, such as Active Directory, Identity Services Engine (ISE), ServiceNow, and Infoblox. This is possible because of the open APIs and SDKs available for Cisco DNA Center. Because of the integration with Active Directory and ISE, all the context of the user is searchable in Cisco DNA Center.

upvoted 1 times

Tyrandemer 1 year, 4 months ago

For information.
From version 2.1.2 Cisco DNA not support multivendor SDK tool.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/release_notes/b_cisco_dna_center_rn_2_1_2.html#concept_ttn_df3_1kb

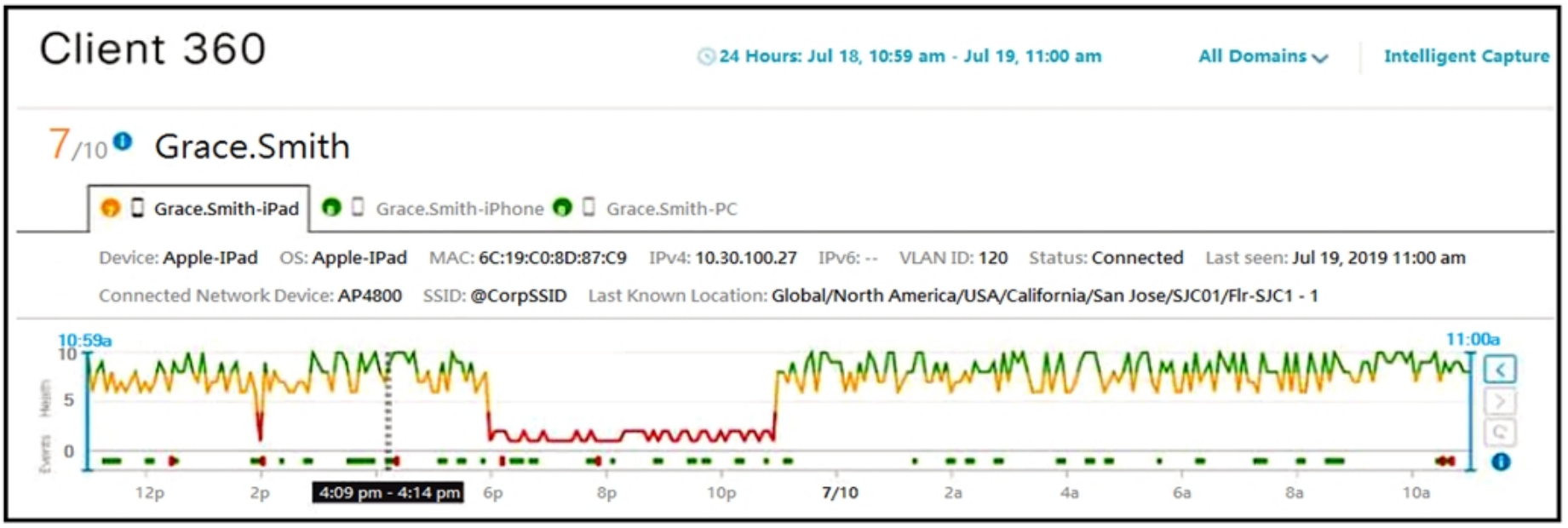
upvoted 3 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

Question #250 *Topic 1*



Refer to the exhibit. Cisco DNA Center has obtained the username of the client and the multiple devices that the client is using on the network. How is Cisco DNA
Center getting these context details?

A. Those details are provided to Cisco DNA Center by the Identity Services Engine.

B. The administrator had to assign the username to the IP address manually in the user database tool on Cisco DNA Center.

C. Cisco DNA Center pulled those details directly from the edge node where the user connected.

D. User entered those details in the Assurance app available on iOS and Android devices.

Correct Answer: *C*

Community vote distribution

A (68%) C (32%)

kthekillerc Highly Voted 2 years, 2 months ago

Provided answer is correct

upvoted 9 times

SandyIndia Highly Voted 2 years, 2 months ago

Identity Services Engine
Cisco Identity Services Engine (ISE) is a secure network access platform enabling increased management awareness, control, and consistency for users and devices accessing an organization's network. ISE is an integral and mandatory component of SD-Access for implementing network access control policy. ISE performs policy implementation, enabling dynamic mapping of users and devices to scalable groups, and simplifying end-to-end security policy enforcement. Within ISE, users and devices are shown in a simple and flexible interface. ISE integrates with Cisco DNA Center by using Cisco Platform Exchange Grid (pxGrid) and REST APIs (Representational State Transfer Application Programming Interfaces) for endpoint event notifications and automation of policy configurations on ISE.

upvoted 7 times

danman32 Most Recent 4 months ago

I believe the answer is A.
Question asks where did DNA get the list of devices the user is using based on the username, and the exhibit lists 3: iPad, iPhone, and PC
The graph shows the statistics for the user's iPad only, which would probably be from edge node, but that's not what the question asked.
Even if that was what the question was asking, not sure it would only be from the edge node.

upvoted 1 times

LanreDipeolu 3 months, 1 week ago

Could the Wireless Fabric Edge Node (WLC) that the client iPad be the "edge node" in the question? I think so. A is definitely the answer

upvoted 1 times

loco_desk 4 months, 2 weeks ago

Selected Answer: A

Cisco ISE

upvoted 2 times

Splashisthegreatestmovie 5 months, 2 weeks ago

After reading the Cisco DNA Assurance guide I'm more confused than ever because it literally could be all of them. DNA is data whore that will take telemetry streams from anything.

upvoted 3 times

Chiaretta 7 months, 2 weeks ago

Selected Answer: C

C is the correct answer

upvoted 1 times

[Removed] 4 months, 3 weeks ago

Care to explain why?

upvoted 2 times

HungarianDish 8 months ago

Selected Answer: A

Client 360 is a component of Assurance. Client information is collected from ISE, see the link below.

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSDN-2777.pdf

"Cisco DNA Assurance ...Delivering Context for Network Troubleshooting Use-Case Example
...
Step 1: Identity Services Engine integration provides Cisco DNA Center with the user's information, group-policies and device information"

upvoted 2 times

Clauster 8 months, 2 weeks ago

Selected Answer: C

Answer is C not A
If you look at the Graph it clearly states "Client360" which is located under "Assurance" on Cisco DNA Center Management Dashboard.
Client360 pulls directly from the device where the user is connected to.
Device360 is similar.
Under "Assurance" there's also Dashboard, Applications, Client360, Device360 and the overall goal is to monitor the network.

upvoted 3 times

Gtekzzz 10 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

kewokil120 10 months, 3 weeks ago

Selected Answer: C

C for two reasons. 802.1x sessions are tracked on AP/Switches with "show auth session" so they know the user context data. I believe the graph shows user experience. User experience can be Wifi signal / auth issues/ timeout issues / etc. Not all of that is known by ISE as it a tacacs/radius server and gives no worries about wifi strength.

upvoted 2 times

Rose66 10 months, 3 weeks ago

Selected Answer: A

ISE delivers all this information

upvoted 1 times

MO_2022 11 months, 3 weeks ago

Selected Answer: A

Identity Services Engine

upvoted 1 times

FrameRelay 1 year, 1 month ago

Selected Answer: A

some may get confused when the question asks "where does DNA get those details", and may get confused in thinking the question is referring to the analytics data etc... which is indeed from the edge device, however in this instance watch out for the key word "context" in the question. Anything that has to do with Context is ISE, no edge device provides context data, its ISE. so correct answer is A.

upvoted 3 times

Wolly_M 1 year, 1 month ago

Selected Answer: A

From the book: Those details are provided to Cisco DNA Center by the Identity Services Engine.

upvoted 1 times

Feliphus 12 months ago

On page 697: "Cisco DNA Center integrates with many other tools, such as Active Directory, Indentity Services Engine (ISE), ServiceNow and Infoblox

upvoted 2 times

Deu_Inder 1 year, 2 months ago

Can anyone tell me how can the edge switch have the username of the user?
I would go with A.

upvoted 1 times

Mahyar49 9 months, 1 week ago

I agree with A but with Dot1x enabled port Switch has username and FQDN

upvoted 1 times

kewokil120 10 months, 3 weeks ago

via 802.1x

upvoted 1 times

nopenotme123 1 year, 3 months ago

Selected Answer: A

Literally looking at a client in ISE and its giving all this info.

upvoted 2 times

Shock_jesus 1 year, 4 months ago

The correct answer is A

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/1-3-3-0/b_cisco_dna_assurance_1_3_3_0_ug/b_cisco_dna_assurance_1_3_2_0_chapter_0111.html

upvoted 2 times

Question #251 *Topic 1*

Which command set configures RSPAN to capture outgoing traffic from VLAN 3 on interface GigabitEthernet 0/3 while ignoring other VLAN traffic on the same interface?

A. monitor session 2 source interface gigabitethernet0/3 rx monitor session 2 filter vlan 3

B. monitor session 2 source interface gigabitethernet0/3 rx monitor session 2 filter vlan 1 - 2, 4 - 4094

C. monitor session 2 source interface gigabitethernet0/3 tx monitor session 2 filter vlan 3

D. monitor session 2 source interface gigabitethernet0/3 tx monitor session 2 filter vlan 1- 2, 4 - 4094

Correct Answer: *C*

Community vote distribution

C (100%)

Violator Highly Voted 1 year, 9 months ago

This question is still asked. Passed today.

upvoted 8 times

Dryra1n Highly Voted 1 year, 4 months ago

This always trips me up. You're filtering "for" the VLAN you want rather than filtering "out" the other VLANs.

upvoted 6 times

JGOGBE 4 months, 1 week ago

From vlan you want

https://community.cisco.com/t5/other-network-architecture-subjects/quot-monitor-session-filter-vlan-quot-command/td-p/179404

upvoted 1 times

djedeen Most Recent 2 months, 3 weeks ago

Selected Answer: C

C: filter specifies clans you want to filter *for*
syntax: monitor session 2 filter vlan 1 - 5 , 9
meaning: Limits the SPAN source traffic to specific VLANs.
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_01101101.html#ID1129

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 4 times

```
configure terminal
ip flow-export destination 192.168.10.1 9991
ip flow-export version 9
```

Refer to the exhibit. What is required to configure a second export destination for IP address 192.168.10.1?

A. Specify a different UDP port.

B. Specify a different TCP port.

C. Configure a version 5 flow-export to the same destination.

D. Specify a different flow ID.

E. Specify a VRF.

Correct Answer: *A*

Community vote distribution

A (100%)

gtddrf Highly Voted 2 years, 3 months ago

Answer is A.
Proper syntax: ip flow-export destination {ip-address | hostname} udp-port
upvoted 17 times

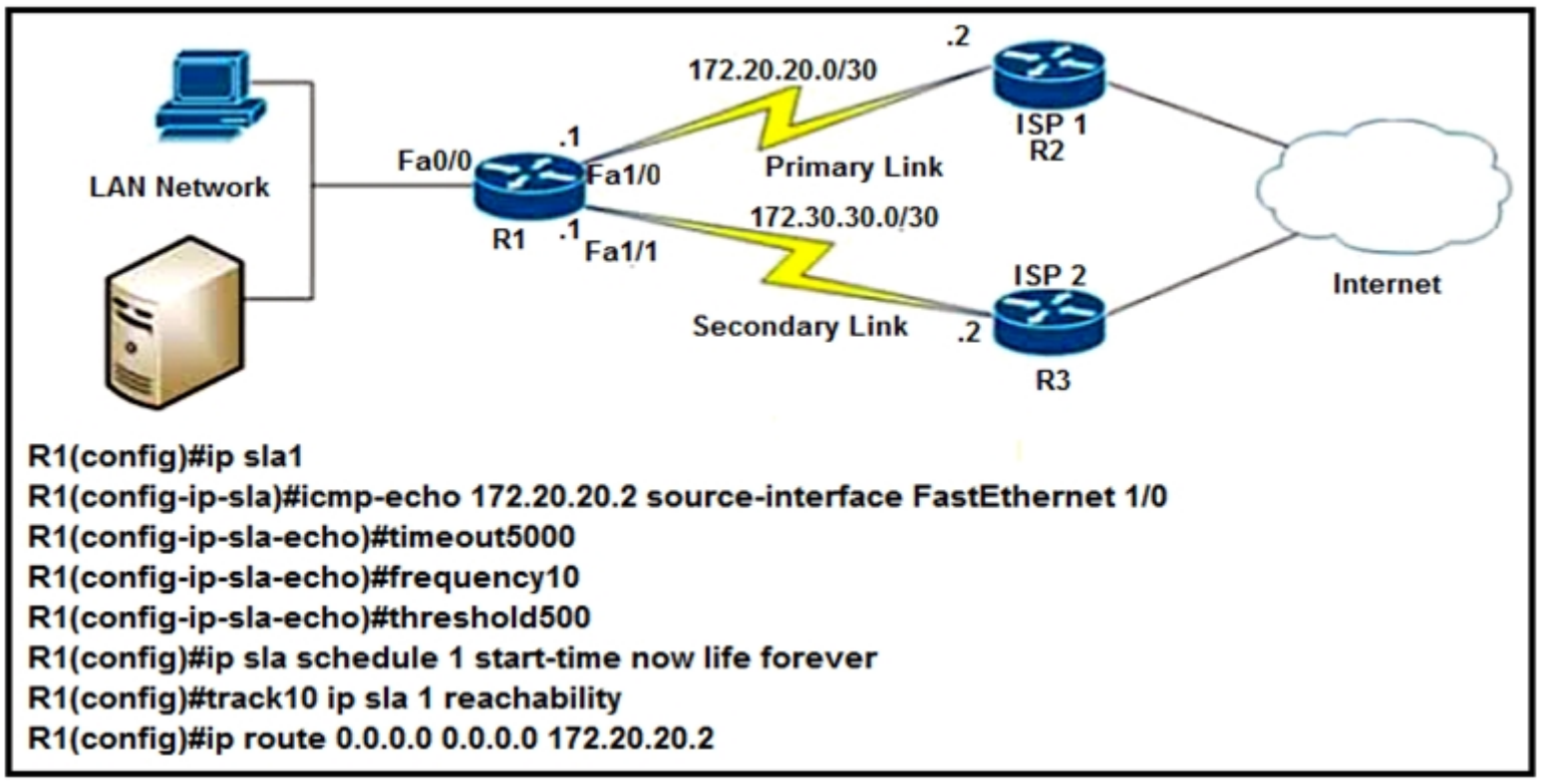
joe_smoe 1 year, 10 months ago

thanks for clarifying with the contextual help
upvoted 3 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: A

yes, it works but with warnings:
cisco_R3(config)#do s runn | sec flow
ip flow-export version 9
ip flow-export destination 1.1.1.2 9999
cisco_R3(config)#ip flow-export destination 1.1.1.2 9999
%Cannot configure Identical Destination address and port 1.1.1.2 9999
cisco_R3(config)#ip flow-export destination 1.1.1.2 9991
%Warning: Second destination address is the same as previous address 1.1.1.2
cisco_R3(config)#
cisco_R3(config)#do s runn | sec flow
ip flow-export version 9
ip flow-export destination 1.1.1.2 9999
ip flow-export destination 1.1.1.2 9991
cisco_R3(config)#
upvoted 3 times



Refer to the exhibit. After implementing the configuration, 172.20.20.2 stops replying to ICMP echos, but the default route fails to be removed. What is the reason for this behavior?

A. The threshold value is wrong.

B. The source-interface is configured incorrectly.

C. The destination must be 172.30.30.2 for icmp-echo.

D. The default route is missing the track feature.

Correct Answer: *D*

Community vote distribution

D (100%)

F103 1 month, 1 week ago

Firstly, you need to know what track static route could do. If the link goes down, then the route with track will tell router to remove this from routing table because it is not usable now.
Then the question misleading as well, it is not the config turning down the ICMP. It actually want to ask once the link 1 down, why it doesnt goes to link 2. The reason is the config static route with no track feature, so the route will keep it in routing table causes connection drop.

upvoted 2 times

Cooldude89 9 months, 2 weeks ago

Selected Answer: D

wrong ip route syntax for tracking

upvoted 2 times

SirJani 9 months, 3 weeks ago

The question setup is misleading. I thought for a while that echo failed due to the configuration. I think what is meant is that the ping fails somewhere between putting the configuration and present time.

upvoted 2 times

nushadu 11 months, 2 weeks ago

Selected Answer: D

cisco_R3#show track
Track 1
IP SLA 1 state
State is Down
1 change, last change 00:04:01
Latest operation return code: No connection
Tracked by:
Static IP Routing 0
cisco_R3#show ip route track-table
ip route 0.0.0.0 0.0.0.0 2.2.2.2 track 1 state is [down]
cisco_R3#
cisco_R3#sh runn | s ip rou
ip route 0.0.0.0 0.0.0.0 2.2.2.2 track 1
...
cisco_R3#
cisco_R3#show ip route static | b Gate

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S 172.16.1.0/24 is directly connected, Ethernet0/0.30
S 192.168.1.0/24 is directly connected, Ethernet0/0.20
cisco_R3#

upvoted 2 times

nushadu 10 months, 3 weeks ago

UP status:

cisco_R3#show ip route static | b Ga
Gateway of last resort is 2.2.2.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 2.2.2.2
...
cisco_R3#

cisco_R3#show ip route track-table
ip route 0.0.0.0 0.0.0.0 2.2.2.2 track 1 state is [up]
cisco_R3#

cisco_R3#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID Type Destination Stats Return Last
(ms) Code Run
---
*1 icmp-echo 2.2.2.2 RTT=3 OK 2 seconds ago

upvoted 1 times

GATUNO 2 years ago

ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10 ,

upvoted 2 times

sasatrickovic 2 years, 1 month ago

ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10

upvoted 3 times

diegodavid82 2 years, 1 month ago

The provided answer is correct. "C".

upvoted 1 times

diegodavid82 2 years, 1 month ago

Sorry, D is the correct option.

upvoted 2 times

Question #254 *Topic 1*

Refer to the exhibit.

```
Router# traceroute 10.10.10.1

Type escape sequence to abort.
Tracing the route to 10.10.10.1

1 10.0.0.1 5 msec 5 msec 5 msec
2 10.5.0.1 15 msec 17 msec 17 msec
3 10.10.10.1     *     *     *
```

An engineer is troubleshooting a connectivity issue and executes a traceroute. What does the result confirm?

A. The destination port is unreachable.

B. The probe timed out.

C. The destination server reported it is too busy.

D. The protocol is unreachable.

Correct Answer: *B*

In Cisco routers, the codes for a traceroute command reply are:

! ג€" success

* ג€" time out

N ג€" network unreachable -

H ג€" host unreachable -

P ג€" protocol unreachable -

A ג€" admin denied -

Q ג€" source quench received (congestion)

? ג€" unknown (any other ICMP message). In Cisco routers, the codes for a traceroute command reply are:

! ג€" success

* ג€" time out

N ג€" network unreachable -

H ג€" host unreachable -

P ג€" protocol unreachable -

A ג€" admin denied -

Q ג€" source quench received (congestion)

? ג€" unknown (any other ICMP message)

Community vote distribution

B (100%)

Dataset 4 months, 2 weeks ago

Selected Answer: B

B is correct

Regards!

upvoted 1 times

Stylar 10 months, 3 weeks ago

https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html

upvoted 1 times

Question #255 *Topic 1*

Which Cisco DNA Center application is responsible for group-based access control permissions?

A. Provision

B. Design

C. Assurance

D. Policy

Correct Answer: *D*

Reference:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-1-0/user_guide/b_cisco_dna_center_ug_1_3_1_0/b_cisco_dna_center_ug_1_3_1_0_chapter_01011.html

Community vote distribution

D (100%)

Ferrantee Highly Voted 1 year, 2 months ago

Design
-Network config
-Network profiles
-Sites and locations

Policies
-Virtual networks
-ISE

Provision
-Discovery devices
-Inventory

Assurance
-Network healthy

upvoted 6 times

danny_f Most Recent 1 year, 7 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-1-0/user_guide/b_cisco_dna_center_ug_1_3_1_0/b_cisco_dna_center_ug_1_3_1_0_chapter_01011.html#concept_zvk_yg4_p3b

upvoted 3 times

Question #256 *Topic 1*

An engineer is concerned with the deployment of a new application that is sensitive to inter-packet delay variance. Which command configures the router to be the destination of jitter measurements?

A. Router(config)# ip sla responder udp-connect 172.29.139.134 5000

B. Router(config)# ip sla responder tcp-connect 172.29.139.134 5000

C. Router(config)# ip sla responder udp-echo 172.29.139.134 5000

D. Router(config)# ip sla responder tcp-echo 172.29.139.134 5000

Correct Answer: *C*

Community vote distribution

C (100%)

Marving Highly Voted 1 year, 10 months ago

Selected Answer: C

Tcp-connect involves establishing a full connection whereas udp-echo echo is used to measure response times and test end-to-end connectivity therefore C is the correct answer

upvoted 9 times

sasatrickovic Highly Voted 2 years, 1 month ago

In this example we deal with Per-direction jitter. We need IP SLAs Responder on a Destination Device. So we need to configure:
R1>enable
R1#configure terminal
R1(config)#ip sla responder
R1(config)#ip sla responder udp-echo 172.29.139.134 5000
R1(config)#end

So, C is a valid answer.

upvoted 8 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: C

cisco_R3(config)#ip sla responder ?
auto-register Setup auto-register to hub
tcp-connect Setup tcp-connect responder
twamp Setup TWAMP responder
udp-echo Setup udp-echo responder
<cr>

cisco_R3(config)#ip sla responder udp-echo ?
ipaddress Permanent address
port Permanent port

cisco_R3(config)#ip sla responder udp-echo ipaddress ?
WORD IP Address or IP HostName

cisco_R3(config)#ip sla responder udp-echo ipaddress 2.2.2.2 ?
port Permanent port
cisco_R3(config)#ip sla responder udp-echo ipaddress 2.2.2.2 port 5000
cisco_R3(config)#ip sla responder
cisco_R3(config)#

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

Ahmedkrichen 2 years, 2 months ago

Correct

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

Question #257 *Topic 1*

Which NGFW mode blocks flows crossing the firewall?

A. tap

B. inline

C. passive

D. inline tap

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html

Community vote distribution

B (100%)

shamkhal 1 year, 9 months ago

Selected Answer: B

provided answer is correct

upvoted 2 times

hex2 1 year, 10 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html

Check out the table under "Here is a high level overview of the various FTD deployment and interface modes". Tap doesn't exist and Inline Pair is the only mode traffic CAN be dropped in. Of course the question implies its asking what mode will block ALL flows, I suspect that's a grammar problem.

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 2 times

circledan 2 years, 8 months ago

Should be B. In the reference, there is table: "Traffic can be DROPPED" column, inline pair - Yes, inline TAP - No.

upvoted 4 times

rezavage 3 years ago

B is correct . only inline mode place the FTD in the path of actual data and the FTD can drop packets. Inline Tap just log the bad packets but do not disturb the flow . and passive mode FTD is sit out of the data path and receive mirrored data from SPAN port.

upvoted 2 times

Summa 3 years, 1 month ago

should be D. INLINE allows those traffic from paired interfaces. INLINE TAP blocks all traffic. PASSIVE does nothing on traffics, allows all.

upvoted 1 times

XalaGyan 3 years, 2 months ago

Answer B is correct for every sort of firewall. if it is not INLINE in the traffic it cannot block anything.

upvoted 2 times

J_C_STUDY 3 years, 3 months ago

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html#anc4

upvoted 1 times

Question #258 *Topic 1*

How does Cisco TrustSec enable more flexible access controls for dynamic networking environments and data centers?

A. uses flexible NetFlow

B. assigns a VLAN to the endpoint

C. classifies traffic based on advanced application recognition

D. classifies traffic based on the contextual identity of the endpoint rather than its IP address

Correct Answer: *D*
Reference:
https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-726831.pdf

Community vote distribution

D (100%)

XalaGyan Highly Voted 3 years, 2 months ago

Answer is D

Introduction
Cisco TrustSec classification and policy enforcement functions are embedded in Cisco® switching, routing, wireless LAN, and firewall products. By classifying traffic based on the contextual identity of the endpoint versus its IP address, Cisco TrustSec enables more flexible access controls for dynamic networking environments and data centers.

https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-726831.pdf

upvoted 6 times

[Removed] Most Recent 5 months ago

Selected Answer: D

correct

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 2 times

jmaroto 2 years, 9 months ago

By classifying traffic
based on the contextual identity of the endpoint versus its IP address, Cisco TrustSec enables more flexible access controls for dynamic networking environments and data centers.

upvoted 3 times

The login method is configured on the VTY lines of a router with these parameters:

* The first method for authentication is TACACS
* If TACACS is unavailable, login is allowed without any provided credentials

Which configuration accomplishes this task?

A.

```
R1#sh run | include aaa
aaa new-model
aaa authentication login telnet group tacacs+ none
aaa session-id common

R1#sh run | section vty
line vty 0 4
R1#
```

B.

```
R1#sh run | include aaa
aaa new-model
aaa authentication login default group tacacs+
aaa session-id common

R1#sh run | section vty
line vty 0 4
  transport input none
R1#
```

C.

R1#**sh run | include aaa**
aaa new-model
aaa authentication login VTY group tacacs+ none
aaa session-id common

R1#**sh run | section vty**
line vty 0 4
 password 7 02050D480809

R1#**sh run | include username**
R1#

D.

R1#**sh run | include aaa**
aaa new-model
aaa authentication login default group tacacs+ none
aaa session-id common

R1#**sh run | section vty**
line vty 0 4
 password 7 02050D480809

R1#**sh run | include username**
R1#

Correct Answer: *D*

XalaGyan Highly Voted 1 year, 11 months ago

gentlemen,
here some helping thoughts.

aaa new-model invalidates the previous configuration

aaa authentication login <name OR default> group <Radius or TACACS> <fall back mechanisms such as NONE>

DO NOT be confused by
VTY or TELNET in the AAA Authentication List name which is just a name and lists the options to the right of it.

the requirements of TACACS and NO PASSWORD -> always watch out that you have the NO PASSWORD = NONE keyword at the end of the line.

next is the question about LOGIN

to LOGIN only you dont need a LINE VTY LOGIN AUTHENTICATION LOCAL or PASSWORD XZY as these would be only required if you wanted to ellevate your default priv-level from 1 to a higher number (in this case 15)

HTH
upvoted 15 times

rogi2023 5 months ago

XalaGyan's explanation very precise and clear = thx, and leads to the answer "D" (lab it, I did it in GNS3)
upvoted 1 times

Mdorgham 1 year, 8 months ago

So A is the correct Answer ,right ?
upvoted 1 times

pajonk22 1 year, 4 months ago

my mistake. If you use "default" group nothing needs to be added to vty line.
Correct is C

upvoted 1 times

danman32 4 months ago

Did you mean answer D? Answer C has a group name.

upvoted 1 times

[Removed] 1 year, 7 months ago

agree. essentially on the VTY lines, you will have to use "login authentication telnet" or "login authentication VTY". But when using default, you wont have to do this.

upvoted 1 times

examShark Highly Voted 2 years, 6 months ago

The given answer is correct
(the aaa new-model disables the line password)

upvoted 6 times

XDR Most Recent 7 months, 3 weeks ago

I'm pretty sure the answer is D.
The aaa auth line is OK, it uses default autentication list with tacacs and for fallback method none.
aaa new-model overdides password line form vty section so we can ignore it.

upvoted 3 times

nushadu 11 months, 2 weeks ago

Guys, I did not see any correct answers from provided choices,
if you use "none" keyword in the end you fail to connect after tacacs failure:
cisco_R3(config-line)#do s runn | s aaa
aaa new-model
aaa authentication login test_0 group tacacs+ none
aaa session-id common
cisco_R3(config-line)#
cisco_R3(config-line)#do s runn | s vty 0 4
line vty 0 4
exec-timeout 30 0
password 7 06030B
logging synchronous
login authentication test_0
transport input telnet
cisco_R3(config-line)#

upvoted 2 times

nushadu 11 months, 2 weeks ago

when you connect from linux you see this:
root@eve-ng:~# telnet 192.168.255.3
Trying 192.168.255.3...
Connected to 192.168.255.3.
Escape character is '^]'.
% Authorization failed.
Connection closed by foreign host.
root@eve-ng:~#

upvoted 2 times

nushadu 11 months, 2 weeks ago

when you change none -> line Cisco IOS will use local line password:
cisco_R3(config-line)#aaa authentication login test_0 group tacacs+ line
cisco_R3(config)#
linux
root@eve-ng:~# telnet 192.168.255.3
Trying 192.168.255.3...
Connected to 192.168.255.3.
Escape character is '^]'.

user ed password ed

Password:

cisco_R3>ena
Password:
cisco_R3#

upvoted 1 times

nushadu 11 months, 2 weeks ago

i do not know the correct answer to this Q...

upvoted 1 times

danman32 4 months ago

The fault with your lab is that you used a name for the AAA Authentication but did not apply the AAA authentication name to the VTY so it resorted to 'default'
You need to use 'default' in the AAA authentication.
aaa authentication login default group tacacs+ none
rather than
aaa authentication login test_0 group tacacs+ none

upvoted 1 times

Hikmat 11 months, 2 weeks ago

transport input method should be defined under line vty
line vty 0 4
password 7 02050D480809
transport input telnet
R9#sh run | sec aaa
aaa new-model
aaa authentication login default group tacacs+ none
aaa session-id common

R7#telnet 155.1.79.9
Trying 155.1.79.9 ... Open
R9>

upvoted 2 times

pajonk22 1 year, 4 months ago

my mistake. If you use "default" group nothing needs to be added to vty line.
Correct is C

upvoted 1 times

danman32 4 months ago

Did you mean answer D? Answer C has a name for the group, D has Default

upvoted 1 times

pajonk22 1 year, 4 months ago

question seem to be incorrect. to use aaa on vty you need a command "login authentication <aaa group name>". If only password is configured it will prompt for username

upvoted 1 times

danman32 4 months ago

You don't need to specify login authentication <group> in VTY if the AAA Authentication was assigned to default.

upvoted 1 times

hasanozdemirrr 2 years, 5 months ago

D is correct answer

upvoted 3 times

whiteherondance 2 years, 6 months ago

I'm a bit confused on this one. Shouldn't the answer be A? The question says 'If TACACS is unavailable, login is allowed without any provided credentials'

Answer D has a password configured on the VTY line - doesn't this mean you'd need to provide credentials to log in, meaning D is incorrect? A is the same as D but doesn't have a password configured, so shouldn't the answer then be A?

upvoted 2 times

whiteherondance 2 years, 6 months ago

ignore my point, A configures telnet so the answer probably is D as examShark has pointed out

upvoted 3 times

danman32 4 months ago

Actually A isn't managing telnet protocol but rather named the AAA authentication 'telnet'
Which is still wrong since you need it to be default.

upvoted 1 times

Question #260 *Topic 1*

Which feature does Cisco TrustSec use to provide scalable, secure communication throughout a network?

A. security group tag ACL assigned to each port on a switch

B. security group tag number assigned to each user on a switch

C. security group tag number assigned to each port on a network

D. security group tag ACL assigned to each router on a network

Correct Answer: *B*
Reference:
https://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/trustsec/C07-730151-00_overview_of_trustSec_og.pdf

Community vote distribution
B (55%) C (45%)

nep1019 Highly Voted 3 years, 5 months ago
According to the Cisco Press official study guide "Cisco TrustSec SGT tags are assigned to authenticated groups of users or end devices". Since the rest mention networks and B mentions users, I'd argue that the correct answer is B.
upvoted 26 times

DJ_Yahia Most Recent 2 months ago
Selected Answer: C
The correct answer is A. security group tag ACL assigned to each port on a switch.

Cisco TrustSec is a security architecture that uses security group tags (SGTs) to classify and control traffic flows in a network. SGTs are assigned to ports, switches, and routers. When a packet enters a network, it is tagged with the SGT of the port it entered through. This tag is then used to determine which security group ACLs should be applied to the packet.

SGT ACLs are lists of rules that define which traffic is allowed and blocked. These ACLs can be used to create flexible and granular security policies.

By using SGTs and SGT ACLs, Cisco TrustSec provides scalable, secure communication throughout a network.

The other answer choices are incorrect:

B. security group tag number assigned to each user on a switch
C. security group tag number assigned to each port on a network
D. security group tag ACL assigned to each router on a network
SGTs are assigned to ports, switches, and routers, not to users or networks.
upvoted 1 times

kewokil120 10 months, 3 weeks ago
Selected Answer: B
B per nep1019
upvoted 1 times

Rose66 10 months, 3 weeks ago
Selected Answer: C
Cisco TrustSec uses tags to represent logical group privilege. This tag, called a Security Group Tag (SGT), is used in access policies. The SGT is understood and is used to enforce traffic by Cisco switches, routers and firewalls . Cisco TrustSec is defined in three phases: classification, propagation and enforcement.
When users and devices connect to a network, the network assigns a specific security group. This process is called classification. Classification can be based on the results of the authentication or by associating the SGT with an IP, VLAN, or port-profile (-> Answer A and answer B are not correct as they say “assigned ... on a switch” only. Answer D is not correct either as it says “assigned to each router”).
upvoted 3 times

nopenotme123 1 year, 3 months ago
Selected Answer: B
I deal with ISE on the regular and its assigned based off the user permission.
upvoted 2 times

Dreket 1 year, 4 months ago
Selected Answer: B
Provided answer is correct. Explanation below:

At the point of network access, a Cisco TrustSec policy group called a Security Group Tag (SGT) is assigned to an endpoint, typically based on that endpoint’s user, device, and location attributes. The SGT denotes the endpoint’s access entitlements, and all traffic from the endpoint will carry the SGT information. The SGT is used by switches,

routers, and firewalls to make forwarding decisions. Because SGT assignments can denote business roles and functions, Cisco TrustSec controls can be defined in terms of business needs and not underlying networking detail.

https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-726831.pdf

upvoted 3 times

Edwinmolinab 1 year, 5 months ago

Selected Answer: C

B to me is not correct because it refers to users and this means for a user on a switch (maybe local), A refers an ACL to each port on a switch and D an ACL for routers, to me the best answer is C.

upvoted 1 times

wesleykm 1 year, 5 months ago

The question asked is “throughout a network:, Answer A & B only on a switch, Answer D only on Router.
Only Answer C is on “each port on a network”.

upvoted 1 times

PSYPHA1 1 year, 10 months ago

B
https://www.routexp.com/2019/05/introduction-to-secure-group-tagging-sgt.html
SGT- Secure Group Tagging which is generally used in the Cisco SD-Access design. An SGT is a 16-bit value that the Cisco ISE assigns to the user or endpoint’s session upon login.

upvoted 1 times

XalaGyan 1 year, 11 months ago

A. security group tag ACL assigned to each port on a switch --> INCORRECT as these talk about the use cases of sgt ACLs not the SGT itself

B. security group tag number assigned to each user on a switch -->90% CORRECT , SGT is a TAG Number that can be used in ACLs but it actually is just a 16bit number.
Why 90% ??? => Because logically thinking it would mean that we have only control and visibility on SWITCH PORTS only, and we all know thats just halve the rent.

C. security group tag number assigned to each port on a network --> 95% CORRECT, as SGTs are described as Numbers and not ACLs AS WELL AS the keyword NETWORK. With Network i guess all our visibility and control problems are sorted on SWITCHES, ROUTERS and maybe FWs.

D. security group tag ACL assigned to each router on a network --> INCORRECT, same issue as above. Why only Routers? ?? what about the other stuff? and SGT is NOT ACL but can be used in ACLS.

Hence: C is the best choice of answers but not 100% accurate.

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 2 times

chris110 2 years, 4 months ago

Maybe its C: Cisco TrustSec uses tags to represent logical group privilege. This tag, called a Security Group Tag (SGT), is used in access policies. The SGT is understood and is used to enforce traffic by Cisco switches, routers and firewalls . Cisco TrustSec is defined in three phases: classification, propagation and enforcement.
When users and devices connect to a network, the network assigns a specific security group. This process is called classification. Classification can be based on the results of the authentication or by associating the SGT with an IP, VLAN, or port-profile (-> Answer ‘security group tag ACL assigned to each port on a switch’ and answer ‘security group tag number assigned to each user on a switch’ are not correct as they say “assigned … on a switch” only. Answer ‘security group tag ACL assigned to each router on a network’ is not correct either as it says “assigned to each router”).

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct
When users and devices connect to a network, the network assignsa specific security group

upvoted 2 times

AnoushAnul 2 years, 9 months ago

An SGT is a 16-bit value that the Cisco ISE assigns to the user or endpoint’s session upon login. The network infrastructure views the SGT as another attribute to assign to the session and will insert the Layer 2 tag to all traffic from that.

https://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/trustsec/C07-730151-00_overview_of_trustSec_og.pdf

B

upvoted 1 times

sledgey121 2 years, 10 months ago

The user SGT is applied at the access point and switch layer, so B is the best answer.

upvoted 1 times

sledgey121 2 years, 10 months ago

When users and devices connect to a network, the network assigns a specific security group. This process is called classification. Classification can be based on the results of the authentication or by associating the SGT with an IP, VLAN,or port-profile. After user traffic is classified,then the SGT is propagated from where classification took place, to where enforcement action is invoked.This process is called propagation.Cisco TrustSec has two methods of SGT propagation:inline tagging and SXP.

upvoted 1 times

Helloory 3 years ago

B is correct answer, why people are thinking about C? dont think just switch, what about wireless? only correct option is B

upvoted 1 times

Question #261 *Topic 1*

Which technology provides a secure communication channel for all traffic at Layer 2 of the OSI model?

A. SSL

B. Cisco TrustSec

C. MACsec

D. IPsec

Correct Answer: *C*

edg Highly Voted 3 years, 3 months ago

Some additional information:
Reference:
https://www.curtisswrightds.com/news/blog/enhancing-network-security-with-macsec.html

MACsec vs IPsec – What's the Difference?
MACsec is for authentication and encryption of traffic over Ethernet on Layer 2 LAN networks. Alternatively, for Layer 3 networks, IPSec is used. Since MACsec and IPsec operate on different network layers, IPsec works on IP packets at Layer 3, while MACsec operates on Ethernet frames at Layer 2. Thus, MACsec can protect all Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP) traffic, which IPsec cannot secure. On the other hand, IPsec can work across the wide area network (WAN) for routers, while MACsec is limited to switches or end-nodes on a LAN.

upvoted 22 times

flash007 Most Recent 4 months, 1 week ago

macsec as it works at layer 2

upvoted 1 times

KZM 1 year ago

MACsec: Layer 2 encryption protocols like the IEEE 802.1AE Media Access Control Security (MACsec) standard must register with the eEdge session manager to receive disconnect notifications and perform cleanup.

upvoted 1 times

Question #262 *Topic 1*

An engineer is configuring local web authentication on a WLAN. The engineer chooses the Authentication radio button under the Layer 3 Security options for Web
Policy.
Which device presents the web authentication for the WLAN?

A. ISE server

B. RADIUS server

C. anchor WLC

D. local WLC

Correct Answer: *D*

Community vote distribution

D (67%) B (33%)

donlennoxx Highly Voted 3 years, 4 months ago

Should be D

upvoted 11 times

Dataset Most Recent 4 months, 2 weeks ago

Selected Answer: D

Radius is an external server for authentication, so the correct is D
Regards!

upvoted 1 times

bk989 6 months, 2 weeks ago

Selected Answer: D

page 733 OCG: LWA is the first form of Web Authentication that was created. For this type of WebAuth, the switch (or wireless controller) redirects HTTP traffic to a locally hosted web portal. D is the correct answer.

upvoted 2 times

monoki 6 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

Jeff555566 9 months, 1 week ago

Selected Answer: D

The WLC presents the web page.

upvoted 1 times

Mahyar49 9 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

Asymptote 11 months ago

Selected Answer: B

Clients must go through both dot1x and web authentication.

Reference:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html#:~:text=Clients%20must%20go%20through%20both%20dot1x%20and%20web%20authentication.

upvoted 3 times

Asymptote 11 months ago

wrong post admin pls remove

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

AnoushAnul 2 years, 9 months ago

If SSD would have been manually configured for anchoring, C would have been correct. I think D would be the case in this scenario... tricky :)
upvoted 4 times

DJOHNR 3 years, 3 months ago
https://mrncciew.com/2013/03/21/wlc-web-authentication/

D
upvoted 3 times

donlennoxx 3 years, 4 months ago
Should be B
upvoted 3 times

sasatrickovic 2 years, 1 month ago
RADIUS is working as a AUTHENTICATION SERVER. The local WLC is the AUTHENTICATOR and it does the AUTH process, "consulting" the RADIUS for checking the user's parameters entered through a web page.
upvoted 4 times

Question #263 *Topic 1*

Which method does the enable secret password option use to encrypt device passwords?

A. MD5

B. PAP

C. CHAP

D. AES

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/107614-64.html

danny_f Highly Voted 1 year, 7 months ago
Can someone let Cisco know MD5 is a hasing alogorithm, not enryption. The wording is wrong. And...how can they still use MD5??!! It's correct but wrong on so many levels.
upvoted 11 times

XBfoundX Most Recent 9 months, 1 week ago
in reality the question should be about hashing the password.... Anyway:

R1(config)#enable secret ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret

If we see the output the only valid option is md5.
upvoted 1 times

BitSo 11 months, 4 weeks ago
MD5 is correct, but "encrypt"? Sure... go ahead and try decrypting it.
upvoted 2 times

KZM 1 year ago
Cisco introduced the enable secret password to improve the security of the enable password command. This command uses the cryptographically strong MD5 algorithm to encrypt passwords.
upvoted 1 times

examShark 2 years, 6 months ago
The given answer is correct
upvoted 2 times

Question #264 *Topic 1*

On which protocol or technology is the fabric data plane based in Cisco SD-Access fabric?

A. VXLAN

B. LISP

C. Cisco TrustSec

D. IS-IS

Correct Answer: *A*

skh Highly Voted 3 years ago

The tunneling technology used for the fabric data plane is based on Virtual Extensible LAN (VXLAN). VXLAN encapsulation is UDP based, meaning that it can be forwarded by any IP-based network (legacy or third party) and creates the overlay network for the SD-Access fabric. Although LISP is the control plane for the SD-Access fabric, it does not use LISP data encapsulation for the data plane; instead, it uses VXLAN encapsulation because it is capable of encapsulating the original Ethernet header to perform MAC-in-IP encapsulation, while LISP does not. Using VXLAN allows the SD-Access fabric to support Layer 2 and Layer 3 virtual topologies (overlays) and the ability to operate over any IP-based network with built-in network segmentation (VRF instance/VN) and built-in group-based policy.

upvoted 12 times

flash007 Most Recent 4 months, 1 week ago

data plane of sd access is vxlan

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

hku68 2 years, 10 months ago

Answer is A

upvoted 1 times

Question #265 *Topic 1*

What is the difference between the enable password and the enable secret password when service password encryption is enabled on an IOS device?

A. The enable secret password is protected via stronger cryptography mechanisms.

B. The enable password cannot be decrypted.

C. The enable password is encrypted with a stronger encryption method.

D. There is no difference and both passwords are encrypted identically.

Correct Answer: *A*

Community vote distribution

A (100%)

skh Highly Voted 3 years ago

The "enable secret" password is always encrypted (independent of the "service passwordencryption" command) using MD5 hash algorithm. The "enable password" does not encrypt the password and can be view in clear text in the running-config. In order to encrypt the "enable password", use the "service password-encryption" command. This command will encrypt the passwords by using the Vigenere encryption algorithm. Unfortunately, the Vigenere encryption method is cryptographically weak and trivial to reverse.
The MD5 hash is a stronger algorithm than Vigenere so answer 'The enable secret password is protected via stronger cryptography mechanisms' is correct.

upvoted 8 times

YTAKE Highly Voted 2 years, 1 month ago

Interesting:
even the exam confuses encryption vs hashing(authentication):
enable secret: uses hashing (you can not retrieve the original message if you are using hashing unlike encryption which you can regardless of how strong the encryption is)

service password: uses encryption(very weak encryption indeed)

just for people who do not know what hashing and encryption are)

upvoted 7 times

ihateciscoreally Most Recent 3 months, 2 weeks ago

B is also correct answer. it cannot be decrypted because it is not even encrypted. but this is not answer they are looking for.

upvoted 1 times

flash007 4 months ago

enable secret password is encrypted with MD5

upvoted 1 times

flash007 4 months, 1 week ago

the enable secret password is encrypted with stronger protection

upvoted 1 times

H3kerman 1 year, 1 month ago

Selected Answer: A

Enable password - type 7:
Uses a simple alphabetical substitution Vigenere cipher with a hardcoded publicly known key. It can be reversed immediately into plaintext by using tools on the Internet. The passwords are stored as encoded strings within the configuration file. Consider them obfuscated, instead of encrypted
Enable secret - type 5:
Introduced around 1992. It uses a very simple Message-Digest 5 (MD5) hashing algorithm - 1,000 iterations of MD5 with a 32-bit salt. The MD5 algorithm is not NIST approved. Type 5 passwords are relatively easy to brute force with modern computers and tools available on the Internet that make it possible to find collisions for MD5 hashes. The passwords are stored as hashes within the configuration file.

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

davdtech 2 years, 8 months ago

The enable secret password uses type 5 encryption which is uncracable. The service password encryption uses type 7 which can be decrypted

upvoted 3 times

Question #266 *Topic 1*

Which access control list allows only TCP traffic with a destination port range of 22-443, excluding port 80?

A. deny tcp any any eq 80 permit tcp any any gt 21 lt 444

B. permit tcp any any range 22 443 deny tcp any any eq 80

C. permit tcp any any eq 80

D. deny tcp any any eq 80 permit tcp any any range 22 443

Correct Answer: *D*

Community vote distribution

D (73%) C (18%) 5%

nead Highly Voted 3 years, 3 months ago

No answer is correct
A. gt and lt not allowed on same ACE
B. Would work if permit and deny ACEs were the other way around
C. Permits ALL ports other than 80
D. Allows port 80. Could be typo. If ne 80 was eq 80, then the ACEs would work
upvoted 29 times

rlilewis 1 year, 6 months ago

I agree, there's supposed to be another option (which I see in other dumps):

Option E)
deny tcp any any eq 80
permit tcp any any range 22 443
upvoted 13 times

mrserxho1 Highly Voted 3 years, 5 months ago

Correct answer is B, "gt 21 lt 444" are not allowed inside the same statment
upvoted 10 times

CBlu 3 years, 5 months ago

D seems correct to me.

How can the "deny" statement be reached if it is covered by the permit statement above? ACL's go sequentially and stop on the first match.
upvoted 6 times

timtgh 1 year, 6 months ago

For packets that are not port 80, the first statement is not a match, so the second statement is checked.
upvoted 1 times

[Removed] 5 months, 2 weeks ago

but you are specifying a range between 22 and 443, 80 is within it.
B is wrong.
D specifies the DENYing of port 80 only, and then we can define what to allow
upvoted 1 times

KZM 1 year ago

Router(config)#access-list 100 permit tcp any any range 22 443
Router(config)#access-list 100 deny tcp any any eq 80
I don't think so. ACL works sequentially. So TCP ports 22 to 443 will permit and not deny port 80.
upvoted 2 times

nushadu 12 months ago

the order of the rules is important, in your case you allow ip packed dst tcp 80 in the first line, the second line\rule will not be checked anyway, the first match will trigger action (permit)
upvoted 1 times

Quick_X 3 years, 4 months ago

Correct, just tested
upvoted 2 times

fuqcue 2 years, 11 months ago

It cannot be B because 80 would be dropped upon being matched in the first statement...
upvoted 3 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Selected Answer: D

D is correct my friends.

upvoted 1 times

flash007 4 months, 1 week ago

deny is first permit is second

upvoted 2 times

ibogovic 5 months ago

Selected Answer: D

The correct answer is D.

The access control list (ACL) that allows only TCP traffic with a destination port range of 22-443, excluding port 80, is:

deny tcp any any eq 80
permit tcp any any range 22 443
This ACL configuration first denies TCP traffic with a destination port of 80 (port 80 is excluded). Then it permits TCP traffic with a destination port in the range of 22-443. By placing the deny statement before the permit statement, it ensures that traffic to port 80 is not allowed, while traffic to other ports in the specified range is permitted.

So, option D is the correct answer.

upvoted 4 times

musclehamster 6 months, 4 weeks ago

Selected Answer: D

The error has been fixed in D.
It is correct now

upvoted 3 times

[Removed] 2 months, 3 weeks ago

Thanks, I was so confused with the most voted comment stating it was wrong

upvoted 1 times

Cooldude89 9 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

Nickplayany 10 months, 1 week ago

Selected Answer: D

deny tcp any any eq 80
permit tcp any any range 22 443

upvoted 1 times

bendarkel 10 months, 3 weeks ago

Selected Answer: D

Correct answer is D

upvoted 1 times

kewokil120 10 months, 3 weeks ago

Selected Answer: D

D is correct. Who voting C needs to re-read ACLs

upvoted 1 times

kewokil120 11 months ago

Selected Answer: D

answer is d

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: D

cisco_R3(config)#ip access-list extended q_266
cisco_R3(config-ext-nacl)#
cisco_R3(config-ext-nacl)#10 deny tcp any any eq 80
cisco_R3(config-ext-nacl)#20 permit tcp any any range 22 443
cisco_R3(config-ext-nacl)#

cisco_R3#s access-l | b 266
Extended IP access list q_266
10 deny tcp any any eq www
20 permit tcp any any range 22 443
cisco_R3#

upvoted 1 times

MO_2022 11 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

kalbos 1 year ago

Selected Answer: D

Answer is D

upvoted 1 times

Stylar 1 year ago

Selected Answer: D

D for sure.
1st deny rule catches the port 80 traffic.
2nd permit allows the rest of our range.
3rd is implicit deny any any.

upvoted 1 times

H3kerman 1 year ago

Selected Answer: D

D is correct. first deny 80 then allow required range

upvoted 1 times

KZM 1 year ago

I think 'D'.
Router(config)#access-list 100 deny tcp any any eq 80
Router(config)#access-list 100 permit tcp any any range 22 443

upvoted 1 times

Question #267 *Topic 1*

A network administrator applies the following configuration to an IOS device: aaa new-model aaa authentication login default local group tacacs+
What is the process of password checks when a login attempt is made to the device?

A. A TACACS+ server is checked first. If that check fails, a local database is checked.

B. A TACACS+ server is checked first. If that check fails, a RADIUS server is checked. If that check fails, a local database is checked.

C. A local database is checked first. If that check fails, a TACACS+ server is checked. If that check fails, a RADIUS server is checked.

D. A local database is checked first. If that check fails, a TACACS+ server is checked.

Correct Answer: *D*
Reference:
https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/200606-aaa-authentication-login- default-local.html

Community vote distribution

D (100%)

skh Highly Voted 3 years ago

D correct
Explanation: The "aaa authentication login default local group tacacs+" command is broken down as follows:

+ The 'aaa authentication' part is simply saying we want to configure authentication settings.
+ The 'login' is stating that we want to prompt for a username/ password when a connection is made to the device.
+ The 'default' means we want to apply for all login connections (such as tty, vty, console and aux). If we use this keyword, we don't need to configure anything else under tty, vty and aux lines. If we don't use this keyword then we have to specify which line(s) we want to apply the authentication feature.
+ The 'local group tacacs+" means all users are authenticated using router's local database (the first method). If the credentials are not found on the local database, then the TACACS+ server is used (the second method).

upvoted 42 times

bora4motion Most Recent 11 months, 3 weeks ago

Selected Answer: D
D looks ok to me.

upvoted 2 times

KZM 1 year ago

Router(config)# new-model
Router(config)# authentication login default local group tacacs+

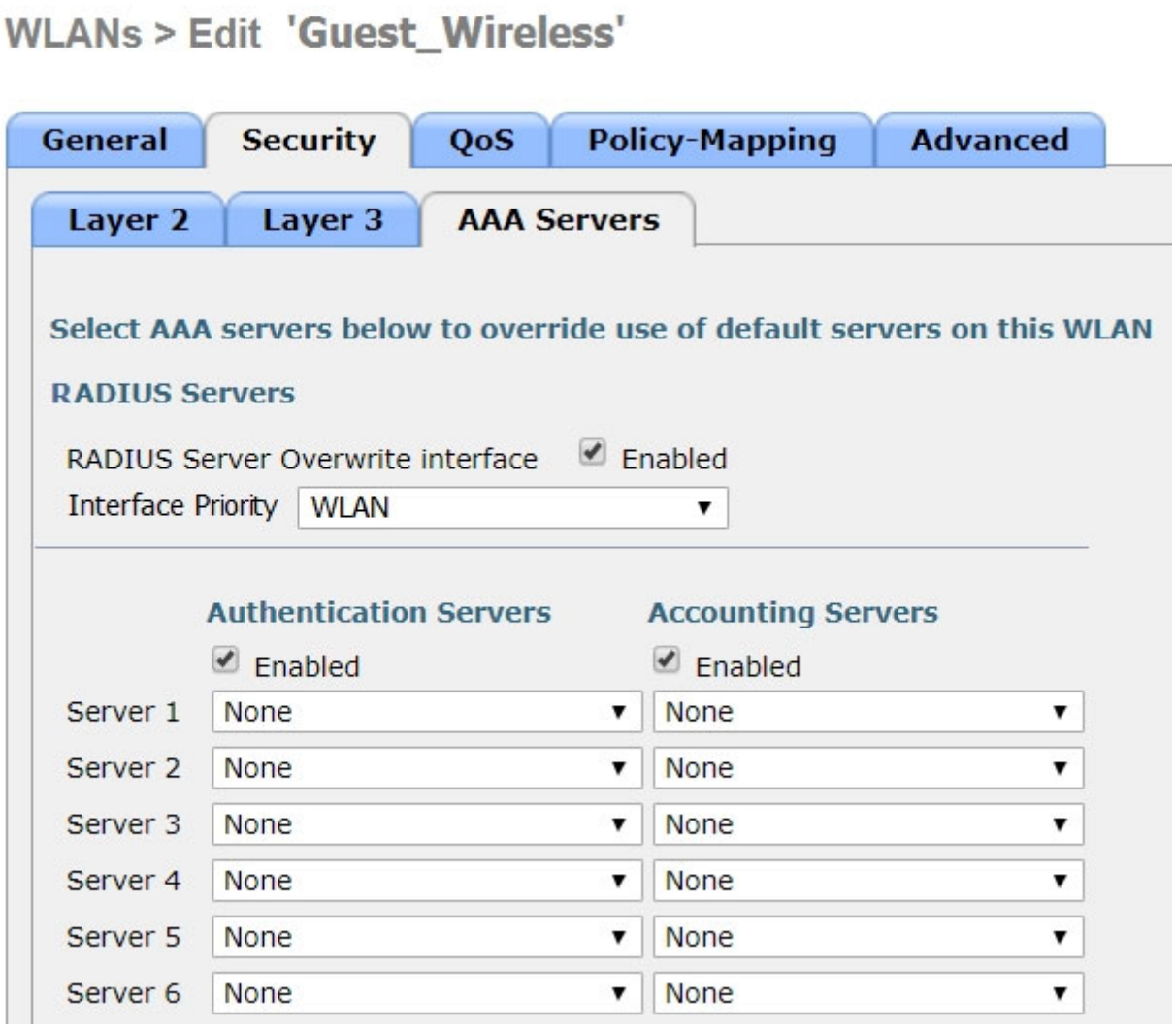
With just "aaa new model" configured, local authentication is applied to all lines and interfaces (except console line line con 0).

Here the AAA method list is applied on all login attempts on all lines of the device, where first local database is checked and then if required, Terminal Access Controller Access Control System (TACACS) server is tried.

https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/200606-aaa-authentication-login-default-local.html

upvoted 1 times

Refer to the exhibit.



Assuming the WLC's interfaces are not in the same subnet as the RADIUS server, which interface would the WLC use as the source for all RADIUS-related traffic?

A. the controller management interface

B. the controller virtual interface

C. the interface specified on the WLAN configuration

D. any interface configured on the WLC

Correct Answer: *C*

Community vote distribution

C (86%) 14%

Ayman_B Highly Voted 10 months, 3 weeks ago

Selected Answer: C

Check the RADIUS Server Overwrite interface check box to enable the per-WLAN RADIUS source support, the controller uses the interface specified on the WLAN configuration as identity and source for
all RADIUS related traffic on that WLAN.

When disabled, the controller uses the management interface as the
identity in the NAS-IP-Address attribute. If the RADIUS server is on a directly connected dynamic interface,
the RADIUS traffic will be sourced from that interface. Otherwise, the management IP address is used

upvoted 6 times

Glass17 Highly Voted 2 years, 3 months ago

I think answer is A.

WLC is not capable to route through WLAN interfaces and use it only if WLC is directly connected to the WLAN interface:

"The controller sources RADIUS traffic from the IP address of its management interface unless the configured RADIUS server exists on a VLAN accessible via one of the controller Dynamic interfaces. If a RADIUS server is reachable via a controller Dynamic interface, RADIUS requests to this specific RADIUS server will be sourced from the controller via the corresponding Dynamic interface. "

"Radius server override interface" is used as a "NAS-IP-Address attribute", but not used as source interface for communication with Radius server

upvoted 5 times

Chuckzero Most Recent 3 months ago

The correct answer is A.

The emphasis is on the WLC's interface not in the same subnet as the RADIUS Server.

upvoted 1 times

Wooker 1 year, 2 months ago

Selected Answer: C

"C" is correct.

upvoted 2 times

danny_f 1 year, 7 months ago

Selected Answer: C

From the guide, the the tick box wasn't checked it would be A. - Check the RADIUS Server Overwrite interface check box to enable the per-WLAN RADIUS source support.
When enabled, the controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on that WLAN

upvoted 1 times

Farid77 1 year, 7 months ago

Selected Answer: C

Correct. It's C as per documentation
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_01100111.pdf

upvoted 3 times

alfaxyz 1 year, 8 months ago

Selected Answer: A

Definitely A
If the RADIUS server is on a directly connected dynamic interface, the RADIUS traffic will be sourced from that interface. Otherwise, the management IP address is used.

There's a reason they state the RADIUS server is in a different subnet here.

upvoted 2 times

Violator 1 year, 9 months ago

This question is still asked. Passed today.

upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

jerryguo1019 2 years, 2 months ago

"C" is right
RADIUS Server Overwrite interface check box to enable the per-WLAN RADIUS source support:
1.When enabled, the controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on that WLAN.
2. When disabled, the controller uses the management interface as the identity in the NAS-IP-Address attribute.

upvoted 2 times

anonymous1966 2 years, 3 months ago

"C" is correct. See what "Radius server overwrite interface" does at:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_01100111.pdf

upvoted 4 times

XalaGyan 1 year, 11 months ago

Step 3 Click the Security tab, and then click the AAA Servers tab.
Step 4 Check the RADIUS Server Overwrite interface check box to enable the per-WLAN RADIUS source support. When enabled, the controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on that WLAN. When disabled, the controller uses the management interface as the identity in the NAS-IP-Address attribute. If the RADIUS server is on a directly connected dynamic interface, the RADIUS traffic will be sourced from that interface. Otherwise, the management IP address is used. In all cases, the NAS-IP-Address attribute remains the management interface, unless the feature is enabled.

upvoted 2 times

examShark 2 years, 6 months ago

The given answer is the most appropriate

upvoted 1 times

Question #269 *Topic 1*

Which component of the Cisco Cyber Threat Defense solution provides user and flow context analysis?

A. Cisco Firepower and FireSIGHT

B. Cisco Stealthwatch system

C. Advanced Malware Protection

D. Cisco Web Security Appliance

Correct Answer: *B*

Community vote distribution

B (100%)

kebkim Highly Voted 1 year, 2 months ago

Stealthwatch collects telemetry from every part of the network and applies advanced security analytics to the data. It creates a baseline of normal web and network activity for a network host, and applies context-aware analysis to automatically detect anomalous behaviors.

upvoted 5 times

examShark Highly Voted 2 years, 6 months ago

The given solution is correct

upvoted 5 times

shefo1 Most Recent 4 weeks, 1 day ago

Of course B is right
from OCG

Cisco Stealthwatch is a collector and aggregator of network telemetry data that performs network security analysis and monitoring to automatically detect threats that manage to infiltrate a network as well as the ones that originate from within a network.

upvoted 1 times

byallmeans 7 months ago

Selected Answer: B

Given answer is correct.

https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

Page 4.

upvoted 1 times

Question #270 *Topic 1*

An engineer must protect their company against ransomware attacks.
Which solution allows the engineer to block the execution stage and prevent file encryption?

A. Use Cisco Firepower and block traffic to TOR networks.

B. Use Cisco AMP deployment with the Malicious Activity Protection engine enabled.

C. Use Cisco Firepower with Intrusion Policy and snort rules blocking SMB exploitation.

D. Use Cisco AMP deployment with the Exploit Prevention engine enabled.

Correct Answer: *B*

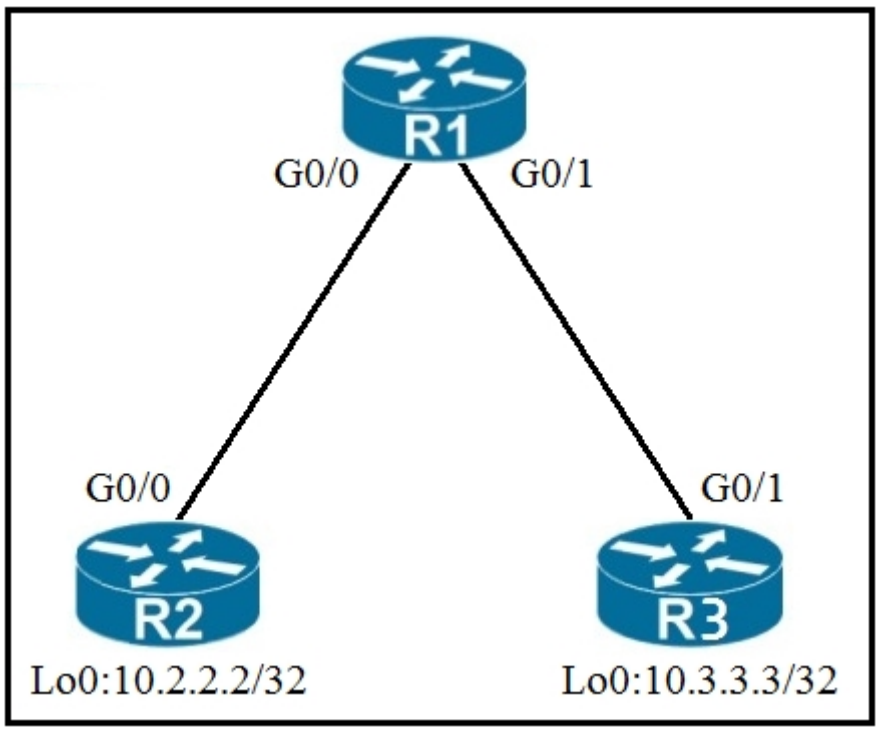
cvndani Highly Voted 1 year, 10 months ago
AMP with MAP :)
upvoted 16 times

Kakat Highly Voted 2 years, 11 months ago
B is correct:
https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.pdf
Malicious Activity Protection provides run-time detection and blocking of abnormal behavior of a running program on the endpoint (for example,behaviors associated with ransomware).
upvoted 5 times

anonymous1966 Most Recent 2 years, 3 months ago
See Malicious activity protection at
https://www.cisco-parts.ru/upload/iblock/632/cisco-advanced-malware-protection.pdf
upvoted 1 times

Question #271 *Topic 1*

Refer to the exhibit.



An engineer must deny Telnet traffic from the loopback interface of router R3 to the loopback interface of router R2 during the weekend hours.
All other traffic between the loopback interfaces of routers R3 and R2 must be allowed at all times.
Which command set accomplishes this task?

A. R3(config)#time-range WEEKEND R3(config-time-range)#periodic Saturday Sunday 00:00 to 23:59 R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND R3(config)#access-list 150 permit ip any any time-range WEEKEND R3(config)#interface G0/1 R3(config-if)#ip access-group 150 out

B. R1(config)#time-range WEEKEND R1(config-time-range)#periodic weekend 00:00 to 23:59 R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND R1(config)#access-list 150 permit ip any any R1(config)#interface G0/1 R1(config-if)#ip access-group 150 in

C. R3(config)#time-range WEEKEND R3(config-time-range)#periodic weekend 00:00 to 23:59 R3(config)#access-list 150 permit tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND R3(config)#access-list 150 permit ip any any time-range WEEKEND R3(config)#interface G0/1 R3(config-if)#ip access-group 150 out

D. R1(config)#time-range WEEKEND R1(config-time-range)#periodic Friday Sunday 00:00 to 00:00 R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND R1(config)#access-list 150 permit ip any any R1(config)#interface G0/1 R1(config-if)#ip access-group 150 in

Correct Answer: *B*

Community vote distribution

B (100%)

netpeer Highly Voted 2 years, 8 months ago

B
Access lists that are applied to interfaces do not filter traffic that originates from that router!
upvoted 18 times

Clauster 8 months, 3 weeks ago

Men i keep forgetting that i need to work on that, thanks
upvoted 2 times

timtgh Highly Voted 1 year, 6 months ago

A - wrong because outbound list won't block telnet from same router, AND it has the time-range on the permit statement.
B- correct!
C- wrong because it has no deny statement
D- wrong because it includes Friday
upvoted 7 times

[Removed] Most Recent 5 months ago

Selected Answer: B
B.
A and C are easily discarded with the fact that ACLs are not processed by the router that originates the traffic.
D is using a wrong time range, I think that if you're going to define the day individually the syntax should be something like this:

time-range TEST
periodic Saturday 00:00 to Sunday 23:59

but the keyword "weekend" covers this day range.
upvoted 1 times

[Removed] 5 months ago
Sorry, I misread, D is using the wrong days entirely. Friday isn't part of weekend period.
upvoted 1 times

Dataset 11 months, 1 week ago
Selected Answer: B
ACL cannot block traffic originates from the router were is applicatted
Regards
upvoted 2 times

nushadu 11 months, 2 weeks ago
Selected Answer: B
cisco_R3(config)#time-range q_277
cisco_R3(config-time-range)#periodic ?
Friday Friday
Monday Monday
Saturday Saturday
Sunday Sunday
Thursday Thursday
Tuesday Tuesday
Wednesday Wednesday
daily Every day of the week
weekdays Monday thru Friday
weekend Saturday and Sunday

cisco_R3(config-time-range)#periodic weekend ?
hh:mm Starting time

cisco_R3(config-time-range)#periodic weekend 00:00 ?
to ending day and time

cisco_R3(config-time-range)#periodic weekend 00:00 to ?
hh:mm Ending time - stays valid until beginning of next minute

cisco_R3(config-time-range)#periodic weekend 00:00 to 23:59
upvoted 3 times

nushadu 11 months, 2 weeks ago
cisco_R3(config-ext-nacl)#do s access-l | b 266
Extended IP access list q_266
10 deny tcp any any eq www time-range q_277 (inactive)
20 permit tcp any any range 22 443

cisco_R3(config-ext-nacl)#do s runn | s access-l
...
ip access-list extended q_266
deny tcp any any eq www time-range q_277
permit tcp any any range 22 443

cisco_R3#show time-range
time-range entry: q_277 (inactive)
periodic weekend 0:00 to 23:59
used in: IP ACL entry
cisco_R3#
upvoted 1 times

Jheax 1 year, 8 months ago
Selected Answer: B
Both A and B will block the telnet traffic during the weekend. But only B will allow the rest of the traffic during the the rest of the days. Answer is B.
upvoted 1 times

Violator 1 year, 9 months ago
This question is still asked. Passed today.
upvoted 1 times

xziomal9 2 years, 2 months ago
C.
RouterR3(config)#time-range WEEKEND
RouterR3(config-time-range)#periodic weekend 00:00 to 23:59
RouterR3(config)#access-list 150 permit tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
RouterR3(config)#access-list 150 permit ip any any time-range WEEKEND
RouterR3(config)#interface G0/1
RouterR3(config-if)#ip access-group 150 out

D.
RouterR1(config)#time-range WEEKEND
RouterR1(config-time-range)#periodic Friday Sunday 00:00 to 00:00
RouterR1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
RouterR1(config)#access-list 150 permit ip any any
RouterR1(config)#interface G0/1
RouterR1(config-if)#ip access-group 150 in

upvoted 4 times

xziomal9 2 years, 2 months ago

A.
RouterR3(config)#time-range WEEKEND
RouterR3(config-time-range)#periodic Saturday Sunday 00:00 to 23:59
RouterR3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
RouterR3(config)#access-list 150 permit ip any any time-range WEEKEND
RouterR3(config)#interface G0/1
RouterR3(config-if)#ip access-group 150 out
B.
RouterR1(config)#time-range WEEKEND
RouterR1(config-time-range)#periodic weekend 00:00 to 23:59
RouterR1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
RouterR1(config)#access-list 150 permit ip any any
RouterR1(config)#interface G0/1
RouterR1(config-if)#ip access-group 150 in

upvoted 4 times

AlexLAN 2 years, 2 months ago

A is the right answer. there is no "periodic weekend" command.

upvoted 1 times

AlexLAN 2 years, 2 months ago

Actually, there is a periodic weekend... but... Ill check it again.

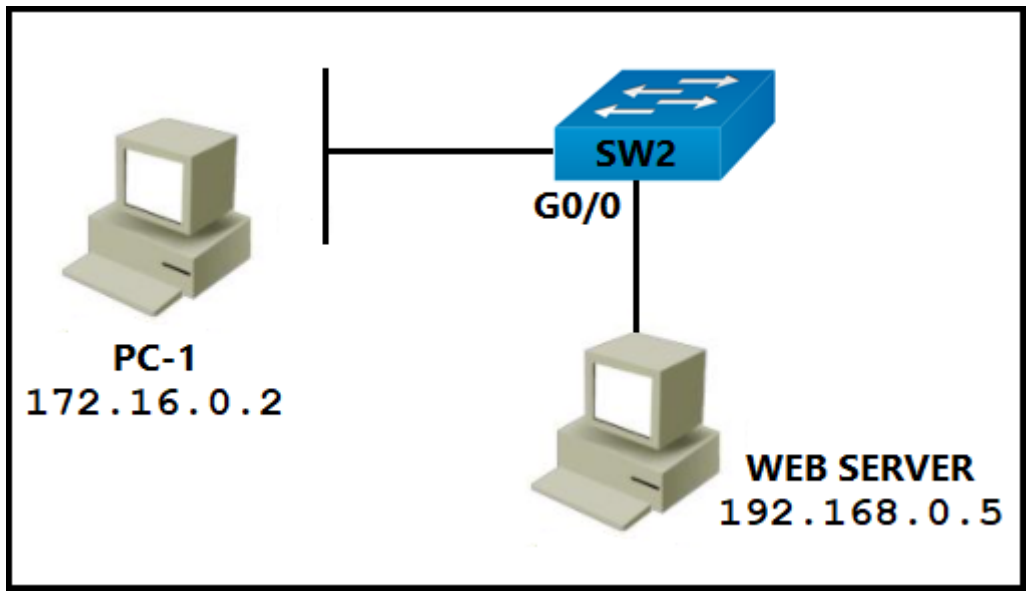
upvoted 2 times

AlexLAN 2 years, 2 months ago

Yes, B is right, the outbound access list can't block traffic from the control plane (CLI).

upvoted 3 times

Question #272 *Topic 1*



Refer to the exhibit. PC-1 must access the web server on port 8080. To allow this traffic, which statement must be added to an access control list that is applied on
SW2 port G0/0 in the inbound direction?

A. permit tcp host 172.16.0.2 host 192.168.0.5 eq 8080

B. permit tcp host 192.168.0.5 host 172.16.0.2 eq 8080

C. permit tcp host 192.168.0.5 eq 8080 host 172.16.0.2

D. permit tcp host 192.168.0.5 lt 8080 host 172.16.0.2

Correct Answer: *C*

Community vote distribution

C (59%) A (35%) 6%

Jclemente Highly Voted 2 years, 8 months ago

The correct answer is C...

upvoted 27 times

netpeer Highly Voted 2 years, 7 months ago

Just noticed the G0/0 is towards the web server NOT the PC...Then is permit host 192.168.0.5 eq 8080 host 172.16.0.2

upvoted 14 times

Jh0nh 1 year, 1 month ago

Same here, looks like the G0/0 is the interface facing the PC but no, it is facing the SERVER, so the answer is C :)

upvoted 2 times

CCNPWILL 1 month, 2 weeks ago

Agreed. Its the traffic coming back from the initial connection. C is correct.

upvoted 1 times

Claudiu1 Most Recent 2 days, 22 hours ago

Selected Answer: C

Be aware that G0/0 port is the one connected to the server.
The catch here is that the ACE doesn't filter any ingress traffic from PC-1. It filters the inbound traffic from the webserver. So naturally, you need to permit the ingress traffic sourced at the web server.

upvoted 1 times

Chuckzero 3 months ago

The correct answer is C.

Since the rule is to be applied Inbound to SW2 Gi0/0, we need to invoke the rule guiding Source Port and Destination Port.

<protocol> <source IP/source network> <source port> <destination IP/destination network> <destination port>

Therefore,

permit tcp host 192.168.0.5 eq 8080 host 172.16.0.2

upvoted 1 times

ihateciscoreally 3 months, 1 week ago

i hope whoever made this exhibit no longer works in cisco.

upvoted 7 times

Njavwa 3 months ago

lol, its a bit tricky
first thing i noticed was where int is facing

upvoted 1 times

Capt_23 5 months, 2 weeks ago

Answer is C.
The ACL is put on the interface facing the web server that receives a request on port 8080 ---> the answer has source port 8080 and is the web-server as the direction of the ACL is input (from outside to the router).

upvoted 1 times

wr4net 6 months, 2 weeks ago

the obvious quick answer choice for most commonly seen deployments would be answer A. but since that is the only one with 172 as the source, there must be some trick going on! So after looking again, C it is, but this is not a typical ACL found almost anywhere and on a switch for that matter. dumb question for real life. also remember that ports can be applied to both source and dest, which means the port will follow each one. this rules out B as syntactically incorrect.

upvoted 1 times

Chiaretta 7 months, 2 weeks ago

Selected Answer: C

This question would be correct if the equipment would be a router not a switch. In that case C is correct.

upvoted 1 times

dragonwise 8 months, 1 week ago

Selected Answer: A

Question says "PC-1 must access the web server on port 8080"
So I'd go for A where PC-1 is the source and server is the destination

upvoted 1 times

mhizha 7 months, 3 weeks ago

If your ACL is in an outbound direction on the G0/0 A would be fine, but in this case the ACL is in a inbound direction meaning that it will be looking at traffic from the server to the PC

upvoted 1 times

Dataset 9 months, 1 week ago

Selected Answer: C

Hi
It is confuse the interfece name placement
C is correct
Regards!

upvoted 1 times

Cooldude89 9 months, 2 weeks ago

Selected Answer: C

Gig0/0 is facing the server

upvoted 1 times

rafaelinho88 10 months ago

Selected Answer: C

The inbound direction of G0/0 of SW2 only filter traffic from Web Server to PC-1 so the source IP address and port is of the Web Server.

upvoted 1 times

StefanOT2 10 months, 3 weeks ago

Selected Answer: A

C will not prevent the PC from accessing port 8080 on the webserver. Only the answer is not allowed, AFTER the access did already happen.
Terrible question, terrible graph, everything terrible. I go for A

upvoted 2 times

kewokil120 10 months, 3 weeks ago

Selected Answer: C

C. It asking for return traffic.

upvoted 1 times

markymark874 11 months ago

Selected Answer: A

Answer is either A or C. Depending on the placement of the g0/0 label. But in normal situtation the ACL should be placed as closed as possible to the source of the traffic you want to control to avoid unecessary resource usage.

upvoted 1 times

nushadu 11 months, 2 weeks ago

Guys, to get this question, first answer this question - what is socket www server (non-standard)?
ip_addr:tcp_8080, right? so traffic FROM WWW server (inbound direction for port Gi0/0)
will always have TCP 8080 port, in other words, it is reverse traffic\reply to the web clients.
of course to match this traffic we need to use this ACL:
cisco_R3(config-ext-nacl)#$cp host 192.168.0.5 eq 8080 host 172.16.0.2
cisco_R3(config-ext-nacl)#
cisco_R3(config-ext-nacl)#do s runn ip access-list extended q_266
cisco_R3(config-ext-nacl)#do s runn | sec ip access-list
deny tcp any any eq www time-range q_277
permit tcp any any range 22 443
permit tcp host 192.168.0.5 eq 8080 host 172.16.0.2 <<<<<<<<<<<<<<<<<<<<<<<<
cisco_R3(config-ext-nacl)#

upvoted 1 times

Stylar 1 year ago

The placement of the G0/0 text is horrible.. Cant make a decision based on this image.

upvoted 1 times

Question #273 *Topic 1*

What is the result of applying this access control list?

ip access-list extended STATEFUL

10 permit tcp any any established

20 deny ip any any

A. TCP traffic with the URG bit set is allowed.

B. TCP traffic with the SYN bit set is allowed.

C. TCP traffic with the ACK bit set is allowed.

D. TCP traffic with the DF bit set is allowed.

Correct Answer: *C*

Community vote distribution

C (100%)

P1Z7C Highly Voted 2 years, 8 months ago

The established keyword indicates that packets belong to an existing connection if the Transmission Control Protocol (TCP) datagram has the Acknowledgment (ACK) or Reset (RST) bit set.

https://community.cisco.com/t5/networking-documents/how-to-configure-acls-to-permit-only-established-connections-and/ta-p/3127503

upvoted 5 times

shefo1 Most Recent 3 weeks ago

Selected Answer: C

of course C is right because
two nodes is connected and established together when ACK message is send from source to destination
first message : SYN from source to destination
second message : SYN,ACK from destination to source
thied message : ACK from source to destination

upvoted 1 times

vladik820 2 months, 1 week ago

Selected Answer: C

Yes, the answer is correct

upvoted 1 times

anonymous1966 2 years, 3 months ago

Correct - https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html

upvoted 4 times

examShark 2 years, 6 months ago

The given solution is correct
The return traffic having an ACK will start a new session in the firewall.

upvoted 3 times

Question #274 *Topic 1*

Which outbound access list, applied to the WAN interface of a router, permits all traffic except for http traffic sourced from the workstation with IP address
10.10.10.1?

A. ip access-list extended 200 deny tcp host 10.10.10.1 eq 80 any permit ip any any

B. ip access-list extended 10 deny tcp host 10.10.10.1 any eq 80 permit ip any any

C. ip access-list extended NO_HTTP deny tcp host 10.10.10.1 any eq 80

D. ip access-list extended 100 deny tcp host 10.10.10.1 any eq 80 permit ip any any

Correct Answer: *D*

Community vote distribution

D (100%)

Sajj_gabi Highly Voted 2 years, 9 months ago

Defo D as its an extended ACL the range is betwee 100-199
Router(config)#ip access-list extended ?
<100-199> Extended IP access-list number
<2000-2699> Extended IP access-list number (expanded range)
WORD Access-list name

upvoted 11 times

danman32 4 months ago

Hmm. But numbers can also be an access-list name, can't it?

upvoted 1 times

KZM Highly Voted 1 year ago

A. 200 is out of extended access-list range (Available range is 100-199) -> Wrong
B. 10 is out of extended access-list range (Available range is 100-199) -> Wrong
C. The extended access-list with the name NO_HTTP can be configured. But as per the command, all traffic will block due to not execute the command permit ip any any ->Wrong

D. Correct
Router(config)#ip access-list extended 100
Router(config-ext-nacl)#deny tcp host 10.10.10.1 any eq 80
Router(config-ext-nacl)#permit ip any any

upvoted 6 times

mgiuseppe86 Most Recent 2 months, 3 weeks ago

A.
ip access-list extended 200
deny tcp host 10.10.10.1 eq 80 any
permit ip any any

B.
ip access-list extended 10
deny tcp host 10.10.10.1 any eq 80
permit ip any any

C.
ip access-list extended NO_HTTP
deny tcp host 10.10.10.1 any eq 80

D.
ip access-list extended 100
deny tcp host 10.10.10.1 any eq 80
permit ip any any

upvoted 1 times

danman32 4 months ago

In all cases, we're dealing with a NAMED access list.
Why? Because it is 'ip access-list [standard|extended] <name> ...' rather than
'access-list <number> [permit|deny] ...'
The ACL name just happens to be numbers.
So B can also be the correct answer, ACL name being 10.
Unless there's a typo somewhere in the answers compared to what's actually on the test.

It just happens that the na

upvoted 1 times

Chuckzero 3 months ago

C cannot be the correct answer because of implicit deny. There is not permit statement.

upvoted 1 times

Clauster 8 months, 2 weeks ago

Selected Answer: D

Correct Answer is D however, there is a typo, it should be written like this:
ip access-list extended 100 deny tcp host 10.10.10.1 eq 80 any < Source host 10.10.10.1 eq 80 going to any destination. The way that the answer has it written that's a destination Port not a source.
permit ip any any

upvoted 2 times

danman32 4 months ago

With the way you propose it be written, you'd be specifying that the source port be 80, not the destination.
We want to block from 10.10.10.1 with any source port to any destination, destination port 80.
The way you suggest, it instead would be:
from 10.10.10.1 source port 80 to any destination with any destination port. Not what we want.

upvoted 1 times

H3kerman 1 year, 1 month ago

Selected Answer: D

D. ip access-list extended 100 <name of acl> deny tcp host 10.10.10.1 <source ip> <any source port> any <any destination ip> eq 80 <destination port>
permit ip any any

upvoted 3 times

BigMouthDog 1 year, 4 months ago

The difference between ans A nad D is not only the etended list number range, it also "eq 80 any" and "any eq 80"

upvoted 2 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

BigMomma4752 2 years, 8 months ago

D is the correct answer.

upvoted 2 times

Facco 2 years, 9 months ago

Correct Answer: D.

Syntax:
[insert line-num] deny tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]]{dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]

https://www.cisco.com/c/en/us/td/docs/app_ntwk_services/waas/waas/v401_v403/command/reference/cmdref/ext_acl.pdf

upvoted 2 times

Question #275 *Topic 1*

```
aaa new-model
aaa authentication login default local-case enable
aaa authentication login ADMIN local-case
username CCNP secret Str0ngP@ssw0rd!
line 0 4
   login authentication ADMIN
```

Refer to the exhibit. An engineer must create a configuration that executes the show run command and then terminates the session when user CCNP logs in.
Which configuration change is required?

A. Add the access-class keyword to the username command.

B. Add the autocommand keyword to the aaa authentication command.

C. Add the access-class keyword to the aaa authentication command.

D. Add the autocommand keyword to the username command.

Correct Answer: *D*

Community vote distribution

D (100%)

hex2 Highly Voted 1 year, 10 months ago

I've been a CCNP for 11 years, and doing Cisco networking for almost 25. Today, right now, is the first time I have ever heard of this capability.
upvoted 49 times

danny_f 1 year, 6 months ago

I HATE thet we get tested on the most random commands that are never used. What a wasted opportunity.
upvoted 19 times

DiscardedPacket 1 year, 5 months ago

agreed, it really is stupid.
upvoted 9 times

juancarlosdlar 10 months, 3 weeks ago

If someone had told me that certification exams would be as stupid as Cisco exams, I would have studied something different.
upvoted 9 times

wr4net 6 months, 2 weeks ago

if this command wasn't so obscure and dumb, I would feel dumb at this point too, having worked on cisco gear for 20+ years. :) at least i wont forget this if it comes up on a test.
upvoted 3 times

McBeano Highly Voted 1 year, 4 months ago

questions like this are why I visit sites like this. It doesn't matter how much you study, this question would have screwed me over everytime, I've never heard of it
upvoted 17 times

danman32 Most Recent 4 months ago

Clearly D is the answer, but there is a problem with how the answer is worded.
It says to ADD the sutocommand to the username command.
But you can't add anything to the command once you specify the password, otherwise what you intended to be an option becomes the password
So you have to have a separate line for username CCNP autocommand since here too autocommand has to be the last option.
upvoted 1 times

dragonwise 8 months, 1 week ago

Cisco exams are for testing real skills anymore. That is too sad
upvoted 2 times

Asymptote 11 months ago

Selected Answer: D

Cisco IOS long had the autocommand option by which you could attach any command to a username and have it execute after successful login. For example, username x autocommand show ip interface brief command would configure the router to display the interface status after someone would log in as user x.

After the autocommand is executed, the user is logged out and the session is disconnected, unless you configure the username user nohangup option, which causes the session to remain active, giving the operator another login prompt.

upvoted 5 times

nushadu 11 months, 2 weeks ago

Selected Answer: D

```
cisco_R3(config)#do s runn | s aaa
aaa new-model
aaa authentication banner ^C
aaa authentication login default local
aaa authentication login test_0 group tacacs+ line
aaa authentication login Q_275 local-case
aaa authorization exec default local if-authenticated
aaa session-id common

cisco_R3(config)#
cisco_R3(config)#do s runn | s vty
line vty 0 4
exec-timeout 30 0
password 7 06030B
logging synchronous
login authentication Q_275
transport input telnet
cisco_R3(config)#

cisco_R3(config)#do s runn | i username
username test privilege 15 password 7 044F0E151B761B19
username ed privilege 15 password 7 082448
username CCNP secret 5 $1$s5fj$YMDYM1MdeEEr/Kt2O5spv/
username CCNP autocommand sho users
cisco_R3(config)#
```

upvoted 1 times

nushadu 11 months, 2 weeks ago

```
login from remote linux:
root@eve-ng:~# telnet 192.168.255.3
Trying 192.168.255.3...
Connected to 192.168.255.3.
Escape character is '^]'.

Username: CCNP
Password:

Line User Host(s) Idle Location
0 con 0 ed idle 00:00:32
* 2 vty 0 CCNP idle 00:00:00 192.168.255.1

Interface User Mode Idle Peer Address
Connection closed by foreign host.
root@eve-ng:~#
```

upvoted 1 times

Lucky1313 1 year, 3 months ago

Selected Answer: D

The command we want to apply can be any length, so the autocommand keyword must be the last option of the line - username CCNP autocommand sh run

upvoted 2 times

Duck2Duck 1 year, 4 months ago

The only real use for the autocommand feature today is to issue "term mon" on login and disable the hangup option.

upvoted 2 times

sayywhat 1 year, 6 months ago

Lol at this question and the responses. Answer is correct though.

upvoted 1 times

youtri 1 year, 11 months ago

autocommand (Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and contain imbedded spaces, commands using the autocommand keyword must be the last option on the line.

upvoted 1 times

youtri 1 year, 11 months ago

username name [autocommand command]

upvoted 2 times

anonymous1966 2 years, 3 months ago

Correct. Reference: https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/username.htm

upvoted 3 times

SmartForNothing 2 years, 4 months ago

if you answered this question wrong then you shouldn't take the exam

upvoted 1 times

Asymptote 11 months ago

So...what is the purpose you visit this site?

upvoted 2 times

Dead_Adriano 2 years, 2 months ago

If you answer this question right then why would you need any exam?

upvoted 8 times

koptos 2 years, 2 months ago

Why is that?

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

```
Router2# show policy-map control-plane

Control Plane
Service-policy input:CISCO
Class-map:CISCO (match-all)
    20 packets, 11280 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match:access-group 120
    police:
      8000 bps, 1500 limit, 1500 extended limit
      conformed 15 packets, 6210 bytes; action:transmit
      exceeded 5 packets, 5070 bytes; action:drop
      violated 0 packets, 0 bytes; action:drop
      conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-day)
    105325 packets, 11415151 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match:any
```

Refer to the exhibit. An engineer configures CoPP and enters the show command to verify the implementation. What is the result of the configuration?

A. All traffic will be policed based on access-list 120.

B. If traffic exceeds the specified rate, it will be transmitted and remarked.

C. Class-default traffic will be dropped.

D. ICMP will be denied based on this configuration.

Correct Answer: *A*

wr4net 6 months, 2 weeks ago

somewhat of a trick because the "match-all" applies to the class map policy only, which can match various oddities like an ACL (access-group 120) and an ip precedence bit for example. you wouldn't really have multiple access groups (AGs) in the match, as that could roll up int many ACE's under just one AG - like 120.

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 4 times

ArchBishop 1 year, 9 months ago

Why would it not be B?

Isn't all traffic classified by access-list 120 going to be policed based on the class-map?

Based on the following line, exceeding traffic is dropped, NOT transmitted..
“Exceeded 5 packets, 5070 bytes, action: drop”

upvoted 1 times

timtgh 1 year, 6 months ago

That's what A says. All traffic is policed by ACL 120. B is wrong because it says to transmit excessive packets.

upvoted 6 times

iGlitch 1 year, 1 month ago

It isn't easy to understand it the other way around. :D

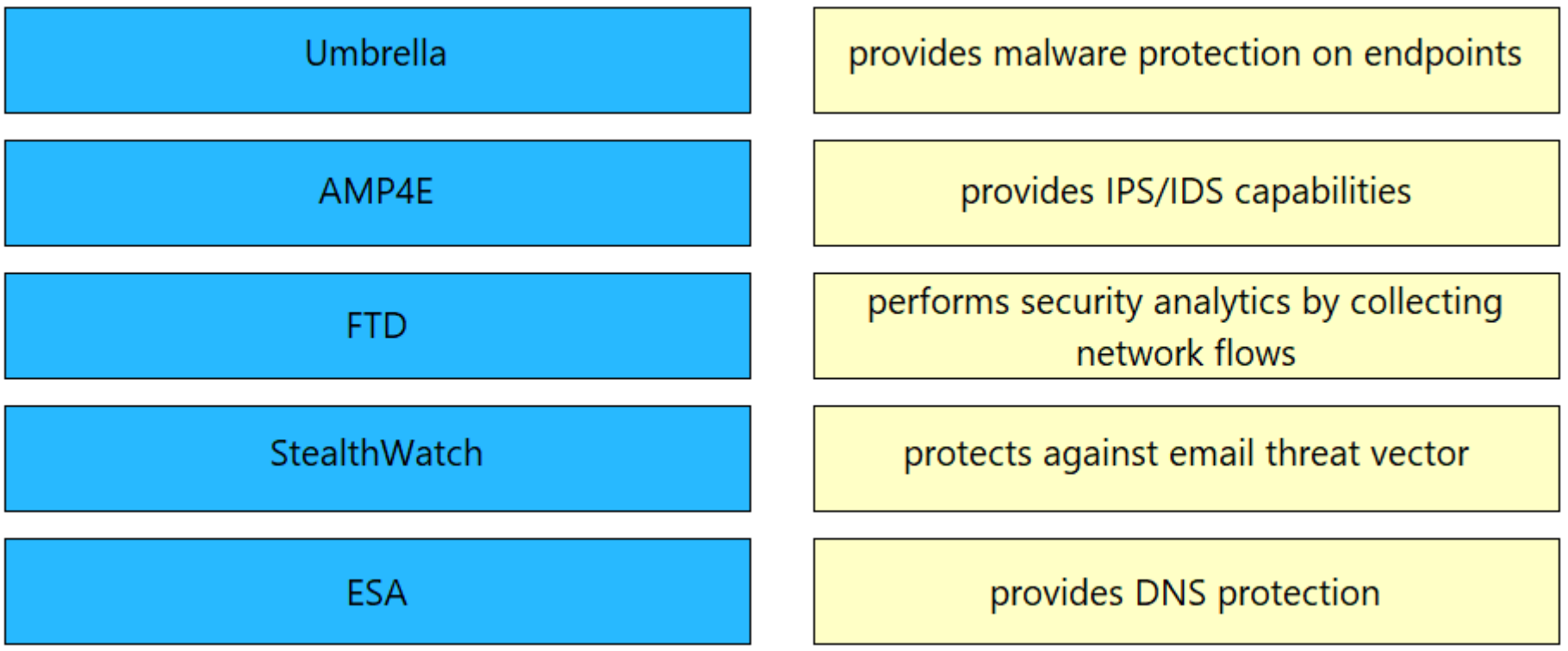
upvoted 1 times

Question #277 *Topic 1*

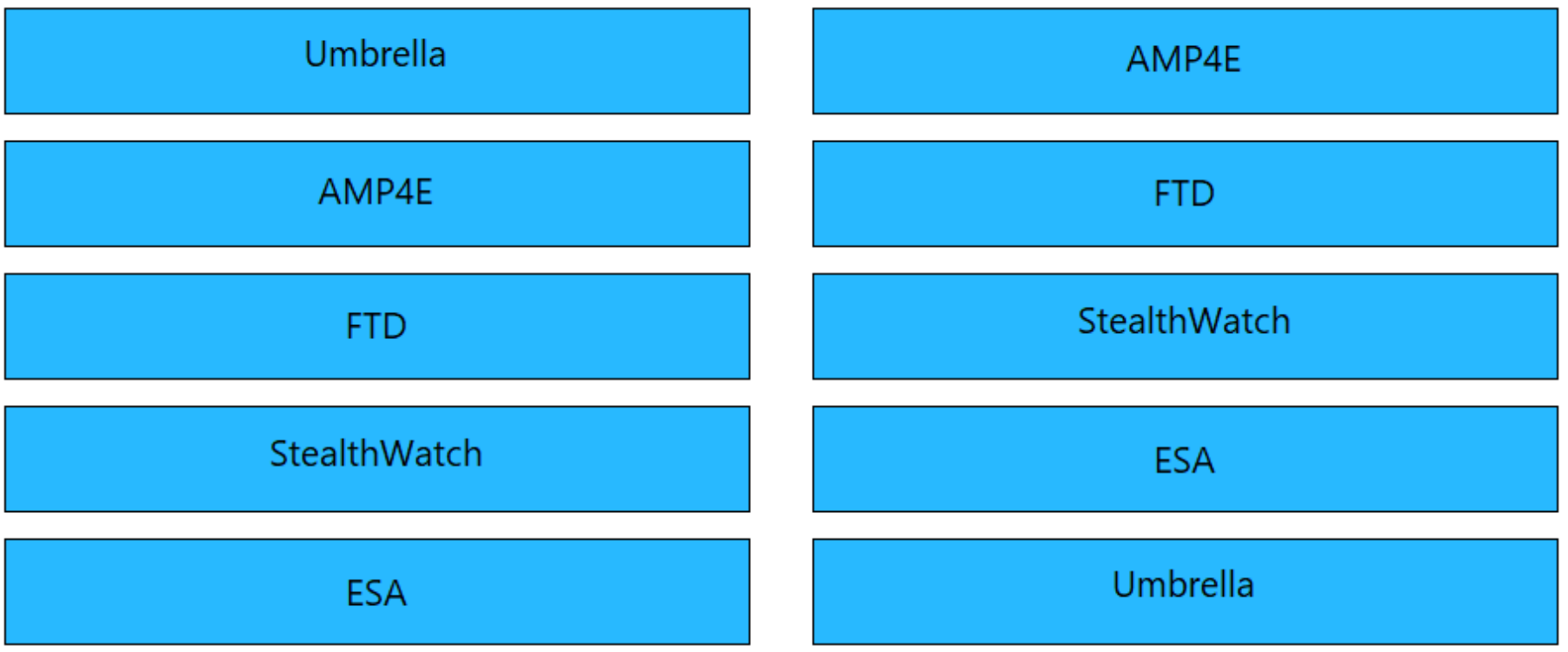
DRAG DROP -

Drag and drop the threat defense solutions from the left onto their descriptions on the right.

Select and Place:



Correct Answer:



AlbertoStu Highly Voted 1 year, 7 months ago

From the Official Cert Guide.
P. 1426 (AMP – Advanced Malware Protection)
P. 1430 (Umbrella – Formerly known as OpenDNS)
P. 1436 (ESA – Email Security Appliance)
P. 1444 (FTD – Firepower Threat Defense)
P. 1446 (Cisco Stealthwatch – is a collector and aggregator of network telemetry data that performs network security analysis and monitoring to automatically detect threats that manage to infiltrate a network as well as the ones that originate form within a network.)

given answer is correct.

upvoted 15 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Given answers are correct.

upvoted 1 times

[Removed] 4 months, 3 weeks ago

Answer looks correct.

upvoted 3 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 4 times

Question #278 *Topic 1*

Refer to the exhibit.

```
aaa new-model
aaa authentication login authorizationlist tacacs+
tacacs-server host 192.168.0.202
tacacs-server key ciscotestkey
line vty 04
login authentication authorizationlist
```

What is the effect of this configuration?

A. The device will allow users at 192.168.0.202 to connect to vty lines 0 through 4 using the password ciscotestkey.

B. The device will authenticate all users connecting to vty lines 0 through 4 against TACACS+.

C. The device will allow only users at 192.168.0.202 to connect to vty lines 0 through 4.

D. When users attempt to connect to vty lines 0 through 4, the device will authenticate them against TACACS+ if local authentication fails.

Correct Answer: *B*

Community vote distribution

B (100%)

mgiuseppe86 2 months, 3 weeks ago

Selected Answer: B

B is correct. Due to what I wrote below.

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

When login is indicated in the aaa authentication method, any passwords in the VTY will be ignored. So this removes A from the equation.

C is wrong because it says only users at 192.168.0.202. That implies they are attempting to telnet/ssh from that server, that IP is an authentication server for TACACS+ not a source connection.

D is wrong because only TACACS+ is listed in the AAA string. There is no fall-back method

B is correct because all users are forced to authenticate against TACACS+ only.

upvoted 1 times

dudalykai 3 months, 1 week ago

There question is constructed incorrectly coz there are no such commands in cli: aaa authentication login authorizationlist tacacs+. After user list "authorizationlist" you have to describe that it is a group and then method radius/tac.
aaa authentication login authorizationlist group tacacs+
The user group is known by tacacs+ server whos IP is - 192.168.0.202
So the answer should be: C

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

There is such a command... you need to first put in aaa new-model to activate AAA Authentication.

SW1(config)#aaa new-model
SW1(config)#authentication login authorizationlist tacacs+
SW1config)#do show run | i aaa
Building configuration...
aaa new-model
aaa authentication login authorizationlist group tacacs+
aaa session-id common

upvoted 1 times

RamazanLokov 6 months ago

I think correct answer D, because first login authentication is custom list applied on VTY

upvoted 1 times

dragonwise 8 months ago

I would say both B and C are correct

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 2 times

Question #279 *Topic 1*

Which deployment option of Cisco NGFW provides scalability?

A. inline tap

B. high availability

C. clustering

D. tap

Correct Answer: *C*

baid 1 year, 9 months ago

Clustering lets you group multiple Firepower Threat Defense (FTD) units together as a single logical device. Clustering is only supported for the FTD device on the Firepower 9300 and the Firepower 4100 series. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

upvoted 4 times

examShark 2 years, 6 months ago

The given answer is correct

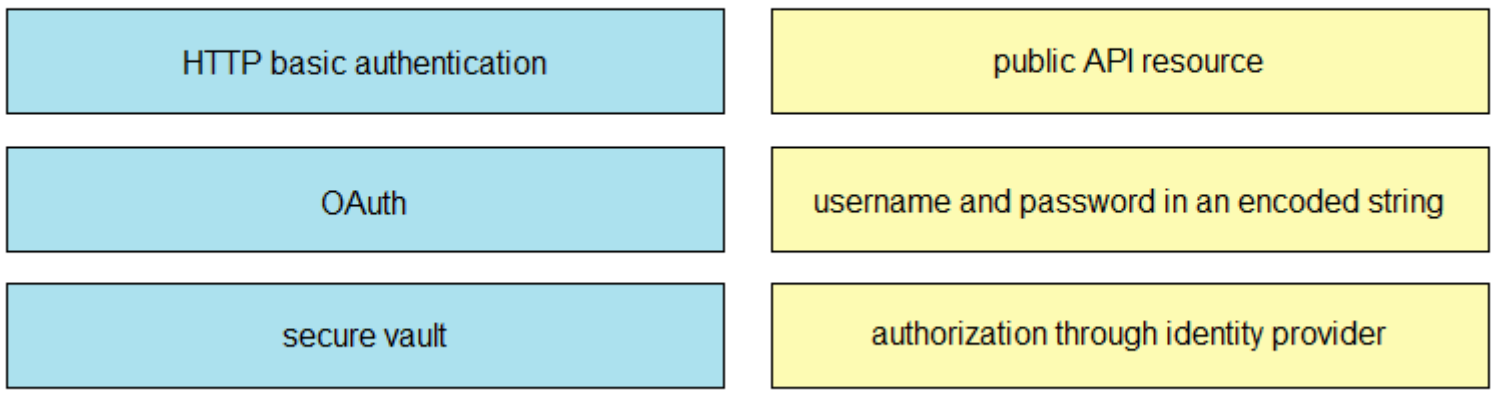
upvoted 4 times

DRAG DROP -

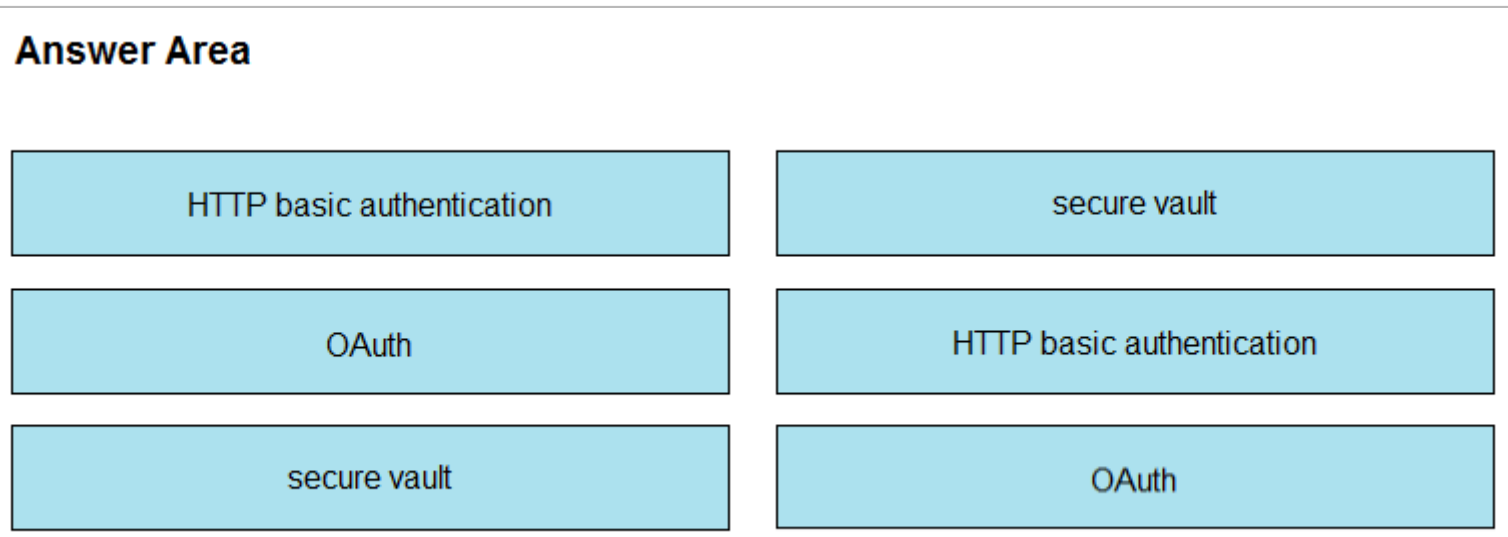
Drag and drop the REST API authentication methods from the left onto their descriptions on the right.

Select and Place:

Answer Area



Correct Answer:



[Removed] Highly Voted 4 months, 3 weeks ago

OAuth
HTTP authentication
Secure Vault

upvoted 5 times

jackr76 Most Recent 7 months ago

How can a public API resource be in a secure vault? It's public (!) and holds no credentials.

I think it should be:
Public API resource - OAuth
username and passeord in an encoded string - secure vault
authorization through indentity provider - HTTP basic authentication

upvoted 4 times

sam6996 4 months, 4 weeks ago

I think the provided answer is right, do a quick google search of cisco secure vault, theres not that much information on it though.

upvoted 1 times

GATUNO 2 years ago

Agree with Johconnor

upvoted 1 times

GATUNO 2 years ago

OAuth is a way to get access to protected data from an application. It's safer and more secure than asking users to log in with passwords., NO CORRECT , , oauth is an application

upvoted 1 times

Johnconnor2021 2 years ago

you are wrong, OAuth needs an identity provider to get the interchange of Tokens and then the user access without the use of user/pass. OAuth is not an application, its a protocol. Two different things. Answer is correct.

upvoted 7 times

Question #281 *Topic 1*

In a Cisco SD-Access solution, what is the role of the Identity Services Engine?

A. It is leveraged for dynamic endpoint to group mapping and policy definition.

B. It provides GUI management and abstraction via apps that share context.

C. It is used to analyze endpoint to app flows and monitor fabric status.

D. It manages the LISP EID database.

Correct Answer: *A*

Community vote distribution

A (100%)

Hamzaaa Highly Voted 2 years, 7 months ago

Cisco Identity Services Engine (ISE) enables a dynamic and automated approach to policy enforcement that simplifies the delivery of highly secure network access control.

upvoted 10 times

JCV13 Most Recent 1 year, 1 month ago

Selected Answer: A

Given answer is correct

upvoted 2 times

examShark 2 years, 6 months ago

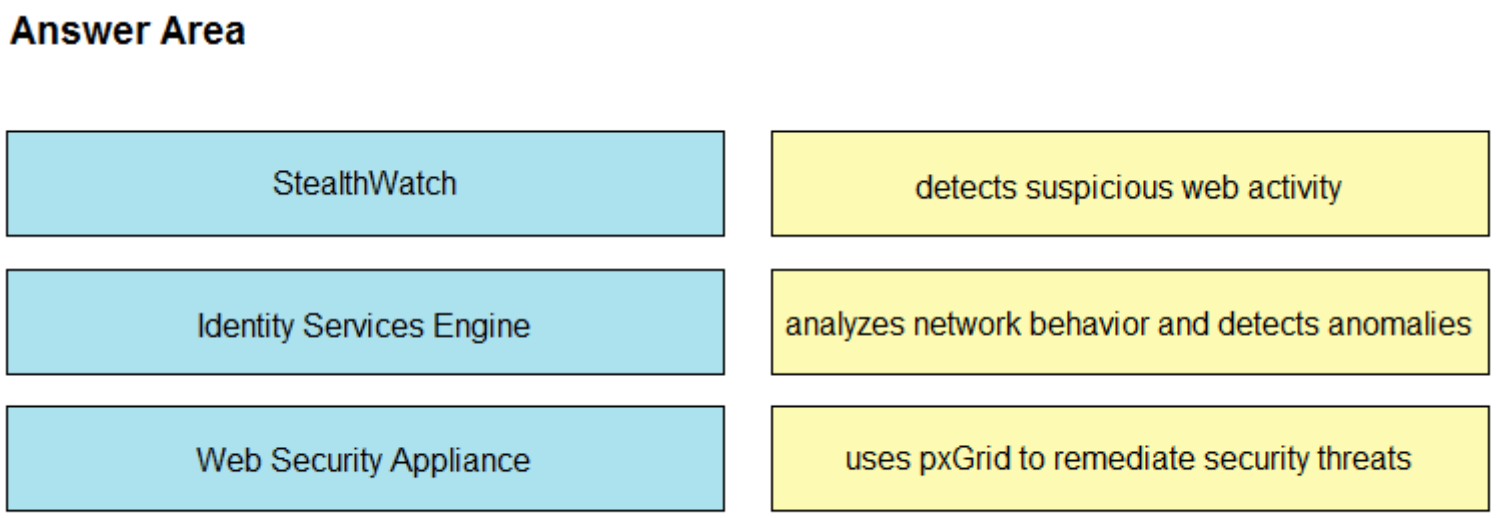
Given answer is correct

upvoted 4 times

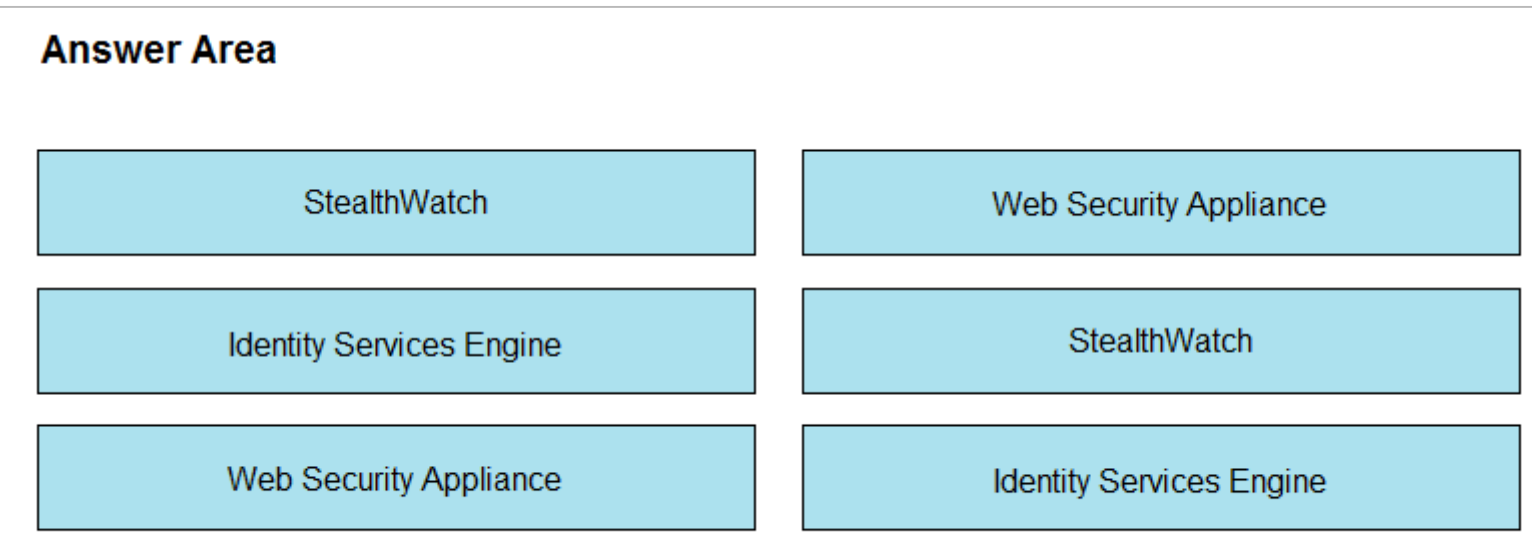
DRAG DROP -

Drag and drop the solutions that compromise Cisco Cyber Threat Defense from the left onto the objectives they accomplish on the right.

Select and Place:



Correct Answer:



CCNPWILL 1 month, 2 weeks ago

Provided answer is correct.

upvoted 1 times

[Removed] 4 months, 3 weeks ago

correct.

upvoted 1 times

bogd 1 year, 9 months ago

I am pretty sure this is about solutions that COMPRISE Cisco Cyber Threat Defense, not COMPROMISE it :) . Nevertheless, the answer seems correct.

upvoted 3 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 2 times

DRAG DROP -
An engineer creates the configuration below. Drag and drop the authentication methods from the left into the order of priority on the right.
Not all options are used.

R1#sh run | i aaa -
aaa new-model
aaa authentication login default group ACE group AAA_RADIUS local-case aaa session-id common
R1#
Select and Place:

Answer Area

tacacs servers of group ACE	priority 1
local configured username in non-case-sensitive format	priority 2
local configured username in case-sensitive format	priority 3
AAA servers of ACE group	priority 4
AAA servers of AAA_RADIUS group	
If no method works, then deny login	

Correct Answer:

Answer Area

tacacs servers of group ACE	local configured username in case-sensitive format
local configured username in non-case-sensitive format	AAA servers of ACE group
local configured username in case-sensitive format	AAA servers of AAA_RADIUS group
AAA servers of ACE group	tacacs servers of group ACE
AAA servers of AAA_RADIUS group	
If no method works, then deny login	

xziomal9 Highly Voted 2 years, 2 months ago
The correct answer is:
priority 1: AAA servers of ACE group
priority 2: AAA servers of AAA_RADIUS group

priority 3: local configured username in case-sensitive format
priority 4: If no method works, then deny login
upvoted 123 times

nushadu 11 months, 3 weeks ago

true,
aaa authentication login default group ACE group AAA_RADIUS local-case
aaa session-id common
upvoted 2 times

Hamzaaa Highly Voted 2 years, 7 months ago

1.AAA ISE
2.AAA Radius
3.Local sensitive case
4.deny if nothing works
upvoted 24 times

[Removed] Most Recent 4 months, 3 weeks ago

Damn! the given answer is so out of the field...

AAA ACE Grp
AAA AAA_RADIUS grp
Local case sensitive
deny login
upvoted 2 times

wr4net 6 months, 1 week ago

I hate this answer given. all dumps sites shows the same answer as examtopics. as far as im concerned, it should be:

priority 1: AAA servers of ACE group (cannot assume AC has tacacs)
priority 2: AAA servers of AAA_RADIUS group (cannot assume radius group name has only radius servers
priority 3: local configured username in case-sensitive format (3rd option in aaa line will be the third priority, case = case sensitive)
priority 4: If no method works, then deny login (last option, if blank is to deny)

unless someone can come up with good logic, otherwise, im sticking to my answer. i thought maybe there was some tacacs versus radius priority if they were a part of the same group, but that's not possible, as groups need keyword "radius', or 'tacacs' specified.
upvoted 1 times

wr4net 6 months, 2 weeks ago

groups are configured as either a radius or tacacs type:
aaa group server tacacs+ MyTacGrpName
aaa group server radius MyRadGrpName

so you cannot assume ACE is a Tac groups. that rules out that option. also last option is always deny if all methods fail.

Lastly, WTF on the word priority. does Priority 1 mean the first (highest) priority, or does priority 4 mean the highest (first) priority. I would assume the P1 = try first. In this case, i would go with:
priority 1: AAA servers of ACE group
priority 2: AAA servers of AAA_RADIUS group
priority 3: local configured username in case-sensitive format
priority 4: If no method works, then deny login

Other dump sites appear to get this wrong too, so im questioning my logic now.
upvoted 1 times

danman32 4 months ago

Even if the priority list was supposed to be reverse order than what we'd interpret, answer still wrong. So you can keep your sanity :)
upvoted 1 times

charafDZ 9 months, 1 week ago

"The "local-case" method is used to enforce the typed username to be case sensitive, but in the case of the "local" method the you could type the username in upper or lower case and the Cisco device will accept it. Imagine that you have the "admin" local user, if the you want to login to the device and the method applied is "local" you could login with the "ADMIN" variant of the user and the router/switch will normally accept it, that doesn't happens if the "local-case" keyword is in the AAA policy, so you will have to type the exact username in "admin" in this case."

https://learningnetwork.cisco.com/s/question/0D53i00000KstF1CAJ/ppp-chap-authentication-local-vs-localcase
upvoted 1 times

x3rox 9 months, 4 weeks ago

local: case insensitive for username
local-case: case sensitive for username
upvoted 2 times

kalbos 1 year ago

group ACE
group AAA_RADIUS
local-case
deny
upvoted 3 times

examShark 2 years, 6 months ago

Given answer is correct

upvoted 2 times

YTAKE 2 years, 2 months ago

I believe so.

1 --- ACE is just the group name, it does not necessarily mean (TACACT+ or Radius)
2 --- The order is also important: the first group is used first, and so on

upvoted 2 times

YTAKE 2 years, 2 months ago

group ACE
group AAA_RADIUS
local-case
deny

upvoted 6 times

examShark 2 years, 6 months ago

sorry, should be:

group ACE
group AAA_RADIUS
local-case
deny

upvoted 23 times

AliMo123 2 years, 7 months ago

The aaa new-model command immediately applies local authentication to all lines and interfaces (except console line line con 0). so first the local configuration will apply.
https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

upvoted 1 times

thenewguy918 2 years, 6 months ago

After reading through the link you provided it looks like the local authentication is only applied to those interfaces immediately after applying the aaa new-model command to prevent locking out remote users (assuming you created a local login before running the command).

But after using the "aaa authentication login default group ACE group AAA_RADIUS local-case" command it replaces the login procedure for all access ports except any that have a different authentication method applied to them manually. The local login is now the 3rd option in the default list after running that command.

The problem with this question is you do not know if the servers in those groups are radius or tacacs. You can assume the AAA_RADIUS group is all radius servers.

upvoted 2 times

thenewguy918 2 years, 6 months ago

actually i guess it wouldn't matter if they are radius or tacacs servers since they are both considered AAA

From what I have gathered I beleive the answer to be
1. AAA Servers of ACE
2. AAA Servers of AAA_RADIUS
3. Local Case Sensative
4. Deny login

upvoted 12 times

netpeer 2 years, 7 months ago

Broken question

upvoted 1 times

timtgh 1 year, 6 months ago

The question is fine, just the answer shown here is wrong.

upvoted 4 times

netpeer 2 years, 7 months ago

and the local-case is the 1st method not the last!!

upvoted 1 times

danman32 4 months ago

No because local-case is last on the list. The server groups are first in the list.

upvoted 1 times

netpeer 2 years, 7 months ago

This seems wrong.
The local work is missing from the list and who says that group has TACAS servers??

upvoted 1 times

Question #284 *Topic 1*

What is provided by the Stealthwatch component of the Cisco Cyber Threat Defense solution?

A. real-time threat management to stop DDoS attacks to the core and access networks

B. real-time awareness of users, devices, and traffic on the network

C. malware control

D. dynamic threat control for web traffic

Correct Answer: *B*

Community vote distribution

B (100%)

SergeBesse 1 year, 2 months ago

Selected Answer: B

correct answer

upvoted 2 times

miccamilla 1 year, 6 months ago

Selected Answer: B

Stealthwatch does not take actions

upvoted 2 times

LM77 1 year, 10 months ago

B is correct

"Cisco Stealthwatch collects and analyzes massive amounts of data to give even the largest, most dynamic networks comprehensive internal visibility and protection. It helps security operations teams gain real-time situational awareness of all users, devices, and traffic on the extended network so they can quickly and effectively respond to threats"

Page 1

https://media.zones.com/images/pdf/cisco-stealthwatch-solution-overview.pdf

upvoted 4 times

cracanici 2 years, 3 months ago

B

It does analysis =awareness

upvoted 4 times

spapi0390 2 years, 4 months ago

A i correct, B is for NGIPS

upvoted 4 times

yuiiuy 2 years, 3 months ago

I agree.

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 4 times

Question #285 *Topic 1*

An engineer must configure an ACL that permits packets which include an ACK in the TCP header. Which entry must be included in the ACL?

A. access-list 110 permit tcp any any eq 21 tcp-ack

B. access-list 10 permit tcp any any eq 21 established

C. access-list 110 permit tcp any any eq 21 established

D. access-list 10 permit ip any any eq 21 tcp-ack

Correct Answer: *C*

Community vote distribution

C (100%)

Chuckzero 3 months ago

Correct is C.
The purpose of using the established keyword is to allow the return traffic of an established connection, while denying any new connection attempts. This can be useful in scenarios where you want to allow responses from outbound connections initiated from within your network while still maintaining security by not allowing new inbound connections on that port.

With the given ACL rule in the answer options, it is clear that we are talking about FTP Server which uses port 21. If a client from inside the network initiates an FTP connection to an external FTP server (which typically uses port 21 for control), the firewall would allow the returning control traffic from the FTP server due to the established keyword.

upvoted 1 times

flash007 4 months, 1 week ago

extended access lists allow ports whereas standards dont

upvoted 4 times

kalbos 1 year ago

Selected Answer: C

it is a extendend access-list
Standard 1–99 and 1300–1999
Extended IP 100–199 and 2000–2699

upvoted 3 times

SergeBesse 1 year, 2 months ago

Selected Answer: C

correct answer

upvoted 1 times

youtri 1 year, 8 months ago

B and D are Numbered ,standared ACL, (0-99)
Numbered, standered ACL does not filter the trafic type (TCP,UDP, IP,ICMP,TCP.....)

upvoted 4 times

Jheax 1 year, 8 months ago

Selected Answer: C

The correct answer is C because the ACL contains the source and destination (it's an extended ACL).

upvoted 4 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

Hustle01 2 years, 5 months ago

Can you please explain , B and C looks similar , the only difference is one has 10 and the other has 110, please can you explain , thanks

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

You cannot create ACLs permitting or denying ports or destination networks in numbered standard ACL lists from 1-99. You must create an extended ACL using access-list 100-199

upvoted 1 times

chris110 2 years, 5 months ago

i think: B is ACL 10, so standard acl. Standard acl makes decisions only by ip. C is ACL 110 (Range 100-199 & 2000-2699 is extended acl) so it makes deciscions by ip, protocol etc.

upvoted 9 times

MookieLoLo 2 years, 1 month ago

it explicit say TCP traffic so the standard ACL won't work so the given answer is correct

upvoted 1 times

Node 2 years, 4 months ago

to add to the above comment, standard ACL do not require to specify the destination. it would have been "permit any" the second any indicates the destination. It is therefore, the wrong sintax.

upvoted 2 times

Question #286 *Topic 1*

A client with IP address 209.165.201.25 must access a web server on port 80 at 209.165.200.225. To allow this traffic, an engineer must add a statement to an access control list that is applied in the inbound direction on the port connecting to the web server.
Which statement allows this traffic?

A. permit tcp host 209.165.200.225 lt 80 host 209.165.201.25

B. permit tcp host 209.165.201.25 host 209.165.200.225 eq 80

C. permit tcp host 209.165.200.225 eq 80 host 209.165.201.25

D. permit tcp host 209.165.200.225 host 209.165.201.25 eq 80

Correct Answer: *D*

Community vote distribution

C (89%) 6%

sleep Highly Voted 3 years, 6 months ago
inbound direction - C
upvoted 67 times

Saqib79 Highly Voted 3 years, 6 months ago
Correct Option is B.
upvoted 28 times

bk989 6 months, 2 weeks ago
it says "inbound"
upvoted 1 times

Carl1999 2 years ago
"on the port connecting to the web server"
-> C
upvoted 4 times

Chuckzero Most Recent 3 months ago
Correct answer is B.

Option C is a wrong syntax for an extended access-list which is based in terms of the source and destination IPs.
upvoted 1 times

Chuckzero 3 months ago
My bad. it is actually source and destination port that we are considering here, so C has the right syntax for source and destination port.
upvoted 1 times

danman32 4 months ago
I don't care what interface or direction you try to apply ACL for answer D, it isn't going to work.
Why? Because port 80 can only be associated with the webserver host IP.
Answer D assumes that port 80 would be associated with the client IP, which would never be the case.
Not in the real world anyway.
upvoted 1 times

XBfoundX 9 months, 1 week ago
The correct answer here is C:

Remember that the the interface with the ACL applied is the server interface.
so the flow at first will be client ==> server
Here there is not any acl applied inbound and outbound.

Then the traffic flow must return like this:
server ==> client
In the server port the acl is applied, so in this case because is return traffic the source ip address and tcp port will be of the server and the destination will be the client.

So the statement of the ACL is:
permit tcp host 209.165.200.225 eq 80 host 209.165.201.25

(permit the traffic sourced by the server to reach the destination)

So the answer is for sure C
upvoted 7 times

Brand 9 months, 1 week ago

Selected Answer: C

the inbound traffic coming from the port connected to the server will contain the server's IP address therefore the ACL statement must have the source IP as the server's IP. The client will reach the server using TCP 80 as the destination so the return traffic sourced by the server will have port 80 as the source TCP. Which in this case I'd go with C.

upvoted 1 times

Dataset 9 months, 1 week ago

Selected Answer: C

Its C , inbound direction on port connecting the host
regards

upvoted 1 times

rafaelinho88 10 months ago

Selected Answer: B

i asked chatgpt and it came with this answer.
permit tcp host 209.165.201.25 host 209.165.200.225 eq 80
so, according to chatgpt, it is B

upvoted 1 times

well123 9 months, 2 weeks ago

no, this will only work if the ACL is applied on the inbound for port facing the client.
the question is "inbound port facing web server"

upvoted 1 times

TSKARAN 10 months ago

Selected Answer: C

NOTE: applied in the inbound direction on the port connecting to the web server.

upvoted 1 times

Nickplayany 10 months, 1 week ago

C. permit tcp host 209.165.200.225 eq 80 host 209.165.201.25 Most Voted

permit tcp host ---- THE SOURCE - THE PORT --- THE DESTINATION.

The exact same question - answer can be found at question 272

upvoted 1 times

Rose66 10 months, 3 weeks ago

Selected Answer: C

Inbound on server side >> C

upvoted 1 times

Asymptote 11 months ago

Selected Answer: C

permit webserver source port 80 toward client random port.

upvoted 1 times

kewokil120 11 months ago

Selected Answer: C

inbound direction - C

upvoted 1 times

Patel777 11 months ago

Selected Answer: C

ACL is applied on inbound direction of web server

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: C

>ACL that is applied in the inbound direction on the port connecting to the web server.
it means we need to match by ACL web_serv_IP_ADDR:TCP_PORT_80 in the SOURCE of the IP packet & DESTINATION remote HOST web client (who initiates HTTP connection)
>C. permit tcp host 209.165.200.225 eq 80 host 209.165.201.25
looks good, i believe ...

upvoted 1 times

MO_2022 11 months, 3 weeks ago

Selected Answer: C

inbound direction - C

upvoted 1 times

nushadu 12 months ago

C. no doubt
upvoted 1 times

Question #287 *Topic 1*

Which standard access control entry permits traffic from odd-numbered hosts in the 10.0.0.0/24 subnet?

A. permit 10.0.0.0 0.0.0.1

B. permit 10.0.0.1 0.0.0.254

C. permit 10.0.0.1 0.0.0.0

D. permit 10.0.0.0 255.255.255.254

Correct Answer: *B*

edg Highly Voted 3 years, 3 months ago
Option "B".

https://en.wikipedia.org/wiki/Wildcard_mask

Any wildcard bit-pattern can be masked for examination. For example, a wildcard mask of 0.0.0.254 (binary equivalent = 00000000.00000000.00000000.11111110) applied to IP address 10.10.10.2 (00001010.00001010.00001010.00000010) will match even-numbered IP addresses 10.10.10.0, 10.10.10.2, 10.10.10.4, 10.10.10.6 etc. Same mask applied to 10.10.10.1 (00001010.00001010.00001010.00000001) will match odd-numbered IP addresses 10.10.10.1, 10.10.10.3, 10.10.10.5 etc
upvoted 18 times

shermeister Highly Voted 2 years, 11 months ago
"B"
https://www.networkfuntimes.com/using-wildcard-masks-to-filter-odd-or-even-numbered-ip-addresses-juniper-junos-cisco-ios/
upvoted 7 times

Feliphus 11 months, 4 weeks ago
Thanks for you link, first time I see a wildmask to split between even-IP-addresses and odd-IP-addresses
access-list 101 permit ip any 10.10.10.0 0.0.0.254 -> even
access-list 102 permit ip any 10.10.10.1 0.0.0.254 -> odd
upvoted 4 times

MerlinTheWizard 10 months ago
it's mostly to test your understanding of it, not really used in enterprise networks, but yeah, it's an interesting one to play around with :)
upvoted 2 times

wr4net 6 months, 2 weeks ago
thx for the link
upvoted 1 times

danman32 Most Recent 4 months ago
Answer is B.
A is not correct, would allow 10.0.0.0 or 10.0.0.1
C is not correct, would allow only 10.0.0.1 (wildcard 0.0.0.0 same as 'host')
D is not correct, would allow any even IP: x.x.x.0
upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago
D is not correct because you have to specify a wildcard mask, not a subnet mask in an ACL.
upvoted 1 times

dragonwise 8 months, 1 week ago
what is happening to Cisco?
upvoted 6 times

MerlinTheWizard 10 months ago
Ah.. this brings back memories :D
upvoted 2 times

Refer to the exhibit.

```
Extended IP access list EGRESS
10 permit ip 10.1.100.0  0.0.0.255 10.1.2.0 0.0.0.255
20 deny ip any any
```

An engineer must modify the access control list EGRESS to allow all IP traffic from subnet 10.1.10.0/24 to 10.1.2.0/24. The access control list is applied in the outbound direction on router interface GigabitEthernet 0/1.

Which configuration command set will allow this traffic without disrupting existing traffic flows?

A.

```
config t
    ip access-list extended EGRESS
    permit ip 10.1.10.0 255.255.255.0 10.1.2.0 255.255.255.0
```

B.

```
config t
    ip access-list extended EGRESS2
     permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
     permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
     deny ip any any
     !
     interface g0/1
      no ip access-group EGRESS out
      ip access-group EGRESS2 out
```

C.

```
config t
    ip access-list extended EGRESS
    permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
```

D.

```
config t
    ip access-list extended EGRESS
    5 permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
```

Correct Answer: *D*

Nhan Highly Voted 2 years, 2 months ago

Basically, use the sequence number to add the entry to the access list so the list will be processing without interrupting

upvoted 6 times

[Removed] Most Recent 4 months, 3 weeks ago

D.

The ACE needs to be before the deny any ACE, or it won't be processed.

upvoted 1 times

markymark874 11 months ago

D is correct since question is asking you to modify not create a new access group.

upvoted 2 times

WINDSON 1 year ago

if i change answer D sequence number to 15. will it work ?

upvoted 1 times

bora4motion 12 months ago

yes, as long as above 20.

upvoted 3 times

Tannhaus 1 year, 5 months ago

Correct answer is D.
B would also work but there would be a short disruption of traffic flow.

upvoted 2 times

youtri 1 year, 11 months ago

given answer is correct,
for more expalanation the sequence number should be less than 19.

upvoted 4 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 2 times

hsitar 2 years, 8 months ago

Since question is about modifying the 'EGRESS' acl, option D is correct.

upvoted 4 times

Which configuration restricts the amount of SSH traffic that a router accepts to 100 kbps?

A.

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
  interface GigabitEthernet0/1
     ip address 209.165.200.225 255.255.255.0
     ip access-group EGRESS out
     service-policy input CoPP_SSH
!
   ip access-list extended CoPP_SSH
      permit tcp any any eq 22
!
```

B.

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
  interface GigabitEthernet0/1
     ip address 209.165.200.225 255.255.255.0
     ip access-group EGRESS out
     service-policy input CoPP_SSH
!
   ip access-list extended CoPP_SSH
      deny tcp any any eq 22
!
```

C.

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
   control-plane
      service-policy input CoPP_SSH
!
  ip access-list extended CoPP_SSH
      permit tcp any any eq 22
!
```

D.

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
   control-plane transit
      service-policy input CoPP_SSH
!
  ip access-list extended CoPP_SSH
     permit tcp any any eq 22
!
```

Correct Answer: *C*

examShark Highly Voted 2 years, 6 months ago
The given answer is correct
upvoted 7 times

seven_legs Highly Voted 1 year, 10 months ago
The given answer is correct (C) as the configuration is blocking traffic to the control plane of the appliance using Control Plane Policing (CoPP).
upvoted 5 times

danman32 Most Recent 4 months ago
Not that either is the correct answer, but can anyone spot the difference between answer A and B?
upvoted 1 times

danman32 4 months ago
OK, found it thanks to discussion. A has permit 22, B has deny 22.
upvoted 1 times

Badger_27 8 months, 3 weeks ago
Another spot the difference challenge
upvoted 1 times

monoki 8 months, 3 weeks ago
do you still see the 350-401 exam on the site? i can't find it, it says 404 error for all the cisco exams.
upvoted 1 times

sayed_2908 1 year, 3 months ago
C and D are the same??
upvoted 1 times

wr4net 6 months, 2 weeks ago
transit keyword = through router
upvoted 1 times

RREVECO 1 year, 2 months ago

NOPE

C) =Traffic generated by ROUTER that matches access list CoPP_SSH is policed.
D) =Traffic passing through ROUTER that matches access list CoPP_SSH is policed.

upvoted 10 times

Claudiu1 2 days, 21 hours ago

just a small correction:
C) = traffic RECEIVED by the ROUTER that matches access list CoPP_SSH is policed.
This is because the policy-map is applied using 'input' keyword.

upvoted 1 times

Nickelkeep 2 years, 3 months ago

The correct answer is A
permit tcp any any eq 22

upvoted 3 times

error_909 2 years, 2 months ago

its C, please review this topic.

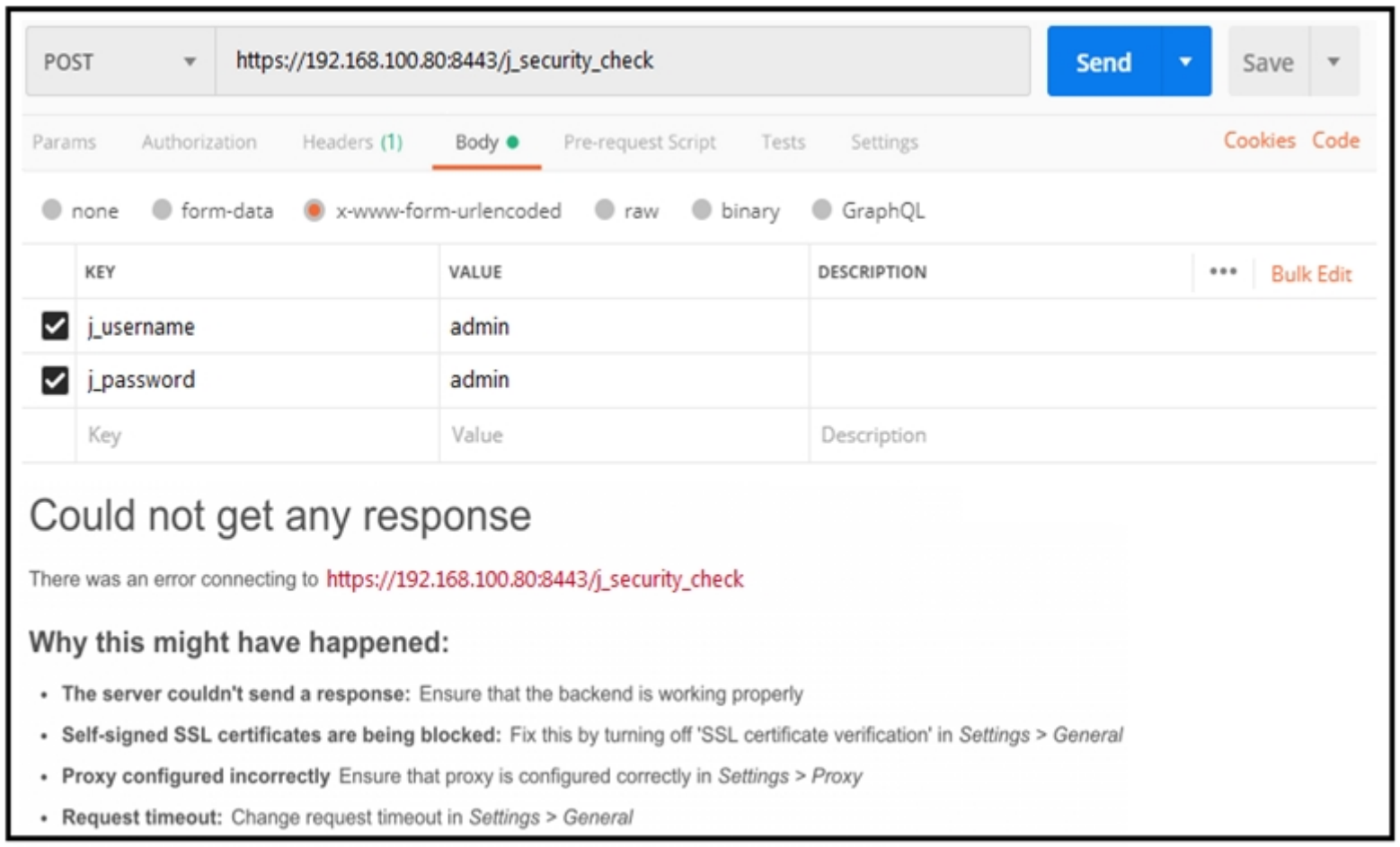
upvoted 8 times

timtgh 1 year, 6 months ago

They all say that, except for B.

upvoted 1 times

```
vedge-001# show control connections

PEER                                PEER
CONTROLLER
PEER  PEER PEER         SITE  DOMAIN PEER
PRIV PEER                           PUB
GROUP
TYPE  PROT SYSTEM IP  ID    ID     PRIVATE IP                          PORT
PUBLIC IP                    PORT LOCAL COLOR   PROXY STATE UPTIME   ID
-------------------------------------------------------------------------
-------------------------------------------------------------------------
------
vsmart  dtls 4.4.4.70  100   1      192.168.100.80
12446 10.10.20.70                   12446 default      No    up
0:02:24:09 0
vbond   dtls 0.0.0.0   0     0      192.168.100.81
12346 10.10.20.80                   12346 default      -     up
0:02:24:10 0
vmanage dtls 4.4.4.90  100   0      192.168.100.82
12446 10.10.20.90                   12446 default
```



Refer to the exhibit. What step resolves the authentication issue?

A. use basic authentication

B. change the port to 12446

C. target 192.168.100.82 in the URI

D. restart the vsmart host

Correct Answer: *D*

Community vote distribution

C (100%)

hsitar Highly Voted 2 years, 8 months ago

C is the correct answer. vManage is used for managing.

upvoted 23 times

mgiuseppe86 2 months, 3 weeks ago

You dont say! Next you tell me vBond is used for bondage!

upvoted 2 times

danman32 Most Recent 4 months ago

Besides wrong IP if we need to connect to vManage, don't we have an issue with postman connecting to the wrong port? That's why I was leaning on answer B.

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

This is a Cisco exam, we don't use logic around here!

upvoted 2 times

rami_mma 8 months, 1 week ago

Selected Answer: C

C is correct

upvoted 2 times

rami_mma 8 months, 1 week ago

Selected Answer: C

C is correct

upvoted 2 times

Brand 9 months, 1 week ago

Selected Answer: C

I don't think Cisco would publicly recommend restarting their devices in the case of authentication failure.

upvoted 4 times

mgiuseppe86 2 months, 3 weeks ago

They once kept me on a call for 12 hours because they refused to let me reboot the cisco cucm server due to an issue.

i rebooted after i had enough tinkering with services and what do you know, it worked!

upvoted 1 times

Rose66 10 months, 3 weeks ago

Selected Answer: C

C for vmanage

upvoted 1 times

JCV13 1 year, 1 month ago

Selected Answer: C

C should be the correct one.

upvoted 1 times

FrameRelay 1 year, 1 month ago

Selected Answer: C

the #show control connections output demonstrated the connection to the vManage isn't up, not that vManage is not running, hence why rebooting won't help, certainly because the only reboot answer refers to vSmart so another component again. Postman needs to point to the vManage IP to establish a connection, therefore answe C is the correct answer.

upvoted 2 times

nour 1 year, 4 months ago

Selected Answer: C

According to "show control connections" command. We should point to 192.168.100.82 instead of 192.168.100.80.

upvoted 3 times

Edwinmolinab 1 year, 4 months ago

vmanage is not up given answer is correct

upvoted 2 times

[Removed] 5 months ago

answer says to restart the vsmart host, not the vmanage host. The vsmart host is up per the output of the show control connections command

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: C

It should be C

upvoted 1 times

xziomal9 1 year, 11 months ago

Selected Answer: C

The correct answer is:
C. target 192.168.100.82 in the URI

upvoted 2 times

xziomal9 2 years, 2 months ago

The correct answer is:
C. target 192.168.100.82 in the URI

upvoted 2 times

kthekillerc 2 years, 2 months ago

Correction, it is C the output show .82 is default controller, we need to target the uri towards .80

upvoted 1 times

certcisco 2 years, 4 months ago

I'm also leaning towards D. The first Screenshot does NOT show "UP" like the other 2 components. Leading me to believe it's not up and restarting would help. Just changing the IP for C is not changing the port...so it wouldn't resolve the problem either.

upvoted 2 times

certcisco 2 years, 4 months ago

Sorry...after looking over the screenshot and more comparison, the vSmart shows as UP. It's the vManage that does not have up status. I'm leaning towards C again.

upvoted 1 times

kthekillerc 2 years, 5 months ago

should be A the error is with the security certificate of vsmart not allowing it to connect. vsmart is what is down not vmanage so it wouldnt be c since that is the vmanage ip address, not b because it already has that port number assigned, no need to restart vsmart it is up and running fine just not authenticating due to certificate issues. should be A

upvoted 3 times

Chkoupipi2 2 years, 7 months ago

I guess C is correct

upvoted 1 times

Refer to the exhibit.

```
Router#sh run | b vty
line vty 0 4
 session-timeout 30
 exec-timeout 120 0
 session-limit 30
 login local
line vty 5 15
 session-timeout 30
 exec-timeout 30 0
 session-limit 30
 login local
```

Security policy requires all idle exec sessions to be terminated in 600 seconds.

Which configuration achieves this goal?

A. line vty 0 15 absolute-timeout 600

B. line vty 0 15 no exec-timeout

C. line vty 0 15 exec-timeout 10 0

D. line vty 0 4 exec-timeout 600

Correct Answer: *C*

Community vote distribution

C (100%)

Jheax Highly Voted 1 year, 8 months ago

Selected Answer: C

exec-timeout is given in minutes, so 600secs is 10mins.

upvoted 6 times

H3kerman Highly Voted 1 year ago

Selected Answer: C

Tested on real device:
WS-C3850(config)#line vty 0 15
WS-C3850(config-line)#exec-timeout ?
<0-35791> Timeout in minutes

WS-C3850(config-line)#exec-timeout 10 ?
<0-2147483> Timeout in seconds
<cr> <cr>

WS-C3850(config-line)#exec-timeout 10 0 ?
<cr> <cr>

upvoted 5 times

myhdtv6 Most Recent 4 months, 2 weeks ago

"Ideal" is the King here...

If not ideal then ABSOLUTE TIMEOUT

**Absolute time out will terminate all the sessions, even if it is an active one
**Exac will only time out the ideal one

upvoted 1 times

Dataset 1 year ago

correct! time is in minutes

upvoted 2 times

Refer to the exhibit.

```
Extended IP access list EGRESS
10 permit ip 10.0.0.0 0.0.0.255 any
!
<Output Omitted>
!
interface GigabitEthernet0/0
ip address 209.165.200.225  255.255.255.0
ip access-group EGRESS out
duplex auto
speed auto
media-type rj45
!
```

An engineer must block all traffic from a router to its directly connected subnet 209.165.200.0/24. The engineer applies access control list EGRESS in the outbound direction on the GigabitEthernet0/0 interface of the router. However, the router can still ping hosts on the 209.165.200.0/24 subnet.

What explains this behavior?

A. Access control lists that are applied outbound to a router interface do not affect traffic that is sourced from the router.

B. After an access control list is applied to an interface, that interface must be shut and no shut for the access control list to take effect.

C. Only standard access control lists can block traffic from a source IP address.

D. The access control list must contain an explicit deny to block traffic from the router.

Correct Answer: *A*

Community vote distribution

A (100%)

nushadu 11 months, 2 weeks ago

Selected Answer: A

https://community.cisco.com/t5/routing/why-do-the-access-lists-not-apply-to-the-locally-generated/td-p/2906340

upvoted 2 times

Jheax 1 year, 8 months ago

Selected Answer: A

Locally (control plane) generated traffic goes from control plane directly to "tx-ring". That is different from processing/forwarding of Transit traffic. Please see the platform's "packet journey" session of Cisco Live or other documentation to see the different internal path & processing for: Transit, forus, exception, locally generated.

upvoted 3 times

Question #293 *Topic 1*

What is a characteristic of a next-generation firewall?

A. only required at the network perimeter

B. required in each layer of the network

C. filters traffic using Layer 3 and Layer 4 information only

D. provides intrusion prevention

Correct Answer: *D*

ashfaque57 8 months, 3 weeks ago

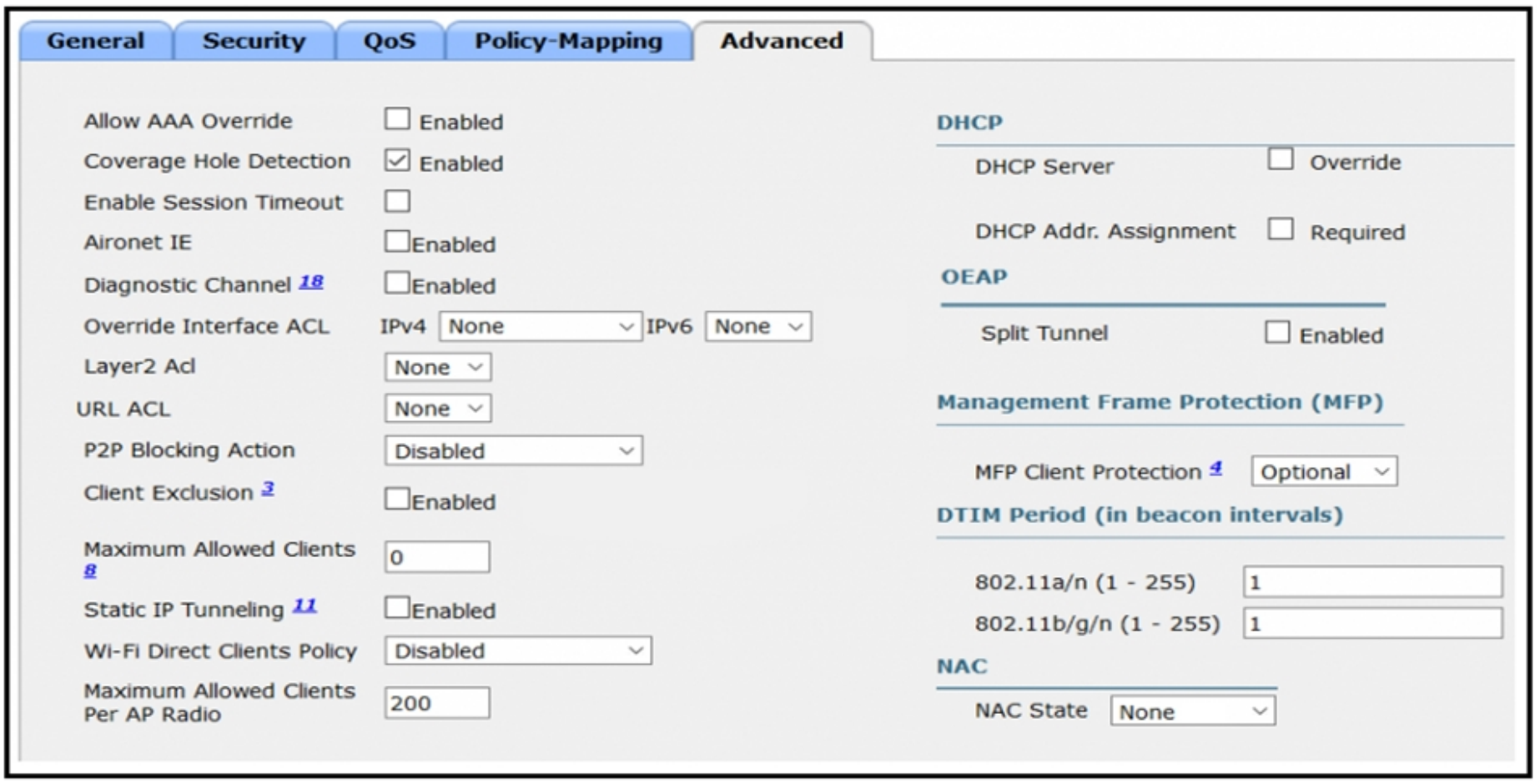
Yes D is Correct answer.

upvoted 2 times

cvndani 1 year, 10 months ago

D is correct

upvoted 2 times



Refer to the exhibit. An engineer is investigating why guest users are able to access other guest user devices when the users are connected to the customer guest
WLAN. What action resolves this issue?

A. implement P2P blocking

B. implement MFP client protection

C. implement Wi-Fi direct policy

D. implement split tunneling

Correct Answer: *A*

Community vote distribution

A (100%)

AlbertoStu 1 year, 7 months ago

Selected Answer: A

This control determines whether the Wireless LAN Controller is configured to prevent clients connected to the same Wireless Local Area Controller from communicating with each other. Wireless Client Isolation prevents wireless clients from communicating with each other over the RF. Packets that arrive on the wireless interface are forwarded only out the wired interface of an Access Point. One wireless client could potentially compromise another client sharing the same wireless network.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01001111.html

upvoted 3 times

AlbertoStu 1 year, 7 months ago

Wrong text was pasted, it should read:

Per WLAN, peer-to-peer configuration is pushed by the controller to FlexConnect AP. In controller software releases prior to 4.2, peer-to-peer blocking is applied globally to all clients on all WLANs and causes traffic between two clients on the same VLAN to be transferred to the upstream VLAN rather than being bridged by the controller . This behavior usually results in traffic being dropped at the upstream switch because switches do not forward packets out the same port on which they are received.

upvoted 1 times

Jheax 1 year, 8 months ago

Selected Answer: A

P2P blocking action needs to be enabled

upvoted 1 times

ciscogear 1 year, 10 months ago

Answer A.
Look at P2P Blocking Action = Disabled

upvoted 2 times

AlexLAN 2 years, 2 months ago

A. Peer 2 Peer blocking is a feature that blocks direct communication between wireless clients that present on the WLAN on the same Wireless LAN Controller.

upvoted 3 times

cracanici 2 years, 3 months ago

They are disabled, yes, but which one needs to be enabled in order to achieve the goal?
A ?

upvoted 1 times

yuiiuy 2 years, 3 months ago

B?
All other options are disabled.

upvoted 1 times

danielponce7 1 year, 10 months ago

MFP talk about encryption method. Reffer:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/82196-mfp.html#intro

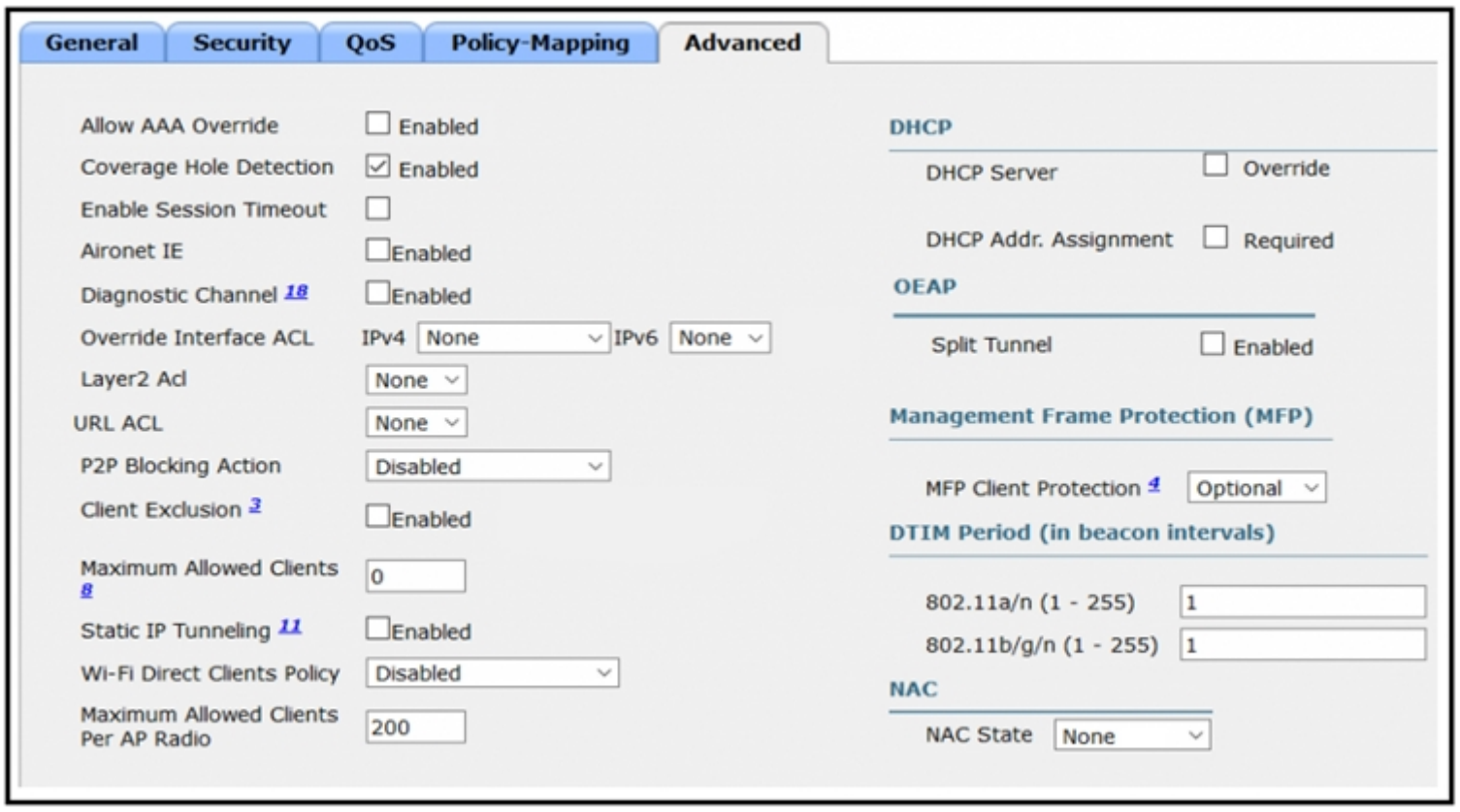
upvoted 2 times

yuiiuy 2 years, 3 months ago

I think this answer to this question is B.

upvoted 1 times

Question #295 *Topic 1*



Refer to the exhibit. An engineer has configured Cisco ISE to assign VLANs to clients based on their method of authentication, but this is not working as expected.
Which action will resolve this issue?

A. enable AAA override

B. set a NAC state

C. utilize RADIUS profiling

D. require a DHCP address assignment

Correct Answer: *C*

Community vote distribution

A (100%)

Adrenalina73 Highly Voted 2 years, 2 months ago

I strongly suggest Enable AAA Override: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/217043-configure-dynamic-vlan-assignment-with-c.html#anc16

From the Advance tab, enable the Allow AAA Override check box to override the WLC configuration when the RADIUS server returns the attributes needed to place the client on the proper VLAN as shown in the image

upvoted 14 times

Jheax Highly Voted 1 year, 8 months ago

Selected Answer: A

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010110111.html

upvoted 5 times

Blue_Water Most Recent 7 months ago

Selected Answer: A

A, Enable AAA Override

upvoted 1 times

asiansensation 8 months, 1 week ago

Answer is B:

AAA override is automatically enabled when you use ISE NAC on a WLAN.

Source: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_0110000.html.xml

upvoted 1 times

reirei 8 months, 1 week ago

but in the exhibit, the AAA override is not checked
upvoted 1 times

Rose66 10 months, 3 weeks ago

Selected Answer: A

Answer should be A
upvoted 1 times

Asymptote 11 months ago

Selected Answer: A

A

Enable AAA Override and Cisco Identity Services Engine (ISE) Assign VLANs features are often used together

Enable AAA Override is a feature that allows the authentication, authorization, and accounting (AAA) server to override the VLAN assignment of a user's device. This allows the AAA server, such as Cisco ISE, to assign a specific VLAN to a user's device based on the user's credentials and the policies configured on the AAA server.
upvoted 3 times

XBfoundX 11 months ago

The answer is A.

On WLC, enable AAA Override parameter using the GUI or CLI.

Enabling this parameter allows the controller to accept the attributes returned by the RADIUS server. The controller then applies these attributes to its clients.

If you don't turn on the override option the WLC will not accept the attribute that the radius server is sending to the WLC basically the client will not get the dynamic vlan ID.

Link below:

https://rscciew.wordpress.com/2014/12/20/aaa-override/
upvoted 2 times

dnjJ56 11 months, 2 weeks ago

Selected Answer: A

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

Extracted from
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_aaa_override.pdf
upvoted 2 times

yousif387 1 year ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010110111.html
upvoted 1 times

Normanby 1 year ago

I just checked - for RADIUS Profiling to function, you need to Tick Allow AAA Override too !!
=Broken Question=
upvoted 1 times

FrameRelay 1 year, 1 month ago

Selected Answer: A

as Jheax explained, AAA is the answer, therefore answer A is correct.
upvoted 1 times

Ioannis34 1 year, 4 months ago

Any thoughts for the right answer?
upvoted 1 times

santiagofarinas 1 year, 4 months ago

An engineer has configured Cisco ISE to assign VLANs (Profiling has been done) however it is not working because the WLC do not accept the parameters sent by the radius server (ISE). So I would say A is correct.
upvoted 1 times

BigMouthDog 1 year, 4 months ago

The answer is 'C', because when you looked at the exhibit, you won't be able to see something related to Radius profiling. You can see 1. AAA override ; 2. NAC state ; & 3. DHCP

upvoted 1 times

Ado_68 1 year, 6 months ago

Of course C is correct answer because ISE use radius protocol and with ISE you can use profiling

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: A

It should be A

upvoted 1 times

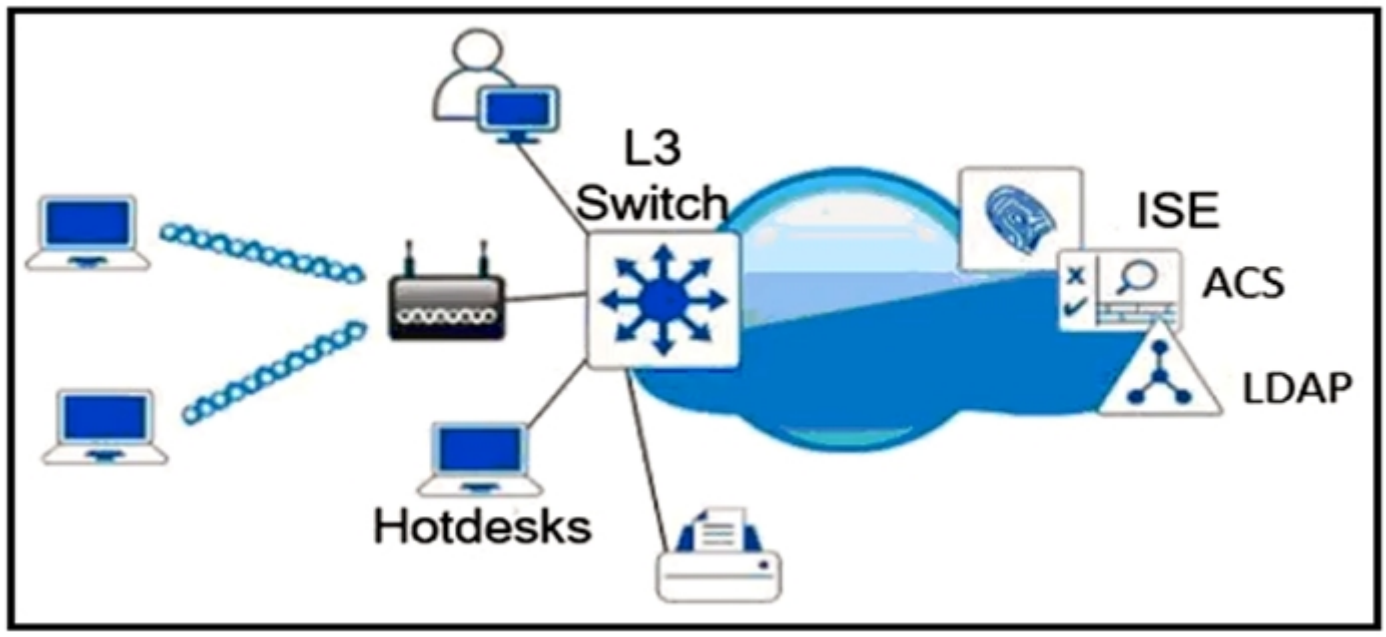
LM77 1 year, 10 months ago

Based on the this article, I would said answer A

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/99121-vlan-acs-ad-config.html

upvoted 1 times

Question #296 *Topic 1*



Refer to the exhibit. Which single security feature is recommended to provide Network Access Control in the enterprise?

A. MAB

B. 802.1X

C. WebAuth

D. port security sticky MAC

Correct Answer: *B*

Community vote distribution

B (75%) A (25%)

Nhan Highly Voted 2 years, 1 month ago

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. The given answer is correct

upvoted 7 times

Chuckzero Most Recent 3 months ago

The correct answer is C.

A is for Layer 2, solely based on device MAC address.
C is for WLC Layer 3 Authentication
D is for Layer 2

Deploying IEEE 802.1X is an excellent approach to enhancing network security through Network Access Control (NAC). 802.1X is a standard for port-based network access control that provides strong authentication and authorization mechanisms, allowing only authorized users and devices to connect to a network.

upvoted 1 times

Toob93 2 months, 3 weeks ago

you mean B is correct, right?

upvoted 1 times

danman32 4 months ago

MAB might be needed for the printer(s), but not for the rest of the network.
For the rest, need 802.1x

upvoted 1 times

kewokil120 11 months ago

Selected Answer: B

802.1x is port security. Mab is kindergarten level security

upvoted 2 times

Asymptote 11 months ago

Selected Answer: A

I go with MAB because no details of the printer and MAB is the safer deployment.

upvoted 1 times

Xerath 11 months, 3 weeks ago

Selected Answer: B

"802.1x", it's even used with WPA2 Enterprise, in a RADIUS server.
https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified
upvoted 1 times

PeterTheCheater 1 year ago
Honestly, not sure about 802.1x. Obviously 802.1x it is the recommended method for an enterprise environment. But in the image there is a printer, some do not support a 1x supplicant. So with MAB auth with make sure that anytype of device will be able to authenticate and access. It is a bit tricky question.
upvoted 2 times

brrrrrrd 1 year, 2 months ago
What does the picture have to do with anything ? Answer is the same lol
upvoted 1 times

mhizha 7 months ago
"Refer to the exhibit..." is how the question starts. The key is if you can use 802.1x on printers or not...
upvoted 1 times

Kingdo 1 year, 10 months ago
Is the printer able to authenticate?
upvoted 1 times

iGlitch 1 year, 1 month ago
Yes, with MAB.
upvoted 1 times

efla 1 year, 7 months ago
printers are now configurable to use .1x auth.
upvoted 1 times

kthekillerc 2 years, 2 months ago
Provided answer is correct
upvoted 3 times

Question #297 *Topic 1*

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
209.165.201.6   209.165.201.1   QM_IDLE           1001 ACTIVE
```

Refer to the exhibit. After configuring an IPsec VPN, an engineer enters the show command to verify the ISAKMP SA status. What does the status show?

A. VPN peers agreed on parameters for the ISAKMP SA.

B. Peers have exchanged keys, but ISAKMP SA remains unauthenticated.

C. ISAKMP SA is authenticated and can be used for Quick Mode.

D. ISAKMP SA has been created, but it has not continued to form.

Correct Answer: *C*

Community vote distribution

C (90%) 10%

Dreket Highly Voted 1 year, 3 months ago

Selected Answer: C

Provided answer is correct. (C)

The ISAKMP negotiations are complete. Phase 1 successfully completed. It remains authenticated with its peer and may be used for subsequent Quick mode exchanges.

https://www.tunnelsup.com/isakmp-ike-phase-1-status-messages/

upvoted 8 times

flash007 Most Recent 4 months, 1 week ago

qm idle is quick mode in isakmp

upvoted 1 times

RREVECO 1 year, 2 months ago

Selected Answer: C

C is correct

upvoted 1 times

smithkeith0023366 1 year, 4 months ago

Selected Answer: B

Official guide says: output shows the ISAKMP SA status is active and in a QM_IDLE state. QM_IDLE means the SA remains authenticated with its peer and may be used for subsequent quick mode exchanges for additional IPsec SAs.

upvoted 1 times

smithkeith0023366 1 year, 4 months ago

Sorry. Answers is C.

upvoted 2 times

diamant 1 year, 3 months ago

AM_ACTIVE / MM_ACTIVE The ISAKMP negotiations are complete. Phase 1 has successfully completed.

upvoted 1 times

gtddrf 2 years, 3 months ago

Answer C is correct.
QM_IDLE state means the tunnel is UP and the IKE SA key exchange was successful, but is idle, it remains authenticated in a (QM) quiescent state but active.

upvoted 3 times

Question #298 *Topic 1*

Which two threats does AMP4E have the ability to block? (Choose two.)

A. email phishing

B. DDoS

C. Microsoft Word macro attack

D. SQL injection

E. ransomware

Correct Answer: *AE*

Community vote distribution

CE (100%)

xziomal9 Highly Voted 2 years, 2 months ago

The correct answer is:
C. Microsoft Word macro attack
E. ransomware

upvoted 11 times

Adrenalina73 Highly Voted 2 years, 2 months ago

I would in favor of C, E :
https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/c11-742008-00-cisco-amp-for-endpoints-wp-v2a.pdf

upvoted 11 times

[Removed] Most Recent 5 months ago

why is finding cisco documentation like pulling teeth? thank you all for posting links, it really helps me save time by not going on a freaking quest.

upvoted 2 times

Rose66 10 months, 3 weeks ago

Selected Answer: CE

Email phishing (A) is more in the realm of WSA/ESA

upvoted 2 times

Asymptote 11 months ago

Selected Answer: CE

protecting email should be the scope of ESA,
macro attack and ransomware typically happens on endpoint.

upvoted 2 times

Jared28 1 year, 5 months ago

Selected Answer: CE

As stated by others, these are the only endpoint attacks, the email security stuff covers A

upvoted 2 times

ChristinaA 1 year, 6 months ago

Selected Answer: CE

Both A & C are endpoint attacks.

upvoted 2 times

ChristinaA 1 year, 6 months ago

I mean C & E.

upvoted 6 times

timtgh 1 year, 6 months ago

Selected Answer: CE

Yes, Word macros and ransomwawre.

upvoted 1 times

bogd 1 year, 9 months ago

Selected Answer: CE

I would go with CE, as both are things that happen locally on the endpoint. Email phishing (A) is more in the realm of WSA/ESA.

upvoted 3 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

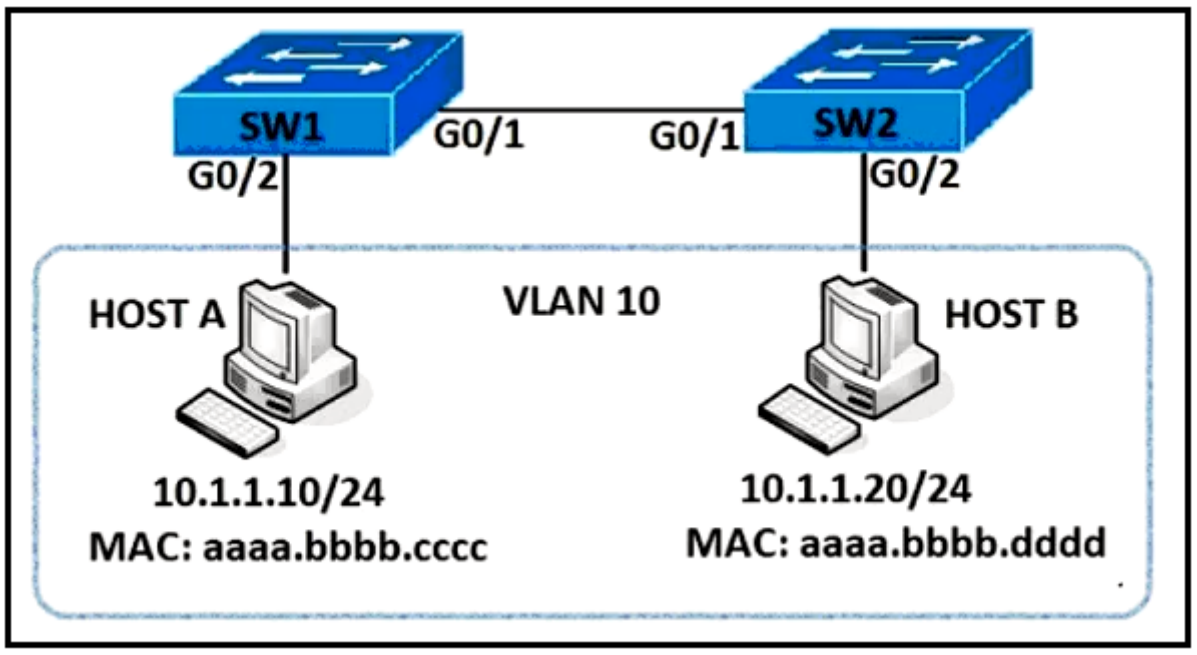
upvoted 1 times

wifishark 2 years, 3 months ago

C and E would be Ok. (macro eq script)
https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html

upvoted 3 times

Question #299 *Topic 1*



Refer to the exhibit. An engineer must deny HTTP traffic from host A to host B while allowing all other communication between the hosts. Drag and drop the commands into the configuration to achieve these results. Some commands may be used more than once. Not all commands are used.

Select and Place:

Answer Area

```
SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# [          ] tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# [          ] ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# [          ]

SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)# [          ]

SW1(config)# vlan filter HOST-A-B vlan 10
```

action drop | action forward | filter | permit | deny | match

Correct Answer:

Answer Area

```
SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# [ permit ] tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# [ permit ] ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# [ action drop ]

SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)# [ action forward ]

SW1(config)# vlan filter HOST-A-B vlan 10
```

action drop | action forward | filter | permit | deny | match

yuiiuy Highly Voted 2 years, 3 months ago

I think the first answer is "Deny".

upvoted 16 times

BigMouthDog 1 year, 4 months ago

it does not make send if the first answer is "Deny". Because you've already denied , you don't need "action drop". However, this is silly because it wastes the processing power

upvoted 2 times

baid 1 year, 8 months ago

Hi, the permit filtrate the traffic 10.1.1.10 to 10.1.1.20, the deny will filtrate other than the traffic 10.1.1.10 to 10.1.1.20. the drop is implemented by vlan access-map, not by access-list. access-list only filtrate the traffic that need be treated by vlan access-map.

upvoted 3 times

Adrenalina73 2 years, 2 months ago

The answer provided is correct, the first answer must permit:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-0SY/configuration/guide/15_0_sy_swcg/vlan_acls.pdf

Router# show ip access-lists net_10Extended IP access list net_10 permit ip 10.0.0.0 0.255.255.255 any
Router(config)# vlan access-map ganymede 10Router(config-access-map)# match ip address net_10Router(config-access-map)# action drop log

upvoted 7 times

Cooldude89 Highly Voted 9 months, 2 weeks ago

Trick question - Given Answer is correct - some options can be used twice
create a condition by permit then later deny by action drop

upvoted 6 times

Brand 9 months, 1 week ago

Make sense...

upvoted 1 times

rafaelinho88 Most Recent 10 months ago

In this case we need to configure a VLAN access-map to deny HTTP traffic and apply it to VLAN 10. To do it, first create an access-list, by which interesting traffic will be matched. The principle of VLAN access-map config is similar to the route-map principle.
After this we'll create a vlan access-map, which has two main parameters: action and match. Match: by this parameter the interesting traffic is matched and here RACL or MAC ACL can be applied as well.
Action: what to do with matched traffic. Two main parameters exist: Drop and Forward. In case of Drop, matched traffic will be dropped, and in case of forward, matched traffic will be allowed

upvoted 1 times

Normanby 1 year ago

The reason the ACLs must Both be 'permit' is that they create the 'test condition' , then based on that test , we drop it later in the Map.

upvoted 5 times

Deu_Inder 1 year, 2 months ago

Provided answer is correct.
permit, permit, action drop, action forward.

upvoted 2 times

ArchBishop 1 year, 10 months ago

When talking about access-lists or prefix-lists associated with *-maps, Permit and Deny take on new meanings.
As we all know, a *-list processes each entry until a match is found.
Once a match is found, processing of the *-list stops.
*-maps operate the same way.

- If the matched statement is 'permit,' the *-list reports back to the *-map with a match success, which allows the *-map to process the associated action. No further *-map sequences are processed.
- If the matched statement is 'deny,' the *-list reports back to the *-map with NO MATCH; wherein the *-map will proceed to the next *-map sequence until a *-map match IS found.
- If NO statement is matched in the *-list, the implicit 'deny any any' is ALWAYS matched. In This case, the *-list will report to the *-map with NO MATCH, and the *-map will proceed to the next sequence until a match IS found.

upvoted 3 times

BigMouthDog 1 year, 10 months ago

The answer provided is correct. Because even the first statement is 'permit' but once it is matched , the action will be dropped

upvoted 2 times

joe_smoe 1 year, 10 months ago

I agree I think the first answer is "Deny". Can someone clarify why this is or isn't true?

upvoted 1 times

dazzler_010 1 year, 8 months ago

If ip access-list extended DENY-HTTP is "Deny", then HTTP traffic will get denied in this ACL and there will be no more matching entry for vlan access-map HOST-A-B 10 to action drop.

upvoted 2 times

GATUNO 2 years, 1 month ago

addrelanina do we have chance to use permit couple times? if is a drop and drag question i see only one permit available

upvoted 1 times

Johnconnor2021 1 year, 12 months ago

The question itself says: "Some commands may be used more than once" Pay attention to the question, read it carefully.

upvoted 3 times

Question #300 *Topic 1*

An engineer must configure the strongest password authentication to locally authenticate on a router. Which configuration must be used?

A. username netadmin secret 5 1b1Ju$kZbBS1Pyh4QzwXyZ1kSZ2

B. username netadmin secret 9 9vFpMf8elb4RVV8$seZ/bDAx1uV

C. username netadmin secret 1b1Ju$k406689705QzwXyZ1kSZ2

D. line Console 0 password 1b1Ju$

Correct Answer: *B*
Reference:
https://learningnetwork.cisco.com/s/article/cisco-routers-password-types

Community vote distribution
B (71%) A (29%)

CKL_SG 5 months, 2 weeks ago

Selected Answer: B

Use Type 6, Type 8 and Type 9 wherever possible.
Type 0, Type 5 and Type 7 should be migrated to other stronger methods.

Type 5
These use a salted MD5 hashing algorithm. These should only be used if Type 6, 8, or 9 is not available on the IOS version you are running. Attempting to use Type 5 in modern IOS XE will throw an error as these will be depreciated soon. In the running config these start with 5.

Type 9
These use the SCRYPT hashing algorithm defined in the informational RFC 7914. SCRYPT uses 80-bit salt, 16384 iterations. It's very memory expensive to run the algorithm and therefore difficult to crack. Running it once occasionally on a Cisco device is fine though, this is currently the Best Practice Type password to use. I have not proven it but I believe it is possible that the popular tool HashCat is able to decrypt these.

In the running config standard Type 9 start with 9.

In the running config convoluted Type 9 start with 14.

https://community.cisco.com/t5/networking-knowledge-base/understanding-the-differences-between-the-cisco-password-secret/ta-p/3163238
upvoted 1 times

Eddyyin 8 months, 1 week ago

Guys, the question is asking for a strongest password for authentication, what if the hash from option A and B are actually generated using a weak password, for example P@ssw0rd?
upvoted 1 times

Alondrix 1 month ago

Type 9, SCRYPT, would still be the best option. The encrypted hash should not be reversible and would be considered ever more difficult to decrypt than any type of encrytion <9.
upvoted 1 times

Asymptote 11 months ago

Selected Answer: B

the main difference between the "secret 9 password" and "algorithm-type scrypt password" commands is the level of security they provide. The "secret 9 password" command uses a less secure proprietary Cisco algorithm, while the "algorithm-type scrypt password" command uses the more secure scrypt PBKDF.
upvoted 1 times

kewokil120 11 months ago

Selected Answer: B

new gear B. Old Gear A
upvoted 2 times

Normanby 1 year ago

Looking too deep - this Q is all about the difference between types , not that actual hashed value :) So therefore = 9 > 5
upvoted 1 times

H3kerman 1 year ago

tested also type 5, the command is valid:
WS-C3850-12XS-S(config)#username netadmin secret 5 1b1Ju$kZbBS1Pyh4QzwXyZ1kSZ2
WARNING: Command has been added to the configuration using a type 5 password. However, type 5 passwords which are considered weak are now deprecated.

WARNING: Auto-converting the entered Type 5 password to Type 9
WS-C3850-12XS-S(config)#do sh run | i netadmin
username netadmin secret 9 14b1Ju$BuhIOqQnewWV5E$QuBZz19ZPY.R8lQwGGGrWe2zWRmB/h0GdTnbaVkNi82

upvoted 2 times

H3kerman 1 year ago

well I'm not sure which is the best answer, maybe to type it without encryption. 9 is the best algorithm to hash the text, but the command is not valid. Tested on real device:
WS-C3850-12XS-S(config)#username netadmin secret 9 9vFpMf8elb4RVV8$seZ/bDAx1uV
ERROR: The secret you entered is not a valid encrypted secret.
To enter an UNENCRYPTED secret, do not specify type 9 encryption.
When you properly enter an UNENCRYPTED secret, it will be encrypted.

upvoted 1 times

shubhambala 1 year, 2 months ago

Selected Answer: B

B bois

upvoted 1 times

redgi0 1 year, 3 months ago

Selected Answer: A

I agree that secret 9 is stronger but the key inserted is too short for that SCRYPT hashed secret.
look at real example :

IOU1(config)#username netadmin secret ?
0 Specifies an UNENCRYPTED secret will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) user secret

IOU1(config)#username netadmin secret 9 9vFpMf8elb4RVV8$seZ/bDAx1uV
ERROR: The secret you entered is not a valid encrypted secret.
To enter an UNENCRYPTED secret, do not specify type 9 encryption.
When you properly enter an UNENCRYPTED secret, it will be encrypted.

upvoted 2 times

redgi0 1 year, 3 months ago

IOU1(config)#username netadmin secret 5 1b1Ju$kZbBS1Pyh4QzwXyZ1kSZ2

IOU1(config)#username netadmin secret 1b1Ju$k406689705QzwXyZ1kSZ2
% Invalid Password length - must contain 1 to 25 characters. Password configuration failed

instead they should have put something like this :
username netadmin secret 9 9nP4LWiOwGSowps$JGbyH6R1Em6K/OBksVrHKaD.RCTYZGXEYIoTO7CQUyk

that would have worked and that would have been the correct answer.

so here the only acceptable solution is A SECRET 5

upvoted 2 times

snowfox 1 year, 3 months ago

LOCAL, LOCAL, LOCAL

upvoted 1 times

babaKazoo 1 year, 4 months ago

Selected Answer: B

8 or 9 is strongest depending on the router, 5 is never the strongest.

upvoted 1 times

danny_f 1 year, 7 months ago

Selected Answer: B

type 9 is the newest available on IOS XE. So new that NIST hasn't approved it yet, they recommend type 8.

upvoted 1 times

hennel 1 year, 7 months ago

Selected Answer: B

Answer B
Unfortunatly type 9 is not available on all (especially older) Cisco platforms, but recommendation is to use it when available.
https://community.cisco.com/t5/networking-documents/understanding-the-differences-between-the-cisco-password-secret/ta-p/3163238

upvoted 2 times

bara_ken 1 year, 7 months ago

Selected Answer: B

This is B

upvoted 1 times

deech 1 year, 7 months ago

Correct Answer: B

upvoted 1 times

fascool 1 year, 7 months ago

Sorry this is wrong, it depends on the router . i tried on another router and it does exist.
0 Specifies an UNENCRYPTED password will follow
5 Specifies that MD5 encrypted password will follow
8 Specifies that SHA-256 encrypted password will follow
9 Specifies that scrypt encrypted password will follow <--
LINE The UNENCRYPTED (cleartext) user password

upvoted 1 times

fascool 1 year, 7 months ago

R1(config)#username netadmin secret 9 34234242424
Invalid encryption type: 9. Password not set. <--

upvoted 1 times

fascool 1 year, 7 months ago

Sorry this is wrong, it depends on the router . i tried on another router and it does exist.
0 Specifies an UNENCRYPTED password will follow
5 Specifies that MD5 encrypted password will follow
8 Specifies that SHA-256 encrypted password will follow
9 Specifies that scrypt encrypted password will follow <--
LINE The UNENCRYPTED (cleartext) user password

upvoted 1 times

fascool 1 year, 7 months ago

Selected Answer: A

R1(config)#enable secret ?
0 Specifies an UNENCRYPTED password will follow
4 Specifies an SHA256 ENCRYPTED secret will follow
5 Specifies an MD5 ENCRYPTED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
level Set exec level password
--- 9 does not exist

upvoted 1 times

Question #301 *Topic 1*

What is a characteristic of MACsec?

A. 802.1AE is built between the host and switch using the MKA protocol, which negotiates encryption keys based on the primary session key from a successful 802.1X session.

B. 802.1AE is negotiated using Cisco AnyConnect NAM and the SAP protocol.

C. 802.1AE is built between the host and switch using the MKA protocol using keys generated via the Diffie-Hellman algorithm (anonymous encryption mode).

D. 802.1AE provides encryption and authentication services.

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/deploy_guide_c17-663760.html

Community vote distribution
A (60%) D (40%)

Jheax Highly Voted 1 year, 8 months ago

Selected Answer: A

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-ofband methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.

upvoted 7 times

Hosein Highly Voted 9 months ago

Selected Answer: D

A is partially correct in describing the use of MKA protocol to negotiate encryption keys, but the key is not necessarily based on the primary session key from a successful 802.1X session

upvoted 6 times

Jasper Most Recent 1 month, 2 weeks ago

A is 100% correct
In summary, 802.1AE (MACsec) focuses on securing data at the link layer by providing encryption for frames on wired Ethernet networks. On the other hand, 802.1X is concerned with controlling access to the network by authenticating and authorizing devices attempting to connect to it. While they serve different purposes, they can be complementary, with 802.1X handling access control and authentication and 802.1AE providing an additional layer of security by encrypting data at the link layer.

upvoted 1 times

[Removed] 3 months, 1 week ago

Selected Answer: D

Media Access Control Security (MACsec) is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices.
https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000/swmacsec.pdf

upvoted 1 times

djedeen 5 months ago

Selected Answer: A

Per text Jheax and following link:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/en/us/td/docs/switches/lan/catalyst4500/XE3-8-0E/15-24E/configuration/guide/xe-380-configuration/swmacsec.html.xml

upvoted 1 times

HarwinderSekhon 5 months ago

Selected Answer: A

MacSec offers no authentication. 802.1X does.
A is the answer.

upvoted 3 times

[Removed] 5 months, 2 weeks ago

Selected Answer: A

Man, this is another one of those, both A and B are correct in my opinion based on the information here https://tinyurl.com/MACsec-topic, but it feels like A is the better answer.

upvoted 1 times

Cesar12345 5 months, 3 weeks ago

Selected Answer: D

According to the link https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf

upvoted 1 times

Question #302 *Topic 1*

Refer to the exhibit. A network engineer attempts to connect to the Router1 console port.
Which configuration is needed to allow Telnet connections?

A. Router1(config)# line vty 0 15 Router1(config-line)# transport output telnet

B. Router1(config)# telnet client

C. Router1(config)# line console 0 Router1(config-line)# transport output telnet

D. Router1(config)# access-list 100 permit tcp any any eq telnet Router1(config)# line console 0 Router1(config-line)# access-class 100 out

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/iosxe/qualified-cli-command-reference-guide/m-line-commands.pdf

Community vote distribution
C (56%) A (44%)

timtgh Highly Voted 1 year, 6 months ago
The question shouldn't say the engineer "attempts" to connect to the Router1 console port. Clearly they are already logged in to the console port and attempting to Telnet out.
upvoted 10 times

dansecu 2 months, 3 weeks ago
yes, and transport is only for vty. correct answer is A
upvoted 1 times

MPERERWE256 5 months, 3 weeks ago
True 💯
upvoted 1 times

mgiuseppe86 Most Recent 2 months, 3 weeks ago
It CANT BE A!!! A implies the user is connected to the router via a line (ssh or telnet already!) The question states the engineer is on the console. and needs to make outbound telnet connections from his console connection... C answers this delimma
upvoted 1 times

djedeen 3 months, 1 week ago
Selected Answer: C
C: Telneting out from console
upvoted 1 times

ajeetnagdev 5 months ago
Answer is C.
Router1(config)# line console 0 Router1(config-line)# transport output telnet
Why - user console in Router1(config)# line console 0 then setup VTY by running following command
Router1(config-line)# transport output telnet
upvoted 1 times

adrian0792 5 months, 1 week ago
C is the correct answer
upvoted 1 times

marjana_mirza 7 months, 2 weeks ago
Correct answer : C
---
explanation:
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line con 0
Router(config-line)#transport output none
Router(config-line)#end
*Apr 19 17:33:16.198: %SYS-5-CONFIG_I: Configured from console by console
Router#disable
Router>telnet 10.0.0.2
% telnet connections not permitted from this terminal
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#line console 0
Router(config-line)#transport output telnet
Router(config-line)#exit
Router(config)#end
Router#
*Apr 19 17:34:06.111: %SYS-5-CONFIG_I: Configured from console by console
Router#disable
Router>telnet 10.0.0.2
Trying 10.0.0.2 ...
% Connection refused by remote host

Router>

upvoted 1 times

XDR 7 months, 3 weeks ago

To answer this question we need the missing exhibit.

upvoted 3 times

rami_mma 8 months, 1 week ago

Selected Answer: A

"allow Telnet connections"

upvoted 2 times

echipbk 10 months, 3 weeks ago

Selected Answer: C

I think C is the correct answer

upvoted 1 times

markymark874 10 months, 4 weeks ago

A is the closest answer.. could be just an error on the output word. maybe it should be input

upvoted 1 times

kewokil120 11 months ago

Selected Answer: A

with out context of the problem. Im going to assume they connected via console because the device as unreachable via mgmt protocol. said person enabled telnet on the vty to enable remote access.

upvoted 1 times

nushadu 11 months, 2 weeks ago

not clear what we need to achieve,
OUTBOUND telnet connection are allowed by default from CONSOLE port as well from VTY:

cisco_R5#show line console 0 | include input|output
Allowed input transports are none.
Allowed output transports are lat pad telnet rlogin lapb-ta mop v120 ssh.

cisco_R5#
cisco_R5#show line vty 0 | include input|output
Allowed input transports are none.
Allowed output transports are lat pad telnet rlogin lapb-ta mop v120 ssh.

cisco_R5#show runn | section line
line con 0
exec-timeout 60 0
logging synchronous
line aux 0
line vty 0 4
login
transport input none

cisco_R5(config)#line vty 0 4
cisco_R5(config-line)#transport input telnet
cisco_R5(config-line)#
cisco_R5(config-line)#do show line vty 0 | include input|output
Allowed input transports are telnet.
Allowed output transports are lat pad telnet rlogin lapb-ta mop v120 ssh.
No output characters are padded
cisco_R5(config-line)#^Z
cisco_R5#

upvoted 1 times

nopenotme123 1 year, 3 months ago

Selected Answer: C

Question is worded horribly but C is the answer that makes sense in this situation.

upvoted 3 times

Tannhaus 1 year, 5 months ago

Selected Answer: C

It must be C.
User connects via console, so it cannot be A, because A allows to use telnet out when connected via vty.

upvoted 3 times

rlilewis 1 year, 6 months ago

Selected Answer: A

Question is unclear if they want telnet to come in or go out. Console doesn't send or receive any telnet so those answers are invalid. I'm guessing A assuming they meant outbound telnet.

upvoted 4 times

bendarkel 9 months, 1 week ago

Console and VTY connections are not the same. The question states console connection.

upvoted 1 times

danny_f 1 year, 7 months ago

Is the wording this bad on the test too?

upvoted 3 times

roncr 1 year, 7 months ago

options A/C should say "transport input telnet" to be valid
The access list on D is applied outbound so it wont catch the connection
C is a joke

upvoted 2 times

nopenotme123 1 year, 3 months ago

Why would you include transport input anything on the console port? Transport output telnet works on the console port fine. Console in and telnet out.

upvoted 2 times

Refer to the exhibit.

```
username admin privilege 15 password 0 Cisco13579!
aaa new-model
!
aaa authentication login default local
aaa authentication enable default none
!
aaa common-criteria policy Administrators
  min-length 1
  max-length 127
  char-changes 4
  lifetime month 2
!
```

A network engineer must configure a password expiry mechanism on the gateway router for all local passwords to expire after 60 days. What is required to complete this task?

A. Add the username admin privilege 15 common-criteria-policy Administrators password 0 Cisco13579! command.

B. The password expiry mechanism is on the AAA server and must be configured there.

C. Add the aaa authentication enable default Administrators command.

D. No further action is required. The configuration is complete.

Correct Answer: *A*

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-e/sec-usr-aaa-15-e-book/sec-aaa-comm-criteria-pwd.pdf

Community vote distribution

A (100%)

Marving Highly Voted 1 year, 10 months ago

Th policy is created but not applied and needs to be applied using the following:
username username common-criteria-policy policy-name password password
so provided answer is correct.

upvoted 8 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: A

Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa common-criteria policy policy1
Device(config-cc-policy)# char-changes 4
Device(config-cc-policy)# max-length 20
Device(config-cc-policy)# min-length 6
Device(config-cc-policy)# numeric-count 2
Device(config-cc-policy)# special-case 2
Device(config-cc-policy)# exit
Device(config)# username user1 common-criteria-policy policy1 password password1
Device(config)# end

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xe-16-10/sec-usr-aaa-xe-16-10-book/sec-aaa-comm-criteria-pwd.html

upvoted 3 times

Refer to the exhibit.

```
R1# sh run | begin line con
line con o
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux o
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 045802150C2E
  login
line vty 5 15
  password 7 045802150C2E
  login
!
end
```

```
R1# sh run | include aaa | enable
no aaa new-model
R1#
```

Which privilege level is assigned to VTY users?

A. 1

B. 7

C. 13

D. 15

Correct Answer: *A*

Community vote distribution

A (75%) D (25%)

edg Highly Voted 3 years, 3 months ago

The answer is letter "A": 1.
https://www.oreilly.com/library/view/hardening-cisco-routers/0596001665/ch04.html
"Default Privilege Levels
The bottom and least privileged level is level 0. This is the only other level besides 1 and 15 that is configured by default on Cisco routers. Next is level 1, the default user level. This level provides the user with many more commands that allow the user to display router information, telnet to other systems, and test network connectivity with ping and traceroute. Level 2, which is not enabled by default, adds a few additional show and clear commands, but provides no opportunity for a user to reconfigure the router. Finally, level 15 allows full access to all router commands."

upvoted 11 times

error_909 Highly Voted 2 years, 2 months ago

if we assume that the enable password is set, then the vty will have the privilege of 15.
If enable password is not set, then the vty privilege level will be 1.

I would assume that is there is no enable password exist since its not shown.
I would choose A

upvoted 9 times

ibogovic Most Recent 4 months, 4 weeks ago

Selected Answer: D

D. 15

In the given configuration, the "line vty 0 4" and "line vty 5 15" commands are used to configure the virtual terminal lines (VTY) for remote access. The "login" command is enabled under both VTY lines, which means that authentication is required for VTY access.

Since the privilege level is not explicitly specified under the VTY lines, it defaults to the highest privilege level, which is 15. Therefore, VTY users will have privilege level 15 when accessing the router.

upvoted 1 times

Toob93 2 months, 3 weeks ago

i think you studying the wrong CCNP. The default is 1 and NOT 15.

upvoted 1 times

mgiuseppe86 2 months, 3 weeks ago

this comment made me laugh out loud

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

sw1#
sw1#telnet 192.168.255.55
Trying 192.168.255.55 ... Open

User Access Verification

Password:
cisco_R5>show privilege
Current privilege level is 1 <<<<<<<<<<<<<<<<<<<<<<<<
cisco_R5>
cisco_R5>ena
Password:
cisco_R5#sh runn | i aaa
no aaa new-model

cisco_R5#sh runn | s line
line con 0
exec-timeout 60 0
logging synchronous
line aux 0
line vty 0 4
password 777
login
transport input telnet

cisco_R5#
cisco_R5#show users
Line User Host(s) Idle Location
0 con 0 idle 00:01:21
* 2 vty 0 idle 00:00:00 192.168.255.2

Interface User Mode Idle Peer Address

cisco_R5#

upvoted 1 times

nushadu 11 months, 2 weeks ago

enable mode == 15
cisco_R5#show privilege
Current privilege level is 15
cisco_R5#

upvoted 1 times

tckoon 1 year, 2 months ago

Selected Answer: A

show run all , will reveal the default privilege of the con & vty

line con 0
exec-timeout 10 0
timeout login response 30
privilege level 1
line vty 0 4
exec-timeout 10 0
timeout login response 30
privilege level 1
flush-at-activation

upvoted 2 times

sOI852POL 2 years, 3 months ago

Given answer is correct, Lines (CON, AUX, VTY) default to level 1 privileges

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct
The vty user will have privi 1. Enable command required to elevate to privi 15.

upvoted 2 times

whiteherondance 2 years, 6 months ago

I think the answer is A - 1. Some people are arguing that it is D -15 because you require level 15 for privilege to perform the 'show run' command, but that argument assumes that the output was generated from a vty connection. If you look at the config for console and aux, they have priv 15 set, meaning we can probably assume the show run command was executed from the con or aux lines, and not the vty line (because it has the default privilege of 1). For this reason, I think it's A.

upvoted 1 times

MarkJames 2 years, 8 months ago

the answer is 15, not 1. # is level 15 and > level one. You cant run show commands in user exc mode.

upvoted 2 times

masterminion 2 years, 8 months ago

How do you know that the connection was made through the VTY line to execute the command and not the Console line

upvoted 5 times

renegade_xt 2 years, 9 months ago

its 15, you cant do "sh run" in level 1 :)
plus the sign is "#" not ">"

https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels

upvoted 1 times

renegade_xt 2 years, 9 months ago

Cancel that, Lines (CON, AUX, VTY) default to level 1 privileges.

https://www.oreilly.com/library/view/hardening-cisco-routers/0596001665/ch04.html

upvoted 3 times

anonymous1966 2 years, 10 months ago

Book: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide
Page: 761
Privilege level 1: Also known as User EXEC mode. The command prompt in this mode includes a greater-than sign (R1>). From this mode it is not possible to make configuration changes; in other words, the command configure terminal is not available.

upvoted 1 times

jarz 3 years ago

I agree with A being the correct answer.

upvoted 1 times

Thelma05 3 years, 1 month ago

Answer is Level 15 privilege mode, Level 1 is an executive mode

upvoted 1 times

timtgh 1 year, 6 months ago

All of the levels are referred to as privilege levels, even though Level 15 has nicknames ("enabled mode" and "privileged mode").

upvoted 1 times

XalaGyan 3 years, 2 months ago

http://resources.intenseschool.com/ccna-security-solutions-to-facs-enable-secret-and-privilege-levels/

upvoted 2 times

Question #305 *Topic 1*

Which statements are used for error handling in Python?

A. try/catch

B. catch/release

C. block/rescue

D. try/except

Correct Answer: *D*

Community vote distribution

D (100%)

J_C_STUDY Highly Voted 3 years, 3 months ago

Reference:
https://docs.python.org/3/tutorial/errors.html
"D"

upvoted 8 times

eww_cybr Most Recent 4 months, 3 weeks ago

Selected Answer: D

OCG CCNA Devnet

What if you wanted Python to tell the users what they did wrong and let them try again or perform some other task to recover from the error? That's where the try-except-else-finally code blocks come into play.

upvoted 2 times

charafDZ 9 months, 1 week ago

"D"
https://www.w3schools.com/python/python_try_except.asp

upvoted 2 times

miccamilla 1 year, 6 months ago

Selected Answer: D

tested in IDLE

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 2 times

Question #306 *Topic 1*

How do agent-based versus agentless configuration management tools compare?

A. Agentless tools use proxy nodes to interface with slave nodes.

B. Agentless tools require no messaging systems between master and slaves.

C. Agent-based tools do not require a high-level language interpreter such as Python or Ruby on slave nodes.

D. Agent-based tools do not require installation of additional software packages on the slave nodes.

Correct Answer: *B*

Community vote distribution

B (100%)

Audi87 Highly Voted 2 years, 8 months ago

I believe the answer is C

upvoted 18 times

Audi87 2 years, 8 months ago

Agentless tool means that no software or agent needs to be installed on the client machines that are to be managed. Ansible is such an agentless tool. In contrast to agentless tool, agent-based tool requires software or agent to be installed on the client. Therefore the master and slave nodes can communicate directly without the need of high-level language interpreter.
An agentless tool uses standard protocols, such as SSH, to push configurations down to a device (and it can be considered a “messaging system”).

upvoted 12 times

Feliphus 11 months, 4 weeks ago

Why is SSH a type of "messaging system" ? I can not sense on that afirmation, the classical messaging system are: IMAP, POP, SMTP. Answer B seems to be OK

upvoted 1 times

Carl1999 2 years ago

"C. Agent-based tools ..." so it needs agent.

upvoted 1 times

djedeen Most Recent 5 months ago

Selected Answer: B

From cisco ENCOR prep book :
There are two core types of configuration management tools, and there is also a third type that is usually a derivation of an agent-based tool:

▪ Agent-based configuration: With agent-based tools, an agent must be installed on every device that the configuration management tool will manage.

▪ Agentless configuration: Agentless tools do not require that an agent be installed on every device; instead, they communicate via SSH or another API that a device supports.

▪ Proxy-agent configuration: This type of configuration does not require an agent on every device, but it does require some type of “process” or “worker” to communicate with the master server and the remote device.

upvoted 1 times

StefanOT2 10 months, 3 weeks ago

Selected Answer: B

B is the only answer which is obviously not wrong. The commands of agent based software is often queued and sent via "messages" like in SaltStack. While Agentless software relies on standard connections and commands e. g. via SSH.

upvoted 1 times

Radwa_ 1 year, 1 month ago

Selected Answer: B

B is correct.
reference: https://www.youtube.com/watch?v=_TVNCTK808I&ab_channel=Simplilearn

upvoted 1 times

BigMouthDog 1 year, 4 months ago

An agentless tool uses standard protocols, such as SSH, to push configurations down to a device (and it can be considered a “messaging system”).
If this is the case, then what does it mean for answer 'B"

upvoted 1 times

BigMouthDog 1 year, 4 months ago

C is wrong because agent based tools such as Chef uses Ruby for device configuration. D is also wrong because agent based tools require an agent being installed on the network device.

upvoted 1 times

Tyrandemer 1 year, 4 months ago

A. (Incorrect) Agentless tools such as Ansible do need SSH (messaging system) between master and slave otherwise how will they communicate.
B. (Incorrect) only agent-based tools use proxy agents on the clients.
C (Correct) Agent-based tools such as Chef, Puppet, SaltStack require instillation of special software (agent) on the client nodes. The server node then talks with the agent directly and there is no need of a high-level language interpreter such as Python or Ruby on slave nodes.
D. (Incorrect) Agent-based tools such as Chef, Puppet, SaltStack do require installation of additional software packages (agents) on the slave nodes.

upvoted 2 times

StefanOT2 10 months, 3 weeks ago

not true when the agent is written in Python or Ruby. SaltStack is Python based e. g.

upvoted 1 times

tltechcert 1 year, 6 months ago

Selected Answer: B

Audi87's explanation is reversed; he is explaining an Agentless tool not requiring but "C" is saying Agent-based tools do not require when they DO require a high-level language interpreter. "B" is the only answer that makes sense as Ansible and Puppet DO use slave nodes as proxies to interface via SSH.

upvoted 1 times

tatrman 2 years, 8 months ago

A==false, because agent-less tools (ansible, salt-ssh or bolt) use plain ssh. Could be tunelled through gw, but that's probably not what they mean by proxying.
What's left is B.

upvoted 4 times

tatrman 2 years, 8 months ago

C or D false, because all agent using tools as Chef, Puppet and Salt are using either python or ruby based agents.

upvoted 2 times

ABC123 2 years, 8 months ago

Agree with Audi87

upvoted 2 times

Refer to the exhibit.

PYTHON CODE:

```
import requests
import json

url='http://YOURIP/ins'
switchuser='USERID'
switchpassword='PASSWORD'

myheaders={'content-type':'application/json'}
payload={
 "ins_api":{
  "version": "1.0",
  "type": "cli_show",
  "chunk": "0",
  "sid": "1"
  "input": "show version",
  "output_format": "json"
 }
}

response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword)).json()

print(response['ins_api']['outputs']['output']['body']['kickstart_ver_str'])
```

HTTP JSON Response:

```
{
 "ins_api":{
 "type": "cli_show",
 "version": "1.0",
 "sid": "eoc",
 "outputs": {
  "output": {
    "input": "show version",
     "msg": "Success",
     "code": "200",
     "body": {
       "bios_ver_str", "07.61",
       "kickstart_ver_str": "7.0(3)|7(4)",
       "bios_cmpl_time": "04/06/2017",
       "kick_file_name":  "bootflash:///nxos.7.0.3.|7.4.bin",
       "kick_cmpl_time", "6/14/1970 2:00:00",
       "kick_tmstmp": "06/14/1970 09:49:04",
       "chassis_id": "Nexus9000 93180YC-EX chassis",
       "cpu_name": "Intel(R) Xeon(R) CPU @ 1.80GHz",
       "memory": 24633488,
       "mem_type": "kB",
       "rr_usecs": 134703,
       "rr_crime": "Sun Mar 10 15:41:46 2019",
       "rr_reason": "Reset Requested by CLI command reload",
       "rr_sys_ver": "7.0(3)|7(4)",
       "rr_service": "",
       "manufacturer": "Cisco Systems, Inc.",
       "TABLE_package_list": {
        "ROW_package_list": {
         "package_id": {}
        }
       }
      }
     }
    }
   }
}
```

Which HTTP JSON response does the Python code output give?

A. 7.0(3)|7(4)

B. 7.61

C. NameError: name 'json' is not defined

D. KeyError: 'kickstart_ver_str'

Correct Answer: *A*

Community vote distribution

A (100%)

tafisto Highly Voted 6 months, 2 weeks ago

how do i get to understand this

upvoted 5 times

Arodoeth 3 months, 2 weeks ago

You can interpret like this: What was the response in the JSON format to the request 'show version' made in the python script? The answer is the version of the kickstart image running on the Nexus9k switch.

upvoted 1 times

pmmg Most Recent 8 months, 2 weeks ago

Selected Answer: A

The last line says to print, and points to kickstart_ver_str.
kickstart_ver_str is 7.0(3)7(4)

upvoted 4 times

Badger_27 8 months, 2 weeks ago

Is this just a case of matching an answer to the body of response.json?

upvoted 2 times

echipbk 10 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 4 times

Dave513 3 years, 1 month ago

Many of API calls will return a JSON object containing another resource's SID. Then the SID the right answer is A.

upvoted 4 times

jzjs 3 years, 3 months ago

sid is defferent
may be D is true

upvoted 1 times

yhee 3 years, 6 months ago

comment

upvoted 1 times

Question #308 *Topic 1*

A network administrator is preparing a Python script to configure a Cisco IOS XE-based device on the network. The administrator is worried that colleagues will make changes to the device while the script is running.
Which operation of the ncclient manager prevents colleagues from making changes to the devices while the script is running?

A. m.lock(config='running')

B. m.lock(target='running')

C. m.freeze(target='running')

D. m.freeze(config='running')

Correct Answer: *B*

ihateciscoreally 3 months, 1 week ago

thank you for covering this in OCG!

upvoted 2 times

examShark 2 years, 6 months ago

The given response is correct

upvoted 2 times

wqoiqw 2 years, 11 months ago

If the clear configuration lock command is specified while a NETCONF global lock is being held, a full synchronization of the configuration is scheduled and a warning syslog message is produced. This command clears only the parser configuration lock.

The following is a sample RPC that shows the <lock> operation:

```
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<lock>
<target>
<running/>
</target>
</lock>
</rpc>
```

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1610/b_1610_programmability_cg/configuring_yang_datamodel.html#ariaid-title6

upvoted 1 times

Question #309 *Topic 1*

Which outcome is achieved with this Python code?
client.connect (ip, port= 22, username= usr, password= pswd) stdin, stdout, stderr = client.exec_command ('show ip bgp 192.168.101.0 bestpath\n ') print (stdout)

A. connects to a Cisco device using SSH and exports the BGP table for the prefix

B. displays the output of the show command in a formatted way

C. connects to a Cisco device using SSH and exports the routing table information

D. connects to a Cisco device using Telnet and exports the routing table information

Correct Answer: *A*

Community vote distribution

A (100%)

nushadu 11 months, 2 weeks ago

Selected Answer: A

cisco_R5#show ip bgp 2.2.2.2 bestpath
BGP routing table entry for 2.2.2.2/32, version 158
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
3 2, (received & used)
192.168.255.22 from 192.168.255.3 (3.3.3.3)
Origin incomplete, localpref 100, valid, external, best
rx pathid: 0, tx pathid: 0x0
cisco_R5#

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 4 times

Question #310 *Topic 1*

Refer to the exhibit. Which JSON syntax is derived from this data?

A. {[{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}]}

B. {'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Reading'}]}

C. {[{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Hobbies': 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Reading'}]}

D. {'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}]}

Correct Answer: *D*

Community vote distribution

D (80%) A (20%)

Hamzaaa Highly Voted 2 years, 7 months ago

please verify, D is the correct answer, the root is person, then hobbies must open a sub vector

upvoted 8 times

Broekie Highly Voted 2 years, 5 months ago

Answer D
I verified the code on the site https://jsonlint.com
Before testing please put every string between quotation mark.
for example: "Person" : so on

upvoted 7 times

rami_mma Most Recent 8 months, 1 week ago

Selected Answer: A

I think they add one extra bracket at the beginning and another bracket at the end, if they remove them the answer should would be A.

upvoted 1 times

echipbk 10 months, 3 weeks ago

Selected Answer: D

D is the correct answer

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: D

Generally speaking, yes, "D" is a working python dictionary but why Cisco wants students study programming?

```
# python3
data = {'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies':
['Running', 'Video games']},
{'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}]}

for key, value in data.items():
for n, i in enumerate(value, 1):
print(f'{key}#{n}')
for x, y in i.items():
print(f'{x} is {y}')
print()
```

upvoted 3 times

nushadu 11 months, 2 weeks ago

output
Person#1
First Name is Johnny
Last Name is Table
Hobbies is ['Running', 'Video games']

Person#2
First Name is Billy
Last Name is Smith
Hobbies is ['Napping', 'Reading']

upvoted 1 times

KZM 1 year ago

D is correct
We can also check JSON code in
https://jsonformatter.curiousconcept.com/#

upvoted 3 times

Violator 1 year, 9 months ago

This question is still asked. Passed today.

upvoted 3 times

xziomal9 2 years, 2 months ago

The correct answer is:
D.

{
'Person':
[
{
'First Name': 'Johnny',
'Last Name': 'Table',
'Hobbies': ['Running', 'Video games']
},

{
'First Name': 'Billy',
'Last Name': 'Smith',
'Hobbies': ['Napping', 'Reading']
}
]
}

upvoted 4 times

xziomal9 2 years ago

{"Person":[{"First Name":"Johnny","Last Name":"Table","Hobbies":["Running","Video games"]},{"First Name":"Billy","Last Name":"Smith","Hobbies":["Napping","Reading"]}]}

upvoted 2 times

error_909 2 years, 2 months ago

Correct Answer:

{
"Persion": [{
"Firstname": "Johnny",
"Lastname": "Table",
"Hobbies": ["Running", "Video Games"]
},

{
"Firstname": "Billy",
"Lastname": "Smith",
"Hobbies": ["Napping", "Reading"]
}
]
}

upvoted 2 times

Masashi_O 2 years, 6 months ago

A. {[{First Name: Johnny, Last Name: Table, Hobbies: [Running, Video games]}, {First Name: Billy, Last Name: Smith, Hobbies: [Napping, Reading]}]}
B. {Person: [{First Name: Johnny, Last Name: Table, Hobbies: Running, Video games}, {First Name: Billy, Last Name: Smith, Hobbies: Napping, Reading}]}
C. {[{First Name: Johnny, Last Name: Table, Hobbies: Running, Hobbies: Video games}, {First Name: Billy, Last Name: Smith, Hobbies: Napping, Reading}]}
D. {Person: [{First Name: Johnny, Last Name: Table, Hobbies: [Running, Video games]}, {First Name: Billy, Last Name: Smith, Hobbies: [Napping, Reading]}]}

upvoted 4 times

ABC123 2 years, 4 months ago

When we paste each of those 4 scripts in https://jsonlint.com they all have scripting errors! :-)

upvoted 1 times

Jared28 1 year, 5 months ago

Replace the single quotes with double quotes.

upvoted 1 times

Question #311 *Topic 1*

Which data is properly formatted with JSON?

A.

```
{
        "name":"Peter"
        "age":"25"
        "likesJson":true
        "characteristics":["small","strong",18]
}
```

B.

```
{
        "name": "Peter",
        "age": "25",
        "likesJson": true,
        "characteristics": ["small","strong",18]
}
```

C.

```
{
        "name": Peter,
        "age": 25,
        "likesJson": true,
        "characteristics": ["small","strong","18"],
}
```

D.

```
{
        "name": "Peter",
        "age": "25",
        "likesJson": true,
        "characteristics": ["small","strong","18"],
}
```

Correct Answer: *B*

netpeer Highly Voted 2 years, 7 months ago

B is correct as all must end with comma except the last statement before }

upvoted 27 times

nushadu 12 months ago

A - syntax error - no commas at the end of the lines
C - syntax error - "name" value Peter must be a type string (in quotas -> "Peter")

upvoted 2 times

RhJ72 2 years, 3 months ago

netpeer is correct. The question asks for correct json formatting. B is the only answer that has correct json formatting. The question around integer is irrelevant. If you put 25, it's an integer, if you put "25", it's a string. from a formatting perspective, both are correct.

upvoted 4 times

eddgg Most Recent 3 months, 3 weeks ago

b is the right option

upvoted 1 times

[Removed] 4 months, 3 weeks ago

B is correct, there is no need for a comma at end of the last statement

upvoted 2 times

kewokil120 11 months ago

B is correct

upvoted 2 times

John13121 11 months, 1 week ago

B is valid, verified with JsonValidator...

upvoted 1 times

nushadu 12 months ago

technically B & D are both correct, I mean Python syntax will not raise any errors ...

upvoted 2 times

nushadu 12 months ago

A - syntax error - no commas at the end of the lines
C - syntax error - "name" value Peter must be a type string (in quotas -> "Peter")

upvoted 1 times

Rockford 2 years, 6 months ago

B is correct, checked in JSONLint validator numbers 18 and 25 can be in "" or not still valid.

upvoted 3 times

hsitar 2 years, 8 months ago

Correct answer should be D

upvoted 1 times

Feliphus 11 months, 4 weeks ago

No, because it has a final unneeded comma

upvoted 1 times

jas26says 2 years, 7 months ago

the comma at the end makes the answer wrong.

upvoted 1 times

Adeleke 2 years, 7 months ago

should the age 25 be in quotation???

upvoted 2 times

lukaszr 2 years, 4 months ago

in quotation 25 is string, without 25 is integer.

upvoted 1 times

Based on the output below, which Python code shows the value of the "upTime" key?


```
{
"response" [{
"family": "Routers",
"type": "Cisco ASR 1001-X Router",
"errorCode": null,
"location": null,
"macAddress": "00:c8:8b:80:bb:00",
"hostname": "asr1001-x.abc.inc",
"role": "BORDER ROUTER",
"lastUpdateTime": 1577391368518,
"serialNumber": "FXS1932Q1SE",
"softwareeVersion": "16.3.2",
"locationName": null,
"upTime": "49 days, 13:43:44:13",
"lastUpdated": "2019-12-22 14:55:23"
}]
}
```


A. json_data = response.json() print(json_data['response'][0]['upTime'])

B. json_data = response.json() print(json_data[response][0][upTime])

C. json_data = json.loads(response.text) print(json_data['response']['family'][upTime'])

D. json_data = response.json() print(json_data['response'][family][upTime'])

Correct Answer: *C*

Community vote distribution

A (88%) 13%

hsjfjbdlw Highly Voted 2 years, 6 months ago

The correct answer is A. The dictionary attributes are strings, so they would need to be addressed with quotations. B implies that variables are being specified as the attribute identifiers.

upvoted 24 times

jas26says Highly Voted 2 years, 7 months ago

The right answer is B.

upvoted 8 times

lukaszr 2 years, 4 months ago

It is not.
instead of print(json_data[response][0][upTime])
should be print(json_data["response"][0]["upTime"])

upvoted 10 times

wifishark 2 years, 3 months ago

A is the right answer

upvoted 8 times

mp777 Most Recent 4 months, 2 weeks ago

there is no 'family' dictionary inherited. so 'family' options go away.
upTime needs to be type string so 'upTime', as there is no other variable upTime.
A is correct.

upvoted 1 times

HarwinderSekhon 6 months ago

Nobody in real life check it with eyes, we all use json formatting tools. Cisco is old school like we are living in old century. Instead ask, how can you format json or what tools can you use.

upvoted 5 times

wr4net 6 months, 2 weeks ago

json is data is typically key:value pairs fo data in a rigid hierarchy, like a tree.
key elements at the same level are separated by commas.
family and uptime are clear at the same level in the tree.
therefore to print uptime, you do not need to reference another same leverl key, such as family.
this take out c and d.
of a & b, all keys are referenced inside of quotes. so Uptime in quotes takes care of that.

As a side note, if uptime were a subtree item falling under family, it would have more brackets in the data element,
and in that case the c/d chaining of subtree elements would make senses. but not here.

upvoted 1 times

Chiaretta 7 months, 1 week ago

Selected Answer: A

A is the right answer

upvoted 2 times

MMaris018 7 months, 3 weeks ago

Selected Answer: C

json.loads() is used to convert JSON into python

upvoted 2 times

juancarlosdlar 10 months, 3 weeks ago

json.loads() method can be used to parse a valid JSON string and convert it into a Python Dictionary.

upvoted 2 times

kewokil120 11 months ago

The correct answer is A

upvoted 1 times

MO_2022 11 months, 3 weeks ago

Selected Answer: A

Note: We need to call the first element "[0]" in "json_data['response'][0]['upTime'])" command because "response" is an array with only one element

upvoted 6 times

[Removed] 5 months, 2 weeks ago

Thank you

upvoted 1 times

nushadu 12 months ago

```
# python code
test_dict = {'val1': [{1: 11, 2: 22, 3: 33}]}
print(test_dict['val1'][0][3])
# result
33
```

upvoted 2 times

Wooker 1 year, 2 months ago

Selected Answer: A

The correct answer is A

upvoted 3 times

BigMouthDog 1 year, 4 months ago

inside the array , i.e. [ ], there is only one item { }, therefore respond refers to [0]

upvoted 1 times

BigMouthDog 1 year, 4 months ago

The answer is 'A', because the question is asked about 'UpTime', not 'family', both of them are object within array 'response' ,i.e. [{"family:xxx", "UpTime:xxx"}...

upvoted 2 times

ougty 1 year, 7 months ago

Selected Answer: A

It should be A

upvoted 1 times

aohashi 1 year, 9 months ago

Selected Answer: A

It should be A

upvoted 1 times

bogd 1 year, 9 months ago

Selected Answer: A

json_data["response"] is an array, and should be numerically indexed ([0]).

upvoted 1 times

Which exhibit displays a valid JSON file?

A.

```
{
    "hostname": "edge_router_1"
    "interfaces": {
         "GigabitEthernet1/1"
         "GigabitEthernet1/2"
         "GigabitEthernet1/3"
    }
}
```

B.

```
{
    "hostname": "edge_router_1",
    "interfaces": {
         "GigabitEthernet1/1",
         "GigabitEthernet1/2",
         "GigabitEthernet1/3",
    },
}
```

C.

```
{
    "hostname": "edge_router_1"
    "interfaces": [
         "GigabitEthernet1/1"
         "GigabitEthernet1/2"
         "GigabitEthernet1/3"
    ]
}
```

D.

```
{
    "hostname": "edge_router_1",
    "interfaces": [
         "GigabitEthernet1/1",
         "GigabitEthernet1/2",
         "GigabitEthernet1/3"
    ]
}
```

Correct Answer: *D*

Saqib79 Highly Voted 3 years, 6 months ago

Correct Option is D.

upvoted 63 times

edlaffer Highly Voted 3 years, 6 months ago

agree on D , validate on JSONlint

upvoted 20 times

[Removed] Most Recent 4 months, 3 weeks ago

D is correct

upvoted 1 times

rabbit2 6 months, 1 week ago

D is the correct option

upvoted 1 times

Dataset 11 months ago

D is the valid answer
Regards

upvoted 1 times

nushadu 12 months ago

here is the problem with commas in the end,
D is 100% correct
but B also will not raise syntax errors but need to test it anyway ...

upvoted 1 times

KZM 1 year, 1 month ago

Data is represented in name/value pairs.
Curly braces hold objects and each name is followed by ':'(colon), the name/value pairs are separated by , (comma).
Square brackets hold arrays and values are separated by ,(comma).

upvoted 1 times

M_Abdulkarim 1 year, 4 months ago

Answer is D, In B interfaces is an object so it should contain pairs of key and value!

upvoted 1 times

ougty 1 year, 4 months ago

Correct answer is D

upvoted 1 times

BigMouthDog 1 year, 4 months ago

B is wrong , JSON syntax does not have 'comma' after the last object. Answer is 'D'

upvoted 1 times

Saamson 1 year, 5 months ago

Highest Voted Answer is D

upvoted 1 times

winder 1 year, 5 months ago

how can you get this wrong.....

upvoted 1 times

ougty 1 year, 7 months ago

D it can only be D

upvoted 3 times

youme 1 year, 9 months ago

{
"name":"John",
"age":30,
"cars":["Ford", "BMW", "Fiat"]
}
Correct option is D

upvoted 3 times

sharon90 1 year, 12 months ago

i wonder why the admins ignore us. Can you please edit the answer? D is the proper one

upvoted 4 times

Nhan 2 years, 2 months ago

DDDDDD LOL

upvoted 2 times

xziomal9 2 years, 2 months ago

The correct answer is:
D.

upvoted 2 times

Refer to the exhibit.

Name is Bob Johnson
Age is 75
Is alive

Favorite foods are:
• Cereal
• Mustard
• Onions

What is the JSON syntax that is formed from the data?

A. {Name: Bob Johnson, Age: 75, Alive: true, Favorite Foods: [Cereal, Mustard, Onions]}

B. {ג€Nameג :€ג€Bob Johnsonג ,€ג€Ageג ,75 :€ג€Aliveג€: true, ג€Favorite Foodsג] :€ג€Cerealג ,€ג€Mustardג ,€ג€Onionsג€]}

C. {'Name': 'Bob Johnson', 'Age': 75, 'Alive': True, 'Favorite Foods': 'Cereal', 'Mustard', 'Onions'}

D. {ג€Nameג :€ג€Bob Johnsonג ,€ג€Ageג€: Seventyfive, ג€Aliveג€: true, ג€Favorite Foodsג] :€ג€Cerealג ,€ג€Mustardג ,€ג€Onionsג€]}

Correct Answer: *B*

Community vote distribution

B (75%) C (25%)

AliMo123 Highly Voted 2 years, 7 months ago

None of them is correct:
the right answer is"
{“Name”: “Bob Johnson”, “Age”: 75, “Alive”: true, “Favorite Foods”: [“Cereal”, “Mustard”, “Onions”]}

upvoted 29 times

timtgh 1 year, 6 months ago

Isn't that just option B, but typed with double quote marks instead of single?

upvoted 6 times

Broekie Highly Voted 2 years, 8 months ago

What is the JSON syntax that is formed the data?
A . {Name: Bob, Johson, Age: 75, Alive: true, Favourite Foods. [Cereal, “Mustard”, ”Onions]}
B . {Name”, ”Bob” Johson”, ”Age”, 75, ”Alive”, true, ”favourite Foods”, [”Cereal, ”Mustard”, Onions”]}
C . {“Name”: “Bob Johnson”,”Age”: 75,“Alive”: “true”,”Favorite Foods”: [“Cereal”,”Mustard”,”Onions”]}
D . {Name”. ”Bob Johson”, ”Age”: Seventyfive, ”Alive” true, ”favourite Foods” ,[Cereal” ”Mustard” ”Onions”]}

Answer: C

upvoted 14 times

tatrman 2 years, 8 months ago

C is wrong because booleans are like numbers
"Alive": true
not
"Alive": "true"

upvoted 11 times

danman32 4 months ago

Broekie mistyped the answers
C doesn't have quotes around the boolean.
however it doesn't have [] around the list of favorite foods.

upvoted 1 times

teikitiz Most Recent 4 months, 2 weeks ago

Selected Answer: B

A. {Name: Bob Johnson, Age: 75, Alive: true, Favorite Foods: [Cereal, Mustard, Onions]}
B. {"Name":"Bob Johnson","Age": 75,"Alive": true,"Favorite Foods": ["Cereal","Mustard","Onions"]}
C. {'Name': 'Bob Johnson', 'Age': 75, 'Alive': True, 'Favorite Foods': 'Cereal', 'Mustard', 'Onions'}
D. {"Name":"Bob Johnson","Age": Seventyfive,"Alive": true,"Favorite Foods": ["Cereal","Mustard","Onions"]}

upvoted 1 times

Burik 5 months ago

Selected Answer: B

Once the text formatting is fixed, it's B.

A. {Name: Bob Johnson, Age: 75, Alive: true, Favorite Foods: [Cereal, Mustard, Onions]}
B. {"Name": "Bob Johnson", "Age": 75, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "Onions"]}
C. {'Name': 'Bob Johnson', 'Age': 75, 'Alive': true, 'Favorite Foods': 'Cereal', 'Mustard', 'Onions'}
D. {"Name": "Bob Johnson", "Age": Seventyfive, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "Onions"]}

A is wrong because it's missing quotes of any kind.
B is valid according to Json Validator.
C is wrong because it uses single quotes and it's missing the array brackets.
D is wrong because it doesn't use the proper numerical value for Age.

upvoted 2 times

danman32 4 months ago

I believe single quotes are valid, as long as you are consistent

upvoted 1 times

[Removed] 5 months, 2 weeks ago

Selected Answer: B

Not sure if everyone sees the same, but the format is some very weird characters.
Instead of "quotes" it has the Euro sign, and what looks like Lambda symbol...

Regardless, Assuming this is a formatting issue, the only correct format is B

A: Wrong: has wrong syntax, its missing quotes around key-value pairs
B: Correct: has a formatting issue, at least to me, but it appears to be a correct format
C: Wrong: would have been correct, but it is missing the array brackets [ ] for the list of food
D: Wrong: the key-value pair "age":seventyfive is incorrect syntax

upvoted 2 times

habibmangal 7 months, 1 week ago

Selected Answer: C

According to ChatGPT option C is correct

upvoted 2 times

winder 1 year, 5 months ago

Selected Answer: B

how did I get this right, lol, it is B

upvoted 1 times

xziomal9 2 years, 2 months ago

A . {Name: Bob, Johson, Age: 75, Alive: true, Favourite Foods. [Cereal, ”Mustard”, ”Onions]}
B . {Name”, ”Bob” Johson”, ”Age”, 75, ”Alive”, true, ”favourite Foods”, [”Cereal, ”Mustard”, Onions”]}
C . {”Name”: ”Bob Johnson”,”Age”: 75,”Alive”: ”true”,”Favorite Foods”: [”Cereal”,”Mustard”,”Onions”]}
D . {Name”. ”Bob Johson”, ”Age”: Seventyfive, ”Alive” true, ”favourite Foods” ,[Cereal” ”Mustard” ”Onions”]}
E. {”Name”:”Bob Johnson”,”age”:75,”alive”:true,”favorite foods”:[”Cereal”,”Mustard”,”Onions”]}

upvoted 2 times

xziomal9 2 years, 2 months ago

The correct answer is:
E. {”Name”:”Bob Johnson”,”age”:75,”alive”:true,”favorite foods”:[”Cereal”,”Mustard”,”Onions”]}

upvoted 7 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 1 times

error_909 2 years, 2 months ago

{
"Name": "BoB Johnson",
"Age": 25,
"Alive": true,
"Favorite Foods": [
"cereal", "Mustard", "Onions"
]
}

upvoted 1 times

Rockford 2 years, 6 months ago

Correct would be this:
{
"Name":"Bob Johnson",
"Age":75,
"Alive": True,
"Favourite foods": ["Cereal","Mustard","Onions"]
}

upvoted 2 times

Rockford 2 years, 6 months ago

My bad! All is correct except:
"Alive": True,
Should be:
"Alive": true,
Lower case t on true...

upvoted 2 times

Question #315 *Topic 1*

Which JSON syntax is valid?

A. {λ€switchλ :€λ€nameλ :€λ€dist1λ ,€λ€interfacesλ] :€λ€gig1λ ,€λ€gig2λ ,€λ€gig3λ€]}

B. {/λ€switch/λ/} :€λ€name/λ :€λ€dist1λ/ ,€λ€interfaces/λ] :€λ€gig1λ ,€λ€gig2λ ,€λ€gig3λ€]}}

C. {λ€switchλ} :€λ€nameλ :€λ€dist1λ ,€λ€interfacesλ] :€λ€gig1λ ,€λ€gig2λ ,€λ€gig3λ€]}}

D. {'switch': ('name': 'dist1', 'interfaces': ['gig1', 'gig2', 'gig3'])}

Correct Answer: *C*

Community vote distribution

C (100%)

henchei Highly Voted 2 years, 8 months ago

The correct answer is C
Explanation: This JSON can be written as follows:
{
'switch': {
'name': 'dist1',
'interfaces': ['gig1', 'gig2', 'gig3']
}}

upvoted 15 times

ABC123 2 years, 4 months ago

Not Valid script

upvoted 1 times

Rockford Highly Voted 2 years, 6 months ago

can't see the answers correctly but the only option that works is:
{
"switch": {
"name": "dist1",
"interfaces": ["gig1", "gig2", "gig3"]
}
}
tested in JSONLint

upvoted 10 times

PureInertiaCopy Most Recent 3 months, 2 weeks ago

Admin! Could you please fix the symbols!
(At my time of writting, the quotation marks are replaced with this weird symbols! (, λ€) It makes it really goddamn hard to read!)

upvoted 6 times

JochenStacker 3 months, 4 weeks ago

The answers I see on screen are just gibberish.

upvoted 2 times

teikitiz 4 months, 2 weeks ago

Selected Answer: C

A. {"switch":"name":"dist1","interfaces": ["gig1","gig2","gig3"]}

B. {/"switch/": {/"name/":"dist1", /"interfaces/": ["gig1","gig2","gig3"]}}

C. {"switch": {"name":"dist1","interfaces": ["gig1","gig2","gig3"]}}

D. {'switch': ('name': 'dist1', 'interfaces': ['gig1', 'gig2', 'gig3'])}

upvoted 5 times

[Removed] 5 months, 2 weeks ago

I can't make out what the fork these symbols are...

upvoted 5 times

PureInertiaCopy 3 months, 2 weeks ago

I coppied all the text and replaced them all with double quotes. It all makes sense after that.

upvoted 1 times

Burik 5 months, 3 weeks ago

Are we supposed to discern what the heck is written in these answers? This is ridiculous.

upvoted 5 times

wr4net 6 months, 2 weeks ago

json data is typically key:value pairs in a rigid hierarchy, like a tree.
key elements at the same level are separated by commas.
keys and values are found in quotes if they are strings, but not always if its a binary (like true/false), they follow this format {"K":"V"}
no / are used in json. if multiple values for one key exist, they are encompassed in brackets - not braces, like this: {"K": ["V1","V2"]}
if a data key breaks off into sub key-value pairs, it will have a brace after it, like the start of hierarchy above it. {"K": {["K2":"V1","K2","V2"]} in this case, the value element for "K" includes all the stuff in brackets, which are themselves K:V pairs

upvoted 2 times

Parot 1 year ago

What the format !? This symbols are not belong to the Json format!

upvoted 2 times

Jared28 1 year, 5 months ago

Selected Answer: C

As per the practice exam in (it's just as badly formatted there too): CCNP: ENCOR: 350-401: CCNP ENTERPRISE: Cisco Certified Network Professional: Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)

upvoted 3 times

ougty 1 year, 7 months ago

Selected Answer: C

Hard to see in this format but it is C

upvoted 2 times

aohashi 1 year, 9 months ago

Selected Answer: C

It should be C

upvoted 2 times

xziomal9 2 years, 2 months ago

A. {“switch”:”name”:”dist1’’,”interfaces”:[“gig1’’,”gig2’’,”gig3”]}
B. {‘switch’:(‘name’:’dist1’,’interfaces’:[‘gig1’,’gig2’,’gig3’])}
C. {“switch”:{“name”:”dist1’’,”interfaces”:[“gig1’’,”gig2’’,”gig3”]}}
D. {/”switch/”:{/”name/”:”dist1’’,/”interfaces/”:[“gig1’’,”gig2’’,”gig3”]}}

upvoted 8 times

xziomal9 2 years, 2 months ago

The correct answer is:
C. {"switch":{"name":"dist1","interfaces":["gig1","gig2","gig3"]}}

upvoted 3 times

xziomal9 2 years, 2 months ago

better view
{
"switch": {
"name": "dist1",
"interfaces": ["gig1", "gig2", "gig3"]
}
}

upvoted 3 times

xziomal9 2 years, 2 months ago

{
"switch": {
"name": "dist1",
"interfaces": ["gig1", "gig2", "gig3"]
}
}

upvoted 1 times

kthekillerc 2 years, 5 months ago

A is the correct answer

upvoted 2 times

AliMo123 2 years, 6 months ago

{
‘switch’: {
‘name’: ‘dist1’,
‘interfaces’: [‘gig1’, ‘gig2’, ‘gig3’]
}}

upvoted 1 times

Hamzaaa 2 years, 7 months ago

C is correct

upvoted 2 times

Question #316 *Topic 1*

What is the structure of a JSON web token?

A. three parts separated by dots: header, payload, and signature

B. three parts separated by dots: version, header, and signature

C. header and payload

D. payload and signature

Correct Answer: *A*
Reference:
https://auth0.com/docs/tokens/references/jwt-structure

mrlyfi 3 months, 2 weeks ago
Provided answer is correct
Advice: remember HPs (Header, Payload and signature)
upvoted 1 times

kebkim 1 year, 2 months ago
JWT in the serialized form represents a string of the following format:

[header].[payload].[signature]
upvoted 2 times

kthekillerc 2 years, 2 months ago
Provided answer is correct
upvoted 2 times

DJOHNR 3 years, 3 months ago
https://www.geeksforgeeks.org/json-web-token-jwt

Answer A
upvoted 4 times

Question #317 *Topic 1*

A response code of 404 is received while using the REST API on Cisco DNA Center to POST to this URI:
/dna/intent/api/v1/template-programmer/project
What does the code mean?

A. The POST/PUT request was fulfilled and a new resource was created. Information about the resource is in the response body.

B. The request was accepted for processing, but the processing was not completed.

C. The client made a request for a resource that does not exist.

D. The server has not implemented the functionality that is needed to fulfill the request.

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/application-policy-infrastructure-controller-enterprise-module/1-2-x/config-guide/ b_apic-em_config_guide_v_1-2-x/b_apic-em_config_guide_v_1-2-x_chapter_01001.html

examShark Highly Voted 2 years, 6 months ago
The given answer is correct
upvoted 9 times

danman32 Most Recent 4 months ago
I hate it when answer URL references no longer exist.
upvoted 1 times

Question #318 *Topic 1*

Which two operations are valid for RESTCONF? (Choose two.)

A. PULL

B. PUSH

C. PATCH

D. REMOVE

E. ADD

F. HEAD

Correct Answer: *CF*
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b_166_programmability_cg/b_166_programmability_cg_chapter_01011.html

sledgey121 Highly Voted 2 years, 10 months ago

HEAD
GET
POST
PUT
PATCH
DELETE

upvoted 17 times

RHK0783 Highly Voted 2 years, 9 months ago

GET -- Read
PATCH -- Update
PUT -- Create or Replace
POST -- Create or Operations (reload, default)
DELETE -- Deletes the targeted resource
HEAD -- Header metadata (no response body)

upvoted 12 times

markymark874 Most Recent 10 months, 4 weeks ago

The following table shows how the RESTCONF operations relate to NETCONF protocol operations:

GET Read
PATCH Update
PUT Create or Replace
POST Create or Operations (reload, default)
DELETE Deletes the targeted resource
HEAD Header metadata (no response body)

upvoted 2 times

xziomal9 2 years, 2 months ago

RESTCONF:
DELETE
GET
HEAD
OPTIONS
PATCH
POST
PUT

upvoted 2 times

Sajj_gabi 2 years, 10 months ago

C is correct Patch is one of the operations

upvoted 1 times

gruffern 2 years, 12 months ago

RESTCONF supports the following HTTP methods and CRUD operations:
GET POST PUT DELETE OPTIONS

Edgeworth, Bradley; Rios, Ramiro Garza; Hucaby, David; Gooley, Jason. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

upvoted 2 times

```
<errors xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf">
    <error>
        <error-message>End-of-file reached in XML stream</error-message>
        <error-path>/ietf-interfaces:interfaces/interface=GigabitEthernet2</error-path>
        <error-tag>malformed-message</error-tag>
        <error-type>application</error-type>
    </error>
< /errors>
```

Refer to the exhibit. An engineer is using XML in an application to send information to a RESTCONF-enabled device. After sending the request, the engineer gets this response message and an HTTP response code of 400. What do these responses tell the engineer?

A. The Accept header sent was application/xml.

B. POST was used instead of PUT to update.

C. The Content-Type header sent was application/xml.

D. A JSON body was used.

Correct Answer: *C*

Community vote distribution

A (67%) C (17%) Other

juliok33p Highly Voted 2 years, 8 months ago

A is Correct

Accept and Content-type are both headers sent from a client (a browser) to a service.
Accept header is a way for a client to specify the media type of the response content it is expecting and Content-type is a way to specify the media type of request being sent from the client to the server.
The response was sent in XML so we can say the Accept header sent was application/xml.

upvoted 19 times

networkispower Highly Voted 11 months ago

Selected Answer: A

Correct answer is A. Tested using Postman.

When using application/xml on the Accept Header (HTTP 400 Bad Request):
{
"errors": {
"error": [
{
"error-message": "mismatched keypaths: /interface , /if:interfaces",
"error-path": "/ietf-interfaces:interfaces",
"error-tag": "malformed-message",
"error-type": "application"
}
]
}
}

When using application/xml on the Content-Type Header (HTTP 415 Unsupported Media Type):
{
"errors": {
"error": [
{
"error-message": "Unsupported media type: application/xml ; Should be one of: application/yang-data+xml, application/yang-data+json.",
"error-tag": "malformed-message",
"error-type": "application"
}
]
}
}

upvoted 11 times

mahnazmohamz Most Recent 2 months ago

help im so confused

upvoted 1 times

HungarianDish 7 months, 4 weeks ago

Could someone research this topic please?

"using XML in an application to send information" => Does this mean using "Content-Type: application/xml"?
If yes, then JSON body would cause HTTP 400 error. Thus, I would go for D) "A JSON body was used."

https://csod.my.site.com/supportcentral/s/article/How-do-I-resolve-HTTP-400-Bad-Request-errors-returned-by-Cornerstone-s-APIs?language=en_US

"Verify that the Content-Type request header matches the raw body data type.
Example: If your raw request body data is in JSON, but the Content-Type request header value contains "application/xml", you will encounter an HTTP 400 error."

Plus:
https://reqbin.com/req/3mrxjgw4/post-xml-example
https://reqbin.com/req/abghm4zf/json-content-type

upvoted 1 times

dnjJ56 11 months, 1 week ago

Selected Answer: C

The errors says " End of Life for XML stream' and it also says ' malformed message'.
That means, the format of the data inside the request, which seems to be XML based on the error, is not compatible with what server expects.

We define the format of the data inside the request using the Content-Type header (not by the Accept header).
So I go with C.

upvoted 1 times

Zizu007 1 year ago

Selected Answer: D

D - Correct;
when using Accept and Content-Type : application/yang-data+xml and Body content is JSON:

<errors xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf">
<error>
<error-message>End-of-file reached in XML stream</error-message>
<error-path>/ietf-interfaces:interfaces</error-path>
<error-tag>malformed-message</error-tag>
<error-type>application</error-type>
</error>
</errors>

when using Accept and Content-Type : application/yang-data+xml and Body content is XML:
Status: 201

upvoted 3 times

Zizu007 1 year ago

A - Wong;
don't get confused between application/xml and application/yang-data+xml. when using
Accept: 'application/xml' you will get this error:
<errors xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf">
<error>
<error-message>No acceptable mime-type supported. Got: application/xml ; Should be one of: application/yang-data+xml, application/yang-data+json, application/vnd.yang.collection+xml, application/vnd.yang.collection+json, application/yang-patch+xml, application/yang-patch+json.</error-message>
<error-tag>invalid-value</error-tag>
<error-type>application</error-type>
</error>
</errors>
---

upvoted 1 times

Zizu007 1 year ago

when using Accept and Content-Type : application/yang-data+xml and Body content is XML:
Status: 201

upvoted 1 times

Zizu007 1 year ago

C - Wrong, same as A.
when using
Content-Type: 'application/xml' you will get this error:
<errors xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf">
<error>
<error-message>Unsupported media type: application/xml ; Should be one of: application/yang-data+xml, application/yang-data+json.
</error-message>
<error-tag>malformed-message</error-tag>
<error-type>application</error-type>
</error>
</errors>
---

upvoted 1 times

Darude 1 year ago

Selected Answer: C

Correct answer is C
problem here is that the path of the interface isn't correct but there is no answer for that. Look at the atached link. there are two examples search for "3.6.3. Encoding Operation Resource Errors" there are two examples of error message one in Content-type in xml and other Content-type in json the result match the error message Content-type in xml LINK:
https://datatracker.ietf.org/doc/html/draft-ietf-netconf-restconf-14#section-3.6.3

upvoted 2 times

Wooker 1 year, 2 months ago

Selected Answer: A

the correct answer is A.

upvoted 1 times

[Removed] 1 year, 3 months ago

Selected Answer: C

Check the first line. It's saying xml but requstion yang-restconf

upvoted 1 times

snowfox 1 year, 4 months ago

So, the answer is C?
So, Accept header sent was NOT application/xml.
But, The Content-Type header sent was application/xml.
So the system showed an error message because contect was application/xml?

upvoted 1 times

Tannhaus 1 year, 4 months ago

Selected Answer: A

I think it's A

upvoted 1 times

Jared28 1 year, 5 months ago

Selected Answer: B

As per the practice exam in: CCNP: ENCOR: 350-401: CCNP ENTERPRISE: Cisco Certified Network Professional: Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)

upvoted 1 times

winder 1 year, 5 months ago

Selected Answer: A

Guys, if you want to share your answer, make sure give "Chosen Answer" option to help others. Thanks

upvoted 2 times

bara_ken 1 year, 7 months ago

Selected Answer: A

This is A

upvoted 1 times

Carl1999 2 years ago

B is corrrect.
guess why 400 badrequest.

upvoted 1 times

Amansoor79 2 years ago

A is the correct answer

upvoted 1 times

xziomal9 2 years, 2 months ago

The correct answer is:
A. The Accept header sent was application/xml.

upvoted 1 times

xziomal9 2 years, 2 months ago

Sorry
The correct answer is:
B. POST was used instead of PUT to update.

upvoted 2 times

Question #320 *Topic 1*

What is used to validate the authenticity of client and is sent in HTTP requests as a JSON object?

A. SSH

B. HTTPS

C. JWT

D. TLS

Correct Answer: *C*

Community vote distribution

C (100%)

RhJ72 Highly Voted 2 years, 3 months ago

JSON Web Token

upvoted 5 times

[Removed] Most Recent 5 months ago

Selected Answer: C

The given answer is correct

upvoted 1 times

youtri 1 year, 10 months ago

encoding JSON code written in POSTMAN

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

Question #321 *Topic 1*

What is YANG used for?

A. scraping data via CLI

B. processing SNMP read-only polls

C. describing data models

D. providing a transport for network configuration data between client and server

Correct Answer: *C*

examShark Highly Voted 2 years, 6 months ago

The given answer is correct

upvoted 10 times

flash007 Most Recent 4 months ago

Yang is data modling

upvoted 1 times

Question #322 *Topic 1*

Which HTTP status code is the correct response for a request with an incorrect password applied to a REST API session?

A. HTTP Status Code: 200

B. HTTP Status Code: 302

C. HTTP Status Code: 401

D. HTTP Status Code: 504

Correct Answer: *C*
Reference:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/401

Community vote distribution
C (100%)

Barti1 3 weeks, 3 days ago

Selected Answer: C
i m agree with what is said in previous one.
upvoted 1 times

wr4net 6 months, 2 weeks ago

Bad Underwear Passes Farts Noxiously Man!
400 Bad Request
401 Unauthorized
402 Payment Required
403 Forbidden
404 Not Found
405 Method Not Allowed
upvoted 3 times

Pilgrim5 7 months, 2 weeks ago

Selected Answer: C
Some HTTP codes and their meanings;
200 - OK
201 - Created
400 - Bad Request
401 - Unauthorized
403 - Forbidden
404 - Not found.
upvoted 1 times

kewokil120 11 months ago

Selected Answer: C
The given answer is correct
upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct
upvoted 4 times

skh 3 years ago

C
Study Guide book
The HTTP status code 401 means Unauthorized—referring to
incorrect login credentials or not having valid authentication to a
destination. The following table lists more HTTP status codes.
HTTP code 401 Unauthorized Client not authenticated to access site or API
call
upvoted 3 times

skh 3 years ago

I think correct https://airbrake.io/blog/http-errors/401-unauthorized-error

As discussed in the introduction, a 401 Unauthorized Error indicates that the client (the web browser, in most cases) has requested a restricted resource (such as a web page) from the server, but the client has failed to provide valid authentication credentials.
upvoted 3 times

Question #323 *Topic 1*

Which protocol does REST API rely on to secure the communication channel?

A. HTTP

B. SSH

C. HTTPS

D. TCP

Correct Answer: *C*

flash007 4 months ago
restapi is a web language http is not secure but https is secure
upvoted 1 times

examShark 2 years, 6 months ago
The given answer is correct
upvoted 4 times

skh 3 years ago
correct C
To achieve secure communication, REST APIs use Hypertext Transfer Protocol Secure (HTTPS)
https://blog.restcase.com/top-5-owasp-security-tips-for-designing-secured-rest-apis/
upvoted 2 times

Question #324 *Topic 1*

At which layer does Cisco DNA Center support REST controls?

A. session layer

B. northbound APIs

C. EEM applets or scripts

D. YAML output from responses to API calls

Correct Answer: *B*

ihateciscoreally 3 months, 1 week ago
APIs are not layer. broken question. another to remember.
upvoted 1 times

examShark 2 years, 6 months ago
The given answer is correct
upvoted 3 times

Hamzaaa 2 years, 7 months ago
Intent API (Northbound)
The Intent API is a Northbound REST API that exposes specific capabilities of the Cisco DNA Center platform.
The Intent API provides policy-based abstraction of business intent, allowing focus on an outcome rather than struggling with individual mechanisms steps.
The RESTful Cisco DNA Center Intent API uses HTTPS verbs (GET, POST, PUT, and DELETE) with JSON structures to discover and control the network.
For more information, see Intent API.
upvoted 3 times

hku68 2 years, 10 months ago
Answer is B
https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/multivendor-support-southbound
upvoted 2 times

Question #325 *Topic 1*

Which algorithms are used to secure REST API from brute attacks and minimize the impact?

A. SHA-512 and SHA-384

B. MD5 algorithm-128 and SHA-384

C. SHA-1, SHA-256, and SHA-512

D. PBKDF2, BCrypt, and SCrypt

Correct Answer: *D*

MasiEB Highly Voted 3 years, 1 month ago
https://restfulapi.net/security-essentials/
D is correct
upvoted 18 times

examShark 2 years, 6 months ago
b-crypt to secure a REST API!
upvoted 4 times

GATUNO Most Recent 2 years ago
Passwords must always be hashed to protect the system (or minimize the damage) even if it is compromised in some hacking attempts. There are many such hashing algorithms that can prove really effective for password security e.g. PBKDF2, bcrypt, and scrypt algorithms. (D)
upvoted 3 times

last7 3 years, 1 month ago
Answer is A.
MD5 & SHA-1 are legacy. PBKDF2 & SCrypt are considered uncrackable, but used by Cisco for local password encryption, and not REST functions.
upvoted 2 times

divt 2 years, 5 months ago
D
One of the best practices to secure REST APIs is using password hash. Passwords must
always be hashed to protect the system (or minimize the damage) even if it is compromised in some hacking attempts. There are many such hashing algorithms which can prove really

effective for password security e.g. PBKDF2, bcrypt and scrypt algorithms.

Other ways to secure REST APIs are: Always use HTTPS, Never expose information on URLs
Usernames, passwords, session tokens, and API keys should not appear in the URL
upvoted 3 times

Question #326 *Topic 1*

Which method of account authentication does OAuth 2.0 use within REST APIs?

A. username/role combination

B. access tokens

C. cookie authentication

D. basic signature workflow

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-api/guide/ftd-rest-api/auth-ftd-rest-api.pdf

examShark Highly Voted 2 years, 6 months ago
The given answer is correct
upvoted 9 times

iGlitch 1 year, 1 month ago
no way!
upvoted 2 times

cvndani Most Recent 1 year, 10 months ago
Access token.
https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-api/guide/ftd-rest-api/auth-ftd-rest-api.pdf
upvoted 2 times

Question #327 *Topic 1*

Which two protocols are used with YANG data models? (Choose two.)

A. TLS

B. RESTCONF

C. SSH

D. NETCONF

E. HTTPS

Correct Answer: *BD*

edg Highly Voted 3 years, 3 months ago

The answers are "B" and "D".

https://ftp.ripe.net/rfc/v3test/test8345.v2v3.html

"8. Security Considerations
The YANG modules specified in this document define a schema for data that is designed to be accessed via network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040]. The lowest NETCONF layer is the secure transport layer, and the mandatory-to-implement secure transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer is HTTPS, and the mandatory-to-implement secure transport is TLS [RFC5246]."

upvoted 9 times

flash007 Most Recent 4 months ago

restconf and netconf

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 3 times

skh 3 years ago

B & D
Study Guide
Data Models and Supporting Protocols
This section provides a high-level overview of some of the most common
data models and tools and how they are leveraged in a programmatic
approach:
Yet Another Next Generation (YANG) modeling language
Network Configuration Protocol (NETCONF) , defined in RFC 4741 and RFC 6241, is an IETF standard protocol that uses the YANG data models to communicate with the various
devices on the network.
RESTCONF , defined in RFC 8040, is used to programmatically interface
with data defined in YANG models while also using the datastore concepts
defined in NETCONF.

upvoted 3 times

Question #328 *Topic 1*

What is a benefit of data modeling languages like YANG?

A. They create more secure and efficient SNMP OIDs.

B. They provide a standardized data structure, which results in configuration scalability and consistency.

C. They enable programmers to change or write their own applications within the device operating system.

D. They make the CLI simpler and more efficient.

Correct Answer: *B*

Nhan 2 years, 1 month ago
The given answer is correct
upvoted 4 times

examShark 2 years, 6 months ago
The given answer is correct
upvoted 2 times

Question #329 *Topic 1*

Which protocol infers that a YANG data model is being used?

A. SNMP

B. RESTCONF

C. REST

D. NX-API

Correct Answer: *B*

examShark Highly Voted 2 years, 6 months ago
The given answer is correct
upvoted 7 times

Question #330 *Topic 1*

Which method displays text directly into the active console with a synchronous EEM applet policy?

A. event manager applet boom event syslog pattern 'UP' action 1.0 syslog priority direct msg 'logging directly to console'

B. event manager applet boom event syslog pattern 'UP' action 1.0 gets 'logging directly to console'

C. event manager applet boom event syslog pattern 'UP' action 1.0 string 'logging directly to console'

D. event manager applet boom event syslog pattern 'UP' action 1.0 puts 'logging directly to console'

Correct Answer: *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-3s/eem-xe-3s-book/eem-policy-cli.html

Community vote distribution
D (100%)

P1Z7C Highly Voted 2 years, 8 months ago
Answer D:
Action gets: Use the action gets command to get an input from the local tty in a synchronous applet and store the value in the given variable.
action puts
Action puts: Prints data directly to the local tty in a synchronous applet when an EEM applet is triggered.
upvoted 21 times

nushadu Most Recent 11 months, 2 weeks ago
Selected Answer: D
!
event manager applet boom
event syslog pattern "UP"
action 1.0 puts "logging directly to console"
!

cisco_R5(config)#int loo1
cisco_R5(config-if)#
*Dec 20 17:36:48.447: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
cisco_R5(config-if)#
*Dec 20 17:36:48.448: %HA_EM-6-LOG: boom: logging directly to console
*Dec 20 17:36:49.456: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
*Dec 20 17:36:49.457: %HA_EM-6-LOG: boom: logging directly to console
cisco_R5(config-if)#
upvoted 2 times

YTAKE 1 year, 11 months ago
Selected Answer: D
D is the correct answer.
upvoted 1 times

xziomal9 2 years, 2 months ago
The correct answer is:
D.
event manager applet boom
event syslog pattern 'UP'
action 1.0 puts 'logging directly to console'
upvoted 1 times

Adrenalina73 2 years, 2 months ago
Answer D:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/15-mt/eem-15-mt-book/eem-policy-cli.html#GUID-F5242149-D934-46C4-8D34-7440499699E2

The action puts command will write the string to the active console. A new line will be displayed unless the nonewline keyword is specified. The output from the action puts command for a synchronous applet is displayed directly to the console, bypassing the system logger. The output of the action puts command for an asynchronous applet is directed to the system logger.
upvoted 2 times

kthekillerc 2 years, 2 months ago
Provided answer is correct
upvoted 1 times

Mac13 2 years, 7 months ago

Answer = D
From IOS context help:
syslog Log a syslog message
gets get line of input from active tty
string string commands
puts print data to active tty

upvoted 2 times

tatrman 2 years, 8 months ago

D) ... The action puts command will write the string to the active console. A new line will be displayed unless the nonewline keyword is specified. The output from the action puts command for a synchronous applet is displayed directly to the console, bypassing the system logger. The output of the action puts command for an asynchronous applet is directed to the system logger.

upvoted 2 times

Metro 2 years, 8 months ago

D is the correct answer

upvoted 4 times

mhizha 2 years, 8 months ago

A is the Answer

upvoted 1 times

Question #331 *Topic 1*

Which two steps are required for a complete Cisco DNA Center upgrade? (Choose two.)

A. automation backup

B. system update

C. golden image selection

D. proxy configuration

E. application updates

Correct Answer: *BE*
Reference:
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/upgrade/b_cisco_dna_center_upgrade_guide/m_upgrade_to_cisco_dna_center_2_2_2_x.html

Community vote distribution

BE (100%)

Saqib79 Highly Voted 3 years, 6 months ago
Correct Options are B & E.
upvoted 35 times

Sparks026 Highly Voted 3 years, 6 months ago
Yes B & E are correct
upvoted 11 times

winder Most Recent 1 year, 5 months ago
Selected Answer: BE
BE is the answer
upvoted 2 times

toni2 1 year, 7 months ago
Selected Answer: BE
Correct Answer BE
upvoted 2 times

aohashi 1 year, 9 months ago
Selected Answer: BE
It should be BE
upvoted 2 times

Fringe 1 year, 10 months ago
Selected Answer: BE
b and e
upvoted 1 times

xziomal9 2 years, 2 months ago
The correct answer is:
B. system update
E. application updates
upvoted 2 times

BigMomma4752 2 years, 8 months ago
The correct answers are B&E.
upvoted 3 times

Jclemente 2 years, 8 months ago
Correct answer should be B & E..
upvoted 2 times

39first 2 years, 9 months ago
B and E.
upvoted 2 times

Helloory 3 years ago
Correct answers are B and E

upvoted 2 times

james4231 3 years, 1 month ago

should be BE
After the system update is complete, at the top of the Application Updates field, click Download All.

upvoted 1 times

slachet 3 years, 2 months ago

Considering boson exam answer and sources (Reference1, Reference2), the process is: 1. have super-admin-role permissions, 2. perform a backup, 3. system update, 4. application update. "Automation backup" is a full backup according to the Reference3.
Reference1=https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/upgrade/b_cisco_dna_center_upgrade_guide/m_upgrade_to_cisco_dna_center_2_1_1_x.html;
Reference2=https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/upgrade/b_cisco_dna_center_upgrade_guide/b_cisco_dna_center_upgrade_guide_w_parts_2_chapter_0110.html;
Reference3=https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/upgrade/b_cisco_dna_center_upgrade_guide/m_upgrade_to_cisco_dna_center_2_1_1_x.html

upvoted 3 times

akbntc 3 years, 3 months ago

Correct Options are B & E.

upvoted 3 times

mimou 3 years, 3 months ago

Procedure
Step 1
A system update appears on the Software Updates page. Click Update.

Step 2
After the system update is complete, at the top of the Application Updates field, click Download All.

The packages begin downloading.
Step 3
After the packages are downloaded, at the top of the Application Updates field, click Update All.

The packages begin updating.
Step 4
Ensure that each application has been updated by reviewing its version in the Installed Apps page. sorry it's B and E

upvoted 6 times

mimou 3 years, 3 months ago

A and B
Prerequisites for Upgrading https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/upgrade/b_cisco_dna_center_upgrade_guide/b_cisco_dna_center_upgrade_guide_w_parts_2_chapter_0110.html

upvoted 2 times

mbustani 3 years, 3 months ago

A & B guys.
Prerequisites for Upgrading

You must complete the system updates before you can perform package updates. Do not download or install any package updates until all system updates have been installed.
You cannot upgrade the packages individually. You must follow all of the steps that are described in this guide.
Create a backup of your Cisco DNA Center database. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/upgrade/b_cisco_dna_center_upgrade_guide/b_cisco_dna_center_upgrade_guide_w_parts_2_chapter_0110.html

upvoted 2 times

Audi87 2 years, 8 months ago

prerequisites for upgrade and complete system upgrade are two different things. B and E is correct

upvoted 2 times

Question #332 *Topic 1*

Which method creates an EEM applet policy that is registered with EEM and runs on demand or manually?

A. event manager applet ondemand event none action 1.0 syslog priority critical msg 'This is a message from ondemand'

B. event manager applet ondemand action 1.0 syslog priority critical msg 'This is a message from ondemand'

C. event manager applet ondemand event register action 1.0 syslog priority critical msg 'This is a message from ondemand'

D. event manager applet ondemand event manual action 1.0 syslog priority critical msg 'This is a message from ondemand'

Correct Answer: *A*

Community vote distribution

A (100%)

edg Highly Voted 3 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-e1.html

EEM usually schedules and runs policies on the basis of an event specification that is contained within the policy itself. The event manager run command allows policies to be run manually. The event none command must first be configured to run the policy manually. The None Event Detector includes arguments when it publishes the none event. This command does not have a no form.

upvoted 8 times

Hugh_Jazz 2 years, 1 month ago

Concur with edg, action none first, then event manager run to manually kick it off.

upvoted 2 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: A

cisco_R5#sh runn | b event
event manager applet boom
event syslog pattern "UP"
action 1.0 puts "logging directly to console"
event manager applet ondemand
event none
action 1.0 syslog priority critical msg "Hello WORLD)))"
!
end

cisco_R5#event manager run ondemand
cisco_R5#
*Dec 20 17:41:10.545: %HA_EM-2-LOG: ondemand: Hello WORLD)))
cisco_R5#

upvoted 2 times

xziomal9 2 years, 2 months ago

A.
event manager applet ondemand
event none
action 1.0 syslog priority critical msg "This is a message from ondemand"
B.
event manager applet ondemand
action 1.0 syslog priority critical msg "This is a message from ondemand"
C.
event manager applet ondemand
event register action 1.0 syslog priority critical msg "This is a message from ondemand"
D.
event manager applet ondemand
event manual action 1.0 syslog priority critical msg "This is a message from ondemand"

The correct answer is:
A

upvoted 2 times

youtri 1 year, 7 months ago

correct, you will see the syslog message when you type this cli comand:
#event manager run ondemand

upvoted 1 times

Question #333 *Topic 1*

What does this EEM applet event accomplish?
"event snmp oid 1.3.6.1.3.7.6.5.3.9.3.8.7 get-type next entry-op gt entry-val 75 poll-interval 5"

A. Upon the value reaching 75%, a SNMP event is generated and sent to the trap server.

B. It reads an SNMP variable, and when the value exceeds 75%, it triggers an action.

C. It issues email when the value is greater than 75% for five polling cycles.

D. It presents a SNMP variable that can be interrogated.

Correct Answer: *B*

HarwinderSekhon 6 months ago

Chat GPT4- The EEM (Embedded Event Manager) applet event you've provided uses SNMP (Simple Network Management Protocol) to monitor a specific OID (Object Identifier) value. The particular settings imply that the applet is polling the SNMP OID every 5 seconds (or whatever unit the network device is using), and when the value of that OID is greater than 75, it triggers an action. The nature of this action isn't defined in the snippet you've provided, but it could be anything from logging a message, to sending an alert, to executing a command.

So, the correct option from those you've provided is:
B. It reads an SNMP variable, and when the value exceeds 75%, it triggers an action.

upvoted 1 times

nightstalker 3 months, 4 weeks ago

please, do not post answers from chatGPT, we really don't need them, even if they're correct

upvoted 3 times

HarwinderSekhon 6 months ago

it does not show any action, I am confused.

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 2 times

Question #334 *Topic 1*

What is a requirement for an Ansible-managed node?

A. It must have an SSH server running.

B. It must be a Linux server or a Cisco device.

C. It must support ad hoc commands.

D. It must have an Ansible Tower installed.

Correct Answer: *A*

Community vote distribution

A (86%) 14%

Patrick1234 Highly Voted 2 years, 5 months ago

How are you ever going to open a session to a node if its not running an ssh server? A is correct.

upvoted 7 times

bogd 1 year, 9 months ago

WinRM for Windows machines, various REST APIs, etc. There are more things managed by Ansible than are dreamt of in your philosophy... :p

upvoted 2 times

Lrrr_FromOmicronPersei8 4 months ago

I salute your sarcasm sir.

upvoted 1 times

due Most Recent 3 months ago

Selected Answer: A

Ansible control machine (where you run Ansible from) and the managed nodes (where Ansible executes tasks) need to have SSH clients installed. However, the specific requirement I mentioned in my previous response is that the managed nodes must have an SSH server running, which is necessary for Ansible to establish connections and remotely manage those nodes.

To clarify:

-Ansible control machine: Requires an SSH client to establish connections to managed nodes.
-Managed nodes: Require an SSH server to accept incoming connections from the Ansible control machine.

upvoted 3 times

LanreDipeolu 3 months ago

Selected Answer: C

If Ansible does not support ad hoc command, it will not run SSH. So the answer is C

upvoted 1 times

Asymptote 11 months ago

Selected Answer: A

In order for a node to be managed by Ansible, it must have an SSH server running and be reachable from the machine running Ansible. Ansible uses SSH to connect to and communicate with managed nodes, so an SSH server is required in order for Ansible to function properly.

It's worth noting that while Ansible is typically used to manage Linux servers, it can also be used to manage nodes running other operating systems, such as Windows, which may have different requirements.

upvoted 2 times

bogd 1 year, 9 months ago

Selected Answer: A

The SSH requirement has not been true for a long time... Think Windows nodes for example, where the connection is made over WinRM.

However, all the other answers are clearly false, so I can only assume the author was only thinking of Linux/Cisco machines. So A it is...

upvoted 1 times

cert_man_1337 2 years, 5 months ago

Taken from the book pager 876-877 "Ansible communicates using SSH for a majority of device, and it can support Windows Remote Management (WinRM) and other transport methods to the clients it manages". As well as the Ansible website https://www.ansible.com/overview/how-ansible-works "SSH is not the only transport possible" Therefore...
A is wrong based on the books and the Ansible website.
B is wrong because WinRM is supported, thus Windows is supported.
C is likely correct because of how Ansible works.
D is wrong because Ansible Towers are not required for an Ansible deployment.

upvoted 2 times

gtddrf 2 years, 3 months ago

Answer is A.
Referencing the same document, it states, "Ansible then executes these modules (over SSH by default), and removes them when finished."

upvoted 5 times

examShark 2 years, 6 months ago

350-401

upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

chris110 2 years, 4 months ago

please explane

upvoted 1 times

Question #335 *Topic 1*

Which characteristic distinguishes Ansible from Chef?

A. Ansible uses Ruby to manage configurations. Chef uses YAML to manage configurations.

B. The Ansible server can run on Linux, Unix or Windows. The Chef server must run on Linux or Unix.

C. Ansible pushes the configuration to the client. Chef client pulls the configuration from the server.

D. Ansible lacks redundancy support for the primary server. Chef runs two primary servers in active/active mode.

Correct Answer: *C*

Ansible works by connecting to your nodes and pushing out small programs, called ג€Ansible modulesג€ to them. These programs are written to be resource models of the desired state of the system. Ansible then executes these modules (over SSH by default), and removes them when finished.
Chef is a much older, mature solution to configure management. Unlike Ansible, it does require an installation of an agent on each server, named chef-client. Also, unlike Ansible, it has a Chef server that each client pulls configuration from.

examShark Highly Voted 2 years, 6 months ago

The given answer is correct

upvoted 7 times

Splashisthegreatestmovie Most Recent 5 months, 2 weeks ago

I hate some of these questions. Answer C which is the only "correct" answer is a comparison and contrast of Ansible and Chef instead of describing a characteristic of Ansible.

upvoted 1 times

ihateciscoreally 3 months, 1 week ago

sometimes you dont know whether to rely on instinct or your knowledge. cisco exams are very valuable but they are so sh*tty constructed...

upvoted 1 times

x3rox 10 months, 1 week ago

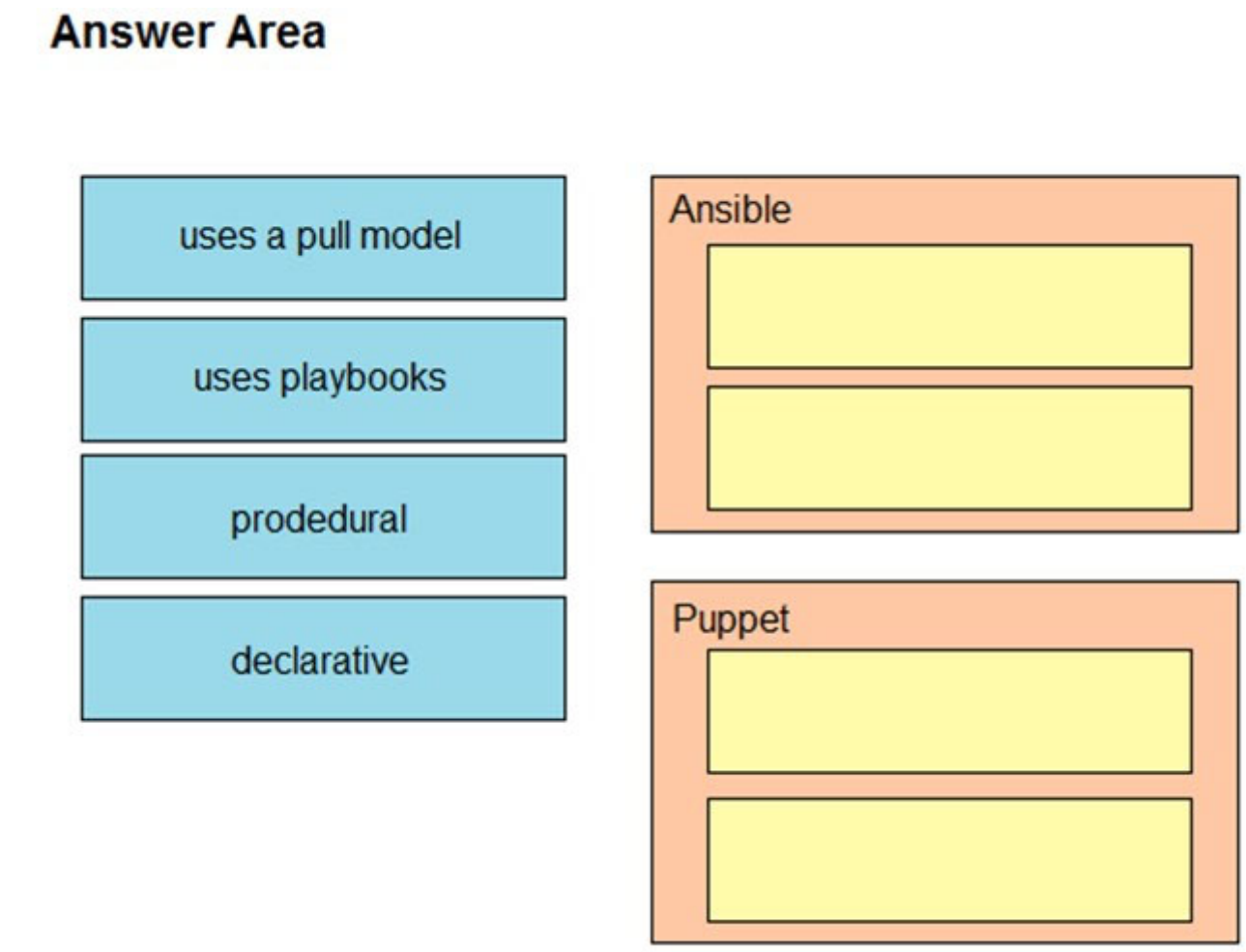
Answer is correct
B: is wrong since it's available for Windows and MacOS as well
https://docs.chef.io/chef_install_script/

upvoted 2 times

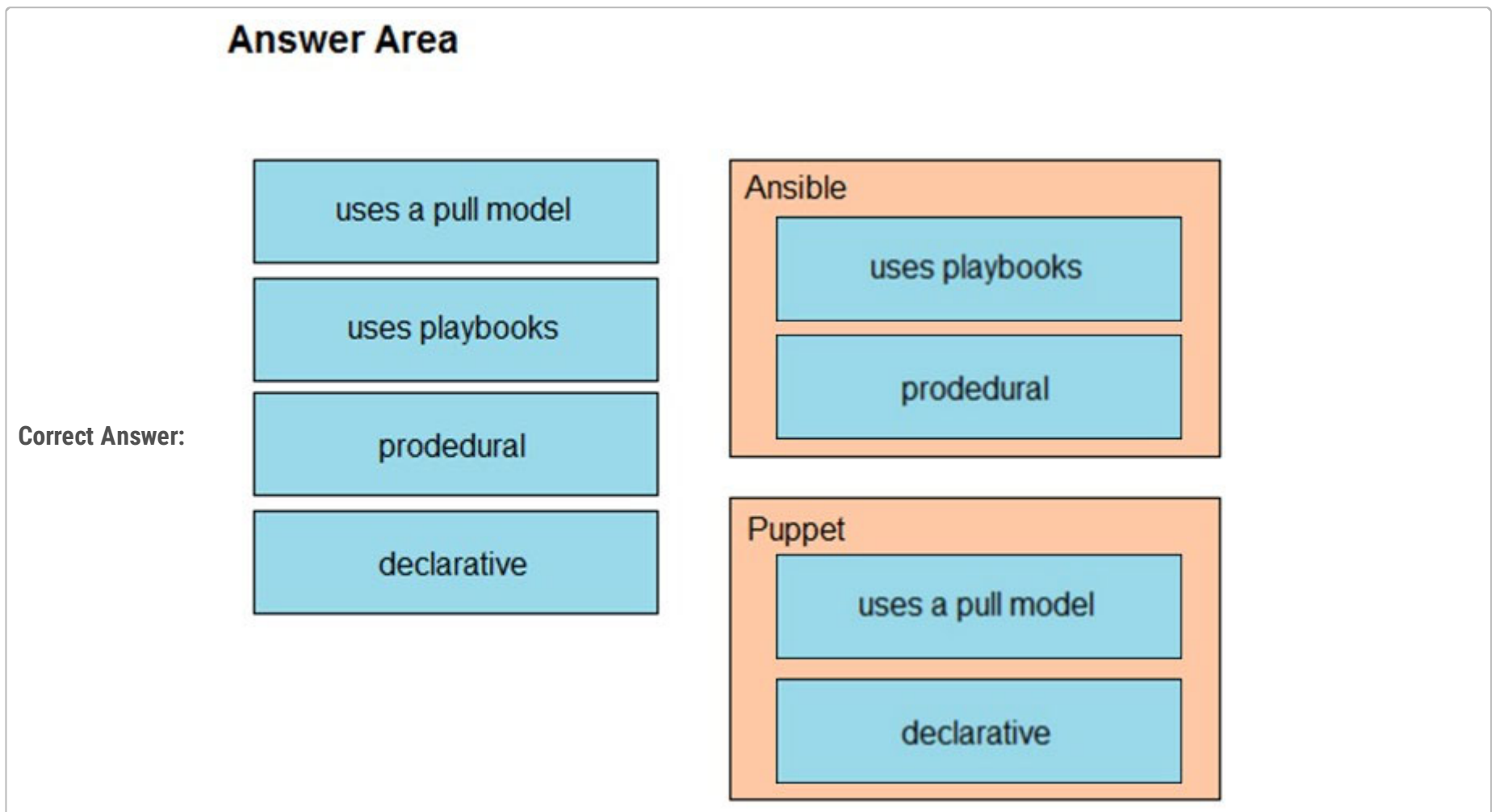
DRAG DROP -

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

Select and Place:



Correct Answer:



HungarianDish Highly Voted 8 months, 2 weeks ago

My favorite:
https://stackoverflow.com/questions/1619834/what-is-the-difference-between-declarative-and-procedural-programming-paradigms

"Let me give you a real-world example: I need a cup of tea.
Procedural:
Go to kitchen
Get sugar, milk, and tea,
Mix them, and heat over the fire till it boils
Put that in a cup and bring it to me

Declarative:
Get me a cup of tea.

In a procedural language, you define the whole process and provide the steps how to do it. You just provide orders and define how the process will be served.

In a declarative language, you just set the command or order, and let it be on the system how to complete that order. You just need your result without digging into how it should be done."

upvoted 12 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Ansible uses playbooks and is procedural. Answer is correct.

upvoted 1 times

XDR 7 months, 3 weeks ago

https://k21academy.com/ansible/terraform-vs-ansible/#procdeural

Terraform follows the declarative approach, ensuring that if your defined environment suffers changes, it rectifies those changes. This tool attempts to reach the desired end state described by the sysadmin. Puppet also follows the declarative approach. With terraform, we can automatically describe the desired state and figure out how to move from one state to the next.

Ansible is of hybrid nature. It follows both declarative and procedural style configuration. It performs ad-hoc commands to implement procedural-style configurations. Please read the documentation of Ansible very carefully to get in-depth knowledge of its behavior. It's important to know whether you need to add or subtract resources to get the desired result or need to indicate the resources required explicitly.

upvoted 1 times

StefanOT2 10 months, 1 week ago

Provided answer is correct.

Puppet is declarative for sure. Ansible uses at least procedural methods.

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 4 times

Rockford 2 years, 6 months ago

Puppet aims to be declarative, ansible is a hybrid of declarative and procedural! Answer is still what they are looking for but options to chose are wrong...

upvoted 3 times

Rockford 2 years, 6 months ago

I take that back, that website is wrong, answer is right...

upvoted 1 times

Rockford 2 years, 6 months ago

Answer is wrong: Ansible uses playbooks and is declaritive!

Declarative Not Procedural- Other configuration tools tend to be procedural do this and then do that and so on. Ansible works by you writing a description of the state of the machine that you want and then it takes steps to fulfil that description.

https://subramanisundaram.medium.com/ansible-infrastructure-automation-fc84ba9bd9da

upvoted 2 times

Xerath 11 months, 3 weeks ago

https://www.google.com/search?q=is+puppet+declarative&oq=puppet+is+decla&aqs=edge.1.69i57j0i22i30l8.4390j0j1&sourceid=chrome&ie=UTF-8 puppet is declarative.

upvoted 1 times

```
with manager.connect(host=192.168.0.1, port=22,
                     username='admin', password='password1', hostkey_verify=True,
                     device_params={'name':'nexus'}) as m:
```

Refer to the exhibit. What does the snippet of code achieve?

A. It creates an SSH connection using the SSH key that is stored, and the password is ignored.

B. It creates a temporary connection to a Cisco Nexus device and retrieves a token to be used for API calls.

C. It opens an ncclient connection to a Cisco Nexus device and maintains it for the duration of the context.

D. It opens a tunnel and encapsulates the login information, if the host key is correct.

Correct Answer: *C*

gtddrf Highly Voted 2 years, 3 months ago

Correct Answer: C
ncclient is a Python library that facilitates client-side scripting and application development around the NETCONF protocol. The Python snippet uses the ncclient to connect and establish a NETCONF session to a Nexus device (which is also a NETCONF server).

upvoted 6 times

kthekillerc Most Recent 2 years, 2 months ago

Provided answer is correct

upvoted 2 times

AliMo123 2 years, 6 months ago

A is correct
Connect via SSH and initialize the NETCONF session. First attempts the publickey authentication method and then password authentication.
To disable attempting publickey authentication altogether, call with allow_agent and look_for_keys as False.
host is the hostname or IP address to connect to
port is by default 830 (PORT_NETCONF_DEFAULT), but some devices use the default SSH port of 22 so this may need to be specified
https://ncclient-fredgan.readthedocs.io/_/downloads/en/sphinx_version/pdf/

upvoted 3 times

Jared28 1 year, 5 months ago

A states it *ignores* the password. The info you provided simply states it occurs after.

upvoted 2 times

examShark 2 years, 6 months ago

The given answer is correct

upvoted 1 times

RexChen 2 years, 6 months ago

https://github.com/ADTRAN/ncclient/blob/d665bde4208b9bf83a472b59f29cc44ea481eecb/ncclient/transport/ssh.py

upvoted 1 times

Question #338 *Topic 1*

Which two characteristics define the Intent API provided by Cisco DNA Center? (Choose two.)

A. northbound API

B. business outcome oriented

C. device-oriented

D. southbound API

E. procedural

Correct Answer: *AB*

juliok33p Highly Voted 2 years, 8 months ago

A & B are Correct

Intent API (Northbound)
The Intent API is a Northbound REST API that exposes specific capabilities of the Cisco DNA Center platform.
The Intent API provides policy-based abstraction of business intent, allowing focus on an outcome rather than struggling with individual mechanisms steps.

https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/intent-api-northbound

upvoted 13 times

kthekillerc Most Recent 2 years, 2 months ago

Provided answer is correct

upvoted 3 times

Question #339 *Topic 1*

In a Cisco DNA Center Plug and Play environment, why would a device be labeled unclaimed?

A. The device has not been assigned a workflow.

B. The device could not be added to the fabric.

C. The device had an error and could not be provisioned.

D. The device is from a third-party vendor.

Correct Answer: *A*

Community vote distribution

A (100%)

Sham Highly Voted 2 years, 8 months ago

the question ask about plug and play environment Devices States element which are :
Error—Device had an error and could not be provisioned.
Unclaimed—Device has not been assigned a workflow.
Planned—Device is added to Network Plug and Play and has been assigned a workflow, but has not yet contacted the server.
Provisioned—Device is successfully onboarded and added to inventory
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-5/user_guide/b_dnac_ug_1_2_5/b_dnac_ug_1_2_4_chapter_010.html

for Device Information states which are :
Unclaimed: Device has not been provisioned.

Planned: Device has been claimed but has not yet contacted the server.

Onboarding: Device onboarding is in progress.

Provisioned: Device is successfully onboarded and added to inventory.

Error: Device had an error and could not be provisioned.

upvoted 19 times

HungarianDish Most Recent 8 months, 2 weeks ago

Selected Answer: A

Same here:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2/user_guide/b_dnac_ug_1_2/b_dnac_ug_1_2_chapter_01111.html.xml

upvoted 1 times

nour 1 year, 3 months ago

Selected Answer: A

The Answer is A
+ Error - Device had an error and could not be provisioned.
+ Unclaimed - Device has not been assigned a workflow.
+ Planned - Device is added to Network Plug and Play and has been assigned a workflow, but has not yet contacted the server.
+ Provisioned - Device is successfully onboarded and added to inventory.

upvoted 2 times

Edwinmolinab 1 year, 4 months ago

Selected Answer: A

Unclaimed—Device has not been provisioned.

Planned—Device has been claimed but has not yet contacted the server.

Onboarding—Device onboarding is in progress.

Provisioned—Device is successfully onboarded and added to inventory.

Error—Device had an error and could not be provisioned.

upvoted 2 times

bara_ken 1 year, 7 months ago

Selected Answer: A

This is A

upvoted 1 times

xziomal9 2 years, 2 months ago

The correct answer is:
A. The device has not been assigned a workflow.

upvoted 2 times

gtddrf 2 years, 4 months ago

Answer is A
From https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-5/user_guide/b_dnac_ug_1_2_5/b_dnac_ug_1_2_4_chapter_010.html
Pie chart showing the number of devices in each of the following states:
Error—Device had an error and could not be provisioned.
Unclaimed—Device has not been assigned a workflow.
Planned—Device is added to Network Plug and Play and has been assigned a workflow, but has not yet contacted the server.
Provisioned—Device is successfully onboarded and added to inventory.

upvoted 3 times

jas26says 2 years, 6 months ago

A is the correct one.

upvoted 4 times

chamies2020 2 years, 8 months ago

I bet also option A.

upvoted 1 times

0F10 2 years, 8 months ago

Resetting a device applies only to devices in the Error state and resets its state to Unclaimed and reloads the device, but does not remove it from the Plug and Play database. Use Delete if you want to delete a device.

upvoted 1 times

[Removed] 2 years, 8 months ago

I think A is correct

upvoted 2 times

WhatNot 2 years, 8 months ago

Unclaimed: Device has not been provisioned.
Planned: Device has been claimed but has not yet contacted the server.
Onboarding: Device onboarding is in progress.
Provisioned: Device is successfully onboarded and added to inventory.
Error: Device had an error and could not be provisioned.

Source:https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/user_guide/b_cisco_dna_center_ug_2_1_2/b_cisco_dna_center_ug_2_1_1_chapter_01101.html#id_90738

The highlighted answer is incorrect. I don't know which answer is the correct one but it is not C. Device had an error and could not be provisioned

upvoted 1 times

Question #340 *Topic 1*

What does the Cisco DNA Center use to enable the delivery of applications through a network and to yield analytics for innovation?

A. process adapters

B. Command Runner

C. intent-based APIs

D. domain adapters

Correct Answer: *C*

Community vote distribution

C (100%)

skh Highly Voted 3 years ago

Correct Answer: C
The Cisco DNA Center open platform for intent-based networking provides 360- degree extensibility across multiple components, including:
+ Intent-based APIs leverage the controller to enable business and IT applications to deliver intent to the network and to reap network analytics and insights for IT and business innovation. These enable APIs that allow Cisco DNA Center to receive input from a variety of sources, both internal to IT and from line-of-business applications, related to application policy, provisioning, software image management, and assurance.
https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-cent-plat-sol-over-cte-en.html
upvoted 6 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Selected Answer: C
Provided answer is correct. C
upvoted 1 times

ihateciscoreally 3 months, 1 week ago

honestly i dont know sh!t about A,B and D so i pick C.
upvoted 1 times

examShark 2 years, 6 months ago

The given answer is correct
upvoted 4 times

Question #341 *Topic 1*

Which devices does Cisco DNA Center configure when deploying an IP-based access control policy?

A. all devices integrating with ISE

B. selected individual devices

C. all devices in selected sites

D. all wired devices

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2/user_guide/b_dnac_ug_1_2/b_dnac_ug_1_2_chapter_01000.html#id_53453

Community vote distribution
C (70%) A (20%) 10%

juliok33p Highly Voted 2 years, 8 months ago
* Answer A is for: Group-Based Access Control
* Answer C is for IP-Based Access Control Policies

Question: Which devices does Cisco Center configure when deploying an "IP-based access control policy"?

ASWER IS CREARLY C
upvoted 31 times

keinokinene Highly Voted 3 years, 3 months ago
correct is A
upvoted 12 times

rggod 2 years, 7 months ago
"...make sure that you have integrated Cisco ISE with Cisco DNA Center. However, Cisco ISE is NOT mandatory if you are adding groups within the Policy > IP Based Access Control > IP Network Groups window while creating a new IP-based access control policy."
upvoted 2 times

doron1122 1 year, 1 month ago
A
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-2/user_guide/b_cisco_dna_center_ug_2_3_2/m_configure-ip-based-access-control-policies.pdf
upvoted 1 times

ihateciscoreally Most Recent 3 months, 1 week ago
sorry cisco but i dont have $80k for checking it myself by buying DNA center deployment :) i came here just to check answer. not covered in OCG of course.
upvoted 1 times

Chiaretta 7 months, 1 week ago
Selected Answer: C
C is correct
upvoted 1 times

HungarianDish 7 months, 3 weeks ago
Selected Answer: C
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-1-0/user_guide/b_cisco_dna_center_ug_1_3_1_0/b_cisco_dna_center_ug_1_3_1_0_chapter_01011.html

As suggested in previous posts.
upvoted 2 times

Dreket 1 year, 4 months ago
Selected Answer: C
The answer is C.

Sites to which a policy is applied. If you configure a wired policy, the policy is applied to all wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/user_guide/b_cisco_dna_center_ug_2_1_2/b_cisco_dna_center_ug_2_1_1_chapter_01100.html#concept_zvk_yg4_p3b
upvoted 3 times

Jared28 1 year, 5 months ago

Selected Answer: A

As per the CCNP: ENCOR: 30-401 CCNP Enterprise: .... Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) official practice exam.
upvoted 1 times

Jared28 1 year, 5 months ago

Upon digging into that thing more, it has a lot of wrong answers, so I'm not certain here now.
upvoted 2 times

AngelPAlonso 1 year, 6 months ago

Selected Answer: B

IP-Based Access Control Policies
An IP-based access control policy controls the traffic going into and coming out of a Cisco device in the same way that an Access Control List (ACL) does. As with an ACL, an IP-based access control policy contains lists of permit and deny conditions that are applied to traffic flows based on various criteria, including protocol type, source IP address, destination IP address, or destination port number.

IP-based access control policies can be used to filter traffic for various purposes, including security, monitoring, route selection, and network address translation
upvoted 1 times

rlilewis 1 year, 6 months ago

Selected Answer: C

Based upon info provided below i'm going for C.
upvoted 1 times

danny_f 1 year, 7 months ago

Looks like C, from the guide - Editing an IP network group on the Policy > IP Based Access Control window is possible without Cisco ISE. But the creation of IP network groups from the IP Based Access Control window requires Cisco ISE.
upvoted 1 times

bara_ken 1 year, 7 months ago

Selected Answer: A

This is A
upvoted 1 times

Hugh_Jazz 2 years, 1 month ago

Answer is C as rggod points out directly from the DNAC Guide:

Workflow to Configure an IP-Based Access Control Policy
Before you begin
To create IP network groups from the Policy > IP Based Access Control > IP Network Groups window, make sure that you have integrated Cisco ISE with Cisco DNA Center. However, Cisco ISE is not mandatory if you are adding groups within the Policy > IP Based Access Control > IP Network Groups window while creating a new IP-based access control policy.
upvoted 1 times

kthekillerc 2 years, 2 months ago

Provided answer is correct
upvoted 1 times

BigMomma4752 2 years, 8 months ago

The correct answer is A.
upvoted 1 times

samirhasanov18 2 years, 11 months ago

A CORRECT
upvoted 3 times

MrBishop 2 years, 11 months ago

The correct answer here is C. all devices in selected sites Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-1-0/user_guide/b_cisco_dna_center_ug_1_3_1_0/b_cisco_dna_center_ug_1_3_1_0_chapter_01011.html Section: Deploy an IP-Based Access Control Policy/Application Policies Explanation: Cisco DNA Center takes all of these parameters and translates them into the proper device CLI commands. When you deploy the policy, Cisco DNA Center configures these commands on the devices defined in the site scope.
upvoted 2 times

onix 2 years, 12 months ago

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-1-0/user_guide/b_cisco_dna_center_ug_1_3_1_0/b_cisco_dna_center_ug_1_3_1_0_chapter_01011.html

Create an IP-Based Access Control Policy
Step 3: Complete the following fields: Site Scope

Sites to which a policy is applied. If you configure a wired policy, the policy is applied to all wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope. For more information, see Site Scope.

Anser: C

upvoted 6 times

Question #342 *Topic 1*

Which tool is used in Cisco DNA Center to build generic configurations that are able to be applied on devices with similar network settings?

A. Command Runner

B. Application Policies

C. Template Editor

D. Authentication Template

Correct Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3/user_guide/b_cisco_dna_center_ug_1_3/b_cisco_dna_center_ug_1_3_chapter_0111.html

Summa Highly Voted 3 years ago

The answer is correct.

updated link is here: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3/user_guide/b_cisco_dna_center_ug_1_3/b_cisco_dna_center_ug_1_3_chapter_0111.html

upvoted 7 times

LM77 Most Recent 1 year, 10 months ago

Answer C

"Cisco DNA Center provides an interactive editor called Template Editor to author CLI templates. Template Editor is a centralized CLI management tool to help design a set of device configurations that you need to build devices in a branch. When you have a site, office, or branch that uses a similar set of devices and configurations, you can use Template Editor to build generic configurations and apply the configurations to one or more devices in the branch"

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3/user_guide/b_cisco_dna_center_ug_1_3/b_cisco_dna_center_ug_1_3_chapter_0111.html

upvoted 3 times

Question #343 *Topic 1*

In which part of the HTTP message is the content type specified?

A. HTTP method

B. body

C. header

D. URI

Correct Answer: *C*
Reference:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Type

LM77 1 year, 10 months ago
Answer C

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Type
upvoted 1 times

examShark 2 years, 6 months ago
The given answer is correct
upvoted 2 times

csalt 3 years, 5 months ago
Layer 3 roaming is similar to Layer 2 roaming in that the controllers exchange mobility messages on the client roam. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains transparent to the wireless client, and the client maintains its original IP address.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/overview.html
upvoted 2 times

youtri 1 year, 11 months ago
what is this !!!!!
what you have written has nothing to do with the question
upvoted 13 times

Question #344 *Topic 1*

An engineer must create an EEM applet that sends a syslog message in the event a change happens in the network due to trouble with an OSPF process. Which action should the engineer use? event manager applet LogMessage event routing network 172.30.197.0/24 type all

A. action 1 syslog msg ג€OSPF ROUTING ERRORג€

B. action 1 syslog send ג€OSPF ROUTING ERRORג€

C. action 1 syslog pattern ג€OSPF ROUTING ERRORג€

D. action 1 syslog write ג€OSPF ROUTING ERRORג€

Correct Answer: *C*

Community vote distribution

A (96%) 4%

Deu_Inder Highly Voted 1 year, 2 months ago

Selected Answer: A

A is correct.
See below.
Only these keywords are available:

Router1(config-applet)#action 1 syslog ?
facility Facility string
filter Filter destination of syslog message
msg Syslog message
priority Priority of syslog message

upvoted 13 times

danman32 Most Recent 4 months ago

syslog pattern is an event you'd be looking for to trigger applying the actions, NOT the actions themselves
So C is clearly wrong

upvoted 2 times

ibogovic 4 months, 4 weeks ago

Selected Answer: A

you need to specify the action to be taken. In this case, the desired action is to send a syslog message. The correct syntax for sending a syslog message is:
action 1 syslog msg <message>
Therefore, the correct command to use in this scenario would be:
action 1 syslog msg OSPF ROUTING ERROR

upvoted 2 times

mrtattoo 6 months, 4 weeks ago

Selected Answer: A

clearly A.

upvoted 1 times

rafaelinho88 10 months ago

Selected Answer: A

The engineer should use the following action in the EEM applet:

event manager applet LogMessage
event routing ospf state change
action 1.0 syslog msg "OSPF process changed in network due to trouble"

This applet will trigger a syslog message whenever a change happens in the OSPF process in the network. The "event routing ospf state change" command will trigger the applet when a change occurs in the OSPF process, and the "action 1.0 syslog msg" will send a syslog message with the specified text.

upvoted 1 times

ittadi 11 months ago

Provided answer is correct

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

!
event manager applet LogMessage
event routing network 2.2.2.2/32 type all

action 1.0 syslog msg "BGP route has been changed"
!

cisco_R5#show ip route 2.2.2.2
Routing entry for 2.2.2.2/32
Known via "bgp 5", distance 20, metric 0
Tag 3, type external
Last update from 192.168.255.22 00:21:19 ago
Routing Descriptor Blocks:
* 192.168.255.22, from 192.168.255.3, 00:21:19 ago
...
cisco_R5#clear ip bgp 3
cisco_R5#
*Dec 20 18:58:12.733: %BGP-3-NOTIFICATION: sent to neighbor 192.168.255.3 6/4 (Administrative Reset) 0 bytes
*Dec 20 18:58:12.738: %BGP-5-ADJCHANGE: neighbor 192.168.255.3 Down User reset
*Dec 20 18:58:12.738: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.255.3 IPv4 Unicast topology base removed from session User reset
cisco_R5#
*Dec 20 18:58:12.739: %HA_EM-6-LOG: LogMessage: BGP route has been changed
*Dec 20 18:58:13.419: %BGP-5-ADJCHANGE: neighbor 192.168.255.3 Up
cisco_R5#
*Dec 20 18:58:13.430: %HA_EM-6-LOG: LogMessage: BGP route has been changed
cisco_R5#

upvoted 2 times

PALURDIN 1 year, 3 months ago

Selected Answer: A

correct answer A

upvoted 4 times

[Removed] 1 year, 3 months ago

Selected Answer: B

I really think it's pattern. check out the dock. We're not looking for an exact message, we are looking for this pattern with the extra information.

upvoted 1 times

nopenotme123 1 year, 3 months ago

A is the only option available for the command. Just verified on our devices.

upvoted 3 times

diegodavid82 2 years, 1 month ago

The provided answer is correct.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-a2.html

upvoted 4 times

dougj 1 year, 1 month ago

The link provided takes you to the action cmd and only shows the msg option - Answer is A and not provided answer!!

upvoted 2 times

Question #345 *Topic 1*

An engineer runs the code against an API of Cisco DNA Center, and the platform returns this output. What does the response indicate?

```
import requests
import sys
import urllib3

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

def main():
    device_uri = "https://192.168.1.1/dna/system/api/v1/auth/token"
    http_result = requests.get(device_uri, auth=("root", "test398555469!"))
    print(http_result)
    if http_result.status_code != requests.codes.ok:
        print("Call failed! Review get_token() .")
        sys.exit()
    print(http_result.json()["Token"])

if _name_ == "_main_":
    sys.exit(main())
```

Output

```
$ python get_token.py
<Response [405]>
Call failed! Review get_token ().
```

A. The authentication credentials are incorrect.

B. The URI string is incorrect.

C. The Cisco DNA Center API port is incorrect.

D. The HTTP method is incorrect.

Correct Answer: *D*

Community vote distribution

D (77%) A (23%)

bogd Highly Voted 1 year, 9 months ago

Selected Answer: A

Token request should be a POST request - see https://developer.cisco.com/docs/dna-center/#!authentication-and-authorization/endpoints-and-methods-used

upvoted 9 times

Cooldude89 Highly Voted 9 months, 1 week ago

Selected Answer: D

The HyperText Transfer Protocol (HTTP) 405 Method Not Allowed response status code indicates that the server knows the request method, but the target resource doesn't support this method.

upvoted 7 times

due Most Recent 3 months ago

Selected Answer: D

Point.
not focus the coding, focus only Response 405.
Some HTTP codes and their meanings;
200 = OK.
201 = Created.
400 = Bad Request.
401 = Unauthorized.
402 = Payment Required.
403 = Forbidden.
404 = Not found.
405 = Method Not Allowed.

upvoted 4 times

djedeen 3 months, 1 week ago

Selected Answer: D

The 405 Method Not Allowed is an HTTP response status code indicating that the server received and recognized the specified request HTTP method, but the server rejected that particular method for the requested resource. This code response confirms that the requested resource is

valid and exists, but the client has used an ***unacceptable HTTP method*** during the request.
upvoted 2 times

myhdtv6 4 months, 2 weeks ago
The HyperText Transfer Protocol (HTTP) 405 Method Not Allowed response status code indicates that the server knows the request method, but the target resource doesn't support this method
upvoted 2 times

MMaris018 7 months, 3 weeks ago
Selected Answer: D
D is correct. It's error 401 if the credentials are incorrect
upvoted 3 times

Dataset 11 months ago
Selected Answer: A
In think A is correct
Regards
upvoted 1 times

sinaghozati 9 months, 2 weeks ago
Invalid authentication credentials would return code 401
upvoted 1 times

milovnik1 11 months, 3 weeks ago
Selected Answer: D
D is correct
Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/405

Invalid authentication credentials would return code 401
upvoted 3 times

bora4motion 1 year ago
Selected Answer: D
to me it looks like D is the answer.
upvoted 2 times

Caradum 1 year ago
HTTP 405 = 'Method not allowed' = Answer D

(A makes no sense. Wrong credentials are HTTP401)
upvoted 4 times

Wooker 1 year, 2 months ago
Selected Answer: D
The token request should be a POST request.

The correct answer is D.
upvoted 2 times

Hugh_Jazz 1 year, 3 months ago
Selected Answer: D
405, Method not allowed is correct.
upvoted 2 times

Dreket 1 year, 4 months ago
Selected Answer: D
The answer is D.

405 Method Not Allowed
The request method is known by the server but is not supported by the target resource. For example, an API may not allow calling DELETE to remove a resource.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Status
upvoted 2 times

pyrokar 1 year, 4 months ago
Selected Answer: D
405 Method Not Allowed
upvoted 1 times

bara_ken 1 year, 7 months ago
Selected Answer: D
This is D
upvoted 2 times

aohashi 1 year, 9 months ago

Selected Answer: D

It should be D

upvoted 2 times

[Removed] 1 year, 9 months ago

Selected Answer: D

Three scenarios in particular can lead to a “Method Not Allowed” error message:

The ban of the corresponding HTTP method is due to a misconfiguration of web servers or software components that are supposed to perform the respective action for the desired URL resource.
The ban of the HTTP method is from the website operator – in most cases, for security reasons. The error lies in a URL resource of the web project in question, on the grounds that its programming requires its method to not be allowed.
The HTTP method is not allowed by the hosting provider of the website operator. This particularly occurs with the POST method, which is required for entering data and is blocked by some providers for security reasons when accessing HTML documents.

https://www.ionos.co.uk/digitalguide/hosting/technical-matters/error-405-method-not-allowed-explanation-and-solutions/

upvoted 2 times

Question #346 *Topic 1*

What are two benefits of YANG? (Choose two.)

A. It enforces the use of a specific encoding format for NETCONF.

B. It collects statistical constraint analysis information.

C. It enables multiple leaf statements to exist within a leaf list.

D. It enforces configuration semantics.

E. It enforces configuration constraints.

Correct Answer: *AE*

Community vote distribution

DE (62%) AE (31%) 8%

kthekillerc Highly Voted 2 years, 2 months ago

Provided answer is correct

upvoted 7 times

ibogovic Highly Voted 4 months, 4 weeks ago

Selected Answer: DE

D. It enforces configuration semantics:
YANG provides a structured and standardized way to define the configuration and operational semantics of network devices. It allows for clear and consistent definitions of data models, specifying how configuration elements relate to each other and what their intended behavior is. This helps ensure that network devices are configured correctly and consistently.

E. It enforces configuration constraints:
YANG allows for the definition of constraints and validation rules on the configuration data. These constraints help ensure that the configuration adheres to specific requirements, such as data type, range, length, and dependencies between configuration elements. By enforcing configuration constraints, YANG helps prevent misconfigurations and improves the overall reliability and stability of the network.

upvoted 5 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Selected Answer: DE

DE is right.

upvoted 1 times

djedeen 3 months, 1 week ago

Selected Answer: DE

D& E: ibogovic's texts are spot on

upvoted 2 times

bob_135 5 months ago

Selected Answer: AE

YANG models can describe constraints to be enforced on the data, restricting the appearance or value of nodes based on the presence or value of other nodes in the hierarchy. These constraints are enforceable by either the client or the server, and valid content MUST abide by them.

https://www.rfc-editor.org/rfc/rfc6020.html

upvoted 2 times

HarwinderSekhon 5 months ago

Selected Answer: AE

A, E seems correct.

upvoted 2 times

jackr76 6 months, 4 weeks ago

Selected Answer: AD

yang is about semantics

https://www.rfc-editor.org/rfc/rfc6020.html

upvoted 1 times

lchabert 1 year, 5 months ago

Multiple answers are corrects ... difficult to choose a best one..

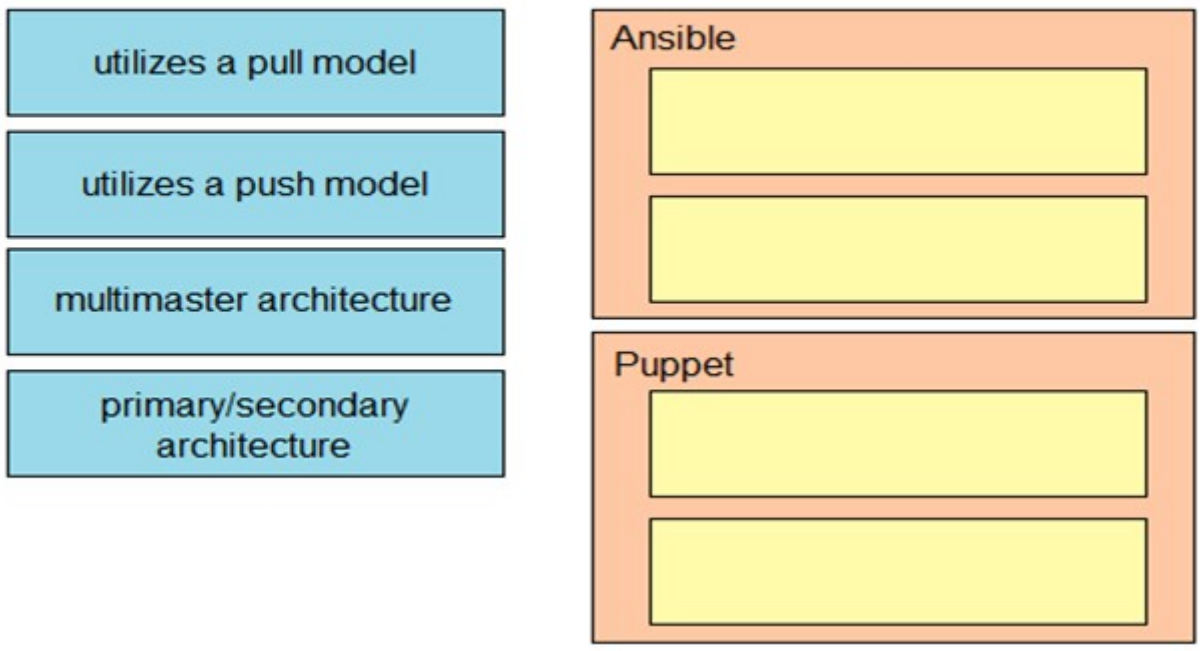
upvoted 2 times

DRAG DROP -

Drag and drop the characteristics from the left onto the orchestration tools they describe on the right.

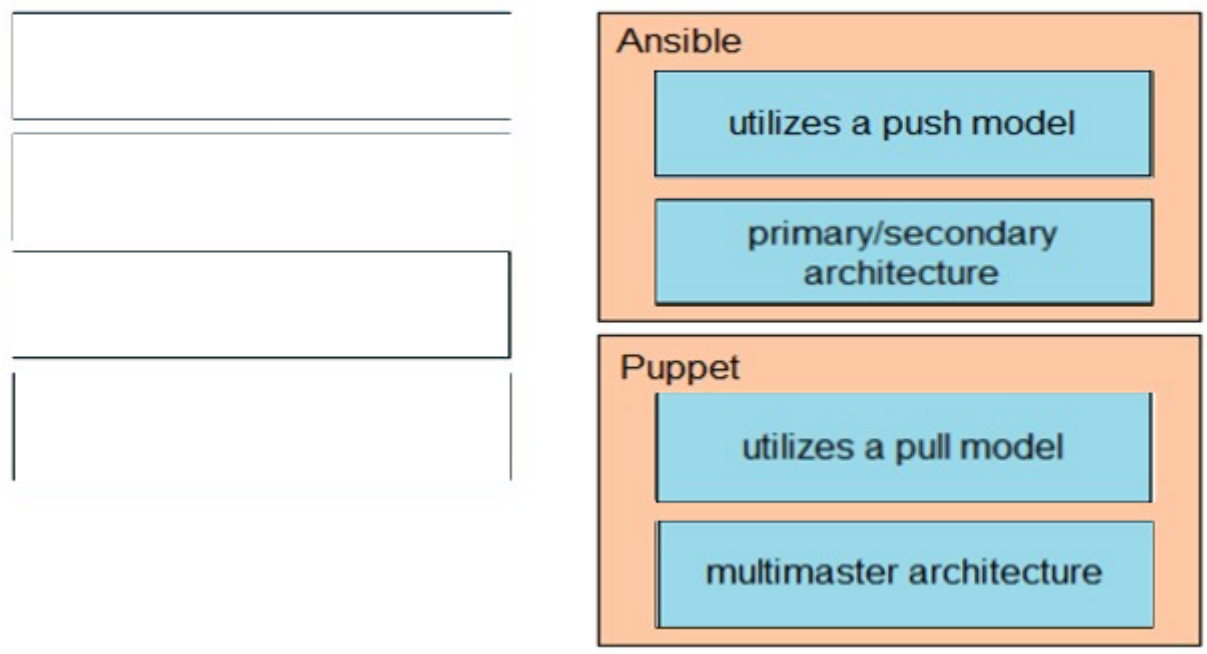
Select and Place:

Answer Area



Correct Answer:

Answer Area



aohashi Highly Voted 1 year, 8 months ago

provided answer is correct.

On Ansible, HA mode is not meant to run in an active/active or multi-master mode.
https://docs.ansible.com/ansible-tower/2.2.0/html/administration/high_availability.html

On Puppet, To scale beyond a certain size, or for geographic distribution or disaster recovery, a deployment may warrant having more than one puppet master server.
https://docs.huihoo.com/puppet/guides/scaling_multiple_masters.html

upvoted 7 times

eddgg Most Recent 2 months, 2 weeks ago

provided answer is correct

upvoted 1 times

due 3 months ago

Ansible = pushes to client.
Chef/puppet = pulls from server.
Ansible = pushes + multi-master.
puppet = pulls + primary/secondary.
#
Answer.
Ansible select.
1. utilizes a pushes model.
2. multi-master architecture.

puppet select.
1. utilizes a pulls model.
2. primary/secondary architecture.

upvoted 1 times

```
import ncclient

with ncclient.manager.connect(host='192.168.1.1', port=830, username='root',
                              password='teset123!', allow_agent=False) as m:
    print(m.get_config('running').data_xml)
```

Refer to the exhibit. After running the code in the exhibit, which step reduces the amount of data that the NETCONF server returns to the NETCONF client, to only the interface's configuration?

A. Use the lxml library to parse the data returned by the NETCONF server for the interface's configuration.

B. Create an XML filter as a string and pass it to get_config() method as an argument.

C. Create a JSON filter as a string and pass it to the get_config() method as an argument.

D. Use the JSON library to parse the data returned by the NETCONF server for the interface's configuration.

Correct Answer: *D*

Community vote distribution

B (100%)

winder Highly Voted 1 year, 5 months ago

Selected Answer: B

First of all, the return data is saved as .xml format;
Then it asks to "reduce amount of data returned" means you need to do the filter before data is downloaded, not after.

B

upvoted 5 times

Wooker Most Recent 1 year, 2 months ago

Selected Answer: B

B is the correct answer.

upvoted 2 times

sanalainen 1 year, 4 months ago

Selected Answer: B

"using the Pythonic approach with ncclient and its get_config() method, has a filter argument where you simply specify the filter type, in this case subtree, along with the XML RPC that you want to get a configuration rpc-reply."

https://yang-prog-lab.ciscolive.com/pod/0/ncclient/get_config

upvoted 4 times

hyjaker 1 year, 7 months ago

Selected Answer: B

The answer should be B to "reduce amount of data returned".

upvoted 2 times

bogd 1 year, 9 months ago

Selected Answer: B

B due to the request to "reduce amount of data returned". Which means filtering at the source, on the network device.

upvoted 3 times

Willy78 1 year, 10 months ago

B is correct answer

D - will not "reduces the amount of data that the NETCONF server returns to the NETCONF client". You will pars date but you will not reduce what server sent

upvoted 4 times

danman32 4 months ago

Not to mention the data returned is in XML format.

upvoted 1 times

Running the script causes the output in the exhibit. Which change to the first line of the script resolves the error?

```
import ncclient

with ncclient.manager.connect(
   host = '192.168.1.1',
   port=830,
   username = 'root',
   password = 'test398101469!',
   allow_agent = False) as m:
   print(m.get_config('running').data_xml)
```

Output

```
$ python get_config.py
Traceback (most recent call last ) :
   File "get_config.py", line 3, in <module>
      with ncclient.manager.connect (host = '192.168.1.1, port = 830, username = 'root',
AttributeError: 'module' object has no attribute 'manager'
```

A. from ncclient import

B. import manager

C. from ncclient import *

D. import ncclient manager

Correct Answer: *C*

Community vote distribution

C (52%) D (43%) 4%

xziomal9 Highly Voted 2 years, 2 months ago

The correct answer is:
C. from ncclient import *

upvoted 15 times

danman32 4 months ago

I tested this. ncclient import * won't work because ncclient is a package, not a module.
Unless the package declares what's included when you use '*' to import the package, nothing is imported. ncclient package doesn't have such a declaration

upvoted 1 times

danman32 4 months ago

The only import/function declaration that worked was:
from ncclient import manager
manager.connect(host=host, port=830, username=user, hostkey_verify=False)

With
from ncclient import manager
ncclient.manager.connect(host=host, port=830, username=user, hostkey_verify=False) did not work, returned that module 'ncclient' had no attribute 'manager'

So because the exhibit has ncclient. as a prefix in the name of the function being called, none of the syntactically valid import methods will work.

upvoted 1 times

wifishark Highly Voted 2 years, 3 months ago

"from ncclient import manager" was the answer
https://github.com/ncclient/ncclient

upvoted 13 times

rlilewis 1 year, 6 months ago

That would be if it were an option, which it's not.

upvoted 3 times

JohnSmithZhao 8 months, 4 weeks ago

but the following:
with ncclient.manager.connect(
need to be changed to:

with manager.connect(
"from ncclient import manager" will work, otherwise it will NOT work.
upvoted 2 times

sihr23 1 year, 1 month ago
This is the correct answer
upvoted 2 times

cracanici 2 years, 2 months ago
So is
from ncclient import *
in this case?
upvoted 4 times

danman32 4 months ago
This won't work because ncclient is a package, not a module. The ncclient package does not include statements to indicate what modules will be imported if you import the package with '*'
upvoted 1 times

Claudiu1 Most Recent 1 day, 16 hours ago
these types of questions are really stupid. Does anyone expect me, as an ENCOR certified technician, to have memorized Python libraries?
upvoted 2 times

mgiuseppe86 2 months, 2 weeks ago
it could be a bad dump paste. I just hope i dont get these questions on my test...
upvoted 1 times

Chuckzero 2 months, 3 weeks ago
The correct answer is D. import ncclient.manager.

There was an omission of dot(.) in that python line statement.

The "import ncclient" is correct in itself, this imports the ncclient library.

The ncclient.manager module provides a higher-level abstraction for managing NETCONF sessions and devices. It simplifies some of the complexities of dealing with NETCONF, such as establishing and managing NETCONF sessions.

Use "import ncclient.manager" when you want to streamline the process of connecting to NETCONF devices and managing sessions as shown in the exhibit.
upvoted 1 times

PureInertiaCopy 3 months, 2 weeks ago
Chat GPT's Response:

It seems like there is a small syntax error in your code. The attribute error is likely due to the incorrect way you're trying to access the manager attribute from the ncclient module. To resolve this, you should import the manager module explicitly from ncclient.

Here's the corrected code with the import statement fixed:

python
Copy code
from ncclient import manager # Import the manager module from ncclient

with manager.connect(
host='192.168.1.1',
port=830,
username='root',
password='test398101469!',
allow_agent=False) as m:
print(m.get_config('running').data_xml) # Fix the method name and parentheses
In this corrected code, I've added the explicit import statement for the manager module from ncclient, and I've also fixed the method name to get_config (removing the extra parenthesis after m.get) to properly request the running configuration data.
upvoted 1 times

HarwinderSekhon 5 months ago
Selected Answer: C
C is correcy
upvoted 1 times

JackDRipper 7 months, 2 weeks ago
The “ncclient.manager” is referenced throughout the code so the correct syntax should be:

import ncclient.manager

Answer D would’ve been correct if there was a period between ncclient and manager. So unless it’s just a typo here, there seems to be no correct answers.
upvoted 2 times

asiansensation 8 months ago

"from" is missing in the answer D, so the answer is C. It is a catch out so be careful.

if it was from ncclient import manager - then D would have been correct.
upvoted 3 times

JohnSmithZhao 8 months, 4 weeks ago
another shit question, none of the option is correct!
upvoted 3 times

mykab 8 months, 4 weeks ago
Selected Answer: D
The best possible answer is D. import ncclient manager
upvoted 1 times

JohnSmithZhao 8 months, 4 weeks ago
has to be "import ncclient.manager"
upvoted 1 times

mellohello 9 months ago
Selected Answer: D
import ncclient manager
upvoted 1 times

Nickplayany 10 months ago
Selected Answer: C
Admin please fix the answer and add the below as correct
from ncclient import manager
upvoted 1 times

MoKhalil 10 months, 3 weeks ago
correct answer is C by trying on python interperter
upvoted 1 times

echipbk 10 months, 4 weeks ago
Selected Answer: C
correct answer is C
upvoted 1 times

Danny_Xu 12 months ago
Selected Answer: C
The answer is C.

"from module_name import * "
All the functions and constants can be imported using *.
upvoted 2 times

Wooker 1 year, 2 months ago
Selected Answer: D
import ncclient.manager
upvoted 3 times

Which line must be added in the Python function to return the JSON object {`cat_9k`: `FXS1932Q2SE`}?

```
import json
def get_data():
    test_json = “””
    {
        “response”: [{
        “managementIpAddress”: “10.10.2.253”,
        “memorySize”: “3398101469”,
        “serialNumber”: “FXS1932Q2SE”,
        “softwareVersion”: “16.3.2”,
        “hostname”: “cat_9k”
       }],
        “version”: “1.0”
}
“””
```

A. return (json.dumps({d['hostname']: d['serialNumber'] for d in json.loads(test_json)['response']}))

B. return (json.dumps({for d in json.loads(test_json)['response']: d['hostname']: d['serialNumber']}))

C. return (json.loads({d['hostname']: d['serialNumber'] for d in json.dumps(test_json)['response'}))

D. return (json.loads({for d in json.dumps(test_json)['response']: d['hostname']: d['serialNumber']}))

Correct Answer: *A*

Community vote distribution

A (88%) 12%

Jared28 Highly Voted 1 year, 5 months ago

Selected Answer: A

Tested as well, A was the only one that functioned.

```
import json

def get_data():
test_json = """
{
"response": [{
"managementipAddress": "10.10.2.253",
"memorySize": "3398345152",
"serialNumber": "FXS1932Q2SE",
"softwareVersion": "16.3.2",
"hostname": "cat_9k"
}],
"version": "1.0"
}
"""
return (json.dumps({d['hostname']: d['serialNumber'] for d in json.loads(test_json)['response']}))

print(get_data())
```

upvoted 9 times

Dre876 Most Recent 2 months, 2 weeks ago

I might as well go take a application programming course at this point.

upvoted 3 times

due 3 months ago

Selected Answer: A

json.loads function for string to object.
json.dumps function for object to string.
question for return object.
Keyword = dumps D for D.

upvoted 1 times

yqpmateo 3 months, 2 weeks ago

Selected Answer: A

json.load method parse a valid JSON string and convert it into a Python dictionary. the test_json variable is a JSON string so the answers that use json.dumps(test_json) are incorrect. Out of the other two, answer A is valid. Here is a python code that proves it:
import json

```
def get_data():
test_json = """
{
"response" : [{
"managementIPAdd":"10.10.10.2",
"memorySize" : "2323232",
"serialNumber" : "FX2342232WWQ",
"softwareVer" : "14.2.3",
"hostname" : "cat_9k"
}],
"vesion":"1.0"
}
"""
for d in json.loads(test_json)['response']:
print(json.dumps({d['hostname']: d['serialNumber']}))
return ( json.dumps({d['hostname']: d['serialNumber'] for d in json.loads(test_json)['response']}))

print(get_data())
```

upvoted 1 times

danman32 4 months ago

I didn't think A or C could be correct because of the position of the 'for d in'

upvoted 1 times

lafrank 7 months, 2 weeks ago

In fact, all answers are incorrect if question is taken literally :-)
B,C and D all contain syntax errors.
While A is syntactically correct, it returns a string and NOT a JSON object as it was stated in the question !

Be careful with print() as it would both print a JSON object and a string object much the same way. Use print(type(get_data()) instead and you would see that the returned value is of type str.

upvoted 3 times

JohnSmithZhao 8 months, 4 weeks ago

json.loads() takes in a string and returns a json object. json. dumps() takes in a json object and returns a string.

upvoted 4 times

Heim_Ox 1 year, 5 months ago

Tested it. A is the correct one that gets the requested output

upvoted 1 times

LeGloupier 1 year, 6 months ago

answer is A
tested, it works as expected
thats a python list comprehension (the list has only one element which is the main dictionary)

upvoted 2 times

Farid77 1 year, 6 months ago

D is the correct answer
... If you have a JSON string, you can parse it by using the json.loads() method.

upvoted 1 times

rlilewis 1 year, 6 months ago

Selected Answer: A

Tested and verified myself. As cvndani said - only A works. All others either give an error:

"for d in" at the start of the { character results in "SyntaxError: invalid syntax"
C returns error "TypeError: string indices must be integers"

upvoted 1 times

bara_ken 1 year, 7 months ago

Selected Answer: B

This is B

upvoted 1 times

bogd 1 year, 9 months ago

Selected Answer: A

A (dictionary comprehension over the JSON contents)

upvoted 3 times

cvndani 1 year, 10 months ago

all options except A give syntax error

upvoted 3 times

VaZi 1 year, 10 months ago

Right answer should be A
json.dumps({d['hostname']: d['serialNum'] for d in json.loads(test_json)['response']})
Checked in Python.
B,D "for d in " - Invalid Syntax
C - Type Error. json.dumps() returns a string, so this syntax is wrong json.dumps(test_json)['response']

upvoted 4 times

pacman64 1 year, 10 months ago

Selected Answer: B

json.loads() method can be used to parse a valid JSON string and convert it into a Python Dictionary

upvoted 1 times

Question #351 *Topic 1*

```
#! /usr/bin/env python3

from env_lab import dnac
import json
import requests
import urllib3
from requests.auth import HTTPBasicAuth
from prettytable import PrettyTable

dnac_devices = PrettyTable(['Hostname','Platform Id','Software Type','Software Version','Up
Time'])
dnac_devices.padding_width = 1
headers = {
            'content-type': "application/json",
            'x-auth-token': ""
          }

def dnac_login(host, username, password):
   url = "https://{}/api/system/v1/auth/token".format(host)
   response = requests.request("POST", url, auth=HTTPBasicAuth(username, password),
                               headers=headers, verify=False)
   return response.json()["Token"]

def network_device_list(dnac, token):
   url = "https://{}/api/v1/network-device".format(dnac['host'])
   headers["x-auth-token"] = token
   response = requests.get(url, headers=headers, verify=False)
   data = response.json()
   for item in data['response']:
      dnac_devices.add_row([item["hostname"],item["platformid"],item["softwareType"],item["soft
wareVersion"],item["upTime"]])
```

Refer to the exhibit. Which code results in the working Python script displaying a list of network devices from the Cisco DNA Center?

A. network_device_list(dnac[λ€hostλ€], dnac[λ€usernameλ€],dnac[λ€passwordλ€]) login = dnac_login(dnac) print(dnac_devices)

B. login = dnac_login(dnac[λ€hostλ€], dnac[λ€usernameλ€], dnac[λ€passwordλ€]) network_device_list(dnac, login) print(dnac_devices)

C. login = dnac_login(dnac[λ€hostλ€], dnac[λ€usernameλ€], dnac[λ€passwordλ€]) network_device_list(dnac, login) for item in dnac_devices: print(dnac_devices.item)

D. network_device_list(dnac[λ€hostλ€], dnac[λ€usernameλ€], dnac[λ€passwordλ€]) login = dnac_login(dnac) for item in dnac_devices: print(dnac_devices.item)

Correct Answer: *C*

Community vote distribution

B (100%)

xdy Highly Voted 2 years ago

A. network_device_list(dnac[host], dnac[username],dnac[password]) login = dnac_login(dnac) print(dnac_devices)
B. login = dnac_login(dnac[host], dnac[username], dnac[password]) network_device_list(dnac, login) print(dnac_devices)
C. login = dnac_login(dnac[host], dnac[username], dnac[password]) network_device_list(dnac, login) for item in dnac_devices: print(dnac_devices.item)
D. network_device_list(dnac[host], dnac[username], dnac[password]) login = dnac_login(dnac) for item in dnac_devices: print(dnac_devices.item)

upvoted 12 times

dragonwise 8 months, 1 week ago

you are a good person. thank you

upvoted 3 times

xziomal9 Highly Voted 2 years, 2 months ago

The correct answer is:
B

upvoted 9 times

xziomal9 2 years, 2 months ago

page 850 from Cert Guide

upvoted 9 times

Saamson 1 year, 5 months ago

Cont. on page 853
Example 28-21
Explanation of the script

upvoted 1 times

due Most Recent 3 months ago

Selected Answer: B

Point.
login = token.
got token by function dnac_login(parameter host,username and password).
got device list by function network_device_list(parameter dnac and token).
got display by function print(dataset dnac_devices).
no need for loop, that is what the pretty table is for.
no "item" under dnac_devices function.
keyword = login -> network_device_list -> print.

upvoted 2 times

Vlad_Is_Love_ua 8 months, 2 weeks ago

Selected Answer: B

token = dnac_login(dnac['host'], dnac['username'], dnac['password'])
network_device_list(dnac, token)
print(dnac_devices)

upvoted 3 times

nopenotme123 1 year, 3 months ago

Selected Answer: B

This question was literally pulled out of the OCG book.

upvoted 2 times

Farid77 1 year, 6 months ago

Selected Answer: B

login = dnac_login(dnac["host"], dnac["username"], dnac["password"])
network_device_list(dnac, login)
print(dnac_devices)

https://github.com/bigevilbeard/dnac-device-info/blob/master/get_dnac_devices.py

upvoted 3 times

snowfox 1 year, 7 months ago

Without Python background, how can we know the answer?

upvoted 3 times

[Removed] 1 year, 7 months ago

no need for loop, that is what the pretty table is for

upvoted 3 times

aohashi 1 year, 9 months ago

Selected Answer: B

It should be B

upvoted 1 times

bogd 1 year, 9 months ago

Selected Answer: B

B. There is no "item" under dnac_devices

upvoted 1 times

TungHuy 1 year, 11 months ago

https://github.com/bigevilbeard/dnac-device-info/blob/master/get_dnac_devices.py

upvoted 3 times

Willy78 1 year, 11 months ago

xziomal9 is right. B is the correct answer.

upvoted 3 times

```
{
  "response": [
    {
      "family": "Routers",
      "interfaceCount": "12",
      "lineCardCount": "9",
      "platformId": "ASR1001-X",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Reachable",
      "hostname": "RouterASR-1",
      "macAddress": "00:c8:8b:80:bb:00",
    },
    {
      "family": "Switches and Hubs",
      "interfaceCount": "41",
      "lineCardCount": "2",
      "platformId": "C9300-24UX",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Authentication Failed",
      "hostname": "cat9000-1",
      "macAddress": "f8:7b:20:67:62:80",
    },
    {
      "family": "Switches and Hubs",
      "interfaceCount": "59",
      "lineCardCount": "2",
      "platformId": "WS-C3850-48U-E",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Unreachable",
      "hostname": "cat3850-1",
      "macAddress": "cc:d8:c1:15:d2:80",
    }
  ],
  "version": "1.0"
}
```


What does the Cisco DNA REST response indicate?

A. Cisco DNA Center has the incorrect credentials for cat3850-1

B. Cisco DNA Center is unable to communicate with cat9000-1

C. Cisco DNA Center has the incorrect credentials for cat9000-1

D. Cisco DNA Center has the incorrect credentials for RouterASR-1

Correct Answer: *C*

Community vote distribution

C (100%)

kthekillerc Highly Voted 2 years, 2 months ago

Provided answer is correct

upvoted 8 times

Tanal2505 Most Recent 1 year, 1 month ago

Surly this the answer is C

"reachabilityStatus";"Authentication Failed",
"hostname":"cat9000-1",

upvoted 3 times

Wanwan 1 year, 3 months ago

The answer is A.
Unreachable: The Device can't connect to Cisco DNA Center, need to correct credentials
Authentication Failed: The device did connected to DNA center but can't determine the device type

upvoted 2 times

Jared28 1 year, 5 months ago

Selected Answer: C

Based on the official practice exam for ENCOR 350-401

upvoted 1 times

Carl1999 2 years ago

A is correct.
incorrect credentials for cat3850-1.
need to respecify the credentials if "reachabilityStatus" is "Unreachable".

upvoted 3 times

Question #353 *Topic 1*

What is a characteristic of YANG?

A. It is a Cisco proprietary language that models NETCONF data.

B. It allows model developers to create custom data types.

C. It structures data in an object-oriented fashion to promote model reuse.

D. It provides loops and conditionals to control flow within models.

Correct Answer: *C*

Community vote distribution

B (62%) C (38%)

Jared28 Highly Voted 1 year, 5 months ago

Selected Answer: C

As per the official study guide/practice exam for 350-401

upvoted 8 times

mgiuseppe86 2 months, 2 weeks ago

At this point I dont even think Cisco understands what YANG does...

upvoted 2 times

PureInertiaCopy Most Recent 3 months, 2 weeks ago

Selected Answer: B

The correct answer is:

B. It allows model developers to create custom data types.

Explanation:

YANG (Yet Another Next Generation) is a data modeling language used to define the structure and semantics of data that is managed by network protocols such as NETCONF (Network Configuration Protocol) or RESTCONF (RESTful Network Configuration Protocol). YANG is not specific to Cisco; it is an industry-standard language used by various networking vendors.

Option A is incorrect because YANG is not a Cisco proprietary language; it is an open standard used by multiple vendors.

Option C is partially correct, as YANG does promote model reuse and modularity through its data structuring approach, but it does not necessarily follow an object-oriented fashion.

Option D is incorrect because YANG does not provide loops and conditionals for controlling flow within models. It is primarily focused on describing the structure and attributes of data, rather than programming logic.

upvoted 1 times

MJane 7 months, 2 weeks ago

Selected Answer: C

- it defines data, not creates.
- and it structures data, doesn't say it's OO

upvoted 1 times

asiansensation 8 months ago

YANG is a data modeling language used to model configuration and state data of network elements, network services, and network protocols. It structures data in a hierarchical tree format similar to object-oriented programming, which promotes model reuse and flexibility.

upvoted 3 times

x3rox 10 months, 1 week ago

Selected Answer: B

The YANG language includes a set of built-in data types. The language also allows, however, the ability for developers to define custom data types.
Source: https://ultraconfig.com.au/blog/learn-yang-full-tutorial-for-beginners/

upvoted 4 times

Rose66 10 months, 3 weeks ago

Selected Answer: B

Seems that the key word is "object-oriented" ... YANG is NOT object-oriented

upvoted 4 times

Rose66 10 months, 3 weeks ago

From RFC6020: "This document describes the syntax and semantics of the YANG language, how the data model defined in a YANG module is represented in the Extensible Markup Language (XML), and how NETCONF operations are used to manipulate the data."

upvoted 2 times

mrtattoo 6 months, 4 weeks ago

object-oriented fashin != object-oriented. In YANG, data is modeled using modules, which are similar to classes in an object-oriented programming language.Modules contain various elements that define the data being modeled, including data types, data nodes, and operations. Data nodes in YANG are similar to objects in an object-oriented programming language, and they can have properties and methods.

upvoted 1 times

WINDSON 11 months ago

Selected Answer: B

https://www.examtopics.com/exams/cisco/350-401/view/36/#

upvoted 1 times

Fadhelben 11 months, 2 weeks ago

Selected Answer: B

From RFC 6020 - YANG:
-YANG structures data models into modules and submodules. (not an object-oriented fashion.)
-YANG defines a set of built-in types, and has a type mechanism through which additional types may be defined.
So I go with B.

upvoted 3 times

milovnik1 11 months, 3 weeks ago

Selected Answer: B

I choose B
"The YANG language includes a set of built-in data types. The language also allows, however, the ability for developers to define custom data types."
Reference:
https://ultraconfig.com.au/blog/learn-yang-full-tutorial-for-beginners/

upvoted 1 times

bara_ken 1 year, 7 months ago

Selected Answer: C

This is C

upvoted 2 times

Marving 1 year, 10 months ago

Selected Answer: B

YANG was developed by IETF so not a Cisco proprietary nor is it an OOP language.
B is correct.

upvoted 4 times

Dedt 1 year, 11 months ago

https://datatracker.ietf.org/doc/html/draft-ietf-netmod-yang-01
YANG strikes a balance between high-level object-oriented modeling and low-level bits-on-the-wire encoding. The reader of a YANG module can easily see the high-level view of the data model while seeing how the object will be encoded in NETCONF operations.

upvoted 1 times

Carl1999 2 years ago

B is correct.
YANG is not an object-oriented fashion.

upvoted 2 times

kthekillerc 2 years, 2 months ago

Provided answer is correct

upvoted 4 times

Question #354 *Topic 1*

DRAG DROP -
Drag and drop the snippets onto the blanks within the code to construct a script that changes the routing from gateway 1 to gateway 2 from 11:00 p.m. to 12:00 a.m. (2300 to 2400) only, daily. Not all options are used, and some options may be used twice.
Select and Place:

Correct Answer: 

Vadkorte Highly Voted 11 months, 1 week ago
Well 10*** is 00:01 which is not 24:00... Daily would be a good option but the correct format is @daily. See https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-e2.html
@daily --An event is triggered once a day. This is the equivalent of specifying 0 0 * * * for the first five fields.
upvoted 5 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago
[event timer] 0 23 [* * *]
[event timer] [1 0 * * *]
read the time backwards
0 23 = 0 minute, 23rd hour (23:00)
1 0 = 1 minute, 0th hour (00:01)
the * * * means day of month, month of year, day of week, since it runs daily, we add a * so it runs every day, since it asks us to run it daily.
upvoted 1 times

XDR 7 months, 3 weeks ago
0 23 * * * --> Everyday at 11:00 PM (23:00)
1 0 * * * --> Everyday at 12:01 AM (00:01)
upvoted 2 times

Bigbongos 10 months, 1 week ago
is this question still on the test?
upvoted 3 times

John13121 10 months, 4 weeks ago
So what is the correct answer ?
instead of *** we have daily, in the first field and why ?
upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago
[event timer] 0 23 [* * *]
[event timer] [1 0 * * *]

read the time backwards
0 23 = 0 minute, 23rd hour (23:00)
1 0 = 1 minute, 0th hour (00:01)
the * * * means day of month, month of year, day of week, since it runs daily, we add a * so it runs every day, since it asks us to run it daily.
upvoted 1 times

KUM_WENG 1 year, 4 months ago
can someone explain this?
upvoted 3 times

snowfox 1 year, 5 months ago
Then, what is the meaning of 10***??? Please respond. Thanks.
upvoted 1 times

Heim_Ox 1 year, 5 months ago
10*** means 1 minute after 0 hour regardless of what day or month it is
abcde
a=minute (0-59)
b=hour (0-23)
c=day of month (1 - 31)
d=month (1 - 12) January is 1
e=day of week (0 - 6) Sunday is 0
upvoted 14 times

Amansoor79 2 years ago
Cron entry "0 23 * * *" means "minute hour dom dow"
dom = day of the month
dow = day of the week

Examples:

01 * * * * This command is run at one min past every hour
17 8 * * * This command is run daily at 8:17 am

upvoted 3 times

bogd 1 year, 9 months ago

Actually, it is "minute hour dom MONTH dow". Other than that, everything else is correct.

upvoted 4 times

Question #355 *Topic 1*

```
ip sla 10

icmp-echo 192.168.10.20

timeout 500

frequency 3

ip sla schedule 10 life forever start-time now
track 10 ip sla 10 reachability
```

Refer to the exhibit. The IP SLA is configured in a router. An engineer must configure an EEM applet to shut down the interface and bring it back up when there is a problem with the IP SLA. Which configuration should the engineer use?

A. event manager applet EEM_IP_SLA event track 10 state down

B. event manager applet EEM_IP_SLA event track 10 state unreachable

C. event manager applet EEM_IP_SLA event sla 10 state unreachable

D. event manager applet EEM_IP_SLA event sla 10 state down

Correct Answer: *A*

Community vote distribution

A (100%)

nushadu Highly Voted 11 months, 2 weeks ago

Selected Answer: A

```
!
ip sla 1
icmp-echo 2.2.2.2 source-interface Loopback0
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1 reachability
!
event manager applet Q_355_shut_port
event track 1 state down
action 1.0 cli command "enable"
action 2.0 cli command "conf t"
action 3.0 cli command "int loo1"
action 4.0 cli command "shut"
action 5.0 syslog msg "Loo1 was shutdown"
!
event manager applet Q_355_no_shut_port
event track 1 state up
action 1.0 cli command "enable"
action 2.0 cli command "conf t"
action 3.0 cli command "int loo1"
action 4.0 cli command "no shut"
action 5.0 syslog msg "Loo1 was enabled"
!
```

upvoted 7 times

nushadu 11 months, 2 weeks ago

actually this shit works (on the remote side I disabled\enabled ICMP):

```
cisco_R5#
*Dec 20 21:03:01.258: %TRACK-6-STATE: 1 ip sla 1 reachability Up -> Down
cisco_R5#
*Dec 20 21:03:01.730: %HA_EM-6-LOG: Q_355_shut_port: Loo1 was shutdown
cisco_R5#
*Dec 20 21:04:01.313: %TRACK-6-STATE: 1 ip sla 1 reachability Down -> Up
cisco_R5#
*Dec 20 21:04:01.783: %HA_EM-6-LOG: Q_355_no_shut_port: Loo1 was enabled
cisco_R5#
*Dec 20 21:04:03.709: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
cisco_R5#
*Dec 20 21:04:03.710: %HA_EM-6-LOG: boom: logging directly to console
*Dec 20 21:04:04.711: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
*Dec 20 21:04:04.712: %HA_EM-6-LOG: boom: logging directly to console
cisco_R5#
```

upvoted 5 times

[Removed] Most Recent 1 year, 7 months ago

Selected Answer: A

The state of the tracked object is either up or down

upvoted 4 times

Carl1999 2 years ago

A is correct.

upvoted 1 times

Refer to the exhibit.

```
list = [1, 2]
list = list * 3
print(list)
```

What is the value of the variable list after the code is run?

A. [1, 2], [1, 2], [1, 2]

B. [1, 2] * 3

C. [1, 2, 1, 2, 1, 2]

D. [3, 6]

Correct Answer: *C*

Community vote distribution

C (100%)

Willy78 Highly Voted 1 year, 10 months ago

Right. Correct answer is C:

```
>>> list = [1, 2]
>>> list = list * 3
>>> print (list)
[1, 2, 1, 2, 1, 2]
```

upvoted 15 times

jason2626 1 year, 3 months ago

Tested as well.

upvoted 2 times

Anilr Highly Voted 1 year, 11 months ago

Correct answer C.

upvoted 8 times

eww_cybr Most Recent 4 months, 4 weeks ago

The code multiplies the list by 3, resulting in the list elements being repeated three times.

```
my_list = [1, 2]
my_list = my_list * 3
print(my_list)
```

The output will be [1, 2, 1, 2, 1, 2], which is the original list [1, 2] repeated three times.

upvoted 2 times

mdawg 1 year, 3 months ago

Selected Answer: C

Ran it through python, should be C

upvoted 2 times

Edwinmolinab 1 year, 4 months ago

Selected Answer: C

according at https://en.wikibooks.org/wiki/Python_Programming/Lists
C is more appropriate

upvoted 3 times

[Removed] 1 year, 7 months ago

Selected Answer: C

Answer C is valid

upvoted 3 times

[Removed] 1 year, 9 months ago

Selected Answer: C

I agree
upvoted 3 times

bogd 1 year, 9 months ago

Selected Answer: C

C - list multiplication
upvoted 3 times

Question #357 *Topic 1*

Refer to the exhibit.

```
psswd = (base64.b64decode('SzFwM001RzchCg==').decode('utf-8')).strip('\n')
d = datetime.date.today()
date = str(10000*d.year + 100*d.month + d.day)
```

Which result does the Python code achieve?

A. The code encrypts a base64 decrypted password.

B. The code converts time to the Epoch LINUX time format.

C. The code converts time to the "year/month/day" time format.

D. The code converts time to the yyyymmdd representation.

Correct Answer: *D*

Community vote distribution

D (100%)

[Removed] Highly Voted 5 months, 1 week ago

Selected Answer: D

I'm very green when it comes to this programming stuff, so I had to sit for a bit and really dig down to grasp the concept. For those like me or not:
YEAR = 2022 * 10000 = 20220000
MONTH = 01 * 100 = 100
DAY = 09

PRINT
20220000
+ 100
+ 09

20220109 = YYYYMMDD

upvoted 9 times

pacman64 Highly Voted 1 year, 10 months ago

Selected Answer: D

print(str(10000*d.year + 100*d.month + d.day))
20220109

upvoted 7 times

Labedu_Singh 1 year, 9 months ago

>>> import datetime
>>> d = datetime.date.today()
>>> print(d)
2022-02-17
>>> print(str(10000*d.year + 100*d.month + d.day))
20220217
>>>

upvoted 3 times

shefo1 Most Recent 2 days, 1 hour ago

Selected Answer: D

easy explain for three lines :

It decodes a base64-encoded string, removes newline characters, gets the current date, and then creates a string representation of the date in the format "yyyymmdd". Therefore, the correct answer is:

D.

upvoted 1 times

abcdabcd666 4 months, 1 week ago

This code is disgusting

upvoted 4 times

myhdtv6 4 months, 2 weeks ago

Guys listen to me if you feel that makes sense if you don't have a Programming knowledge and wants to solve this for the sake of exam.

see the very last line in question "date=str(.....)"

there is + + + in btwn

and outside the bracket there is a string

string is a not a number (integer), string could be anything , like a word or alphabets or characters,

and remember, whenever there is a string and you see + + +,

THAT SIMPLY MEANS IT WILL MAKE THE WHOLE WORD SIT TOGTHER WITH EACH OTHER WITHOUT DOING ANY "ADDTITION", + + + IS TO COMBINE THE THE LETTERS OR WHATEVER IS GIVEN, NOT TO EXECUTE ADDITION

NOW CHECK THE OPTIONS...

D. has YYYYMMDD, means combination of String and + make it sit together.

I hope it is understandable

upvoted 5 times

[Removed] 1 year, 7 months ago

Selected Answer: D

D is valid answer

upvoted 1 times

ElJetiIngeniero 1 year, 8 months ago

Selected Answer: D

Tried this in python, answer is D

upvoted 1 times

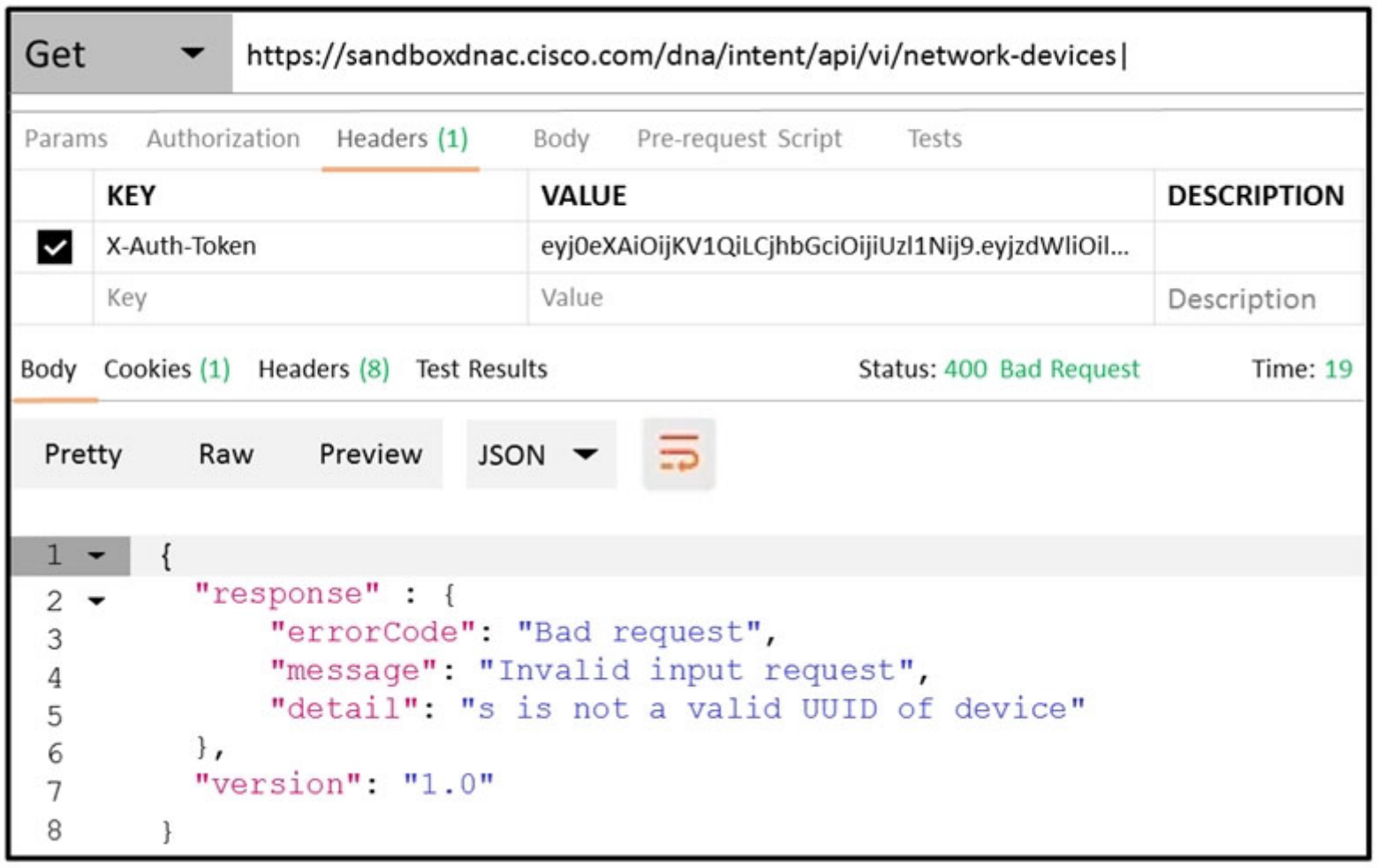
aohashi 1 year, 9 months ago

Selected Answer: D

It should be D

upvoted 1 times

Refer to the exhibit.



POSTMAN is showing an attempt to retrieve network device information from Cisco DNA Center API. What is the issue?

A. The URI string is incorrect.

B. The token has expired.

C. Authentication has failed.

D. The JSON payload contains the incorrect UUID.

Correct Answer: *A*

Community vote distribution

A (61%) D (39%)

VaZi Highly Voted 1 year, 10 months ago

Selected Answer: D

It should be D. The JSON payload contains the incorrect UUID.
400 - "The client made a request that the server could not understand (for example, the request syntax is incorrect)."
https://developer.cisco.com/docs/dna-center/#!get-module-info-by-id
A - 404 - Not found (Wrong URL)
B,C - 401 - Not authenticated

upvoted 16 times

Zizu007 Highly Voted 1 year ago

Selected Answer: A

With 's'
GET https://DNAC:Port//dna/intent/api/v1/network-devices
{
"response": {
"errorCode": "Bad request",
"message": "Invalid input request",
"detail": "s is not a valid UUID of device"
},
"version": "1.0"
}

without 's'
GET https://DNAC:Port//dna/intent/api/v1/network-device
{
"response": [
{

"type": "Cisco 3504 Wireless LAN Controller",
"description": "Cisco Controller Wireless Version:8.5.140.0",
"serialNumber": "FOL25040021",
---------- lines omitted ----------

upvoted 13 times

CCNPWILL 1 month, 2 weeks ago

... Which means the URI is incorrect. Answer is A.

upvoted 1 times

Adnan5252 Most Recent 3 months ago

asking these type of question is not right from the cisco they should give full information or full access

upvoted 1 times

djedeen 3 months, 1 week ago

Selected Answer: A

Tricky one: 's' at the end of 'network-device' is incorrect, hence the message text 's is not ...'
GET /dna/intent/api/v1/network-device/<device_id>
** note no s **

upvoted 1 times

PureInertiaCopy 3 months, 2 weeks ago

ChatGPT:

It looks like you've provided a JSON-formatted response. Is there something specific you would like to know or discuss about this JSON response? Please provide more context or ask a question, and I'll be happy to assist you.

Me:
Does that mean the JSON payload contains the incorrect UUID?

ChatGPT:
Yes, based on the provided JSON payload, it appears that the response is indicating that the input request contains an invalid UUID (Universally Unique Identifier) for a device. The "errorCode" is set to "Bad request," and the "message" provides the description "Invalid input request," with additional details mentioning that the provided UUID "s" is not a valid UUID for a device.

This suggests that the UUID "s" is not recognized as a valid identifier for a device in the context of the system or service that generated this response.

upvoted 1 times

Adnan5252 3 months ago

dont ask chapgpt they dumb as hell they just make talk like ok you are right yeah yeah you are right ok does this right ? yeah you saying right so dont chat gt

upvoted 1 times

Muste 5 months ago

at the end of the URl there is "|" if you remove it everything is ok

upvoted 2 times

mgiuseppe86 2 months, 2 weeks ago

No, i believe that is the typing indicator and the person who took the screenshot had their tpying indicator there while it was blinking on. So A is a BS answer

upvoted 1 times

msstanick 5 months ago

Selected Answer: A

That's another sneaky question as actually both A & D are correct. It is just a matter of what is the root cause and A is as it triggers D. I mean, using an incorrect URI with 's' causes JSON payload to use the UUID of 's' which is incorrect so we get error 400 insread of error 404.

upvoted 1 times

Rose66 10 months, 3 weeks ago

Selected Answer: A

The HyperText Transfer Protocol (HTTP) 400 Bad Request response status code indicates that the server cannot or will not process the request due to something that is perceived to be a client error (for example, malformed request syntax, invalid request message framing, or deceptive request routing). (Source:https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/400)

upvoted 1 times

M_Abdulkarim 1 year, 3 months ago

Selected Answer: D

I think answer is D,
if URL is incorrect then we should get 404

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

No, i believe that is the typing indicator and the person who took the screenshot had their typing indicator there while it was blinking on. So A is a BS answer

upvoted 1 times

nopenotme123 1 year, 3 months ago

Wrong. Its A. 400 Bad reqest : The server cannot or will not process the request due to something that is perceived to be a client error (e.g., malformed request syntax, invalid request message framing, or deceptive request routing).

This is also taken right out of the book.

upvoted 2 times

d3iyu 1 year, 4 months ago

Selected Answer: A

GET /dna/intent/api/v1/network-device

upvoted 2 times

dancer1234 1 year, 4 months ago

Selected Answer: A

This is a GET, there is no JSON body

upvoted 3 times

johnmcclane78 1 year, 4 months ago

Correct URI:
GET /dna/intent/api/v1/network-device
GET /dna/intent/api/v1/network-device/<device_id>
Source: https://developer.cisco.com/docs/dna-center/#!devices/endpoints-and-methods-used
So, A looks correct

upvoted 2 times

Jared28 1 year, 5 months ago

Selected Answer: A

As per guide CCNP Enterprise 350-401 ENCOR Cisco Certified Network Professional

upvoted 1 times

winder 1 year, 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

riccardorossi 1 year, 5 months ago

The final "s" of url "/network-devices" is interpreted as UUID ((should be /network-device/), so the correct answer is A.

upvoted 2 times

DLLLLLLLL 1 year, 6 months ago

Selected Answer: A

... api/v1/network-device/"+id+"/config"

upvoted 2 times

[Removed] 1 year, 7 months ago

the uuid is part of the URI string

upvoted 1 times

Refer to the exhibit.

Script

```
import ncclient

with ncclient.manager.connect(host='192.168.1.1', port=830, username='root', password='test123!",
       allow_agent=False) as m:
         print(m.get_config('running').data_xml)
```

Output

```
$ python get_config.py
Traceback (most recent call last):
     File "get_config.py", line 3, in <module>
       with ncclient.manager.connect(host='192.168.1.1', port=830, username='root',
          AttributeError: 'module' object has no attribute 'manager'
```

Running the script causes the output in the exhibit. What should be the first line of the script?

A. from ncclient import manager

B. import manager

C. from ncclient import *

D. ncclient manager import

Correct Answer: *A*

Community vote distribution

A (84%) C (16%)

cvndani Highly Voted 1 year, 10 months ago

Selected Answer: A

I think that the correct answer is A

upvoted 6 times

HarwinderSekhon Most Recent 5 months ago

Selected Answer: A

A AND C ARE CORRECT BUT A IS MORE SPECIFIC.

upvoted 1 times

danman32 5 months, 1 week ago

This is a confusing aspect of Python.
ncclient isn't a module but rather a package that contains the module manager (manager.py)
The question is, would you get an error that the module could not be found if you only imported the package even if you called the function by its full package.module.function()?
If so, then you would need "from ncclient import manager"
Or you could 'import ncclient.manager" in which case when calling connect(), you would need the full path.
https://www.programiz.com/python-programming/package

upvoted 1 times

XDR 7 months, 3 weeks ago

Selected Answer: A

It's a little bit tricky, you don't have to remove the first line:
from ncclient import manager
import ncclient

This way works, so answer is A

upvoted 2 times

M_Abdulkarim 1 year, 3 months ago

Selected Answer: A

I think Both A and C are correct, but import * will import unnecessary modules

upvoted 3 times

rlilewis 1 year, 6 months ago

Selected Answer: A

https://ncclient.readthedocs.io/en/latest/
Multiple examples shown using "from ncclient import manager" and then using manager.connect
upvoted 3 times

rettich 1 year, 9 months ago

Selected Answer: A
See Link from CHGclimber
upvoted 1 times

bogd 1 year, 9 months ago

No answer seems correct - a "from" import would require "with manager.connect", but the code uses "with ncclient.manager.connect".
upvoted 3 times

CHGclimber 1 year, 9 months ago

I would recommend A:
https://developer.cisco.com/codeexchange/github/repo/ncclient/ncclient/
upvoted 3 times

danman32 4 months ago

Problem though is that with A, the snippet "with ncclient.manager.connect" would have to be "with manager.connect", which is what the github example has.
upvoted 1 times

Trust48 1 year, 10 months ago

Selected Answer: C
provided answer is correct
upvoted 3 times

Question #360 *Topic 1*

Refer to the exhibit.

```
event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.3 get-type next entry-op gt entry-
val 80 poll-interval 5
!
action 1.0 cli command "enable"
action 2.0 syslog msg "high cpu"
action 3.0 cli command "term length 0"
```

An engineer must create a script that appends the output of the show process cpu sorted command to a file. Which action completes the configuration?

A. action 4.0 syslog command "show process cpu sorted | append flash:high-cpu-file"

B. action 4.0 cli command "show process cpu sorted | append flash:high-cpu-file"

C. action 4.0 cns-event "show process cpu sorted | append flash:high-cpu-file"

D. action 4.0 publish-event "show process cpu sorted | append flash:high-cpu-file"

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-a2.html

Stylar 10 months, 2 weeks ago

https://community.cisco.com/t5/networking-knowledge-base/cisco-eem-basic-overview-and-sample-configurations/ta-p/3148479
upvoted 2 times

Ioannis34 11 months ago

provided answer is correct
upvoted 2 times

Question #361 *Topic 1*

What is an advantage of utilizing data models in a multivendor environment?

A. lowering CPU load incurred to managed devices

B. improving communication security with binary encoded protocols

C. facilitating a unified approach to configuration and management

D. removing the distinction between configuration and runtime state data

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/routers/ncs6000/software/ncs6k-7-4/programmability/configuration/guide/b-programmability-cg-ncs6000-74x/m- unified-data-models.pdf

Community vote distribution

C (100%)

mahnazmohamz 1 month, 4 weeks ago

Selected Answer: C

correct

upvoted 1 times

robi1020 11 months, 3 weeks ago

Selected Answer: C

Correct

upvoted 3 times

Question #362 *Topic 1*

How is a data modeling language used?

A. To enable data to be easily structured, grouped, validated, and replicated.

B. To represent finite and well-defined network elements that cannot be changed.

C. To model the flows of unstructured data within the infrastructure.

D. To provide human readability to scripting languages.

Correct Answer: *A*

Community vote distribution

A (100%)

Sajj_gabi Highly Voted 2 years, 9 months ago

A is the correct one any comments

upvoted 24 times

raizer 2 years, 1 month ago

A:
Data models enable data to be easily structured, grouped, and replicated to represent information related to network devices, features, and solutions.

from:
https://developer.cisco.com/docs/nx-os/#!the-nature-of-data-models

upvoted 6 times

Satekhi Most Recent 1 year, 4 months ago

Data models enable data to be easily structured, grouped, and replicated to represent information related to network devices, features, and solutions.

https://developer.cisco.com/docs/nx-os/#!the-nature-of-data-models

upvoted 2 times

Jared28 1 year, 5 months ago

Selected Answer: A

As per the practice exam in: CCNP: ENCOR: 350-401: CCNP ENTERPRISE: Cisco Certified Network Professional: Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)

upvoted 1 times

AlbertoStu 1 year, 8 months ago

Selected Answer: A

https://developer.cisco.com/docs/nx-os/#!the-nature-of-data-models

upvoted 1 times

ElJetiIngeniero 1 year, 8 months ago

Selected Answer: A

It should be A

upvoted 1 times

PSYPHA1 1 year, 8 months ago

YANG was developed by the IETF NETCONF Data Modeling Language Working Group (NETMOD) to be easily read by humans and as of this writing,
https://whatis.techtarget.com/definition/YANG-data-modeling-language

upvoted 1 times

laterst 1 year, 8 months ago

Selected Answer: A

going for A on this one.
Human readable is classic CLI (arguably :D), data modelling languages make data readable and modifiable for systems, where structure, goruping and replication is key. You don't want to parse human-readable text for information, you want a clear structure to directly reference what you're looking for. A

upvoted 2 times

aohashi 1 year, 9 months ago

Selected Answer: A

It should be A

upvoted 1 times

bogd 1 year, 9 months ago

Selected Answer: A

A - see raizer's comment for docs link

upvoted 1 times

KiraShane 1 year, 9 months ago

I will go D.
For me, the question is mainly talking about "language" firstly, so scripting should be the purpose.

upvoted 1 times

xziomal9 2 years, 2 months ago

The correct answer is:
A. To enable data to be easily structured, grouped, validated, and replicated.

upvoted 1 times

Rockford 2 years, 6 months ago

How is it use? A
Why is it used? D
Therefore in this instance it is A.

upvoted 2 times

BigMomma4752 2 years, 8 months ago

The correct answer is D.

upvoted 1 times

Jclemente 2 years, 8 months ago

I agree with A...

upvoted 1 times

Paco_SP 2 years, 8 months ago

If the question is about YANG, maybe D is the best answer.

Yet Another Next Generation (YANG) data modeling language.
YANG is a data modeling language used to describe configuration and operational data, remote procedure calls and notifications for network devices. The salient features of YANG are:

Human-readable format, easy to learn and represent
Supports definition of operations
Reusable types and groupings
Data modularity through modules and submodules
Supports the definition of operations (RPCs)
Well-defined versioning rules
Extensibility through augmentation

upvoted 2 times

WhatNot 2 years, 9 months ago

Agree, should be A

upvoted 2 times

Sajj_gabi 2 years, 9 months ago

I think its A

upvoted 3 times

Question #363 *Topic 1*

A network engineer is configuring OSPF on a router. The engineer wants to prevent having a route to 172.16.0.0/16 learned via OSPF in the routing table and configures a prefix list using the command ip prefix-list OFFICE seq 5 deny 172.16.0.0/16. Which two additional configuration commands must be applied to accomplish the goal? (Choose two.)

A. ip prefix-list OFFICE seq 10 permit 0.0.0.0/0 le 32

B. distribute-list prefix OFFICE in under the OSPF process

C. distribute-list OFFICE in under the OSPF process

D. distribute-list OFFICE out under the OSPF process

E. ip prefix-list OFFICE seq 10 permit 0.0.0.0/0 ge 32

Correct Answer: *AB*

Community vote distribution

AB (88%) 12%

[Removed] Highly Voted 5 months, 1 week ago

Selected Answer: AB

when referencing a prefix-list, you need to specify that its a prefix you are referencing, without the keyword prefix, you'll be referencing an ACL

upvoted 5 times

HarwinderSekhon 5 months ago

Yes. ACL vs Prefix.

upvoted 1 times

djedeen Most Recent 3 months, 1 week ago

Selected Answer: AB

permit 0.0.0.0/0 le 32 -> all networks (subnet mask of /32 or smaller, e.g. everything).

upvoted 2 times

nikramor 6 months, 1 week ago

Selected Answer: AB

Given answer is correct

upvoted 1 times

bendarkel 9 months ago

Selected Answer: AB

Correct answers: A and B

upvoted 2 times

TSKARAN 10 months, 2 weeks ago

CORRECT Answer: AB

vIOS-R1(config)#router ospf 10
vIOS-R1(config-router)#dis?
discard-route distance distribute-list

vIOS-R1(config-router)#distr
vIOS-R1(config-router)#distribute-list ?
<1-199> IP access list number
<1300-2699> IP expanded access list number
WORD Access-list name
gateway Filtering incoming updates based on gateway
prefix Filter prefixes in routing updates
route-map Filter prefixes based on the route-map

vIOS-R1(config-router)#distribute-list pre
vIOS-R1(config-router)#distribute-list prefix ?
WORD Name of an IP prefix-list

vIOS-R1(config-router)#distribute-list prefix OFFICE ?
gateway Filtering incoming updates based on gateway
in Filter incoming routing updates
out Filter outgoing routing updates

vIOS-R1(config-router)#distribute-list prefix OFFICE

upvoted 4 times

kewokil120 11 months ago

Selected Answer: AB

I like ab

upvoted 3 times

nushadu 11 months, 2 weeks ago

Selected Answer: AB

pay attention to 172.16.13.0/24 & 172.16.113.0/24 netw (they'll disappear in the end)

```
sw1(config-router)#do s run | s router ospf 1
router ospf 1
passive-interface default
no passive-interface Vlan10
network 0.0.0.0 255.255.255.255 area 0
sw1(config-router)#
sw1(config-router)#do s ip rou ospf | b Gate
Gateway of last resort is 192.168.255.1 to network 0.0.0.0

3.0.0.0/32 is subnetted, 1 subnets
O 3.3.3.3 [110/2] via 192.168.255.3, 00:00:17, Vlan10
172.16.0.0/24 is subnetted, 2 subnets
O 172.16.13.0 [110/11] via 192.168.255.3, 00:00:17, Vlan10 <<<<<<<<<<<<<< remove it
O 172.16.113.0 [110/11] via 192.168.255.3, 00:00:17, Vlan10 <<<<<<<<<<<<<<< remove it
sw1(config-router)#
sw1(config-router)#do s runn | s pref
ip prefix-list PL_1 seq 10 deny 172.16.13.0/24
ip prefix-list PL_1 seq 11 deny 172.16.113.0/24
ip prefix-list PL_1 seq 20 permit 0.0.0.0/0 le 32
sw1(config-router)#
```

upvoted 1 times

nushadu 11 months, 2 weeks ago

```
sw1(config-router)#distribute-list prefix PL_1 in
sw1(config-router)#
sw1(config-router)#do s ip rou ospf | b Gate
Gateway of last resort is 192.168.255.1 to network 0.0.0.0

3.0.0.0/32 is subnetted, 1 subnets
O 3.3.3.3 [110/2] via 192.168.255.3, 00:00:03, Vlan10
sw1(config-router)#

### rollback

sw1(config-router)#
sw1(config-router)#no distribute-list prefix PL_1 in
sw1(config-router)#
sw1(config-router)#do s ip rou ospf | b Gate
Gateway of last resort is 192.168.255.1 to network 0.0.0.0

3.0.0.0/32 is subnetted, 1 subnets
O 3.3.3.3 [110/2] via 192.168.255.3, 00:00:02, Vlan10
172.16.0.0/24 is subnetted, 2 subnets
O 172.16.13.0 [110/11] via 192.168.255.3, 00:00:02, Vlan10
O 172.16.113.0 [110/11] via 192.168.255.3, 00:00:02, Vlan10
sw1(config-router)#
```

upvoted 1 times

Xerath 11 months, 2 weeks ago

Selected Answer: AB

A & B are 100% correct.

upvoted 1 times

jucevabe 1 year, 2 months ago

AyB tested in GNS3

upvoted 2 times

jucevabe 1 year, 2 months ago

```
R1(config-router)#distri
R1(config-router)#distribute-list ?
<1-199> IP access list number
<1300-2699> IP expanded access list number
WORD Access-list name
gateway Filtering incoming updates based on gateway
prefix Filter prefixes in routing updates
route-map Filter prefixes based on the route-map

R1(config-router)#distribute-list pref
R1(config-router)#distribute-list prefix OFFICE
% Incomplete command.
```

R1(config-router)#distribute-list prefix OFFICE ?
gateway Filtering incoming updates based on gateway
in Filter incoming routing updates
out Filter outgoing routing updates

R1(config-router)#distribute-list prefix OFFICE in
R1(config-router)#
R1#
*Sep 15 15:23:26.891: %SYS-5-CONFIG_I: Configured from console by console
R1#

EN GNS3 router 7200

upvoted 1 times

greencafe24 1 year, 2 months ago

Selected Answer: AC

Wrong answer. AC is correct. Command B doesn't exist.

Router(config)#router ospf 1
Router(config-router)#distribute-list test ?
in Filter incoming routing updates
out Filter outgoing routing updates

upvoted 2 times

greencafe24 1 year, 2 months ago

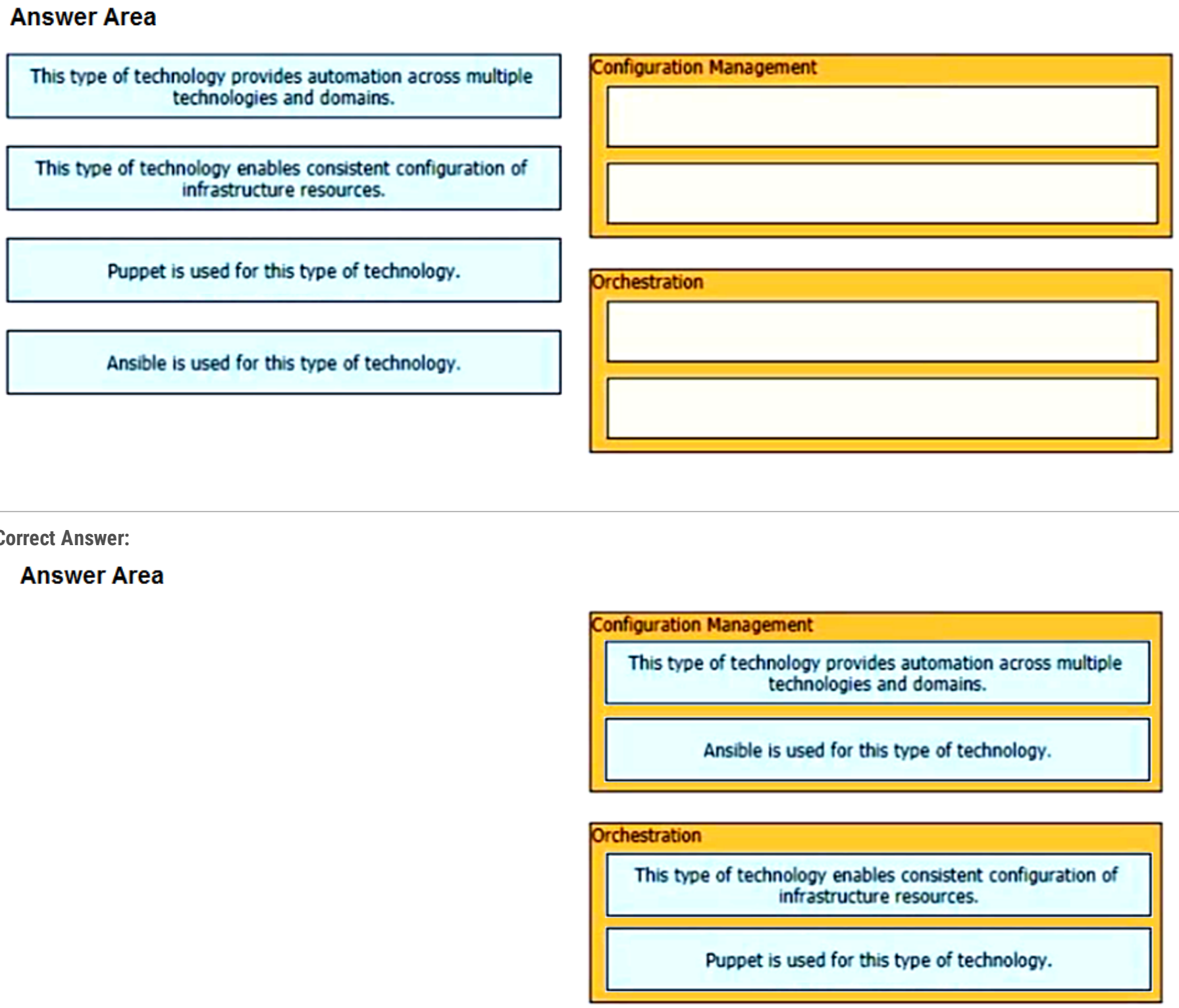
Forget what I said, I don't know how to remove my comment.
AB is correct.

upvoted 6 times

DRAG DROP -

Drag and drop the characteristics from the left onto the technology types on the right.

Select and Place:



Correct Answer:

gibblock Highly Voted 7 months, 3 weeks ago

Configuration Management
- this type ... enables consistent configuration of infrastructure resources
- ansible
Orchestration
- this type ... across multiple technologies and domains
- puppet

OCG Page 886. Puppet Bolt - Orchestrator-driven tasks

upvoted 16 times

amir5498 Highly Voted 7 months, 4 weeks ago

1. Configuration Management:
- Puppet is used for this type of technology
- This type of technology enables consistent configuration of infrastructure resources.
2. Orchestration:
- This type of technology provides automation across multiple technologies and domains
- Ansible is used for this type of technology

upvoted 13 times

Toto1 Most Recent 6 days, 7 hours ago

How is Puppet Different from Ansible?
Among other differences (see below), Puppet uses declarative automation – that means you tell Puppet your desired configurations and Puppet will figure out how to get there. Ansible uses imperative automation, which means you lay out the steps required to get to that desired state instead of the tool figuring it out.

https://www.puppet.com/blog/ansible-vs-puppet#faq

upvoted 1 times

jackr76 6 months, 4 weeks ago

Ansible (CLI tool)
Desired State / Declarative
Agent-less
procedural - Hybrid met declarative
push the configuration to the client.
uses playbooks (cfg/yaml)
primary/secondary architecture
"automation"
win-update demo bas: agentless
Intent-based
Puppet (CLI tool)
Desired State / Declarative
Agent-Based
Active/passive - replicate data to other server
Manifests
Multimaster architecture
Asses impact before applying

upvoted 2 times

eojedad 8 months ago

here two links with info, but not clear about puppet or ansible

https://www.linkedin.com/pulse/understanding-terms-infrastructure-code-management-ansible-sangode
https://kodekloud.com/blog/configuration-vs-orchestration-management/

upvoted 1 times

eojedad 8 months ago

Puppet is a robust configuration management and automation tool... OCG page 1801

upvoted 2 times

mmhawish 10 months, 1 week ago

Orchestration: Automate across multivendor physical and virtual network elements using sophisticated abstraction capabilities.

Puppet: Define and enforce configurations across operating systems, middleware, and applications in a programmatic way

Ansible is an open source, command-line IT automation software application written in Python. It can configure systems, deploy software, and orchestrate advanced workflows to support application deployment, system updates, and more.
Ansible is designed to be very simple, reliable, and consistent for configuration management.

upvoted 3 times

StefanOT2 10 months, 2 weeks ago

The given answer is not correct.
Configuration Management =
- Ansible
- ...enables consistent configuration...

upvoted 3 times

MO_2022 11 months, 3 weeks ago

I would put "enables consistent configuration" under configuration management.

upvoted 3 times

ShadyAbdekmalek 12 months ago

I this the provided answer confused Automation and Orchestration

upvoted 1 times

ShadyAbdekmalek 12 months ago

* I think the provided answer confused Automation and Orchestration technology types

upvoted 1 times

mikinet 1 year, 1 month ago

"Puppet is more of a configuration management tool" https://www.devopsgroup.com/blog/puppet-vs-ansible/

upvoted 2 times

Newbie350 1 year, 2 months ago

From the link below, I understand that Ansible is more suitable in Orchestration category:
https://www.ciscopress.com/articles/article.asp?p=3100057&seqNum=3

"[Ansible] Playbooks are files that are used to define the desired or final state and also used to orchestrate operation across multiple nodes."

upvoted 1 times

RREVECO 1 year, 2 months ago

the structure is correct:
https://www.ansible.com/

Ansible Automation Platform has grown over the past years to provide powerful automation solutions that work for operators, administrators and IT decision makers across a variety of technology domains. It's a leading enterprise automation solution from Red Hat®, a thriving open source

community, and the de facto standard technology of IT automation.

BOOK: ccnp-and-ccie-enterprise-core-encor-350-401-official-cert-guide

Chapter 29. Introduction to Automation Tools

Puppet Bolt connects to devices by using SSH or WinRM connections. Puppet Bolt is an open source tool that is based on the Ruby language and can be installed as a single package.

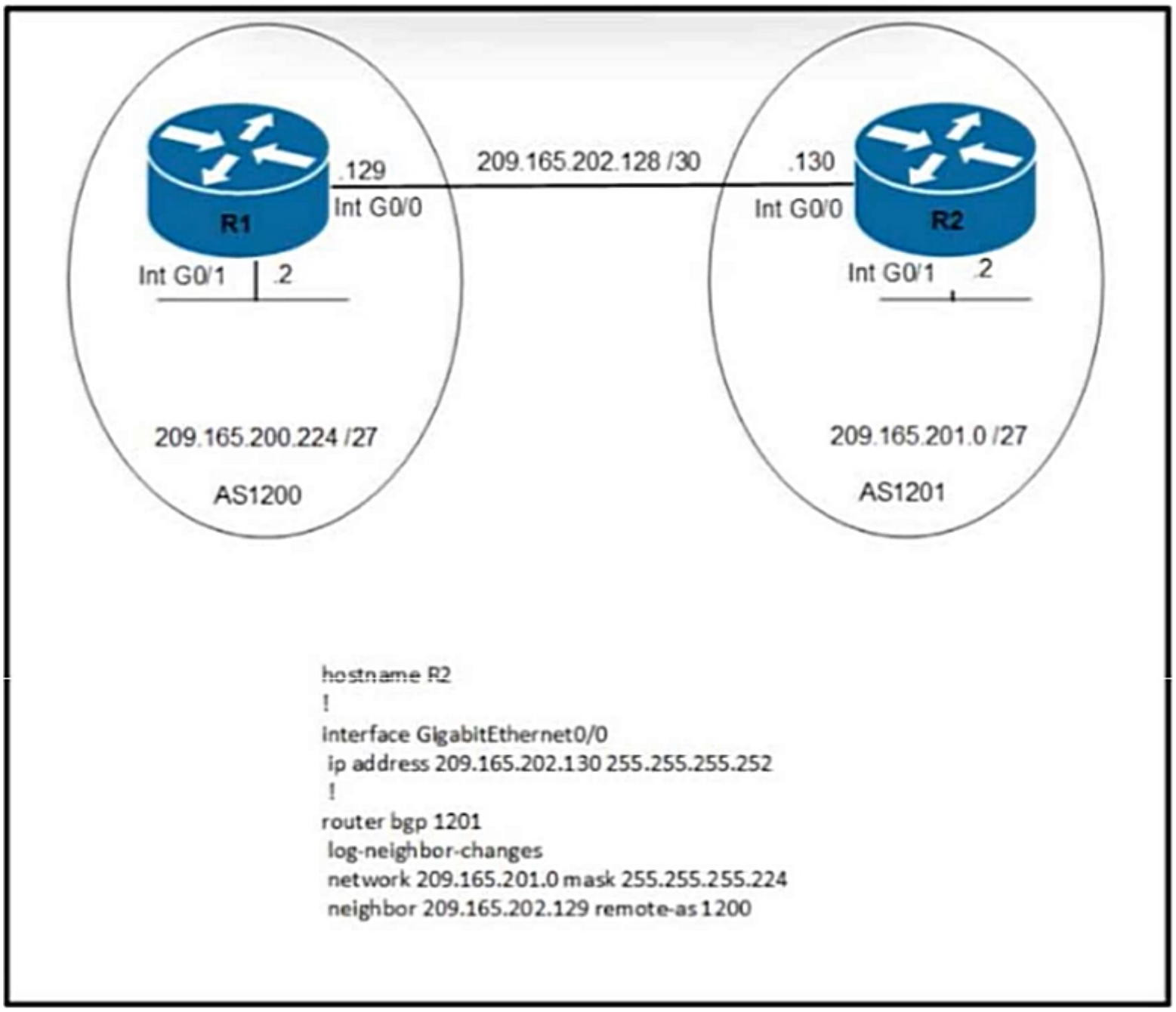
"Orchestrator-driven tasks: Orchestrator-driven" tasks can leverage the Puppet architecture to use services to connect to devices. This design is meant for large-scale environments.

upvoted 1 times

Deu_Inder 1 year, 2 months ago

I would put "enables consistent configuration" under configuration management.

upvoted 3 times



Refer to the exhibit. Which command set must be applied on R1 to establish a BGP neighborship with R2 and to allow communication from R1 to reach the networks?

A.

```
router bgp 1200
 network 209.165.200.224 mask 255.255.255.224
 neighbor 209.165.202.130 remote-as 1200
```

B.

```
router bgp 1201
 network 209.165.200.224 mask 255.255.255.224
 neighbor 209.165.202.130 remote-as 1201
```

C.

```
router bgp 1200
 network 209.165.201.0 mask 255.255.255.224
 neighbor 209.165.202.130 remote-as 1201
```

D.

```
router bgp 1200
 network 209.165.200.224 mask 255.255.255.224
 neighbor 209.165.201.2 remote-as 1200
```

Correct Answer: *B*

Nickplayany Highly Voted 10 months ago

Admin please fix the answers!! All of them are wrong.

The correct one below:

router bgp 1200 network 209.165.200.224
mask 255.255.255.224
neighbor 209.165.202.130
remote-as 1201

upvoted 21 times

Haidary Most Recent 1 week ago

All the answers are wrong.In answer B we should change the AS for R1 from 1201 to 1200.
upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago
How are people saying B? The neighbor is not even correct. It will never form a bgp neighborship. C is the only viable answer regardless that the network statement is wrong.
upvoted 2 times

LanreDipeolu 3 months ago
"B" is a ridiculously wrong answer. The technical answer is "C". You don't issue a router bgp AS statement on the adjacent AS number.
It should read:
R1
router bgp 1200
network 209.165.200.224 mask 255.255.255.224
neighbor 209.165.202.130 remote-as 1201
upvoted 1 times

[Removed] 5 months, 1 week ago
These are all wrong...
upvoted 2 times

[Removed] 5 months, 2 weeks ago
No correct answer, they all either point to the wrong Remote-AS, or are configured with the wrong local AS, or are trying to do a neighborship with the wrong subnet.
upvoted 1 times

Splashisthegreatestmovie 5 months, 2 weeks ago
The incorrect network advertisement in answer C doesn't bother me because the question is specifically asking us to build a neighborship. The peering configuration works in answer C so I'm picking C
upvoted 3 times

rogi2023 4 months, 1 week ago
You are right BGP neighborship is established and if you read carefully the task is: "establish a BGP neighborship with R2 and to allow communication from R1 to reach the networks?" allow communication from R1 - which perfectly works. - So C is correct with minor error not advertising its networks. HTH
upvoted 1 times

Burik 5 months, 2 weeks ago
No answer is correct. That would be B if router bgp was 1200.

router bgp 1200
network 209.165.200.224 mask 255.255.255.224
neighbor 209.165.202.130 remote-as 1201
upvoted 1 times

Chiaretta 7 months, 1 week ago
router bgp 1200
neighhbor 209.165.202.130 remote-as 1201
network 209z.165.200.224 mask 255.255.255.224
upvoted 1 times

bk989 7 months, 2 weeks ago
It cannot be B because of wrong peering defined on other side.
The peering will be off if misconfigured on 1 side. And give this error.
The peering will be off if misconfigured on 1 side.

*Apr 15 08:06:49.403: %SYS-5-CONFIG_I: Configured from console by console
*Apr 15 08:06:49.875: %BGP-3-NOTIFICATION: sent to neighbor 1.1.1.1 2/2 (peer in wrong AS) 2 bytes 0064
upvoted 2 times

owenshinobi 8 months, 1 week ago
C is correct.
because BGP neighbors establish and traffic from R1 can go to R2.
In the question does not specify traffic from R2 must return to R1.
upvoted 1 times

bullett00th 8 months, 1 week ago
There is a Typo in Question B. It should be: router bgp 1200
upvoted 1 times

HungarianDish 8 months, 2 weeks ago
C is working at least. Peering and reachability from R1 to R2's network is Ok.
upvoted 3 times

Clauster 8 months, 2 weeks ago
The Correct Answer is B and here's why.
O tho C would of been the correct answer but unfortunately the Network Statement is missing and so it gets disqualified.

B Is the correct answer because you can use different AS for BGP on a router, in this example they used Router BGP 1201 to throw us off, we were expecting to be Router BGP 1200 simply because in our mind these are two different AS, and you are right, but at the same time this doesn't mean that the Answer B is incorrect, in fact when you do Router BGP 1201 now you are running iBGP and it will no longer be eBGP, these two routers will become neighbors in the same Atonomous System 1201 and Adjacency will come up.

upvoted 2 times

HungarianDish 8 months, 2 weeks ago

I tested the config from option B, and it is throwing me the error "wrong as". If we would like to do a configuration similar to B, we would need to use consistently as 1201 on R2 (neighbor 209.165.202.129 remote-as 1201). Thus, we would get iBGP peering. This is not the case in the exhibit. It seems to me that all options are wrong at the moment.

upvoted 1 times

Doh247 9 months, 1 week ago

C will allow the adjacency to be formed, and reachability to R2 segment. Yes, the network statement is wrong, but that isn't what the question is asking. Best of a bad lot.

upvoted 4 times

[Removed] 5 months, 1 week ago

If you want a working bgp peering, then C is the only one that forms the peering.
All the other ones are going to throw an error

upvoted 1 times

kewokil120 11 months ago

none of them is correct

upvoted 3 times

MO_2022 11 months ago

A. router bgp 1200
network 209.165.200.224 mask 255.255.255.224
neighbor 209.165.202.130 remote-as 1201

upvoted 4 times

```
restconf
!
ip http server
ip http authentication local
ip http secure-server
!
```

Refer to the exhibit. Which command must be configured for RESTCONF to operate on port 8888?

A. restconf port 8888

B. ip http restconf port 8888

C. ip http port 8888

D. restconf http port 8888

Correct Answer: *C*

Community vote distribution

C (100%)

StefanOT2 Highly Voted 10 months, 2 weeks ago

Selected Answer: C

The given answer C is correct.

Restconf can run on https and on http. To set the http server to port 8888 you need the command at C. Off course no one would work via http (when https is available), but the Cisco apprentice who made this question does not care to much about it.

upvoted 5 times

net_eng10021 6 months ago

lol.....

upvoted 1 times

robi1020 Most Recent 11 months, 3 weeks ago

Selected Answer: C

Router(config)#ip http port ?
80 Default port number
<1024-65535> Port number range

upvoted 1 times

Question #367 *Topic 1*

Why would a log file contain a * next to the date?

A. The network device was receiving NTP time when the log messages were recorded.

B. The network device was unable to reach the NTP server when the log messages were recorded.

C. The network device is not configured to use NTP.

D. The network device is not configured to use NTP time stamps for logging.

Correct Answer: *D*

Community vote distribution

C (56%) B (36%) 8%

VLAN4461 3 months ago

Asterisk(*):-
If the system clock has not been set, the date and time are preceded by an asterisk (*), which indicates that the date and time have not been set and should be verified.

dot (.):-
The dot means the router has gone out of sync with its configured NTP server and therefore the date/time may be incorrect.

https://community.cisco.com/t5/switching/what-does-the-and-mean-at-the-beginning-of-a-log-buffer-entry/td-p/2494471

upvoted 1 times

sonjad 4 months, 1 week ago

I think D is correct. * is not related to ntp server settings at all. It just says that time was not configured by admin. As soon as I set clock manually, "*" disappeared in logs. It happens without any ntp config.

upvoted 1 times

sonjad 4 months, 1 week ago

I've changed my mind. It's true that "C" is not accurate enough. "*" means that the time is not set and might be not accurate. And you can clear "*" by setting time not only using NTP but also manually. Nevertheless "D" looks even less suitable for me now. Default time stamps format would not cause "*". It's just a format after all
https://community.cisco.com/t5/switching/what-does-the-and-mean-at-the-beginning-of-a-log-buffer-entry/td-p/2494471

upvoted 2 times

massimp 6 months, 2 weeks ago

Selected Answer: C

C is correct.
Tried in real lab with a device previously connected to NTP server :

ASR1002-X#sh ntp status
Clock is synchronized, stratum 4, reference is 192.168.0.12

ASR1002-X#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ASR1002-X(config)#no ntp server 192.168.0.12

.May 13 15:02:06.514: %SYS-5-CONFIG_I: Configured from console by vty0 (10.61.104.185)
So, it's not B.

upvoted 3 times

Chiaretta 7 months, 1 week ago

Selected Answer: C

C is correct.
At the moment of log receving the NTP was non configured.
If would show a dot at the moment of log receving NTP was not in sync

upvoted 2 times

JackDRipper 7 months, 4 weeks ago

Selected Answer: C

An asterisk "*" before the timestamp points to answer C as the reason.
A period/dot "." before the timestamp points to answer B.

upvoted 3 times

HungarianDish 8 months ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r3-9/system_management/command/reference/yr39xr12k_chapter4.html

The system clock keeps an “authoritative” flag that indicates whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source, such as system calendar (CLI) or Network Time Protocol (NTP), the flag is set. If the time is not authoritative, it is used only for display.

* Time is not authoritative.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/15-2mt/bsm-time-calendar-set.html

Within the CLI command syntax, the hardware clock is referred to as the system calendar.
upvoted 3 times

HungarianDish 8 months ago
same here:
https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/show_clock.htm
upvoted 3 times

dragonwise 8 months ago
Selected Answer: B
I have tested it in a lab and the answer is B
upvoted 3 times

Clauster 8 months, 2 weeks ago
Selected Answer: B
Answer is B
Check out CCIE answer
https://community.cisco.com/t5/switching/what-does-the-and-mean-at-the-beginning-of-a-log-buffer-entry/td-p/2494471
upvoted 2 times

x3rox 9 months, 1 week ago
Cisco IOS Configuration Fundamentals Command Reference:

ASTERISK * - Time is not authoritative: the software clock is not in sync or has never been set.
BLANK - Time is authoritative: the software clock is in sync or has just been set manually.
DOT . - Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers.
upvoted 3 times

x3rox 9 months, 1 week ago
source: https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_s2.html#wp1486074
upvoted 1 times

olaniyijt 10 months ago
If nothing is before the date, it means that your router clock was set manually or is in sync with a NTP server by the time of the log.
If with an asterisk, it means you didn't set the clock or it isn't synced with a NTP server.
If there's a period, it means the clock was in sync but the NTP server is not accessible.

https://networkengineering.stackexchange.com/questions/10168/interpreting-cisco-logging-symbols#:~:text=If%20nothing%20is%20before%20the,synced%20with%20a%20NTP%20server.
upvoted 1 times

gordon888 10 months ago
Selected Answer: B
B. The network device was unable to reach the NTP server when the log messages were recorded.
Most accurate
in lab:

//刚起机，配置正确ntp但ntp没学到时间时：

//When the machine is just started and ntp is configured correctly, but ntp has not learned the time:
*Jan 28 02:03:50.603: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
000020: *Jan 28 2023 10:03:50 bj: %SYS-6-CLOCKUPDATE: System clock has been updated from 02:03:50 UTC Sat Jan 28 2023 to 10:03:50 bj Sat Jan 28 2023, configured from console by console.
000021: Jan 28 2023 10:03:51 bj: %SSH-5-DISABLED: SSH 1.99 has been disabled
000022: Jan 28 2023 10:03:55 bj: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
upvoted 2 times

Rose66 10 months, 3 weeks ago
Selected Answer: C
I will go for C: If the system clock has not been set, the date and time are preceded by an asterisk (*) to indicate that the date and time are probably not correct.
upvoted 4 times

kewokil120 10 months, 3 weeks ago
Selected Answer: B
I like B. I have a cisco switch that normally does not show * and it configured with NTP. During an issue window the * appeared in it logs.
upvoted 1 times

markymark874 10 months, 4 weeks ago

Selected Answer: C

The datetime keyword adds time stamps in the format mmm dd hh:mm:ss, indicating the date and time according to the system clock. If the system clock has not been set, the date and time are preceded by an asterisk (*), which indicates that the date and time have not been set and should be verified.

upvoted 2 times

dnjJ56 11 months, 1 week ago

Selected Answer: C

(*) is printed when NTP is not configured on the device.
(.) is printed when NTP is configured, device was once in synced, but now can't reach the NTP server.
C is the correct Answer. Tested in the lab.

upvoted 4 times

kg2280 8 months ago

answer is B. If you configured NTP, but you cannot reach the NTP server, you will have the * As soon as the switch can reach the NTP server, the * will disappear. Also tested in lab

upvoted 1 times

cjk3 11 months, 1 week ago

Selected Answer: D

https://community.cisco.com/t5/network-security/what-does-asterisk-mean-in-show-clock/td-p/1644594

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: B

after setup NTP server the asterisk * disappeared from the logs begin of the line:

#sh log
...
*Dec 20 22:10:02.892: %SYS-5-CONFIG_I: Configured from console by console
*Dec 20 22:11:48.253: NTP Core (INFO): keys initilized.
*Dec 20 22:11:48.258: NTP Core (NOTICE): proto: precision = usec
*Dec 20 22:11:48.258: NTP Core (NOTICE): ntpd PPM
*Dec 20 22:11:48.287: NTP Core (INFO): 162.159.200.123 8014 84 reachable
*Dec 20 22:11:48.287: NTP Core (INFO): 162.159.200.123 902D 8D popcorn popcorn
*Dec 20 22:11:50.285: NTP Core (INFO): 162.159.200.123 963A 8A sys_peer
*Dec 20 22:11:50.285: NTP Core (NOTICE): trans state : 5
*Dec 20 22:11:50.285: NTP Core (NOTICE): Clock is synchronized.
Dec 20 22:12:17.604: %SYS-5-CONFIG_I: Configured from console by console
Dec 20 22:14:00.611: %IDBMAN-4-ACTIVEPORTSINAGGPORT: Port-channel1(16 / 1) has -1136578896 active ports, but is being removed
Dec 20 22:14:06.164: %SYS-5-CONFIG_I: Configured from console by console
sw1#

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw1#show ntp associations

address ref clock st when poll reach delay offset disp
*~162.159.200.123 10.73.8.213 3 1 64 377 19.936 -4.785 3.160
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
sw1#

sw1#show ntp status
Clock is synchronized, stratum 4, reference is 162.159.200.123
nominal freq is 250.0000 Hz, actual freq is 250.0001 Hz, precision is 2**10
ntp uptime is 81700 (1/100 of seconds), resolution is 4000
reference time is E74CB4D0.49374C90 (22:25:20.286 UTC Tue Dec 20 2022)
clock offset is -4.7850 msec, root delay is 43.72 msec
root dispersion is 9.22 msec, peer dispersion is 3.16 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000339 s/s
system poll interval is 64, last update was 5 sec ago.
sw1#

upvoted 1 times

nushadu 11 months, 2 weeks ago

sw1#show run | section ntp
ntp logging
ntp server 0.pl.pool.ntp.org prefer

sw1#show run | section name
ip name-server 8.8.8.8
ip name-server 8.8.4.4
sw1#
Translating "0.pl.pool.ntp.org"...domain server (8.8.8.8) [OK]

*Dec 21 09:32:55.348: NTP Core (INFO): 213.199.225.30 8014 84 reachable
*Dec 21 09:32:55.348: NTP Core (INFO): 213.199.225.30 962A 8A sys_peer
*Dec 21 09:32:55.348: NTP Core (NOTICE): trans state : 5

*Dec 21 09:32:55.348: NTP Core (NOTICE): Clock is synchronized.
sw1#
sw1#
sw1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
sw1(config)#^Z
sw1#
sw1#
Dec 21 09:39:48.375: %SYS-5-CONFIG_I: Configured from console by console <<<<<<<<< no asterics
sw1#

upvoted 1 times

nushadu 11 months, 1 week ago

#sh logg
*Dec 27 16:13:15.659: %BGP-5-NBR_RESET: Neighbor 192.168.255.55 passive reset (BGP Notification sent)
*Dec 27 16:13:15.659: %BGP-5-ADJCHANGE: neighbor 192.168.255.55 passive Down AFI/SAFI not supported
*Dec 27 16:13:23.893: %BGP-5-ADJCHANGE: neighbor 192.168.255.55 Up
*Dec 27 16:13:33.385: %TRACK-6-STATE: 3 ip route 5.5.5.5/32 reachability Down -> Up
*Dec 27 16:13:33.385: %TRACK-6-STATE: 4 ip route 5.5.5.55/32 reachability Down -> Up <<<<< asterisks in the logs

cisco_R3# show ntp associations
address ref clock st when poll reach delay offset disp
~1.1.1.1 .INIT. 16 - 1024 0 0.000 0.000 15937. <<<<<<<<<<< fail to connect to NTP serv.
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

cisco_R3#show running-config | s ntp
ntp server 1.1.1.1 prefer
cisco_R3#

upvoted 1 times

nushadu 10 months, 3 weeks ago

I've changed my mind - C.

sw2#
*Jan 6 16:57:25.810: %SYS-5-CONFIG_I: Configured from console by console <<<<<<<<<<<<

sw2#show ntp associations
sw2#show ntp stat
%NTP is not enabled.
sw2#

upvoted 1 times

rogi2023 5 months ago

great lab-work. (*) is printed when NTP is not configured on the device.
(.) is printed when NTP is configured, device was once in synced, but now can't reach the NTP server.
But what is the diff between answer C and D ?? IMHO they are saying the same..only D is more precise/specific.

upvoted 1 times

Question #368 *Topic 1*

What is one difference between EIGRP and OSPF?

A. EIGRP uses the DUAL distance vector algorithm, and OSPF uses the Dijkstra link-state algorithm.

B. OSPF uses the DUAL distance vector algorithm, and EIGRP uses the Dijkstra link-state algorithm.

C. EIGRP uses the variance command for unequal cost load balancing, and OSPF supports unequal cost balancing by default.

D. OSPF is a Cisco proprietary protocol, and EIGRP is an IETF open standard protocol.

Correct Answer: *A*

Community vote distribution

A (100%)

CCNPWILL 1 month, 2 weeks ago

Provided answer is correct.

upvoted 1 times

Asymptote 11 months ago

Selected Answer: A

I Support ExamTopic

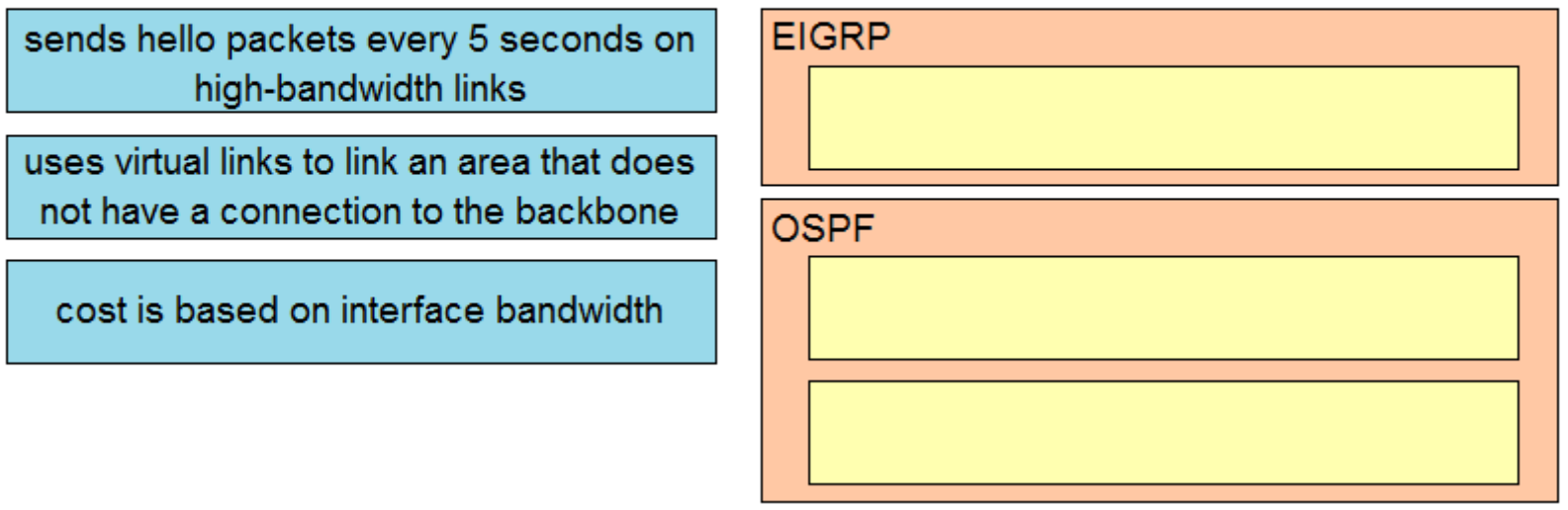
upvoted 1 times

DRAG DROP -

Drag and drop the characteristics from the left onto the routing protocols they describe on the right.

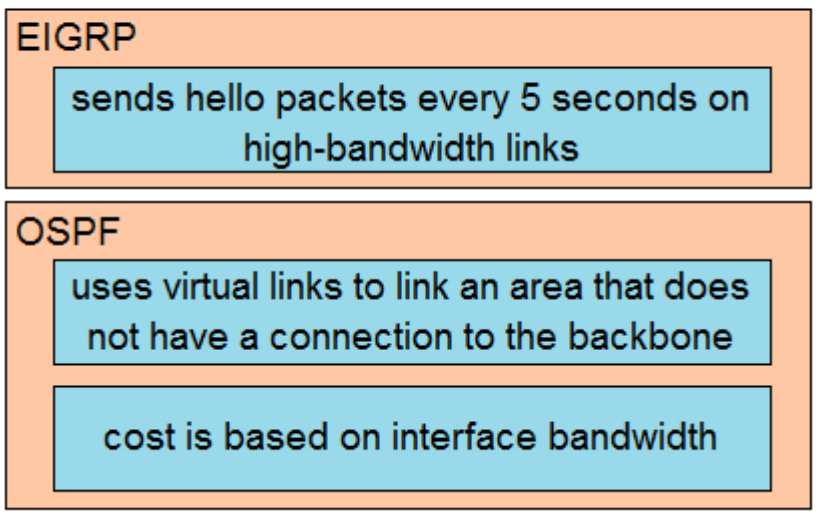
Select and Place:

Answer Area



Correct Answer:

Answer Area



CCNPWILL 1 month, 2 weeks ago

Provided answer is correct.

upvoted 1 times

Dataset 4 months ago

the answer is correct
Regards

upvoted 1 times

Rose66 10 months, 3 weeks ago

Provided answer is correct: "EIGRP sends hello packets every 5 seconds on high bandwidth links and every 60 seconds on low bandwidth multipoint links." Source: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html

upvoted 3 times

Question #370 *Topic 1*

A network engineer must configure a router to send logging messages to a syslog server based on these requirements:
* uses syslog IP address: 10.10.10.1
* uses a reliable protocol
* must not use any well-known TCP/UDP ports
Which configuration must be used?

A. logging host 10.10.10.1 transport tcp port 1024

B. logging host 10.10.10.1 transport udp port 1024

C. logging host 10.10.10.1 transport udp port 1023

D. logging origin-id 10.10.10.1

Correct Answer: *A*

Community vote distribution

A (89%) 11%

Haidary 1 week ago

As the 1024 is not a well-known port and tcp is a rliable protocol, then the answer A is correct.

upvoted 1 times

ihateciscoreally 3 months, 2 weeks ago

port 1024 is well-known so why answer is A? questions states "must not use any well-known TCP/UDP ports".

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Because it also asks for it to be reliable? UDP packets are not reliable. one way communication.

A is the only possible answer.

D is a BS answer Cisco throws in to throw you off

upvoted 1 times

Dataset 7 months, 1 week ago

Selected Answer: A

"reliable" is the magic word
A is correct
regards

upvoted 3 times

kg2280 8 months ago

Selected Answer: B

A&B are good. Syslog is originally designed to work over UDP but it ca also work over TCP.
R1(config)#logging host 1.1.1.1 transport ?
tcp Transport Control Protocol
udp User Datagram Protocol

upvoted 1 times

kg2280 8 months ago

Only A because : uses a reliable protocol

upvoted 1 times

Cooldude89 9 months, 1 week ago

Selected Answer: A

Well Known Ports: 0 through 1023. Registered Ports: 1024 through 49151. Dynamic/Private : 49152 through 65535.

upvoted 3 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

sw1(config)#logging host 1.1.1.1 transport tcp port 1024

upvoted 2 times

Deu_Inder 1 year, 2 months ago

A is the only option with a reliable protocol. And hence A is correct.

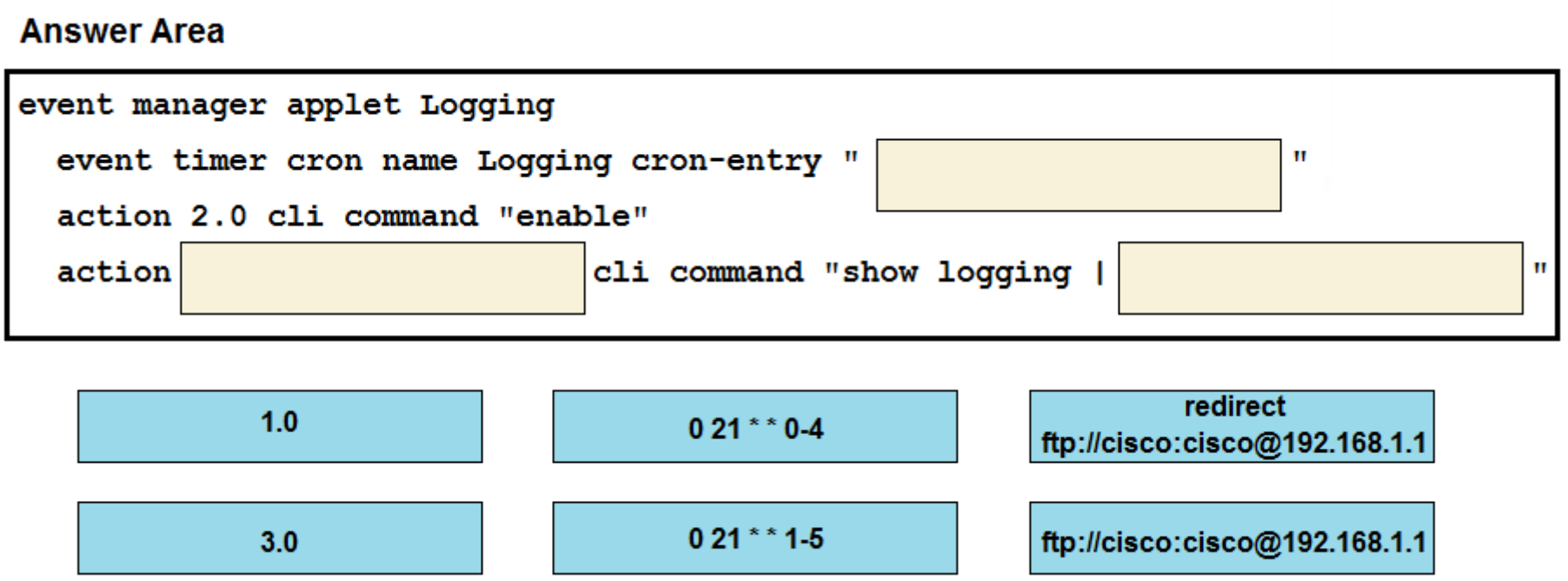
upvoted 3 times

DRAG DROP -

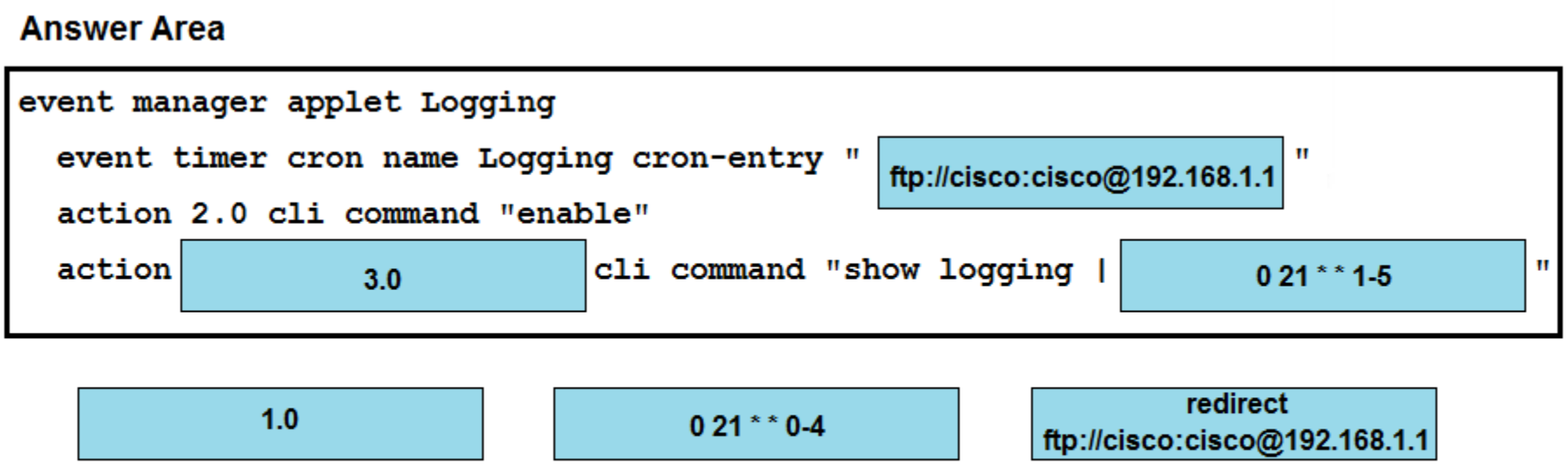
Drag and drop the snippets onto the blanks within the code to construct a script that shows all logging that occurred on the appliance from Sunday until 9:00 p.m.

Thursday. Not all options are used.

Select and Place:



Correct Answer:



Caradum Highly Voted 1 year ago

Answer is wrong.

Correct answer, tested it on my 3650 switch:
event timer cron name Logging cron-entry "0 21 * * 0-4"
action 2.0 cli command "enable"
action 3.0 cli command "show logging | redirect ftp://cisco:cisco@192.168.1.1

If you need to learn cron, check this site: https://crontab.guru
0 21 * * 0-4 translates to:
'At 21:00 on every day-of-week from Sunday through Thursday.'

upvoted 51 times

LanreDipeolu 3 months ago

This is the most valuable comment, I have come across. Thanks.
The site is very demystifying.

upvoted 1 times

siteoforigin Highly Voted 1 year, 2 months ago

Cron entry should be 0 21 * * 0-4. Cron entry day starts with 0 (being Sunday)
Search for CRON here:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-e2.html

upvoted 15 times

x3rox 10 months ago

Thank you. Excellent resource mate.
0 = min
21 = hour
* = any day
* = any month
0-4 = Sunday till Thursday. (not including Thursday - Sun 0, Mon 1, Tue 2, wed 3 then stop at Thursday 0).

upvoted 4 times

shubhambala 1 year, 2 months ago

spot on!

upvoted 2 times

HarwinderSekhon Most Recent 5 months ago

EngSwitch#show logging | redirect ?
flash1: Uniform Resource Locator
flash: Uniform Resource Locator
fstage: Uniform Resource Locator
ftp: Uniform Resource Locator
http: Uniform Resource Locator
https: Uniform Resource Locator
nvram: Uniform Resource Locator
rcp: Uniform Resource Locator
scp: Uniform Resource Locator
tftp: Uniform Resource Locator

Ans is

event timer cron name Logging cron-entry "0 21 * * 0-4"
action 2.0 cli command "enable"
action 3.0 cli command "show logging | redirect ftp://cisco:cisco@192.168.1.1

upvoted 2 times

MO_2022 11 months, 1 week ago

Answer:
1 – 0 21 * * 0-4
2 – 3.0
3 – redirect ftp://cisco:cisco@192.168.1.1

upvoted 5 times

Typovy 1 year ago

Sunday is represented either by 0 and 1 so 0-4 is valid. When using 'pipe' '|' u have to specify what you want for example "include" or "redirect"

upvoted 1 times

network_gig 1 year, 1 month ago

Tested it on my switch, valid script is:
event timer cron name Logging cron-entry "0 21 * * 0-4"
action 2.0 cli command "enable"
action 3.0 cli command "show logging | ftp://cisco:cisco@192.168.1.1

upvoted 3 times

iGlitch 1 year, 1 month ago

You should've included "redirect" before ftp

upvoted 1 times

dougj 1 year, 1 month ago

Sunday is day 0 in CRON

upvoted 1 times

Titini 1 year, 2 months ago

0 21 * *1-5, 3.0, sh logg | redirect tftp:xxxxxx

upvoted 3 times

Caledonia 1 year, 2 months ago

I am afraid the provided answer is not completely correct . action 3.0 is correct. after the 'cron entry' it should be 0 21 ** 1-5 and show logging | ftp://

upvoted 2 times

Deu_Inder 1 year, 2 months ago

I am afraid the provided answer is not completely correct .

action 3.0 is correct.

after the 'cron entry' it should be 0 21 ** 1-5
and
show logging | redirect ftp://

upvoted 5 times

mgiuseppe86 2 months, 2 weeks ago

Start of the week is sunday, 0, saturday is 7.

0 through 4 is sunday to thursday

upvoted 1 times

bullett00th 8 months, 1 week ago

0 21 * * 1-5 is not correct as this means Monday till Friday
0 21 * * 0-4 is Sunday till Thursday

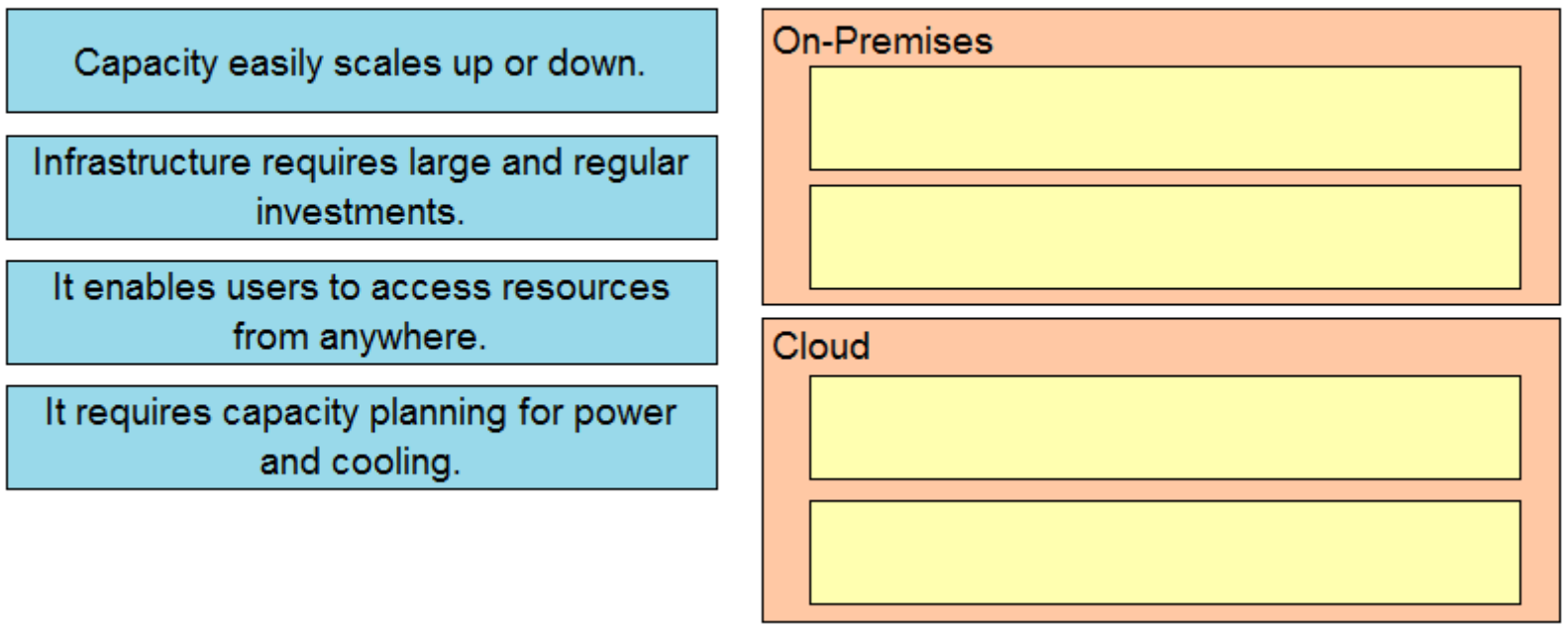
upvoted 1 times

DRAG DROP -

Drag and drop the characteristics from the left onto the infrastructure deployment models on the right.

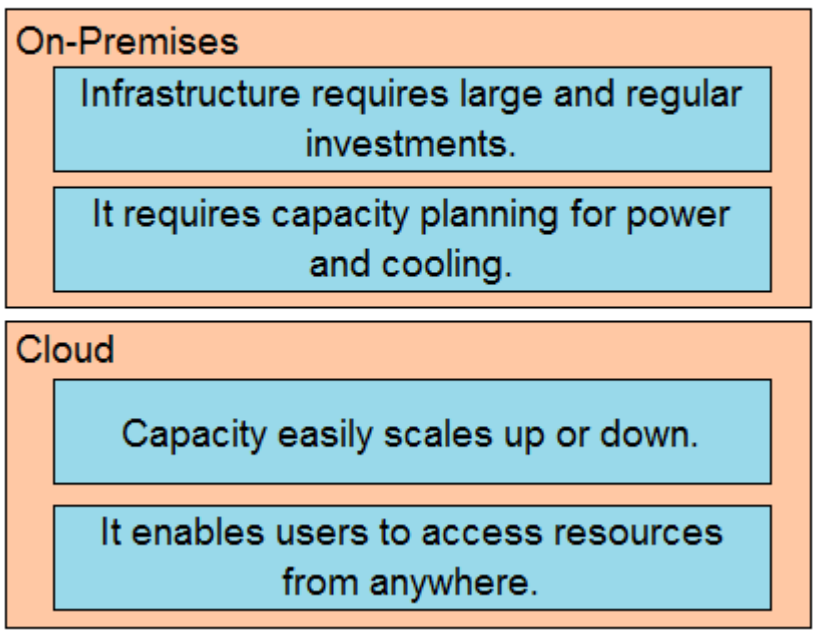
Select and Place:

Answer Area



Correct Answer:

Answer Area



CCNPWILL 1 month, 2 weeks ago

Provided answers are correct.

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

If you need a brain dump to answer this question, you don't belong in IT

upvoted 1 times

Asymptote 11 months ago

100% correct

upvoted 2 times

yoshiki111 11 months, 1 week ago

this answer is correct

upvoted 2 times

```
Router# show running-config

! lines omitted for brevity

username cisco password 0 cisco

aaa authentication login group1 group radius line
aaa authentication login group2 group radius local
aaa authentication login group3 group radius none

line con 0
password 0 cisco123
login authentication group1
line aux 0
login authentication group3
line vty 0 4
password 0 test123
login authentication group2
```

Refer to the exhibit. A network engineer must log in to the router via the console, but the RADIUS servers are not reachable. Which credentials allow console access?

A. no username and only the password λ€test123λ€

B. no username and only the password λ€cisco123λ€

C. the username λ€ciscoλ€ and the password λ€ciscoλ€

D. the username λ€ciscoλ€ and the password λ€cisco123λ€

Correct Answer: *B*

Community vote distribution

B (80%) A (20%)

mgiuseppe86 2 months, 2 weeks ago

I dont know man. This is a weird one. You cant have 'aaa authentication' strings in the config unless 'aaa new-model' was defined first.

You cannot remove 'aaa new-model' from a config ether. Once it is enabled, it's enabled for life unless you configured it and didnt save the config and rebooted the device.

As others here pointed out saying aaa new-model was omitted from the output doesnt mean its gone, we have to assume it's there.

The 'aaa authentication login' strings are throwing off the entire question. If those were omitted too then there is no way to actually tell aaa new-model was turned on and we can safely assume aaa is not active on this device

However, On one hand, line con 0 is calling for group1 which will read from radius first and if not, it will take the line password.

It's a catch 22. If it does use 'line' then we interpret that aaa new-model as turned on. but then because aaa new-model is turned on, your username and password should authenticate you into the console.

In a lab, i have created this exact scenario and the answer is indeed B. but with aaa new-model turned on.

upvoted 2 times

bendarkel 9 months ago

Selected Answer: B

B is the correct answer.

upvoted 2 times

well123 9 months, 1 week ago

Selected Answer: B

console password, no username.

upvoted 2 times

StefanOT2 10 months, 3 weeks ago

Selected Answer: A

aaa new-model is missing. So Answer A should be fine.

upvoted 1 times

Vadkorte 5 months, 2 weeks ago

>aaa new-model is missing.
Its omitted. I dont think you can configure any aaa command without enabling it with "aaa new-model"

upvoted 1 times

StefanOT2 10 months, 3 weeks ago

Sorry typo. It is off course B.

upvoted 4 times

danman32 4 months ago

Even if it was missing, question is accessing console, not telnet/SSH.
Password in answer A applies to VTY

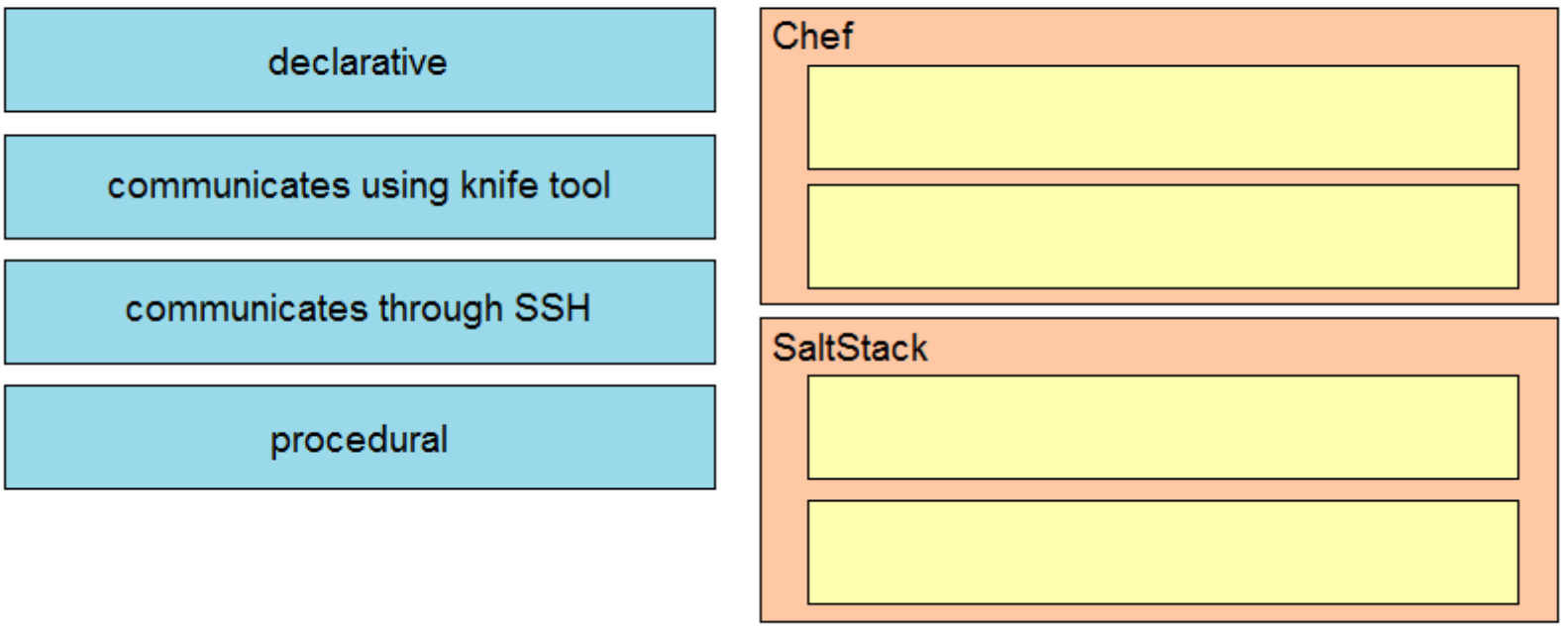
upvoted 1 times

DRAG DROP -

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

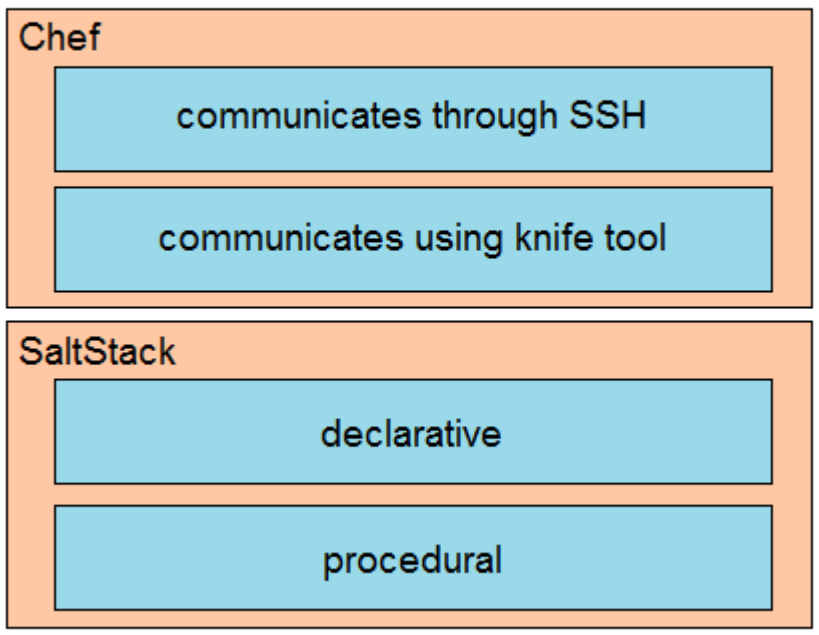
Select and Place:

Answer Area



Correct Answer:

Answer Area



Caradum Highly Voted 1 year ago

Chef = procedural and utilizes the knife tool (like a real chef haha...)
SaltStack = declarative and utilizes SSH

upvoted 29 times

Stylar Highly Voted 1 year ago

Chef: Uses knife tool / Procedural
Salt-Stack: Declarative - Uses SSH

upvoted 8 times

Dataset Most Recent 4 months ago

Hi admin
Please fix the answer
Chef uses knife and is procedural
SaltStack is declaratuve and uses SSH
Thanks!
Regards

upvoted 2 times

[Removed] 5 months, 2 weeks ago

Given answer is WRONG.

Chef = Procedural/Knife Tool
SaltStack = Uses SSH/Declarative
upvoted 2 times

Pilgrim5 7 months, 2 weeks ago
Ansible & Chef === procedural
Saltstack & puppet === declarative
upvoted 4 times

GeorgeFortiGate 1 year ago
Chef is procedural . Answer is wrong.
upvoted 3 times

Caledonia 1 year, 2 months ago
Salt Stack = declarative and uses ssh
upvoted 3 times

wendolin 1 year, 2 months ago
Salt Stack = declarative and uses ssh
upvoted 3 times

Question #375 *Topic 1*

Which configuration allows administrators to configure the device through the console port and use a network authentication server?

A. aaa new-model aaa authentication login default local aaa authorization console aaa authorization config-commands username netadmin secret 9 9vFpMf8elb4RVV8$seZ/bDAx1uV

B. aaa new-model aaa authentication login default local aaa authorization console aaa authorization config-commands

C. aaa new-model aaa authentication login default line

D. aaa new-model aaa authentication login default group radius aaa authorization console aaa authorization config-commands

Correct Answer: *D*

Community vote distribution

D (100%)

PureInertiaCopy 3 months, 2 weeks ago

A.

aaa new-model
aaa authentication login default local
aaa authorization console
aaa authorization config-commands username netadmin secret 9 9vFpMf8elb4RVV8$seZ/bDAx1uV

B.

aaa new-model
aaa authentication login default local
aaa authorization console
aaa authorization config-commands

C.

aaa new-model
aaa authentication login default line

D.

aaa new-model
aaa authentication login default group radius
aaa authorization console
aaa authorization config-commands

upvoted 2 times

dogdoglee 12 months ago

Selected Answer: D

only D using network authentication server (radius)

upvoted 3 times

Caradum 1 year ago

Selected Answer: D

Weird possible answers...

By process of elemination only D possible. Because its the only answer which utilizes the AAA servers.

upvoted 2 times

iGlitch 1 year, 1 month ago

D, it's the only option that uses AAA server.
Not C, because we want to configure using consol and not authenticate via consol line.

upvoted 3 times

Question #376 *Topic 1*

What is the process for moving a virtual machine from one host machine to another with no downtime?

A. high availability

B. disaster recovery

C. live migration

D. multisite replication

Correct Answer: *C*

respectively 1 month, 1 week ago
"windows engineer wakes up"
upvoted 1 times

flash007 4 months ago
in vmware mode this is called vmotion
upvoted 1 times

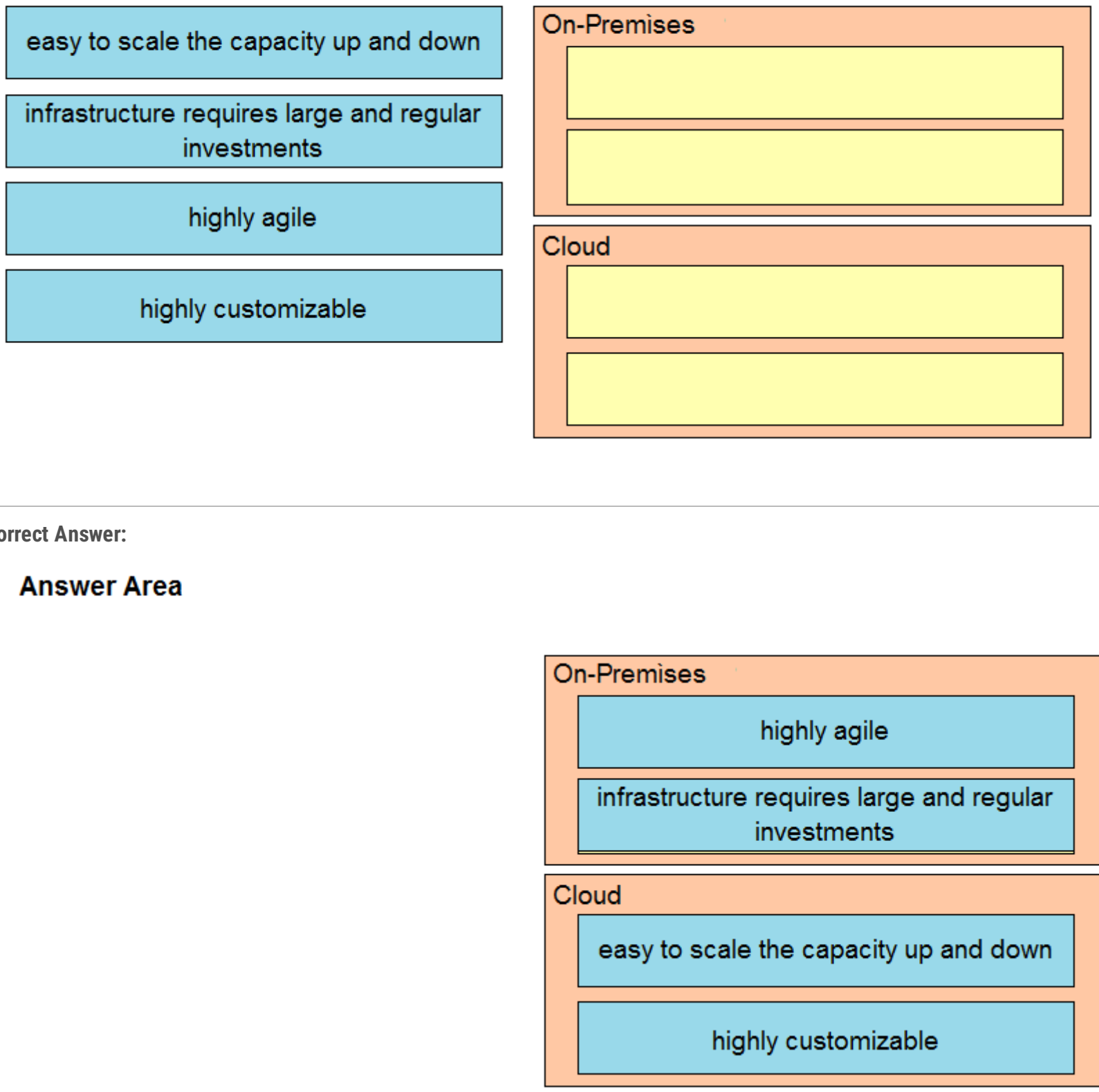
yoshiki111 11 months, 1 week ago
this anser is correct.
upvoted 2 times

DRAG DROP -

Drag and drop the characteristics from the left onto the infrastructure deployment models they describe on the right.

Select and Place:

Answer Area



Correct Answer:

Answer Area

pepgua Highly Voted 1 year, 2 months ago

"Highly agile" should go to Cloud and "highly customizable" to On-Prem. Agility is one of the main benefits of Cloud.

upvoted 50 times

MO_2022 11 months, 3 weeks ago

agree.

upvoted 3 times

iGlitch 1 year, 1 month ago

Agree.

upvoted 3 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago

I suppose the person who gave the original answer doesnt know english. Do they not know what the word agile means? It's the whole reason cloud exists!!!!

upvoted 2 times

HamzaBadar 7 months, 4 weeks ago

Agile should go to cloud and customizable to on premises.

upvoted 3 times

mykab 8 months, 4 weeks ago

Correct answer is -

Cloud -

Highly agile
easy to scale the capacity up and down

On premises -

Infrastructure requires large and regular investments
highly customizable

upvoted 3 times

well123 9 months, 1 week ago

Wrong answer,should be:

- On premises
Infrastructure requires large and regular investments
highly customizable

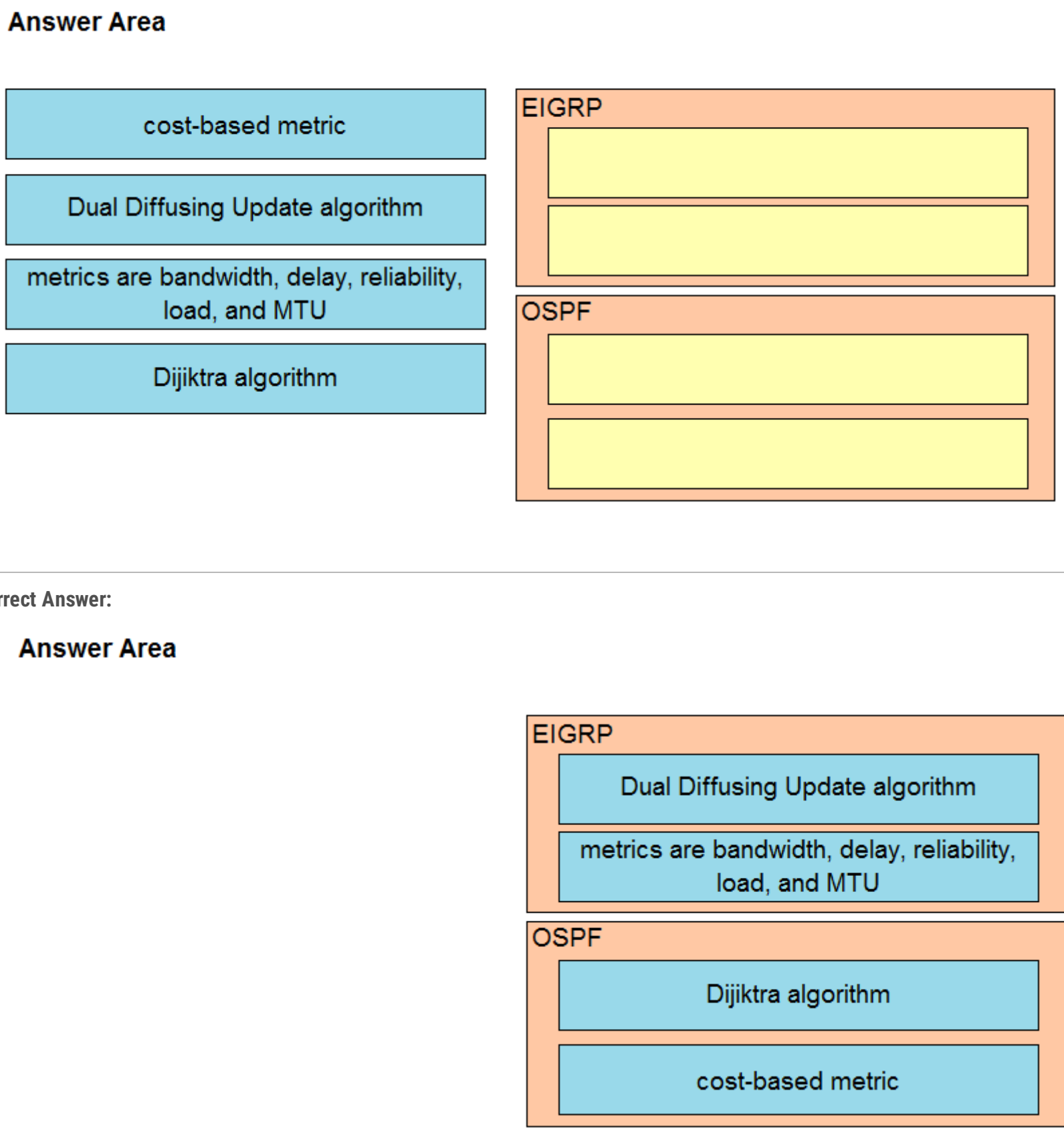
-cloud
easy to scale the capacity up and down
highly customizable

upvoted 2 times

DRAG DROP -

Drag and drop the characteristics from the left onto the routing protocols they describe on the right.

Select and Place:



Correct Answer:

Asymptote Highly Voted 11 months ago

Answer 100% correct

upvoted 7 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Easy gimme question... Provided answers are correct... for a change.

upvoted 1 times

Pilgrim5 7 months, 2 weeks ago

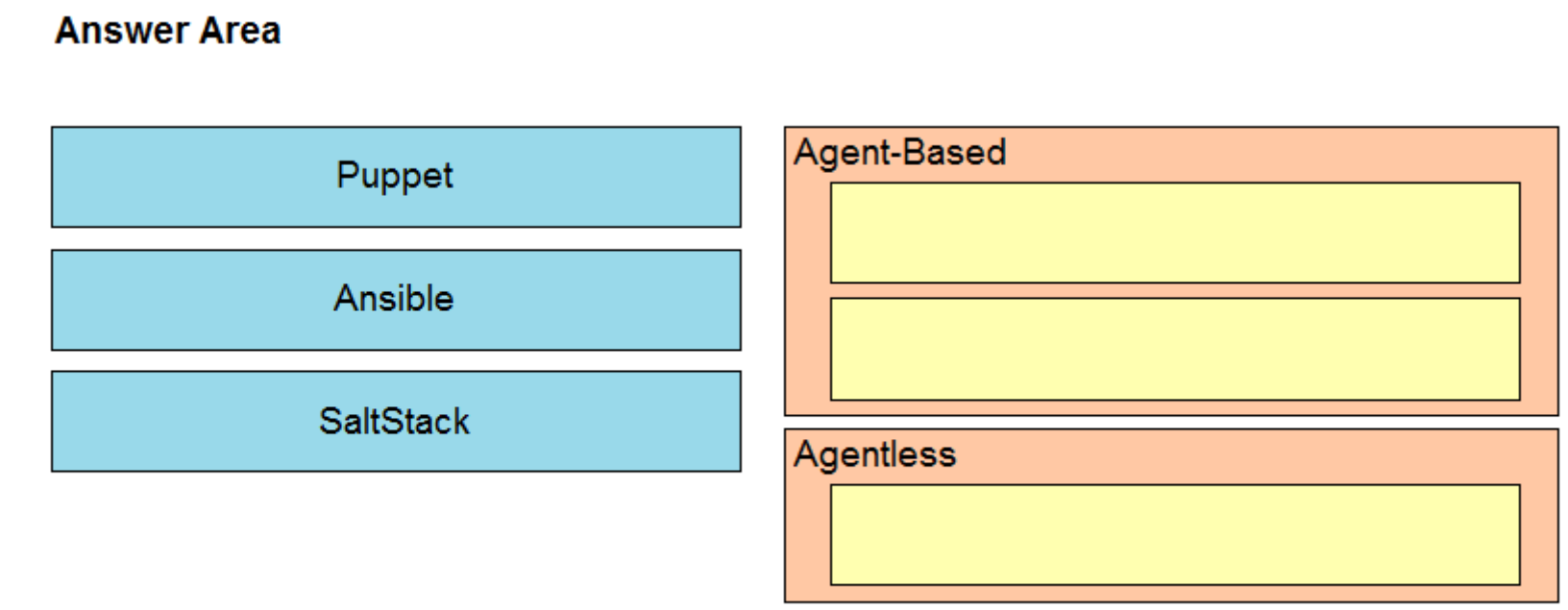
Given answer is correct

upvoted 1 times

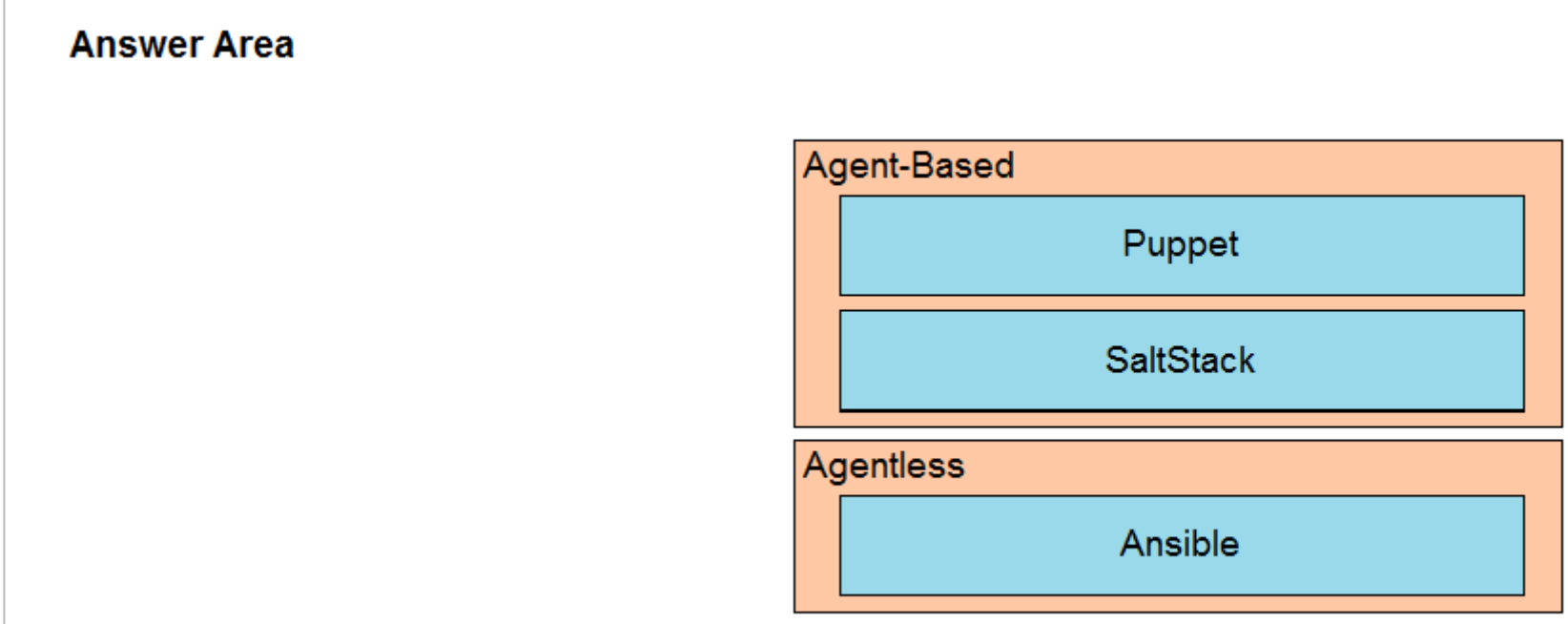
DRAG DROP -

Drag and drop the tools from the left onto the agent types on the right.

Select and Place:



Correct Answer:



Asymptote Highly Voted 11 months ago

Answer is 100% correct

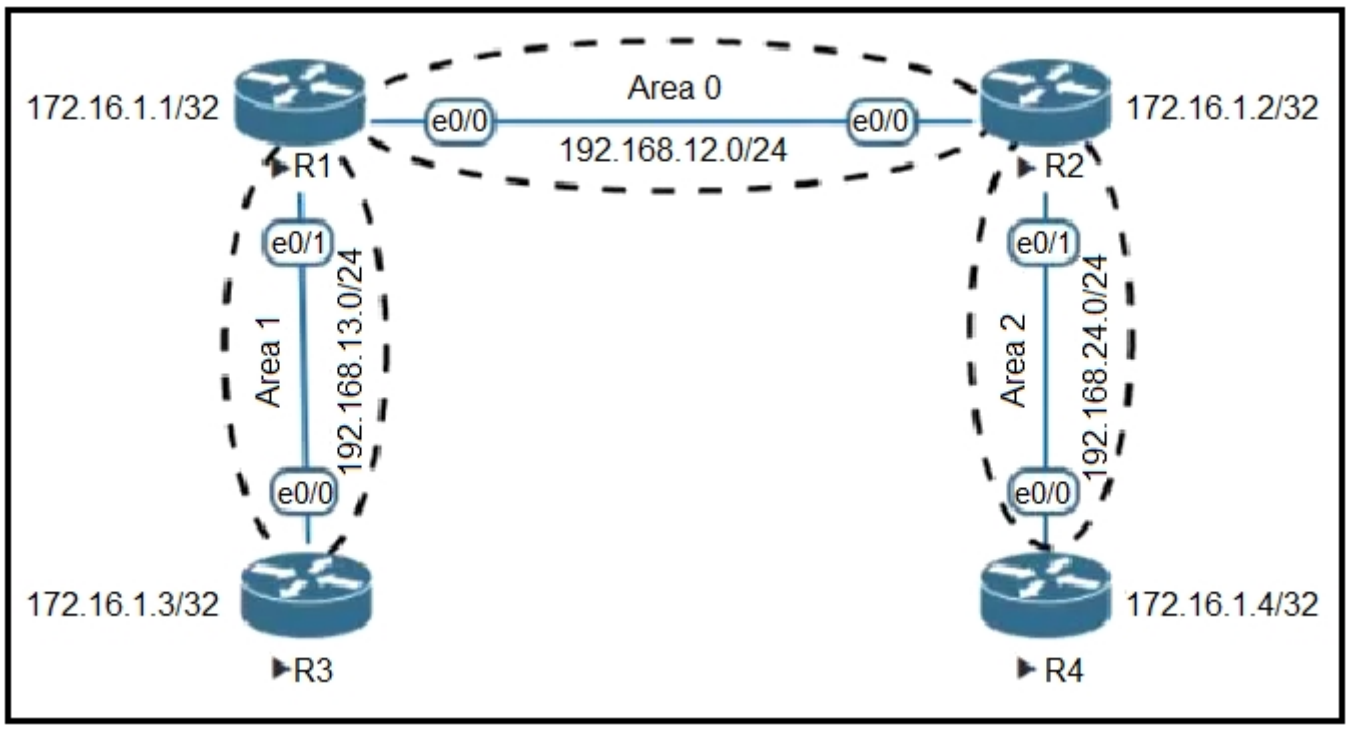
upvoted 6 times

Pilgrim5 Most Recent 7 months, 2 weeks ago

Given answer is right..

upvoted 1 times

Question #380 *Topic 1*



Refer to the exhibit. An engineer must create a configuration that prevents R3 from receiving the LSA about 172.16.1.4/32. Which configuration set achieves this goal?

A. On R3 ip access-list standard R4_L0 deny host 172.16.1.4 permit any router ospf 200 distribute-list R4_L0 in

B. On R1 ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32 ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32 router ospf 200 area 1 filter-list prefix INTO-AREA1 out

C. On R1 ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32 ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32 router ospf 200 area 1 filter-list prefix INTO-AREA1 in

D. On R3 ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32 ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32 router ospf 200 area 1 filter-list prefix INTO-AREA1 in

Correct Answer: *C*

Community vote distribution

C (80%) B (20%)

Ferrantee Highly Voted 1 year, 2 months ago

Correct is C

The policy must be applied on R1 and we have 2 ways.
-Apply outbound area 0 (This will affect others areas in this ABR
-Apply inbound area 1 (More accurate)

Validate on EVE-NG

upvoted 12 times

[Removed] Most Recent 5 months, 1 week ago

Selected Answer: C

Answer is C: at first i thought it was B, but the keywords in and out are a bit confusing without proper practice.
In the command: ospf area 2 filter-list INTO-AREA1
The option of "in" indicates networks going into the specified area
The option of "out" indicates networks coming from the specified area

upvoted 2 times

[Removed] 5 months ago

I've done this in GNS3 to make sure I did understand correctly. Answer is C. However this isn't the only way to accomplish this. For me a better solution would have been to apply the prefix-list into R3 itself as a distribute-list prefix PREFIX in to deny the route coming into the R3 routing table.

upvoted 1 times

dragonwise 8 months ago

A.
On R3
ip access-list standard R4_L0
deny host 172.16.1.4
permit any
router ospf 200
distribute-list R4_L0 in

B.
On R1
ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32
ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32
router ospf 200
area 1 filter-list prefix INTO-AREA1 out

C.
On R1
ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32
ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32
router ospf 200
area 1 filter-list prefix INTO-AREA1 in

D.
On R3
ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32
ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32
router ospf 200
area 1 filter-list prefix INTO-AREA1 in

upvoted 4 times

dragonwise 8 months ago

Selected Answer: C

Simulated the exact lab and found that the answer is C

the ABR will filter the subnet by not advertising it to the other routers in area 1. It will keep to itself thou

upvoted 2 times

bendarkel 9 months ago

Selected Answer: C

Correction...meant to say C is the correct answer. R1 (ABR) is filtering the LSA as it goes into area 1.

upvoted 2 times

bendarkel 9 months ago

Selected Answer: B

B is correct. R1 (ABR) is filtering the LSA as it goes into area 1.

upvoted 2 times

bendarkel 9 months ago

Correction...meant to say C is the correct answer. R1 (ABR) is filtering the LSA as it goes into area 1.

upvoted 1 times

markymark874 10 months, 4 weeks ago

Selected Answer: B

R3 should not receive the routes but R1 can receive the routes . To prevent R3 from getting the routes, R1 should filter the routes it nees to pass to R3 which is egress direction. b is correct

upvoted 2 times

nushadu 11 months, 2 weeks ago

Selected Answer: C

this is ABR, pay attention to 172.16.13.0/24 (this netw will be filtered)

cisco_R3(config-router)#do s runn | i PL_3
ip prefix-list PL_3 seq 10 deny 172.16.13.0/24
ip prefix-list PL_3 seq 20 permit 0.0.0.0/0 le 32
cisco_R3(config-router)#
cisco_R3(config-router)#area 22 filter-list prefix PL_3 ?
in Filter networks sent to this area <<<<<<<<<<<<<<<<<<<
out Filter networks sent from this area

cisco_R3(config-router)#area 22 filter-list prefix PL_3 in
cisco_R3(config-router)#
cisco_R3(config-router)#do s runn | s ospf
ip ospf 1 area 22
router ospf 1
area 22 filter-list prefix PL_3 in
passive-interface default
no passive-interface Ethernet0/0.10
no passive-interface Ethernet0/0.50
network 0.0.0.0 255.255.255.255 area 0

cisco_R3(config-router)#do s runn int Ethernet0/0.50
interface Ethernet0/0.50
encapsulation dot1Q 50
ip address 10.111.10.1 255.255.255.252
ip ospf 1 area 22
end

upvoted 2 times

nushadu 11 months, 2 weeks ago

far-end GRT before filtering:
cisco_R5#show ip route ospf
3.0.0.0/32 is subnetted, 1 subnets
O IA 3.3.3.3 [110/11] via 10.111.10.1, 00:01:12, Ethernet0/0.50
172.16.0.0/24 is subnetted, 2 subnets
O IA 172.16.13.0 [110/20] via 10.111.10.1, 00:00:43, Ethernet0/0.50 <<<<<<<<<<<<<<<<<<<
O IA 172.16.113.0 [110/20] via 10.111.10.1, 00:01:12, Ethernet0/0.50
cisco_R5#

after - netw 172.16.13.0/24 disapeared:

cisco_R5#show ip route ospf
3.0.0.0/32 is subnetted, 1 subnets
O IA 3.3.3.3 [110/11] via 10.111.10.1, 00:06:23, Ethernet0/0.50
172.16.0.0/24 is subnetted, 2 subnets
O IA 172.16.113.0 [110/20] via 10.111.10.1, 00:06:23, Ethernet0/0.50
cisco_R5#

upvoted 1 times

H3kerman 1 year ago

Selected Answer: C

in - Filters networks sent TO this area
out - Filters network sent FROM this area

upvoted 4 times

jjeans 1 year ago

Selected Answer: C

C is correct.

Prefix-list must be area1 inbound.
"area inbound" is different compared with "device inbound".

upvoted 1 times

Typovy 1 year ago

Selected Answer: C

C is valid, tested in EVE. We are filtering route that are entrying area 1 so we filter in. R1 is ABR

upvoted 3 times

Anarky19 1 year, 2 months ago

Correct answer b)
On R1 ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32 ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32 router ospf 200 area 1 filter-list prefix INTO-AREA1 out

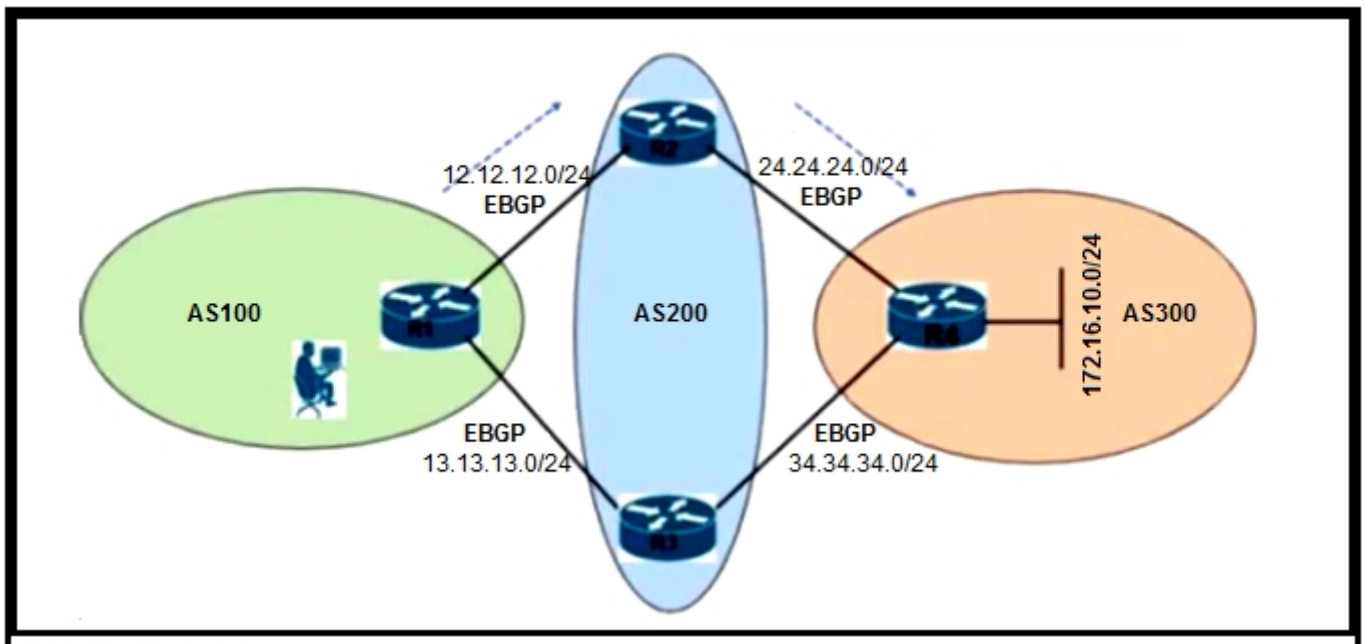
R1 is the ABR.

upvoted 3 times

bendarkel 1 year, 1 month ago

Concur.....B is the correct answer.

upvoted 6 times




```
R1#sh ip bgp
BGP table version is 2, local router ID is 13.13.13.13.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I Invalid, N Not found
       Network               Next
Hop            Metric      LocPrf      Weight      Path
*  172.16.1.0/24           13.13.13.3                                0
     200 300 i
*>                         12.12.12.2                                  0
          200 300 i
```

Refer to the exhibit. An engineer is reaching network 172.16.10.0/24 via the R1-R2-R4 path. Which configuration forces the traffic to take a path of R1-R3-R4?

A. R1(config)#route-map RM_LOCAL_PREF permit 10 R1(config-route-map)#set local-preference 101 R1(config-route-map)#exit R1(config)#router bgp 100 R1(config-router)#neighbor 13.13.13.3 route-map RM_LOCAL_PREF in R1(config-router)#end R1#clear ip bgp 13.13.13.3 soft in

B. R1(config)#route-map RM_AS_PATH_PREPEND R1(config-route-map)#set as-path prepend 200 200 R1(config-route-map)#exit R1(config)#router bgp 100 R1(config-router)#neighbor 12.12.12.2 route-map RM_AS_PATH_PREPEND in R1(config-router)#end R1#clear ip bgp 12.12.12.2 soft in

C. R1(config)#router bgp 100 R1(config-router)#neighbor 13.13.13.3 weight 1 R1(config-router)#end

D. R2(config)#route-map RM_MED permit 10 R2(config-route-map)#set metric 1 R2(config-route-map)#exit R2(config)#router bgp 200 R2(config-router)#neighbor 12.12.12.1 route-map RM_MED out R2(config-router)#end R2#clear ip bgp 12.12.12.1 soft out

Correct Answer: *B*

Community vote distribution

A (86%) 11%

x3rox Highly Voted 10 months ago

Selected Answer: A

This is the explanation why A is the ONLY Correct answer.
A: This will prefer both router to choose R1 - R3 - R4, as Local Preference is shared within the same AS.
B: AS-PREPEND is adding 200 200 - that's is NOT allowed as this is the neighbor AS and you can only prepend the local AS.
C: This will not work because Weight attribute requires a route map - The Router won't allow to set the weight directly like this - TESTED.
D. The MED attribute is only affecting how inbound traffic will reach us and NOT how we go out.

upvoted 11 times

MerlinTheWizard 10 months ago

weight doesn't require a route-map, it can be configured per neighbor - a perfectly valid solution if you're not required to handle the asymetric routing. The problem with option C is that you need to clear the neighbor afterwards. Not sure how you tested this, but if you need reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/command/irg-cr-book/bgp-m1.html#wp2222404444

upvoted 2 times

x3rox 9 months, 1 week ago

I retract. I tested it again after reading your post. I don't know why I failed testing it last time. I reanalyze the question again and this is my thinking now.
Answer A: Will work as Local Preference is set to prefer route via R3.
Answer B: WRONG
Answer C: Missing the clear configuration. Not because weight is not allowed in this form.
Answer D: I think it will work too. I R3 set the MED out towards AS100, R1 will prefer to route via R3 as the default MED is 0 and lower is better.
But between MED and Local Preference, the second takes preference. Answer should be A.

upvoted 2 times

x3rox 9 months, 1 week ago

*...R2 set the MED..

upvoted 2 times

x3rox 9 months, 1 week ago

Also, it's the engineer should not have access to configure R2 for MED configurations....

upvoted 2 times

bier132 4 months, 1 week ago

regarding your post:
C: This will not work because Weight attribute requires a route map - The Router won't allow to set the weight directly like this - TESTED.
Not true, tested in GNS3 with IOS-XE Version 17.03.04a
R1(config-router)#neighbor 13.13.13.3 weight 1
R1(config-router)#do sh run | s r b
router bgp 100
bgp log-neighbor-changes
network 1.1.1.1 mask 255.255.255.255
neighbor 12.12.12.2 remote-as 200
neighbor 13.13.13.3 remote-as 200
neighbor 13.13.13.3 weight 1
R1(config-router)#

I guess C is wrong because the clear statement is missing.

upvoted 1 times

dragonwise Highly Voted 8 months ago

A.
R1(config)#route-map RM_LOCAL_PREF permit 10
R1(config-route-map)#set local-preference 101
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 route-map RM_LOCAL_PREF in
R1(config-router)#end
R1#clear ip bgp 13.13.13.3 soft in

B.
R1(config)#route-map RM_AS_PATH_PREPEND
R1(config-route-map)#set as-path prepend 200 200
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 12.12.12.2 route-map RM_AS_PATH_PREPEND in
R1(config-router)#end
R1#clear ip bgp 12.12.12.2 soft in

C.
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 weight 1
R1(config-router)#end

D.
R2(config)#route-map RM_MED permit 10
R2(config-route-map)#set metric 1
R2(config-route-map)#exit
R2(config)#router bgp 200
R2(config-router)#neighbor 12.12.12.1 route-map RM_MED out
R2(config-router)#end
R2#clear ip bgp 12.12.12.1 soft out

upvoted 7 times

msstanick Most Recent 5 months, 3 weeks ago

Selected Answer: A

Another interesting one. Firs of all - B is wrong! One cannot prepend a foreign AS 200. Not to mention that prepanding ASes influences the traffic flow in the other way around it is required in this case.

i checked options A & D as they both made sense and... they actually did. Both of them wil do the trick as A is modyfing a local pref from 100 to 101 making the path via R3 more desirable while D is adding +1 to the MED which makes the route via R2 less desirable which is also fine.

IOU1#sh bgp ipv4 uni

* 172.16.10.0/24 12.12.12.12 1 0 200 300 i

*> 13.13.13.13 101 0 200 300 i

Since LP is the 2nd criteria and MED is lower I would go with A.
upvoted 2 times

net_eng10021 6 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13759-37.html
upvoted 1 times

Dataset 7 months, 1 week ago

Selected Answer: A

Its A for me
Regards
upvoted 1 times

HamzaBadar 7 months, 3 weeks ago

I rechecked in GNS3. Although both A and B work but simplest and easy way is C.
upvoted 1 times

HamzaBadar 7 months, 4 weeks ago

Option A tested in GNS3 and it works as per requirement. Therefore correct answer is A.
upvoted 1 times

HungarianDish 7 months, 3 weeks ago

What is your opinion on this article?:
https://community.cisco.com/t5/networking-knowledge-base/understanding-bgp-best-path-selection-manipulation/ta-p/3150576
=>
A,B,D are all correct. C could be correct, too. Although "clear ip bgp..." is missing from C. Answer might need to be selected based on the order of the best path selection.
upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

How can B be correct? You cant prepend a remote-as R1 is in AS100. It's attempting to prepend AS200 200
upvoted 1 times

HungarianDish 8 months ago

This question is based on this article:
https://community.cisco.com/t5/networking-knowledge-base/understanding-bgp-best-path-selection-manipulation/ta-p/3150576

The article lists all the solutions A, B, and D as appropriate. C is missing "clear ip bgp ...", so the attribute weight is out.

B is okay, too, because it is an as-path prepend inbound. You can set the neighbor's as or operator "last-as ..." for inbound updates. See:
https://blog.ipspace.net/2009/03/as-path-prepending-technical-details.html

It is not clear to me why answer A is better than the other answers, unless we consider the order of the best path selection. Local preference will be checked before the other possible solutions (as-path prepend and MED).
upvoted 1 times

bendarkel 9 months ago

Selected Answer: A

Correct answer is A.
upvoted 1 times

landgar 10 months, 2 weeks ago

Selected Answer: A

AS path prepend is only used in OUTGOING BGP updates, to influence incoming traffic.
Weght default value is 1 and could have been right, but clear soft session is not set. Weight has local meaning (scope just inside R1 router).
Local_pref is used to select an output path, a BGP AS scope (iBGP updates).
upvoted 1 times

x3rox 9 months, 1 week ago

you are correct. AS PATH is only used out. so B is wrong again.
upvoted 1 times

HungarianDish 8 months ago

AS path prepend can be used inbound, please see:
https://community.cisco.com/t5/networking-knowledge-base/understanding-bgp-best-path-selection-manipulation/ta-p/3150576

https://ipwithease.com/bgp-as-prepend-inbound-configuration-example/

https://blog.ipspace.net/2009/03/as-path-prepending-technical-details.html
upvoted 1 times

MerlinTheWizard 10 months ago

default weight is 0 (remote prefix) or 32768 (self-originated prefix), not 1

upvoted 1 times

x3rox 9 months, 1 week ago

Correct

upvoted 1 times

markymark874 10 months, 4 weeks ago

Selected Answer: A

A. Use local preference metric to influence route

upvoted 1 times

nushadu 11 months, 2 weeks ago

Selected Answer: A

route-map Q_381 permit 10
set local-preference 101
!
router bgp 3
bgp router-id 3.3.3.3
bgp log-neighbor-changes
neighbor GR_AS2 peer-group
neighbor GR_AS2 remote-as 2
neighbor GR_AS2 password 7 1511021F0725
neighbor 192.168.255.22 peer-group GR_AS2
neighbor 192.168.255.55 remote-as 5
!
address-family ipv4
redistribute connected
neighbor GR_AS2 soft-reconfiguration inbound
neighbor GR_AS2 route-map Q_381 in
neighbor 192.168.255.22 activate
neighbor 192.168.255.55 activate
neighbor 192.168.255.55 soft-reconfiguration inbound
neighbor 192.168.255.55 route-map to_R5 in
exit-address-family
!

upvoted 1 times

nushadu 11 months, 2 weeks ago

before applying route-map:
isco_R3#show ip bgp 200.200.200.0
BGP routing table entry for 200.200.200.0/24, version 13
Paths: (3 available, best #2, table default)
Advertised to update-groups:
2
Refresh Epoch 1
2, (received & used)
192.168.255.22 from 192.168.255.22 (2.2.2.2)
Origin incomplete, metric 0, localpref 100, valid, external
rx pathid: 0, tx pathid: 0
Refresh Epoch 1
5
192.168.255.55 from 192.168.255.55 (5.5.5.5) <<<<<<<<<<<<<<<<<<<<<<
Origin IGP, metric 100, localpref 100, valid, external, best <<<<<<<<<<<<<<<<<<
rx pathid: 0, tx pathid: 0x0
Refresh Epoch 1
5, (received-only)
192.168.255.55 from 192.168.255.55 (5.5.5.5)
Origin incomplete, metric 100, localpref 100, valid, external
rx pathid: 0, tx pathid: 0
cisco_R3#

upvoted 1 times

nushadu 11 months, 2 weeks ago

after (next-hop & local pref has been chaged):

cisco_R3#show ip bgp 200.200.200.0
BGP routing table entry for 200.200.200.0/24, version 17
Paths: (4 available, best #1, table default)
Advertised to update-groups:
2
Refresh Epoch 1
2
192.168.255.22 from 192.168.255.22 (2.2.2.2) <<<<<<<<<<<<<<<<<<<<<<
Origin incomplete, metric 0, localpref 101, valid, external, best <<<<<<<<<<<<<<<<<<
rx pathid: 0, tx pathid: 0x0
Refresh Epoch 1
2, (received-only)
192.168.255.22 from 192.168.255.22 (2.2.2.2)
Origin incomplete, metric 0, localpref 100, valid, external
rx pathid: 0, tx pathid: 0

Refresh Epoch 1
5
192.168.255.55 from 192.168.255.55 (5.5.5.5)
Origin IGP, metric 100, localpref 100, valid, external
rx pathid: 0, tx pathid: 0
Refresh Epoch 1
cisco_R3#

upvoted 1 times

nushadu 11 months, 2 weeks ago

cisco_R3#show ip route bgp | b Ga
Gateway of last resort is not set

2.0.0.0/32 is subnetted, 1 subnets
B 2.2.2.2 [20/0] via 192.168.255.22, 00:08:49
5.0.0.0/32 is subnetted, 1 subnets
B 5.5.5.5 [20/0] via 192.168.255.55, 00:35:45
B 200.200.200.0/24 [20/0] via 192.168.255.22, 00:08:49
cisco_R3#

upvoted 1 times

Xerath 11 months, 2 weeks ago

Selected Answer: A

I think it's "A".

upvoted 1 times

tckoon 1 year, 2 months ago

Selected Answer: C

router with 2 paths , weight is way use for selection. default wieght is "0" , so set path R1-R3 bgp peer weight to 1 mean it is preference. Weight is local significant on R1 local router. clear bgp is not require at all.
Local preference is for multiple routers on same AS# path selection.
AS prepend and metric is for incoming traffinc to R1

upvoted 4 times

rogi2023 5 months ago

strongly agree with tckoon. "Weight is local significant on R1 local router. clear bgp is not require at all." - therefore just keep it simple - Answer C.

upvoted 1 times

HungarianDish 8 months ago

AS prepend -> we can use this for inbound updates (for prefixes learned from a neighbor), and so we manipulate outgoing traffic

upvoted 1 times

HungarianDish 8 months ago

It says that we need "clear ip bgp ..." for weight attribute.
"The Prefixes learned from R3 must be updated for this configuration to take affect. You can request a route refresh from R3 to accomplish this with the command clear ip bgp 13.13.13.3 soft in."
https://community.cisco.com/t5/networking-knowledge-base/understanding-bgp-best-path-selection-manipulation/ta-p/3150576

"Once you have defined two devices to be BGP neighbors, they will form a BGP connection and exchange routing information. If you subsequently change a BGP filter, weight, distance, version, or timer, or if you make a similar configuration change, you must reset BGP connections in order for the configuration change to take effect."

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3se/3850/irg-xe-3se-3850-book/irg-soft-reset.pdf

upvoted 1 times

ccnptoppler34 1 year, 2 months ago

Selected Answer: A

CORRECTION
Choice A: This would cause AS100 to route traffic via R1-R3-R4 which is what the question asks, although traffic from AS200 would still take a path to R2-R1 (Asymmetric routing) [CORRECT]

Choice B: This would cause AS200 to route traffic via an R3-R1 Path, but AS100 would still route traffic from R1-R2 (Asymmetric routing) [INCORRECT]

Choice C: This would set work, but "clear ip bgp 10.13.13.3 soft in" is missing [INCORRECT]

Choice D: Setting MED on an outbound route map will influence AS200s path selection [INCORRECT]

upvoted 5 times

ccnptoppler34 1 year, 2 months ago

Selected Answer: A

Choice A: This would cause AS100 to route traffic from R1-R3-R4 which is what the question asks, although traffic from AS200 would still take a path to R3-R4 (Asymmetric routing) [CORRECT]

Choice B: This would cause AS200 to route traffic for AS100 via an R3-R1 Path, but AS100 would still route traffic from R1-R2 (Asymmetric routing) [INCORRECT]

Choice C: This would set work, but "clear ip bgp 10.13.13.3 soft in" is missing [INCORRECT]

Choice D: Setting MED on an outbound route map will influence AS200s path selection [INCORRECT]

upvoted 3 times

Deu_Inder 1 year, 2 months ago

Maybe I understand now why it is not C. The 'clear ip bgp....' command is missing there.

upvoted 1 times

x3rox 10 months ago

not only that but the weight attribute requires a route map, the router won't allow this settings directly like this.

upvoted 1 times

Question #382 *Topic 1*

In a Cisco SD-Access solution, which protocol is used by an extended node to connect to a single edge node?

A. VXLAN

B. IS-IS

C. 802.1Q

D. CTS

Correct Answer: *C*

Community vote distribution

C (100%)

Asymptote Highly Voted 11 months ago

Selected Answer: C

open page 19
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2832.pdf

upvoted 15 times

byallmeans Most Recent 7 months ago

Selected Answer: C

C is correct answer

upvoted 1 times

```
R1#show policy-map control-plane
 Control Plane

  Service-policy output: CoPP

    Class-map: SNMP-Out (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name SNMP
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps

    Class-map: class-default (match-any)
      13858 packets, 1378745 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

Refer to the exhibit. How does the router handle traffic after the CoPP policy is configured on the router?

A. Traffic generated by R1 that matches access list SNMP is policed.

B. Traffic coming to R1 that matches access list SNMP is policed.

C. Traffic passing through R1 that matches access list SNMP is policed.

D. Traffic coming to R1 that does not match access list SNMP is dropped.

Correct Answer: *A*

Community vote distribution

A (61%) B (30%) 9%

fernandocirino Highly Voted 1 year ago

I believe the correct answer is A because it is described on the output "Service-policy output: CoPP, so traffic will be policed.

upvoted 10 times

Degen6969 7 months ago

Can confirm, output for input reads: “Service-policy input:”

upvoted 1 times

Colmenarez Most Recent 4 months ago

Selected Answer: C

Come on guys, the correct answer is C.

"Another special note on Cisco ACLs is that ACLs never apply to traffic generated by the router. So, even if you have an inbound and an outbound ACL on a router denying all traffic, the router will still be able to send any packet it wants; the return packet, however, will be blocked as usual"

https://www.ciscopress.com/articles/article.asp?p=174313&seqNum=4

upvoted 2 times

kewokil120 10 months, 3 weeks ago

Selected Answer: A

Service Policy is in the output direction. So traffic generated by router will be policed.

upvoted 4 times

echipbk 10 months, 3 weeks ago

Selected Answer: A

A is correct. Notice the keyword "output"

upvoted 2 times

echipbk 10 months, 3 weeks ago

https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/cpp.html

* input—Applies the specified service policy to packets received on the control plane.
* output—Applies the specified service policy to packets transmitted from the control plane and enables the router to silently discard packets.

upvoted 5 times

markymark874 10 months, 4 weeks ago

Selected Answer: A

A is correct. Because service policy is applied to control plane. So router generates the traffic. Control plane is the key word why Choose A.

upvoted 1 times

kewokil120 10 months, 4 weeks ago

Selected Answer: A

I believe the correct answer is A because it is described on the output "Service-policy output: CoPP, so traffic will be policed

upvoted 1 times

Adeel143 11 months ago

Selected Answer: A

would go with A

upvoted 1 times

kewokil120 11 months ago

Selected Answer: A

I believe the correct answer is A because it is described on the output "Service-policy output: CoPP, so traffic will be policed.

upvoted 1 times

Fadhelben 11 months, 2 weeks ago

Selected Answer: A

Given answer is correct, I have tested it. Only Traffic generated from R1 is policed.

upvoted 1 times

Ciscopass 1 year, 1 month ago

Selected Answer: A

Output Rate-Limiting Support

Output rate-limiting is performed in silent (packet discard) mode. Silent mode enables a router to silently discard packets using policy maps applied to output control plane traffic with the service-policy output command.

https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/cpp.html

upvoted 3 times

zpacket 1 year, 1 month ago

Selected Answer: B

"Only ingress CoPP is supported. The system-cpp-policy policy-map is available on the control plane interface, and only in the ingress direction".

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-11/configuration_guide/sec/b_1611_sec_9300_cg/configuring_control_plane_policing.pdf

Therefore, A can't be right. B is the answer.

upvoted 4 times

echipbk 10 months, 3 weeks ago

The system-cpp-policy policy map is a system-default policy map. The policy map mentioned in the question is a manual policy map named CoPP

upvoted 2 times

Eroman 1 year, 2 months ago

Selected Answer: B

A is not true. Because SNMP access list can't match traffic originated from R1.

B is true.

C s not true. Because passing traffic controlled bu data plane.

upvoted 3 times

MerlinTheWizard 10 months ago

SNMP ACL is used for simply identifying the packets generated by the control plane of R1 - this is not an ACL being applied in the out direction on an interface.

upvoted 1 times

Eroman 1 year, 2 months ago

D is not true. Because we can't say this with this information.

upvoted 1 times

Ferrantee 1 year, 2 months ago

A is true. Because control plane traffic include all traffic which is TO or GENERATED by the device.

upvoted 4 times

Question #384 *Topic 1*

What is a characteristic of Cisco StackWise technology?

A. It is supported on the Cisco 4500 series.

B. It supports devices that are geographically separated

C. It combines exactly two devices.

D. It uses proprietary cabling.

Correct Answer: *D*
Reference:
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-stackwise-architecture-cte-en.html

Community vote distribution

D (100%)

djedeen 3 months, 1 week ago

Selected Answer: D

There are 3 different technologies:
VSS: Cat 4500, 6500: std 1/10G, can be geo separated
Stackwise: 3750: up to 9 switches, proprietary cables, close range
Stackwise Virtual: Cat 9400,9500,9600, some 3850s: geo distribution works, more like VSS.

upvoted 1 times

Lungful 4 months ago

Selected Answer: D

I think D. Newer versions of StackWise can support more than 2 devices. VSS from question #84 supports only 2 devices.
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-stackwise-cat9200-series-wp-cte-en.html

upvoted 1 times

alex711 4 months, 2 weeks ago

I think, C is correct.

upvoted 1 times

Ricksonbyarmbar 4 months, 3 weeks ago

no, the ans is C

upvoted 1 times

GeorgeFortiGate 1 year ago

Selected Answer: D

Cisco Stackwise switches. It is proprietary

upvoted 4 times

Question #385 *Topic 1*

What is one primary REST security design principle?

A. fail-safe defaults

B. password hash

C. adding a timestamp in requests

D. OAuth

Correct Answer: *A*

Community vote distribution

A (100%)

aaabattery Highly Voted 8 months, 1 week ago

Selected Answer: A

- Least Privilege
- Fail-Safe Defaults
- Economy of Mechanism
- Complete Mediation
- Open Design
- Separation of Privilege
- Least Common Mechanism
- Psychological Acceptability

https://medium.com/strike-sh/rest-security-design-principles-434bd6ee57ea

upvoted 5 times

nushadu Most Recent 11 months, 2 weeks ago

Selected Answer: A

Fail-Safe Defaults
A user's default access level to any resource in the system should be "denied" unless they have been granted a "permit" explicitly.

upvoted 3 times

```
response = requests.patch(
     url = 'https://192.168.1.1/restconf/dataCisco-IOS-XE-
native:native/interface/GigabitEthernet=2',
     auth = ('admin', 'admin'),
     headers = {
          'Accept':'application/yang-data+json',
          'Content-Type': 'application/yang-data+json'
     },
     data = json.dumps({
          'Cisco-IOS-XE-native:GigabitEthernet': {
               'ip': {
                    'address': {
                         'primary': {
                              'address": '10.10.10.1',
                              'mask': '255.255.255.0'
                         }
                    }
               }
          }
     }),
     verify = False)

#Print the HTTP response code
print('Response Code: ' + str(response.status_code))
```

Refer to the exhibit. After the code is run on a Cisco IOS-XE router, the response code is 204. What is the result of the script?

A. The configuration fails because interface GigabitEthernet2 is missing on the target device.

B. Interface GigabitEthemet2 is configured with IP address 10.10.10.1/24.

C. The configuration fails because another interface is already configured with IP address 10.10.10.1/24.

D. The configuration is successfully sent to the device in cleartext.

Correct Answer: *B*

Community vote distribution

B (80%) A (17%)

Darude Highly Voted 1 year, 1 month ago

Selected Answer: B

Provided answer is correct
https://ultraconfig.com.au/blog/restconf-tutorial-everything-you-need-to-know-about-restconf-in-2020/
please don't comment if you havent reference to prove it.

upvoted 12 times

Manvek Most Recent 4 months, 2 weeks ago

Selected Answer: B

HTTP code 2xx means the request was successful. This discard but A and C as possible answers.

204 (No content) indicates the server fulfilled the request but has no body to return. Looking at the script, it just ask to configure the equipment and it expect no response, so B is the answer.

upvoted 1 times

dragonwise 7 months, 3 weeks ago

Selected Answer: D

Code: 204

Status Name: No Content

Description:
The request has succeeded, but the response has no additional information to send

upvoted 1 times

Just_little_me 1 week, 6 days ago

D = The configuration is successfully sent to the device in cleartext. <-- its https so how can it be in cleartext

upvoted 1 times

mhizha 6 months, 4 weeks ago

The problem with D is that the script is using HTTPS and that will discredit the "clear test part"

upvoted 2 times

kewokil120 11 months ago

Selected Answer: B

B , 2xx = success

upvoted 2 times

Fadhelben 11 months, 2 weeks ago

Selected Answer: B

Given answer is correct.
From RFC 7231 Section 6.3.5:
The 204 (No Content) status code indicates that the server has successfully fulfilled the request and that there is no additional content to send in the response payload body. Metadata in the response header fields refer to the target resource and its selected representation after the requested action was applied.

upvoted 3 times

dogdoglee 12 months ago

Selected Answer: B

B , 2xx = success

upvoted 2 times

Stylar 1 year ago

Selected Answer: B

Guys.. 2xx HTTP range means a successful attempt. B is the correct one here.

upvoted 1 times

Ciscopass 1 year ago

Selected Answer: B

2xx http codes mean success. B is correct

upvoted 1 times

iGlitch 1 year, 1 month ago

Selected Answer: B

2xx http codes mean success, so A and C are wrong.
D says clear text which is wrong because of the (application/yang-data+json header).
Therefor B is the correct answer.

upvoted 2 times

onkel_andi 1 year, 1 month ago

Selected Answer: A

204 no content.

upvoted 2 times

network_gig 1 year, 1 month ago

404 is no content.

upvoted 1 times

AndreasThornus 12 months ago

404 is not found.
204 means the action was succesful but there is no response content to return.

upvoted 5 times

Wooker 1 year, 2 months ago

Selected Answer: A

Answer: A

upvoted 1 times

tckoon 1 year, 2 months ago

Selected Answer: A

configuration failed because of Ge2 is not found in device

204 No Content
There is no content to send for this request, but the headers may be useful. The user agent may update its cached headers for this resource with the new ones.

upvoted 2 times

MerlinTheWizard 10 months ago

Nope..
2xx are messages for success. "The 204 (No Content) status code indicates that the server has successfully fulfilled the request and that there is no additional content to send in the response payload body." - Body is empty because there is nothing more to say. This eliminates A/C.
And of course, restconf uses HTTPS, so D is no-go as well.

upvoted 3 times

Question #387 *Topic 1*

Which time protocol offers security features and utilizes site-local IPv6 multicast addresses?

A. NTPv3

B. PTP IEEE 1588v1

C. NTPv4

D. PTP IEEE 1588v2

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/15-0sy/ip6-ntpv4.html

Community vote distribution

C (100%)

Asymptote 11 months ago

Selected Answer: C
NTPv4 is an extension of NTP version 3, which supports both IPv4 and IPv6.

Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/15-0sy/ip6-ntpv4.html#:~:text=NTPv4%20is%20an%20extension%20of%20NTP%20version%203%2C%20which%20supports%20both%20IPv4%20and%20IPv6.

upvoted 2 times

kebkim 1 year, 2 months ago

The Network Time Protocol (NTP) is widely used to synchronize computer clocks in the Internet. This document describes NTP version 4 (NTPv4), which is backwards compatible with NTP version 3 (NTPv3), described in RFC 1305, as well as previous versions of the protocol. NTPv4 includes a modified protocol header to accommodate the Internet Protocol version 6 address family.
https://www.rfc-editor.org/rfc/rfc5905.html

upvoted 4 times

```
Router1#
Router1#show run int tunnel 0
Building configuration...

Current configuration : 95 bytes
!
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel destination 192.168.10.2
end

Router1#show ip int br
Interface                  IP-Address      Ok? Method Status                Protocol
GigabitEthernet0/0         192.168.1.1     YES manual up                    up
GigabitEthernet0/1         unassinged      YES unset  administratively down down
GigabitEthernet0/2         unassinged      YES unset  administratively down down
GigabitEthernet0/3         unassinged      YES unset  administratively down down
Loopback0                  192.168.10.1    YES manual up                    up
Tunnel0                    172.16.1.1      YES manual up                    down
Router1#
```

Refer to the exhibit. Which command must be applied to Router1 to bring the GRE tunnel to an up/up state?

A. Router1(config-if)#tunnel source Loopback0

B. Router1(config-if)#tunnel mode gre multipoint

C. Router1(config-if)#tunnel source GigabitEthernet0/1

D. Router1(config)#interface tunnel0

Correct Answer: *A*

Community vote distribution

A (100%)

mgiuseppe86 2 months, 2 weeks ago

A is right but that is just strange business.
How can lo0 on R1 talk to lo0 on R2 unless there are static routes that use g0/0 as their gateway.

upvoted 1 times

endy023 10 months, 4 weeks ago

the given answer is correct because int tunnel 0 is wrong not specified !, G0/1 is not assigned and wont work, only the LO interface works and it matches the ip scheme.

upvoted 1 times

markymark874 10 months, 4 weeks ago

Selected Answer: A

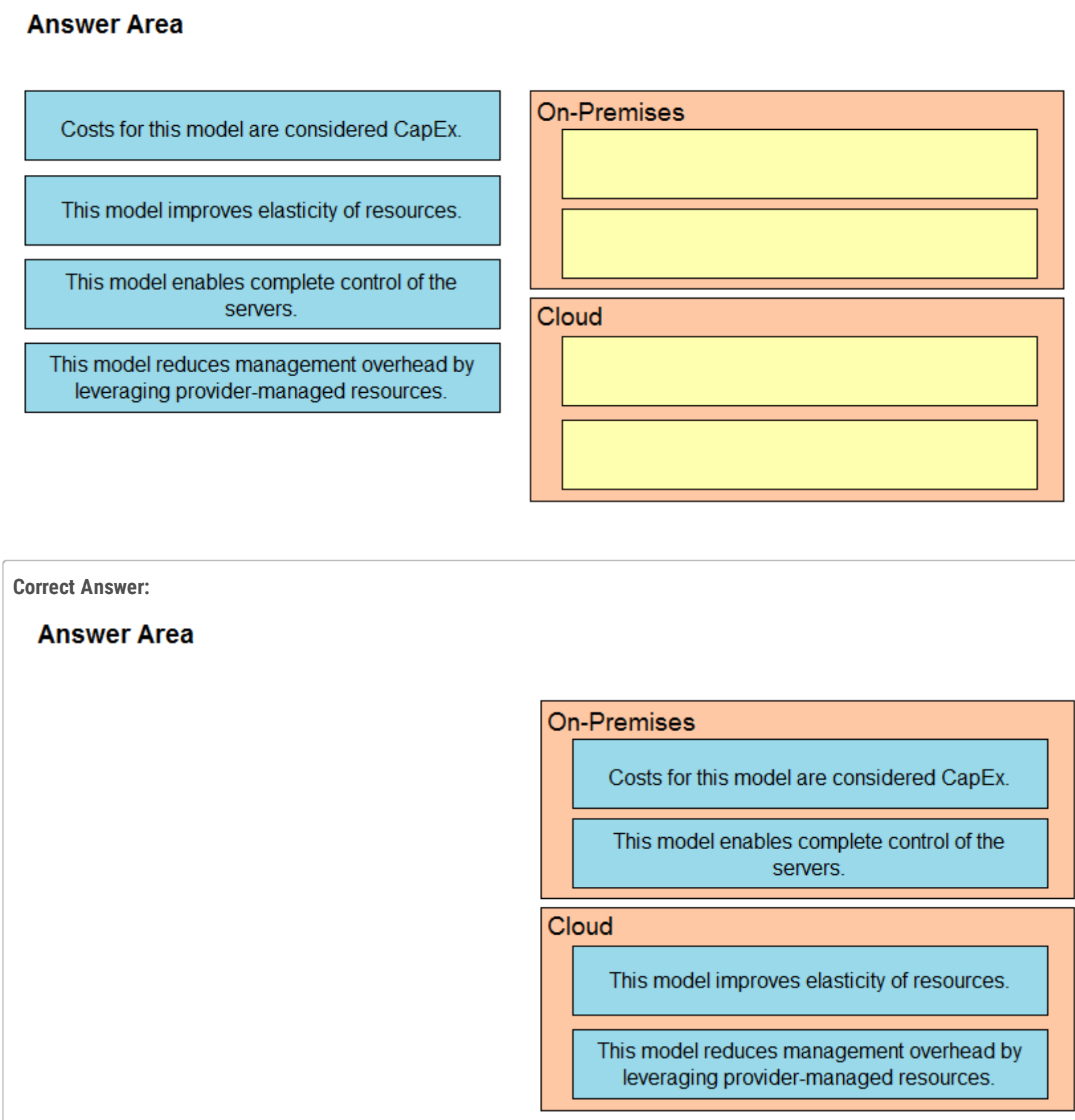
A is correct bec of the destination IP

upvoted 2 times

DRAG DROP -

Drag and drop the characteristics from the left onto the infrastructure deployment models on the right.

Select and Place:



Correct Answer:

Asymptote Highly Voted 11 months ago

100% correct

upvoted 5 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Provided answers are correct.... for a change.

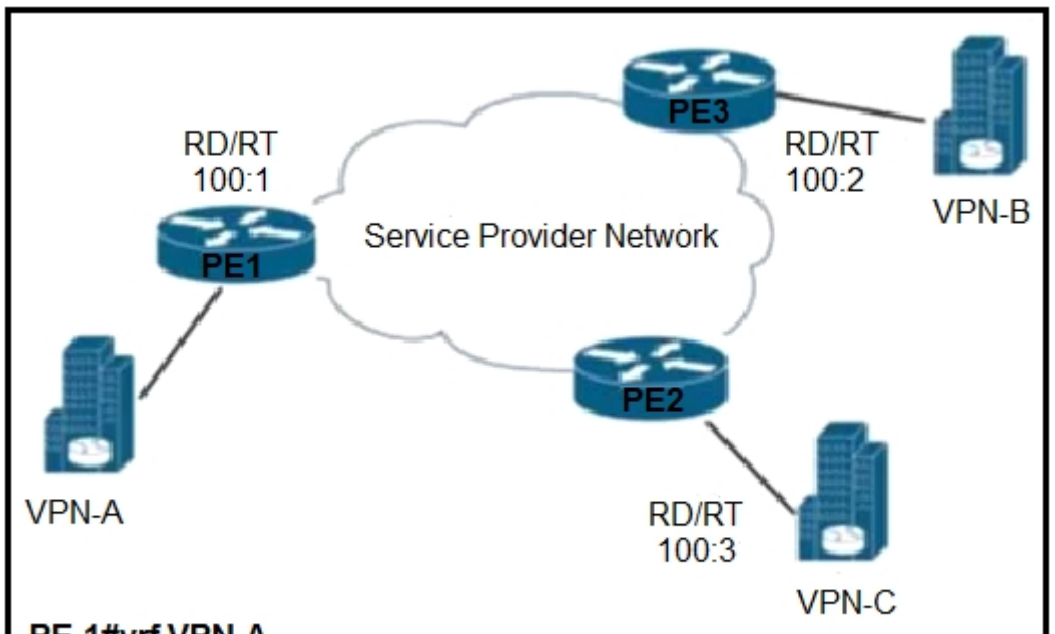
upvoted 1 times

Lungful 4 months ago

Answer is correct.

upvoted 1 times

Question #390 *Topic 1*




```
PE-1#vrf VPN-A
 address-family ipv4 unicast
 import route-target 100:3
 export route-target 100:1
!
PE1# show vrf all detail
VRF VPN-A; RD 1:100; VPN ID not set
Description not set
Interfaces:
 GigabitEthernet0/0/0/0
Address family IPV4 Unicast
 Import VPN route-target communities:
  RT:100:3
 Export VPN route-target communities:
  RT:100:1
 No import route policy
 No export route policy
!
```

Refer to the exhibit. VPN-A sends point-to-point traffic to VPN-B and receives traffic only from VPN-C. VPN-B sends point-to-point traffic to VPN-C and receives traffic only from VPN-A. Which configuration is applied?

A. PE-2 vrf VPN-B address-family ipv4 unicast import route-target 100:1 export route-target 100:2

B. PE-3 vrf VPN-B address-family ipv4 unicast import route-target 100:2 export route-target 100:2

C. PE-2 vrf VPN-B address-family ipv4 unicast import route-target 100:2 export route-target 100:2

D. PE-3 vrf VPN-B address-family ipv4 unicast import route-target 100:1 export route-target 100:2

Correct Answer: *A*

Community vote distribution

D (100%)

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: D

VPN-A sends point-to-point traffic to VPN-B -> VPN-B must import RT value that VPN-A exports (100:1).

upvoted 11 times

djedeen Most Recent 2 months, 2 weeks ago

Selected Answer: D

Good point - cannot export what you don't originate so this rules out A & C. Of B & D only D matches the flow described.

upvoted 1 times

danman32 4 months ago

Analyzing this question with the comments you all gave clarified a lot with this RD/RT business.
OCG did a horrible job explaining communities in relation to VRFs.

upvoted 2 times

ihateciscoreally 3 months, 1 week ago

4 retarded amigos who wrote OCG dedicated TWO PAGES for VRF (VRF-lite to be exact). so yeah, VRF was covered in maybe 5%.

upvoted 1 times

olaniyijt 7 months, 3 weeks ago

Answer is D

A.
PE-2 vrf VPN-B
address-family ipv4 unicast
import route-target 100:1
export route-target 100:2

B.
PE-3 vrf VPN-B address-family ipv4 unicast
import route-target 100:2
export route-target 100:2

C.
PE-2 vrf VPN-B address-family ipv4 unicast
import route-target 100:2
export route-target 100:2

D.
PE-3 vrf VPN-B address-family ipv4 unicast
import route-target 100:1
export route-target 100:2

upvoted 1 times

LanreDipeolu 3 months ago

Niyi, you cannot export what you don't originate. Your export route-target 100:2 from PE-3 is not appropriate. That is why the post answer "A" is right.

upvoted 1 times

Nickplayany 9 months, 1 week ago

Selected Answer: D

It´s D just follow the already given path and change the import export

upvoted 2 times

KinLeung0413 10 months ago

Can anyone tell me why the suggested answer is A? From my acknowledgement, the answer is D. I do not understand why the answer is A.

upvoted 2 times

PureInertiaCopy 3 months, 2 weeks ago

So I just worked it out to be A myself. I have little to no knowledge of this topic so I was using logical deduction.

I thought that the question was asking what configuration is causing VPN C to response to VPN A when VPN A wants to talk to VPN B.

Answer option A was the only one that I could think that could be causing that. Now that I have seen that everyone is saying it's D. I'm just confused.

upvoted 1 times

PureInertiaCopy 3 months, 2 weeks ago

Just realised that my initial reasoning makes no sense...
I'm not sure how I arrived at that conclusion. Answer option D is the only one that would make sense. I must have misread the question.

upvoted 1 times

markymark874 10 months, 2 weeks ago

Selected Answer: D

Asnwer is D . Pe3 imports from pe1

upvoted 1 times

nasaexam 12 months ago

Selected Answer: D

Answer is D
Export of 100:2 makes sense only from PE3, which excludes answers A and C.
VPN-C receives traffic from VPN-A, so PE-3 imported 100:1. That is answer D

upvoted 1 times

danman32 4 months ago

Did you mean VPN-B receives traffic from VPN-A?

upvoted 1 times

danman32 4 months ago

I also realized for answer B, it would be importing its own routes (PE-3 import 100.2 which is its own RD) and that doesn't make sense either.
So only answer that makes any sense would be D.

upvoted 1 times

tckoon 1 year, 2 months ago

Selected Answer: D

Answer is D , configure it on PE3

upvoted 1 times

Pamirt 1 year, 2 months ago

Selected Answer: D

the correct answer is D

upvoted 3 times

Question #391 *Topic 1*

A customer wants to use a single SSID to authenticate IoT devices using different passwords. Which Layer 2 security type must be configured in conjunction with
Cisco ISE to achieve this requirement?

A. Central Web Authentication

B. Cisco Centralized Key Management

C. Identity PSK

D. Fast Transition

Correct Answer: *C*

Community vote distribution

C (100%)

SergeBesse Highly Voted 1 year, 2 months ago

Selected Answer: C

With the advent of internet of things, the number of devices that connect to the internet is increased multifold. Not all of these devices support 802.1x supplicant and need an alternate mechanism to connect to the internet. One of the security mechanisms, WPA-PSK could be considered as an alternative. With the current configuration, the pre-shared-key is the same for all clients that connect to the same WLAN. In certain deployments such as Educational Institutions, this results in the key being shared to unauthorized users resulting in security breach. Therefore, above mentioned and other requirements lead to the need for provisioning unique pre-shared keys for different clients on a large scale.

Identity PSKs are unique pre-shared keys created for individuals or groups of users on the same SSID.

No complex configuration required for clients. The same simplicity of PSK, making it ideal for IoT, BYOD, and guest deployments.

Supported on most devices, where 802.1X may not, enabling stronger security for IoT.

Easily revoke access, for a single device or individual, without affecting everyone else.

Thousands of keys can easily be managed and distributed via the AAA server.

upvoted 15 times

Rcont Most Recent 4 months, 2 weeks ago

Selected Answer: C

the answer is correct.

upvoted 1 times

Question #392 *Topic 1*

In which two ways does TCAM differ from CAM? (Choose two.)

A. CAM is used to make Layer 2 forwarding decisions, and TCAM is used for Layer 3 address lookups.

B. CAM is used by routers for IP address lookups, and TCAM is used to make Layer 2 forwarding decisions.

C. CAM is used for software switching mechanisms, and TCAM is used for hardware switching mechanisms.

D. The MAC address table is contained in TCAM, and ACL and QoS information is stored in CAM.

E. The MAC address table is contained in CAM, and ACL and QoS information is stored in TCAM.

Correct Answer: *AE*

Community vote distribution

AE (100%)

LanreDipeolu 3 months ago

AE is the correct answer for this. Because of QoS storage in TCAM and Layer 3 address look-up by TCAM

upvoted 1 times

ihateciscoreally 3 months, 1 week ago

A,C and E are correct here.

upvoted 1 times

Colmenarez 4 months ago

Selected Answer: AE

A & E are correct

upvoted 2 times

Rowdy_47 5 months, 2 weeks ago

Selected Answer: AE

"The CAM table is the primary table used to make Layer 2 forwarding decisions."
A- Correct, therefore B incorrect

As frames arrive on switch ports, the source MAC addresses are learned and recorded in the CAM table.

TCAM provides three results: 0, 1, and "don't care." TCAM is most useful for building tables for searching on longest matches such as IP routing tables organized by IP prefixes. The TCAM table stores ACL, QoS and other information generally associated with upper-layer processing.
E- Correct, therefore D incorrect

Correct answers are A and E

https://community.cisco.com/t5/networking-knowledge-base/cam-content-addressable-memory-vs-tcam-ternary-content/ta-p/3107938

upvoted 1 times

straightAnswers 8 months ago

I think. C also correct options.

upvoted 2 times

HarwinderSekhon 5 months, 3 weeks ago

Agree. TCAM is hardware

upvoted 2 times

CCNPWILL 1 month, 2 weeks ago

CAM is not software switching mechanism though. its all forwarded using CEF. even layer 2. which is hardware.

upvoted 1 times

Ioannis34 11 months ago

provided answer is correct

upvoted 4 times

Question #393 *Topic 1*

When firewall capabilities are considered, which feature is found only in Cisco next-generation firewalls?

A. malware protection

B. stateful inspection

C. traffic filtering

D. active/standby high availability

Correct Answer: *A*

Community vote distribution

A (100%)

shubhambala Highly Voted 1 year, 2 months ago

Selected Answer: A

cisco flexing

upvoted 11 times

Backward_CEE 6 months ago

like always

upvoted 3 times

SergeBesse Highly Voted 1 year, 2 months ago

Selected Answer: A

Malware protection
IPS/IDS
URL Filtering

upvoted 5 times

Bluntedcase Most Recent 5 months, 2 weeks ago

Pretty arrogant of Cisco to make this statement... Palo Alto & Checkpoint also offer malware protection

upvoted 4 times

Lungful 4 months ago

Right? I was like, "that doesn't sound right"...

upvoted 1 times

Question #394 *Topic 1*

A network engineer is enabling HTTPS access to the core switch, which requires a certificate to be installed on the switch signed by the corporate certificate authority. Which configuration commands are required to issue a certificate signing request from the core switch?

A. Core-Switch(config)#crypto pki enroll Core-Switch Core-Switch(config)#ip http secure-trustpoint Core-Switch

B. Core-Switch(config)#ip http secure-trustpoint Core-Switch Core-Switch(config)#crypto pki enroll Core-Switch

C. Core-Switch(config)#crypto pki trustpoint Core-Switch Core-Switch(ca-trustpoint)#enrollment terminal Core-Switch(config)#crypto pki enroll Core-Switch

D. Core-Switch(config)#crypto pki trustpoint Core-Switch Core-Switch(ca-trustpoint)#enrollment terminal Core-Switch(config)#ip http secure-trustpoint Core-Switch

Correct Answer: *D*

Community vote distribution

C (100%)

Zikosheka Highly Voted 1 year, 2 months ago

Selected Answer: C

1. generate an RSA key
2. Create a trust point.
3. Enter the command "Crypto PKI enroll"

upvoted 10 times

ihateciscoreally Most Recent 3 months, 2 weeks ago

love questions about topics not covered in blueprint and OCG. another answer to remebmer. thats why dumps are 100% justified. thank you examtopics.

upvoted 4 times

danman32 4 months ago

Since the question asks about generating CSRs and not importing a signed cert, you can eliminate A, B, and D because those have commands to assign a valid certificate with key pair to HTTPS. Can't do that until you have the certificate signing complete.

upvoted 1 times

mrtattoo 7 months ago

Selected Answer: C

definitely C
https://www.cisco.com/c/en/us/td/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/convert/sec_pki_xe_3s_book/sec_cert_enroll_pki_xe.html

upvoted 1 times

HamzaBadar 7 months, 4 weeks ago

Tested in GNS3, C is correct. Last command of option C generates certificate, but last command of option D does not generate any certificate.

upvoted 1 times

dragonwise 8 months ago

A.
Core-Switch(config)#crypto pki enroll Core-Switch
Core-Switch(config)#ip http secure-trustpoint Core-Switch

B.
Core-Switch(config)#ip http secure-trustpoint Core-Switch
Core-Switch(config)#crypto pki enroll Core-Switch

C.
Core-Switch(config)#crypto pki trustpoint Core-Switch
Core-Switch(ca-trustpoint)#enrollment terminal
Core-Switch(config)#crypto pki enroll Core-Switch

D.
Core-Switch(config)#crypto pki trustpoint Core-Switch
Core-Switch(ca-trustpoint)#enrollment terminal
Core-Switch(config)#ip http secure-trustpoint Core-Switch

upvoted 4 times

kewokil120 11 months ago

Selected Answer: C

c seems to be the best

upvoted 2 times

shubhambala 1 year, 2 months ago

Selected Answer: C

C folks

upvoted 1 times

tckoon 1 year, 2 months ago

Selected Answer: C

https://community.cisco.com/t5/vpn/certificate-signing-request-csr-guideline/td-p/2778928

1. generate an RSA key
2. Create a trust point.
3. Enter the command "Crypto PKI enroll"

upvoted 3 times

jj970us 1 year, 2 months ago

Selected Answer: C

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/convert/sec_pki_xe_3s_book/sec_cert_enroll_pki_xe.html

upvoted 1 times

Question #395 *Topic 1*

An engineer must create a new SSID on a Cisco 9800 wireless LAN controller. The client has asked to use a pre-shared key for authentication. Which profile must the engineer edit to achieve this requirement?

A. Policy

B. RF

C. Flex

D. WLAN

Correct Answer: *A*

Community vote distribution

D (100%)

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: D

WLAN Profile
...
Security Settings (i.e. PSK, 802.1x, WebAuth)

Reference: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213911-understand-catalyst-9800-wireless-contro.html#anc5

upvoted 11 times

kewokil120 Most Recent 10 months, 3 weeks ago

Selected Answer: D

D. WLAN

upvoted 2 times

Asymptote 11 months ago

Selected Answer: D

Navigate to Configuration > Wireless > WLANs > WLAN name > Security > Layer2 , and fix the password.

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213970-catalyst-9800-wireless-controllers-commo.html#:~:text=Navigate%20to%C2%A0%C2%A0Configuration%20%3E%20Wireless%20%3E%20WLANs%20%3E%20WLAN%20name%20%3E%20Security%20%3E%20Layer2%C2%A0%2C%C2%A0and%20fix%20the%20password.

upvoted 3 times

Darude 1 year ago

Selected Answer: D

WLAN Profile = SSID
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller_series_web_dg.html

upvoted 2 times

Question #396 *Topic 1*

An engineer is configuring a new SSID to present users with a splash page for authentication. Which WLAN Layer 3 setting must be configured to provide this functionality?

A. Local Policy

B. WPA2 Policy

C. CCKM

D. Web Policy

Correct Answer: *D*
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/100787-splash-page-redirect.html

Community vote distribution

D (100%)

[Removed] 5 months ago

Selected Answer: D

correct

upvoted 1 times

yeyuno 9 months, 1 week ago

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/100787-splash-page-redirect.html

D is correct, step 12
"Check the Web Policy box, and then click the Splash Page Web Redirect radio button."

Image clearly show Layer 3 settigs --> Web Policy

upvoted 2 times

Ioannis34 10 months ago

WRONG. D is correct.

upvoted 2 times

Bigbongos 10 months, 1 week ago

B is correct

upvoted 1 times

Question #397 *Topic 1*

A customer requests a design that includes GLBP as the FHRP. The network architect discovers that the members of the GLBP group have different throughput capabilities. Which GLBP load balancing method supports this environment?

A. round robin

B. host dependent

C. weighted

D. least connection

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ip-services/product_data_sheet0900aecd803a546c.html

Community vote distribution

C (100%)

kebkim Highly Voted 1 year, 2 months ago

WEIGHTED

This is the ability GLBP to place a weight on each device when calculating the amount of load sharing that will occur through MAC assignment. Each GLBP router in the group will advertise its weighting and assignment; the AVG will act based on that value.
For example, if there are two routers in a group and router A has double the forwarding capacity of router B, the weighting value of router A should be configured to be double the amount of router B.

upvoted 6 times

[Removed] Most Recent 5 months ago

Selected Answer: C

correct, as stated by @kebkim

upvoted 1 times

```
R1#show ip bgp sum
BGP router identifier 1.1.1.1, local AS number 650001
<output omitted>

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.50.2    4        65002       0       0        1    0    0 00:00:46 Idle (Admin)
```

Refer to the exhibit. Which command set changes the neighbor state from Idle (Admin) to Active?

A. R1(config)#router bgp 65001 R1(config-router)#neighbor 192.168.50.2 remote-as 65001

B. R1(config)#router bgp 65001 R1(config-router)#neighbor 192.168.50.2 activate

C. R1(config)#router bgp 65001 R1(config-router)#no neighbor 192.168.50.2 shutdown

D. R1(config)#router bgp 65002 R1(config-router)#neighbor 192.168.50.2 activate

Correct Answer: *C*

Community vote distribution

C (100%)

network_gig Highly Voted 1 year, 1 month ago

Selected Answer: C

idle (Admin) means that the BGP session is in a shutdown state and that needs to go no shut.

upvoted 5 times

Normanby 1 year ago

Not Quite...
- Idle = no work to do as I know everything. (good)
- Active = panic, because I am lost and need to find out more information. (bad)

So right now BGP is happy - shutting it down will make it unhappy, and Active.

upvoted 1 times

Normanby 1 year ago

Sorry, It is 'idle' because it is unable to even start to do anything, so removing the shutdown command will allow it to begin to try to work = Active.

upvoted 3 times

Colmenarez Most Recent 4 months ago

Selected Answer: C

ISP(config-router)#do sh ip bgp sum

BGP router identifier 2.2.2.2, local AS number 65000

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
192.168.50.2 4 65001 0 0 1 0 0 never Idle (Admin)

ISP(config-router)#no neighbor 192.168.50.2 shutdown

ISP(config-router)#do sh ip bgp sum
BGP router identifier 2.2.2.2, local AS number 65000

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
192.168.50.2 4 65001 0 0 1 0 0 never Idle

upvoted 1 times

dragonwise 8 months ago

A.
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 remote-as 65001

B.
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 activate

C.
R1(config)#router bgp 65001

R1(config-router)#no neighbor 192.168.50.2 shutdown

D.
R1(config)#router bgp 65002
R1(config-router)#neighbor 192.168.50.2 activate
upvoted 2 times

Darude 1 year, 1 month ago

Selected Answer: C

ansver is correct:
https://www.noction.com/blog/debug-bgp-states
upvoted 2 times

Question #399 *Topic 1*

A network engineer configures a WLAN controller with increased security for web access. There is IP connectivity with the WLAN controller, but the engineer cannot start a management session from a web browser. Which action resolves the issue?

A. Disable Adobe Flash Player.

B. Use a private or incognito session.

C. Use a browser that supports 128-bit or larger ciphers.

D. Disable JavaScript on the web browser.

Correct Answer: *C*

mgiuseppe86 Highly Voted 2 months, 2 weeks ago

These are the questions that really irk me about Cisco. What if this was the one question that failed me? This has NOTHING to do with being a network engineer/administrator. This is more of a desktop application troubleshooting question.

Call me oldschool but in my opinion CCNP should be straight up Routing/Switching/QoS/Firewall/*some cloud*

Not this garbage
upvoted 6 times

forccnp Most Recent 1 year ago

given answer is correct
upvoted 4 times

Question #400 *Topic 1*

What does a northbound API accomplish?

A. programmatic control of abstracted network resources through a centralized controller

B. access to controlled network resources from a centralized node

C. communication between SDN controllers and physical switches

D. controlled access to switches from automated security applications

Correct Answer: *A*

Community vote distribution

A (100%)

Stylar Highly Voted 10 months, 1 week ago

Provided answer is correct

upvoted 6 times

eddgg Most Recent 3 months, 3 weeks ago

Selected Answer: A

A northbound API (Application Programming Interface) is a type of API that allows programmatic communication and control of abstracted network resources through a centralized controller in a Software-Defined Networking (SDN) architecture.

upvoted 1 times

Question #401 *Topic 1*

In a Cisco SD-WAN solution, how is the health of a data plane tunnel monitored?

A. with IP SLA

B. ARP probing

C. using BFD

D. with OMP

Correct Answer: *C*

Community vote distribution

C (100%)

kebkim Highly Voted 1 year, 2 months ago

Cisco SD-WAN BFD :
Runs on SD-WAN tunnel to detect failures in the overlay tunnel

upvoted 5 times

eddgg Most Recent 3 months ago

Selected Answer: C

bfd is correct

upvoted 1 times

HamzaBadar 7 months, 4 weeks ago

Bidirectional Forwarding Detection is used for health check in data plane of SD-WAN.

upvoted 3 times

Question #402 *Topic 1*

Which solution do IaaS service providers use to extend a Layer 2 segment across a Layer 3 network?

A. VXLAN

B. VTEP

C. VRF

D. VLAN

Correct Answer: *A*

Community vote distribution

A (100%)

shefo1 1 month, 2 weeks ago

Selected Answer: A

The answer is **A. VXLAN**.

VXLAN is a network virtualization technology that allows Layer 2 networks to be extended across Layer 3 networks. It uses a MAC-in-UDP encapsulation scheme to create a Layer 2 tunnel over a Layer 3 network.

IaaS service providers use VXLAN to extend Layer 2 segments across their networks so that customers can have a single Layer 2 network even if their devices are located in different locations. This allows customers to easily move their devices between locations without having to reconfigure their networks.

The other options are not correct:

* VTEP (Virtual Tunnel Endpoint) is a device that encapsulates and decapsulates VXLAN traffic.
* VRF (Virtual Routing and Forwarding) is a technology that allows multiple routing tables to exist on a single router.
* VLAN (Virtual Local Area Network) is a Layer 2 technology that segments a network into multiple broadcast domains.

I hope this helps!

upvoted 2 times

Dv123456 5 months ago

Provided answer is correct

upvoted 1 times

Question #403 *Topic 1*

By default, which virtual MAC address does HSRP group 16 use?

A. c0:41:41:43:07:10

B. 00:05:5c:07:0c:16

C. 00:00:0c:07:ac:10

D. 05:00:0c:07:ac:16

Correct Answer: *C*

mgiuseppe86 2 months, 2 weeks ago

16 = 00010000 in binary then split into base16 so 0001 and 0000. Convert those individual hex bits back into decimal. so 1|0 = answer is 10

upvoted 1 times

eddgg 3 months ago

c is the right answer

upvoted 1 times

nushadu 12 months ago

tested:
val = 16
val
Out[3]: 16
hex(val)
Out[4]: '0x10'
==
C. is correct

upvoted 4 times

Japsurd 1 year ago

Vlan20 - Group 16
State is Init (interface down)
Virtual IP address is 20.0.0.1
Active virtual MAC address is unknown (MAC Not In Use)
Local virtual MAC address is 0000.0c07.ac10 (v1 default)

upvoted 1 times

Lapegues 1 year, 1 month ago

HSRPv1 uses the virtual mac address of 0000.0c07. acxx where xx represent HSRP group number. 00.00.0c.07.ac.16.

upvoted 4 times

Normanby 1 year ago

hex , so Group 16 = 10hex == 00.00.0c.07.ac.10

upvoted 3 times

kebkim 1 year, 2 months ago

The virtual MAC of HSRP is 0000.0c07.acxx with xx representing the HSRP group number in hexadecimal.

upvoted 3 times

shubhambala 1 year, 2 months ago

so is ans D?

upvoted 1 times

Refer to the exhibit. Why was the response code generated?

A. The resource was unreachable.

B. Access was denied based on the user permissions.

C. Access was denied based on the credentials.

D. The resource is no longer available on the server.

Correct Answer: *B*

Community vote distribution

B (81%) C (19%)

iGlitch Highly Voted 1 year, 1 month ago

Selected Answer: B

401 = Unauthorized (Bad credentials)
403 = Forbidden (Service refused, for insufficient permissions)

Answer is B.

upvoted 13 times

tsamoko Most Recent 2 months, 3 weeks ago

Selected Answer: C

403 ->forbiden = access no granted based on suplied credentials, 401 = unauthorized = user persmisions

upvoted 1 times

SnoopDD 11 months, 3 weeks ago

Selected Answer: C

403 Forbidden - Access not granted based on supplied credentials

upvoted 2 times

Joseph123 1 year, 2 months ago

Correct answer is C. Code 403 is bad credentials

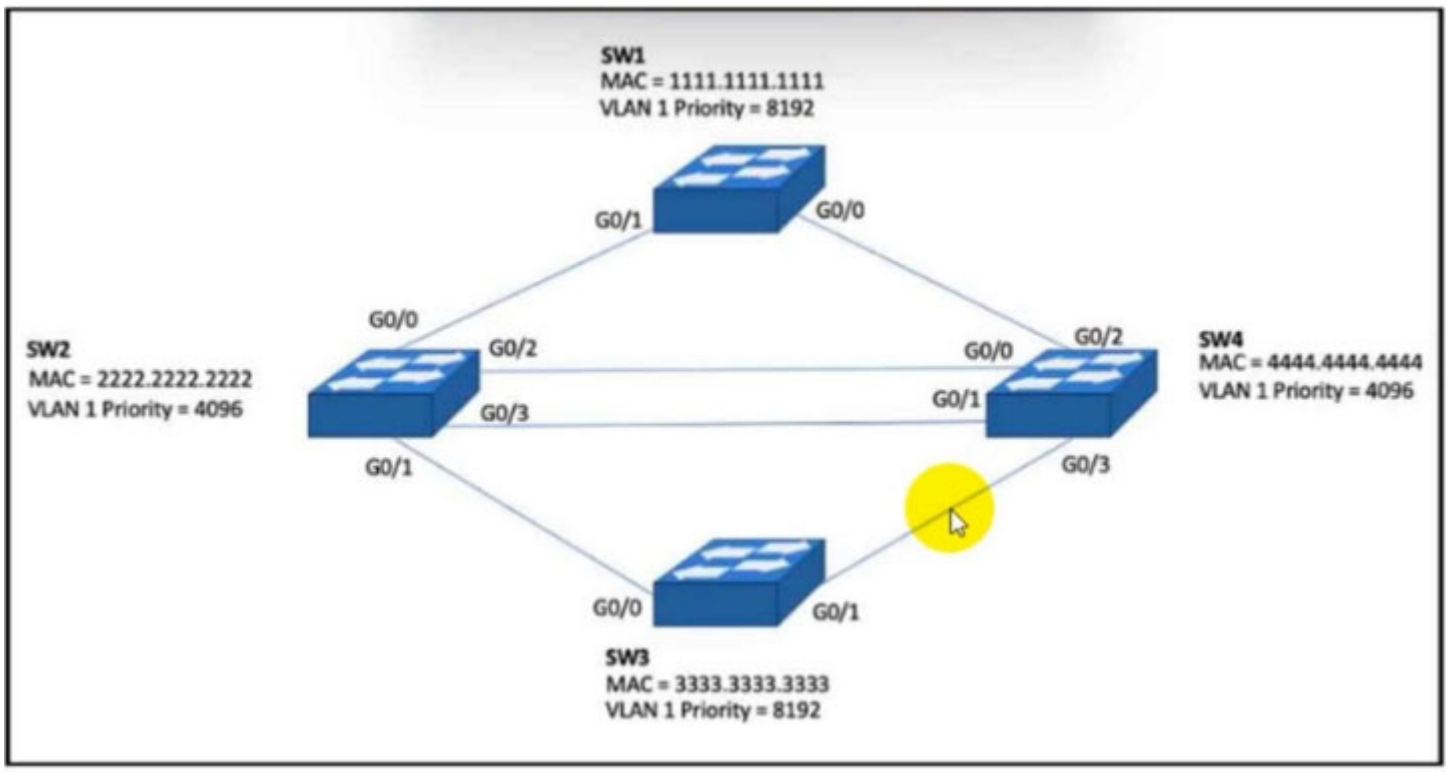
upvoted 1 times

jdholmes423 1 year, 2 months ago

The given answer is correct. If the credentials were bad, the return code would have been 401 instead. 403 implies that the creds were good, but the permissions associated with the account in question limit what resources it can access.

upvoted 9 times

Question #405 *Topic 1*



Refer the exhibit. Which configuration elects SW4 as the root bridge for VLAN 1 and puts G0/2 on SW2 into a blocking state?

A. SW4(config)#spanning-tree vlan 1 priority 0 ! SW2(config)#int G0/2 SW2(config-if)#spanning-tree cost 128

B. SW4(config)#spanning-tree vlan 1 priority 0 ! SW2(config)#interface G0/2 SW2(config-if)#spanning-tree vlan 1 port-priority 64

C. SW4(config)#spanning-tree vlan 1 priority 32768 ! SW2(config)#int G0/2 SW2(config-if)#spanning-tree cost 128

D. SW4(config)#spanning-tree vlan 1 priority 32768 ! SW2(config)#interface G0/2 SW2(config-if)#spanning-tree vlan 1 port-priority 0

Correct Answer: *A*

Community vote distribution

A (100%)

dragonwise Highly Voted 8 months ago

A.
SW4(config)#spanning-tree vlan 1 priority 0 !
SW2(config)#int G0/2
SW2(config-if)#spanning-tree cost 128

B.
SW4(config)#spanning-tree vlan 1 priority 0 !
SW2(config)#interface G0/2
SW2(config-if)#spanning-tree vlan 1 port-priority 64

C.
SW4(config)#spanning-tree vlan 1 priority 32768 !
SW2(config)#int G0/2
SW2(config-if)#spanning-tree cost 128

D.
SW4(config)#spanning-tree vlan 1 priority 32768 !
SW2(config)#interface G0/2
SW2(config-if)#spanning-tree vlan 1 port-priority 0

upvoted 6 times

danman32 Most Recent 4 months ago

Answers C and D can be eliminated as they would make SW2 root since it has priority 4096.
Answer B can also be eliminated on the surface because first it isn't specifying STP for VLAN 1, and port priority affects the port decision for the neighboring switch (SW4), not the local switch. But SW4 is root so both of its ports will be designated.
I goofed misinterpreted cost as priority, also bothered that it wasn't setting cost on STP instance for VLAN1.

upvoted 1 times

Colmenarez 4 months ago

Selected Answer: A

La respuesta correcta es A.

SW4 spanni vlan 1 priority 0 <---- esto fuerza al SW4 ser el root para vlan 1
SW2 int G 0/2
SW2 spann cost 128 <--- este comando realmente no esta haciendo nada, ya que el costo por default de casa puerto es 128. pero igual el puerto G0/2 por orden de preferencia

upvoted 2 times

HungarianDish 8 months, 2 weeks ago

Selected Answer: A

https://community.cisco.com/t5/routing/spanning-tree-with-port-priority/td-p/1815059
"You just configure "port priority" on upstream switches on designated ports or modify "port cost" on downstream switches on root ports"

https://packetlife.net/blog/2008/sep/5/spanning-tree-port-costs/
The default cost of the 1 Gig link would be 4. Changing the cost to 128 makes the link less preferred.

upvoted 4 times

x3rox 10 months ago

Selected Answer: A

This is the correct explanation of why option A is correct:
*spanning-tree vlan 1 priority 0 is hardcoding SW4 to be the root as it has the lowest priority
*By changing the cost of the link (which is first looked at before the sender Port-ID) on SW2 causes SW2 to elect the other port as a RP as the other link has lowest cost then 128.

upvoted 4 times

nushadu 11 months, 1 week ago

Selected Answer: A

! root switch, 2 links to fat-end:
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 0
sw2(config-if)#do s spann vl 1

VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 1
Address aabb.cc00.4000
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 1 (priority 0 sys-id-ext 1)
Address aabb.cc00.4000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/3 Desg FWD 100 128.4 Shr
Po2 Desg FWD 100 128.65 Shr

sw2(config-if)#

upvoted 1 times

nushadu 11 months, 1 week ago

far-end, lower STP port cost (99 in this case) wins:

sw1(config-if)#do s spann vl 1

VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 1
Address aabb.cc00.4000
Cost 99
Port 65 (Port-channel2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4097 (priority 4096 sys-id-ext 1)
Address aabb.cc00.1000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 100 128.1 Shr
Et0/3 Altn BLK 100 128.4 Shr
Po2 Root FWD 99 128.65 Shr <<<<<<<<<<<<<<<<<<<< current root port

sw1(config-if)#

upvoted 1 times

nushadu 11 months, 1 week ago

removing cost and root port has been changed:
sw1(config-if)#no spanning-tree cost 99
sw1(config-if)#do s spann vl 1

VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 1
Address aabb.cc00.4000
Cost 100
Port 4 (Ethernet0/3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4097 (priority 4096 sys-id-ext 1)
Address aabb.cc00.1000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/0 Desg BLK 100 128.1 Shr
Et0/3 Root FWD 100 128.4 Shr <<<<<<<<<<<<<<<<<<<<
Po2 Altn BLK 100 128.65 Shr

sw1(config-if)#

upvoted 1 times

forccnp 1 year ago

Selected Answer: A

A is correct

upvoted 2 times

Question #406 *Topic 1*

What happens when a FlexConnect AP changes to standalone mode?

A. All client roaming continues to work.

B. Only clients on central switching WLANs stay connected.

C. All clients on all WLANs are disconnected.

D. All controller-dependent activities stop working except the DFS.

Correct Answer: *C*

Community vote distribution

D (94%) 6%

dnjJ56 Highly Voted 11 months, 2 weeks ago

Selected Answer: D

When a FlexConnect access point enters standalone mode, it disassociates all clients that are on centrally switched WLANs. [not all clients, locally switched WLAN clients stay connected]

Controller-dependent activities, such as network access control (NAC) and web authentication (guest access), are disabled, and the access point does not send any intrusion detection system (IDS) reports to the controller.

Most radio resource management (RRM) features (such as neighbor discovery; noise, interference, load, and coverage measurements; use of the neighbor list; and rogue containment and detection) are disabled. However, a FlexConnect access point supports dynamic frequency selection in standalone mode.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html

upvoted 12 times

mikhailov_ivan90 Highly Voted 10 months, 1 week ago

Selected Answer: D

in my oppinion it should be D. It's the question for catching you , make you wrong and bring your money to Cisco again :) Read the question several time please, each word. they asked about "standalone" mode, it's a sub mode only within FlexConnect mode, it's not about local and flexconnect. So, an AP won't be rebooted 100%. The key word in the C option is "all" wlans, but in the book we have an exact phrase which means that all clients with centrally switched wlans only will be disconected, it's not all wlans. By exception method D is correct.

upvoted 7 times

Chiaretta Most Recent 7 months, 1 week ago

Selected Answer: D

D is the correct answer

upvoted 1 times

Cooldude89 9 months, 2 weeks ago

Selected Answer: D

D is more appropriate

upvoted 2 times

TSKARAN 10 months, 1 week ago

Selected Answer: C

When AP is changed from local mode to FlexConnect mode, the AP does not reboot. However, when the AP is changed from FlexConnect mode to local mode, the AP reboots and displays the following error message:

Warning: Changing AP Mode will reboot the AP and will rejoin the controller after a few minutes. Are you sure you want to continue?

Ref: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html

upvoted 1 times

Clauster 8 months, 2 weeks ago

And doesn't rebooting disconnect all of the clients in the WLANs?

upvoted 1 times

bora4motion 11 months, 4 weeks ago

Selected Answer: C

I'm going with C here.

upvoted 1 times

Normanby 1 year ago

Selected Answer: C

When you change the 'mode' of an AP, it reboots, so how can it still talk to clients while rebooting ? - all clients are disconnected.

upvoted 1 times

Caradum 1 year ago

Standalone Mode is a submode of a flexconnect AP. A flexconnect falls into the 'standalone mode' when it looses connection to the WLC, so no reboot occurs.

upvoted 1 times

Normanby 1 year ago

Thank you - Finally Found it:-
When a FlexConnect access point enters standalone mode, it disassociates all clients that are on centrally switched WLANs. For web-authentication WLANs, existing clients are not disassociated, but the FlexConnect access point stops sending beacons when the number of associated clients reaches zero (0). It also sends disassociation messages to new clients associating to web-authentication WLANs. Controller-dependent activities, such as network access control (NAC) and web authentication (guest access), are disabled, and the access point does not send any intrusion detection system (IDS) reports to the controller. Most radio resource management (RRM) features (such as neighbor discovery; noise, interference, load, and coverage measurements; use of the neighbor list; and rogue containment and detection) are disabled. However, a FlexConnect access point supports dynamic frequency selection in standalone mode.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html

Not a Great Question :(

upvoted 3 times

Normanby 1 year ago

When you change the 'mode' of an AP, it reboots, so how can it still talk to clients while rebooting ? - all clients are disconnected.

upvoted 1 times

coreyx 1 year, 1 month ago

D is correct.
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213911-understand-catalyst-9800-wireless-contro.html

upvoted 2 times

Joseph123 1 year, 2 months ago

Selected Answer: D

Correct answer is D

upvoted 1 times

PALURDIN 1 year, 2 months ago

Selected Answer: D

answer is D

upvoted 3 times

jj970us 1 year, 2 months ago

Selected Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html

upvoted 4 times

PALURDIN 1 year, 2 months ago

Confirmmed: http://revolutionwifi.blogspot.com/2010/06/h-reap-deployment-guidelines-and.html#:~:text=RRM%20features%20are%20disabled%20when%20in%20standalone%20mode%20(DFS/TPC%20is%20still%20supported%2C%20however)

upvoted 2 times

Question #407 *Topic 1*

If the maximum power level assignment for global TPC 802.11a/n/ac is configured to 10 dBm. which power level effectively doubles the transmit power?

A. 13 dBm

B. 14 dBm

C. 17 dBm

D. 20 dBm

Correct Answer: *C*

Community vote distribution

A (100%)

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: A

3 dB of gain = +3 dB = doubles signal strength (Let's say, the base is P. So 10*log10(P/P) = 10*log101 = 0 dB and 10*log10(2P/P) = 10*log10(2) = 3dB -> double signal)

upvoted 17 times

siteoforigin 1 year, 2 months ago

Agreed, page 493 of the Cert guide goes over this. Answer is A

upvoted 2 times

Joseph123 Highly Voted 1 year, 2 months ago

Selected Answer: A

Remember the rule of 3s and 10s

upvoted 11 times

ermanzan Most Recent 5 months, 2 weeks ago

Selected Answer: A

Agree with A, 3 dB doubles the signal stregth

upvoted 1 times

mellohello 9 months, 1 week ago

Selected Answer: A

Law of 3s

upvoted 2 times

rafaelinho88 9 months, 4 weeks ago

Selected Answer: A

If the maximum power level assignment for global Transmit Power Control (TPC) for 802.11a/n/ac is configured to 10 dBm, then doubling the transmit power would require an increase of 3 dBm. A 3 dBm increase represents a doubling of the power level, so a power level of 13 dBm would effectively double the transmit power. However, it's important to note that TPC settings can vary depending on the specific implementation and regulatory requirements, so the actual power levels available may be different in different situations.

upvoted 3 times

Rose66 10 months, 3 weeks ago

Selected Answer: A

aggree with jj970us

upvoted 1 times

Stylar 1 year ago

Selected Answer: A

Definitely A.

upvoted 1 times

Gedson 1 year ago

Selected Answer: A

Definitivamente es la A

upvoted 1 times

H3kerman 1 year ago

Selected Answer: A

it's widely known fact +3dB means doubled

upvoted 1 times

Caledonia 1 year, 2 months ago

Selected Answer: A

The answer is A, it is just math simply.

upvoted 3 times

siteoforigin 1 year, 2 months ago

Selected Answer: A

Page 493 of the Cert guide goes over this. Answer is A

upvoted 2 times

Question #408 *Topic 1*

An engineer must create an EEM script to enable OSPF debugging in the event the OSPF neighborship goes down. Which script must the engineer apply?

A. event manager applet ENABLE_OSPF_DEBUG event syslog pattern ג€%OSPF-5-ADJCHG: Process 6, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWNג€ action 1.0 cli command ג€enableג€ action 2.0 cli command ג€debug ip ospf eventג€ action 3.0 cli command ג€debug ip ospf adjג€ action 4.0 syslog priority informational msg ג€ENABLE_OSPF_DEBUGג€

B. event manager applet ENABLE_OSPF_DEBUG event syslog pattern ג€%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULLג€ action 1.0 cli command ג€debug ip ospf eventג€ action 2.0 cli command ג€debug ip ospf adjג€ action 3.0 syslog priority informational msg ג€ENABLE_OSPF_DEBUGג€

C. event manager applet ENABLE_OSPF_DEBUG event syslog pattern ג€%OSPF-1-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWNג€ action 1.0 cli command ג€debug ip ospf eventג€ action 2.0 cli command ג€debug ip ospf adjג€ action 3.0 syslog priority informational msg ג€ENABLE_OSPF_DEBUGג€

D. event manager applet ENABLE_OSPF_DEBUG event syslog pattern ג€%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULLג€ action 1.0 cli command ג€enableג€ action 2.0 cli command ג€debug ip ospf eventג€ action 3.0 cli command ג€debug ip ospf adjג€ action 4.0 syslog priority informational msg ג€ENABLE_OSPF_DEBUGג€

Correct Answer: *A*

Community vote distribution

A (100%)

x3rox Highly Voted 10 months ago

Selected Answer: A

This is the correct explanation of why A is the correct answer:
There are 4 options, but only 2 has "FULL to DOWN" which is what we are tying to catch. Out of these two only A begin the script with "enable" which is required in EEM because the applet assumes that the user is in EXEC mode, not privileged EXEC or config mode.

upvoted 14 times

myhdtv6 Most Recent 4 months, 1 week ago

Guys, other then the technicalities of OSPF, I took this question with the different prospect.

6 is the informational debug msgs right ??

I went with it straight, is that wrong ?

upvoted 1 times

ALOVEVIKS 6 months, 2 weeks ago

I have no proper output of this question, how to fix ?

upvoted 1 times

robi1020 11 months, 3 weeks ago

Selected Answer: A

It need to be "FULL to DOWN" is syslog 1st line

upvoted 2 times

Raipen24 1 year ago

5 - notification
6-informational

A is on 6 debug info

upvoted 3 times

HungarianDish 8 months ago

debug is 7, informational is 6 (default). it sending a syslog message of priority level 6.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-a2.html

upvoted 2 times

Tacolicious 1 year ago

Selected Answer: A

Only A&D enable a debug based on earlier events. So B&C are definitely wrong. Between A and D: A also mentions the OSPF neighborship going down, which D doesn't. So the correct answer here is A

upvoted 2 times

onkel_andi 1 year, 1 month ago

Selected Answer: A

A is correct
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-16/216091-best-practices-and-useful-scripts-for-ee.html

upvoted 1 times

Question #409 *Topic 1*

A customer wants to provide wireless access to contractors using a guest portal on Cisco ISE. The portal is also used by employees. A solution is implemented, but contractors receive a certificate error when they attempt to access the portal. Employees can access the portal without any errors.
Which change must be implemented to allow the contractors and employees to access the portal?

A. Install a trusted third-party certificate on the Cisco ISE.

B. Install an internal CA signed certificate on the Cisco ISE.

C. Install a trusted third-party certificate on the contractor devices.

D. Install an internal CA signed certificate on the contractor devices.

Correct Answer: *B*

Community vote distribution

A (78%) D (22%)

zpacket Highly Voted 1 year, 1 month ago

Selected Answer: A

"It is recommended to use the Company Internal CA for Admin and EAP certificates, and a publicly-signed certificate for Guest/Sponsor/Hotspot/etc portals. The reason is that if a user or guest comes onto the network and ISE portal uses a privately-signed certificate for the Guest Portal, they get certificate errors or potentially have their browser block them from the portal page. To avoid all that, use a publicly-signed certificate for Portal use to ensure better user experience".

Thanks @jj970us for the reference -
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215621-tls-ssl-certificates-in-ise.html

upvoted 13 times

AndreasThornus 12 months ago

I agree with this one. Why would you go to the effort of making a web portal available, only to have to install certificates on contractor devices you don't manage.

upvoted 3 times

mikhailov_ivan90 Highly Voted 10 months, 2 weeks ago

Selected Answer: D

tricky question with several meaning from Cisco again, looks like they don't want to check your knowledge but want to make you get mistake and pay for the exam again (capitan obvious). So, they didn't mention in the question anything about kind of contractor devices , right? it can be anything , even something very old without the last chain of "green" public CAs, right? In this case there is only one option - it's adding the ISE cert to trusted on on all devices. I'd choose D.

upvoted 6 times

HarwinderSekhon 5 months, 3 weeks ago

That is why cisco exams except CCNA are loosing popularity.

upvoted 3 times

danman32 4 months ago

Not to mention the widening scope of trivia knowledge for the exams and the cost

upvoted 1 times

rami_mma Most Recent 8 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

PeterTheCheater 1 year ago

Selected Answer: D

If the issue is not happening with employees devices means that the certificate on ISE is signed by an Internal CA recognised by employees devices
Installing a third-party certificate on ISE has a cost, while installing a internal CA signed certificate on contractor devices does not.
And since they are your contractors,i.e. work for you, you can do this certificate installation. It is not like providing public wifi to citizens.
I think in this case the right answer is D.

upvoted 2 times

danman32 4 months ago

Contractors could be anyone, not just someone you have effectively as an employee.

upvoted 1 times

Normanby 1 year ago

Selected Answer: A

A is the 'best' solution , but I have done 'D' in the past - faster and cheaper :)

upvoted 5 times

Larp 1 year, 1 month ago

Selected Answer: A

A is the answer.
The certificate needs to be trusted by contractor's computers, which will not trust the internal CA of the company.

upvoted 1 times

onkel_andi 1 year, 1 month ago

Selected Answer: A

Contractors would get a certificate error if the answer would be B) because they don't trust the CA from the Company.
So answer is A)

upvoted 2 times

Caledonia 1 year, 2 months ago

Selected Answer: A

It is A

upvoted 2 times

jj970us 1 year, 2 months ago

Selected Answer: A

Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215621-tls-ssl-certificates-in-ise.html

upvoted 4 times

Question #410 *Topic 1*

An engineer must configure a new loopback interface on a router and advertise the interface as a /24 in OSPF. Which command set accomplishes this task?

A. R2(config)#interface Loopback0 R2(config-if)#ip address 172.22.2.1 255.255.255.0 R2(config-if)#ip ospf network broadcast R2(config-if)#ip ospf 100 area 0

B. R2(config)#interface Loopback0 R2(config-if)#ip address 172.22.2.1 255.255.255.0 R2(config-if)#ip ospf network point-to-point R2(config-if)#ip ospf 100 area 0

C. R2(config)#interface Loopback0 R2(config-if)#ip address 172.22.2.1 255.255.255.0 R2(config-if)#ip ospf network point-to-multipoint R2(config-if)#router ospf 100

D. R2(config-router)#network 172.22.2.0 0.0.0.255 area 0 R2(config)#interface Loopback0 R2(config-if)#ip address 172.22.2.1 255.255.255.0 R2(config-if)#ip ospf 100 area 0

Correct Answer: *B*

Community vote distribution

B (100%)

Abdullavip Highly Voted 1 year, 1 month ago

B is correct. When OSPF is running on a given loopback interface, it sees the network type of "LOOPBACK" and it knows that it can not establish an adjacency through that loopback interface with another router so it advertises that loopback as a host route or the only IP address on that logical interface. As Martin explained so nicely you can tell OSPF that it is not a loopback and it is a point-to-point network type, and OSPF says "OK I am going to advertise the interface with its correct mask". In MPLS environment where OSPF is the IGP in the core, and you have configured the loopback interface of the PE router with a /24 mask, you can have some problems, because there is a discrepancy, the loopback's mask is 24 but OSPF is advertising a mask of /32. There are few solutions to fix this problem, one solution is to reconfigure the mask to be /32, another solution is to configure the loopback interface with "ip ospf network point-to-point".

upvoted 18 times

gordon888 Highly Voted 10 months ago

Selected Answer: B

test(config)#int loopback 99
test(config-if)#ip add 10.99.1.1 255.255.255.0
test(config-if)#ip ospf network broadcast
% OSPF: Invalid type for interface Loopback99
test(config-if)#ip ospf network non-broadcast
% OSPF: Invalid type for interface Loopback99
test(config-if)#
test(config-if)#ip ospf network point-to-multipoint
% OSPF: Invalid type for interface Loopback99
test(config-if)#ip ospf network point-to-point
!
interface Loopback99
ip address 10.99.1.1 255.255.255.0
ip ospf network point-to-point
end

upvoted 6 times

[Removed] Most Recent 5 months, 1 week ago

Selected Answer: B

Correct answer is B,
A loopback interface cannot have an ospf network type other than point-to-point

upvoted 1 times

dragonwise 8 months ago

A.
R2(config)#interface Loopback0
R2(config-if)#ip address 172.22.2.1 255.255.255.0
R2(config-if)#ip ospf network broadcast
R2(config-if)#ip ospf 100 area 0

B.
R2(config)#interface Loopback0
R2(config-if)#ip address 172.22.2.1 255.255.255.0
R2(config-if)#ip ospf network point-to-point
R2(config-if)#ip ospf 100 area 0

C.
R2(config)#interface Loopback0
R2(config-if)#ip address 172.22.2.1 255.255.255.0

R2(config-if)#ip ospf network point-to-multipoint
R2(config-if)#router ospf 100

D.
R2(config-router)#network 172.22.2.0 0.0.0.255 area 0
R2(config)#interface Loopback0
R2(config-if)#ip address 172.22.2.1 255.255.255.0
R2(config-if)#ip ospf 100 area 0
upvoted 4 times

nushadu 11 months, 1 week ago

Selected Answer: B

cisco_R5(config-if)#do s runn int loo1
Building configuration...

Current configuration : 113 bytes
!
interface Loopback1
ip address 55.0.0.5 255.255.255.0
ip ospf network point-to-point
ip ospf 1 area 22
end

cisco_R5(config-if)#

far-end before " ip ospf network point-to-point" see netw mask has been changed
cisco_R3(config-subif)#do s ip ro os | b Gate
Gateway of last resort is not set

55.0.0.0/32 is subnetted, 1 subnets <<<<<<<<<<<<<<<<<<<<<<<<<<<<
O 55.0.0.5 [110/11] via 10.111.10.2, 00:00:11, Ethernet0/0.50
cisco_R3(config-subif)#

after:
cisco_R3(config-subif)#do s ip ro os | b Gate
Gateway of last resort is not set

55.0.0.0/24 is subnetted, 1 subnets <<<<<<<<<<<<<<<<<
O 55.0.0.0 [110/11] via 10.111.10.2, 00:00:06, Ethernet0/0.50
cisco_R3(config-subif)#
upvoted 1 times

onkel_andi 1 year, 1 month ago

B is correct
upvoted 2 times

Summo 1 year, 1 month ago

answer is D
upvoted 1 times

Summo 1 year, 1 month ago

sorry my bad answer is B
upvoted 2 times

Joseph123 1 year, 2 months ago

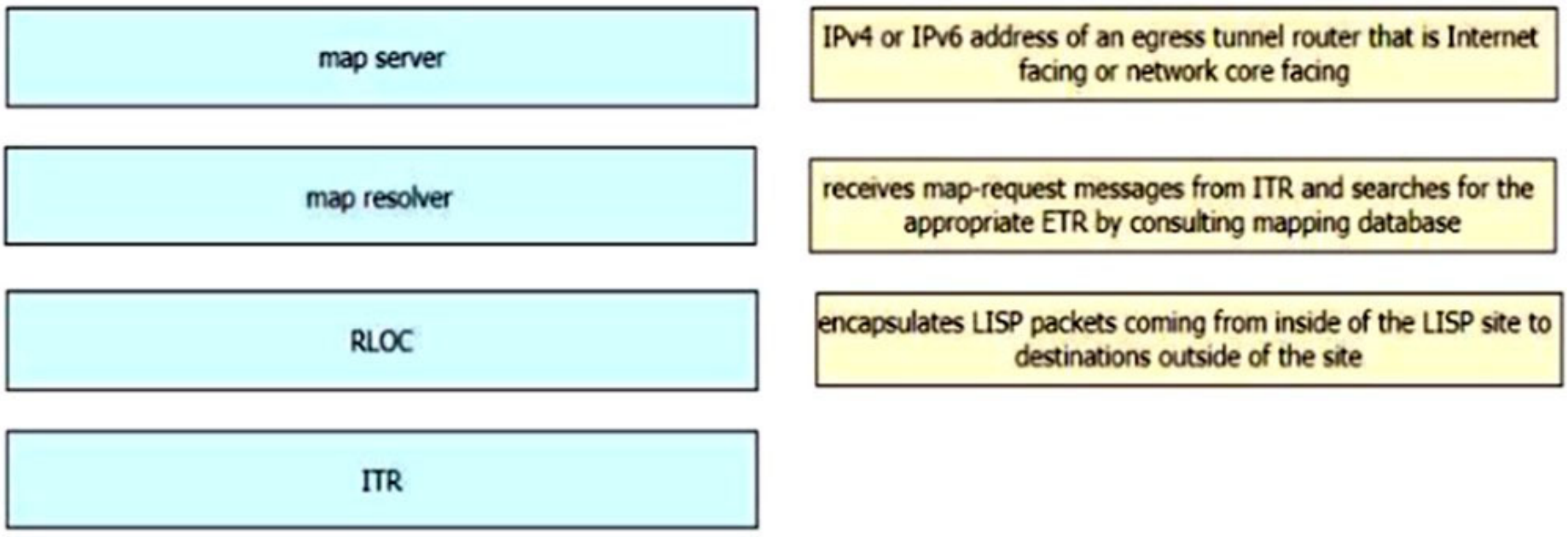
Given answer is correct
upvoted 2 times

Question #411 *Topic 1*

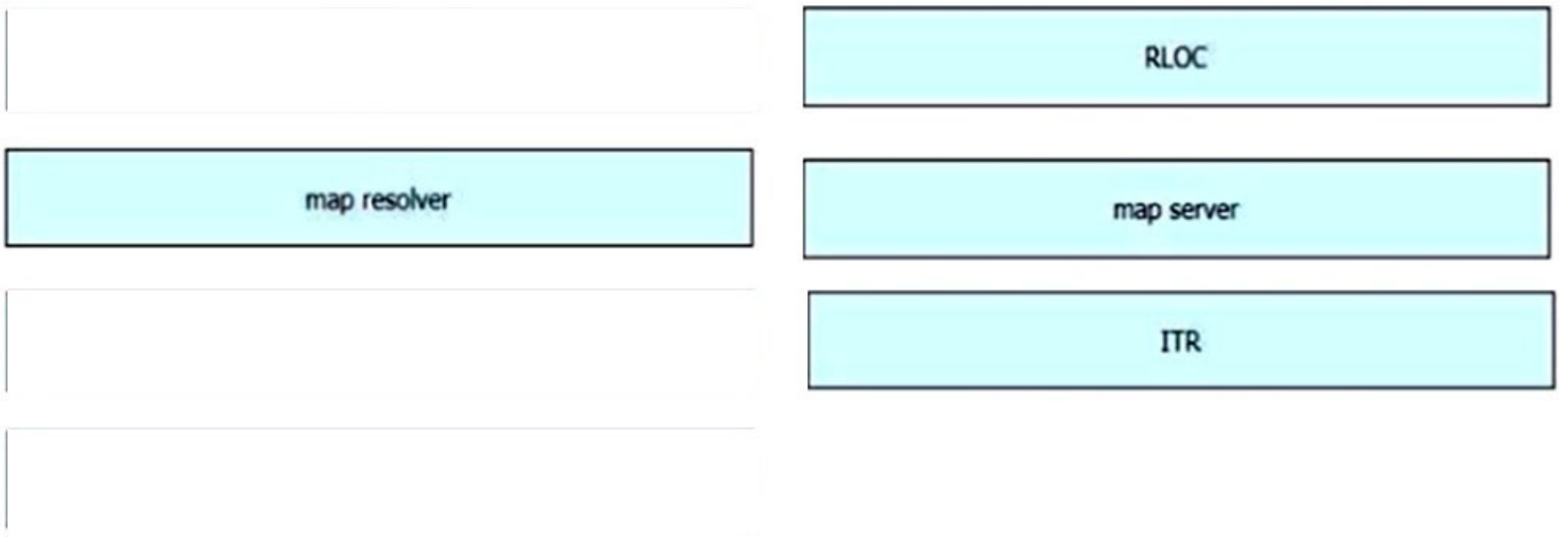
DRAG DROP -

Drag and drop the LISP components on the left to their descriptions on the right. Not all options are used.

Select and Place:



Correct Answer:



RREVECO Highly Voted 1 year, 2 months ago

ANS
RLOC, RESOLVER, ITR
Map resolver (MR): This is a network device (typically a router) that receives LISP-encapsulated map requests from an ITR and finds the appropriate ETR to answer those requests by consulting the map server.

upvoted 20 times

msstanick Most Recent 5 months, 3 weeks ago

To my mind:
- RLOC
- MR
- ITR

This is from Cisco's 31 days before CCNP book: "Map resolver (MR): It accepts encapsulated Map-Request messages sent by ITRs, decapsulates them, and then forwards them over the ALT router toward the ETRs responsible for the EIDs being requested."

So, MS creates the database (based on ETR registerations) that the MR is using.

upvoted 1 times

Dyks 5 months, 4 weeks ago

Roof, map resolvers, itr

upvoted 1 times

net_eng10021 6 months ago

D.

The function of the LISP MR is to accept encapsulated Map-Request messages from ingress tunnel routers (ITRs), decapsulate those messages, and then forward the messages to the MS responsible for the egress tunnel routers (ETRs) that are authoritative for the requested EIDs.

upvoted 1 times

mhizha 6 months, 2 weeks ago

I agree with RLOC and Resolver what i dont understand is why the 3rd option is ITR. This is not making sense to me.

upvoted 1 times

Splashisthegreatestmovie 5 months, 2 weeks ago

ITR encapsulates. ETR decapsulates. So the key word is encapsulate.

upvoted 2 times

chaocheng 8 months, 1 week ago

ANS
RLOC, RESOLVER, ITR

routing locator (RLOC) An IPv4 or IPv6 address of an ETR that is Internet facing or network core facing

map resolver (MR) A network device (typically a router) that receives LISP-encapsulated map requests from an ITR and finds the appropriate ETR to answer those requests by consulting the map server. If requested by the ETR, the MS can reply on behalf of the ETR.

ingress tunnel router (ITR) A router that LISP-encapsulates IP packets coming from EIDs that are destined outside the LISP site.

upvoted 1 times

chefexam 9 months, 2 weeks ago

The statement is mixed up!?

"receives map request messages from ITR" ---> MR
"searches the appropriate ETR by consulting mapping database" ---> MS

So basically what they are describing is a MS/MR device...

upvoted 1 times

wdp 10 months ago

The map resolver (MR), on the other hand, accepts LISP encapsulated map requests from an ITR. Based on a map request, two things may happen.

If the destination IP address is part of the EID namespace, the MR finds the appropriate EID-to-RLOC mapping by consulting the distributed mapping database system.

https://www.ciscopress.com/articles/article.asp?p=2992605

upvoted 1 times

Zizu007 1 year ago

Given answer is correct!

When MS and MR function runs on separate devices:
1. ITR --'map-request'--> MAP-Resolver (MR)
2. MR --- forwards 'map-request' -----> MAP-Server (MS)
3. MS --- check DB for RLOC -- finds (ETR)
4. MS -- Sends 'map-request' to ------> Egress Tunnel Router (ETR)
5. ETR -- sends 'MAP-Reply' directly to ----->ITR

When MS and MR function runs on same devices (which is this question):
1. ITR --'map-request'--> MAP-Resolver (MR/MS)
2. MS --- check DB for RLOC -- find (ETR)
3. MS -- Sends 'map-request' to ------> Egress Tunnel Router (ETR)
4. ETR -- sends 'MAP-Reply' directly to ----->ITR

upvoted 4 times

danman32 4 months ago

But the available choices have both MR and MS so you have to assume they are separate.
Otherwise both would be correct since question doesn't specify if the MS/MR function is on the same router or not

upvoted 1 times

Stylar 1 year ago

RLOC, RESOLVER, ITR for sure.
Link provided by PALURDIN.

upvoted 2 times

Deu_Inder 1 year, 2 months ago

Ans:
RLOC, Resolver, ITR.

upvoted 2 times

PALURDIN 1 year, 2 months ago

I guess it is map resolver instead of map server:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html#GUID-92481C7B-F44D-4D8C-8085-A2E98530CA50:~:text=and%20ITR%20components).-,LISP%20Map%20Resolver,-Like%20an%20MS

upvoted 2 times

```
Router#show policy-map control-plane
Control Plane

 Service-policy input: CoPP

  Class-map: class-telnet (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: access-group 100
    police:
        cir 100000 bps, bc 3125 bytes
      conformed 0 packets, 0 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 0 bps, exceed 0 bps

  Class-map: class-default (match-any)
    56 packets, 9874 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any

Router#show access-list 100
Extended IP access list 100
    10 permit tcp any any eq telnet
```

Refer to the exhibit. Which commands are required to allow SSH connections to the router?

A.

```
Router(config)#access-list 10 permit tcp any eq 22 any
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 10
Router(config)#policy-map CoPP
Router(config-pmap)#class class-ssh
Router(config-pmap-c)#police 100000 conform-action transmit
```

B.

```
Router(config)#access-list 100 permit tcp any any eq 22
Router(config)#access-list 101 permit tcp any any eq 22
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP
Router(config-pmap)#class class-ssh
Router(config-pmap-c)#police 100000 conform-action transmit
```

C.

```
Router(config)#access-list 100 permit udp any any eq 22
Router(config)#access-list 101 permit tcp any any eq 22
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP
Router(config-pmap)#police 100000 conform-action transmit
```

D.

```
Router(config)#access-list 100 permit tcp any eq 22 any
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 10
Router(config)#policy-map CoPP
Router(config-pmap)#class class-ssh
Router(config-pmap-c)#police 100000 conform-action transmit
```

Correct Answer: *A*

Deu_Inder Highly Voted 1 year, 2 months ago

Question is badly worded. They should say that SSH needs to be policed.
Answer B is right.

upvoted 10 times

FerroForce Highly Voted 7 months ago

B is correct. Extended ACL could not be 10.

upvoted 7 times

danman32 Most Recent 4 months ago

Why is there an entry for access-list 100 in B and C?
Access-list 100 will have no effect on the newly created class-map, but could break the existing class-map.

upvoted 2 times

PureInertiaCopy 3 months, 2 weeks ago

Wondering the exact same thing...

upvoted 1 times

andyforreg 4 months, 2 weeks ago

Answer - B

upvoted 1 times

nikramor 4 months, 2 weeks ago

B is correct

upvoted 2 times

HarwinderSekhon 5 months ago

B is correct.

upvoted 3 times

lafrank 7 months, 2 weeks ago

A can't be correct, as access-list 10 is standard ACL and as such it is not supporting port definition

upvoted 2 times

Ayman_B 7 months, 3 weeks ago

I could not find any defefirent between A and B , both of them are correct . can any body clarifying the deffirent

upvoted 1 times

Pilgrim5 7 months, 1 week ago

The difference is in the beginning access list statements.

A - access-list 10 is wrong because standard access lists only support source address and mask. They don't support adding destination addresses, masks or source and destination ports.

B - access-list 100 is right because this is an extended access list and extended access lists support source and destination addresses and masks and also source and destination ports.

Standard access lists - 1-99
Extended access lists - 100-199

upvoted 2 times

bendarkel 10 months ago

B is correct. A is wrong because per the ACL, the traffic is being sourced from port 22.

upvoted 3 times

kewokil120 10 months, 2 weeks ago

B is right

upvoted 2 times

H3kerman 1 year ago

A can't be right, because ACL 10 is standard, bud defined in config is extended.

I would vote B

upvoted 4 times

burban97 1 year ago

If I'm not mistaken standard acl 10 (standard) based off
source only

upvoted 1 times

loannis34 1 year, 1 month ago

answer is B

upvoted 3 times

onkel_andi 1 year, 1 month ago

Answer is A)
SSH will be added to the CoPP Policy Map

upvoted 2 times

GeorgeFortiGate 1 year ago

It is not. Asks for SSH traffic , how the source have port 80 ? This is going to be the destination port first of all. then it is also: Access List "10".

upvoted 1 times

GeorgeFortiGate 1 year ago

Correct answer is B

upvoted 1 times

iGlitch 1 year ago

the ACL itself is wrong, the eq keyword should be placed at the end because we want to match incoming ssh requests so the destination "ssh server" will use port 22, and the source "ssh client" will use a random port number.

The answer is B

upvoted 2 times

Caledonia 1 year, 2 months ago

Answer is B

upvoted 4 times

Question #413 *Topic 1*

What is a characteristic of a type 2 hypervisor?

A. complicated deployment

B. ideal for data center

C. referred to as bare-metal

D. ideal for client/end-user system

Correct Answer: *D*

Community vote distribution

D (80%) B (20%)

Leoveil Highly Voted 11 months, 2 weeks ago

Selected Answer: D

A-B-C refer to Hypervisor 1

upvoted 5 times

ShadyAbdekmalek Most Recent 11 months, 3 weeks ago

Selected Answer: D

D. ideal for client/end-user system

upvoted 1 times

kalbos 1 year ago

Selected Answer: D

Answer is D

upvoted 1 times

Redzero07 1 year ago

Selected Answer: D

Answer is D

upvoted 1 times

GeorgeFortiGate 1 year ago

Selected Answer: B

Correct answer is B

upvoted 2 times

Edwinmolinab 1 year ago

For datacenter type 1 hypervisor are better

upvoted 3 times

Question #414 *Topic 1*

Which two features does the Cisco SD-Access architecture add to a traditional campus network? (Choose two.)

A. modular QoS

B. software-defined segmentation

C. identity services

D. private VLANs

E. SD-WAN

Correct Answer: *BC*

Community vote distribution

BC (100%)

RREVECO 1 year, 2 months ago

Selected Answer: BC

"""software-defined segmentation"
ref:
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Segmentation-Design-Guide-2018MAY.pdf

"""Identity services"""""
ref: ccnp and ccie enterprise core encor 350-401 official cert guide

upvoted 3 times

Deu_Inder 1 year, 2 months ago

Given answer is correct.

upvoted 2 times

Question #415 *Topic 1*

Which congestion queuing method on Cisco IOS based routers uses four static queues?

A. weighted fair

B. custom

C. low latency

D. priority

Correct Answer: *D*

Community vote distribution

D (100%)

Asymptote Highly Voted 10 months, 4 weeks ago

Selected Answer: D

Priority Queuing (PQ)—This type of queuing places traffic into one of four queues. Each queue has a different level of priority, and higher-priority queues must be emptied before packets are emptied from lower-priority queues. This behavior can “starve out” lower- priority traffic.

Reference:
https://www.ciscopress.com/articles/article.asp?p=352991&seqNum=7#:~:text=Priority%20Queuing%20(PQ)%E2%80%94This%20type%20of%20queuing%20places%20traffic%20into%20one%20of%20four%20queues.%20Each%20queue%20has%20a%20different%20level%20of%20priority%2C%20and%20higher%2Dpriority%20queues%20must%20be%20emptied%20before%20packets%20are%20emptied%20from%20lower%2Dpriority%20queues.%20This%20behavior%20can%20%E2%80%9Cstarve%20out%E2%80%9D%20lower%2D%20priority%20traffic.

upvoted 5 times

Japsurd Most Recent 11 months, 1 week ago

Selected Answer: D

https://packetlife.net/media/library/19/QoS.pdf

upvoted 2 times

straightAnswers 8 months, 2 weeks ago

Thanks for sharing this

upvoted 1 times

Joseph123 1 year, 2 months ago

Correctomundo

upvoted 2 times

DRAG DROP -

An engineer plans to use Python to convert text files that contain device information to JSON Drag and drop the code snippets from the bottom onto the blanks in the code to construct the request. Not all options are used.

Select and Place:

Answer Area

```
import json

input_file = 'raw-data.txt'
dictionary_1 = {}
fields = ['Device_type', 'IP_Address', 'IOS_type', 'Username', 'Password']

                                                    
    l = 1
    for line in text:
        description = list(line.strip().split(None, 4))
        print(description)
        Device_Number = 'Device' + str(l)
        i = 0
        dictionary_2 = {}
        while i < len(fields):
            dictionary_2[fields[i]] = description[i]
            i = i + 1
        dictionary_1[Device_Number] = dictionary_2
        l = l + 1

                                                    
json.dump(dictionary_1, out_file, indent=4)
                                                    
```

raw-data.txt

```
{
    "Device1": {
        "Device_type": "switch",
        "IOS_type": "ios",
        "IP_Address": "10.1.1.1",
        "Username": "user1",
        "Password": "pass1"
    },
    "Device2": {
        "Device_type": "router",
        "IOS_type": "ios-xr",
        "IP_Address": "10.1.1.2",
        "Username": "user2",
        "Password": "pass2"
    },
    "Device3": {
        "Device_type": "nexus-9k",
        "IOS_type": "nx-os",
        "IP_Address": "10.1.1.3",
        "Username": "user3",
        "Password": "pass3"
    }
}
```

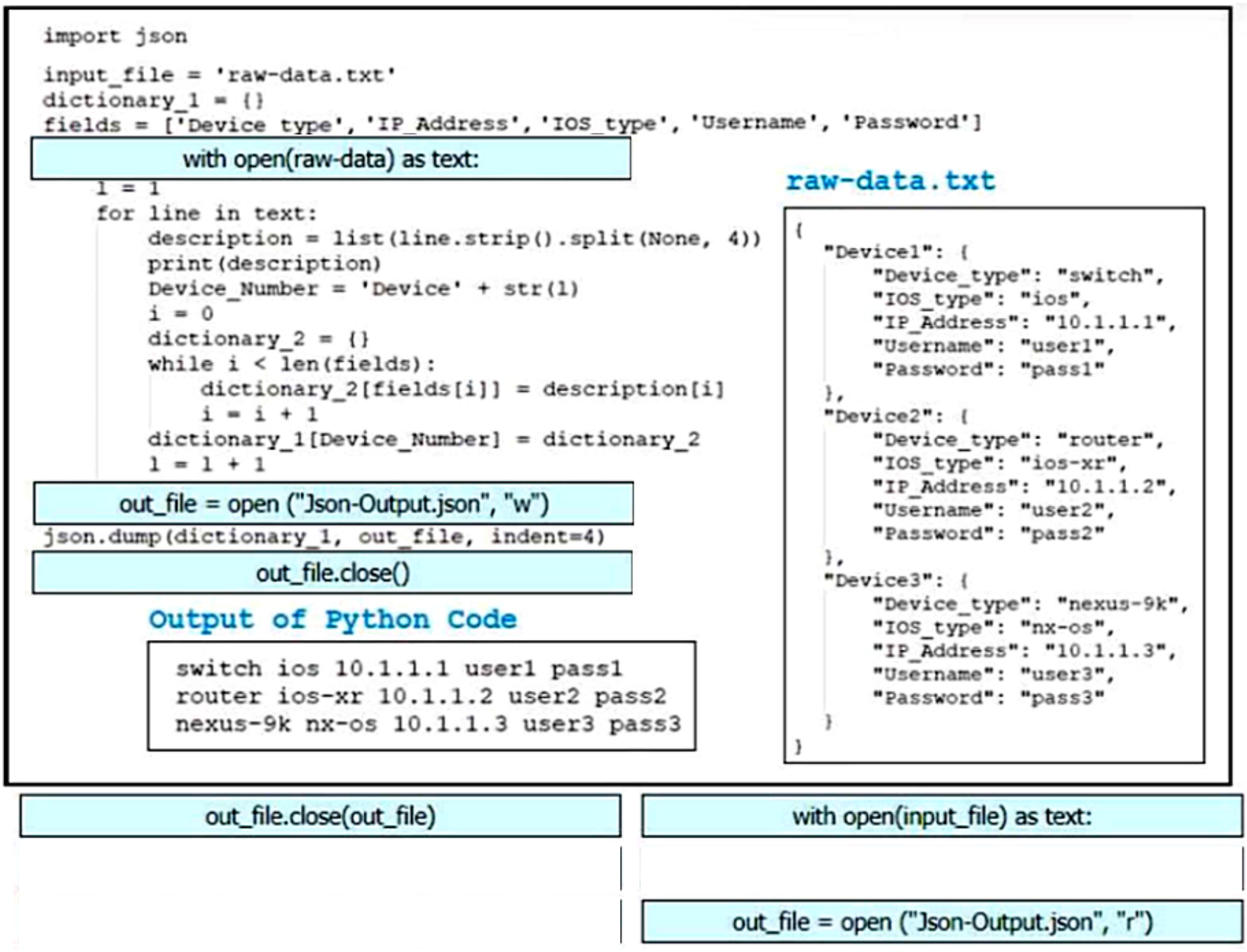
Output of Python Code

```
switch ios 10.1.1.1 user1 pass1
router ios-xr 10.1.1.2 user2 pass2
nexus-9k nx-os 10.1.1.3 user3 pass3
```

out_file.close(out_file)	with open(input_file) as text:
with open(raw-data) as text:	out_file.close()
out_file = open ("Json-Output.json", "w")	out_file = open ("Json-Output.json", "r")

Correct Answer:

Answer Area



uzbin Highly Voted 1 year, 2 months ago

File 'raw-data.tx' is referenced by the variable input_file, so first text box should contain - with open(input_file) as text:

Rest looks correct.

upvoted 22 times

Makaveli1 11 months, 1 week ago

No, the variable "input_file" will contain text string 'raw-data.txt', not the file. To open the file you use the context manager.

>>> input_file = 'raw-data.txt'
>>> input_file
'raw-data.txt'

The given answer is correct.

upvoted 2 times

danman32 4 months ago

the function open() requires text as input option, whether that is literal or through a variable containing text that specifies the file name.
The given answer specifies an undefined variable.

upvoted 1 times

HarwinderSekhon 5 months, 3 weeks ago

Tested --
myfilename = 'dummy.txt'

open the file for reading (replace 'file.txt' with your file name)
with open(myfilename, 'r') as file:
# read the content of the file
data = file.read()
# print the content
print(data)

upvoted 1 times

nushadu 11 months, 1 week ago

you are wrong;

with open('some_file.txt', 'w') as f:

f.write('hello') <<<<<<<<<<< write text into the file

with open('some_file.txt') as f:
print(f.read()) <<<<<<<<<<<<<<<< read

hello <<<<<<<<<<<<<< output

my_file = 'some_file.txt' <<<<<<<<<<<< just variable
with open(my_file) as f: <<<<<<<<<<<< use it in the code
print(f.read())

hello

upvoted 2 times

Caradum 1 year ago

uzbin is right.

upvoted 1 times

nhawley 1 year, 1 month ago

Agreed, you should reference the variable input_file

upvoted 1 times

kewokil120 Most Recent 10 months, 1 week ago

UZBIN is right.

upvoted 1 times

Question #417 *Topic 1*

Which resource is able to be shared among virtual machines deployed on the same physical server?

A. disk

B. VM configuration file

C. applications

D. operating system

Correct Answer: *A*

Community vote distribution

A (100%)

Ciscoman021 8 months, 1 week ago

Selected Answer: A

Disk is the resource that is able to be shared among virtual machines deployed on the same physical server.

upvoted 1 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: A

A. a disk is a resource and can get shared.

upvoted 3 times

Xerath 11 months, 2 weeks ago

Selected Answer: A

Provided answer is correct.

upvoted 1 times

```
SW2#
%CDP-4-NATIVE_VLAN_MISMATCH:  Native VLAN mismatch discovered on
GigabitEthernet0/1 (1), with SW1 GigabitEthernet 0/1 (30).
SW2#
```

Refer to the exhibit. An engineer must set up connectivity between a campus aggregation layer and a branch office access layer. The engineer uses dynamic trunking protocol to establish this connection; however, management traffic on VLAN1 is not passing. Which action resolves the issue and allow communication for all configured VLANs?

A. Disable Spanning Tree for the native VLAN.

B. Allow all VLANs on the trunk links.

C. Change both interfaces to access ports.

D. Configure the correct native VLAN on the remote interface

Correct Answer: *D*

Community vote distribution

D (100%)

mgiuseppe86 2 months, 2 weeks ago

After doing so many Cisco exams you subconsciously are trained on thinking the most obvious answer isnt correct because Cisco will throw 14 double negatives and random words to throw you off.

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Cisco exams are more of English literature exams meant for Hoodini

upvoted 1 times

ihateciscoreally 3 months, 1 week ago

its cisco question, its cant be so straightforward.

upvoted 2 times

nushadu 11 months, 1 week ago

Selected Answer: D

sw1(config-if)#switchport trunk native vlan 122
sw1(config-if)#
Dec 21 21:37:35.737: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet0/1 (122), with sw2 Ethernet0/1 (1).
Dec 21 21:37:35.738: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet0/3 (122), with sw2 Ethernet0/3 (1).
sw1(config-if)#
Dec 21 21:38:35.744: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet0/3 (122), with sw2 Ethernet0/3 (1).
Dec 21 21:38:35.744: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet0/1 (122), with sw2 Ethernet0/1 (1).
sw1(config-if)#do show interfaces po2 swi | i Native
Trunking Native Mode VLAN: 122 (VLAN0122) <<<<<<<<<<<<<<<<<<<<
Administrative Native VLAN tagging: enabled
Administrative private-vlan trunk Native VLAN tagging: enabled
sw1(config-if)#

upvoted 2 times

nushadu 11 months, 1 week ago

far-end:
sw2#show interfaces po2 swi | i Native
Trunking Native Mode VLAN: 1 (default) <<<<<<<<<<<<<<<<<<<<
Administrative Native VLAN tagging: enabled
Administrative private-vlan trunk Native VLAN tagging: enabled
sw2#
sw2#
sw2#
*Dec 21 21:39:35.745: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet0/1 (1), with sw1.local.lab Ethernet0/1 (122).
*Dec 21 21:39:35.745: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet0/3 (1), with sw1.local.lab Ethernet0/3 (122).
sw2#

upvoted 1 times

forccnp 1 year ago

Selected Answer: D

D is correct

upvoted 2 times

Question #419 *Topic 1*

Which three resources must the hypervisor make available to the virtual machines? (Choose three.)

A. Memory

B. bandwidth

C. IP address

D. Processor

E. storage

F. secure access

Correct Answer: *ADE*

Community vote distribution

ADE (100%)

Xerath 11 months, 3 weeks ago

Selected Answer: ADE

Provided answer is correct,
- Memory (RAM)
- Processor (cpu cores)
- Storage (disk)

those are the resources that can be distributed among virtual machines.

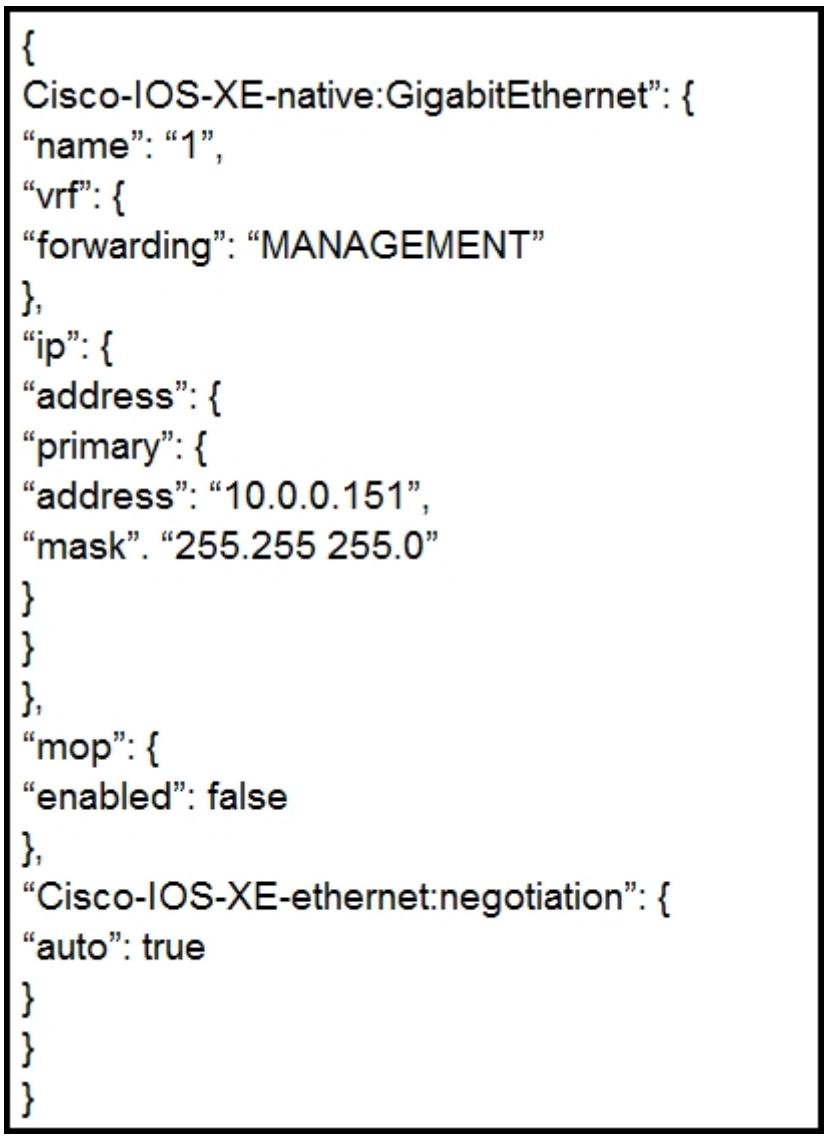
upvoted 4 times

ricaela10 1 year ago

Hi, can someone confirm if memory,processor and storage is the correct answer..

upvoted 3 times

DRAG DROP -



Refer to the exhibit. Drag and drop the snippets into the RESTCONF request to form the request that returns this response. Not all options are used.

Select and Place:

Answer Area

URL - http://10.10.10.10/restconf/api/running/native/ [ ]

HTTP Verb- [ ]

Body- N/A

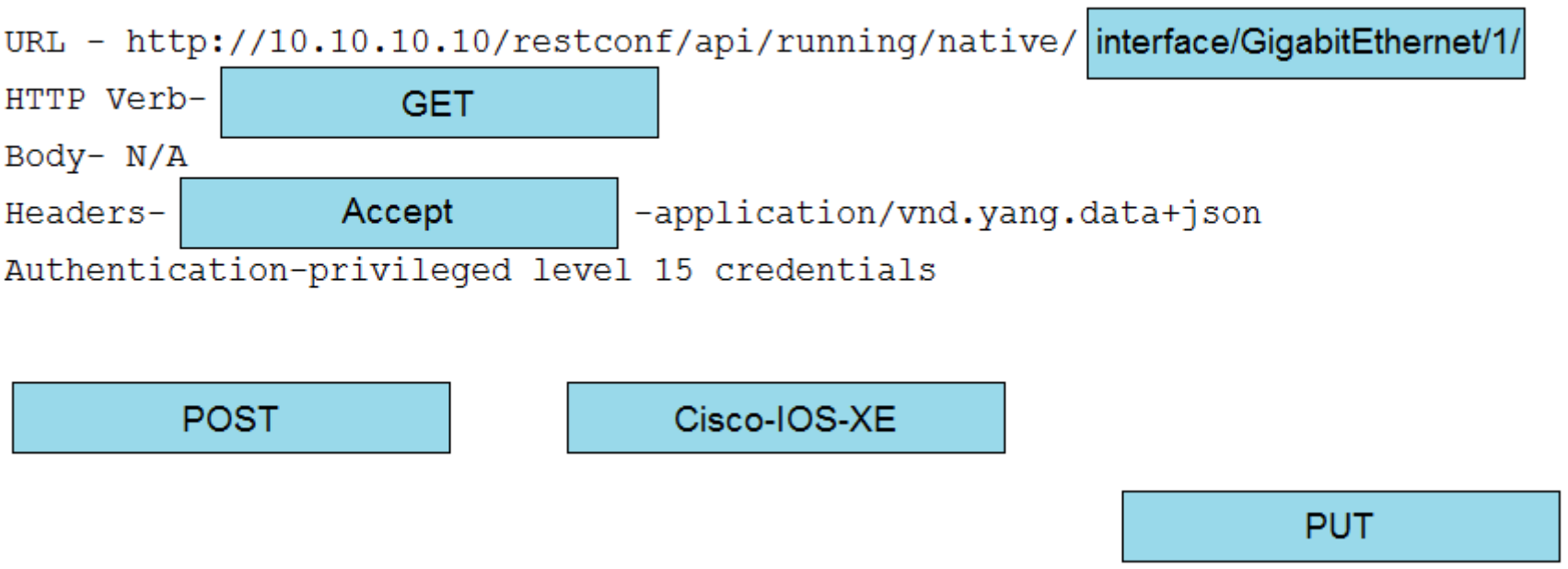
Headers- [ ] -application/vnd.yang.data+json

Authentication-privileged level 15 credentials

POST	Cisco-IOS-XE	GET
Accept	interface/GigabitEthernet/1/	PUT

Correct Answer:

Answer Area



dragonwise 8 months ago

Does anybody know what is the Accept keyword for?

upvoted 1 times

bk989 7 months, 2 weeks ago

The "Accept" header field can be used by user agents to specify response media types that are acceptable. The Accept header always indicates what kind of response from the server a client can accept.

upvoted 3 times

Stylar 1 year ago

GET retrieves data.
PUT or POST if successful would return a 204 no content code.
If you would then need to check if it was done, you would use GET to see what has happened.

upvoted 2 times

dougj 1 year, 1 month ago

GET is used to retrieve config data, both POST and PUT are used to send data

upvoted 1 times

Deu_Inder 1 year, 2 months ago

Hi, can anyone help me with 'http verb' here? How can it be get? We are putting the configuration from a client machint to the device running RESTCONF (a https server) right?

upvoted 1 times

FrameRelay 1 year, 1 month ago

no, the question reads "form the request that returns this response", therefore has to be a GET because its returning the values, not configuring them.

upvoted 6 times

M_B 10 months, 3 weeks ago

The question states "RESTCONF Rquest" so should be GET

upvoted 1 times

RREVECO 1 year, 2 months ago

I think it's GET
the question says: "Drag and drop the snippets into the RESTCONF request to form the request that returns this response"
POST = create
PUT = replace
GET = get/get-config

upvoted 5 times

FrameRelay 1 year, 1 month ago

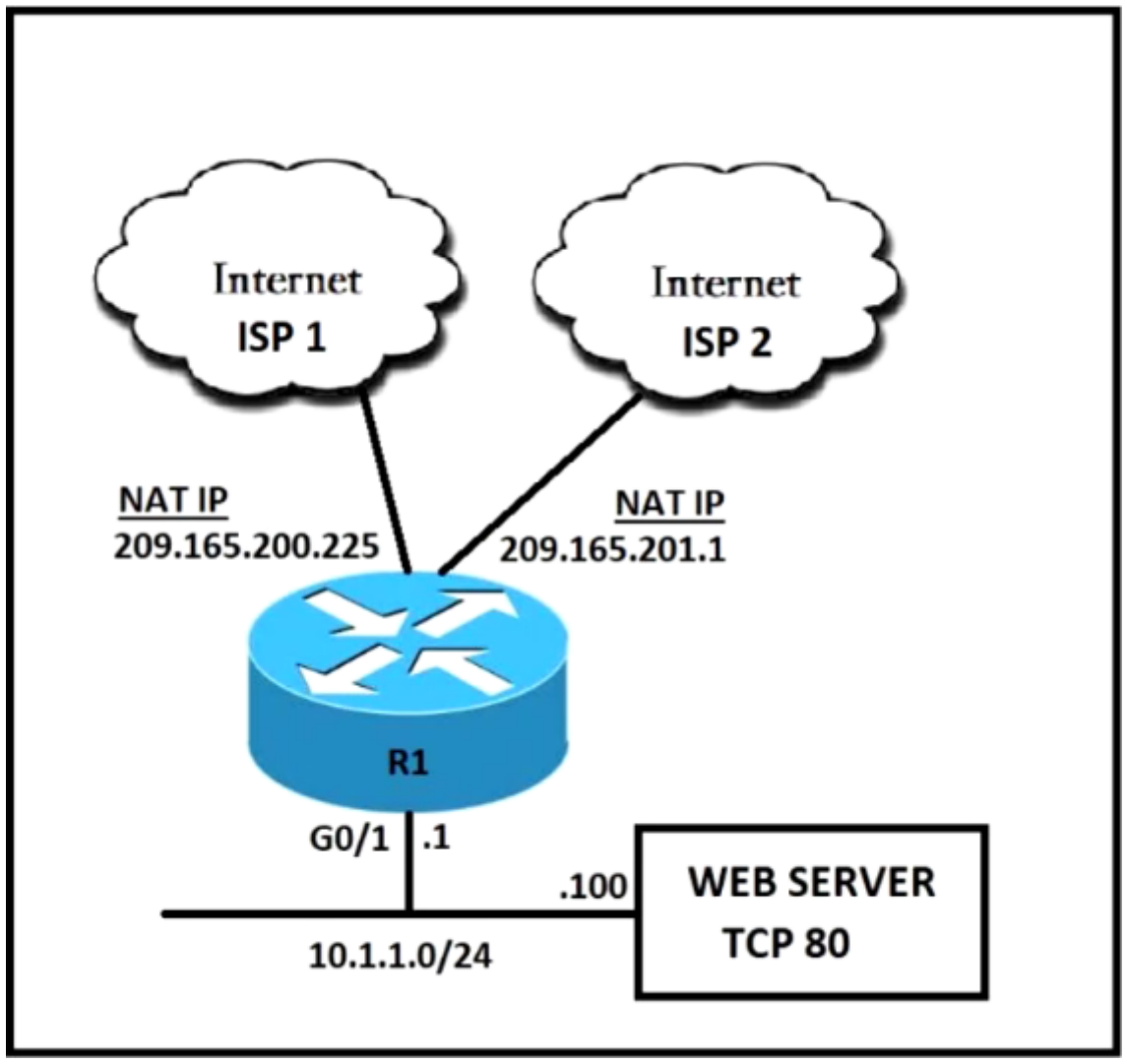
Agreed, GET

upvoted 2 times

uzbin 1 year, 2 months ago

It is PUT or POST.
I am leaning towards PUT.

upvoted 1 times



Refer to the exhibit. An engineer must configure static NAT on R1 to allow users HTTP access to the web server on TCP port 80. The web server must be reachable through ISP 1 and ISP 2. Which command set should be applied to R1 to fulfill these requirements?

A. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 extendable ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 extendable

B. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80

C. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 no-alias ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 no-alias

D. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 ip nat inside source static tcp 10.1.1.100 8080 209.165.201.1 8080

Correct Answer: *A*

kebkim Highly Voted 1 year, 1 month ago
The NAT extendable parameter can be used if you want to translate a private IP address to more than one public IP address.
upvoted 12 times

ihateciscoreally 3 months, 2 weeks ago
And if you enter "no-alias", the NAT-router won't answer for ARP replies for that IP.
upvoted 1 times

dragonwise Most Recent 8 months ago
A.
ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 extendable
ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 extendable

B.
ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80
ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80

C.
ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 no-alias
ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 no-alias

D.
ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80
ip nat inside source static tcp 10.1.1.100 8080 209.165.201.1 8080
upvoted 2 times

Stylar 10 months, 1 week ago
https://networklessons.com/uncategorized/nat-extendable-on-cisco-ios

upvoted 4 times

Deu_Inder 1 year, 2 months ago

Provided answer is correct.

upvoted 2 times

```
Switch1#show lacp internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port         Port
Port      Flags  State      Priority      Key       Key     Number       State
Gi0/0     SP     hot-sby    20            0x1       0x1     0x1          0x5
Gi0/1     SA     bnd1       15            0x1       0x1     0x2          0x3C
```

Refer to the exhibit. An engineer attempts to bundle interface Gi0/0 into the port channel, but it does not function as expected. Which action resolves the issue?

A. Enable fast LACP PDUs on interface Gi0/0.

B. Set LACP max-bundle to 2 on interface Port-channel1.

C. Configure no shutdown on interface Gi0/0.

D. Configure channel-group 1 mode active on interface Gi0/0.

Correct Answer: *B*

Community vote distribution

B (100%)

x3rox 10 months ago

Selected Answer: B

This is the explanation of why B is Correct:
From Cisco:
The value specified in the max-bundle-number argument determines the number of active links that are bundled in the port channel. The remaining links are in hot-standby mode.

In the output we see 1 port as standby, therefore we must issue max-bundle 2 so both interfaces are active.

upvoted 2 times

Stylar 10 months, 1 week ago

LACP (Link Aggregation Control Protocol) open (IEEE) standard. Supports more than 8links in a channel, but only 8 can be in operation and rest as standby

upvoted 2 times

nushadu 11 months, 1 week ago

Selected Answer: B

sw1(config-if)# do s lacp int
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode

Channel group 2
LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
Et0/1 SA bndl 32768 0x2 0x2 0x2 0x3D
Et0/3 SP hot-sby 32768 0x2 0x2 0x4 0x4
sw1(config-if)#
sw1(config-if)#
sw1(config-if)#
sw1(config-if)#do s runn interface Port-channel2
Building configuration...

Current configuration : 123 bytes
!
interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
lacp max-bundle 1
end

sw1(config-if)#
upvoted 4 times

nushadu 11 months, 1 week ago

2nd port issue fixed:
sw1(config-if)#lacp max-bundle 2
sw1(config-if)#
Dec 21 21:51:58.051: %LINK-3-UPDOWN: Interface Port-channel2, changed state to up
Dec 21 21:51:59.055: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to up
sw1(config-if)# do s lacp int
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode

Channel group 2
LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
Et0/1 SA bndl 32768 0x2 0x2 0x2 0x3D
Et0/3 SP bndl 32768 0x2 0x2 0x4 0x3C <<<<<<<<<<<<<<<<<<<<<<<<<
sw1(config-if)#
upvoted 3 times

net_eng10021 6 months ago

Excellent post @nushadu
upvoted 1 times

temphurricane1091 11 months, 2 weeks ago

B has nothing to do with this, answer is D
upvoted 2 times

mgiuseppe86 2 months, 2 weeks ago

D is for a static port-channel "on". we are using Active/Passive with is LACP.
upvoted 1 times

Danny_Xu 1 year, 1 month ago

Selected Answer: B

The answer B is correct.
LACP hot-standby port:
"When enabled, LACP tries to configure the maximum number of LACP-compatible ports in a channel, up to a maximum of 16 ports. "
https://www.cisco.com/c/en/us/td/docs/switches/blades/3020/software/release/12-2_50_se/configuration/guide/scg/swethchl.pdf
upvoted 1 times

RREVECO 1 year, 2 months ago

Selected Answer: B

"B" it´s correct.

look Flags on G0/0 (SP) device is in passive mode.
upvoted 1 times

uzbin 1 year, 2 months ago

Given answer is correct.
upvoted 2 times

Question #423 *Topic 1*

In a Cisco StackWise Virtual environment, which planes are virtually combined in the common logical switch?

A. management and data

B. control, and forwarding

C. control and management

D. control and data

Correct Answer: *C*

Community vote distribution

C (100%)

iGlitch 1 year ago

Selected Answer: C

Answer is correct. read the "StackWise Virtual architecture" from the link below:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html

upvoted 4 times

```
logging buffered discriminator Disc1
logging monitor discriminator Disc1
logging host 10.1.55.237 discriminator Disc1
```

Refer to the exhibit. A network engineer is enabling logging to a local buffer, to the terminal, and to a syslog server for all debugging level logs filtered by facility code 7. Which command is needed to complete this configuration snippet?

A. logging buffered debugging

B. logging discriminator Disc1 severity includes 7

C. logging buffered discriminator Disc1 debugging

D. logging discriminator Disc1 severity includes 7 facility includes fac7

Correct Answer: *B*

Community vote distribution

D (89%) 11%

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: D

The “logging discriminator Disc1 severity includes 7 facility includes fac7” command enables the logging discriminator named Disc1 to filter messages with a severity level of 7 (debugging level) and facility code 7.

upvoted 6 times

PureInertiaCopy 3 months, 2 weeks ago

There is no facility code "fac7" ...

upvoted 1 times

Rose66 Highly Voted 10 months, 3 weeks ago

Selected Answer: D

logging discriminator discr-name [[facility] [mnemonics] [msg-body] {drops string | includes string }] [severity {drops sev-num | includes sev-num }] [rate-limit msglimit]

Example:

Device(config)# logging discriminator pacfltr1 facility includes facl357

See https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/esm/configuration/xe-16-12/esm-xe-16-12-book/reliable-del-filter.html

upvoted 5 times

djedeen Most Recent 3 months, 1 week ago

Selected Answer: D

I think D is correct, here is a sample from Cisco for facility code 357:
(config)# logging discriminator pacfltr1 facility includes facl357

upvoted 1 times

byallmeans 6 months, 3 weeks ago

Selected Answer: B

"fac7" is not a regular expression for facility 7. Plus, facility 7 is default so you don't need to specify it in discriminator. In my humble opinion, answer should be B.

upvoted 2 times

byallmeans 6 months, 3 weeks ago

I may be wrong though, since it's specifically saying "facility code", which for Cisco's case, default is code 23 (local7). Answer D is still sensible.

upvoted 1 times

Cooldude89 9 months, 2 weeks ago

Selected Answer: D

Going with D

upvoted 1 times

Caledonia 1 year, 2 months ago

Selected Answer: D

Answer is D
upvoted 3 times

DRAG DROP -

Drag and drop the snippets onto the blanks within the code to construct a script that adds a prefix list to a route map and sets the local preference. Not all options are used.

Select and Place:

Answer Area

```
{
   "@message-id": "101",
   "edit-config": {
      "target": {
         [          ]
      },
      "config": {
         "native": {
            "ip":
               "prefix-list": {
                  "prefixes": {
                     [          ]
                        "permit": {
                           "prefix-only-list": {
                              "prefix": "192.168.1.0/24"
                           }
                        }
                     }
                  }
               }
            }
            "route-map": {
               "name": "Routes",
               "route-map-without-order-seq": {
            [          ] "10",
                  "set": {
                     "local-preference": "200"
                  },
            [          ]{
                     "ip": {
                        "address": {
                           "prefix-list": "100"
                        }
                     }
                  }
               }
            }
         }
      }
   }
}
```

"running": null

"seq_no":

"config": null

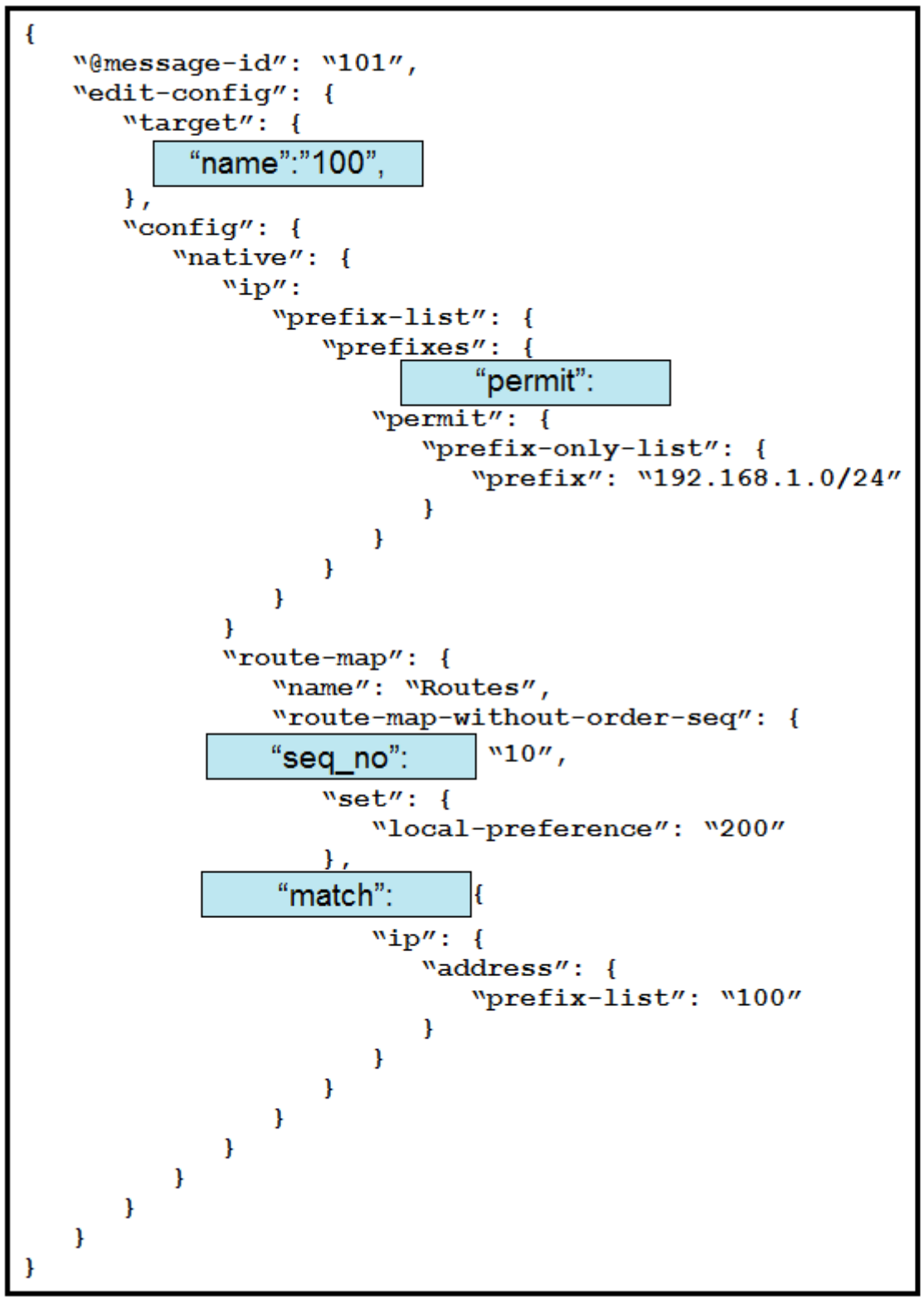
"permit":

"match":

"name":"100",

Correct Answer:

Answer Area



Caledonia Highly Voted 1 year, 2 months ago

The answer is wrong.

"running": null
Name:100
Permit
Match

upvoted 32 times

Cer_Pit Highly Voted 1 year, 1 month ago

Suggested answer is wrong. If I understand correctly, correct should be:

* "running": null
* "name":"100"
* "permit"
* "match"

The order in the route-map is a bit odd, the "match" part comes first and after that comes the "set" part...
But, in the running-config (that is the target) in IOS this would be:

* ip prefix-list 100 seq 10 permit 0.0.0.0/0 <- name of prefix-list is "100"
* route-map Routes permit 10 <- "permit" 10
* match ip address prefix-list 100 <- "match" the prefix-list "100"
* set local-preference 200

upvoted 11 times

eww_cybr Most Recent 4 months, 4 weeks ago

"running": null
Name:100
Permit
Match

NETCONF <edit-config> Request: CLI Format
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<edit-config>
<target>
<running/>
</target>
<config>

upvoted 2 times

HarwinderSekhon 5 months, 2 weeks ago

Is it a Resconf sample?

upvoted 1 times

jackr76 8 months, 2 weeks ago

- "running": null
- "name":"100"
- "permit"
- "match"

TIP: runapem

upvoted 4 times

bora4motion 11 months, 2 weeks ago

1 - running
2 - name
3 - seq (this is a route-map)
4 - match the acl/prefix for the route-map.

upvoted 9 times

MO_2022 11 months, 3 weeks ago

Answer:
1. “running”: null
2. “name”:”100”,
3. “seq_no”:
4. “match”:

upvoted 4 times

Stylar 12 months ago

I would put the following:

1. “running”: null <<<<target running config
2. “name”:”100”, <<<<< prefix list name "100"
3. “seq_no”: <<<<<<< there is no permit command within a route map. this is the only logical selection here.
4. “match”: again within a route map we can either set, or match.

upvoted 9 times

Degen6969 7 months ago

There is permit/deny ‘seq no’

https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/route-maps.pdf

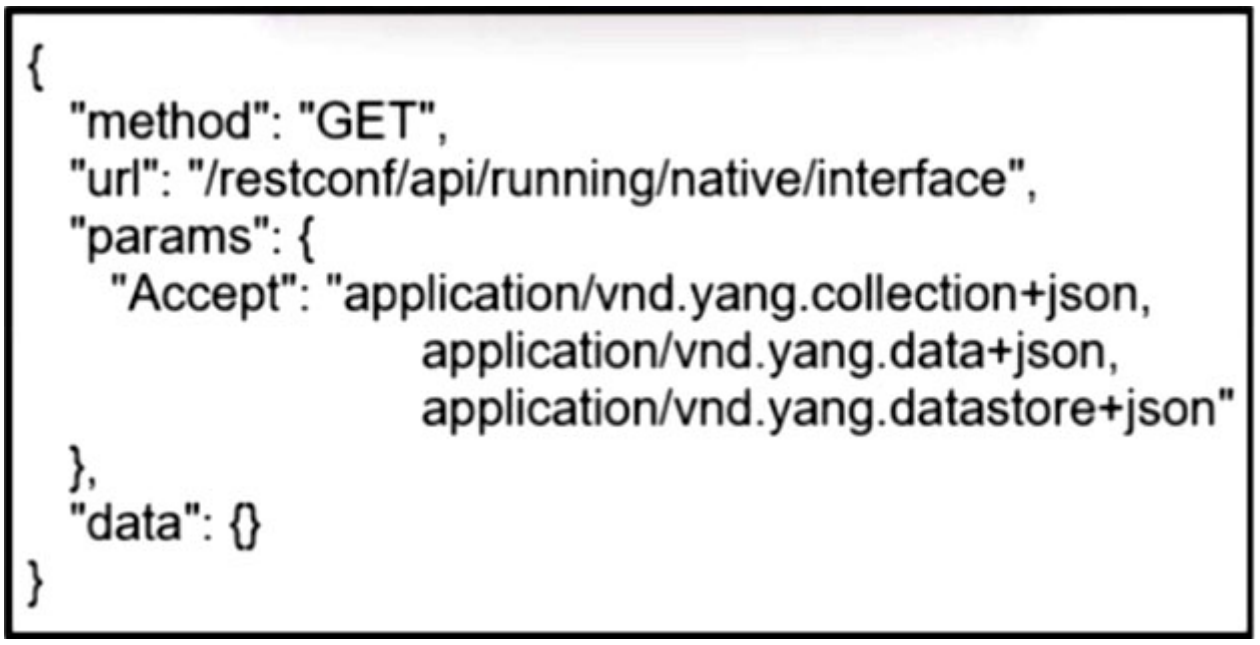
upvoted 1 times

LanreDipeolu 2 months, 4 weeks ago

link did not work. Please re-paste.

upvoted 1 times

Question #426 *Topic 1*



```
{
  "method": "GET",
  "url": "/restconf/api/running/native/interface",
  "params": {
    "Accept": "application/vnd.yang.collection+json,
               application/vnd.yang.data+json,
               application/vnd.yang.datastore+json"
  },
  "data": {}
}
```

Refer to the exhibit. What is the result of the API request?

A. The native interface information is read from the network appliance.

B. The information for all interfaces is read from the network appliance.

C. The ג€paramsג€ variable reads data fields from the network appliance.

D. The ג€paramsג€ variable sends data fields to the network appliance.

Correct Answer: *A*

Community vote distribution

B (95%) 5%

Alberht Highly Voted 1 year, 2 months ago

Selected Answer: B

I think All Interfaces could be the answer as there is no such thing as one native interface on a device. See below link.

upvoted 7 times

Darude Highly Voted 1 year ago

Selected Answer: B

I Find it the correct answer is B
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRCRT-2700-LG.pdf page 10 step 7
:Issue an API call to see all configured interfaces on the system.
Method: GET
URL: https://csr1kv/restconf/data/Cisco-IOS-XE-native:native/interface

upvoted 7 times

Chuckzero Most Recent 2 months, 3 weeks ago

The correct answer is B.

The JSON object structure provided is actually reading the Native interfaces, but all the information for all interface is read from the network appliance.

The Params: This section includes multiple "Accept" headers with different media types, indicating the content types that the client is willing to accept as a response from the server. The provided media types are "application/vnd.yang.collection+json," "application/vnd.yang.data+json," and "application/vnd.yang.datastore+json."

upvoted 1 times

markymark874 10 months, 4 weeks ago

Selected Answer: B

B is correct

upvoted 4 times

iGlitch 1 year ago

Selected Answer: B

Answer is B

upvoted 3 times

tckoon 1 year, 1 month ago

Selected Answer: A

A is correct answer.
info from slide mention ther is ietf-interface and native interface on rescon url structure.
https://www.netacad.com/sites/default/files/images/careers/Webinars/DevNet2/programmability_w_devnet_session_6_content_slides.pdf

upvoted 1 times

Alberht 1 year, 2 months ago

I read https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b_166_programmability_cg/restconf_prog_int.pdf and /restconf/api isn't even mentioned. Plus in the native part there is always a specific interface mentioned. I think All Interfaces could be the answer as there is no such thing as one native interface on a device.

upvoted 2 times

Deu_Inder 1 year, 2 months ago

Is A the right answer?

upvoted 1 times

Degen6969 7 months ago

See darude comment above, B should be correct.

upvoted 1 times

Question #427 *Topic 1*

Which definition describes JWT in regard to REST API security?

A. an encrypted JSON token that is used for authentication

B. an encrypted JSON token that is used for authorization

C. an encoded JSON token that is used to securely exchange information

D. an encoded JSON token that is used for authentication

Correct Answer: *D*

Community vote distribution

C (58%) D (42%)

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: C

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object.
references: https://jwt.io/introduction/

upvoted 8 times

Edwinmolinab 1 year ago

I don´t agree even if your definition is correct. Here the question is for a REST API could be D because in this case it is used for authentication

upvoted 1 times

Calica Most Recent 2 months, 4 weeks ago

ChatGPT: D. an encoded JSON token that is used for authentication

JWT (JSON Web Token) is commonly used for authentication in REST API security. It is an encoded token that contains user or system information, and it is used to verify the identity of a user or system when making requests to an API.

upvoted 1 times

Marjansh 3 months ago

A JSON web token(JWT) is JSON Object which is used to securely transfer information over the web(between two parties). It can be used for an authentication system and can also be used for information exchange. The token is mainly composed of header, payload, signature. These three parts are separated by dots(.)

upvoted 1 times

djedeen 3 months, 1 week ago

Selected Answer: C

Challenging semantics, but the reference to #651 below tells me it is C.

upvoted 1 times

[Removed] 4 months, 4 weeks ago

Selected Answer: D

I'm still new to APIs and programming, but if I know cisco, they are about answering what is asked, and they hold your feet to the fires of semantics. This question is asking what JWT is in the context of REST APIs, and based on some sources, it specifically talks about authentication. While C is correct in the what JWT's purpose is, D is answering the question asked.

https://blog.logrocket.com/secure-rest-api-jwt-authentication/

upvoted 4 times

CHERIFNDIAYE 5 months, 3 weeks ago

Selected Answer: C

the correct answer is C.
JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object

upvoted 1 times

SUk10 6 months ago

Answer is C
REST API is a creation of data transmission, Although JWT is created for authentication purposes, the question simply ask what is the definition of JWT in regards to REST API.

upvoted 1 times

mrtattoo 6 months, 4 weeks ago

Selected Answer: D

You could argue that answer C is partially correct, as JWTs can be used to securely exchange information between parties. However, in the context of REST API security, the primary use case of JWTs is for authentication, not for exchanging information.

JWTs are commonly used to transmit authentication information between a client and a server, allowing the client to prove its identity to the server. The server generates a JWT that includes a set of claims about the authenticated user, such as their ID or roles, and sends this token back to the client. The client can then include the JWT in subsequent requests to the server to prove its identity.

While a JWT can include additional information beyond just authentication claims, its primary purpose in the context of REST API security is for authentication. Therefore, answer D ("an encoded JSON token that is used for authentication") is the most accurate answer to the question.

upvoted 3 times

Degen6969 7 months ago

Selected Answer: D

In regards to REST APIs

https://blog.logrocket.com/secure-rest-api-jwt-authentication/

upvoted 2 times

NetAdmin950 8 months ago

Selected Answer: C

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed.

upvoted 2 times

Clauster 8 months, 1 week ago

Selected Answer: D

JWT is in no way shape of form encrypted. It is used to Authenticate which is more secure, but really it's used to authenticate.

upvoted 1 times

Clauster 8 months, 1 week ago

Selected Answer: C

For those of you who are still confused about this, check out question
651:
JSON web tokens (JWT) are used to secure JSON based communications. Which of the following fields make up a JWT? (Choose three.)

A. Header
B. Trailer
C. Payload
D. Sequence number
E. Signature

It is clearly used to secure communications.
:)

upvoted 3 times

Clauster 8 months, 3 weeks ago

Selected Answer: C

The Answer is C
The Answer can be found here:

https://www.ionos.com/digitalguide/websites/web-development/json-web-token-jwt/#:~:text=A%20JSON%20Web%20Token%20%28JWT%29%20is%20an%20access,doesn%E2%80%99t%20need%20to%20be%20saved%20on%20the%20server.

upvoted 1 times

snarkymark 9 months, 2 weeks ago

Choosing D, based on the following:
https://levelup.gitconnected.com/how-to-secure-your-rest-api-using-jwt-a923ba4a497e

upvoted 2 times

Degen6969 7 months ago

And

https://blog.logrocket.com/secure-rest-api-jwt-authentication/

upvoted 2 times

Cooldude89 9 months, 3 weeks ago

C is correct
JWT can be used to pass the identity of authenticated users between an identity provider and a service provider (which are not necessarily the same system)

upvoted 1 times

rafaelinho88 9 months, 4 weeks ago

Selected Answer: C

JSON Web Token (JWT) is a compact and self-contained method for securely transmitting information between parties as a JSON object. In the context of REST API security, JWT is commonly used to transmit claims or assertions between parties to ensure authentication and authorization. The JSON object is digitally signed using a secret key or a public/private key pair to guarantee the authenticity of the information.

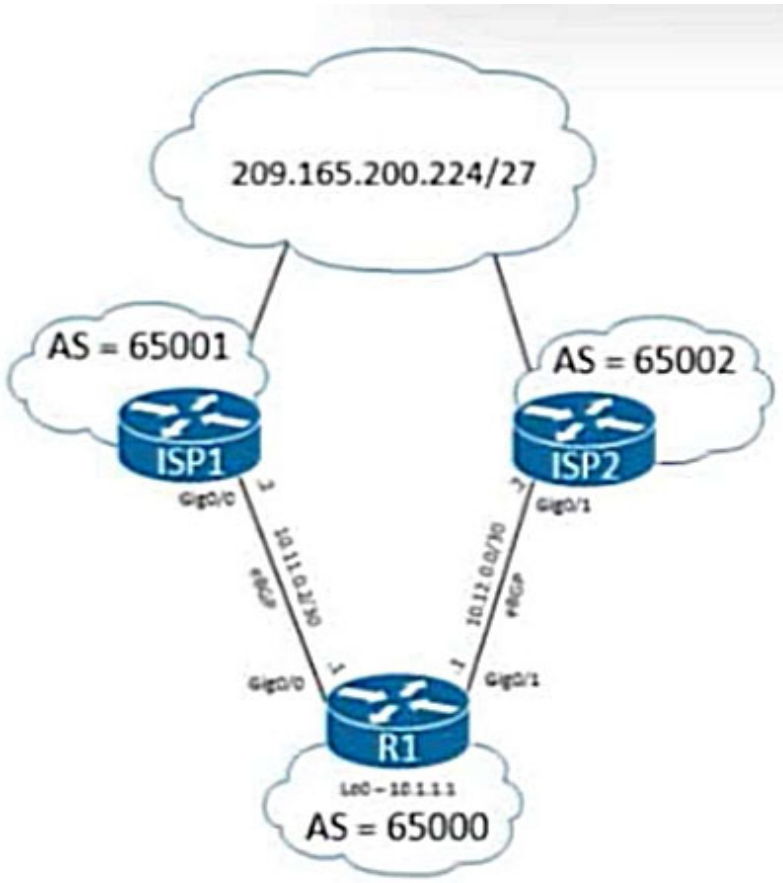
upvoted 1 times

Ayman_B 10 months, 2 weeks ago

Selected Answer: D

JWT is used to securely transmit information between parties.
In this case, when a client sends a request to a REST API, it includes a JWT in the request headers. The API then uses the information in the JWT to authenticate the client and authorize the request.

upvoted 3 times




```
R1#show run | section bgp
router bgp 65000
 bgp router-id 10.1.1.1
 bgp log-neighbor-changes
 network 10.1.1.1 mask 255.255.255.255
 neighbor 10.11.0.2 remote-as 65001
 neighbor 10.11.0.2 route-map AS65001 in
 neighbor 10.12.0.2 remote-as 65002
 neighbor 10.12.0.2 route-map AS65002 in

R1#show route-map
route-map AS65001, permit, sequence 10
  Match clauses:
  Set clauses:
    weight 200
  Policy routing matches: 0 packets, 0 bytes
route-map AS65002, permit, sequence 10
  Match clauses:
  Set clauses:
    as-path prepend 65000 65000 65000
  Policy routing matches: 0 packets, 0 bytes

R1#show bgp 209.165.200.224/27
BGP routing table entry for 209.165.200.224/27, version 3
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
     2
  Refresh Epoch 3
65001 64500
  10.11.0.2 from 10.11.0.2 (10.1.1.2)
    Origin IGP, localpref 100, weight 200, valid, external, best
    rx pathid: 0, tx pathid: 0x0
Refresh Epoch 2
65000 65000 65000 65002 64500
  10.12.0.2 from 10.12.0.2 (10.1.1.3)
    Origin IGP, localpref 100, valid, external
    rx pathid: 0, tx pathid: 0
```

Refer to the exhibit. A client has two directly connected eBGP peering links with diverse ISPs. Both providers advertise the same public prefix 209.165.200.224/27 to R1 without any route manipulation. Traffic leaves R1 outbound via ISP1 but returns inbound via ISP2. Which configuration prevents asymmetrical routing and makes ISP1 the preferred path inbound and outbound?

A.

```
R1# config t
R1(config)# router bgp 65000
R1(config-router)# neighbor 10.11.0.2 route-map AS65001 out
```

B.

```
R1# config t
R1(config)# route-map AS65002 permit 10
R1(config-route-map)# set weight 100
```

C.

```
R1# config t
R1(config)# router bgp 65000
R1(config-router)# neighbor 10.12.0.2 route-map AS65002 out
```

D.

```
R1# config t
R1(config)# route-map AS65001 permit 10
R1(config-route-map)# set local-preference 100
```

Correct Answer: *C*

landgar 10 months, 2 weeks ago

Exported routes from R1 should be advertised with AS path prepend to ISP2, to make it less preferred. This is the same way as the incoming routes coming with a longer AS path by ISP2. The 3 ASs 65000 in the incoming routes is to mislead us.

upvoted 1 times

markymark874 10 months, 4 weeks ago

C is correct. Change the bgp neighbor setting to out instead of in for ISP2 to influence the routes sent to ISP2 to make the routing less preferred.

upvoted 2 times

Asymptote 10 months, 4 weeks ago

C is the correct answer.

R1 makes ISP2 less preferenced by adding more AS path to its best path advertisement.
prepended AS path is transitive and the upstream will choose the lesser AS path as the best path which is ISP1 to reach R1.

upvoted 1 times

nushadu 12 months ago

as I got it, from AS 64500 (not shown in the map but you see it in as path) point of view after "answer C" 3 hops were added to the as path towards ISP2 and ISP2 propagates this info further, so as64500 chooses the shortest path with 3 hops compare to six, agree? :))

upvoted 1 times

nushadu 11 months, 1 week ago

the problem here with the DIRECTION of applying route-map, it must be EXPORTED to peer (OUT in Cisco terminology) but in the current config, it is IMPORTED (IN direction) so we need just to change direction from in -> out in cmd.
"C" is my answ.

upvoted 2 times

attiko 1 year ago

The Answer is C, correct.

upvoted 1 times

FrameRelay 1 year, 1 month ago

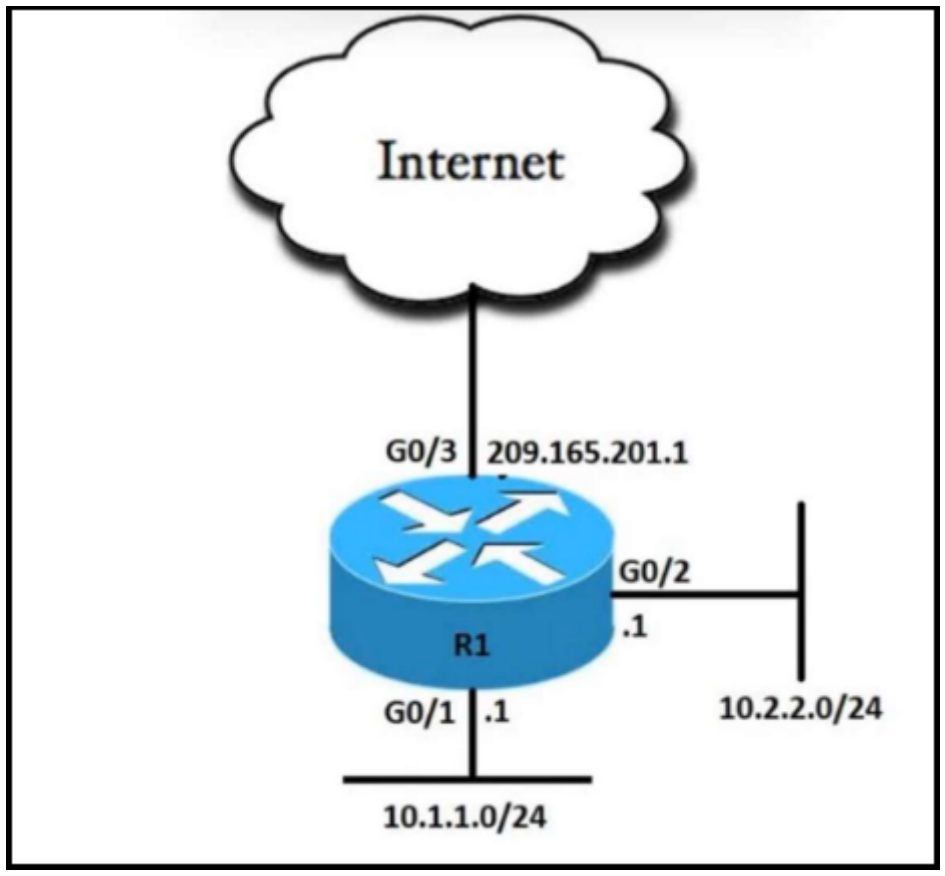
when I am not sure like I am now I go for exclusion, D is out of the question since local preference has only affect locally, then B is also out because the ACL would again have affect only on the local router and because we are setting weight to 100, the weight on the link toward ISP1 is still better as the weight is 200, therefore a null change there. A and C remain as contendents, and the weight change makes sense but because we are trying to influence ISP2 path choice, C accually has a better method by prepending 3 extra hops to the path, so to me it looks like C makes the most sense.

upvoted 3 times

jj970us 1 year, 2 months ago

Is C is the correct answer?

upvoted 2 times



Refer to the exhibit. An engineer must allow all users in the 10.2.2.0/24 subnet to access the internet. To conserve address space, the public interface address of
209.165.201.1 must be used for all external communication.
Which command set accomplishes these requirements?

A.

```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 209.165.201.1
```

B.

```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/3
```

C.

```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/2 overload
```

D.

```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/3 overload
```

Correct Answer: *D*

CCNPWILL 1 month, 2 weeks ago
overload is needed for PAT. that kills 2 answers. Need overload on outside interface... leaves one answer... D.
upvoted 2 times

adrian0792 5 months, 2 weeks ago
D is correct
upvoted 2 times

Xerath 11 months, 2 weeks ago
Answer is "D".
upvoted 3 times

attiko 1 year ago
D is correct
upvoted 1 times

Wooker 1 year, 2 months ago
D is correct.
upvoted 2 times

Joseph123 1 year, 2 months ago
Correct answer is C
upvoted 1 times

FrameRelay 1 year, 1 month ago
unfortunately no, the Natting is done on the outside interface not the inside interface. D is correct. IP NAT INSIDE (source) (dest) overload
upvoted 1 times

uzbin 1 year, 2 months ago
D is correct.
Outside interface is Gi0/3. C references wrong interface is ip nat inside ...statement
upvoted 3 times

Question #430 *Topic 1*

What is a TLOC in a Cisco SD-WAN deployment?

A. value that identifies a specific tunnel within the Cisco SD-WAN overlay

B. identifier that represents a specific service offered by nodes within the Cisco SD-WAN overlay

C. attribute that acts as a next hop for network prefixes

D. component set by the administrator to differentiate similar nodes that offer a common service

Correct Answer: *C*

Community vote distribution

C (53%) A (47%)

landgar Highly Voted 10 months, 2 weeks ago

TLOC for the overlay acts as IP next hop for the underlay:
https://www.networkacademy.io/ccie-enterprise/sdwan/underlay-vs-overlay-routing
upvoted 5 times

LanreDipeolu Most Recent 2 months, 4 weeks ago

Good contribution from everyone. THX
upvoted 2 times

djedeen 3 months, 1 week ago

Selected Answer: C

OMP Routes
VPN: Every OMP route is associated with a VPN, and every Cisco SD-WAN device keeps a separate routing table for each VPN. ...
Originator: This is the System-IP of the router, from which the route was originally learned from. ...
TLOC: This is the next-hop identifier of the OMP route.
upvoted 1 times

Soggyt74 3 months, 3 weeks ago

Selected Answer: C

TLOC: This is the transport location identifier of the next hop for OMP routes. It is
similar to the BGP NEXT_HOP attribute.

CCNP Enterprise Design ENSLD 300-420 Official Cert Guide page 353
upvoted 1 times

[Removed] 5 months ago

Selected Answer: A

Looks like A and C are technically correct. At least based on the following documentation:

Choose what you will, I chose A based on this information but C looks correct too.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-unicast-routing.html

"Configure the Number of Advertised Routes
A Cisco IOS XE SD-WAN device can have up to eight WAN interfaces, and each WAN interface has a different TLOC (...) that is configured as a tunnel interface. (...) This means that each router can have up to eight TLOCs. The device advertises each route–TLOC tuple to the Cisco vSmart Controller."

"OMP Route Advertisements
(...), OMP advertises to its peers the routes and services that it has learned from its local site, along with their corresponding transport location mappings, which are called TLOCs. These routes are called OMP routes or vRoutes to distinguish them from standard IP routes. T(...)."
upvoted 2 times

Danny_Xu 12 months ago

Selected Answer: A

"Put simply, TLOCs are data plane setup instructions sent by each WAN Edge to the vSmart. The vSmart then distributes the maps to the other WAN Edge routers per the topology policy, facilitating the data plane tunnel establishment."
https://carpe-dmvpn.com/2019/12/14/tlocs-cisco-sd-wan/
So that I will go to answer A.
upvoted 2 times

Typovy 12 months ago

Selected Answer: C

"TLOCs serve another important function besides data plane connectivity. In OMP terms (the routing protocol used over the SD-WAN Fabric), the TLOC serves as a next-hop for route advertisements."

upvoted 2 times

Huntkey 1 year ago

Selected Answer: C

OMP Routes, also referred to as vRoutes, are prefixes learned at the local site via connected interfaces, static routes, and dynamic routing protocols (such as OSPF, EIGRP, and BGP) running on the service side of the vEdge. These prefixes are redistributed into OMP and advertised to the vSmart controller so that they can be carried across the overlay fabric to all other WAN edge nodes. OMP routes resolve their next-hop to a TLOC. An OMP route is installed in the forwarding table only if the next-hop TLOC is known and there is a BFD session in UP state associated with that TLOC;

upvoted 1 times

Huntkey 1 year ago

https://www.networkacademy.io/ccie-enterprise/sdwan/omp-overview#:~:text=OMP%20routes%3A%20OMP%20Routes%2C%20also,service%20side%20of%20the%20vEdge.

upvoted 1 times

exz97317 1 year ago

According to the official Cisco SD-WAN book:
"TLOCs are what identify the WAN Edge to the physical underlay"
Meaning Answer A would be wrong because it says "SD-WAN overlay"
I would go with answer C

upvoted 1 times

GeorgeFortiGate 1 year ago

Selected Answer: A

A TLOC is a Cisco WAN Edge devicea Transport Locator that represents an attachment point where connects to a WAN transport. A TLOC is uniquely identified by a tuple of three values - (System-IP address, Color, Encapsulation)
A TLOC route consists of all required information needed by a remote peer in order to establish an overlay tunnel with that TLOC. This includes private and public IP addresses and ports, site-id, preference, weight, status, encapsulation info such as encryption and authentication parameters, and much more.

upvoted 2 times

Abdullavip 1 year ago

Selected Answer: A

In IOS-XE SDWAN, the routing table itself only shows the valid next-hop as the System-IP of the advertising TLOC. The routing table only shows the valid next-hop TLOC system-ip per route, not all the TLOCs that can be used to get there. The main takeaway is to remember that a TLOC is not a physical next-hop in terms of data plane. It is a map to a specific WAN Edge on a particular transport color. Correct Answer is A.

upvoted 2 times

RREVECO 1 year, 2 months ago

Selected Answer: C

The answer C is correct.

ref: book Cisco Software-Defined Wide Area Networks
Chapter OMP routes, page 48–51
TLOC: The Transport Location (TLOC) identifier is the next hop of the OMP route. This attribute is very similar to the BGP_NEXT_HOP attribute. Within the TLOC, there are three values:

upvoted 4 times

jj970us 1 year, 2 months ago

The answer C is correct.
Reference: https://carpe-dmvpn.com/2019/12/14/tlocs-cisco-sd-wan/

upvoted 1 times

Deu_Inder 1 year, 2 months ago

Thanks for the link.

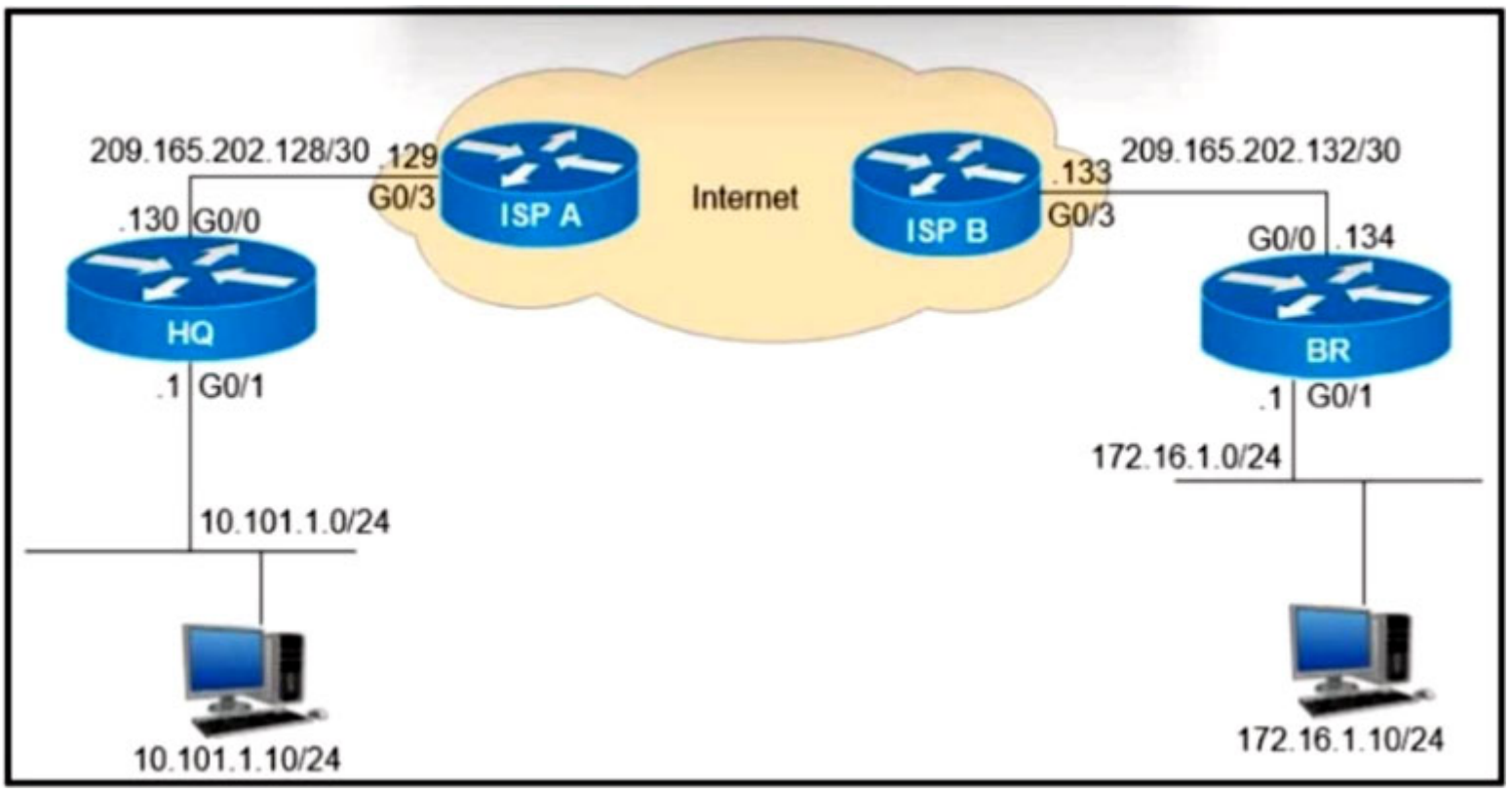
upvoted 1 times

Joseph123 1 year, 2 months ago

Correct answer should be A

upvoted 1 times

Question #431 *Topic 1*



Refer to the exhibit. Which configuration must be applied to the HQ router to set up a GRE tunnel between the HQ and BR routers?

A.
```
interface Tunnel1
 ip address 209.165.202.130 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

B.
```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

C.
```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.134
```

D.
```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.133
```

Correct Answer: *C*

attiko Highly Voted 1 year ago
C is the right answer, the destination address for the tunnel should be the public IP of the other router, in our case ending with 134.
upvoted 8 times

HarwinderSekhon Highly Voted 5 months, 3 weeks ago
Ignore everything and just focus tunnel destination.
upvoted 5 times

rmonteroherrera 2 months, 2 weeks ago
exactly
upvoted 1 times

Stylar Most Recent 10 months, 1 week ago
C is correct, if we ignore the fact that the space 10.111.X.X is not inserted in the diagram
upvoted 4 times

KOJJY 11 months, 3 weeks ago
C is correct
upvoted 1 times

bora4motion 1 year ago

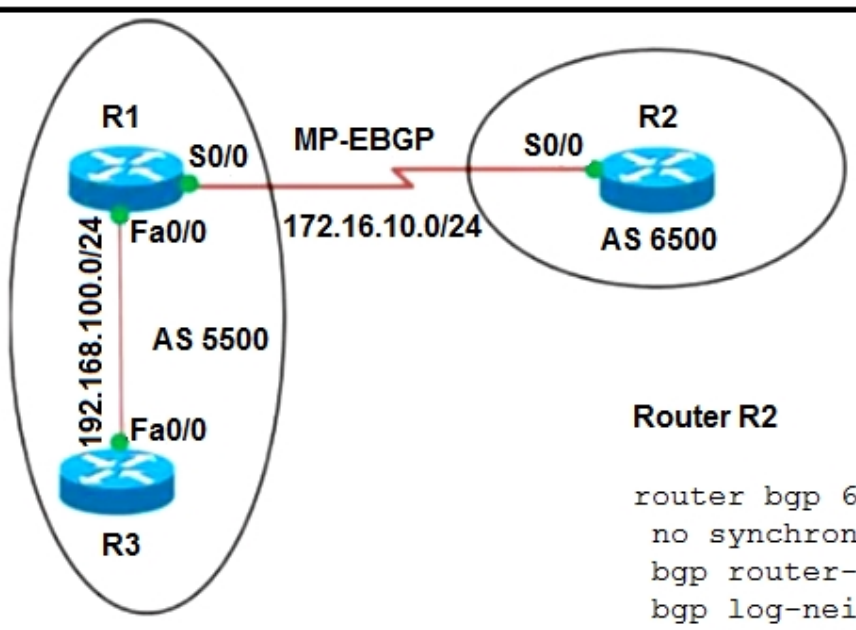
C is correct

upvoted 1 times

bora4motion 1 year ago

C is correct.

upvoted 1 times



Router R1

```
router bgp 5500
 no synchronization
 bgp router-id 10.10.10.10
 bgp log-neighbor-changes
 network 192.168.100.0
 redistribute connected
 neighbor 172.16.10.2 remote-as 5500
 neighbor 172.16.10.2 soft-reconfiguration inbound
 neighbor 192.168.100.11 remote-as 5500
 no auto-summary
 !
 address-family vpnv4
  neighbor 172.16.10.2 activate
  neighbor 172.16.10.2 send-community both
 exit-address-family
```

Router R2

```
router bgp 6500
 no synchronization
 bgp router-id 20.20.20.20
 bgp log-neighbor-changes
 neighbor 172.16.10.1 remote-as 5500
 no auto-summary
 !
 !
 address-family vpnv4
  neighbor 172.16.10.1 activate
  neighbor 172.16.10.1 send-community both
 exit-address-family
 !
 address-family ipv4 vrf WAN
  redistribute connected
  redistribute static
  neighbor 172.16.10.1 remote-as 5500
  neighbor 172.16.10.1 activate
  no synchronization
  exit-address-family
```

Refer to the exhibit. An engineer configures the BGP adjacency between R1 and R2; however, it fails to establish. Which action resolves the issue?

A. Change the network statement on R1 to 172.16.10.0.

B. Change the remote-as number on R1 to 6500.

C. Change the remote-as number for 192.168.100.11.

D. Enable synchronization on R1 and R2.

Correct Answer: *B*

Community vote distribution

B (100%)

KOJJY 11 months, 3 weeks ago

Selected Answer: B

B 1000%

upvoted 4 times

bora4motion 1 year ago

Selected Answer: B

B is correct, AS needs to be changed from 5500 to 6500

upvoted 1 times

attiko 1 year ago

Selected Answer: B

B is correct, The EBGP neighbor for R1 is in the AS 6500, and not the same AS 5500

upvoted 1 times

Joseph123 1 year, 2 months ago

B is correct

upvoted 1 times

```
Switch1# show interfaces trunk
! Output omitted for brevity
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802.1q trunking 10

Port Vlans allowed on trunk
Gi1/0/20 1-4094

Switch2# show interfaces trunk
! Output omitted for brevity
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802.1q trunking 10

Port Vlans allowed on trunk
Gi1/0/20 1-4094
```

Refer to the exhibit. The trunk does not work over the back-to-back link between Switch1 interface Gig1/0/20 and Switch2 interface Gig1/0/20. Which configuration fixes the problem?

A. Switch 1(config)#interface gig1/0/20 Switch1(config-if)#switchport mode dynamic auto

B. Switch2(config)#interface gig1/0/20 Switch2(config-if)#switchport mode dynamic desirable

C. Switch2(config)#interface gig1/0/20 Switch2(config-if)#switchport mode dynamic auto

D. Switch1(config)#interface gig1/0/20 Switch1(config-if)#switchport trunk native vlan 1 Switch2(config)#interface gig1/0/20 Switch2(config-if)#switchport trunk native vlan 1

Correct Answer: *B*

Community vote distribution

B (100%)

CCNPWILL 1 month, 2 weeks ago

Correct. auto/auto no trunk. provided answer is correct.

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

In PagP, Auto/Auto doesnt form a trunk. Auto/Desirable does

upvoted 1 times

dragonwise 8 months ago

A.
Switch 1(config)#interface gig1/0/20
Switch1(config-if)#switchport mode dynamic auto

B.
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic desirable

C.
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic auto

D.
Switch1(config)#interface gig1/0/20
Switch1(config-if)#switchport trunk native vlan 1
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport trunk native vlan 1

upvoted 1 times

mitosenoriko 1 year, 1 month ago

Selected Answer: B

answer B

upvoted 2 times

Radwa_ 1 year, 1 month ago

Selected Answer: B

Provided answer is correct

upvoted 1 times

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# description source1
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/4 - 8 tx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/3
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 100
Device(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
Device(config-mon-erspan-src-dst)# ip prec 5
Device(config-mon-erspan-src-dst)# ip ttl 32
Device(config-mon-erspan-src-dst)# mtu 1700
Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)# vrf 1
Device(config-mon-erspan-src-dst)# no shutdown
Device(config-mon-erspan-src-dst)# end
```

Refer to the exhibit. An engineer must configure an ERSPAN session with the remote end of the session 10.10.0.1. Which commands must be added to complete the configuration?

A. Device(config)#monitor session 1 type erspan-source Device(config-mon-erspan-src)#destination Device(config-mon-erspan-src-dst)#no origin ip address 10.10.0.1 Device(config-mon-erspan-src-dst)#ip address 10.10.0.1

B. Device(config)#monitor session 1 type erspan-source Device(config-mon-erspan-src)#destination Device(config-mon-erspan-src-dst)#no vrf 1

C. Device(config)#monitor session 1 type erspan-source Device(config-mon-erspan-src)#destination Device(config-mon-erspan-src-dst)#no origin ip address 10.10.0.1 Device(config-mon-erspan-src-dst)#ip destination address 10.10.0.1

D. Device(config)#monitor session 1 type erspan-destination Device(config-mon-erspan-src)#source Device(config-mon-erspan-src-dst)#origin ip address 10.1.0.1

Correct Answer: *B*

Community vote distribution

A (100%)

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: A

Reference: https://networklessons.com/cisco/ccie-routing-switching-written/erspan

The configuration in the exhibit is missing destination IP address for the GRE tunnel so we have to add it with the “ip address 10.10.0.1”.

upvoted 11 times

dragonwise Highly Voted 8 months ago

A.
Device(config)#monitor session 1 type erspan-source
Device(config-mon-erspan-src)#destination
Device(config-mon-erspan-src-dst)#no origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)#ip address 10.10.0.1

B.
Device(config)#monitor session 1 type erspan-source
Device(config-mon-erspan-src)#destination
Device(config-mon-erspan-src-dst)#no vrf 1

C.
Device(config)#monitor session 1 type erspan-source
Device(config-mon-erspan-src)#destination
Device(config-mon-erspan-src-dst)#no origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)#ip destination address 10.10.0.1

D.

Device(config)#monitor session 1 type erspan-destination
Device(config-mon-erspan-src)#source
Device(config-mon-erspan-src-dst)#origin ip address 10.1.0.1

upvoted 8 times

[Removed] Most Recent 4 months, 3 weeks ago

Selected Answer: A

Correct

upvoted 1 times

bendarkel 9 months ago

Selected Answer: A

A is the correct answer.

upvoted 2 times

Cooldude89 9 months, 2 weeks ago

Selected Answer: A

A is correct syntax
C was close...

upvoted 1 times

markymark874 10 months, 4 weeks ago

Selected Answer: A

A- is correct missing ip address for the tunnel. So need to remove the extra config and add the ip address

upvoted 1 times

KOJJY 11 months, 3 weeks ago

Selected Answer: A

answer is A

upvoted 1 times

Caledonia 1 year, 2 months ago

Selected Answer: A

The answer is A

upvoted 3 times

An engineer must configure a router to leak routes between two VRFs. Which configuration must the engineer apply?

A.

```
ip access-list extended acl-to-red
  permit ip any 10.1.1.0 0.0.0.255
route-map rm-to-red permit 10
  match ip address 50
ip vrf RED
  rd 1:1
  import ipv4 unicast map rm-to-red
```

B.

```
ip access-list extended acl-to-red
  permit ip 10.1.1.0 0.0.0.255 any
route-map rm-to-red permit 10
  match ip address acl-to-red
ip vrf RED
  rd 1:1
  import ipv4 unicast map rm-to-red
```

C.

```
ip access-list extended acl-to-red
  permit ip 10.1.1.0 0.0.0.255 any
route-map rm-to-red permit 10
  match ip address acl-to-red
ip vrf RED
  rd 1:1
  import ipv4 unicast route-map acl-to-red
```

D.

```
ip access-list extended acl-to-red
  permit ip 10.1.1.0 0.0.0.255 any
route-map rm-to-red permit 10
  match ip address acl-to-red
ip vrf RED
  rd 1:1
  import ipv4 unicast acl-to-red
```

Correct Answer: *C*

PALURDIN Highly Voted 1 year, 2 months ago

Correct answer is B:
https://www.cisco.com/c/en/us/td/docs/ios/12_2s/feature/guide/fs_bgivt.html

upvoted 11 times

[Removed] Most Recent 5 months, 1 week ago

B is the answer
The referencing object under vrf configuration mode should be the route-map not the ACL

upvoted 1 times

FerroForce 7 months ago

The answer is B. Pay attention to the name of route-map and ACL

upvoted 3 times

dragonwise 8 months ago

I think it really depends on the router's software
For example,
Router1, I got this:
R1(config-vrf)#import ipv4 unicast ?
<1-2147483647> Upper limit on import prefixes without hogging memory
map Route-map based VRF import

R1(config-vrf)#import ipv4 unicast

In Router2, I got this:
ip vrf customer-a

address-family ipv4
import route-map export-to-vrf
exit-address-family
upvoted 1 times

klaasvaak 9 months, 1 week ago

Correct answer I B:
upvoted 1 times

yrzy 9 months, 2 weeks ago

Correct answer is B:
upvoted 1 times

TSKARAN 10 months ago

Answer: B

R-1(config-vrf)#import ipv4 ?
multicast Import prefixes from IPv4 Multicast table
unicast Import prefixes from IPv4 Unicast table

R-1(config-vrf)#import ipv4 un
R-1(config-vrf)#import ipv4 unicast ?
<1-2147483647> Upper limit on import prefixes without hogging memory
map Route-map based VRF import

SW-1(config-vrf)#import ipv4 unicast ma
R-1(config-vrf)#import ipv4 unicast map
upvoted 2 times

markymark874 10 months, 4 weeks ago

Correct answer is B
upvoted 3 times

dnjJ56 11 months, 1 week ago

Correct Answer B:

Tested in LAB. Need to do a few more things to get the leaking working.
Like running VRF Lite with BGP and distributing the routes to BGP.
https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200158-Configure-Route-Leaking-between-Global-a.html
(this article uses a STD ACL, but EXTENDED ACL also works with destination set to Any, like in the Answer B)

A: reference to wrong ACL, ACL also has source/dest reversed.
C: import statement has route-map. should be just 'map'.
D: import statement is missing the 'map' keyword.
upvoted 3 times

nushadu 11 months, 1 week ago

yes, agree
upvoted 1 times

nushadu 11 months, 1 week ago

C. is technically (syntax) correct but I did not see route leaking in the lab, probably IOL restricyions:
!
ip vrf cust_1
rd 11:11
import ipv4 unicast map cust_2_to_cust_1
!
route-map cust_2_to_cust_1 permit 10
match ip address cust_2_netw
!
ip access-list extended cust_2_netw
permit ip 172.16.1.0 0.0.0.255 any
!
cisco_R3(config)#do s ip ro vrf cust_1 | b Ga
Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Ethernet0/0.20
L 192.168.1.1/32 is directly connected, Ethernet0/0.20
L 192.168.1.200/32 is directly connected, Ethernet0/0.20
cisco_R3(config)#
cisco_R3(config)#do s ip ro vrf cust_2 | b Ga
Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Ethernet0/0.30
L 172.16.1.1/32 is directly connected, Ethernet0/0.30
S 192.168.1.0/24 [1/0] via 192.168.1.1
cisco_R3(config)#
upvoted 1 times

x3rox 10 months ago

the sintac is incorrect. Your code has different sintext than answer C.
import ipv4 unicast | multicast [prefix-limit] map route-map (Look at the keyword "map". Answer C has route-map keyword.)
Answer is B

upvoted 1 times

nushadu 11 months, 1 week ago

update! B is my answ.

upvoted 1 times

robi1020 11 months, 3 weeks ago

1. enable
2. configure terminal
3. ip vrf vrf-name
4. rd route-distinguisher
5. import ipv4 unicast | multicast [prefix-limit] map route-map
6. exit
7. route-map map-tag [permit | deny] [sequence-number]

etc.....

Its "B"

upvoted 1 times

shoo83 1 year ago

B is correct,
The key word is using unicast map instead of route-map

upvoted 1 times

H3kerman 1 year ago

C can't be right ecause in route map is defined name of ACL, I would vote B

upvoted 1 times

Wooker 1 year, 2 months ago

answer is B

upvoted 2 times

Caledonia 1 year, 2 months ago

Agree the answer is B

upvoted 3 times

Question #436 *Topic 1*

Which Python code snippet must be added to the script to save the returned configuration as a JSON-formatted file?

```
import json
import requests

Creds = ("admin", "S!415421481$Ptx")
Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

BaseURL = https://cpe/restconf/data"
URL = BaseURL + "/Cisco-IOS-XE-native/interface/GigabitEtherenet"

Response = requests.get(URL, auth = Creds, headers = Headers, verify = False)
```

A.

```
with open("ifaces.json", "w") as OutFile:
  JSONResponse = json.loads(Response.text)
  OutFile.write(JSONResponse)
```

B.

```
with open("ifaces.json", "w") as OutFile:
  OutFile.write(Response)
```

C.

```
with open("ifaces.json", "w") as OutFile:
  OutFile.write(Response.text)
```

D.

```
with open("ifaces.json", "w") as OutFile:
 OutFile.write(Response.json())
```

Correct Answer: *A*

Faridtnx Highly Voted 10 months, 2 weeks ago

I've read the for ENCOR we just need to "6.1 Interpret basic Python components and scripts". I wonder why I see alot of high level question about Python here

upvoted 25 times

[Removed] 5 months, 1 week ago

It is really bothering me how many questions there are about programing languages.

upvoted 11 times

mgiuseppe86 2 months, 2 weeks ago

Im a bit nervous about this stuff. If these are brain dumps from the actual exam, why is this stuff on here? This is not networking. ENCOR is very misleading.

upvoted 3 times

PureInertiaCopy 3 months, 2 weeks ago

Same here...

upvoted 2 times

Solaaa 9 months, 1 week ago

I am wondering as well

upvoted 6 times

attiko Highly Voted 1 year ago

Answer is C, I verified by writing the below program to test:

```
import json
import requests
```

```
url = "http://ip.jsontest.com"
response = requests.get(url)

print(response)

with open("ifaces.json","w") as outfile:
outfile.write(response.text)
```

upvoted 12 times

Zizu007 1 year ago

A: wrong - python error: "argument must be str, not dict"
B: wrong - python error: "argument must be str, not Response"
C: Correct. file created as .json
D: Wrong - python error: "argument must be str, not dict"

upvoted 5 times

Colmenarez 4 months ago

A is correct. json.loads() is taken response.text

upvoted 1 times

PureInertiaCopy Most Recent 3 months, 2 weeks ago

The correct answer is C.

C. with open("ifaces.json", "w") as OutFile:
OutFile.write(Response.text)

Explanation: When you make a request using the requests.get() method, the response object Response contains the server's response in text format. To save this response as a JSON-formatted file, you need to write the text attribute of the response to the file. Option C does this correctly by using OutFile.write(Response.text).

Options A and D are incorrect because they attempt to convert the response content to JSON using json.loads() or Response.json(), respectively. However, in this case, the response is already in text format and should be directly written to the file.

Option B is incorrect because it attempts to write the entire response object (Response) to the file, which will not be in valid JSON format.

upvoted 2 times

Dannyboy7 5 months, 2 weeks ago

Answer is C

upvoted 1 times

msstanick 5 months, 3 weeks ago

Ok, I think I got it -> C. Explanation as below.

A wrong:
json.loads() is used to make a python dictionary out of a json string - this is not what we are looking for as we actually should get a json string.

B wrong:
This will provide the http response, not a text string. E.g. <Response [200]> if all good.

C correct:

Since APIs return JSON strings by default we only need to write them into a file.

Script example:

```
url = "http://ip.jsontest.com"
response = requests.get(url=url)
print(response.text," ",type(response.text))
```

Result:
{"ip": "77.112.51.84"}
<class 'str'>

D wrong:
outfile.write(response.json()) changes the type of the data from string to dictionary so we're getting an error: TypeError: write() argument must be str, not dict

upvoted 2 times

dnjJ56 11 months, 2 weeks ago

C Is correct.
Tested all answers.

upvoted 3 times

Huntkey 1 year ago

Should be C. If you just write "response", I believe you will get the "200"

upvoted 2 times

Zikosheka 1 year, 1 month ago

I will go with B

upvoted 2 times

zeta99 1 year, 1 month ago

B is correct.

Response is a variable not a file

upvoted 4 times

Wooker 1 year, 2 months ago

B is correct.

https://stackabuse.com/reading-and-writing-json-to-a-file-in-python/

upvoted 2 times

Wooker 1 year, 2 months ago

sorry, C is correct.

upvoted 2 times

Titini 1 year, 2 months ago

D is correct

upvoted 2 times

ImFran 11 months, 2 weeks ago

This reference is the key https://requests.readthedocs.io/en/latest/user/quickstart/#json-response-content

upvoted 1 times

```
DSW1#sh spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    24596
              Address     0018.7363.4300
              Cost        2
              Port        13 (FastEthernet1/0/11)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID     Priority    28692  (priority 28672 sys-id-ext 20)
              Address     001b.0d8e.e080
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa1/0/7             Desg FWD 2         128.9    P2p
Fa1/0/10            Desg FWD 2         128.12   P2p
Fa1/0/11            Root FWD 2         128.13   P2p
Fa1/0/12            Altn BLK 2         128.14   P2p
```

Refer to the exhibit. What does the output confirm about the switch's spanning tree configuration?

A. The spanning-tree operation mode for this switch is PVST.

B. The spanning-tree operation mode for this switch is PVST+.

C. The spanning-tree mode stp ieee command was entered on this switch.

D. The spanning-tree operation mode for this switch is IEEE.

Correct Answer: *B*

Community vote distribution

B (100%)

rafaelinho88 Highly Voted 9 months, 4 weeks ago

Selected Answer: B

The default spanning-tree mode in Cisco switch is PVST+. This spanning-tree mode is based on the IEEE 802.1D standard and Cisco proprietary extensions. PVST+ is same as standard IEEE 802.1D but it runs on each VLAN. In the output we see the line “Spanning tree enabled protocol ieee” under “VLAN 20” so it can say the switch is running in PVST+ mode.

upvoted 7 times

Ferrantee Highly Voted 1 year, 2 months ago

B - PVST+ enables support to IEEE Devices, "SPanning tree enabled protocol IEEE" output confirms PVST+

upvoted 5 times

landgar Most Recent 10 months, 2 weeks ago

Selected Answer: B

The reason of using PVST+ is that it is applied to VLAN 20. PVST does not exist, and IEEE is the same as STP.

upvoted 2 times

nushadu 11 months, 1 week ago

Selected Answer: B

sw2(config)#
sw2(config)#do s spanning-tree vl 1 summ | i mode
Switch is in pvst mode
sw2(config)#
sw2(config)#
sw2(config)#do s spanning-tree vl 1 det | i ieee

VLAN0001 is executing the ieee compatible Spanning Tree protocol
sw2(config)#do s spanning-tree vl 1 | i ieee
Spanning tree enabled protocol ieee
sw2(config)#
sw2(config)#do s runn | s mode pv
spanning-tree mode pvst
sw2(config)#

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/routers/ncs5xx/ncs520/configuration/guide/LAN-switch/17-1-1/b-lanswitch-17-1-1-ncs520/b-lanswitch-17-1-1-ncs520_chapter_0110.html.xml

upvoted 2 times

DRAG DROP -

Drag and drop the snippets onto the blanks within the code to construct a script that advertises the network prefix 192.168.5.0/24 into a BGP session. Not all options are used.

Select and Place:

Answer Area

```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>
        <ios-bgp:address-family>
          <ios-bgp:no-vrf>
            <ios-bgp:ipv4>
              <ios-bgp:af-name>unicast</ios-bgp:af-name>
              <ios-bgp:ipv4-unicast>
                <ios-bgp:network>
                  <ios-bgp:with-mask>
                    <ios-bgp:number>                    </ios-bgp:number>
                    <ios-bgp:                    >                    </ios-bgp:mask>
                  </ios-bgp:with-mask>
                </ios-bgp:network>
              </ios-bgp:ipv4-unicast>
            </ios-bgp:ipv4>
          </ios-bgp:no-vrf>
        </ios-bgp:address-family>
      </ios-bgp:bgp>
    </router>
  </native>
</config>
```

192.168.5.0 | 255.255.255.0 | with-mask | mask | subnet-mask

Correct Answer:

Answer Area

```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>
        <ios-bgp:address-family>
          <ios-bgp:no-vrf>
            <ios-bgp:ipv4>
              <ios-bgp:af-name>unicast</ios-bgp:af-name>
              <ios-bgp:ipv4-unicast>
                <ios-bgp:network>
                  <ios-bgp:with-mask>
                    <ios-bgp:number>192.168.5.0</ios-bgp:number>
                    <ios-bgp:255.255.255.0>mask</ios-bgp:mask>
                  </ios-bgp:with-mask>
                </ios-bgp:network>
              </ios-bgp:ipv4-unicast>
            </ios-bgp:ipv4>
          </ios-bgp:no-vrf>
        </ios-bgp:address-family>
      </ios-bgp:bgp>
    </router>
  </native>
</config>
```

with-mask | subnet-mask

PALURDIN Highly Voted 1 year, 2 months ago

mask is first and then 255.255.255.0

upvoted 37 times

olaniyijt Highly Voted 7 months, 3 weeks ago

192.168.5.0
Mask
255.255.255.0

upvoted 6 times

Lungful Most Recent 4 months ago

Definitely swap "mask" and "255.255.255.0"

upvoted 1 times

x3rox 10 months ago

MASK > 255.255.255.0

upvoted 1 times

landgar 10 months, 1 week ago

Just look at the closing tags (</...>). PALURDIN is right

upvoted 1 times

xzckk 12 months ago

should be <ios-bgp:mask>255.255.255.0

upvoted 6 times

Based on the router's API output in JSON format below, which Python code will display the value of the `hostname` key?

```
{
   “response”: [{
        “family”: “Switches”,
        “macAddress”: “00:41:41:43:07:00”,
        “hostname”: “SwitchIDF14”,
        “upTime”: “352 days, 6:17:26:10”,
        “lastUpdated”: “2020-07-12 21:15:29”,
   }]
}
```

A. json_data = response,json() print(json_data['response'][0]['hostname'])

B. json_data = json.loads(response.text) print(json_data['response']['family']['hostname'])

C. json_data = json.loads(response.text) print(json_data[response][0][hostname])

D. json_data = response.json() print(json_data['response'][family][hostname'])

Correct Answer: *A*

Community vote distribution

A (100%)

LanreDipeolu 2 months, 4 weeks ago

{
"response":[{
"family": "Switches",
"macAddress": "00:4141:43:07:00",
"hostname": "SwitchIDF14",
"upTime": "352 days, 6:17:26:10",
"lastUpdate": "2020-07-12 21:15:29",
}]
}

print ("the family name is ", json_data['response'][0]['family'])
the family name is Switches
or
print ("the hostname name is ", json_data['response'][0]['hostname'])

the hostname name is SwitchIDF14
A is the answer

upvoted 2 times

msstanick 5 months, 3 weeks ago

Selected Answer: A

It is A indeed. First we need to make a python dict so response.json() and use it for printing.

json_data = {
"response": [{
"family": "Switches",
"macAddress": "ff:ff:ff:ff:ff:ff",
"hostname": "SwitchDF14"
}]
}

print("The hostname is: ",json_data['response'][0]['hostname'])

The hostname is: SwitchDF14

upvoted 1 times

landgar 10 months, 1 week ago

Selected Answer: A

A is right, but with response.json()

upvoted 2 times

Caradum 1 year ago

A must be correct. "response,json()" the comma must be a typo and should be a dot, because all other answer are clearly wrong.

B & D make the same mistake: 'hostname' is not a child element of 'family'.
C has no semicolons in the square brackets.

upvoted 4 times

attiko 1 year ago

Selected Answer: A

A is the correct answer, verified by writing a script on my PC

upvoted 1 times

jhonelo2011 1 year, 1 month ago

Selected Answer: A

It is A, the output was generated from an API get request using "requests" library.
https://www.geeksforgeeks.org/response-json-python-requests/

upvoted 3 times

kebkim 1 year, 1 month ago

I guess B is correct.

upvoted 2 times

Question #440 *Topic 1*

Which function is performed by vSmart in the Cisco SD-WAN architecture'?

A. distribution of IPsec keys

B. execution of localized policies

C. redistribution between OMP and other routing protocols

D. facilitation of NAT detection and traversal

Correct Answer: *B*

Community vote distribution

A (81%) Other

tckoon Highly Voted 1 year, 1 month ago

Selected Answer: A

Authentication: As mentioned, the Cisco SD-WAN control plane contributes the underlying infrastructure for data plane security. In addition, authentication is enforced by two other mechanisms:

In the traditional key exchange model, the Cisco vSmart Controller sends IPsec encryption keys to each edge device

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge-20-x/security-book/security-overview.html

upvoted 11 times

BALAKE Most Recent 2 months, 2 weeks ago

I think the key here is that the localized policies are executed by the switches and not vSMART?

upvoted 1 times

BALAKE 2 months, 2 weeks ago

executed by the SD-WAN device rather...didnt mean to put switches I was thinking catalyst and i am tired...
" Localized control policy is policy that is configured on a Cisco IOS XE Catalyst SD-WAN device"

upvoted 1 times

Soggyt74 3 months, 3 weeks ago

Selected Answer: B

The vSmart component resides in the control plane. vSmart controllers provide routing, enforce data plane policies, and enforce network-wide segmentation. Because policies are created on vManage, vSmart is the component responsible for enforcing these policies centrally.

CCNP Enterprise Design ENSLD 300-420 Official Cert Guide page 352

upvoted 2 times

CKL_SG 4 months, 3 weeks ago

Selected Answer: A

In the traditional key exchange model, the Cisco vSmart Controller sends IPsec encryption keys to each edge device.

upvoted 1 times

msstanick 5 months, 3 weeks ago

Selected Answer: A

Looks like A per 31 days before CCNP book: "The vSmart controller acts as a distribution point to establish data plane connectivity between the WAN Edge routers. This information exchange includes service LAN-side reachability, transport WAN-side IP addressing, IPsec encryption keys, site identifiers, and so on. Together with WAN Edge routers, vSmart controllers act as a distribution system for the pertinent information required to establish data plane connectivity directly between the WAN Edge routers."

upvoted 1 times

net_eng10021 6 months ago

Selected Answer: D

Looks like B may be incorrect.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/localized-policy.html

Localized Control Policy
Control policy operates on the control plane traffic in the Cisco IOS XE SD-WAN overlay network, influencing the determination of routing paths through the overlay network. Localized control policy is policy that is configured on a Cisco IOS XE SD-WAN device (hence, it is local) and affects BGP and OSPF routing decisions on the site-local network that the device is part of.

To configure localized policies, use the Cisco vManage policy configuration wizard.

upvoted 1 times

mrtattoo 6 months, 4 weeks ago

Selected Answer: B

ChatGPT gave the following answer (i also provided the links below) and all your points:

After reviewing the additional link provided, my answer remains the same. The vSmart controller is primarily responsible for executing centralized policies in the Cisco SD-WAN architecture, which include policies related to traffic, security, and other aspects of network management.

The document provides further detail on the role of vSmart in the SD-WAN architecture, stating that "vSmart controllers provide centralized policy management, act as the decision engine for traffic forwarding, and manage encryption keys for IPsec tunnels." This confirms that while vSmart may be involved in the management of encryption keys, its primary function is still the execution of centralized policies.

Therefore, my final answer is still B. Execution of centralized policies.

upvoted 1 times

jackr76 6 months, 3 weeks ago

chatgpt must have missed the bottom of this page: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/policy-overview.html#id_113339

And "In the traditional key exchange model, the Cisco vSmart Controller sends IPsec encryption keys to each edge device." in https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge-20-x/security-book/security-overview.html

For me it is A

upvoted 1 times

danman32 4 months ago

ChatGPT did mention vSmart is involved in management of encryption keys, but felt that the primary function of vSmart is execution of centralized policies.
But execution of CENTRALIZED policies, not LOCAL policies which is what answer B has.
So answer does seem to be A.

upvoted 1 times

Soggyt74 3 months, 3 weeks ago

ChatGPT was right

upvoted 1 times

markymark874 10 months, 4 weeks ago

Selected Answer: A

A is correct verified from the link provided by tckoon

upvoted 1 times

iGlitch 1 year ago

Selected Answer: A

It can't be B, because "Localized policies" are those policies that are applied locally on the vEdge routers.
A is the best answer.

upvoted 1 times

loannis34 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

greencafe24 1 year, 2 months ago

Selected Answer: A

A is the correct answer.

upvoted 1 times

Jason233 1 year, 2 months ago

In the traditional key exchange model, the vSmarts sends IPsec encryption keys to each edge device.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book.pdf - page 15

upvoted 3 times

Deu_Inder 1 year, 2 months ago

I would go by A, although I dont have a reliable link for that.

upvoted 1 times

```
Cat3650# show logging
[ ... cut ... ]
*Sep 11 19:06:25.595: %PM-4-ERR_DISABLE: channel-misconfig error detected on Po1, putting Gi1/0/2
in err-disable state
*Sep 11 19:06:25.606: %PM-4-ERR_DISABLE: channel-misconfig error detected on Po1, putting Gi1/0/3
in err-disable state
*Sep 11 19:06:25.622: %PM-4-ERR_DISABLE: channel-misconfig error detected on Po1, putting Po1 in
err-disable state

Cat3650# show etherchannel summary
[ ... cut ... ]
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------
1      Po1(SD)           -         Gi1/0/2(D)   Gi1/0/3(D)

Cat3650# show interface status err-disabled
Port      Name      Status        Reason            Err-disabled Vlans

Gi1/0/2             err-disabled  channel-misconfig
Gi1/0/3             err-disabled  channel-misconfig
Po1                 err-disabled  channel-misconfig
```

Refer to the exhibit. The administrator troubleshoots an EtherChannel that keeps moving to err-disabled. Which two actions must be taken to resolve the issue?
(Choose two.)

A. Ensure that the corresponding port channel interface on the neighbor switch is named Port-channel1.

B. Ensure that the switchport parameters of Port-channel1 match the parameters of the port channel on the neighbor switch.

C. Ensure that interfaces Gi1/0/2 and Gi1/0/3 connect to the same neighboring switch.

D. Reload the switch to force EtherChannel renegotiation.

E. Ensure that the neighbor interfaces of Gi1/0/2 and Gi1/0/3 are configured as members of the same EtherChannel.

Correct Answer: *BE*

Community vote distribution

BE (51%) BC (49%)

VergilP Highly Voted 1 year, 1 month ago

Selected Answer: BC

It's doesn't matter what port the neighbor switch use，neighbor switch can use 1/0/47 and 1/0/48 to bind in Po1 is OK，in the picture i don't see any neighbor switch config
I'm going for B/C

upvoted 10 times

GeorgeFortiGate Highly Voted 1 year ago

Selected Answer: BC

We can decide with exclude method:
A = Wrong answer Group number is local to each switch
B = Correct answer because we should make sure that parameters are correct
C = Correct answer We also need to make sure that our interfaces trace to the same switch
D = Wrong answer No way to reboot the switch and solve the issue.
E = Wrong answer We do not care which interfaces we have on the neighboring device so C is not correct in my opinion.

upvoted 6 times

adamzet33 Most Recent 3 weeks, 2 days ago

Selected Answer: BE

E is about having no matter which ports on remote device but in same Po

upvoted 1 times

blueblue2 2 months, 2 weeks ago

Selected Answer: BE

The err-disable status indicates tha the port was automatically disabled by the switch operating system software because of an error condition encountered on the port.

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

I have labbed this in CML. The answer is indeed E. I receive the same exact errors when i put two of the neighbor interfaces in different port-channel group, either 1/2 and 1/no-group

upvoted 1 times

Mephystopheles 3 months, 2 weeks ago

Selected Answer: BE

B and E.
Keep in mind that c3650 switches are stackable switches, so you could easily have 6 switch members stacked and having the port-channel interfaces going to any of those switches.
Option C is definitely not an issue in this scenario.

upvoted 2 times

Lungful 4 months ago

Selected Answer: BE

"Ensure that the neighbor interfaces of Gi1/0/2 and Gi1/0/3" I think refers to the whatever interfaces are on the other side of the etherchannel from Gi1/0/2 and Gi1/0/3. B and E are correct to me.

upvoted 1 times

[Removed] 5 months, 1 week ago

Selected Answer: BE

Here is what we know:
1)Interfaces on local switch are g1/0/2 and g1/0/3, and are bundled into port-channel 1
2) They are in err-disabled

Now, we have no information on the neighbor switch, and we need to deduce the correct answer based on the options available and the given information.
A) Port-channels do not require matching port-channel id on the neighbor device, so this is wrong
B) Port-channel parameters do need to be compatible, meaning, we need to have compatible protocols and modes on both sides of the port-channel, e.i. PAGP = auto/desirable, LACP= active/passive, static=ON
C) This isn't entirely necessary, as you could have a StackWise setup of switches, in this case you can connect to different switches, same goes for vPC or VSS architecture
D) No.
E) We do need to ensure that the neighboring switch has their interfaces in the port-channel connecting to the local switch

From this we can confidently conclude that B and E are the right answers.
The only reason C isn't correct is because we do not know where it is only connecting to one switch or if its using StackWise/VSS/vPC

upvoted 1 times

Chiaretta 7 months, 1 week ago

Selected Answer: BE

I think B and E are the correct answer.
The C seems correct but the only case you can connect an etherchannel in different phisical equipments is that the equipments are StackWise o VSS connected.

upvoted 1 times

byallmeans 6 months, 3 weeks ago

The problem with E is we don't know whether neighboring switch uses ports Gi1/0/2 and Gi1/0/3. We only have this information of the local switch. Which makes E answer as bad as C.

upvoted 1 times

mhizha 6 months, 2 weeks ago

"... neighbor interface of Gi1/0/2 and Gi1/0/3... " does not refer to Gi1/0/2 and Gi1/0/3 on the other switch. This can be any port numbers.

upvoted 4 times

rami_mma 8 months, 1 week ago

Selected Answer: BE

I would choose B and E.

upvoted 1 times

snarkymark 9 months, 2 weeks ago

Its another terrible question. If you go but what is shown on the screen the output is a CAT3650, not a Nexus. BUT, 3650s are stackable too, also allowing the etherchannel to connect to different switches. So also going with BE.

upvoted 3 times

eff3 10 months ago

Selected Answer: BE

same neighboring switch is not a requirement (e.g.: ACI Leaf with vPC)
BE is correct

upvoted 1 times

tonytam1991 9 months, 1 week ago

The switch is 3650 you idiot

upvoted 2 times

markymark874 10 months, 4 weeks ago

Selected Answer: BE

Err disable state is due to misconfig of etherchannels or ports on both switches.
https://community.cisco.com/t5/networking-knowledge-base/port-status-is-errdisable-due-to-etherchannel-misconfiguration/ta-p/3131226#:~:text=The%20errdisable%20status%20indicates%20that,issue%20the%20show%20port%20command.

upvoted 3 times

Bambju 11 months, 1 week ago

Selected Answer: BE

The errdisable status indicates that the port was automatically disabled by the switch operating system software because of an error condition encountered on the port.

Check the EtherChannel configuration on both switches. If one side is configured for EtherChannel in the On mode, the peer ports must also be in On mode or they will go to errdisable.

upvoted 2 times

bora4motion 1 year ago

Selected Answer: BE

It's a difficult one: C seems legit but you can have ether channel to two Nexus boxes (or Cat9500, or two members of the same stack) and there you go C out the window.
I'm going with BE.

upvoted 1 times

PeterTheCheater 1 year ago

Selected Answer: BE

BE are correct

upvoted 1 times

Tacolicious 1 year ago

Selected Answer: BC

I think that, if they're not giving the explicit information, we'd have to asume there are no special conditions here, like VSS/VPC. Otherwise you can start nitpicking about pretty much half the questions in the exam.

That being said. Most people agree that it's not A or D. The reasoning why i'll choose BC is because E just doesnt make sense to me. It doesn't matter which interfaces are connected on the other switch, they don't have to match. And neither does the port-channel number, that's locally significant. So i'd rather believe we're dealing with a regular switch-2-switch port-channel in this question, than to rule out an answer that is actually correct in many circumstances.

upvoted 2 times

bora4motion 11 months, 2 weeks ago

You can have etherchannel configured to two different switches which are members of a stack, or to two Nexus switches - this makes C an incorrect answer.

upvoted 2 times

PeterTheCheater 1 year ago

E says that make sure the interfaces on the remote switches connected to G2 and G3 on local switch belong to the same etherchannel. I think E is the right one.

upvoted 2 times

danman32 4 months ago

Good eye! We've been all assuming reference of G2 and G3 were meaning the interface names of the remote switch, but really it is saying the remote interfaces (whatever they are designated as) connected to THIS switch's G2/G3
I wasn't sure if you would get an err-disabled if as in C, G2/G3 were connected to two different remote switches that were not a stack or VSS

upvoted 1 times

Question #442 *Topic 1*

```
Device# configure terminal
Device(config)# netconf ssh acl 1
Device(config)# netconf lock-time 100
Device(config)# netconf max-sessions 1
Device(config)# netconf max-message 10
```

Refer to the exhibit. A network engineer must configure NETCONF. After creating the configuration, the engineer gets output from the command show line, but not from show running-config. Which command completes the configuration?

A. Device(config)# netconf max-sessions 100

B. Device(config)# no netconf ssh acl 1

C. Device(config)# netconf lock-time 500

D. Device(config)# netconf max-message 1000

Correct Answer: *B*

Community vote distribution

D (100%)

FrameRelay Highly Voted 1 year, 1 month ago

is this Q in the exam, I'm not sure why I bought the book, this level of NETCONF is not covered.

upvoted 17 times

Feliphus 11 months, 4 weeks ago

Only our collaboration work as testers help us reading and contributing in the discussion.
I totally agree, there is no sense, Cisco wants you to pay the (very) expensive specialized course and forget the OCG books. But they can't say it blatantly
It must be that they don't earn enough money, it's shameful

upvoted 17 times

Badger_27 8 months, 4 weeks ago

Yeah its completely absurd.

upvoted 8 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago

Cisco probably puts this question in the exam even though it's not covered by OCG because they want to know if people are brain dumping it and answering it. It's entirely plausible. These questions are BS and should never dictate anyone becoming a successful Network Engineer as a career.

upvoted 1 times

CCNPWILL 1 month, 2 weeks ago

Possibly, but some people do have work experience or work on a daily with such protocols and could genuinely know the answer. or we could just " get lucky " and answer it correctly :D

upvoted 1 times

Cynthia2023 3 months, 3 weeks ago

- `max-sessions`: The valid range is 4 to 16 sessions.
- `lock-time`: The valid range is 1 to 300 seconds.
- `max-message`: The valid range is 1 to 2147483. The default value is infinite, meaning there is no limit imposed by default on the size of messages.

These are the valid ranges for these parameters in the context of NETCONF configuration on Cisco devices.

If you issue the command `netconf max-sessions 1`, the device will recognize this as an invalid command and will not apply it. As a result, the device will maintain the default value for the maximum number of concurrent NETCONF sessions, which is typically 4.

upvoted 1 times

Cynthia2023 3 months, 3 weeks ago

The size of a general configuration file can vary widely depending on the complexity of the configuration, the number of devices being configured, and the specific commands used. Configuration files can range from a few kilobytes (KB) to several megabytes (MB) in size. It's important to note that some network devices or platforms might have limitations on the maximum size of configuration files they can handle.

Device(config)# netconf max-message 1000

This command increases the maximum NETCONF message size to 1000 kilobytes, which is a common practice to ensure that larger messages can be exchanged as needed.

upvoted 1 times

danman32 4 months ago

The scenario is that output is available for 'show line' but not for 'show run'. So what's different about these two scenarios and which answer addresses that?
Difference is the size of the message and only answer D addresses that.

I thought perhaps answer B, remove ssh acl 1 as perhaps the ACL is wrong, but then you wouldn't get an output for 'show line' as well as 'show run'

upvoted 1 times

Dannyboy7 5 months, 2 weeks ago

D is correct

upvoted 1 times

Anas_Ahmad 11 months, 2 weeks ago

Selected Answer: D

Device(config)# netconf max-message 1000 is the right answer

upvoted 2 times

luctieuphung 12 months ago

D is correct. Command: netconf max-message <1-2147483> Kbytes. The engineer gets output from the command show line, but not from show running-config, because max-message is too small, it is not enough for data of running-config.

upvoted 4 times

dogdoglee 12 months ago

Selected Answer: D

A : The valid range is 4 to 16 (X
B : Disable netconf over sshv2 (X
C : The valid range is 1 to 300 (X
D : The valid range is 1 to 2147483. The default value is infinite. (O

upvoted 3 times

Tacolicious 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

Summo 1 year, 1 month ago

NETCONF over SSHv2 requires that a vty line be available for each NETCONF session as specified in the netconf max-sessioncommand

upvoted 1 times

RREVECO 1 year, 2 months ago

Selected Answer: D

I think "D" is correct
ref https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cns/configuration/xe-16-9/cns-xe-16-9-book/netconf-sshv2.html

A) netconf max-sessions 100 "value out of range" (range 4-16 default is 4)
B) y C) the question does not refer to access to the equipment)

D) Specifies the maximum size, in kilobytes (KB), for the messages received in a NETCONF session. (makes sense relative to the size of a show running-config)

upvoted 4 times

uzbin 1 year, 2 months ago

D - looks to be the best answer. max-message is the size in KB of Netconf messages / response. 10KB too small for whol config..?

upvoted 3 times

Deu_Inder 1 year, 2 months ago

A: 'netconf max-sessions 100' is not valid on C7200-ADVENTERPRISEK9-M version 15.2(4)M7. Tested in GNS3.
C: 'netconf lock-time 500' is not valid on C7200-ADVENTERPRISEK9-M version 15.2(4)M7. Tested in GNS3.
D: 'netconf max-message 1000' is valid. Do not yet understand how this would help.

Would be great if someone can give a hand here.

upvoted 3 times

wendolin 1 year, 2 months ago

sorry A should be changed, but no valid answer is supplied

upvoted 1 times

wendolin 1 year, 2 months ago

Step 5
netconf max-sessions session =>
(Optional)Specifies the maximum number of concurrent NETCONF
sessions allowed.

Example:
Device(config)# netconf max-sessions 5

• The valid range is 4 to 16. The default value is 4.

===> C

upvoted 1 times

Question #443 *Topic 1*

Which protocol is implemented to establish secure control plane adjacencies between Cisco SD-WAN nodes?

A. IKE

B. TLS

C. IPsec

D. ESP

Correct Answer: *B*

Community vote distribution

B (67%) C (33%)

Ferrantee Highly Voted 1 year, 2 months ago

"The WAN Edge routers form a permanent Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) control connection to the vSmart controllers and connect to both of the vSmart controllers over each transport"
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html
upvoted 11 times

PureInertiaCopy 3 months, 2 weeks ago

Looks like it is B...

The WAN Edge routers securely communicate to other WAN Edge routers using IPsec tunnels over each transport. The Bidirectional Forwarding Detection (BFD) protocol is enabled by default and runs over each of these tunnels, detecting loss, latency, jitter, and path failures.
upvoted 1 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Selected Answer: B

Yes TLS. TLS between edge and vsmart.
IPSEC terminology is used when referring to BFD, which is the data plane.
upvoted 1 times

Lungful 4 months ago

Selected Answer: B

Voting. See my other posts.
upvoted 1 times

Lungful 4 months ago

On one hand, I see this "Key management: Edge routers generate symmetric keys that are used for secure communication with other edge routers, using the standard IPsec protocol."
reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html

But then I see that it only references the Data Plane with IPsec when the question is asking about the control plane. I am unsure.

TLS is definitely between the controllers and edge nodes but is that what the question is asking about?
upvoted 1 times

Lungful 4 months ago

Also https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html has a diagram showing which protocols are used where.
upvoted 1 times

Lungful 4 months ago

After reading more into the link above, I am going with TLS as the answer as this is asking about the Control plane specifically. "The Cisco SD-WAN control plane has been designed with network and device security in mind. The foundation of the control plane is one of two security protocols derived from SSL (Secure Sockets Layer)—the Datagram Transport Layer Security (DTLS) protocol and the Transport Layer Security (TLS) protocol."
upvoted 1 times

NLFluke 4 months, 1 week ago

Selected Answer: B

Given answer is correct.
upvoted 1 times

Bingchengchen236 4 months, 2 weeks ago

Selected Answer: C

should choose C, in Official Cert Guide, page 634, it is written "SD-WAN router automatically establishes a secure Datagram Transport Layer Security (DTLS) connection with the vSmart controller and forms an OMP neighborship over the tunnel to exchange routing information. It also

establishes standard IPsec sessions with other SD-WAN routers in the fabric. "
the question is asking about the connection between SD-WAN routers

upvoted 3 times

danman32 4 months ago

But isn't the IPSec connection between routers for the data plane? Question asks about control plane.

upvoted 1 times

msstanick 5 months, 3 weeks ago

Selected Answer: B

B is correct per 31 days befpre CCNP book: "The WAN Edge routers form a permanent Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) control connection to the vSmart controllers and connect to both of the vSmart controllers over each transport (mpls and biz-internet)."

upvoted 2 times

carlovalle 7 months, 3 weeks ago

IPSec is between edges and DTLS or TLS is between edges and controllers

upvoted 4 times

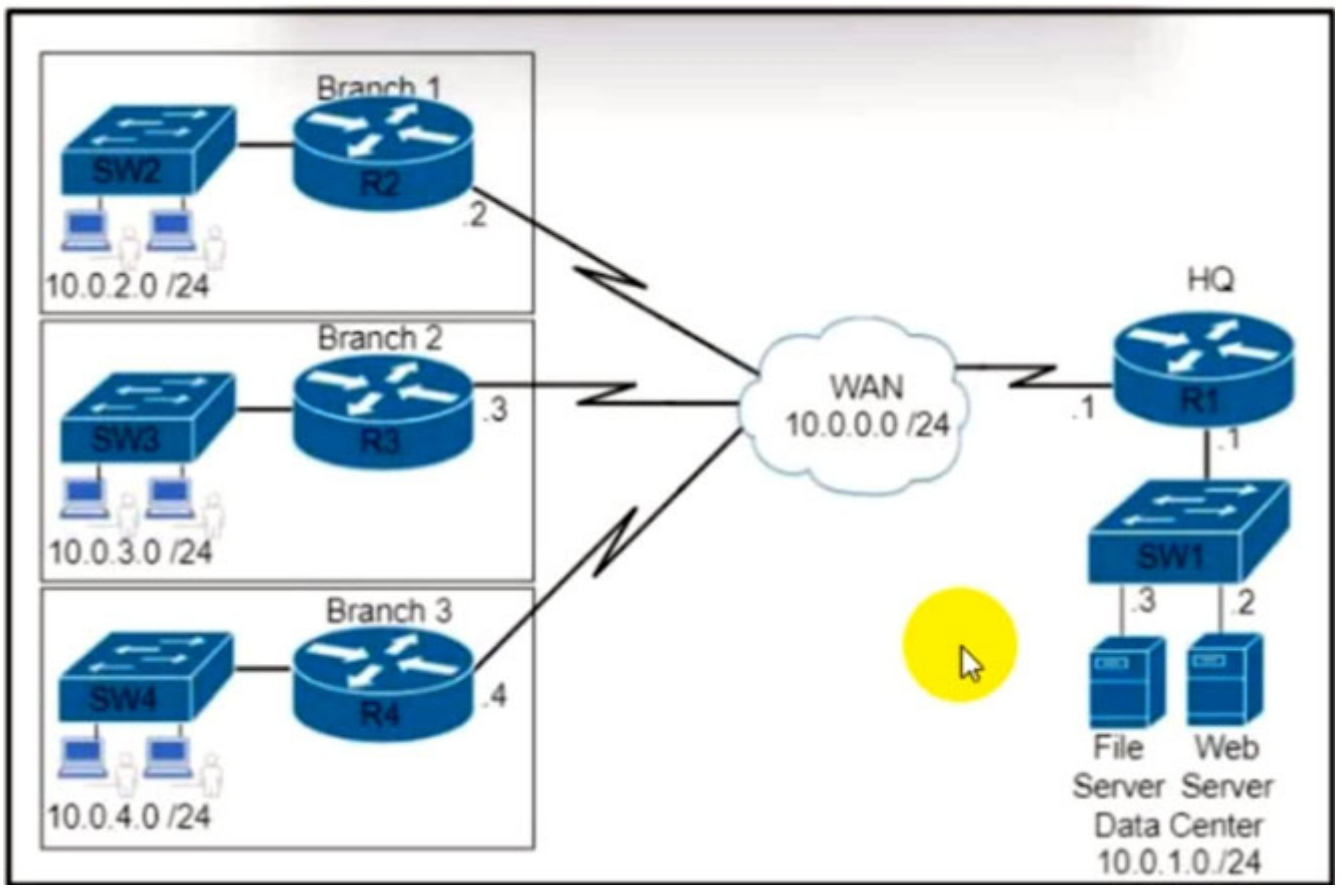
pmmg 9 months, 2 weeks ago

Selected Answer: B

Given answer is correct.

upvoted 1 times

Question #444 *Topic 1*



Refer to the exhibit. Which command set is needed to configure and verify router R3 to measure the response time from router R3 to the file server located in the data center?

A.

```
ip sla 6
 icmp-echo 172.29.139.134 source-ip 172.29.139.132
 frequency 300
ip sla schedule 6  start-time now

show ip sla statistics 6
```

B.

```
ip sla 6
 icmp-echo 10.0.1.3 source-ip 10.0.0.3
 frequency 300
ip sla schedule 6 life forever start-time now

show ip sla statistics 6
```

C.

```
ip sla 6
 icmp-echo 172.29.139.134 source-ip 172.29.139.132
 frequency 300
ip sla schedule 6  start-time now

show ip protocol
```

D.

```
ip sla 6
 icmp-echo 10.0.1.3 source-ip 10.0.0.3
 frequency 300
ip sla schedule 6 life forever start-time now

show ip protocol
```

Correct Answer: *B*

danman32 4 months ago

Surprisingly Cisco easily has you throw out two answers
There's nothing here about 172.29.139.x, not even the WAN.
Unless there is a typo in the exhibit.

upvoted 2 times

nushadu 11 months, 1 week ago

B.
cisco_R3(config)#do s runn | s ip sla
track 1 ip sla 1

ip sla 6
icmp-echo 2.2.2.2 source-ip 3.3.3.3
frequency 3000
ip sla schedule 6 life forever start-time now

cisco_R3(config)#do s ip sla stat 6
IPSLAs Latest Operation Statistics

IPSLA operation id: 6
Latest RTT: 3 milliseconds
Latest operation start time: 12:57:15 UTC Thu Dec 22 2022
Latest operation return code: OK
Number of successes: 1
Number of failures: 0
Operation time to live: Forever

cisco_R3(config)#do s ip sla summ
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID Type Destination Stats Return Last
(ms) Code Run
---
*6 icmp-echo 2.2.2.2 RTT=3 OK 55 seconds ag
o
cisco_R3(config)#

upvoted 4 times

forccnp 11 months, 3 weeks ago

wrong answers

upvoted 1 times

bora4motion 1 year ago

B though not complete.

upvoted 1 times

GeorgeFortiGate 1 year ago

I think something is wrong with the question and the answers.

Besides that i think answer is B BUT the "ip sla schedule 6 life forever start-time now" ---- > "ip sla schedule 6 start-time now life forever"

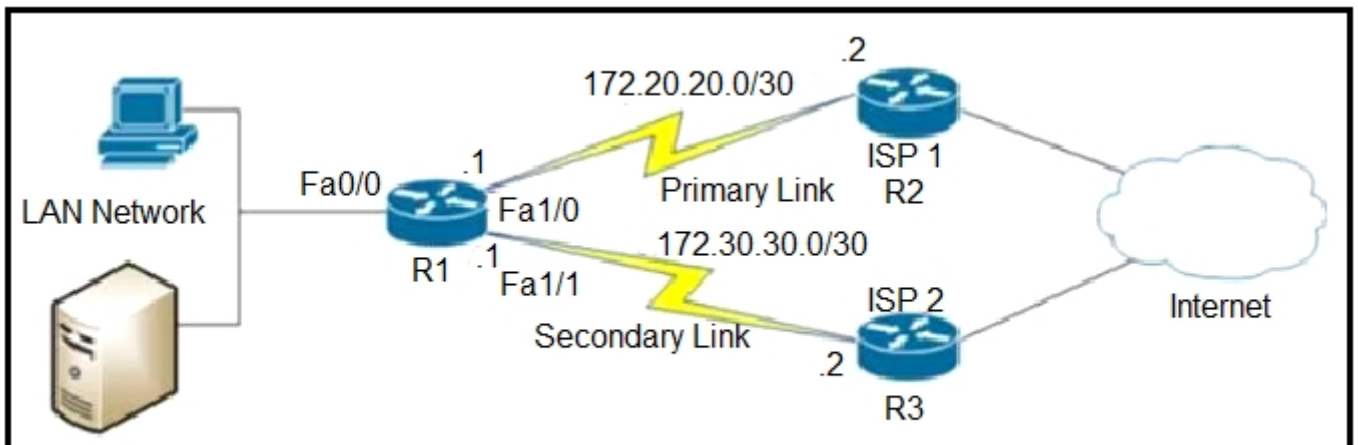
upvoted 1 times

Xerath 11 months, 2 weeks ago

It doesn't matter if you start with: "life forever", or "start-time now", the command will work in both scenarios, verified using gns3.

upvoted 5 times

Question #445 *Topic 1*




```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 172.20.20.2 source-interface FastEthernet0/0
R1(config-ip-sla-echo)#timeout 5000
R1(config-ip-sla-echo)#frequency 10
R1(config-ip-sla-echo)#threshold 500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track 10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10
R1(config)#no ip route 0.0.0.0 0.0.0.0 172.20.20.2
R1(config)#ip route 0.0.0.0 0.0.0.0 172.30.30.2 5
```

Refer to the exhibit. What are two reasons for IP SLA tracking failure? (Choose two.)

A. The threshold value is wrong.

B. The destination must be 172.30.30.2 for icmp-echo.

C. The default route has the wrong next hop IP address.

D. A route back to the R1 LAN network is missing in R2.

E. The source-interface is configured incorrectly.

Correct Answer: *AD*

Community vote distribution

DE (63%) AE (16%) 11% 5%

net_eng10021 Highly Voted 5 months, 3 weeks ago

Another awful question. However, it's realistic. It's realistic because poor communications skills are so common in this field.

upvoted 7 times

NLFluke Most Recent 4 months, 1 week ago

Selected Answer: DE

Since its using Source-interface Fa0/0 we can assume the R2 will not have a route back to it, to solve the issue, adjust the source-interface to Fa1/0.

upvoted 2 times

Dv123456 4 months, 1 week ago

It's CE, if you delete the default route to 172.20.20.2 obviously the tracking doesn't work, and the source interface is clearly wrong.

upvoted 2 times

alex711 4 months, 2 weeks ago

Selected Answer: CE

It is CE

upvoted 2 times

olaniyijt 7 months, 3 weeks ago

I'll say D and E

A. The threshold value is wrong
- Not wrong. Works on routers.

B. The destination must be 172.30.30.2 for icmp-echo.
- It could be either of the two ISP's

C. The default route has the wrong next hop IP address.
- The command "no ip route 0.0.0.0 0.0.0.0 172.20.20.2" will not remove "ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10" if it exists on the router. And if it does not exist, it will throw this error: "%No matching route to delete"

D. A route back to the R1 LAN network is missing in R2.
- R1 LAN is the source interface. Ideally, the IP SLA source-interface should be the interface facing the ISP (except in cases of BGP redistribution).

E. The source-interface is configured incorrectly.
- Now this means almost the same thing as option D, but since we've been asked to choose two options, we are forced to choose it too.

upvoted 2 times

HungarianDish 8 months ago

I labbed this up in CML. Only E) is correct. No second matching answer yet.

A. The threshold value is wrong.
=> Threshold is correct, I tested it + see my previous post below. (frequency seconds) > (timeout milliseconds) > (threshold milliseconds)

B. The destination must be 172.30.30.2 for icmp-echo.
=> "icmp-echo 172.20.20.2" is correct, no changes required.

C. The default route has the wrong next hop IP address.
=> If you have a default route, and also the same default route with tracking, then you can delete the normal default route ("ip route 0.0.0.0 0.0.0.0 172.20.20.2"), and the other default route with tracking won't be affected ("ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10"). It remains in the configuration. So, the default route configuration looks good.

D. A route back to the R1 LAN network is missing in R2
=> It is not necessary to have reachibility from R2 to R1's LAN for IP SLA and tracking to work. IP SLA + track works fine without this, it won't cause a failure.

E. The source-interface is configured incorrectly.
=> It is true. Based on the picture it should be "icmp-echo 172.20.20.2 source-interface fa1/0".

upvoted 2 times

dragonwise 8 months ago

Actually D and E are contradicting each other
One of them should be present

upvoted 1 times

rami_mma 8 months, 1 week ago

Selected Answer: DE

D and E is correct

upvoted 1 times

Nickplayany 8 months, 1 week ago

Selected Answer: DE

Guys it´s D and E

Just check the SAME question here Question #253 <- Get the answer

upvoted 1 times

danman32 4 months ago

Actually Q253 is different but you can gather some information from it.
A. Threshold is OK since it was OK in Q253 so not one of the two answers
B. Destination should not be 172.30.30.2 for icmp-echo so not one of the 2 answers
C. Both default routes are OK (the No removes any previous untracked default route through 172.20.20.2 so not one of the two answers
Clearly E is an answer, should not be using LAN IP as SLA source (this was a possible answer in Q253 but the SLA source interface there was Fa1/0 so wasn't the answer there)
But if you are using LAN IP as SLA source, and R2 needs a route back to it and likely does not and D is the only answer we have left to correctly choose.

upvoted 1 times

HungarianDish 10 months ago

Threshold is OK.

(frequency seconds) > (timeout milliseconds) > (threshold milliseconds)

(frequency 10 seconds = 10000ms) > (timeout 5000ms) > (threshold 500ms)

https://notes.networklessons.com/ip-sla-parameters

upvoted 3 times

gordon888 10 months ago

Selected Answer: AE

A and E
D. I don't think so. The ISP is propably not interested in my LAN IP-Range, especially when it is private range. So with E (another source interface) it is not necessary to go for D

upvoted 1 times

gordon888 10 months ago

Correction: LAB test threshold=500ms, SLA works normally. Answer: DE ok

upvoted 1 times

landgar 10 months, 1 week ago

Selected Answer: DE

Fa0/0 is probably hidden for R2, so also R2 won´t have routing to reach it.

upvoted 2 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: AE

A and E
D. I don't think so. The ISP is propably not interested in my LAN IP-Range, especially when it is private range. So with E (another source interface) it is not necessary to go for D.

upvoted 2 times

markymark874 10 months, 4 weeks ago

Selected Answer: AD

A- reason why the ipsla fails bec the threshold received is higher than what is set.
D- since the source is r1 fa0/0, R2 needs to have a return route to r1 fa0/0.
E- source interface either can be fa0/0 or fa0/1. It can both reach destination since R1 is directly connected to the R2 there will be a route to it.
So answer is AD causing the ipsla to get a fail results

upvoted 1 times

Asymptote 10 months, 4 weeks ago

Selected Answer: E

172.20.20.2 is the IP belong to ISP1,
R1 Fa1/0 IP is 172.20.20.1
the SLA source is configured the wrong source IP.

upvoted 1 times

Asymptote 10 months, 4 weeks ago

Sorry this is a wrong answer as i was really tired after long hour study this morning.

The correct answer should be DE.
Router R2 shouldnt know any networks behind the router R1.

upvoted 1 times

iGlitch 1 year ago

Selected Answer: DE

Tricky but I tested A, B, and C and concluded that all were invalid scenarios.
I've tried D and it's correct. E is intentionally vague but it's the only left choice.

upvoted 3 times

FrameRelay 1 year, 1 month ago

E is certainly a correct option because the interface configured in the IP SLA must be the outgoing interface. However looking for a second option, there really should be an answer that says, route to R2 is missing, because with the no ip route 0.0.0.0 0.0.0.0 .... we deleted the only way R1 knew about the route to R2. however when I look at the options, I disagree with D because in this instance there is no way to validate R2 can't find the route to R1 but its actually R1 that hasn't got the route to R2.....

upvoted 3 times

Darude 1 year, 1 month ago

There is no need to configure outgoing interface you can source the echo from any interface you want so E= wrong answer (advanced ping use the same concept) so if the R2 has no route to the LAN interface of R1 it won't work D=correct, in the output we see that they deleted the working
default route (even if on some ios wont work as presented by Deu_Inder BUT THEY DID!)
it leaves C the second correct answer.

upvoted 1 times

danman32 4 months ago

Actually you do need to specify the source IP/interface when using SLA/track to control default route to redundant WAN connections. If link to ISP 1 goes down but not ISP 1 itself, 172.20.20.2 might still be reachable from route through ISP3 so SLA begins succeeding, tracked route is restored, SLA fails and resorts to route to ISP3, and so on, SLA flapping.

upvoted 1 times

```
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
 record v4_r1
 exit
!
sampler SAMPLER-1
 mode random 1 out-of 2
 exit
!
ip cef
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
```

Refer to the exhibit. Which command set must be added to the configuration to analyze 50 packets out of every 100?

A. sampler SAMPLER-1 mode random 1-out-of 2 flow FLOW-MONITOR-1 interface GigabitEthernet 0/0/0 ip flow monitor SAMPLER-1 input

B. flow monitor FLOW-MONITOR-1 record v4_r1 sampler SAMPLER-1 interface GigabitEthernet 0/0/0 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input

C. sampler SAMPLER-1 no mode random 1-out-of 2 mode percent 50 interface GigabitEthernet 0/0/0 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input

D. interface GigabitEthernet 0/0/0 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input

Correct Answer: *B*

Community vote distribution

D (100%)

ihateciscoreally 3 months, 1 week ago

configuration of sampler was only thing not covered in OCG.

upvoted 2 times

danman32 4 months, 1 week ago

What doesn't help analyzing the answers is not having the indentations/config mode for each statement.
B and D are similar, with Bappearing you're retyping what's already there.
But I think B was saying to put the sampler definition within the monitor definition and that's wrong.

upvoted 1 times

snarkymark 9 months, 2 weeks ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/xe-3se/3850/use-fnflow-redce-cpu.html

upvoted 1 times

dnjJ56 11 months, 1 week ago

Selected Answer: D

Just need to apply the flow monitor and the sampler to the interface.
Sampler already capturing 50 out of 100 (1 out of 2)

upvoted 4 times

iGlitch 1 year ago

Selected Answer: D

Everything is complete and configured correctly, we just have to apply it on an interface.
The answer is D.

upvoted 2 times

kebkim 1 year, 2 months ago

Dis correct.
Example:
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input

upvoted 3 times

greencafe24 1 year, 2 months ago

Selected Answer: D

D is correct

upvoted 1 times

Deu_Inder 1 year, 2 months ago

Selected Answer: D

Answer D is correct.
Analysing 1-out-of 2 is analysing 50 percent.

upvoted 4 times

Mbonz 1 year, 2 months ago

Correct answer is c

upvoted 1 times

jj970us 1 year, 2 months ago

Selected Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/xe-3se/3850/use-fnflow-redce-cpu.html

upvoted 3 times

Question #447 *Topic 1*

Why would an engineer use YANG?

A. to transport data between a controller and a network device

B. to model data for NETCONF

C. to access data using SNMP

D. to translate JSON into an equivalent XML syntax

Correct Answer: *B*

Community vote distribution

B (100%)

eddgg 4 months ago

Selected Answer: B

this is a correct answer

upvoted 1 times

eddgg 4 months ago

correct answer

upvoted 1 times

snarkymark 9 months, 2 weeks ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/16-3/configuration_guide/b_163_consolidated_3650_cg/b_163_consolidated_3650_cg_chapter_010011011.pdf

upvoted 1 times

kebkim 1 year, 2 months ago

NETCONF is a standard based and Extensible Markup Language (XML) encoded protocol that provides the transport to communicate the YANG formatted configuration or operational data request from an application that runs on a centralized management platform (for example a laptop) to the Cisco device that a user wishes to configure or request operational (show command) data from.

upvoted 2 times

Question #448 *Topic 1*

A network monitoring system uses SNMP polling to record the statistics of router interfaces. The SNMP queries work as expected until an engineer installs a new interface and reloads the router. After this action, all SNMP queries for the router fail. What is the cause of this issue?

A. The SNMP interface index changed after reboot.

B. The SNMP server traps are disabled for the link state.

C. The SNMP server traps are disabled for the interface index.

D. The SNMP community is configured incorrectly.

Correct Answer: *A*

Community vote distribution

A (100%)

jhonmeikel 4 months ago

In Cisco IOS, there is a command snmp-server ifindex persist, which tells IOS to keep ifindex value unchanged even after reboot

upvoted 1 times

danman32 4 months ago

Question scenario says SNMP polling is being used so that eliminates answers B and C that reference SNMP traps. Traps are a push, polling is a pull.

upvoted 2 times

danman32 4 months ago

I would have loved to say configuration wasn't saved after the SNMP was configured, that's why after reboot SNMP didn't work.

But barring that, only thing that would change after an interface is added is SNMP interface indexes.

upvoted 1 times

jzzmth 11 months ago

Cisco is probably looking for answer A, but wouldn't D also be a possibility if the start-up config contained a wrong community string?

upvoted 3 times

danman32 4 months ago

I think you can assume the running-config and startup-config are the same, other than the interface change that was mentioned in the question.

upvoted 1 times

nushadu 11 months, 1 week ago

Selected Answer: A

https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/ifindx.html

upvoted 4 times

kebkim 1 year, 2 months ago

SNMP interface index :
One of the most commonly used identifiers in SNMP-based network management applications is the Interface Index (ifIndex) value. IfIndex is a unique identifying number associated with a physical or logical interface. For most software, the ifIndex is the name of the interface.

upvoted 1 times

Question #449 *Topic 1*

Which character formatting is required for DHCP Option 43 to function with current AP models?

A. MD5

B. Base64

C. ASCII

D. Hex

Correct Answer: *C*

Community vote distribution

D (100%)

Clauster 8 months, 1 week ago

Selected Answer: D

The Answer is D

This Article straight from Cisco White Papers mentions it again and again and again, just do a CTRL F and search the word Hex and you will see all the mentions of Hex, it doesn't say it is required but it doesn't have to, just by simply reading the article you can make that conclusion that it is.

upvoted 3 times

mgiuseppe86 2 months, 2 weeks ago

You expect people to read? The whole reason they are on this site is because they don't want to read, dont want to study and just do an exam and click the right answers they saw on brain dumps!

upvoted 1 times

adamzet33 3 weeks, 2 days ago

and you are the only one who is different

upvoted 1 times

Rose66 10 months, 2 weeks ago

Selected Answer: D

When DHCP servers are programmed to offer WLAN Controller IP addresses as Option 43 for Cisco Aironet LAPs, the sub-option TLV block is defined in this way:

Type - 0xf1 (decimal 241).

Length - Number of controller IP addresses * 4.

Value - List of the WLC management interfaces, typically translated to hexadecimal values.

The semantics of DHCP server configuration vary based on the DHCP server vendor. This document contains specific instructions on the Microsoft DHCP server, Cisco IOS DHCP server, Linux ISC DHCP Server, Cisco Network Registrar DHCP server, and Lucent QIP DHCP Server. For other DHCP server products, consult the vendor documentation for instructions on vendor specific options. (Source:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html)

upvoted 2 times

BlightedTomato 11 months, 2 weeks ago

the answer is C

ASCII (American Standard Code for Information Interchange) is the most common character encoding format for text data in computers and on the internet. In standard ASCII-encoded data, there are unique values for 128 alphabetic, numeric or special additional characters and control codes.
Hex is not a character formatting is a number system.

upvoted 2 times

danman32 4 months ago

Right, and use of option 43 requires a number. You could I suppose use decimal but that would make it difficult to figure out and to read, since the sub-options encoded in DHCP option 43 are byte boundaries.

upvoted 1 times

Normanby 1 year ago

Selected Answer: D

Add the Option 43 line with this syntax:

option 43 hex <hexadecimal string>
The hexadecimal string in step 3 is assembled as a sequence of the TLV values for the Option 43 suboption: Type + Length + Value. Type is always the suboption code 0xf1. Length is the number of controller management IP addresses times 4 in hex. Value is the IP address of the controller listed sequentially in hex.

For example, suppose there are two controllers with management interface IP addresses, 192.168.10.5 and 192.168.10.20. The type is 0xf1. The length is 2 * 4 = 8 = 0x08. The IP addresses translate to c0a80a05 (192.168.10.5) and c0a80a14 (192.168.10.20). When the string is assembled, it yields f108c0a80a05c0a80a14. The Cisco IOS command that is added to the DHCP scope is:

option 43 hex f108c0a80a05c0a80a14

upvoted 1 times

bora4motion 1 year ago

Selected Answer: D

100% D

upvoted 1 times

ils9100 1 year, 1 month ago

Agreed with Dougj here,
When DHCP servers are programmed to offer WLAN Controller IP addresses as Option 43 for Cisco 1000 Series APs the sub-option TLV block is defined in this way:

Type - 0x66 (decimal 102).

Length: - A count of the characters of the ASCII string in the Value field. Length must include the commas if there is more than one controller specified, but not a zero-terminator.

Value: - A non-zero terminated ASCII string that is a comma-separated list of controllers. No spaces must be embedded in the list.

When DHCP servers are programmed to offer WLAN Controller IP addresses as Option 43 for other Cisco Aironet LAPs, the sub-option TLV block is defined in this way:

Type - 0xf1 (decimal 241).

Length - Number of controller IP addresses * 4.

Value - List of the WLC management interfaces, typically translated to hexadecimal values.

upvoted 1 times

dougj 1 year, 1 month ago

Selected Answer: D

ASCII was only used for the old Cisco 1000 series access points

upvoted 1 times

Wooker 1 year, 2 months ago

Selected Answer: D

Answer: D

upvoted 2 times

Ciscopass 1 year, 2 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html

upvoted 2 times

Jason233 1 year, 2 months ago

Answer C applies when using Cisco DNAC / fabric, option 43 would also point to the DNAC VIP IP, Answer D is correct.

upvoted 3 times

Lukaszaw 1 year, 2 months ago

Why not C ?

upvoted 1 times

jj970us 1 year, 2 months ago

Selected Answer: D

It is HEX.

upvoted 4 times

Question #450 *Topic 1*

Which benefit is realized by implementing SSO?

A. IP first-hop redundancy

B. communication between different nodes for cluster setup

C. physical link redundancy

D. minimal network downtime following an RP switchover

Correct Answer: *D*

Community vote distribution

D (100%)

bora4motion 1 year ago

Selected Answer: D

Answer is D

upvoted 2 times

diamant 1 year ago

https://study-ccnp.com/understanding-sso-cisco-stateful-switchover/

upvoted 2 times

```
R2#show standby
FastEthernet1/0 - Group 40
  State is Standby
    4 state changes, last state change 00:01:51
  Virtual IP address is 10.10.1.1
  Active virtual MAC address is 0000.0c07.ac28 (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac28 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.856 secs
  Preemption disabled
  Active router is 10.10.1.3, priority 85 (expires in 8.672 sec)
  Standby router is local
  Priority 90 (configured 90)
    Track interface FastEthernet0/0 state Up decrement 10
  Group name is "hsrp-Fa1/0-40" (default)
```

Refer to the exhibit. After configuring HSRP an engineer enters the show standby command. Which two facts are derived from the output? (Choose two.)

A. R2 becomes the active router after the hold time expires.

B. If Fa0/0 is shut down, the HSRP priority on R2 becomes 80.

C. R2 Fa1/0 regains the primary role when the link comes back up.

D. The router with IP 10.10.1.3 is active because it has a higher IP address.

E. R2 is using the default HSRP hello and hold timers.

Correct Answer: *BE*

Community vote distribution

BE (65%) AE (35%)

markymark874 Highly Voted 10 months, 4 weeks ago

Selected Answer: BE

BE
key words to look is the track status up dec 10 and current priority
upvoted 7 times

HungarianDish Highly Voted 8 months ago

Selected Answer: BE

So many misleading comments. Current status of track object is "Up" as displayed under "show standby". o, current priority is 90. If fa0/0 goes down, track object changes to "Down", and so priority decrements by 10 (to 80).

Timers are default.
upvoted 6 times

[Removed] 5 months, 1 week ago

You can absolutely track a different interface than the one configured as HSRP.
upvoted 1 times

sergiosolotrabajo Most Recent 1 month, 2 weeks ago

Selected Answer: BE

A: Incorrect, we don't know if there are more routers on the HSRP group, the preemption being disabled also reasures me that R2 will not become active router, just another router will come up as active.

B: Correct, the command "track interface FastEthernet0/0 state Up decrement 10" will be checking if the state is Up, when it goes down, the action occurs.

E: Correct, nothing to add xD.
upvoted 1 times

sergiosolotrabajo 1 month, 2 weeks ago

Edit: "just another router with higher priority will come up as active"
upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Confirmed it is B in CML

HSRP_R2(config-track)#int g0/0
HSRP_R2(config-if)#shut
*Sep 11 19:43:32.681: %RG_FAULTS-6-PRICHANGE: RG Infra RG[1] Priority update. new priority [90] old priority [100] Reason: Fault occurred on the traffic interface
*Sep 11 19:43:32.706: %TRACK-6-STATE: 1 interface Gi0/0 line-protocol Updo show standby
GigabitEthernet0/1 - Group 0
State is Standby
1 state change, last state change 00:03:53
Virtual IP address is 10.10.1.1
Active virtual MAC address is 0000.0c07.ac00
Local virtual MAC address is 0000.0c07.ac00 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.704 secs
Preemption disabled
Active router is 10.10.1.2, priority 85 (expires in 8.880 sec)
Standby router is local
>>>>>>>>>>>> Priority 80 (configured 90) <<<<<<<<<<<<<<<<<<<<<<<<
Track object 1 state Down decrement 10
Group name is "hsrp-Gi0/1-0" (default)

upvoted 1 times

JesssRoney 4 months, 2 weeks ago

Selected Answer: BE

I will go for BE

upvoted 1 times

Lale 5 months ago

Selected Answer: BE

It has not been mentioned that there are only two routers in the HSRP group. A group can have up to 32 routers. Maybe there is another router R3 that also has a priority of 90 but R2 was elected as primary.

Therefore BE

upvoted 1 times

dragonwise 8 months ago

AE
B is wrong because the interface is not fa0/0

upvoted 1 times

HungarianDish 8 months ago

With HSRP it is common to track the interface connecting to an upstream device. However, HSRP is set up on the LAN interface (or vlan interface), which serves as a default gateway for the LAN. So, the different interfaces are OK.

upvoted 3 times

chefexam 9 months, 2 weeks ago

Selected Answer: AE

A - Well, that's the default behaviour of HSRP- TRUE
B - When the interface is up, the SLA REDUCES the priority - WRONG
C - Preemption is disabled - WRONG
D - The priorities don't match - WRONG
E - 3 and 10 are the HSRP default timers - TRUE

Maybe Fa0/0 just went down, therefore the HSRP priority went up from 80 to 90.

upvoted 4 times

HungarianDish 8 months ago

B) It has not much to do with IP SLA. The track configuration under "show standby" means that the current state of the track object is "Up". If fa0/0 is shut down, then the state changes to "Down."

Something like this:
DSW2(config)#int fa0/1
DSW2(config-if)#shut
00:02:25: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
00:02:25: %TRACKING-5-STATE: 1 interface Fa0/1 state Up->Down

DSW2(config-if)#do sh stand
Vlan 1 - Group 1
State is Active
2 state changes, last state change 00:2:34
Virtual IP address is 172.16.3.1
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01(v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.102secs
Preemption enabled
Active router is local

Standby router is 172.16.3.3, priority 99 (expires in 3.555 sec)
Priority 91 (default 100)
Track interface FastEthernet0/1 state Down decrement 9
upvoted 2 times

kewokil120 10 months, 1 week ago

Selected Answer: AE

When hold timers expires. It assumes R1 is gone and goes active. E because timers are default.
upvoted 2 times

Rose66 10 months, 2 weeks ago

Selected Answer: BE

I agree with Normanby ... As PREEMTION IS DISABLED A can't be a correct choice.....
upvoted 2 times

kewokil120 10 months, 4 weeks ago

Selected Answer: AE

The track reduces priority when the interface is up.
When the dead timer expires it assumes to be active because it think the other router is gone.
upvoted 1 times

HungarianDish 8 months ago

The track reduces priority when the state is "Down". As current state is "Up", "show standby" displays "Up".
upvoted 2 times

nushadu 11 months, 1 week ago

Selected Answer: BE

cisco_R3(config-subif)#do s runn int Ethernet0/0.60
Building configuration...

Current configuration : 180 bytes
!
interface Ethernet0/0.60
encapsulation dot1Q 60
ip address 10.111.11.1 255.255.255.0
standby 40 ip 10.111.11.254
standby 40 priority 90
standby 40 track 2 decrement 10
end
...
!
track 2 interface Loopback1 line-protocol
!

cisco_R3(config-subif)#do s stand
...
Ethernet0/0.60 - Group 40
State is Active
2 state changes, last state change 00:20:03
Virtual IP address is 10.111.11.254
Active virtual MAC address is 0000.0c07.ac28
Local virtual MAC address is 0000.0c07.ac28 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.896 secs
Preemption disabled
Active router is local
Standby router is unknown
Priority 90 (configured 90)
Track object 2 state Up decrement 10
Group name is "hsrp-Et0/0.60-40" (default)
cisco_R3(config-subif)#
upvoted 1 times

nushadu 11 months, 1 week ago

cisco_R3(config-subif)#in loo1
cisco_R3(config-if)#shutdown
cisco_R3(config-if)#
*Dec 22 15:41:59.953: %TRACK-6-STATE: 2 interface Lo1 line-protocol Up -> Down
cisco_R3(config-if)#
*Dec 22 15:42:01.958: %LINK-5-CHANGED: Interface Loopback1, changed state to administratively down
*Dec 22 15:42:02.960: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to down
cisco_R3(config-if)#do s stand
...
Ethernet0/0.60 - Group 40
State is Active
2 state changes, last state change 00:23:15
Virtual IP address is 10.111.11.254
Active virtual MAC address is 0000.0c07.ac28
Local virtual MAC address is 0000.0c07.ac28 (v1 default)

Hello time 3 sec, hold time 10 sec
Next hello sent in 1.920 secs
Preemption disabled
Active router is local
Standby router is unknown
Priority 80 (configured 90) <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Track object 2 state Down decrement 10
Group name is "hsrp-Et0/0.60-40" (default)
cisco_R3(config-if)#

upvoted 1 times

MJane 11 months, 2 weeks ago

B is true
https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/113553-to-hsrpv2-config.html

upvoted 1 times

KOJJY 11 months, 3 weeks ago

Selected Answer: AE

the trick on tracking UP .
for that it A,E

upvoted 3 times

nushadu 11 months, 4 weeks ago

Selected Answer: BE

B.E. imho))

upvoted 1 times

Typovy 12 months ago

Selected Answer: BE

B and E correct. Object is tracking for 'Up' not 'Down'. So the priority is changed when the interfaces comes up

upvoted 1 times

Typovy 11 months, 4 weeks ago

I mean A&E

upvoted 2 times

bora4motion 1 year ago

Selected Answer: BE

It's quite a tricky question however B and E is correct.

upvoted 1 times

Question #452 *Topic 1*

Which two parameters are examples of a QoS traffic descriptor? (Choose two.)

A. DSCP

B. MPLS EXP bits

C. packet size

D. bandwidth

E. ToS

Correct Answer: *AB*

Community vote distribution

AB (68%) AE (32%)

iGlitch Highly Voted 1 year ago

Selected Answer: AB

From the OCG page 368:
"The following traffic descriptors are typically used for classification:
■ Internal: QoS groups (locally significant to a router)
■ Layer 1: Physical interface, subinterface, or port
■ Layer 2: MAC address and 802.1Q/p Class of Service (CoS) bits
■ Layer 2.5: MPLS Experimental (EXP) bits
■ Layer 3: Differentiated Services Code Points (DSCP), IP Precedence (IPP), and source/
destination IP address
■ Layer 4: TCP or UDP ports
■ Layer 7: Next Generation Network-Based Application Recognition (NBAR2)".

A and B are correct.

upvoted 14 times

teikitiz Most Recent 4 months, 4 weeks ago

Selected Answer: AB

The ToS byte in the IP header contains DSCP info, but it's DSCP that actually describes precedence/drop priority

upvoted 1 times

[Removed] 5 months, 1 week ago

Selected Answer: AE

This one seems to be badly worded... or it should specify 3 answers.
A,B, and E

upvoted 3 times

Muste 6 months, 1 week ago

By Chatgpt:-
The two parameters that are examples of a QoS traffic descriptor are:

A. DSCP (Differentiated Services Code Point), which is a field in the IP header that specifies the level of service for a particular packet.

D. Bandwidth, which is the amount of data that can be transmitted over a network in a given period of time.

Note: MPLS EXP bits and ToS (Type of Service) are also related to QoS but are not traffic descriptors themselves. The MPLS EXP bits are used to specify the priority of MPLS packets, while ToS is an older field in the IP header that has been replaced by DSCP. Packet size is not a QoS traffic descriptor but can be used in QoS policies to limit the amount of bandwidth that a certain type of traffic can use.

upvoted 1 times

foreignbishop 6 months, 1 week ago

Selected Answer: AE

https://www.cisco.com/c/en/us/td/docs/routers/ncs4000/software/qos/configuration_guide/b-qos-cg/b-qos-cg_chapter_0101.pdf

Traffic Descriptors from this question are A and E per the link above.

upvoted 1 times

Ayman_B 10 months, 2 weeks ago

Selected Answer: AE

(ToS) and (DSCP) both of them are parameter that used to mark traffic with a specific value, indicating its priority level.
while MPLS EXP bits is a parameter that is a part of (QoS) traffic descriptor. The MPLS EXP bits are 3-bit fields in the MPLS label header that can be used to indicate the level of priority of the packet and MPLS Experimental (EXP) bits is the descriptor for classification Layer 2.5

upvoted 2 times

yousif387 1 year ago

Selected Answer: AB

provided answer true

upvoted 1 times

dougj 1 year, 1 month ago

Selected Answer: AE

The ToS bit could also a descriptor for QoS as it is used to classify packets for QoS treatment by routers

upvoted 2 times

dougj 1 year, 1 month ago

All three, A,B and E are technically correct and E is the only one actually highlighted in the QoS descriptor section here:
https://www.cisco.com/c/en/us/td/docs/routers/ncs4000/software/qos/configuration_guide/b-qos-cg/b-qos-cg_chapter_0101.pdf

upvoted 1 times

kebkim 1 year, 2 months ago

The MPLS experimental bits (EXP) field is a 3-bit field in the MPLS header that you can use to define the QoS treatment (per-hop behavior) that a node should give to a packet. In an IP network, the DiffServ Code Point (DSCP) (a 6-bit field) defines a class and drop precedence.

upvoted 3 times

teoht 1 year, 2 months ago

Selected Answer: AB

A, B is the answer

upvoted 1 times

```
ip vrf BLUE
 rd 1:1
!
interface Vlan100
 description GLOBAL_INTERFACE
 ip address 10.10.1.254 255.255.255.0
!
access-list 101 permit ip 10.10.5.0 0.0.0.255 10.10.1.0
255.255.255.0
!
route-map VRF_TO_GLOBAL permit 10
 match ip address 101
set global
!
interface Vlan500
 description VRF_BLUE
 ip vrf forwarding BLUE
 ip address 10.10.5.254 255.255.255.0
ip policy route-map VRF_TO_GLOBAL
```

Refer to the exhibit. An engineer attempts to create a configuration to allow the Blue VRF to leak into the global routing table, but the configuration does not function as expected. Which action resolves this issue?

A. Change the source network that is specified in access-list 101.

B. Change the access-list destination mask to a wildcard.

C. Change the access-list number in the route map.

D. Change the route-map configuration to VRF_BLUE.

Correct Answer: *B*

Community vote distribution

B (100%)

AndreasThornus Highly Voted 11 months, 4 weeks ago

Access List has line wrapped - answer B is given correctly present yes.

upvoted 5 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Selected Answer: B

We need wildcard mask to be corrected. host bits needs to be specified in this configuration.

B

upvoted 1 times

VLAN4461 3 months ago

Almost the exact question in the PBR example:
https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200158-Configure-Route-Leaking-between-Global-a.html

upvoted 2 times

Question #454 *Topic 1*

An engineer must configure a multicast UDP jitter operation. Which configuration should be applied?

A. Router(config)#ip sla 1 Router(config)#udp-jitter 192.0.2.115 65051

B. Router(config)#ip sla 1 Router(config)#udp jitter 239.1.1.1 65051 end-point list List source-ip 192.168.1.1

C. Router(config)#ip sla 1 Router(config)#udp-jitter 192.0.2.115 65051 num-packets 20

D. Router(config)#ip sla 1 Router(config)#udp jitter 10.0.0.1 source-ip 192.168.1.1

Correct Answer: *B*

Community vote distribution

B (86%) 7%

Eroman Highly Voted 1 year, 2 months ago

Selected Answer: B

B is true

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-s/sla-15-s-book/sla_mcast_suppt.pdf

upvoted 5 times

nasaexam 11 months, 4 weeks ago

B can not be right.
"udp-jitter" = correct command
"udp jitter" = incorrect command

upvoted 1 times

danman32 4 months ago

Likely a typo

upvoted 1 times

danman32 Most Recent 4 months ago

Only B specifies a destination as a multicast address, and we're asked about MULTICAST jitter. You need the remaining parameters in the udp-jitter because of the multicast address.

upvoted 1 times

HarwinderSekhon 5 months ago

Selected Answer: B

B

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/xe-16-10/sla-xe-16-10-book/sla-mcast-suppt.pdf
Page 6

upvoted 1 times

dragonwise 8 months ago

A.
Router(config)#ip sla 1
Router(config)#udp-jitter 192.0.2.115 65051

B.
Router(config)#ip sla 1
Router(config)#udp jitter 239.1.1.1 65051 end-point list List source-ip 192.168.1.1

C.
Router(config)#ip sla 1
Router(config)#udp-jitter 192.0.2.115 65051 num-packets 20

D.
Router(config)#ip sla 1
Router(config)#udp jitter 10.0.0.1 source-ip 192.168.1.1

upvoted 2 times

Leoveil 10 months, 2 weeks ago

Selected Answer: B

none of the other answers has a multicast address (224.0.0.0 - 239.255.255.255)

upvoted 3 times

TSKARAN 10 months, 2 weeks ago

Configures the IPSLAs operation as a multicast UDPjitter operation and enters multicast UDP jitter configuration mode.

udp-jitter {destination-ip-address| destination-hostname}
destination-port endpoint-list endpoint-list [ssm]
[source-ip ip-address] [source-port port-number]
[num-packets number-of-packets] [interval
interpacket-interval]

Example:
Device(config-ip-sla)# udp-jitter 239.1.1.1 5000
endpoint-list mcast-rcvrs source-ip 10.10.10.106
source-port 7012 num-packets 50 interval 25

The given answer B is misssing - , upd jitter >> udp-jitter
upvoted 1 times

Rose66 10 months, 2 weeks ago

Selected Answer: B

I think there is only the '-' missing... needs to be 'B' because endpoint-list is mandatory:
udp-jitter {destination-ip-address| destination-hostname} destination-port endpoint-list endpoint-list [ssm] [source-ip ip-address] [source-port port-number]
[num-packets number-of-packets] [interval interpacket-interval]
upvoted 1 times

AndreasThornus 11 months, 4 weeks ago

The question states that this is about multicast jitter so B is correct.

When configuring IP SLA, the available commands CHANGE when you specify a multicast address. For example "udp-jitter 239.1.1.1 ..." allows you to enter an endpoint list. This "endpoint" option doesn't appear as valid syntax when using regular class A/B/C addresses.
upvoted 3 times

nushadu 11 months, 1 week ago

yes, that is true:
cisco_R3(config-ip-sla)#udp-jitter 239.1.1.1 65000 endpoint-list ?
WORD Endpoint list name <<<<<<<<<<<<<<<<<<<< IP multicast range

cisco_R3(config-ip-sla)#udp-jitter 10.0.0.22 ?
<1-65535> Port Number. Recommended ports greater than 1023. For codec
options recommended port range is an Even Port range between
16384-32767 or 49152-65535

cisco_R3(config-ip-sla)#udp-jitter 10.0.0.22 65000 ? <<<<<<<<<<<< "normal" IP addr
codec codec type to be configured
control Enable or disable control packets
interval Inter Packet Interval
num-packets Number of Packets to be transmitted
source-ip Source address
source-port Source Port
<cr>

cisco_R3(config-ip-sla)#udp-jitter 10.0.0.22 65000
upvoted 1 times

dougj 1 year, 1 month ago

Selected Answer: B

Basically you could argue that A, B and D are correct answers but only with regards to UDP Jitter IP SLA configuration. This question refers to multicast network meaning only B is correct as it identifes a multicast responder in the command line
upvoted 1 times

dougj 1 year, 1 month ago

sorry C could also be correct as a UDP Jitter config line
upvoted 1 times

iEpsilon 1 year, 1 month ago

Selected Answer: C

A is correct but C is more precise
upvoted 1 times

onkel_andi 1 year, 1 month ago

Selected Answer: B

B is correct
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/ipsla/configuration/xe-3s/sla-xe-3s-book/sla_mcast_suppt.html.xml
upvoted 1 times

Wooker 1 year, 2 months ago

Selected Answer: D

multicast UDP jitter operation ...
The correct answer is D.

upvoted 1 times

Wooker 1 year, 2 months ago

sorry C

upvoted 1 times

kebkim 1 year, 2 months ago

C is Answer.
configure terminal
ip sla 1
udp-jitter 192.0.2.115 65051 num-packets 20
request-data-size 160
tos 128
frequency 30
ip sla schedule 1 start-time after 00:05:00

upvoted 3 times

```
enable secret cisco

username cisco privilege 15 secret cisco

aaa new-model
aaa authentication login default group radius local
aaa authorization network default group radius
```

Refer to the exhibit. The network administrator must be able to perform configuration changes when all the RADIUS servers are unreachable. Which configuration allows all commands to be authorized if the user has successfully authenticated?

A. aaa authentication login default group radius local none

B. aaa authorization exec default group radius

C. aaa authorization exec default group radius if-authenticated

D. aaa authorization exec default group radius none

Correct Answer: *C*

Community vote distribution

C (86%) 14%

kmb192006 Highly Voted 7 months, 2 weeks ago

Selected Answer: C

Although C & D can both let network administrator to perform changes when RADIUS servers are unreachable, C is doing what the question asking for - "to be authorized if the user has successfully authenticated"

"if-authenticated" allows user get authorized (every command the user enter is authorized) in the session if user is authenticated by any of methods defined in aaa

meanwhile "none" disable authorization (every command the user enter does not need authorization) for the session if the defined authorization method in aaa is unreachable

ENCOR OCG Page 775 has specified that

upvoted 6 times

dragonwise Most Recent 8 months ago

Selected Answer: D

Answer is D because RADIUS server is unavailable, and local user need to issue commands. And with "non" is there, the local user will not be subject of authorization will issue commands without restrictions

upvoted 1 times

Cooldude89 9 months, 2 weeks ago

C is correct
GNS3 Output :
R1(config)#aaa authorization exec default group radius ?
group Use server-group.
if-authenticated Succeed if user has authenticated.
krb5-instance Use Kerberos instance privilege maps.
local Use local database.
none No authorization (always succeeds).

upvoted 2 times

kebkim 1 year, 2 months ago

C is the answer.
The aaa authorization exec default group radius if-authenticated command configures the network access server to contact the RADIUS server to determine if users are permitted to start an EXEC shell when they log in. If an error occurs when the network access server contacts the RADIUS server, the fallback method is to permit the CLI to start, provided the user has been properly authenticated.

upvoted 4 times

Question #456 *Topic 1*

In a Cisco SD-WAN solution, which two functions are performed by OMP? (Choose two.)

A. advertisement of network prefixes and their attributes

B. configuration of control and data policies

C. gathering of underlay infrastructure data

D. delivery of crypto keys

E. segmentation and differentiation of traffic

Correct Answer: *AD*
Reference:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing-book/m-unicast-routing.html

Community vote distribution

AD (50%) AB (31%) Other

jj970us Highly Voted 1 year, 2 months ago

A and D is correct.
The OMP protocol is responsible for:
– Distribution of Transport Locators (TLOCs) among network sites in the sd-wan domain.
– Distribution of service-side reachability information.
– Distribution of service-chaining information.
– Distribution of data plane security parameters, VPN labels, and crypto keys.
– Distribution of data and application-aware routing (AAR) policies. (Answer E is not correct as OMP is only distribute, not configure data policies)
Reference: https://www.networkacademy.io/ccie-enterprise/sdwan/omp-overview

upvoted 21 times

CCNPWILL Most Recent 1 month, 2 weeks ago

A and D are correct... by OMP... not vSmart. vSmart does B sure... but we are talking about OMP specifically.

upvoted 1 times

WereAllinThisTogether 4 months, 2 weeks ago

A and C
OMP collects data about the underlay infrastructure, including link quality, latency, bandwidth, and other performance metrics. This information is crucial for making intelligent routing decisions based on the current state of the network. OMP uses this data to select the optimal paths for traffic and ensure efficient utilization of available network resources.

upvoted 1 times

Darkboy7 5 months ago

https://www.networkacademy.io/ccie-enterprise/sdwan/what-is-sd-wan
A and D

upvoted 1 times

Bluntedcase 5 months, 2 weeks ago

Selected Answer: D

p634 in the OCG (under vSmart):
"OMP is a proprietary routing protocol similar to BGP that can advertise routes, next hop, keys and policy information needed to establish and maintain the SD-WAN fabric."

So for me I'd go for A&D too

upvoted 1 times

Vip44000 6 months ago

Selected Answer: AD

OMP is a proprietary routing protocol similar to BGP that can advertise routes, next hops, keys, and policy information needed to establish and maintain the SD-WAN fabric

Source: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guid
Page: 634
Chapter: 23
Section: vSmart Controller

upvoted 1 times

Muste 6 months, 1 week ago

Selected Answer: AC

in a Cisco SD-WAN solution, the OMP (Overlay Management Protocol) does not deliver crypto keys. The OMP is primarily responsible for advertising network prefixes and their attributes, as well as gathering underlay infrastructure data. Crypto keys, on the other hand, are typically

managed and delivered by other components of the SD-WAN solution, such as the control plane and security services. These components handle the encryption and decryption of traffic and the management of cryptographic keys for secure communication within the SD-WAN network.

The vSmart controller manages the generation, distribution, and rotation of cryptographic keys used for securing the communication between SD-WAN devices. It ensures that the keys are securely exchanged and synchronized among the devices in the network, allowing for encrypted traffic flow and secure connectivity.

upvoted 1 times

mykab 8 months, 3 weeks ago

Selected Answer: AC

The two functions that are performed by OMP (Overlay Management Protocol) in a Cisco SD-WAN solution are:

A. Advertisement of network prefixes and their attributes: OMP advertises the network prefixes and their attributes to all the nodes in the overlay network. These attributes include the path metrics, bandwidth, delay, jitter, and packet loss, which are used to calculate the best path for forwarding the traffic.

C. Gathering of underlay infrastructure data: OMP gathers the underlay network infrastructure data, such as the link quality, availability, and bandwidth, from the vEdge routers, which are then used to calculate the best path for forwarding the traffic. This helps in achieving optimal utilization of the available network resources.

Therefore, options A and C are correct. Option B is performed by vSmart controllers, option D is performed by vManage, and option E is performed by vEdge routers.

upvoted 1 times

Stylar 10 months ago

from OCG book:
Facilitation of network communication on the SD-WAN fabric, including data plane connectivity among sites, service chaining, and multi-VPN topology information
■ Advertisement of services available to the fabric and their related locations
■ Distribution of data plane security information, including encryption keys
■ Best-path selection and routing policy advertisement.

upvoted 4 times

saiyuki1209 10 months, 3 weeks ago

Selected Answer: AD

A & D correct

upvoted 1 times

Nickplayany 11 months ago

Selected Answer: AD

A & D. B says configuration which is wrong...

upvoted 3 times

H3kerman 1 year ago

Selected Answer: AD

Service routes orginated from vEdges/vSmarts

Reachability [vRoutes, TLOCs]
Security [Encryption Keys]
Service routes [Firewall/IDS]
Policies throughout the fabric [Data/App-route Policies]

https://www.grandmetric.com/knowledge-base/design_and_configure/sd-wan-overlay-management-protocol-omp/

upvoted 1 times

Ado_68 1 year ago

I'm going for A/D because OMP is used for distribution of control and data policies but NOT for configuration what question B. says

upvoted 1 times

VergilP 1 year, 1 month ago

Selected Answer: AD

I'm going for A/D

upvoted 2 times

Radwa_ 1 year, 1 month ago

Selected Answer: AB

The Cisco SD-WAN Overlay Management Protocol (OMP) is the protocol responsible for establishing and maintaining the Cisco SD-WAN control plane. It provides the following services:

Orchestration of overlay network communication, including connectivity among network sites, service chaining, and VPN or VRF topologies
Distribution of service-level routing information and related location mappings
Distribution of data plane security parameters
Central control and distribution of routing policy
Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing-book/m-unicast-routing.html

upvoted 1 times

Caledonia 1 year, 2 months ago

Selected Answer: AB

The answer is A, B

upvoted 4 times

Question #457 *Topic 1*

How can an engineer prevent basic replay attacks from people who try to brute force a system via REST API?

A. Add a timestamp to the request in the API header.

B. Use a password hash.

C. Add OAuth to the request in the API header.

D. Use HTTPS.

Correct Answer: *A*

Reference:

https://security.stackexchange.com/questions/221708/golang-rest-api-security-checks

Community vote distribution

A (100%)

kebkim Highly Voted 1 year, 2 months ago

A is the Answer.
Here's the list of best practices in securing RESTful API.
1. Always Use HTTPS - Traffic must be encrypted
2. Never expose information on URLs - as this can be captured in web server logs, which makes them easily exploitable.
3. Consider Oauth
4. Adding Timestamp in Request - This will prevent very basic replay attacks from people who are trying to brute force your system
5. Input Parameter Validation - Put strong validation checks and reject the request immediately if validation fails.
6. Use Auditing and Logging - Any subject or entity can be audited

upvoted 9 times

markymark874 Highly Voted 10 months, 4 weeks ago

Selected Answer: A

https://hakin9.org/how-to-secure-your-rest-api-from-attackers/

upvoted 5 times

Question #458 *Topic 1*

What are the main components of Cisco TrustSec?

A. Cisco ISE and Enterprise Directory Services

B. Cisco ISE, network switches, firewalls, and routers

C. Cisco ISE and TACACS+

D. Cisco ASA and Cisco Firepower Threat Defense

Correct Answer: *B*

Community vote distribution

B (100%)

tckoon Highly Voted 1 year, 2 months ago

B is correct
https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-726831.pdf

upvoted 5 times

AndreasThornus Most Recent 11 months, 3 weeks ago

Selected Answer: B

B - Cisco TrustSec and Secure Access Solution Components
• FlexAuth (802.1X, WebAuth, MAB): All Cisco Catalyst® switching platforms
• Device sensors: Cisco Catalyst 3000 Series; Cisco Catalyst 4500 Series with Supervisor 7(L)-E; Cisco Wireless LAN Controllers
• Cisco TrustSec:
- Cisco Catalyst 2960-S/SF/C, 3560, 3560-E/C, 3750, 3750-E Series: SXP only
- Cisco Catalyst 3560-X, 3750-X Series: SXP, SGT, SGACL
- Cisco Catalyst 4500 Series with Supervisor 6(L)-E, 7(L)-E: SXP only
- Cisco Catalyst 6500 with Supervisor Engine 2T: SXP, SGT, SGACL
- Cisco Nexus 7000 and 5000 Series: SXP, SGT, SGACL
- Cisco Nexus 1000v: SXP only
- Cisco Wireless LAN Controller 2500, 5500, Cisco Wireless Service Module (WiSM) 2, Cisco Wireless Controller on Cisco Services-Ready Engine (SRE): SXP only
- Cisco Integrated Services Router G2: SXP, Security Group Firewall (SG-FW)
- Cisco ASR 1000 Series Aggregation Services Router: SXP, SG-FW
- Cisco ASA 5500 Series Adaptive Security Appliances: SXP, SG-FW
- Virtual Desktop Infrastructure (VDI) and Cisco AnyConnect® Secure Mobility Client with Remote Desktop Protocol (RDP)

upvoted 3 times

Titini 1 year, 2 months ago

C is correct

upvoted 1 times

Question #459 *Topic 1*

What is a characteristic of a WLC that is in master controller mode?

A. Configuration on the master controller is executed on all wireless LAN controllers.

B. The master controller is responsible for load balancing all connecting clients to other controllers.

C. All new APs that join the WLAN are assigned to the master controller.

D. All wireless LAN controllers are managed by the master controller.

Correct Answer: *C*

kebkim Highly Voted 1 year, 2 months ago

When there is a master controller enabled, all newly added access points with no primary, secondary, or tertiary controllers assigned associate with the master controller on the same subnet.

upvoted 7 times

Question #460 *Topic 1*

Which Cisco FlexConnect state allows wireless users that are connected to the network to continue working after the connection to the WLC has been lost?

A. Authentication Down/Switching Down

B. Authentication-Central/Switch-Local

C. Authentication-Central/Switch-Central

D. Authentication-Down/Switch-Local

Correct Answer: *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide/ ch7_HREA.html

Community vote distribution

D (83%) B (17%)

djedeen 3 months, 1 week ago

Authentication-Down/Switch-Local: A WLAN that requires central authentication rejects new users. Existing authenticated users continue to be switched locally until session time-out if configured. The WLAN continues to beacon and respond to probes until there are no more existing users associated to the WLAN. This state occurs as a result of the AP going into standalone mode.

upvoted 1 times

PureInertiaCopy 3 months, 2 weeks ago

D. Authentication-Down/Switch-Local

Cisco FlexConnect allows remote sites to locally switch traffic without having to traverse the WAN back to the central controller. In the context of FlexConnect, the "Authentication Down" state refers to the situation where the connection between the access point (AP) and the central Wireless LAN Controller (WLC) is lost. In this state, the AP can still provide basic wireless services to the clients that are already authenticated, even if it cannot communicate with the central controller.

The "Switch-Local" mode means that the AP will locally switch user traffic without sending it back to the central controller. This allows wireless users that are connected to the network to continue working even after the connection to the WLC has been lost, as long as their authentication state is maintained.

So, the correct answer is:

D. Authentication-Down/Switch-Local

upvoted 1 times

net_eng10021 6 months ago

Selected Answer: D

Authentication-Down/Switch-Local: A WLAN that requires central authentication rejects new users. Existing authenticated users continue to be switched locally until session time-out if configured. The WLAN continues to beacon and respond to probes until there are no more existing users associated to the WLAN. This state occurs as a result of the AP going into standalone mode.

upvoted 1 times

Muste 6 months, 1 week ago

Selected Answer: B

The Main Point is the network to continue working and it can't continue working in the authentication down/witch localy
Authentication Down—Local Switching: This state occurs as a result of the AP going into standalone mode. A WLAN that requires central authentication rejects new users. Existing authenticated users continue to be switched locally until session timeout (if configured). The WLAN continues to beacon and respond to probes until there are no more (existing) users associated to the WLAN. for the network to continue even after it has lost connection to the WLC it must be in Authentication Central: Switch Locally

upvoted 1 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: D

It is D
Taken from this Cisco document: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html
"authentication down, local switching—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode."

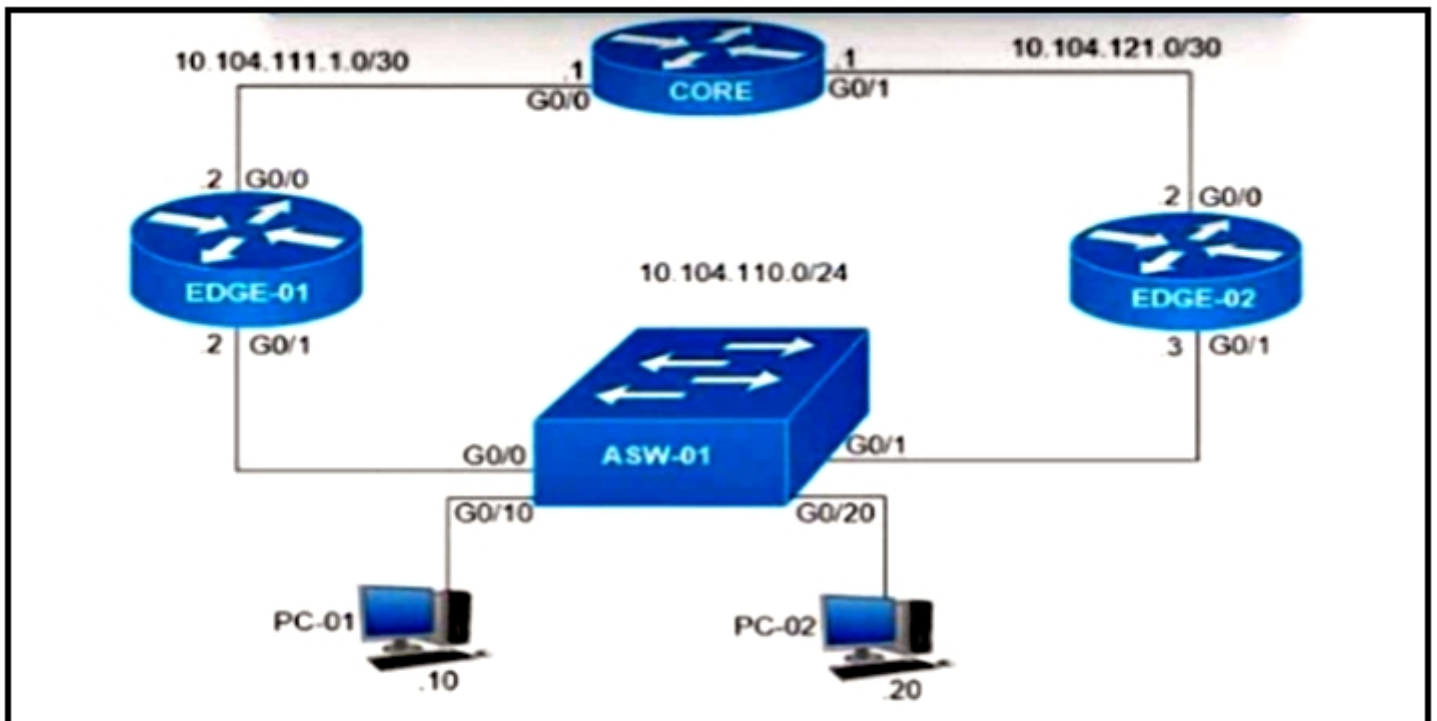
upvoted 4 times

Alberht 1 year, 2 months ago

D
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide/ch7_HREA.pdf Figure 7-4

upvoted 2 times

Question #461 *Topic 1*




```
Edge-01(config)#track 10 interface Gigabitethernet 0/0 line-protocol
Edge-02(config)#track 10 interface Gigabitethernet 0/0 line-protocol

Edge-01#show vrrp brief
Interface          Grp Pri Time  Own Pre State      Master addr     Group addr
G0/1               10  100 3609          Y  Master   10.104.110.2    10.104.110.1

Edge-02#show vrrp brief
Interface          Grp Pri Time  Own Pre State      Master addr     Group addr
G0/1               10  80  3687          Y  Backup   10.104.110.2    10.104.110.1
```

Refer to the exhibit. Object tracking has been configured for VRRP-enabled routers Edge-01 and Edge-02. Which commands cause Edge-02 to preempt Edge-01 in the event that interface G0/0 goes down on Edge-01?

A. Edge-01(config)#interface G0/1 Edge-01(config-if)#vrrp 10 track 10 decrement 30

B. Edge-02(config)#interface G0/1 Edge-02(config-if)#vrrp 10 track 10 decrement 30

C. Edge-02(config)#interface G0/1 Edge-02(config-if)#vrrp 10 track 10 decrement 10

D. Edge-01(config)#interface G0/1 Edge-01(config-if)#vrrp 10 track 10 decrement 10

Correct Answer: *A*

Community vote distribution

A (100%)

mgiuseppe86 2 months, 2 weeks ago

A is obvious. We just want E2 to become Active, so if g0/0 on E1 goes down, the priority decrements by 30 making it a lower priority (70) than E2 (80)

upvoted 1 times

adrian0792 5 months, 2 weeks ago

could it option D, only is change of decrement

upvoted 2 times

[Removed] 2 months, 2 weeks ago

Under normal circumstances yes but the configs have custom priority set for E2. Option D wouldn't decrement far enough to be lower

upvoted 1 times

PureInertiaCopy 3 months, 2 weeks ago

My thoughts exactly

upvoted 2 times

nushadu 11 months, 1 week ago

Selected Answer: A

cisco_R3(config-subif)#do s run interface Ethernet0/0.70
Building configuration...

Current configuration : 229 bytes
!
interface Ethernet0/0.70
description vrf_RED
encapsulation dot1Q 70

ip vrf forwarding RED
ip address 10.111.12.1 255.255.255.0
ip policy route-map RED_TO_GLOBAL
vrrp 11 ip 10.111.12.254
vrrp 11 track 2 decrement 30
end

cisco_R3(config-subif)#do s vrrp

Ethernet0/0.70 - Group 11
State is Master
Virtual IP address is 10.111.12.254
Virtual MAC address is 0000.5e00.010b
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 70
Track object 2 state Down decrement 30
Master Router is 10.111.12.1 (local), priority is 70 <<<<<<<<<<<<<<
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec

cisco_R3(config-subif)#

upvoted 3 times

nushadu 11 months, 1 week ago

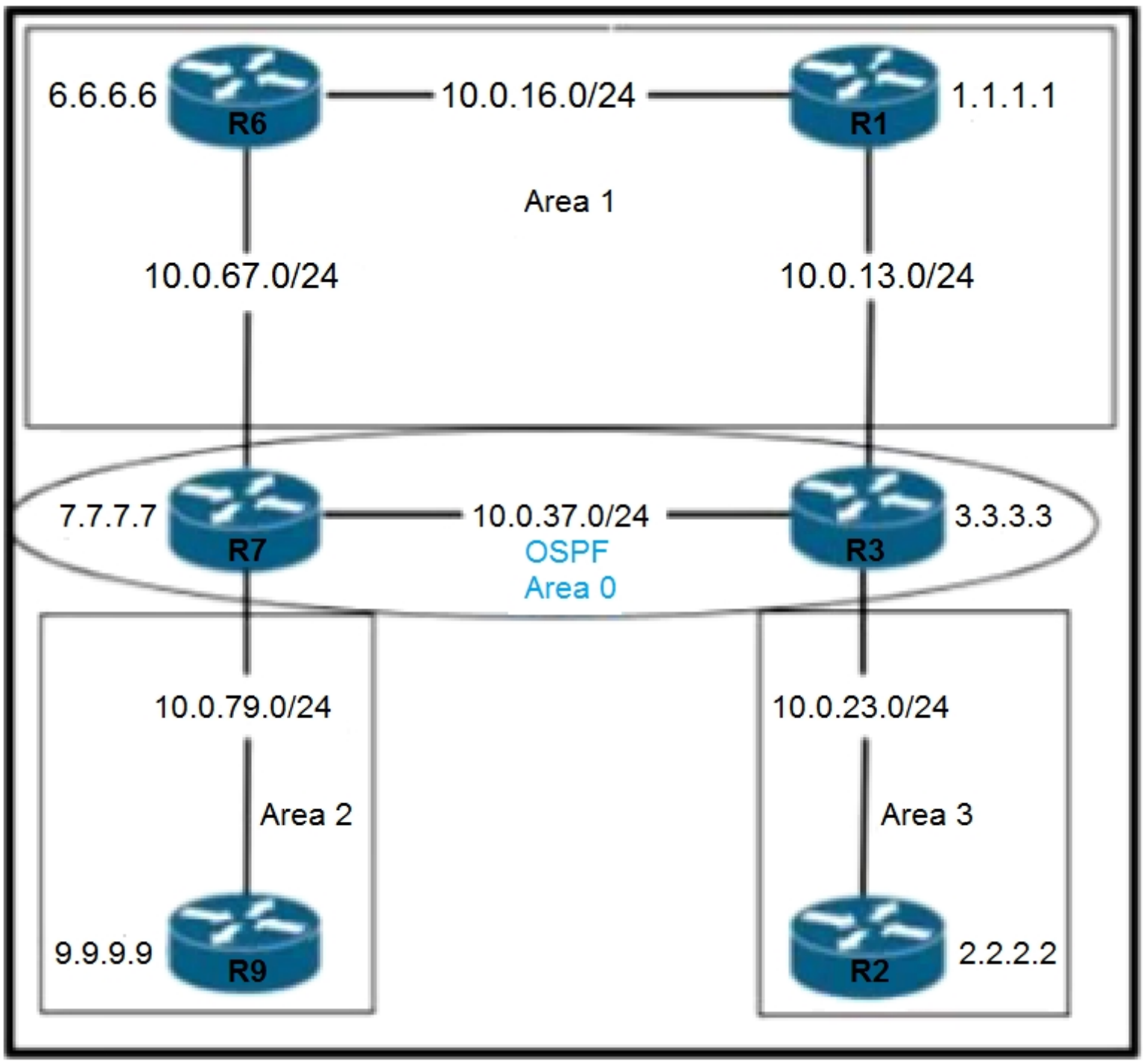
cisco_R3(config-subif)#
cisco_R3(config-subif)#int loo1
cisco_R3(config-if)#no shu
cisco_R3(config-if)#
*Dec 22 17:46:10.897: %TRACK-6-STATE: 2 interface Lo1 line-protocol Down -> Up
cisco_R3(config-if)#
*Dec 22 17:46:12.903: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
*Dec 22 17:46:13.904: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
cisco_R3(config-if)#do s vrrp

Ethernet0/0.70 - Group 11
State is Master
Virtual IP address is 10.111.12.254
Virtual MAC address is 0000.5e00.010b
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Track object 2 state Up decrement 30
Master Router is 10.111.12.1 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec

cisco_R3(config-if)#

upvoted 1 times

Question #462 *Topic 1*



Refer to the exhibit. An engineer must prevent the R6 loopback from getting into Area 2 and Area 3 from Area 0. Which action must the engineer take?

A. Apply a filter list outbound on R3 and R7.

B. Apply a filter list inbound on R2 and R9.

C. Apply a filter list inbound on R3 and R7.

D. Apply a filter list outbound on R7 only.

Correct Answer: *C*

Community vote distribution

C (60%) A (38%)

siteoforigin Highly Voted 1 year, 2 months ago

Selected Answer: A

An Inbound filter list on R3 and R7 would prevent the route from being installed in Area 0, the criteria were to make sure it did not reach Area 2 and 3 only. An outbound filter can be applied on ABR's, so I believe A is the answer.

upvoted 17 times

jjeans 1 year ago

You are NOT correct!

Outbound for filter lists is not correct.
FIlter-lists are related to areas, not devices.
So.. area 2 and area 3 from view of R3 unf R7 is INBOUND!

upvoted 10 times

RREVECO 1 year, 2 months ago

WRONG.
distribute-list out command. This command only works on the routes being redistributed by Autonomous system boundary Router into OSPF
https://community.cisco.com/t5/networking-knowledge-base/distribute-list-out-command-in-ospf/ta-p/3120931

The correct answer it´s "C"
upvoted 7 times

H_al 1 year, 1 month ago
What does that command have to do with the question? You apply a filter list using the "filter-list prefix" command, where prefix is a previously defined rule that blocks the network we don't want to reach Area 2 and 3. The outbound filter list applied on R3 and R7 would stop advertising LSA3 out of all it's other connected areas (including area 0). So it would work.
upvoted 2 times

jjeans 1 year ago
No, outbound direction is NOT correct.

CISCOs definition of that command is:
Router(config-router)# area <area-id> filter-list prefix <prefix-list-name> in
>> Configures the router to filter interarea routes INTO the specified area.

You are arguing with device direction view you know from ACLs, but filter-lists have area direction views, which are different. So INBOUND direction is correct.
upvoted 4 times

Amoako Highly Voted 1 year, 1 month ago
The correct answer it´s "C"

Tested this in eve-ng.

=== ON R7=====
ip prefix-list BLOCK seq 5 deny 6.6.6.6/32
ip prefix-list BLOCK seq 10 permit 0.0.0.0/0 le 32
router ospf 1
area 2 filter-list prefix BLOCK in

=== ON R3=====
ip prefix-list BLOCK seq 5 deny 6.6.6.6/32
ip prefix-list BLOCK seq 10 permit 0.0.0.0/0 le 32
router ospf 1
area 3 filter-list prefix BLOCK in
upvoted 16 times

Ablovi Most Recent 1 week, 6 days ago
Outbound will also prevent routers in area 0 to learn LSA type 3
Inbound will prevent only the targeted area to learn that LSA type 3.
!
ip prefix-list FILTER_R6_Lo0 deny 6.6.6.6/32
ip prefix-list FILTER_R6_Lo0 permit 0.0.0.0/0 le 32
!
router ospf 1
area 2 filter-list prefix FILTER_R6_Lo0 in
area 3 filter-list prefix FILTER_R6_Lo0 in
!
I meant C is the best answer.
upvoted 1 times

Ablovi 1 week, 6 days ago
Outbound will also prevent routers in area 0 to learn LSA type 3
Inbound will prevent only the targeted area to learn that LSA type 3.
!
ip prefix-list FILTER_R6_Lo0 deny 6.6.6.6/32
ip prefix-list FILTER_R6_Lo0 permit 0.0.0.0/0 le 32
!
router ospf 1
area 2 filter-list prefix FILTER_R6_Lo0 in
area 3 filter-list prefix FILTER_R6_Lo0 in
!
So A is the best answer.
upvoted 1 times

Ablovi 1 week, 6 days ago
Please Ignore
upvoted 1 times

Ablovi 1 week, 6 days ago
From Cisco training source:
To configure Type-3 LSA filtering, use the area area-number filter-list prefix prefix-list-name in | out command under OSPF configuration mode. The referenced prefix list is used to match the subnets and masks to be filtered. The area-number and the in | out option of the area filter-list command work together, as follows:
When out is configured, IOS filters prefixes coming out of the configured area.
When in is configured, IOS filters prefixes going into the configured area.
upvoted 1 times

blueblue2 2 months, 1 week ago

Selected Answer: C

R7
ip prefix-list FILTRO seq 5 deny 6.6.6.6/32
ip prefix-list FILTRO seq 10 permit 0.0.0.0/0 le 32

router ospf 1
area 2 filter-list prefix FILTRO in

R3
ip prefix-list FILTRO seq 5 deny 6.6.6.6/32
ip prefix-list FILTRO seq 10 permit 0.0.0.0/0 le 32

router ospf 1
area 3 filter-list prefix FILTRO in

upvoted 1 times

djedeen 3 months, 1 week ago

Selected Answer: C

Only on ABRs, and only for LSA T3
'in' filters LSA type 3 into an area
'out' filters LSA type 3 out of an area

upvoted 1 times

PureInertiaCopy 3 months, 2 weeks ago

To prevent the R6 loopback from getting into Area 2 and Area 3 from Area 0, the engineer should apply a filter list inbound on R3 and R7. This will filter out the routes coming from R6's loopback interface and prevent them from being advertised into Area 2 and Area 3.

So, the correct answer is:

C. Apply a filter list inbound on R3 and R7.

upvoted 2 times

PureInertiaCopy 3 months, 2 weeks ago

My mistake. This is incorrect. The answer is A.

upvoted 1 times

ihateciscoreally 3 months, 2 weeks ago

filtering traffic in OSPF is inverted ACLs:

inbound -> TO area
outbound -> FROM area

so when you apply prefix-list "area 2 filter-list prefix BLOCK in" (@Amoako) it means: filter traffic TO area 2.

upvoted 1 times

ihateciscoreally 3 months, 2 weeks ago

thus answer should be C!

upvoted 1 times

[Removed] 4 months, 4 weeks ago

Selected Answer: C

This one is tricky if you don't understand the logic of Filter-Lists in OSPF.
In a nutshell, a Filter-List can only be applied at the ABRs to filter TYPE 3 LSAs, so this immediately indicates you can only apply the filter list at R7 and/or R3.
Now, the direction of the filter list is very important to understand. Let's take an example configuration:

area 2 filter-list prefix DENY [in | out]

Here we use area 2 as an example, and we have referenced a prefix-list named DENY. Now, we have two options for directions, INBOUND and OUTBOUND.

The IN keyword states that we will filter prefixes based on the prefix-list referenced towards the area identified in the command. Meaning that TYPE 3 LSAs going to Area 2 will be filtered based on the prefix-list.

Inversely, if we used OUT, it means that TYPE 3 LSAs coming FROM Area 2 will be filtered based on the prefix-list.

upvoted 5 times

rogi2023 4 months, 1 week ago

very clear explanation from hugodiaz as alwasys !!

upvoted 1 times

rogi2023 4 months, 1 week ago

on R7 you are referencing Area2 and therefore filter list IN
on R3 you are referencing Area3 and therefore filter list IN

upvoted 1 times

msstanick 5 months, 3 weeks ago

Selected Answer: C

It is C, not A.

I made the same mistake in the first place. Applying route filtering in OSPF is not like applying ACLs. In fact, it works the other way around. You must think from the ABR perspective that is - what LSAs should I pass from area 0 into area 1 or 3? This is why it has to be IN, not OUT.

upvoted 4 times

HamzaBadar 7 months, 4 weeks ago

Confirmed in GNS3, it will work in only inbound on area 2 not outbound on area 0. C is correct.

upvoted 3 times

Jack2002 7 months, 4 weeks ago

Selected Answer: C

Inbound for filter lists is correct, because we filter route from entering an Area.
FIlter-lists are related to areas, not devices.

upvoted 2 times

DavideDL 8 months ago

Selected Answer: C

I think we all agree with both A anc C produce the correct result.

I'll just focus on the words "prevent the R6 loopback from getting into Area 2 and Area 3".
If we filter out area 0 we will filter R6 loopback for every future new area , instead we need to filter only for Area2 and Area3.
In this case It's more appropriate to filter inbound on Area 2 and Area 3.

upvoted 3 times

rami_mma 8 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

JackDRipper 8 months, 1 week ago

The wording is terrible. In human-speak, you want it filtered outbound from R3/R7 (that's in Area 0) to Areas 2 and 3. But the command to do it is "... IN", on R3/R7 to Areas 2 and 3. Seems like a toss between A & C, depending on what the author was thinking at the time this question was written.

upvoted 1 times

olaniyijt 9 months, 2 weeks ago

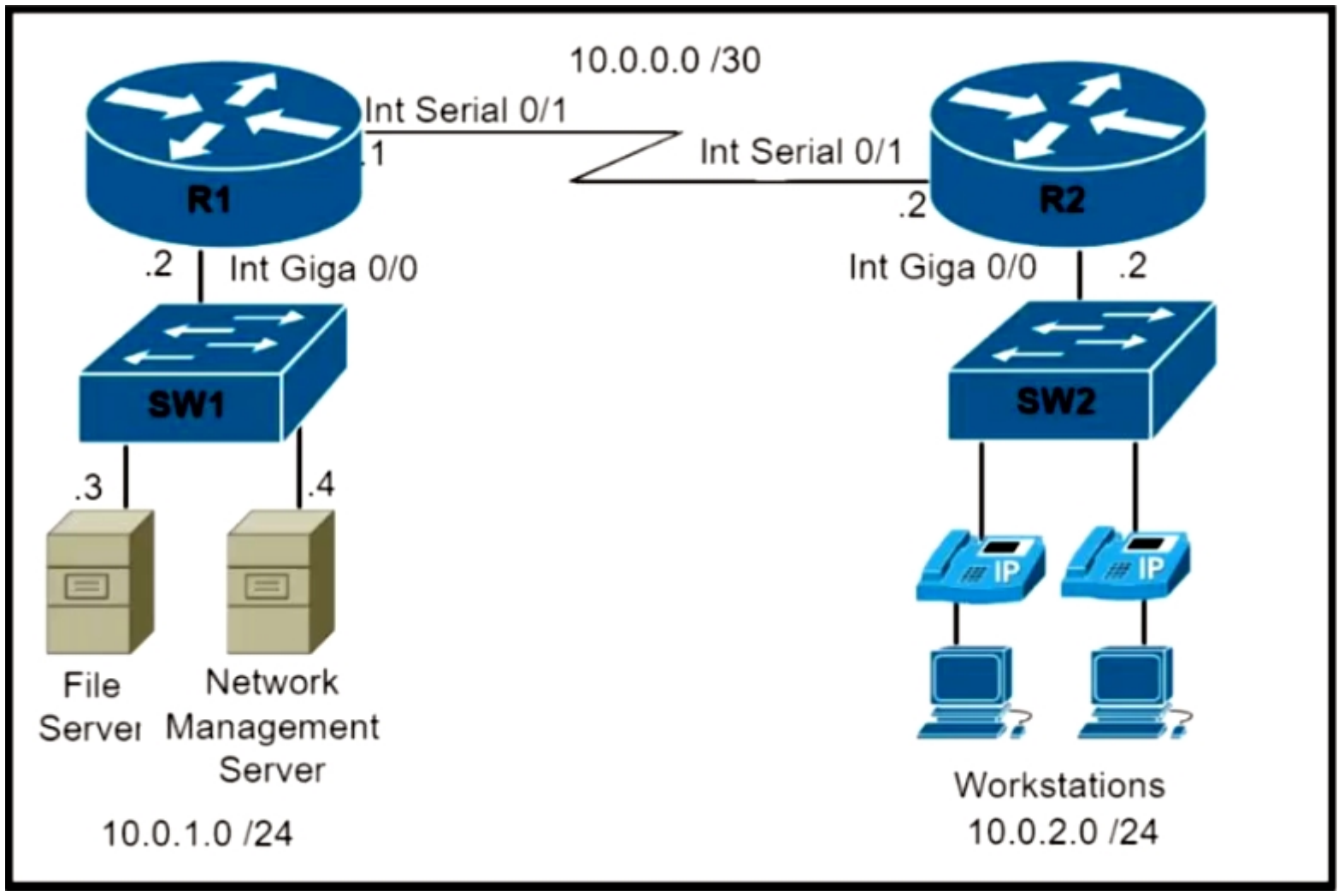
C is correct.

When applying a filter-list inbound to a particular non-transit area, it literally is used to stop that area receiving the prefix.

https://ccieblog.co.uk/ospf/ospf-filter-lists

upvoted 1 times

Question #463 *Topic 1*



An engineer must configure and validate a CoPP policy that allows the network management server to monitor router R1 via SNMP while protecting the control plane. Which two commands or command sets must be used? (Choose two.)

A. access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp access-list 150 permit udp 10.0.1.4 0.0.0.0 eq snmp host 10.0.1.2 class-map match-all CoPP-management match access-group 150 policy-map CoPP-policy class CoPP-management police 8000 conform-action transmit exceed-action transmit violate-action drop control-plane Service-policy input CoPP-policy

B. show ip interface brief

C. show quality-of-service-profile

D. access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp class-map match-all CoPP-management match access-group 150 policy-map CoPP-policy class CoPP-management police 8000 conform-action transmit exceed-action transmit violate-action transmit control-plane Service-policy input CoPP-policy

E. show policy-map control-plane

Correct Answer: *AE*

Community vote distribution

AE (67%) DE (33%)

dragonwise Highly Voted 8 months ago

A.
access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp
access-list 150 permit udp 10.0.1.4 0.0.0.0 eq snmp host 10.0.1.2
class-map match-all CoPP-management
match access-group 150
policy-map CoPP-policy
class CoPP-management
police 8000 conform-action transmit exceed-action transmit violate-action drop
control-plane Service-policy input CoPP-policy

B.
show ip interface brief

C.
show quality-of-service-profile

D.
access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp
class-map match-all CoPP-management
match access-group 150
policy-map CoPP-policy

class CoPP-management
police 8000 conform-action transmit exceed-action transmit violate-action transmit
control-plane Service-policy input CoPP-policy

E.
show policy-map control-plane
upvoted 8 times

Rose66 Most Recent 10 months, 2 weeks ago

Selected Answer: AE

A has "It has violate-action drop"
upvoted 3 times

markymark874 10 months, 4 weeks ago

Selected Answer: AE

Since question says needs to protect, so A is the answer. It has violate-action drop.
upvoted 3 times

forccnp 11 months, 2 weeks ago

Selected Answer: DE

It should be D and E
upvoted 3 times

PS5 1 year ago

SNMP is management plane so surely it should be D and E ??
upvoted 1 times

Wrad 11 months, 1 week ago

But D only has "transmit" statements, so not much of a protection.
E is only a show command and the question is for "must configure" so also not a perfect match, but maybe the best of the options.
upvoted 1 times

Feliphus 11 months, 3 weeks ago

I think is D and E as well
A option has this ACL 150:
access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp
access-list 150 permit udp 10.0.1.4 0.0.0.0 eq snmp host 10.0.1.2
But D option only:
access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp
A option has a violation-action drop, but D option has a violation-action transmit
the SNMP traffic will be never dropped
upvoted 1 times

rmonteroherrera 2 months, 2 weeks ago

So, ACL would not be dropping traffic by its implicit deny? Would not the violate-action drop be applied only for the police 8000? Besides, Option A ACL second line does not make much of a sense having snmp polling permitted on to a server IMO.
upvoted 1 times

RexChen 1 year ago

why not DE?
upvoted 1 times

Zizu007 1 year ago

A - violation-action drop
D - violation-action transmit
upvoted 2 times

fernandocirino 1 year ago

Correct answer is A and E

access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp
access-list 150 permit udp 10.0.1.4 0.0.0.0 eq snmp host 10.0.1.2

class-map match-all CoPP-management
match access-group 150
!
!
policy-map CoPP-policy
class CoPP-management
police 8000 conform-action transmit exceed-action transmit violate-action drop

!
control-plane
service-policy input CoPP-policy
upvoted 3 times

Question #464 *Topic 1*

A vulnerability assessment highlighted that remote access to the switches is permitted using unsecure and unencrypted protocols. Which configuration must be applied to allow only secure and reliable remote access for device administration?

A. line vty 0 15 login local transport input all

B. line vty 0 15 login local transport input ssh

C. line vty 0 15 login local transport input telnet ssh

D. line vty 0 15 login local transport input none

Correct Answer: *B*

Community vote distribution

B (100%)

eddgg 3 months, 3 weeks ago

Selected Answer: B

correct b, ssh is secure and reliable

upvoted 1 times

bora4motion 1 year ago

Selected Answer: B

b is correct

upvoted 3 times

Dataset 8 months, 1 week ago

Hi ! why is correct?
regards

upvoted 1 times

IvAlAx 7 months, 2 weeks ago

beacause telnet send data in clear text.

upvoted 1 times

Question #465 *Topic 1*

Which feature is used to propagate ARP, broadcast, and link-local frames across a Cisco SD-Access fabric to address connectivity needs for silent hosts that require reception of traffic to start communicating?

A. Multisite Fabric

B. Native Fabric Multicast

C. SDA Transit

D. Layer 2 Flooding

Correct Answer: *D*

Community vote distribution

D (88%) 13%

kewokil120 Highly Voted 10 months, 4 weeks ago

Selected Answer: D

https://community.cisco.com/t5/networking-knowledge-base/cisco-sd-access-layer2-flooding/ta-p/3943916

upvoted 7 times

Summo Highly Voted 1 year, 1 month ago

https://www.youtube.com/watch?v=KaUAqRw9Whw

upvoted 6 times

sam6996 Most Recent 4 months, 3 weeks ago

Given answer is correct, this is also a good reference,
https://www.linkedin.com/pulse/cisco-sd-access-silent-hosts-better-solution-andreas-b%C3%A6kdahl/

upvoted 1 times

Muste 6 months, 1 week ago

Selected Answer: B

Native Fabric Multicast is the feature used to propagate ARP, broadcast, and link-local frames across a Cisco SD-Access fabric to address connectivity needs for silent hosts. It ensures that these types of frames are distributed to all the necessary endpoints in the fabric, including the silent hosts, allowing them to receive the required traffic and initiate communication.

upvoted 1 times

Muste 6 months, 1 week ago

sorry please disregard this definition it's from chatgpt and i just realised it's reliable

upvoted 3 times

Question #466 *Topic 1*

Which function does a fabric wireless LAN controller perform in a Cisco SD-Access deployment?

A. manages fabric-enabled APs and forwards client registration and roaming information to the Control Plane Node

B. coordinates configuration of autonomous nonfabric access points within the fabric

C. performs the assurance engine role for both wired and wireless clients

D. is dedicated to onboard clients in fabric-enabled and nonfabric-enabled APs within the fabric

Correct Answer: *A*

Community vote distribution

A (100%)

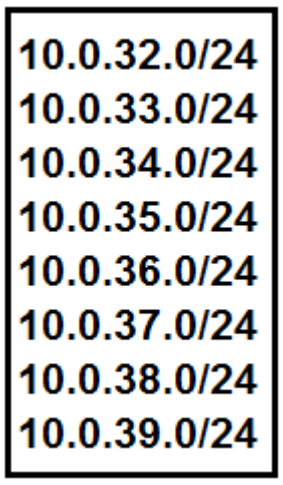
AndreasThornus Highly Voted 11 months, 2 weeks ago

Selected Answer: A

From: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#FabricWLC

Both fabric WLCs and non-fabric WLCs provide AP image and configuration management, client session management, and mobility services. Fabric WLCs provide additional services for fabric integration such as registering MAC addresses of wireless clients into the host tracking database of the fabric control plane nodes during wireless client join events and supplying fabric edge node RLOC-association updates to the HTDB during client roam events.

upvoted 5 times



Refer to the exhibit. An engineer must permit traffic from these networks and block all other traffic. An informational log message should be triggered when traffic enters from these prefixes. Which access list must be used?

A. access-list acl_subnets permit ip 10.0.32.0 0.0.7.255 access-list acl_subnets deny ip any log

B. access-list acl_subnets permit ip 10.0.32.0 255.255.248.0 log

C. access-list acl_subnets permit ip 10.0.32.0 0.0.7.255 log

D. access-list acl_subnets permit ip 10.0.32.0 0.0.0.255 log

Correct Answer: *C*

Community vote distribution

C (100%)

PureInertiaCopy 3 months, 2 weeks ago

There is an "implicit deny" at the end of accesslist . If you do not specify an ACE (Access Control Entry) "permit ip any any" at the end of the ACL then it will deny everything that doesn't match the initial ACEs.

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

0.0.0.255 is wildcard of 255.255.255.0 and we will need to aggregate IP's in this case so it can't be 0.0.0.255 for sure since we are talking about multiple /24 subnets

upvoted 1 times

x3rox 9 months, 1 week ago

A - WRONG
First line is missing an 'any'
C - is correct, as the implicit deny rule takes cares of the rest of the subnets as per requirements.

upvoted 2 times

snarkymark 9 months, 2 weeks ago

Selected Answer: C

C is correct because A does not have "log" applied to the first line, which is a requirement.
An implicit deny takes care of C.
https://community.cisco.com/t5/routing/is-deny-any-default-at-the-end-for-all-access-lists-created/td-p/4092573

upvoted 2 times

```
>>> netconf_data[“GigabitEthernet”][0][“enabled”]
u’false’
>>> netconf_data[“GigabitEthernet”][1][“enabled"]
u’true’
>>> netconf_data[“GigabitEthernet”][2][“enabled”]
u’false’
>>> netconf_data[“GigabitEthernet”[0][“description”]
u’my description’
```

Refer to the exhibit. Which Python code snippet prints the descriptions of disabled interfaces only?

A.

```
for interface in netconf_data[“GigabitEthernet”]:
        if interface[“enabled”] != ‘false’:
                print(interface[“description”])
```

B.

```
for interface in netconf_data[“GigabitEthernet”]:
        if interface[“enabled”] != ‘true’:
                print(interface[“description”])
```

C.

```
for interface in netconf_data[“GigabitEthernet”]:
        if interface[“disabled”] != ‘true’:
        print(interface[“description”])
```

D.

```
for interface in netconf_data[“GigabitEthernet”]:
        print(interface[“enabled”])
        print(interface[“description”])
```

Correct Answer: *B*

Alberht Highly Voted 1 year, 2 months ago

!= is the "Is not true operator" think along these lines and B is clarly correct.

upvoted 16 times

spamgayy Most Recent 6 months, 3 weeks ago

Answer is B

upvoted 1 times

Clauster 8 months, 2 weeks ago

Answer is Clearly C

upvoted 1 times

Clauster 8 months, 1 week ago

Answer is B, my apologies i wish we could change our answers

upvoted 4 times

Brand 9 months, 3 weeks ago

Am I the only one who thinks the question is asking "description of disabled interfaces only" and sees the answer B has "if interface enabled = true"? Or am I missing something here.

upvoted 4 times

olaniyijt 9 months, 2 weeks ago

B seems to be the most correct answer.

Consider the != operator which simply means "not true".
If "enabled" is not true, then it means the interface is disabled.

upvoted 6 times

straightAnswers 8 months, 2 weeks ago

Thanks

upvoted 2 times

kewokil120 10 months, 4 weeks ago

B is the answer.

upvoted 2 times

Question #469 *Topic 1*

Which measure is used by an NTP server to indicate its closeness to the authoritative time source?

A. stratum

B. time zone

C. latency

D. hop count

Correct Answer: *A*

Community vote distribution

A (100%)

kewokil120 10 months, 4 weeks ago

Selected Answer: A

A is correct

upvoted 2 times

bora4motion 1 year ago

Selected Answer: A

A is correct

upvoted 1 times

Radwa_ 1 year, 1 month ago

Selected Answer: A

NTP uses a stratum to describe the distance between a network device and an authoritative time source: A stratum 1 time server is directly attached to an authoritative time source (such as a radio or atomic clock or a GPS time source)

upvoted 1 times

Question #470 *Topic 1*

When is the Design workflow used in Cisco DNA Center?

A. in a greenfield deployment, with no existing infrastructure

B. in a greenfield or brownfield deployment, to wipe out existing data

C. in a brownfield deployment, to modify configuration of existing devices in the network

D. in a brownfield deployment, to provision and onboard new network devices

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/user_guide/b_cisco_dna_center_ug_2_1_2/b_cisco_dna_center_ug_2_1_1_chapter_0110.html

Community vote distribution

A (100%)

x3rox Highly Voted 10 months ago

Selected Answer: A

The Design area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. ---> Use the Design workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the Discovery feature.

upvoted 7 times

BenGuare 3 months, 1 week ago

Bit strange as if you wanted to update network settings for a brownfield site i'd go to Design (e.g. to update a logging destination). Thanks for the ref though.

upvoted 1 times

jzzmth Most Recent 11 months ago

Selected Answer: A

Provided answer and reference are correct.

upvoted 3 times

danman32 4 months ago

Reference no longer works

upvoted 1 times

Question #471 *Topic 1*

What are two characteristics of VXLAN? (Choose two)

A. It lacks support for host mobility.

B. It uses VTEPs to encapsulate and decapsulate frames.

C. It allows for up to 16 million VXLAN segments.

D. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay.

E. It has a 12-bit network identifier.

Correct Answer: *BC*

Community vote distribution

BC (100%)

kewokil120 10 months, 4 weeks ago

Selected Answer: BC

B and C are correct.

upvoted 2 times

Japsurd 1 year ago

B and C are correct.

upvoted 2 times

diamant 1 year, 1 month ago

Virtual eXtensible Local Area Network (VXLAN) is a tunneling protocol that tunnels Ethernet (layer 2) traffic over an IP (layer 3) network. Traditional layer 2 networks have issues because of three main reasons: Spanning-tree. Limited amount of VLANs. Large MAC address tables. Spanning-tree blocks any redundant links to avoid loops

The GRE tunnel runs on top of a physical underlay network. With VXLAN, the overlay is a layer 2 Ethernet network. The underlay network is a layer 3 IP network. Another name for the underlay network is a transport network. The underlay network is simple; its only job is to get packets from A to B.

upvoted 3 times

```
GigabitEthernet0/1 is up, line protocol is up
Internet Address 192.168.50.1/24, Area 0, Attached via Interface Enable
Process ID 1, Router ID 192.168.50.1/24, Network Type BROADCAST, Cost: 1
Topology-MTID   Cost     Disabled       Shutdown      Topology Name
      0          1          no             no            Base
Enabled by interface config, including secondary ip addresses
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.50.1, Interface address 192.168.50.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:07
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 1 msec, maximum is 1 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

Refer to the exhibit. An engineer configures OSPF and wants to verify the configuration. Which configuration is applied to this device?

A. R1(config)#interface Gi0/1 R1(config-if)#ip ospf enable R1(contig-if)#ip ospf network broadcast R1(config-if)#no shutdown

B. R1(config)#router ospf 1 R1(config-router)#network 0.0.0.0 0.0.0.0 area 0 R1(config-router)#no passive-interface Gi0/1

C. R1(config)#interface Gi0/1 R1(config-if)#ip ospf 1 area 0 R1(config-if)#no shutdown

D. R1(config)#router ospf 1 R1(config-router)#network 192.168.50.0 0.0.0.255 area 0

Correct Answer: *D*

Community vote distribution

C (93%) 7%

Deu_Inder Highly Voted 1 year, 2 months ago

Selected Answer: C

See the exhibit. It says "Attached via Interface Enable".

upvoted 12 times

[Removed] 4 months, 3 weeks ago

And if that wasn't enough, a little further down it says "Enabled by interface config"

upvoted 3 times

TSKARAN Highly Voted 10 months, 2 weeks ago

C is the correct answer

You can configure ospf two ways,

Under global config:
router osfp 1
network ip wildcard-mask >> Attached via Network Statement

Under interface:
inter gi0/2#ip ospf 1 area 0 >> Attached via Interface Enable

upvoted 6 times

wonkey Most Recent 2 months, 1 week ago

can anyone explain to me why not option A ? in exhibit it say network type Broadcast

upvoted 1 times

olaniyijt 7 months, 2 weeks ago

A.
R1(config)#interface Gi0/1
R1(config-if)#ip ospf enable
R1(contig-if)#ip ospf network broadcast

R1(config-if)#no shutdown

B.
R1(config)#router ospf 1
R1(config-router)#network 0.0.0.0 0.0.0.0 area 0
R1(config-router)#no passive-interface Gi0/1

C.
R1(config)#interface Gi0/1
R1(config-if)#ip ospf 1 area 0
R1(config-if)#no shutdown

D.
R1(config)#router ospf 1
R1(config-router)#network 192.168.50.0 0.0.0.255 area 0

upvoted 2 times

rami_mma 8 months, 1 week ago

Selected Answer: C

C is correct

upvoted 2 times

bendarkel 9 months, 3 weeks ago

Selected Answer: C

C is the correct answer. The "show osfp interface gig0/1" output clearly shows the process is enabled by interface config.

upvoted 4 times

kewokil120 10 months, 4 weeks ago

Selected Answer: C

Could go C or D. Since it a interface command. I say C as it refers to interface commands.

upvoted 1 times

nushadu 11 months, 1 week ago

Selected Answer: C

cisco_R3#show ip ospf interface ethernet 0/0.50
Ethernet0/0.50 is up, line protocol is up
Internet Address 10.111.10.1/30, Area 22, Attached via Interface Enable <<<<<<<<<<<<<
Process ID 1, Router ID 3.3.3.3, Network Type POINT_TO_POINT, Cost: 10
Topology-MTID Cost Disabled Shutdown Topology Name
0 10 no no Base
Enabled by interface config, including secondary ip addresses
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:00
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 5, maximum is 6
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 5.5.5.5
Suppress hello for 0 neighbor(s)
cisco_R3#

upvoted 1 times

nushadu 11 months, 1 week ago

cisco_R3#show runn interface ethernet 0/0.50
Building configuration...

Current configuration : 176 bytes
!
interface Ethernet0/0.50
encapsulation dot1Q 50
ip address 10.111.10.1 255.255.255.252
standby 40 ip 10.111.10.254
ip ospf network point-to-point
ip ospf 1 area 22
end

cisco_R3#show runn | s ospf
router ospf 1
area 22 filter-list prefix PL_3 in
passive-interface default
no passive-interface Ethernet0/0.10
no passive-interface Ethernet0/0.50
network 0.0.0.0 255.255.255.255 area 0
cisco_R3#

upvoted 1 times

nushadu 11 months, 1 week ago

cisco_R3#show runn interface ethernet 0/0.10
interface Ethernet0/0.10
description to_sw1
encapsulation dot1Q 10
ip address 192.168.255.3 255.255.255.0
end

cisco_R3#show ip ospf interface ethernet 0/0.10
Ethernet0/0.10 is up, line protocol is up
Internet Address 192.168.255.3/24, Area 0, Attached via Network Statement <<<<<<<<<<<<<<
Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10 <<<<<<<<<<<<
Topology-MTID Cost Disabled Shutdown Topology Name
0 10 no no Base
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 192.168.255.2, Interface address 192.168.255.2
Backup Designated router (ID) 3.3.3.3, Interface address 192.168.255.3
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:04
...
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.255.2 (Designated Router)
cisco_R3#

upvoted 1 times

Edwinmolinab 1 year ago

Selected Answer: C

This statement is Enabled by interface config

upvoted 3 times

H3kerman 1 year ago

Selected Answer: C

When you ue the "show ip ospf interface intx/x/x" command, what difference will you see in the old vs new OSPFv2 config?
- One will say attached via Interface Enable, the other will say Attached via Network Statement
https://www.chegg.com/flashcards/chapter-20-implementing-ospf-61b573b4-141b-4f63-bac9-ee35462d315e/deck

upvoted 1 times

Normanby 1 year ago

Sorry - I see it now: this interface has a secondary address , so have to use Network statement ???

upvoted 1 times

Normanby 1 year ago

Selected Answer: D

Once again a trick Q, or one based on other implied info.
I am guessing the only reason 'C' is wrong, is somewhere in this output is an indication that the interface has been 'up' for some time - so the 'no shutdown' command was not needed.....

upvoted 2 times

examtopicsacct 5 months, 3 weeks ago

You are missing the interface enable from the output

upvoted 1 times

Amoako 1 year, 1 month ago

Correct answer is C

upvoted 1 times

smithkeith0023366 1 year, 2 months ago

Selected Answer: C

Voting: C.

upvoted 2 times

Question #473 *Topic 1*

What is the function of a control-plane node in a Cisco SD-Access solution?

A. to run a mapping system that manages endpoint to network device relationships

B. to implement policies and communicate with networks outside the fabric

C. to connect external Layer 3 networks to the SD-Access fabric

D. to connect APs and wireless endpoints to the SD-Access fabric

Correct Answer: *A*

Community vote distribution

A (100%)

Dataset Highly Voted 10 months, 3 weeks ago

Selected Answer: A

"manages.." is the magic word

Regards

upvoted 5 times

jzzmth Most Recent 11 months ago

Provided answer is correct:
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#Control_Plane_Node

upvoted 3 times

Question #474 *Topic 1*

What is a characteristic of a Type 2 hypervisor?

A. It eliminates the need for an underlying operating system.

B. Problems in the base operating system can affect the entire system.

C. Its main task is to manage hardware resources between different operating systems.

D. It is completely independent of the operating system.

Correct Answer: *B*
Reference:
https://careerkaizen.com/vmware-interview-questions/

Community vote distribution
B (83%) A (17%)

HarwinderSekhon 5 months, 2 weeks ago
it was easy to answer but its crazy how cisco pulls test questions from other websites as opposed to OCG book lol.
upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago
I have my vSphere DCV-VCP6 and these questions slay me. This to me is not what CCNP should be about.
upvoted 1 times

TSKARAN 11 months ago
Eg: if you use Virtual Box or VMware workstation on top of Windows 10 or 11, when you get the issue in Windows OS, it will impact the hypervisor. (Type-2)
So, B is the correct answer.
upvoted 3 times

jstaruch 1 year, 1 month ago
Selected Answer: B
Type 2 It is completely dependent on Host Operating System for its operations. While having a base operating system allows better specification of policies, any problem in the base operating system affects the entire system even if the hypervisor running above the base OS is secure.
upvoted 3 times

dougj 1 year, 1 month ago
Selected Answer: B
Correct answer is B, a type 1 hypervisor is on a bare metal server, a type 2 relies on underlying software
upvoted 2 times

Wooker 1 year, 2 months ago
Selected Answer: A
correct answer is A
upvoted 1 times

xzckk 12 months ago
Type 2 needs an underlying operating system. So A is wrong
upvoted 3 times

Question #475 *Topic 1*

What is the purpose of a data modeling language?

A. to describe the structure and meaning of exchanged data

B. to standardize the procedures that are executed when parsing sent and received data

C. to establish a framework to process data by using an object-oriented programming approach

D. to specify the rules for transcoding between text and binary data encodings

Correct Answer: *C*

Community vote distribution

A (100%)

dougj Highly Voted 1 year, 1 month ago

Selected Answer: A

I think A is correct, not all data models are object oriented so C is wrong

upvoted 5 times

rami_mma Most Recent 8 months, 1 week ago

Selected Answer: A

meaning of exchanged data

upvoted 2 times

landgar 10 months, 1 week ago

Selected Answer: A

A is the correct one.
C: framework is incorrect

upvoted 3 times

Rose66 10 months, 2 weeks ago

Selected Answer: A

Data models can be implemented using numerous data representation and storage formats, including arrays, linked lists, stacks, and graphs (e.g hierarchical trees). The hierarchical tree is very efficient in representing repetitive and hierarchical data and is typically associated with routing or switching platform configurations. Therefore it is the most common data model format used for networking platforms.
(Source: https://developer.cisco.com/docs/nx-os/#!the-nature-of-data-models)

upvoted 2 times

ils9100 1 year, 1 month ago

You are not reading the question correctly, it's asking for the purpose!

upvoted 1 times

Radwa_ 1 year, 1 month ago

Selected Answer: A

Data models enable data to be easily structured, grouped, and replicated to represent information related to network devices, features, and solutions.

from:
https://developer.cisco.com/docs/nx-os/#!the-nature-of-data-models

upvoted 3 times

tckoon 1 year, 2 months ago

Selected Answer: A

Data modeling is the process of creating a visual representation of either a whole information system or parts of it to communicate connections between data points and structures

upvoted 2 times

Question #476 *Topic 1*

Which IPv4 packet field carries the QoS IP classification marking?

A. ID

B. TTL

C. FCS

D. ToS

Correct Answer: *D*

Community vote distribution

D (100%)

Radwa_ 1 year, 1 month ago

Selected Answer: D

What is used to perform QoS packet classification, the TOS field in the Layer 3 header

upvoted 2 times

Question #477 *Topic 1*

Which two solutions are used for backing up a Cisco DNA Center Assurance database? (Choose two.)

A. bare metal server

B. remote server

C. NFS share

D. local server

E. non-linux server

Correct Answer: *BC*

Community vote distribution

BC (100%)

kebkim Highly Voted 1 year, 1 month ago

B,C

Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name.To support Assurance data backups, the server must be a Linux-based NFS server that meets the following requirements: - Support NFS v4 and NFS v3. - Cisco DNA Center stores backup copies of Assurance data on an external NFS device and automation data on an external remote sync (rsync) target location. - The remote share for backing up an Assurance database (NDP) must be an NFS share.

upvoted 9 times

CKL_SG Most Recent 4 months, 3 weeks ago

Selected Answer: BC

Answer are correct b c

Url below mention using remote server and nfs server for backup and restore

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2/admin/b_dnac_admin_guide_1_2/b_dnac_admin_guide_1_2_chapter_0101.html.xml

upvoted 1 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: BC

B and C

Remote Server via SSH/Rsync

NFS with a file copy

Can be looked up here: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/admin_guide/b_cisco_dna_center_admin_guide_2_1_2/b_cisco_dna_center_admin_guide_2_1_1_chapter_0110.html

upvoted 3 times

GeorgeFortiGate 1 year ago

Selected Answer: BC

Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name.To support Assurance data backups, the server must be a Linux-based NFS server that meets the following requirements:– Support NFS v4 and NFS v3.– Cisco DNA Center stores backup copies of Assurance data on an external NFS device and automation data on an external remote sync (rsync) target location.– The remote share for backing up an Assurance database (NDP) must be an NFS share

upvoted 2 times

Lukaszaw 1 year, 2 months ago

A and C I think.

upvoted 3 times

```
R2#debug arp
ARP packet debugging is on
R2#show ip rap
Protocol Address  Age (min) Hardware Add Type Interface
internet 192.168.0.5   - ca02.099f.001d ARPA FastEthernet1/1
R2#show ip interface brief
Interface          IP-Address OK? Method Status     Protocol
FastElhermet0/0 unassigned   YES NVRAM     administratively down down
FastEthernet0/1  unassigned   YES NVRAM     administratively down down
FastEthernet1/0  unassigned   YES manual up         up
FastEthernet1/1  192.168.0.5  YES NVRAM up          up
Loopback0        10.0.0.2     YES NVRAM up          up
Loopback1        10.0.0.5     YES NVRAM up          up

R2#show ip route
Codes: C - connected, S- static, R - RIP, M - mobile, B - BGP
    D - EIGRP, EX-EIGRP external, Q- OSPF, IA- QSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2- IS-IS level-2
    ia - IS-IS inter area, * - candidate default, U – per-user static route
    o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/32 is subnetted, 2 subnets
C       10.0.0.2 is directly connected, Loopback0
C       10.0.0.5 is directly connected Loopback1
     192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.4 is directly connected, FastEthernet1/1

R2#
"Jan 17 16:49:46.083: IP ARP req filtered src 192.168.0.1 ca03.05a5.001d, dst 192.168.0.5
0000 0000 0000 wrong cable, interface FastEthernet1/1
"Jan 17 16:49:48.071: IP ARP req filtered src 192.168.0.1 ca03.05a5 001d, dst 192.168.0.5
0000.0000.0000 wrong cable, interface FastEtnemet1/1

***output omitted***
```

```
R3#debug arp
ARP packet debugging is on
R3#show ip rap
Protocol Address Age (min) Hardware Add Type Interface
Internet 192.168.0.1 - ca03.05a5.001d ARPA FastEthernet1/1
Internet 192.168.0.9 - ca03.05a5.001c ARPA FastEthernet1/0
R3#show ip interface brief
Interface              IP-Address    OK? Method Status      Protocol
FastEthernet0/0    unassigned       YES NVRAM     administratively down down
FastEthernet0/1    unassigned       YES NVRAM     administratively down down
FastEthernet1/0    192.168.0.9      YES NVRAM up             up
FastEthemet1/1     192.168.0.1      YES manual up            up
Loopback0          10.0.0.3         YES NVRAM up             up
R3#ping 192.168.0.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.5, timeout is 2 seconds:

000030: "Jan 17 16:49:45.879 IP ARP creating incomplete entry for 192.168.0.5 interface FastEthernet1/1
000031: "Jan 17 16:49:45.879 IP ARP sent req src 192.168.0.1 ca03.05a5.001d.
         dst 192.168.0.5 0000.0000.0000 FastEthernet1/1
         ***output omitted***
000035: "Jan 17 16:49:53.875: IP ARP: sent req src 192.168.0.1 ca03.05a5.001d.
         dst 192.168.0.5 0000.0000.0000 FastEthernet1/1.
Success rate is 0 percent (0/5)
R3#show ip rap
Protocol  Address        Age (min) Hardware Add Type Interface
Internet 192.168.0.1    - ca03.05a5.001d ARPA FastEthernet1/1
Internet 192 168.0.5    0 Incomplete ARPA
Internet 192 168.0.9    - ca03.05a5.001c ARPA FastEthernet1/0
R3# show ip route
Codes: C- connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX- EIGRP external, O - OSPF, IA- OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P- periodic downloaded static route

Gateway of last resort is not set

   10.0.0.0/32 is subnetted, 1 subnets
C     10.0.0.3 is directly connected, Loopback0
   192.168 0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.8/30 is directly connected, FastEthernet1/0
C       192.168.0.0/29 is directly connected, FastEthernet1/1
```

Refer to the exhibit. Communication between R2 and R3 over FastEthenet1/1 falls. What is the root cause of the failure?

A. The subnet mask is different between the two interfaces.

B. The interface of R3 is not operational.

C. The wrong type of cable is connected between the two interfaces.

D. IP CEF is disabled on R3.

Correct Answer: *A*

Community vote distribution

A (100%)

Deu_Inder Highly Voted 1 year, 2 months ago

Selected Answer: A

Provided answer is correct.
I tested this in GNS3. Kept the subnet mask on one side /30 and the other side /29. Got on one side debug outputs:
*Sep 8 22:58:38.295: IP ARP req filtered src 10.10.12.1 ca01.37c4.0000, dst 10.10.12.5 0000.0000.0000 wrong cable, interface FastEthernet0/0
And the other side:
*Sep 8 22:58:37.747: IP ARP: creating incomplete entry for IP address: 10.10.12.5 interface FastEthernet0/0

The output with wrong cable is misleading.

upvoted 12 times

nushadu Most Recent 11 months, 1 week ago

Selected Answer: A

```
!
interface Ethernet0/0.70
encapsulation dot1Q 70
ip address 10.111.12.6 255.255.255.248
end

cisco_R5#ping 10.111.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.111.12.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
cisco_R5#show ip arp
```

Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.111.10.1 194 aabb.cc00.3000 ARPA Ethernet0/0.50
Internet 10.111.10.2 - aabb.cc00.5000 ARPA Ethernet0/0.50
Internet 10.111.12.1 0 Incomplete ARPA <<<<<<<<<<<<<<<<<<<<<<<<<<
Internet 10.111.12.6 - aabb.cc00.5000 ARPA Ethernet0/0.70
Internet 192.168.255.2 126 aabb.cc80.1000 ARPA Ethernet0/0.10
Internet 192.168.255.3 192 aabb.cc00.3000 ARPA Ethernet0/0.10
Internet 192.168.255.22 195 aabb.cc00.2000 ARPA Ethernet0/0.10
Internet 192.168.255.55 - aabb.cc00.5000 ARPA Ethernet0/0.10
cisco_R5#

upvoted 1 times

nushadu 11 months, 1 week ago

far-end:

*Dec 22 19:01:02.395: IP ARP req filtered src 10.111.12.6 aabb.cc00.5000, dst 10.111.12.1 0000.0000.0000 wrong cable, interface Ethernet0/0
cisco_R3#
*Dec 22 19:01:04.400: IP ARP req filtered src 10.111.12.6 aabb.cc00.5000, dst 10.111.12.1 0000.0000.0000 wrong cable, interface Ethernet0/0
cisco_R3#
*Dec 22 19:01:06.404: IP ARP req filtered src 10.111.12.6 aabb.cc00.5000, dst 10.111.12.1 0000.0000.0000 wrong cable, interface Ethernet0/0
cisco_R3#
*Dec 22 19:01:08.406: IP ARP req filtered src 10.111.12.6 aabb.cc00.5000, dst 10.111.12.1 0000.0000.0000 wrong cable, interface Ethernet0/0
cisco_R3#
cisco_R3#show runn int e0/0.70
!
interface Ethernet0/0.70
encapsulation dot1Q 70
ip address 10.111.12.1 255.255.255.252
end

cisco_R3#

upvoted 2 times

Lukaszaw 1 year, 2 months ago

shouldn't be C?

upvoted 1 times

Question #479 *Topic 1*

What is one characteristic of the Cisco SD-Access control plane?

A. It allows host mobility only in the wireless network.

B. It is based on VXLAN technology.

C. Each router processes every possible destination and route.

D. It stores remote routes in a centralized database server.

Correct Answer: *D*

Community vote distribution

D (100%)

jstaruch Highly Voted 1 year, 1 month ago

Selected Answer: D

Instead of a typical traditional routing-based decision, the fabric devices query the control plane node to determine the routing locator associated with the destination address (EID-to-RLOC mapping) and use that RLOC information as the traffic destination. In case of a failure to resolve the destination routing locator, the traffic is sent to the default fabric border node. The response received from the control plane node is stored in the LISP map-cache, which is merged to the Cisco Express Forwarding (CEF) table and installed in hardware.

upvoted 6 times

dougj Highly Voted 1 year, 1 month ago

Selected Answer: D

Answer is D, it is describing the MAP Server

upvoted 5 times

[Removed] Most Recent 5 months, 1 week ago

Selected Answer: D

Here is a good process to eliminate the other options:

A- Wrong, it allows mobility through the fabric
B- Wrong, VXLAN is part of the data-plane, not the control-plane
C- Wrong, this would be unscalable, instead the routes are processed in a centralized manner
D- Correct.

upvoted 2 times

KOJJY 11 months, 3 weeks ago

Selected Answer: D

it's D for sure

upvoted 1 times

highmip 1 year, 1 month ago

Answer is C?

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

Bceause RLOC only process connected site and not each prefix. Control plane resolve that

upvoted 1 times

Question #480 *Topic 1*

A customer transitions a wired environment to a Cisco SD-Access solution. The customer does not want to integrate the wireless network with the fabric. Which wireless deployment approach enables the two systems to coexist and meets the customer requirement?

A. Deploy the wireless network over the top of the fabric.

B. Implement a Cisco DNA Center to manage the two networks.

C. Deploy a separate network for the wireless environment.

D. Deploy the APs in autonomous mode.

Correct Answer: *D*

Community vote distribution

A (100%)

siteoforigin Highly Voted 1 year, 2 months ago

Selected Answer: A

Looking at the SD-Access Design Considerations > Wireless Design Section:

SD-Access supports two options for integrating wireless access into the network. One option is to use traditional Cisco Unified Wireless Network (CUWN) local-mode configurations over-the-top as a non-native service. In this mode, the SD-Access fabric is simply a transport network for the wireless traffic, which can be useful during migrations to transport CAPWAP-tunneled endpoint traffic from the APs to the WLCs.

upvoted 9 times

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: A

Reference: https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf

upvoted 5 times

RREVECO 1 year, 2 months ago

THANKS!!!!
Cisco Unified Wireless Network wireless OTT
In this case traditional wireless is carried on top of the SD-Access fabric. This mode is important as a migration step for customers that decide to implement SD-Access first on the wired network and then plan the wireless integration.

upvoted 3 times

rami_mma Most Recent 8 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

snarkymark 10 months ago

A is correct:
Cisco Unified Wireless Network wireless OTT network design:
Option 2:
Another reason for deploying wireless OTT could be that customer doesn't want or cannot migrate to fabric for wireless. This might be because they have a majority of older APs (802.11n or older) that are not supported with SD-Access, or the customer might require a certification of the new WLC software required to run SD-Access Wireless (8.5and above), or the customer may simply want to leave the wireless "as is" and not touch it.

upvoted 1 times

echipbk 11 months ago

Selected Answer: A

The answer is A

upvoted 1 times

ils9100 1 year, 1 month ago

All good if they plan on integrating in the future, but doesn't the question state - the customer does not want to?

upvoted 2 times

AndreasThornus 11 months, 3 weeks ago

Then you deploy the Wireless Network over the top of the overlay network and it is oblivious to the SD-Access fabric. A is correct.

upvoted 2 times

Question #481 *Topic 1*

By default, which virtual MAC address does HSRP group 14 use?

A. 04:17:01:05:7c:0e

B. 00:05:0c:07:ac:14

C. 00:00:0c:07:ac:0e

D. 00:05:5e:19:0c:14

Correct Answer: *C*

Community vote distribution

C (100%)

[Removed] 5 months, 1 week ago

easiest way to convert decimal to hex, in case you aren't familiar with:

Take the decimal number, in this case 14
Divide by 16, ie 14/16
Notice 14 does not divide by 16 evenly, the quotient is 0 with a remainder of 14
So we have 14/16=0R14, where R means Remainder
Convert the Remainder decimal 14 to Hex using our handy memory table 0-9,ABCDEF
We have 0E as the answer, because 14 in Hex is E and, well we have a quotien of 0 prior to it
If the decimal was 16 and we divided by 16, the we would have 16/16 = 1R0 = 0x10 Hex

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Very complicated.

Easiest way is this

14 = 00001110 in binary (8 bits)

Break up those 8 bits into 2 sections of 4 bits

= 0000 and 1110

now convert that back to decimal

0 and 14

now convert those to hex
0 = 0
14=E

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

0 0
1 1
2 2
3 3
4 4
5 5
6 6
7 7
8 8
9 9
10 A
11 B
12 C
13 D
14 E
So 0E

upvoted 1 times

nushadu 11 months, 4 weeks ago

hex(14)
Out[2]: '0xe'

upvoted 2 times

Joseph123 1 year, 2 months ago

Selected Answer: C

Given answer is correct
upvoted 3 times

Question #482 *Topic 1*

Which LISP component decapsulates messages and forwards them to the map server responsible for the egress tunnel routers?

A. Router Locator

B. Map Resolver

C. Proxy ETR

D. Ingress Tunnel Router

Correct Answer: *B*

Community vote distribution

B (100%)

kebkim Highly Voted 1 year, 2 months ago

The function of the LISP MR is to accept encapsulated Map-Request messages from ingress tunnel routers (ITRs), decapsulate those messages, and then forward the messages to the MS responsible for the egress tunnel routers (ETRs) that are authoritative for the requested EIDs.

upvoted 9 times

PureInertiaCopy Most Recent 3 months, 2 weeks ago

Selected Answer: B

LISP Map Resolver
Like an MS, a LISP MR connects to the ALT. The function of the LISP MR is to accept encapsulated Map-Request messages from ingress tunnel routers (ITRs), decapsulate those messages, and then forward the messages to the MS responsible for the egress tunnel routers (ETRs) that are authoritative for the requested EIDs.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html#GUID-89BB8D34-63BF-43DE-8743-5572D357CDB3

upvoted 1 times

[Removed] 5 months, 1 week ago

Selected Answer: B

Correct

upvoted 1 times

well123 9 months ago

Selected Answer: B

provided answer is correct

upvoted 2 times

Darude 1 year ago

Selected Answer: B

reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.pdf

upvoted 2 times

[Removed] 5 months, 1 week ago

Word for word.

upvoted 1 times

Question #483 *Topic 1*

An engineer must design a wireless network for a school system based on these requirements:

☞ The network must be able to triangulate client location based on RSSI.

☞ Each client must be able to sustain 5 Mbps of throughput at all times.

☞ Each classroom has up to 30 clients.

☞ Primary coverage is 5 GHz.

Which design should be used?

A. Place APs in a grid orientation throughout the building, located as close as possible to the center of each classroom.

B. Mount one AP in the center of each classroom.

C. Space APs evenly on both sides of the hallways.

D. Place APs near exterior walls and corners of the building, and fill in the center area with a staggered pattern.

Correct Answer: *D*

Community vote distribution

D (70%) A (30%)

Joseph123 Highly Voted 1 year, 2 months ago

Doesnt A feel like the better choice for this?

upvoted 16 times

wdp Highly Voted 10 months ago

In real life you would do a site survey :-)

upvoted 15 times

felix_simon Most Recent 5 months, 2 weeks ago

Selected Answer: A

Although six APs with a minimum data rate of 2 Mbps might adequately service an area, it might take twice as many APs to support a minimum data rate of 5 Mbps.

https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/RFDesign.html

upvoted 1 times

rami_mma 8 months, 1 week ago

Selected Answer: A

I would choose A, it is much better design than D.

upvoted 1 times

DavideDL 8 months, 1 week ago

Selected Answer: D

For a location management deployment, the APs are laid out in a staggered pattern. Figure 3-5 shows a typical pattern. The staggered pattern allows for more accurate estimation of the location of a device.

https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/RFDesign.html

upvoted 7 times

kewokil120 10 months, 4 weeks ago

Selected Answer: D

I think D will have better location.

upvoted 1 times

jzzmth 11 months ago

Selected Answer: D

I'm going with D because that seems to be the best design for triangulation.

upvoted 3 times

AlexEMedeiros 11 months, 1 week ago

Selected Answer: A

I go with A, because we're are dealing w/ 5Ghz

upvoted 2 times

Ciscopass 11 months, 2 weeks ago

Selected Answer: D

I am leaning towards F because it says: ... and fill in the center area with a staggered pattern.
So you have the AP's near the wall and ALSO in the center.

upvoted 1 times

AndreasThornus 12 months ago

I can't find an official Cisco source but the design best practice methods listed here "https://wlanprofessionals.com/wireless-design-principles-and-best-practices/" would suggest D.

"If deploying Real Time Location System (RTLS), remember the AP placement differs from a data or voice WLANs. With RTLS grade wireless, APs are to be installed within and in the perimeters of the coverage area to form a triangulation pattern. A client device must be heard by at least 3 nearby APs to calculate an accurate location. The more APs hearing a client the better for accuracy and redundancy purposes."

upvoted 2 times

bora4motion 1 year ago

Selected Answer: A

I'm going with A. It's just stupid to install WAPs right next to a wall.

upvoted 2 times

PeterTheCheater 1 year ago

Selected Answer: D

We need location, APs must be placed aroung the perimeter

upvoted 1 times

bora4motion 1 year ago

Clearly you don't do wireless design.

upvoted 4 times

Normanby 1 year ago

But, lets be honest: One in the center of each classroom is SO much easier deployment, and for location tracking, you know what classroom it is in, so just walk down there and stand in the doorway - you will see who the 'naughty' client is in 2 seconds !

upvoted 2 times

Normanby 1 year ago

Selected Answer: D

I have seen this at many conferences and webinars - If triangulation is an important factor: line the perimeter with APs (with flat panel antennas). In fact next time you are at Cisco Live, you will see this design all around the perimeter of the venue...

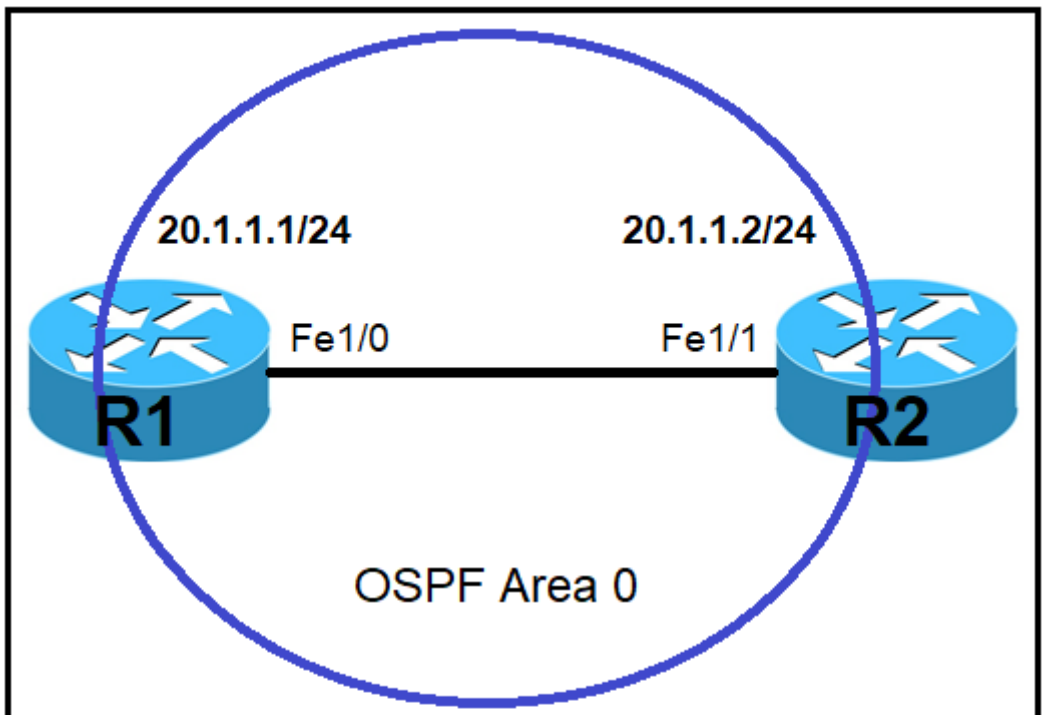
upvoted 3 times

Darude 1 year ago

Selected Answer: A

The best practice is to NOT place APs near exterior walls and corners and Hallways of the building! and to triangulate client location we need many APs. I go for A
reference:https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Wi-Fi-Cloud/deploy/deployment_best-practices_device-channel.html

upvoted 2 times




```
hostname R1
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
auto-cost reference-bandwidth 1000
!
hostname R2
router ospf 2
network 20.0.0.0 0.0.0.255 area 0
```

Refer to the exhibit. Which command must be applied to R2 for an OSPF neighborship to form?

A. network 20.1.1.0 0.0.0.0 area 0

B. network 20.1.1.2 0.0.0.0 area 0

C. network 20.0.0.2 0.0.0.3 area 0

D. network 20.0.0.2 0.0.0.0 area 0

Correct Answer: *B*

Community vote distribution

B (73%) A (27%)

adrian0792 5 months, 2 weeks ago

Selected Answer: B

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

Selected Answer: B

You regularly think about /30 networks and here you need to know 32 bit single IP can turn on OSPF and other side is accepting 0.0.0.0 any network.

upvoted 1 times

PKamato 7 months, 1 week ago

Selected Answer: A

Please guys and gals, read carefully

upvoted 1 times

PKamato 7 months, 1 week ago

oops typo, its B, ignore my first comment

upvoted 2 times

dragonwise 8 months ago

why in the world would any one apply this kind of configuration?

upvoted 4 times

mgiuseppe86 2 months, 2 weeks ago

Actually, I put the concept of B into practice on hundreds of routers where i configure OSPF.
I actually hate doing blanket ospf network configs that cover /24s and such. doing network x.x.x.x 0.0.0.0 area Y is actually safer and best practice.

Think about if you have multiple 10.x.x.x networks that are subnetted 50 ways to sunday and you make a new 10.x.x.x network on that router, all of a sudden its now part of OSPF. F that bro, if i want it a part of OSPf, ill add the network statement to my router config with the 0.0.0.0 wildcard mask.

upvoted 1 times

bendarkel 1 year ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

attiko 1 year ago

Selected Answer: B

Confirmed by test in my lab:

R1#sh run | sec ospf
router ospf 1
log-adjacency-changes
auto-cost reference-bandwidth 1000
network 0.0.0.0 255.255.255.255 area 0

R2#sh run | sec ospf
router ospf 2
log-adjacency-changes
network 20.0.0.0 0.0.0.255 area 0
network 20.1.1.2 0.0.0.0 area 0
R2#
R2#
R2#
R2#sh ip os nei

Neighbor ID Pri State Dead Time Address Interface
20.1.1.1 1 FULL/DR 00:00:32 20.1.1.1 GigabitEthernet0/0
R2#

upvoted 4 times

whatthewhat 1 year, 1 month ago

Selected Answer: A

A - the network statement matches the subnet

upvoted 1 times

bendarkel 1 year ago

You cannot use the network statement and specify the subnet wildcard with all zeros.

upvoted 6 times

dougj 1 year, 1 month ago

Selected Answer: B

B looks to be best answer

upvoted 2 times

jdholmes423 1 year, 1 month ago

Selected Answer: A

I vote option A because option B is an IP address and not a network. Every choice here has the 'network' keyword.

upvoted 1 times

bora4motion 11 months, 4 weeks ago

OSPF will still be down. You can't advertise the network address with a wild card of 0.0.0.0
B is the correct answer and will bring OSPF up.

upvoted 2 times

BryCR 1 year, 1 month ago

B is a good option, it is referring to a network /32, which a network of one single IP address, so, OSPF will be tried it neighboring on network 20.1.1.2/32

upvoted 1 times

Question #485 *Topic 1*

What is one characteristic of VXLAN?

A. It supports a maximum of 4096 VLANs

B. It supports multitenant segments

C. It uses STP to prevent loops in the underlay network

D. It uses the Layer 2 header to transfer packets through the network underlay

Correct Answer: *B*

Azmanforlife 2 months, 2 weeks ago

Seems like all the answer are correct:

What is one characteristic of VXLAN? It supports a maximum of 4096 VLANs. It supports multitenant segments. It uses STP to prevent loops in the underlay network. It uses the Layer 2 header to transfer packets through the network underlay.

upvoted 1 times

Azmanforlife 2 months, 2 weeks ago

PIs ignore.

upvoted 1 times

Stylar 10 months ago

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/pf/configuration/guide/b-pf-configuration/b-pf-configuration_chapter_01011.pdf

upvoted 3 times

jucevabe 1 year, 2 months ago

Correct

upvoted 3 times

Question #486 *Topic 1*

What is the function of vBond in a Cisco SD-WAN deployment?

A. initiating connections with SD-WAN routers automatically

B. pushing of configuration toward SD-WAN routers

C. onboarding of SD-WAN routers into the SD-WAN overlay

D. gathering telemetry data from SD-WAN routers

Correct Answer: *A*

Community vote distribution

C (84%) A (16%)

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: C

Orchestration plane (vBond) assists in securely onboarding the SD-WAN WAN Edge routers into the SD-WAN overlay.
References: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf

upvoted 14 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Answer is C... VBond onboards the device into the overlay. It authenticates the devices onto the fabric. even from PnP portal... thats the purpose of the vBond. If you answer A you will be sorry.

upvoted 1 times

jeffro9898 4 months, 3 weeks ago

Answer "A" "initiating connections with SD-WAN routers automatically" is wrong and here is why: Page 36 of Cisco SDWAN Ciscopress book, states that "The WAN Edge will attempt to build a temporary connection to the vBond..." So it is the WAN Edge (AKA SD-WAN router) that initiates the connection to vBond. vBond does not sit there looking to initiate connections with SD-WAN routers, the SD-WAN router needs to reach out first, and then vBond provides the SD-WAN the information that it needs, such as vManage and vSmart IPs.

upvoted 1 times

ajeetnagdev 4 months, 4 weeks ago

Answer A is correct. vBond – initiates the bring up process of every vEdge device.
https://www.google.com/search?q=What+is+the+function+of+vBond+in+a+Cisco+SD-WAN+deployment%3F&rlz=1C1GCEA_enAU912AU912&oq=What+is+the+function+of+vBond+in+a+Cisco+SD-WAN+deployment%3F&aqs=chrome..69i57j0i30.910508327j0j15&sourceid=chrome&ie=UTF-8

upvoted 1 times

eff3 10 months ago

Selected Answer: C

vBond is correct

upvoted 2 times

landgar 10 months, 1 week ago

Selected Answer: A

vBond gives the IP of the vManage, in the initial transient connection.
The vManage sends the config (onboarding) to the vEdge.

upvoted 1 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: A

Going for A. It comes closest to what vBond is doing reading through all the linked documents here.
I don't think it is C. vBonds function is not to onboard. It is only giving the IP of the vManage Server to the Router (and this can be done automatically). vManage is onboarding the routers.

upvoted 2 times

Asymptote 10 months, 3 weeks ago

Selected Answer: C

C (vBond not initia connection to vEdges automatically)

WAN Edge onboarding process Upon bootup, the WAN Edge device contacts the vBond orchestrator to establish a secure transient DTLS control connection.

Reference (Page 6):
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf

upvoted 2 times

dougj 1 year, 1 month ago

Selected Answer: A

I think answer here is still A. The vBond only assists in the onboarding, it is not responsible for onboarding, that is completed by vManage. The part vBond plys in the onboarding is to automatically initiate the connection with the WAN edge routers, authenticate them and provide them with a list of vManage and vSmart devices

upvoted 1 times

uzbin 1 year, 2 months ago

C - initial comms started by vedge to vbond, not by vbond.

upvoted 1 times

Joseph123 1 year, 2 months ago

Selected Answer: C

Answer is C

upvoted 1 times

Caledonia 1 year, 2 months ago

Selected Answer: C

it is answer C

upvoted 1 times

siteoforigin 1 year, 2 months ago

Selected Answer: C

It onboards Edge routers, see:
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html#OrchestrationPlane

upvoted 1 times

```
switch1(config)# interface GigabitEthernet 1/1
switch1(config-if)# switchport mode trunk
switch1(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-90
switch1(config)# exit
switch1(config)# monitor session 1 source vlan 10
switch1(config)# monitor session 1 destination remote vlan 70


switch2(config)# interface GigabitEthernet 1/1
switch2(config-if)# switchport mode trunk
switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,80-90
switch2(config)# exit
switch2(config)# monitor session 2 source remote vlan 70
switch2(config)# monitor session 2 destination interface GigabitEthernet1/1
```

Refer to the exhibit. A network administrator configured RSPAN to troubleshoot an issue between switch 1 and switch2. The switches are connected using interface GigabitEthernet 1/1. An external packet capture device is connected to swich2 interface GigabitEthernet 1/2. Which two commands must be added to complete this configuration? (Choose two.)

A. switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-80

B. switch2(config)# monitor session 1 source remote vlan 70 switch2(config)# monitor session 1 destination interface GigabitEthernet1/2

C. switch1(config)# interface GigabitEthernet 1/1 switch1 (config-if)# switchport mode access switch1 (config-if)# switchport access vlan 10 switch2(config)# interface GigabitEthernet 1/1 switch2(config-if)# switchport mode access switch2(config-if)# switchport access vlan 10

D. switch2(config)# monitor session 2 destination vlan 10

E. switch2(config)# monitor session 1 source remote vlan 70 switch2(config)# monitor session 1 destination interface GigabitEthernet1/1

Correct Answer: *AB*

Community vote distribution

AB (92%) 8%

Badger_27 Highly Voted 8 months, 4 weeks ago

Selected Answer: AB

Its AB but in the real would I would add the VLAN to the trunk not overwrite the config

upvoted 6 times

danman32 Most Recent 4 months ago

Definitely a problem with the allowed VLANs on SW2. Your RSPAN is conveyed on VLAN 70 but VLAN 70 isn't allowed
But with the reconfiguration of the VLAN, you lost VLANs 81-90. Typo perhaps?

Why change session # on SW2? Just fix the destination on session 2

upvoted 2 times

dragonwise 7 months, 3 weeks ago

A.
switch2(config-if)#
switchport trunk allowed vlan 10,20,30,40,50,60,70-80

B.
switch2(config)# monitor session 1 source remote vlan 70
switch2(config)# monitor session 1 destination interface GigabitEthernet1/2

C.
switch1(config)# interface GigabitEthernet 1/1
switch1 (config-if)#
switchport mode access
switch1 (config-if)#
switchport access vlan 10
switch2(config)# interface GigabitEthernet 1/1
switch2(config-if)#
switchport mode access
switch2(config-if)#
switchport access vlan 10

D.
switch2(config)# monitor session 2 destination vlan 10

E.
switch2(config)# monitor session 1 source remote vlan 70
switch2(config)# monitor session 1 destination interface GigabitEthernet1/1

upvoted 1 times

rafaelinho88 9 months, 3 weeks ago

Selected Answer: AB

Switch2 is not allowing VLAN 70 which is used on Switch1 for RSPAN
so we must allow it -> Option A is correct (although it would not allow VLAN 81 to 90 to go through).
"An external packet capture device is connected to switch2 interface GigabitEthernet1/2" so we must configure Gi1/2 as the destination port.
For your information, this is how to configure Remote SPAN (RSPAN) feature on two switches. Traffic on FastEthernet0/1 of Switch 1 will be sent to Fa0/10 of Switch2 via VLAN 40.
+ Configure on both switches
Switch1,2(config)#vlan 40
Switch1,2(config-vlan)#remote-span
+ Configure on Switch1
Switch1(config)# monitor session 1 source interface FastEthernet 0/1
Switch1(config)# monitor session 1 destination remote vlan 40
+ Configure on Switch2
Switch2(config)#monitor session 5 source remote vlan 40
Switch2(config)# monitor session 5 destination interface FastEthernet 0/10

upvoted 3 times

markymark874 10 months, 4 weeks ago

Selected Answer: AB

Gi1/1 is the source in sw2 so destination should be different

upvoted 1 times

Xerath 11 months, 2 weeks ago

Selected Answer: AB

Provided answers are correct.

upvoted 1 times

Typovy 12 months ago

Selected Answer: AB

A,B correct

upvoted 1 times

iGlitch 1 year ago

Provided answers are correct.

upvoted 1 times

iEpsilon 1 year ago

Selected Answer: AE

It should be A and E.

upvoted 1 times

AndreasThornus 12 months ago

Not sure about E. The question states the packet capture device is connected to Gi1/2 and answer E config points towards Gi1/1.

upvoted 2 times

danman32 4 months ago

Besides that, G1/1 is your trunk link. You don't want to send your capture back through the trunk!

upvoted 1 times

Question #488 *Topic 1*

Which function does a Cisco SD-Access extended node perform?

A. provides fabric extension to nonfabric devices through remote registration and configuration

B. performs tunneling between fabric and nonfabric devices to route traffic over unknown networks

C. used to extend the fabric connecting to downstream nonfabric enabled Layer 2 switches

D. in charge of establishing Layer 3 adjacencies with nonfabric unmanaged node

Correct Answer: *C*

Community vote distribution

C (100%)

[Removed] 2 months, 1 week ago

Would these also be known as VXLAN gateways? It's the only thing that could come to mind with that answer/definition.

upvoted 1 times

ihateciscoreally 4 months ago

not covered in OCG. "extended node" was mentioned two times without any examples.

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

A, C were two confusing one.

upvoted 1 times

KOJJY 11 months, 3 weeks ago

Selected Answer: C

100% correct
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2832.pdf

upvoted 3 times

Question #489 *Topic 1*

Which router is elected the IGMP Querier when more than one router is in the same LAN segment?

A. The router with the shortest uptime.

B. The router with the longest uptime.

C. The router with the highest IP address.

D. The router with the lowest IP address.

Correct Answer: *D*

Community vote distribution

D (90%) 10%

kewokil120 Highly Voted 10 months, 4 weeks ago

Selected Answer: D

IGMPV1 is highest. IGMPV2 uses lowest per https://www.ciscopress.com/articles/article.asp?p=2738463&seqNum=6

upvoted 5 times

rami_mma Most Recent 8 months, 1 week ago

Selected Answer: D

lowest interface IP

upvoted 2 times

rafaelinho88 9 months, 3 weeks ago

Selected Answer: D

Query messages are used to elect the IGMP querier as follows:
1. When IGMPv2 devices start, they each multicast a general query message to the allsystems grou address of 224.0.0.1 with their interface address in the source IP address field of the message.
2. When an IGMPv2 device receives a general query message, the device compares the source IP address in the message with its own interface address. The device with the lowest IP address on the subnet is elected the IGMP querier.
3. All devices (excluding the querier) start the query timer, which is reset whenever a general query message is received from the IGMP querier. If the query timer expires, it is assumed that the IGMP querier has gone down, and the election process is performed again to elect a new IGMP querier.

upvoted 2 times

reza88 11 months, 3 weeks ago

in this document it mentioned highets IP addres. is teh answer highest IP?
https://www.ciscopress.com/articles/article.asp?p=2738463&seqNum=6#:~:text=If%20there%20are%20multiple%20queriers,with%20the%20highest%20IP%20address.

upvoted 1 times

civan 11 months ago

"If there are multiple routers on a subnet, the DR is the device with the highest IP address and the querier is the device with the lowest IP address."

upvoted 5 times

bora4motion 1 year ago

Selected Answer: C

lowest IP

upvoted 1 times

loannis34 10 months, 3 weeks ago

Answer D you mean.

upvoted 4 times

kebkim 1 year, 2 months ago

when there are two routers in the same subnet then only one of them should send query messages. The election ensures only one router becomes the active querier. The router with the lowest IP address becomes the active querier.

upvoted 3 times

jucevabe 1 year, 2 months ago

sorry you're right uzbin , I read wrong, the one with the lowest IP

upvoted 2 times

jucevabe 1 year, 2 months ago

https://www.ciscopress.com/articles/article.asp?p=2738463&seqNum=6#:~:text=If%20there%20are%20multiple%20queriers,with%20the%20highest%20IP%20address.

upvoted 2 times

jucevabe 1 year, 2 months ago

Answer C

upvoted 2 times

uzbin 1 year, 2 months ago

Lowest IP becomes quarrier.
Google search.

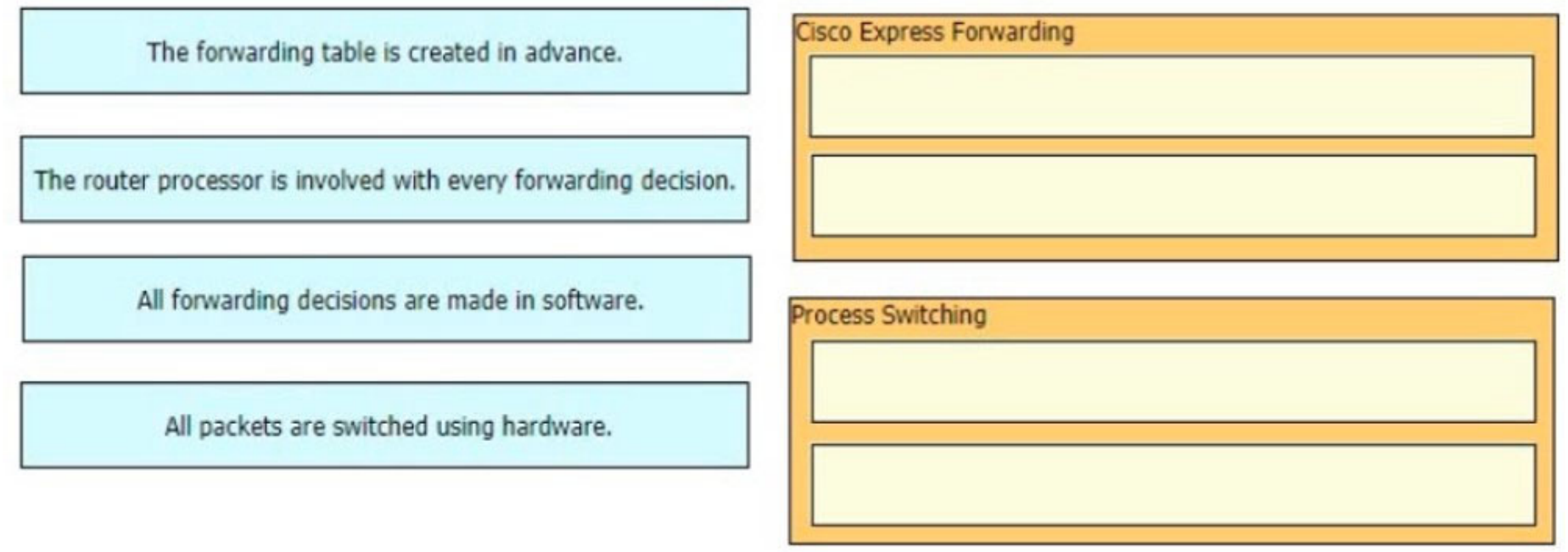
upvoted 2 times

Question #490 *Topic 1*

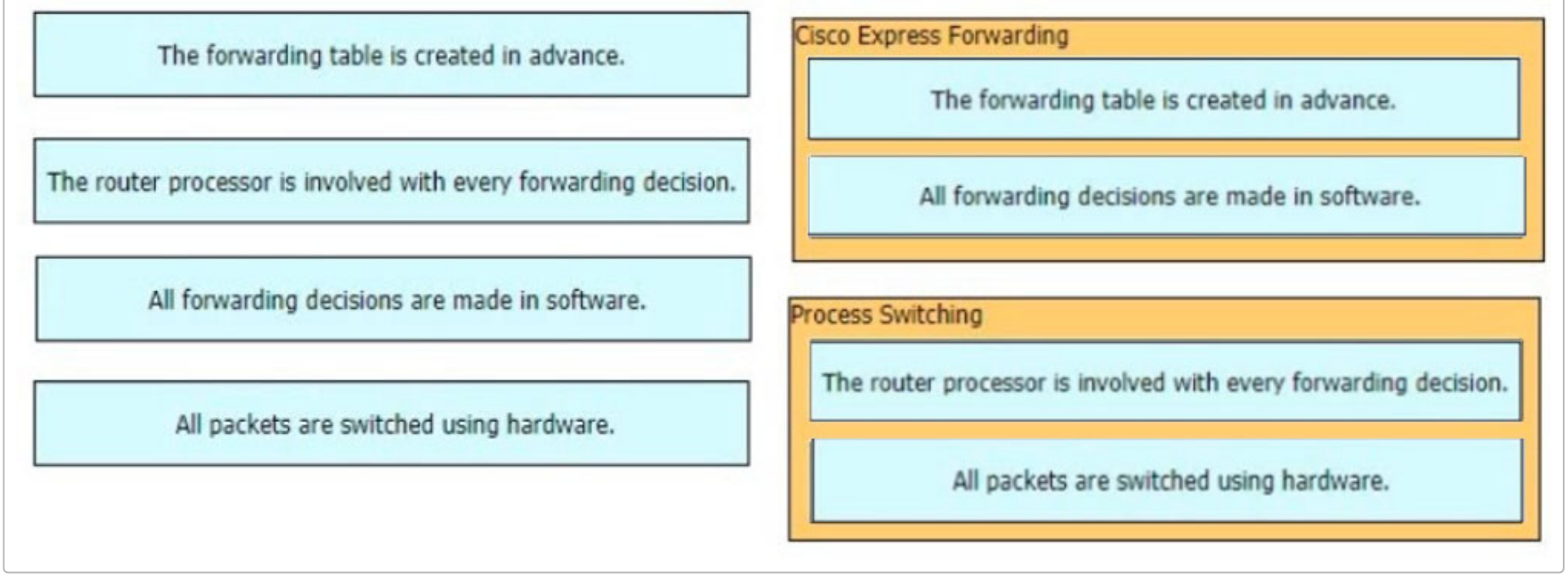
DRAG DROP -

Drag and drop the characteristics from the left onto the switching mechanisms they describe on the right.

Select and Place:



Correct Answer:



Nickplayany Highly Voted 10 months ago

CEF:

The forwarding table is created in advance.
All packets are switched using hardware.

PS:
The router processor is involved with every forwarding decision.
All forwarding decisions are made in software.

ADMIN please fix that. Thank you!

upvoted 27 times

CBlu 9 months, 3 weeks ago

Answers like this really show that some of these questions are really off

upvoted 2 times

Joseph123 Highly Voted 1 year, 2 months ago

(CEF) Cisco Express Forwarding (also known as topology based switching):

Forwarding table created in hardware beforehand. All packets will be switched using hardware. This is the fastest method but there are some limitations. Multilayer switches and routers use CEF.

Process switching:

All packets are examined by the CPU and all forwarding decisions are made in software...very slow!

upvoted 21 times

samitherider Most Recent 2 months, 4 weeks ago

CEF all packet are switched using Hardware
upvoted 1 times

danman32 4 months ago
Interestingly two of the blocks are practically saying the same thing
upvoted 1 times

CKL_SG 4 months, 3 weeks ago
There are different switching methods to forward IP packets. Here are the different switching options:

Process switching:
All packets are examined by the CPU and all forwarding decisions are made in software...very slow!
Fast switching (also known as route caching):
The first packet in a flow is examined by the CPU; the forwarding decision is cached in hardware for the next packets in the same flow. This is a faster method.
(CEF) Cisco Express Forwarding (also known as topology based switching):
Forwarding table created in hardware beforehand. All packets will be switched using hardware. This is the fastest method but there are some limitations. Multilayer switches and routers use CEF.
https://safe.menlosecurity.com/https://networklessons.com/switching/cef-cisco-express-forwarding
upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago
cef support both software and hardware.
upvoted 1 times

Mani9Don 5 months, 4 weeks ago
CEF - software

PS - hardware
upvoted 1 times

Clauster 8 months, 3 weeks ago
Men i wish Moderator updates the correct answers, this one almost got me but i knew the correct answer
upvoted 2 times

jucevabe 1 year, 2 months ago
CEF makes en hardware : https://networklessons.com/switching/cef-cisco-express-forwarding
upvoted 3 times

Deu_Inder 1 year, 2 months ago
I think CEF makes the forwarding decisions in hardware.
upvoted 3 times

Question #491 *Topic 1*

In which two ways does the routing protocol OSPF differ from EIGRP? (Choose two.)

A. OSPF provides shorter convergence time than EIGRP.

B. OSPF supports only equal-cost load balancing EIGRP supports unequal-cost load balancing.

C. OSPF is distance vector protocol. EIGRP is a link-state protocol.

D. OSPF supports an unlimited number of hops EIGRP supports a maximum of 255 hops.

E. OSPF supports unequal-cost load balancing EIGRP supports only equal-cost load balancing.

Correct Answer: *AB*

Community vote distribution

BD (100%)

Japsurd Highly Voted 1 year, 2 months ago

Selected Answer: BD

B and D. EIGRP has faster convergence time than OSPF because EIGRP has a backup route (feasible successor) readily available. OSPF would have to first signal with LSAs, then run SPF calculation, then update the RIB and the FIB.

upvoted 6 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago

Its so obvious A is not the answer. Cisco has to FLEX their pelvic once in a while

upvoted 2 times

AleR 4 months, 2 weeks ago

Selected Answer: BD

B and D are the correct ones

upvoted 2 times

net_eng10021 6 months ago

Selected Answer: BD

Seems that eigrp would provide faster convergence so A would be incorrect.

upvoted 1 times

mrtattoo 7 months ago

Selected Answer: BD

definitely B & D

upvoted 2 times

rami_mma 8 months, 1 week ago

Selected Answer: BD

B and D

upvoted 3 times

imbhebhi 8 months, 2 weeks ago

I also think it's B&D

upvoted 1 times

Rose66 10 months, 2 weeks ago

Selected Answer: BD

definitly BD

upvoted 1 times

Asymptote 10 months, 3 weeks ago

Selected Answer: BD

Google and you get answer easily.

upvoted 2 times

dancott 11 months, 3 weeks ago

Selected Answer: BD

Defo not A as OSPF sorts out the new route after it is already down

upvoted 1 times

forccnp 12 months ago

Selected Answer: BD

B and Da are correct answers!!

upvoted 2 times

bora4motion 1 year ago

Selected Answer: BD

BD, and in theory EIGRP should be faster than OSPF as per Cisco.

upvoted 1 times

jstaruch 1 year, 2 months ago

There is one ponit about D
Hop count is 2 This is not used in metric calculations, but does limit the maximum size of an EIGRP AS. The maximum number of hops that EIGRP accepts is 100 by default, although the maximum can be configured to 220 with metric maximum hops.
https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html

upvoted 1 times

ccnptoppler34 1 year, 2 months ago

Selected Answer: BD

The answer is BD

upvoted 1 times

jucevabe 1 year, 2 months ago

yes , BD

upvoted 1 times

Caledonia 1 year, 2 months ago

Selected Answer: BD

The answer is BD

upvoted 4 times

```
enable secret cisco

aaa new-model

tacacs server ise-1
address 10.1.1.1
key cisco123!

tacacs server ISE-2
address 10.2.2.1
key cisco123!

aaa group server tacacs+ ISE-Servers
server name ise-1
server name ise-2
```

Refer to the exhibit. A network engineer must configure the router to use the ISE-Servers group for authentication. If both ISE servers are unavailable, the local username database must be used. If no usernames are defined in the configuration, then the enable password must be the last resort to log in. Which configuration must be applied to achieve this result?

A. aaa authorization exec default group ISE-Servers local enable

B. aaa authentication login error-enable aaa authentication login default group enable local ISE-Servers

C. aaa authentication login default group ISE-Servers local enable

D. aaa authentication login default group enable local ISE-Servers

Correct Answer: *C*

Community vote distribution

C (100%)

Dataset 10 months, 2 weeks ago

Selected Answer: C

C i correct
the authentication order is ISE servers/Loggin Local / Enable pass
Regards

upvoted 2 times

bora4motion 11 months, 2 weeks ago

Selected Answer: C

C looks correct to me: ISE > LOCAL > ENABLE

upvoted 2 times

Question #493 *Topic 1*

When using BFD in a network design, which consideration must be made?

A. BFD is used with dynamic routing protocols to provide subsecond convergence.

B. BFD is used with first hop routing protocols to provide subsecond convergence.

C. BFD is used with NSF and graceful to provide subsecond convergence.

D. BFD is more CPU-intensive than using reduced hold timers with routing protocols.

Correct Answer: *D*

Community vote distribution

A (88%) 12%

rami_mma 8 months ago

Selected Answer: D

D is the correct option, since you can achieve subsecond without BDF

upvoted 1 times

Nickplayany 10 months ago

Selected Answer: A

It´s A - that´s the reason ISPs using this protocol.

upvoted 2 times

Rose66 10 months, 2 weeks ago

Selected Answer: A

D is wrong.... from https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fs_bfd.html#wp1043332
"Because some parts of BFD can be distributed to the data plane, it can be less CPU-intensive than the reduced EIGRP, IS-IS, and OSPF timers, which exist wholly at the control plane."

upvoted 4 times

Asymptote 10 months, 3 weeks ago

Selected Answer: A

A is correct,
D is wrong, because reduced CPU burden is the core reason why BDF is introduced.

upvoted 2 times

nushadu 11 months, 4 weeks ago

Selected Answer: A

D is completely wrong ... BFD is running in hardware NOT in software\CPU...
A. is my choise

upvoted 2 times

nushadu 11 months, 1 week ago

+ it depends on model\hardware
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xe-3s/asr903/irb-xe-3s-asr903-book/irb-bi-fwd-det.html

upvoted 1 times

bora4motion 1 year ago

B - I use that with OSPF.

upvoted 1 times

bora4motion 1 year ago

I meant to say A.

upvoted 1 times

yousif387 1 year ago

Selected Answer: D

BFD can be used with static routes also

upvoted 1 times

network_gig 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 2 times

dougj 1 year, 1 month ago

Selected Answer: A

Correct answer is A. See here for detail: https://www.cisco.com/en/US/docs/ios/12_4t/ip_route/configuration/guide/t_bfd.html

upvoted 2 times

Wooker 1 year, 2 months ago

Selected Answer: A

The correct answer is A.

upvoted 2 times

Joseph123 1 year, 2 months ago

Selected Answer: A

Correct answer is A

upvoted 3 times

kebkim 1 year, 2 months ago

A?
Because some parts of BFD can be distributed to the data plane, it can be less CPU-intensive than the reduced EIGRP, IS-IS, and OSPF timers, which exist wholly at the control plane.

upvoted 2 times

siteoforigin 1 year, 2 months ago

Agreed, I think it is A as well.
This doc also says it is less CPU intensive that low protocol timers:
https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fs_bfd.html#wp1043332

upvoted 3 times

Caledonia 1 year, 2 months ago

Selected Answer: A

The answer is A. We use BFD with BGP to provide fast routing reconvergence.
A. BFD is used with dynamic routing protocols to provide subsecond convergence.

upvoted 3 times

Deu_Inder 1 year, 2 months ago

Selected Answer: D

Provided answer is correct.

upvoted 1 times

Question #494 *Topic 1*

```
interface GigabitEthernet1
 ip address 10.10.10.1 255.255.255.0
!
access-list 10 permit 10.10.10.1
!
monitor session 10 type erspan-source
 source interface Gi1
 destination
  erspan-id 10
  ip address 192.168.1.1
!
```

Refer to the exhibit. Which command filters the ERSPAN session packets only to interface GigabitEthernet1?

A. source ip 10.10.10.1

B. filter access-group 10

C. destination ip 10.10.10.1

D. source interface gigabitethernet1 ip 10.10.10.1

Correct Answer: *B*

Community vote distribution

B (100%)

CCNPWILL 1 month, 2 weeks ago

Now to remember this question... which answers filters? ... The only answer with the filter keyword of course....

upvoted 1 times

PureInertiaCopy 3 months, 2 weeks ago

No wildcard mask is applied to the access list... And no "Host" keyword...

upvoted 1 times

danman32 4 months ago

Answer B is the correct answer, it is the only item there doing any filtering.
But the environment doesn't make sense. Gi1 is already the source and it is a layer 3 interface, so no filtering is needed.
As a matter of fact, since you're filtering packets based on a unicast IP, you'll be losing packets that may come through G1 such as broadcast, multicast, etc. and that's really not what was asked.

upvoted 2 times

x3rox 10 months ago

Now I'm reading this:
Only ACL name is supported to associate to the ERSPAN source session. If the ACL does not exist or if there is no entry defined in the access control list, the ACL name is not attached to the ERSPAN source session.

upvoted 4 times

x3rox 10 months ago

Selected Answer: B

Correct Answer is B:
From Cisco IOS XE Everest 16.4.1 release, ERSPAN has been enhanced to better monitor packets and reduce network traffic. This enhancement supports ACL on ERSPAN source session to filter only specific IP traffic according to the ACL, and is supported on the IOS XE platform. Both IPv4 and IPv6 traffic can be monitored by associating an ACL with the ERSPAN session. The ERSPAN session can associate only one IP ACL entry with its name.
Thank you @Rose66

upvoted 2 times

Rose66 10 months, 2 weeks ago

Selected Answer: B

provided answer is correct... see https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xe-16/lanswitch-xe-16-book/lnsw-conf-erspan.html

upvoted 2 times

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand—alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel—groups in use: 1
Number of aggregators:           1

Group  Port—channel  Protocol  Ports
------+-------------+---------+-------------------------------
1      Pol (SD)              -      Fa0/1 (D)   Fa0/2 (D)
```

```
S1# show run | begin interface port-channel
interface Port—channel1
 switchport mode trunk
!
interface FastEthernet0/1
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 1 mode on
!
<Output omitted>
```

```
S2# show run | begin interface port-channel
interface Port—channel1
 switchport mode trunk
!
interface FastEthernet0/1
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 1 mode desirable
!
<Output omitted>
```

Refer to the exhibit. Traffic is not passing between SW1 and SW2. Which action fixes the issue?

A. Configure switch port mode to ISL on S2

B. Configure LACP mode on S1 to active

C. Configure PAgP mode on S1 to desirable

D. Configure LACP mode on S1 to passive

Correct Answer: *C*

Community vote distribution

C (100%)

landgar Highly Voted 10 months, 1 week ago

Selected Answer: C

On: no negotiation
PagP: auto, desirable
LACP: active, passive

upvoted 9 times

x3rox 10 months ago

Thank you

upvoted 1 times

CCNPWILL Most Recent 1 month, 2 weeks ago

Answer is correct. C

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

PagP – auto/desirable | desirable/desirable
LACP – active/passive | active/active
Static – on/on

upvoted 1 times

Dataset 1 year, 1 month ago

Its correct

upvoted 2 times

Which Python code snippet must be added to the script to store the changed interface configuration to a local JSON-formatted file?

```
import json
import requests

Creds = ("user", "Z#419010526$mnV")
Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

BaseURL = https://cpe/restconf/data"
URL = BaseURL + "/Cisco-IOS-XE-native:native/interface"

Response = requests.get(URL, auth = Creds, headers = Headers, verify = False)
UpdatedConfig = Response.text.replace("2001:db8:1:", "2001:db8:café:"
```

A.

```
OutFile = open("ifaces.json", "w")
OutFile.write(Response.text)
OutFile.close()
```

B.

```
OutFile = open("ifaces.json", "w")
OutFile.write(UpdatedConfig)
OutFile.close()
```

C.

```
OutFile = open("ifaces.json", "w")
json.dump(UpdatedConfig,OutFile)
OutFile.close()
```

D.

```
OutFile = open("ifaces.json", "w")
OutFile.write(Response.json())
OutFile.close()
```

Correct Answer: *B*

iGlitch Highly Voted 12 months ago

B is correct because:
1 - 'response' type is (class Response).
2 - 'UpdateConfig' converted 'response' to a String, so it's a String.
3 - When using write() the passed argument must be a String.

NOT C, json.dump(ARG1, ARG2) method takes a python dictionary NOT a String, and convert it as a JSON file.

HTH

upvoted 6 times

Chuckzero Most Recent 2 months, 3 weeks ago

The correct answer is B.

This question is testing your knowledge of the difference between json.dump() and json.dumps().

When you see json.dump() -> It is used for saving JSON-formatted data to a file.

json.dumps() - Dumps the data to a memory for future use. You can call the json-formatted data later for use such as sending it over a network or embedding it to a web page.

upvoted 1 times

Zizu007 1 year ago

B is correct.
C is wrong:
json.dump() expects python <dict> type as input. in this case "Response.text.replace()" is a <str> data type in Python.

upvoted 3 times

kuzma 1 year, 1 month ago

UpdatedConfig = Response.text bla-bla-bla -> type str
type str not serialisible, so json.dump(UpdatedConfig, OutFile) - returns error
Answer B, but it is no json-formatted file

upvoted 4 times

Zizu007 1 year ago

B is correct. read the file again in python with json.load().

upvoted 1 times

Lalane 1 year ago

Correct answer is "C", json.dump (dump without s) allow you convert a text file to json format

upvoted 1 times

iGlitch 12 months ago

You got it all wrong my g :(

upvoted 1 times

doron1122 1 year, 1 month ago

Looks like its C
https://pynative.com/python-json-dumps-and-dump-for-json-encoding/

upvoted 4 times

Clauster 8 months, 2 weeks ago

Thanks, the answer is def C

upvoted 1 times

Titini 1 year, 2 months ago

Why not C

upvoted 1 times

iGlitch 12 months ago

Because:
1 - 'response' type is (class Response).
2 - 'UpdateConfig' converted 'response' to a String, so it's a String.
3 - When using write() the passed argument must be a String.

NOT C, json.dump(ARG1, ARG2) method takes a python dictionary NOT a String, and convert it as a JSON file.

HTH

upvoted 1 times

Question #497 *Topic 1*

```
R2#show standby
FastEthernet1/0 - Group 50
  State is Active
    2 state changes, last state change 00:04:02
  Virtual IP address is 10.10.1.1
  Active virtual MAC address is 0000.0c07.ac32 (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac32 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.504 secs
  Preemption enabled, delay reload 90 secs
  Active router is local
  Standby router is unknown
  Priority 200 (configured 200)
    Track interface FastEthernet0/0 state Up decrement 20
  Group name is "hsrp-Fa1/0-50" (default)
R2#
%IP-4-DUPADDR: Duplicate address 10.10.1.1 on FastEthernet1/0, sourced by 0000.0c07.ac28
R2#
```

Refer to the exhibit. An engineer configures a new HSRP group. While reviewing the HSRP status, the engineer sees the logging message generated on R2.

What is the cause of the message?

A. The HSRP configuration has caused a routing loop

B. The same virtual IP address has been configured for two HSRP groups

C. A PC is on the network using the IP address 10.10.1.1

D. The HSRP configuration has caused a spanning-tree loop

Correct Answer: *B*

Community vote distribution

B (92%) 8%

landgar 10 months, 1 week ago

Selected Answer: B

It's just a warning. Groups are different, so no problems

upvoted 4 times

danman32 4 months ago

Actually no, there will be problems. You can't have active duplicate IPs associated with different MACs on a subnet. The reason HSRP works is because only one host (router) in an HSRP group is active with the VIP/MAC.
But with two independent groups, both are speaking and in this case, with conflicting IPs

upvoted 1 times

Rose66 10 months, 2 weeks ago

Selected Answer: B

look at the MAC address of the LOG Message: "%IP-4-DUPADDR: Duplicate address 10.10.1.1 on FastEthernet1/0, sourced by 0000.0c07.ac28" ...
The MAC Address is a Virtual HSRP MAC Address!!!

upvoted 2 times

nushadu 10 months, 3 weeks ago

Selected Answer: B

I've tested again and cought this bug, the same error actually nyway you can chache MAC manually, by default yes, it belongs to HSRP process, the difference only in the groups 10 vs 11;

*Jan 10 10:11:31.992: %IP-4-DUPADDR: Duplicate address 10.99.0.254 on Ethernet0/1.10, sourced by 0000.0c07.ac0a
cisco_R5#
cisco_R5#s runn int ethernet 0/1.10
Building configuration...

Current configuration : 119 bytes
!
interface Ethernet0/1.10
encapsulation dot1Q 10
ip address 10.99.0.5 255.255.255.0
standby 11 ip 10.99.0.254 <<<<<<<<<<<<<<
end

cisco_R5#

upvoted 1 times

nushadu 10 months, 3 weeks ago

far end:

*Jan 10 10:11:01.888: %IP-4-DUPADDR: Duplicate address 10.99.0.254 on Ethernet0/1.10, sourced by 0000.0c07.ac0b
cisco_R2(config-subif)#
cisco_R2(config-subif)#do s runn int ethernet 0/1.10
Building configuration...

Current configuration : 119 bytes
!
interface Ethernet0/1.10
encapsulation dot1Q 10
ip address 10.99.0.2 255.255.255.0
standby 10 ip 10.99.0.254 <<<<<<<<<<<<<<<<<<<<<<<
end

cisco_R2(config-subif)#
*Jan 10 10:11:31.993: %IP-4-DUPADDR: Duplicate address 10.99.0.254 on Ethernet0/1.10, sourced by 0000.0c07.ac0b
cisco_R2(config-subif)#

upvoted 1 times

nushadu 10 months, 3 weeks ago

fix:

cisco_R2(config-subif)#int ethernet 0/1.10
cisco_R2(config-subif)#no standby 10 <<<<<<<<<<<<<<<<<<<
*Jan 10 10:16:33.457: %HSRP-5-STATECHANGE: Ethernet0/1.10 Grp 10 state Active -> Disabled
cisco_R2(config-subif)# standby 11 ip 10.99.0.254 <<<<<<<<<<<<<<<<<<<
cisco_R2(config-subif)#
*Jan 10 10:17:03.504: %HSRP-5-STATECHANGE: Ethernet0/1.10 Grp 11 state Speak -> Standby
cisco_R2(config-subif)#do s standby br
P indicates configured to preempt.
|
Interface Grp Pri P State Active Standby Virtual IP
Et0/0.10 200 100 Active local unknown 192.168.255.254
Et0/1.10 11 100 Standby 10.99.0.5 local 10.99.0.254 <<<<<<<<<<<<<<<<
cisco_R2(config-subif)#
cisco_R2(config-subif)#do s runn int ethernet 0/1.10
!
interface Ethernet0/1.10
encapsulation dot1Q 10
ip address 10.99.0.2 255.255.255.0
standby 11 ip 10.99.0.254
end

upvoted 1 times

civan 11 months ago

Selected Answer: B

Notice the sourced mac address is an HSRP mac: 0000.0c07.acxx

upvoted 4 times

nushadu 11 months, 1 week ago

Selected Answer: C

cisco_R3(config-subif)#
*Dec 22 20:44:43.970: %IP-4-DUPADDR: Duplicate address 10.111.12.6 on Ethernet0/0.70, sourced by aabb.cc00.5000
cisco_R3(config-subif)#do show runn int Ethernet0/0.70
Building configuration...

Current configuration : 123 bytes
!
interface Ethernet0/0.70
encapsulation dot1Q 70
ip address 10.111.12.1 255.255.255.248
standby 11 ip 10.111.12.6
end

cisco_R3(config-subif)#
*Dec 22 20:45:13.974: %IP-4-DUPADDR: Duplicate address 10.111.12.6 on Ethernet0/0.70, sourced by aabb.cc00.5000
cisco_R3(config-subif)#

upvoted 1 times

Rose66 10 months, 2 weeks ago

you are wrong... look at the MAC address of the LOG Message: "%IP-4-DUPADDR: Duplicate address 10.10.1.1 on FastEthernet1/0, sourced by 0000.0c07.ac28" ... The MAC Address is a Virtual HSRP MAC Address!!!

upvoted 1 times

nushadu 11 months, 1 week ago

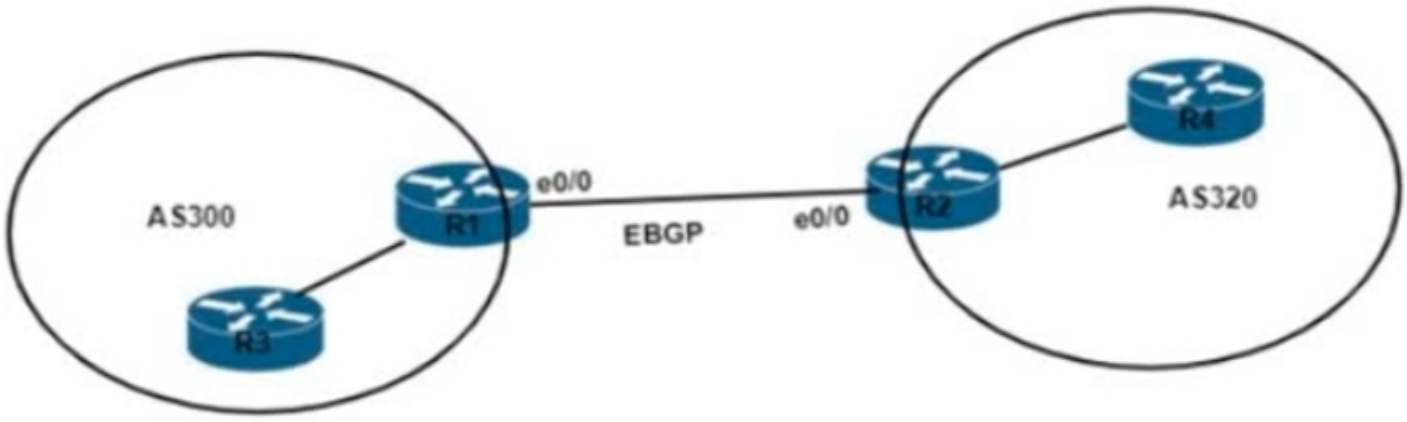
far-end:
cisco_R5(config-subif)#do s runn interface ethernet 0/0.70
Building configuration...

Current configuration : 96 bytes
!
interface Ethernet0/0.70
encapsulation dot1Q 70
ip address 10.111.12.6 255.255.255.248
end

cisco_R5(config-subif)#

upvoted 1 times

Question #498 *Topic 1*



Router R1

```
interface Ethernet0
ip address 131.108.1.1 255.255.255.0
interface Loopback1
ip address 1.1.1.1 255.255.255.255
```

Router R2

```
interface Ethernet0
ip address 131.108.1.2 255.255.255.0
interface Loopback1
ip address 2.2.2.2 255.255.255.255
```

```
R2#debug ip bgp
BGP debugging is on
R2#
Nov 28 13:25:12: BGP: 131.108.1.11 open active, local address 131.108.1.2
Nov 28 13:25:42: BGP: 131.108.1.11 open failed: Connection timed out;
remote host not responding
```

Refer to the exhibit. Which configuration must be implemented to establish EBGP peering between R1 and R2?

A.

R2
```
router bgp 300
neighbor 131.108.1.1 remote-as 320
```
R1
```
router bgp 320
neighbor 131.108.1.2 remote-as 300
```

B.

R2
```
router bgp 320
neighbor 131.108.1.11 remote-as 300
```
R1
```
router bgp 300
neighbor 131.108.1.2 remote-as 320
```

C.

R2
```
router bgp 320
neighbor 131.108.1.1 remote-as 300
```
R1
```
router bgp 300
neighbor 131.108.1.2 remote-as 320
```

D.

R2
```
router bgp 320
neighbor 1.1.1.1 remote-as 300
```
R1
```
router bgp 300
neighbor 2.2.2.2 remote-as 320
```

Correct Answer: *C*

bora4motion Highly Voted 11 months, 4 weeks ago
C is the correct answer.
upvoted 5 times

adrian0792 Most Recent 5 months, 2 weeks ago
C is the correct answer.

upvoted 2 times

vedranr 6 months ago

Why not D?

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

We dont have enough info to assume D is correct. if the update-source lo1 command was shown then it would kbe

upvoted 1 times

Splashisthegreatestmovie 5 months, 2 weeks ago

D could work but you need extra stuff in the config like update-source lo x.x.x.x

upvoted 2 times

Chiaretta 8 months ago

The correct answer is C, the log is saing that neighbor configuration on R2 is wrong.

router bgp 320
neighbor 131.108.1.11 remote-as 300

upvoted 1 times

danman32 4 months ago

Thanks for pointing that out. I was wondering where the error in the debug was coming from.

upvoted 1 times

Wrad 11 months ago

Hi. Does someone know, were the .11 in the debug is coming from?

upvoted 1 times

JackDRipper 8 months ago

From the neighbor statement on R2. Meaning, the "admin" typed in the wrong neighbor address and he got that error in the debug. Answer C corrects it. See Chiaretta's reply.

upvoted 1 times

Asymptote 10 months, 3 weeks ago

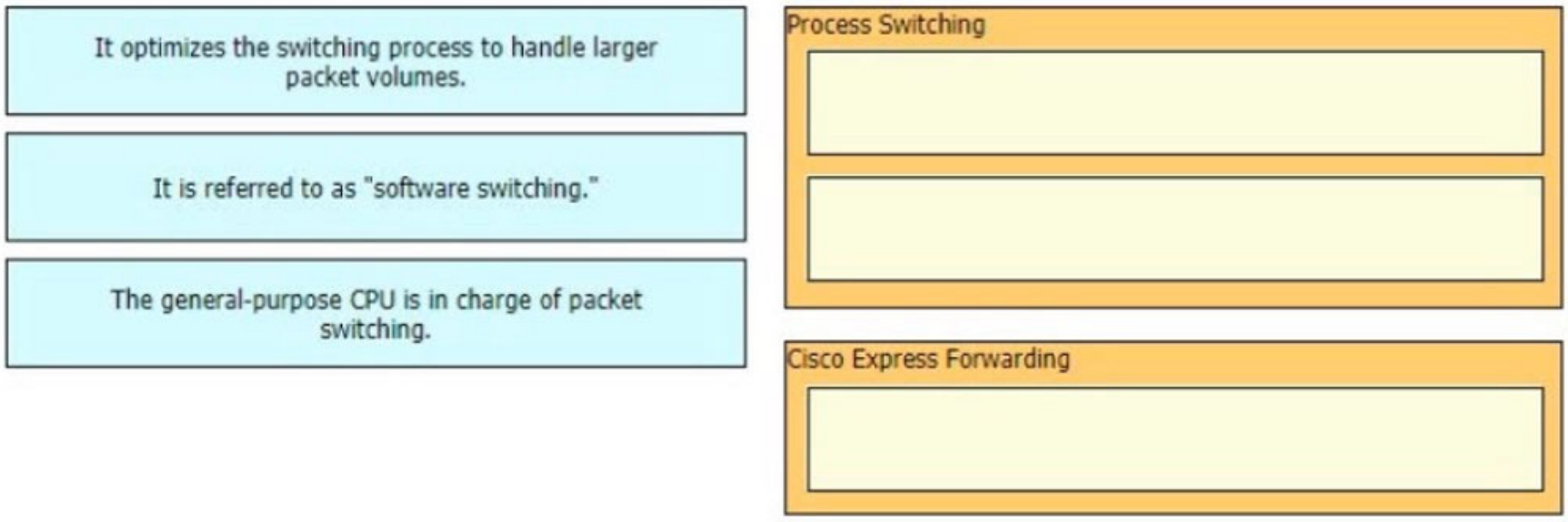
Might be the network admin typed it wrong.

upvoted 1 times

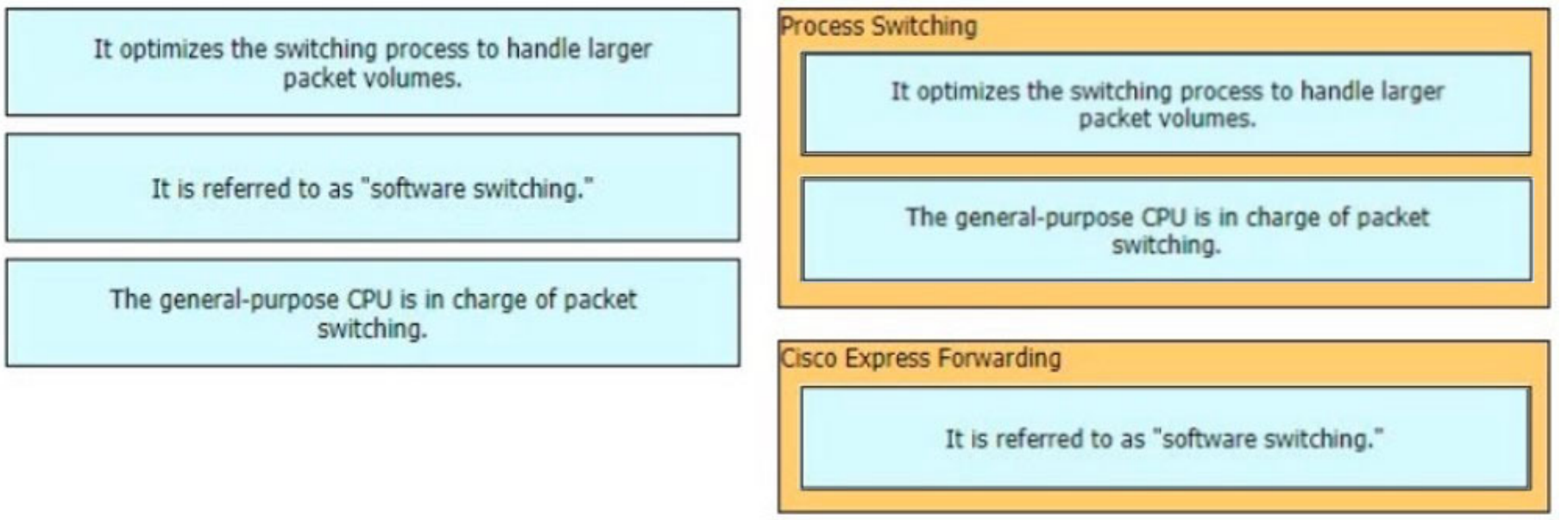
DRAG DROP -

Drag and drop the characteristics from the left onto the switching architectures on the right.

Select and Place:



Correct Answer:



siteoforigin Highly Voted 1 year, 2 months ago

Answer should be:
Process switching uses the general CPU and is referred to as software switching
CEF Can handle larger amounts of traffic

upvoted 37 times

olaniyijt Highly Voted 9 months, 2 weeks ago

PROCESS SWITCHING
- It is referred to as "Software Switching"
- The general purpose CPU is in charge of packet switching

CEF
- It optimizes the switching process to handle larger packet volumes

upvoted 12 times

CCNPWILL Most Recent 1 month, 2 weeks ago

How could admin get this wrong... CEF has been explained as hardware switching in numerous docs. the only answer that really compliments CEF is optimizes blah blah... you know Cisco always boosts its own tech. Easy gimme question!

upvoted 1 times

PureInertiaCopy 3 months, 2 weeks ago

How could you get this wrong?

Process Switching
Process switching, also referred to as software switching or slow path, is a switching mechanism in which the general-purpose CPU on a router is in charge of packet switching. In IOS, the ip_input process runs on the general-purpose CPU for processing incoming IP packets. Process switching is the fallback for CEF because it is dedicated to processing punted IP packets when they cannot be switched by CEF.

Cisco Express Forwarding (CEF)
is a Cisco proprietary switching mechanism developed to keep up with the demands of evolving network infrastructures. It has been the default switching mechanism on most Cisco platforms that do all their packet switching using the general-purpose CPU (software-based routers) since the 1990s, and it is the default switching mechanism used by all Cisco platforms that use specialized application-specific integrated circuits (ASICs) and network processing units (NPUs) for high packet throughput (hardware-based routers).

upvoted 2 times

PureInertiaCopy 3 months, 2 weeks ago

This is from the OCG.
ENCOR 350-401

upvoted 1 times

danman32 4 months ago

What is wrong with these people publishing the answers?
Since when is CEF related to software and CPU?

upvoted 1 times

mikhailov_ivan90 10 months, 1 week ago

Given answer is incorrect. From the ENCOR book:
Process switching:
Every packet\frame examined by CPU
All forwarding decisions made in software

upvoted 3 times

AlexEMedeiros 11 months, 1 week ago

PROCESS SWITCHING o
it is referred as software sw
the general purpose CPU is in charge of packet sw
CEF
it optimizes the switching process to handle larger packet volumes

upvoted 1 times

Edwinmolinab 1 year ago

The answer is wrong according by https://study-ccnp.com/process-switching-mechanism-explained/

upvoted 1 times

Joseph123 1 year, 2 months ago

Given answer is bs. Siteoforigin is correct.

upvoted 4 times

Caledonia 1 year, 2 months ago

agree with "siteoforigin ",

upvoted 3 times

Question #500 *Topic 1*

A server running Linux is providing support for virtual machines along with DNS and DHCP services for a small business. Which technology does this represent?

A. container

B. Type 1 hypervisor

C. Type 2 hypervisor

D. hardware pass-thru

Correct Answer: *B*

Community vote distribution

C (85%) B (15%)

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: C

Type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly.

upvoted 12 times

CBlu Highly Voted 9 months, 3 weeks ago

This question is really stupid and so is the discussion about type 1 and 2 hypervisors.

ESX runs on linux just as much as... linux running kvm

Stupid ambiguous question. But if I were to guess, I would say the answer is C because whoever wrote it doesn't consider anything except vmware a type 1 hypervisor.

But who knows what that person was thinking.

upvoted 8 times

JJBIG Most Recent 3 months, 3 weeks ago

A server running Linux = Type 1 hypervisor
DNS and DHCP virtual machine = Type 2 hypervisor
Both can be the answer

upvoted 1 times

Darkboy7 5 months ago

The answer is inside the questions.

A server running Linux(Host os) is providing support for virtual machines along with DNS and DHCP services(Guest os) for a small business. Which technology does this represent

upvoted 1 times

danman32 4 months ago

Well actually the Linux server could just as well itself be a VM.
Bad question

upvoted 1 times

ruiolegario 6 months, 3 weeks ago

ps. "for VIRTUAL MACHINES"

upvoted 1 times

Dataset 7 months ago

Selected Answer: B

linux running on the server...so Linux is the host SO
Hipervisor type 1
Regards

upvoted 1 times

nana_amp 7 months, 2 weeks ago

Selected Answer: C

I think the key here is "...along with DNS and DHCP services". Clearly implies that the server has a host OS installed already, making it a type 2 hypervisor

upvoted 4 times

dragonwise 8 months ago

the question is vague
It doesn't mention that the linux server is the host, or a VM

upvoted 1 times

rami_mma 8 months, 1 week ago

Selected Answer: C

C is correct

upvoted 2 times

rafaelinho88 9 months, 3 weeks ago

Selected Answer: C

n contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. A big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows)

upvoted 1 times

landgar 10 months, 1 week ago

Selected Answer: C

Running Linux --> C

upvoted 1 times

Rose66 10 months, 2 weeks ago

Selected Answer: C

A server running Linux is providing support for virtual machines >> Type2 hypervisor

upvoted 1 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: C

It is C, a type 2 Hypervisor (a Linux OS which additionally runs a virtualization software).
The server is hosting DNS and DHCP (so it must run an OS) and additionally it supports VMs.

upvoted 1 times

Xerath 11 months, 2 weeks ago

Selected Answer: C

Any hypervisor running on top of an OS, rather than directly on the physical hardware is a type 2 hypervisor. (I know that VMware ESXi uses linux based OS, called photon OS, but I think that the question is asking in general about a hypervisor that's running on top of another OS)

Answer is "C".

upvoted 1 times

nushadu 11 months, 4 weeks ago

the stupid question actually, VMWare ESXi is also Linux OS ...

upvoted 2 times

ClPo 7 months, 2 weeks ago

IIRC: they dropped the Linux part after ESX4.1

upvoted 2 times

AndreasThornus 12 months ago

C.
The key is that the Linux machine is also running DNS and DHCP services. This suggests the Linux host is running as an OS with VMs on top i.e. a type 2 hypervisor. Not a bare metal (type 1) hypervisor.

upvoted 4 times

Caradum 1 year ago

Selected Answer: B

Linux uses KVM as a hypervisor, which is very familiar to HyperV, which is a type 1 hypervisor. So from my pov, in the question there is specificly stated, that Linux is beeing used, so i go with B.

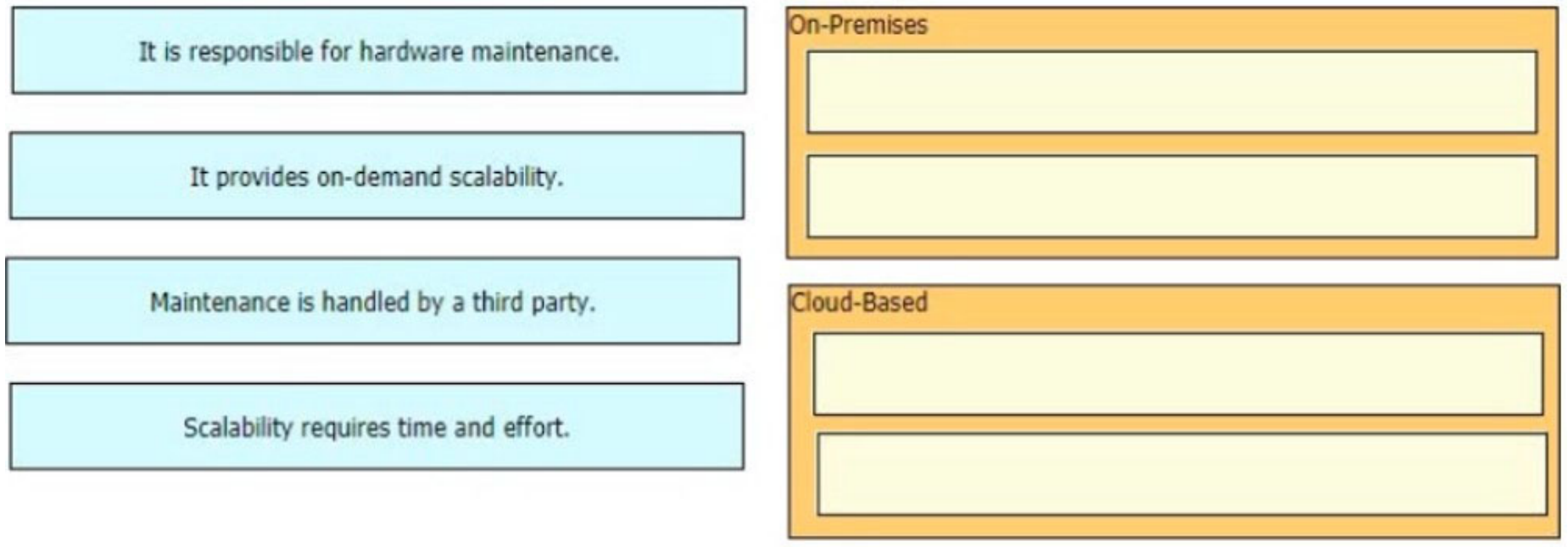
upvoted 2 times

Question #501 *Topic 1*

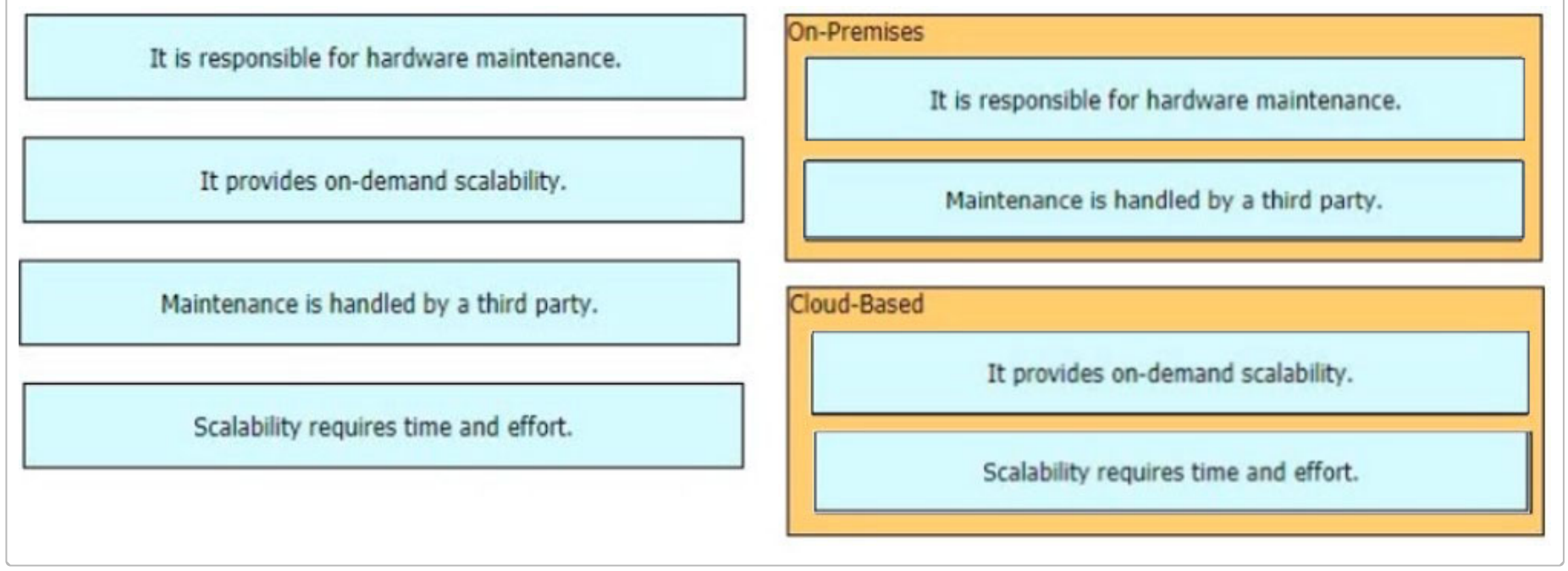
DRAG DROP -

Drag and drop the characteristics from the left onto the deployment types on the right.

Select and Place:



Correct Answer:



Lukaszaw Highly Voted 1 year, 2 months ago

Here is a mistake. Under on-premises should be:
-it is responsible for hardware maintenance
-scalability requires time and effort

upvoted 55 times

PureInertiaCopy Most Recent 3 months, 2 weeks ago

Here's my answer:

ON PREMISE:

Q501.
- Scalability requires time and effort
- It is responsible for hardware maintenance

CLOUD ENVIRONMENT:

Q501.
- It provides on-demand scalability
- Maintenance is handled by a third party

upvoted 4 times

danman32 4 months ago

What's really dumb is that the provided answers for cloud are contradictory.
On Demand scalability means it does NOT require time and effort

upvoted 1 times

AleR 4 months, 2 weeks ago

Correct answer for On-Premises:

-it is responsible for hardware maintenance
-scalability requires time and effort

"Maintenance done by third-party" should NOT be there
upvoted 3 times

[Removed] 5 months ago
Answer looks wrong to me.

On-Premises:
Scalability requires time and effort
It is responsible for hardware maintenance

Cloud-Based:
On-demand scalability
Maintenance done by third-party
upvoted 3 times

Dataset 7 months ago
admin....please fix the answer
on-premises :
-it is responsible for hardware maintenance
-scalability requires time and effort
Regards
upvoted 3 times

ClPo 7 months, 2 weeks ago
How can so many of these simple questions have a wrong answer?
upvoted 4 times

olaniyijt 9 months, 2 weeks ago
Provided answer is wrong. Lukaszaw is correct.
upvoted 2 times

OrangeCat 9 months, 2 weeks ago
it should be
On-Premises
- it is responsible for hardware maintenance
- scalability requires time and effort
Cloud-base
- it provide on-demand scalability
- maintenance is handled by a third party
upvoted 1 times

mdawg 9 months, 3 weeks ago
lmaoo how can it have on demand (easy and fast, no loopholes) scalability but it also take time and effort? i cry
upvoted 2 times

Asymptote 10 months, 3 weeks ago
Question with drag and drop almost 90% wrong answer including this one.
Lukaszaw provided a correct answer.
upvoted 3 times

bora4motion 1 year ago
Yep - this one's wrong. Lukaszaw is correct.
upvoted 1 times

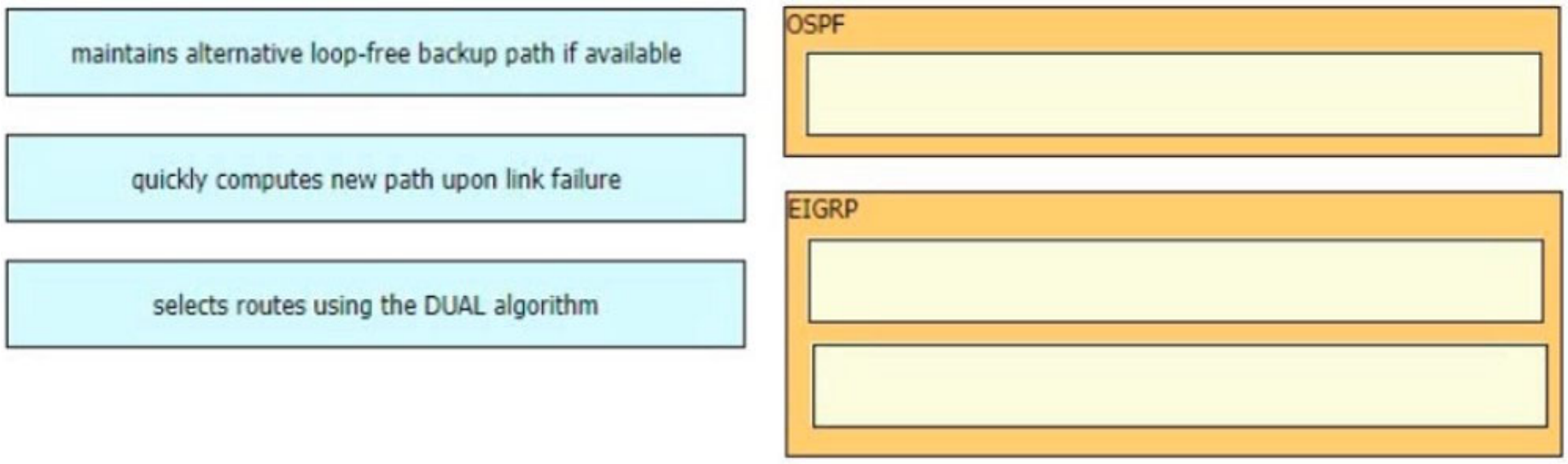
Caledonia 1 year, 2 months ago
Provided answer is wrong. Agree with Lukaszaw
upvoted 2 times

Question #502 *Topic 1*

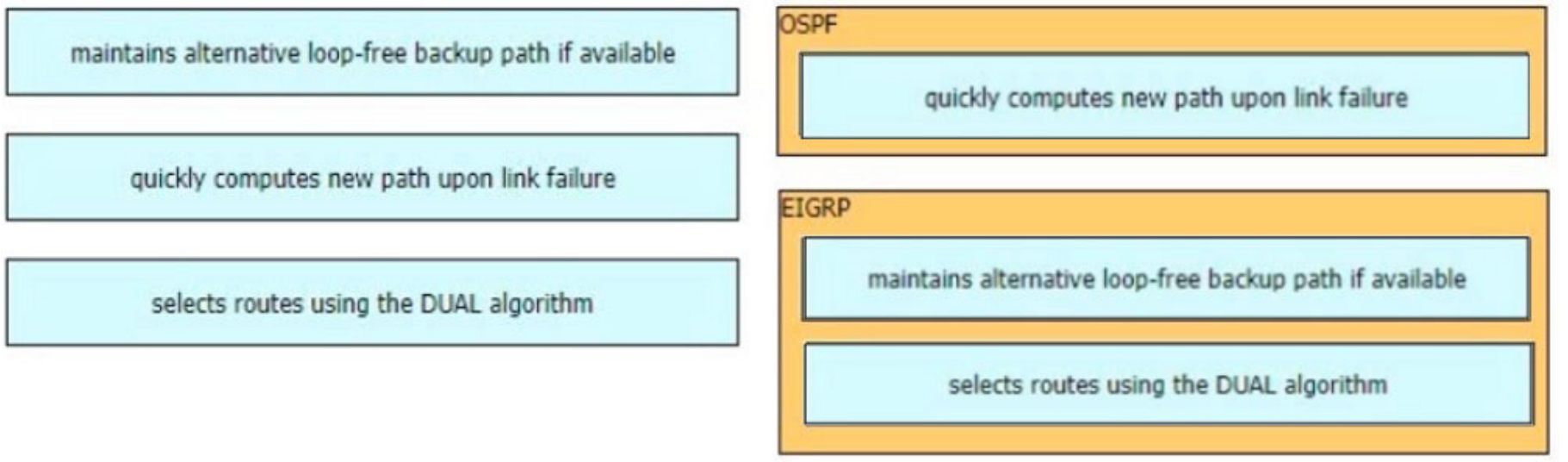
DRAG DROP -

Drag and drop the characteristics from the left onto the routing protocols they describe on the right.

Select and Place:



Correct Answer:



CCNPWILL 1 month, 2 weeks ago

Correct... but they should swap out the answer for OSPF.. like uses concept of areas.. something obvious and specific to OSPF... they both ' quickly ' reconverge networks =\. thats what screwed this question honestly.

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Rember boys and girls.. when reading an EIGRP question, any positive-sounding description is automatically EIGRP.

"Quickly computes new paths?" - MUST BE EIGRP!
"Can load-balance unequal cost LB?" - MUST BE EIGRP!
Only CISCO DESIGNS THE BEST PROTOCOLS

upvoted 3 times

VLAN4461 3 months ago

This question is outdated. OSPF now has loop free alternate fast reroute capabilities that rival EIGRP with a feasible successor. Not that OSPF cannot always converge fast, like when an area has 50 nodes and all have to run the Dykstra algorithm. Likewise, EIGRP without a feasible successor may take a while to converge, especially if it gets stuck in active.
https://networklessons.com/cisco/ccie-routing-switching-written/ospf-loop-free-alternate-lfa-fast-reroute-frr

upvoted 1 times

[Removed] 5 months ago

Correct

upvoted 1 times

TSKARAN 10 months ago

Provided answer is correct,
But,
EIGRP is considered to have faster convergence times than OSPF, particularly in the case of a link failure, and EIGRP can converge within a few hundred milliseconds, while OSPF can take a few seconds.

upvoted 4 times

edajede 6 months, 1 week ago

On the other side, OSPF has full picture of the network. EIGRP needs to send Query if can't find the way.

upvoted 1 times

JackDRipper 8 months, 1 week ago

Answer is correct.

"Quickly computes new path upon link failure". True for OSPF as it needs to re-compute and LSAs generated upon a link failure.

On the other hand, EIGRP is always ready with the 2nd-best route (ie. Feasible Successor), if available.

upvoted 2 times

Radwa_ 1 year, 1 month ago

The provided answer is correct.

upvoted 2 times

Question #503 *Topic 1*

Which features does Cisco EDR use to provide threat detection and response protection?

A. containment, threat intelligence, and machine learning

B. firewalling and intrusion prevention

C. container-based agents

D. cloud analysis and endpoint firewall controls

Correct Answer: *A*

Community vote distribution

A (100%)

examtopicsacct Highly Voted 5 months, 3 weeks ago

Zero mention of this in OCG. I'm beginning to think that 25%-50% of these questions aren't covered in the official materials.

upvoted 6 times

HarwinderSekhon 5 months, 2 weeks ago

fuck C1sC0

upvoted 5 times

Splashisthegreatestmovie Most Recent 5 months, 2 weeks ago

This product is formally called AMP4E

upvoted 2 times

snarkymark 10 months ago

A is correct.
https://www.cisco.com/c/dam/en/us/products/collateral/security/mdr-for-cisco-secure-endpoint.pdf

upvoted 2 times

poy4242 11 months, 1 week ago

Is Cisco EDR really in the scope of EN-COR ? I think this is more S-COR question.

upvoted 4 times

mgiuseppe86 2 months, 2 weeks ago

This is a brain dump from 350-401 is it not? so someone actually saw this question on the exam?

upvoted 1 times

bora4motion 1 year ago

Selected Answer: A

To me it looks like A is the right choice.
https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html#~edr-capabilities

upvoted 3 times

Question #504 *Topic 1*

```
Router#show run | b vty

line vty 0 4

 session-timeout 30

 exec-timeout 120 0

 session-limit 30

 login local

line vty 5 15

 session-timeout 30

 exec-timeout 30 0

 session-limit 30

 login local
```

Refer to the exhibit. Only administrators from the subnet 10.10.10.0/24 are permitted to have access to the router. A secure protocol must be used for the remote access and management of the router instead of clear-text protocols. Which configuration achieves this goal?

A.

```
access-list 23 permit 10.10.10.0 0.0.0.255
line vty 0 15
access-class 23 in
transport input ssh
```

B.

```
access-list 23 permit 10.10.10.0 0.0.0.255
line vty 0 15
access-class 23 out
transport input all
```

C.

```
access-list 23 permit 10.10.10.0 0.0.0.255
line vty 0 4
access-class 23 in
transport input ssh
```

D.

```
access-list 23 permit 10.10.10.0 255.255.255.0
line vty 0 15
access-class 23 in
transport input ssh
```

Correct Answer: *A*

bora4motion Highly Voted 1 year ago

A is correct!

upvoted 10 times

Pilgrim5 Highly Voted 7 months, 1 week ago

B - wrong because the transport input allows all connections (including telnet which is not secure)

C - wrong because vty 0 4 is used instead of 0 15 because the question says secure all connections to the router

D - wrong because subnet mask is used in the access list instead of the wildcard

A is the only reasonable option!

upvoted 7 times

[Removed] 5 months ago

Thanks for the breakdown, this is a good way to do process of elimination

upvoted 2 times

[Removed] Most Recent 5 months ago

Correct

upvoted 1 times

Question #505 *Topic 1*

An engineer is configuring Local WebAuth on a Cisco Wireless LAN Controller. According to RFC 5737, which virtual IP address must be used in this configuration?

A. 172.20.10.1

B. 192.168.0.1

C. 1.1.1.1

D. 192.0.2.1

Correct Answer: *B*

Community vote distribution

D (100%)

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: D

3. Documentation Address Blocks
The blocks 192.0.2.0/24 (TEST-NET-1), 198.51.100.0/24 (TEST-NET-2),
and 203.0.113.0/24 (TEST-NET-3) are provided for use in
documentation.

upvoted 16 times

PALURDIN 1 year, 2 months ago

This can be confirmed in page 14 of this document:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/web-authentication/b-configuring-web-based-authentication-on-cisco-catalyst-9800-series-controllers.pdf

upvoted 7 times

danman32 Most Recent 4 months ago

It is interesting to note that 1.1.1.1 and the like are internet routable IPs and often misused for things such as L3 HA links between routers.
Worked for a company that did that, found they could not use/reach WARP DNS.
Has you wonder about common loopback and Router ID IPs.

upvoted 1 times

msstanick 5 months, 3 weeks ago

Selected Answer: D

I did some labs in PT aobut LAP/WLC configs - the default virtual IP address that gets created when configuring the WLC is 192.168.2.1 so D.

upvoted 2 times

mrtattoo 7 months ago

Selected Answer: D

RFC 5737 clearly shows 192.0.2.1, so D is correct

upvoted 1 times

rafaelinho88 9 months, 3 weeks ago

Selected Answer: D

According to RFC 5737, the virtual IP address that must be used for this configuration is 192.0.2.0/24. This is reserved for documentation and examples and should not be used in actual production networks.

upvoted 2 times

Kasia1992 10 months ago

Selected Answer: D

192.0.2.1 for sure

upvoted 3 times

endy023 10 months, 3 weeks ago

3. Documentation Address Blocks

The blocks 192.0.2.0/24 (TEST-NET-1), 198.51.100.0/24 (TEST-NET-2),
and 203.0.113.0/24 (TEST-NET-3) are provided for use in
documentation.

upvoted 3 times

bora4motion 1 year ago

Selected Answer: D

This is a very tricky question because a few years back Cisco was recommending the use of 1.1.1.1 as VIP with the WLC. D is correct.

upvoted 4 times

loannis34 1 year, 2 months ago

Selected Answer: D

D is correct

upvoted 2 times

kebkim 1 year, 2 months ago

D.
The virtual interface IP address (IPv4 or IPv6) is used only in communications between the controller and wireless clients. It serves as the redirect address for the web authentication login page. It is recommended that you configure a nonroutable IP address for the virtual interface, ideally not overlapping with the network infrastructure addresses. Use one of the options proposed in RFC 5737, for example, 192.0.2.0/24, 198.51.100.0/24, and 203.0.113.0/24 networks.

upvoted 2 times

Caledonia 1 year, 2 months ago

Selected Answer: D

The answer is D

upvoted 1 times

ronin 1 year, 2 months ago

Selected Answer: D

upvoted 1 times

```
R2#
*May 27 15:33:59.642: OSPF-1 ADJ   Gi1: Send DBD to 192.168.201.137 seq 0xDE7 opt 0x52 flag 0x7 len 32
*May 27 15:33:59.642: OSPF-1 ADJ   Gi1: Retransmitting DBD to 192.168.201.137 [15]
*May 27 15:33:59.645: OSPF-1 ADJ   Gi1: Rcv DBD from 192.168.201.137 seq 0xDE7 opt 0x52 flag 0x2 len 112  mtu 9100 state EXSTART
```

Refer to the exhibit. The OSPF neighborship fails between two routers. What is the cause of this issue?

A. The OSPF process is stopped on the neighbor router.

B. The OSPF router ID is missing on this router.

C. The OSPF router ID is missing on the neighbor router.

D. There is an MTU mismatch between the two routers.

Correct Answer: *D*

Community vote distribution

D (100%)

nushadu Highly Voted 11 months, 1 week ago

Selected Answer: D

cisco_R2(config-subif)#do debug ip osp adj
OSPF adjacency debugging is on
cisco_R2(config-subif)#ip mtu 1111 <<<<<<<<<<<<<<<<
cisco_R2(config-subif)#
cisco_R2(config-subif)#
cisco_R2(config-subif)#do clear ip ospf

!!!debug shows this:
cisco_R2(config-subif)#
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Rcv DBD from 6.6.6.6 seq 0x19FD opt 0x52 flag 0x7 len 32 mtu 1500 state EXSTART
<<<<<<<<<<<<<<
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Nbr 6.6.6.6 has larger interface MTU <<<<<<<<<
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Rcv DBD from 6.6.6.6 seq 0x26B opt 0x52 flag 0x2 len 112 mtu 1500 state EXSTART
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Nbr 6.6.6.6 has larger interface MTU
*Dec 23 13:02:27.395: OSPF-1 ADJ Et0/0.10: Rcv DBD from 6.6.6.6 seq 0x26B opt 0x52 flag 0x2 len 112 mtu 1500 state EXSTART

upvoted 5 times

Lungful Most Recent 4 months ago

Selected Answer: D

Voting, D - MTU issue.

upvoted 1 times

[Removed] 5 months ago

Selected Answer: D

As stated, MTU mismatch

upvoted 1 times

bora4motion 1 year ago

Selected Answer: D

Stuck in ExStart and jumbo points to MTU.

upvoted 3 times

amadeu 1 year, 1 month ago

D, is the correct.

upvoted 1 times

kebkim 1 year, 1 month ago

Neighbor Stuck in Exstart Exchange State :
OSPF neighbors that are in the exstart or exchange state are trying to exchange DD packets. The adjacency should continue past this state. If it does not, there is a problem with the DD exchange, such as a maximum transmission unit (MTU) mismatch or the receipt of an unexpected DD sequence number.

upvoted 4 times

Question #507 *Topic 1*

What is one benefit of adopting a data modeling language?

A. augmenting the use of management protocols like SNMP for status subscriptions

B. refactoring vendor and platform specific configurations with widely compatible configurations

C. augmenting management process using vendor centric actions around models

D. deploying machine-friendly codes to manage a high number of devices

Correct Answer: *B*

Community vote distribution

B (85%) D (15%)

sull3y Highly Voted 8 months ago

Both options B and D are relevant to the question, but if we consider the term "widely compatible configurations" specifically, then option B would be the most relevant.

Refactoring vendor and platform-specific configurations with widely compatible configurations means creating a standardized way to represent network data that can be used across different vendor platforms, which would make configurations widely compatible. This is a direct benefit of adopting a data modeling language.

On the other hand, while deploying machine-friendly codes to manage a high number of devices is also a potential benefit, it is not directly related to the idea of creating widely compatible configurations, which is what the question is asking about.

upvoted 5 times

HungarianDish Highly Voted 8 months ago

Selected Answer: B

I did not find any documents which would clearly exclude answer D, still, I am going for B. Consistency and standardization seem to be the main advantage of data models, which is more in line with answer B (vendor/platform independent).

https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/programability/63x/b-programmability-cg-63x-ncs5xx/cg_63_data_models_scope_need_and_benefits.pdf
"Data models can be used to automate configuration tasks across heterogeneous devices in a network."

https://developer.cisco.com/docs/ios-xe/#!model-based-management-introduction/data-models
Open Models are supported for IOS-XE.
"Open models are models designed to be independent of the underlying platform implementation."

https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/programability/63x/b-programmability-cg-63x-ncs5xx/cg_63_data_models_scope_need_and_benefits.pdf
Although this document reads "automating the configuration using data models
results in scalability."
Scalability seems to be linked rather to hierarchical network design.

upvoted 5 times

ibogovic Most Recent 4 months, 3 weeks ago

Selected Answer: B

B. Refactoring vendor and platform-specific configurations with widely compatible configurations.

By adopting a data modeling language, organizations can create vendor-neutral and platform-agnostic configurations that are widely compatible across different network devices and platforms.

This benefit of refactoring vendor and platform-specific configurations allows for greater flexibility and interoperability in network deployments. Instead of being tied to proprietary configuration formats and limited vendor-specific features, adopting a data modeling language enables organizations to create reusable and consistent configurations that can be applied to a variety of network devices from different vendors.

upvoted 2 times

[Removed] 5 months ago

Selected Answer: B

There's no specific resource I could fine, but a few that can point to B being the best answer, one such resource I found was this:

https://www.sciencedirect.com/topics/computer-science/data-modeling-language

upvoted 2 times

teikitiz 4 months, 4 weeks ago

I agree. D refers machine-friendly. Most of the efforts towards data modeling attempt user-friendliness, so ruled this one out.

upvoted 1 times

Clauster 8 months, 1 week ago

Selected Answer: B

Answer is B, they are not talking about Code Languages they are talking about Data Structure like Yang which leverages RESTCONF and NETCONF, they are used to make vendors configuration compatible with each other, that's the entire point of YANG

upvoted 2 times

sebol773 8 months, 3 weeks ago

Selected Answer: D

should be D

upvoted 2 times

eojedad 8 months, 4 weeks ago

I think D is the right answer

upvoted 1 times

ibrahimtraore156 9 months ago

D is the right answer

upvoted 1 times

Bigbongos 10 months ago

is b correct? seems off

upvoted 3 times

Question #508 *Topic 1*

In Cisco DNA Center what is the integration API?

A. southbound consumer-facing RESTful API, which enables network discovery and configuration management

B. westbound interface, which allows the exchange of data to be used by ITSM, IPAM and reporting

C. an interface between the controller and the network devices, which enables network discovery and configuration management

D. northbound consumer-facing RESTful API which enables network discovery and configuration management

Correct Answer: *B*

Community vote distribution

B (100%)

siteoforigin Highly Voted 1 year, 2 months ago

Selected Answer: B

https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/integration-api-westbound

upvoted 6 times

kebkim Most Recent 1 year, 2 months ago

Westbound—Integration APIs

The westbound APIs provide the capability to publish the network data, events and notifications to the external systems and consume information in Cisco DNA Center from the connected systems.

upvoted 4 times

Question #509 *Topic 1*

An engineer must configure a new WLAN that allows a user to enter a passphrase and provides forward secrecy as a security measure. Which Layer 2 WLAN configuration is required on the Cisco WLC?

A. WPA3 Enterprise

B. WPA2 Personal

C. WPA2 Enterprise

D. WPA3 Personal

Correct Answer: *D*

Community vote distribution

D (100%)

Cer_Pit Highly Voted 1 year ago

Selected Answer: D

D is correct

WPA3-Personal provides the following key advantages:
• Creates a shared secret that is different for each SAE authentication.
• Protects against brute force “dictionary” attacks and passive attacks.
• Provides forward secrecy. <---
Reference: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/wpa3-dep-guide-og.pdf

WPA3 Personal provides forward secrecy.
Reference: https://blogs.cisco.com/networking/wpa3-bringing-robust-security-for-wi-fi-networks

upvoted 7 times

due Most Recent 2 months, 4 weeks ago

Selected Answer: D

Keyword,
"enter a passphrase" = WPA Personal (WPA-PSK): WPA Personal uses a Pre-Shared Key (PSK)
"forward secrecy as a security measure" = WPA3: Implements perfect forward secrecy, WPA2 can can decrypt all the captured.

= WPA3 Personal

upvoted 2 times

Deu_Inder 1 year, 2 months ago

Selected Answer: D

D looks good.
https://www.wi-fi.org/discover-wi-fi/security

upvoted 2 times

Question #510 *Topic 1*

How does an on-premises infrastructure compare to a cloud infrastructure?

A. On-premises offers faster deployment than cloud.

B. On-premises requires less power and cooling resources than cloud.

C. On-premises offers lower latency for physically adjacent systems than cloud.

D. On-premises can increase compute power faster than cloud.

Correct Answer: *C*

Community vote distribution

C (100%)

[Removed] 5 months ago

Selected Answer: C

correct

upvoted 2 times

bora4motion 1 year ago

Selected Answer: C

C is correct

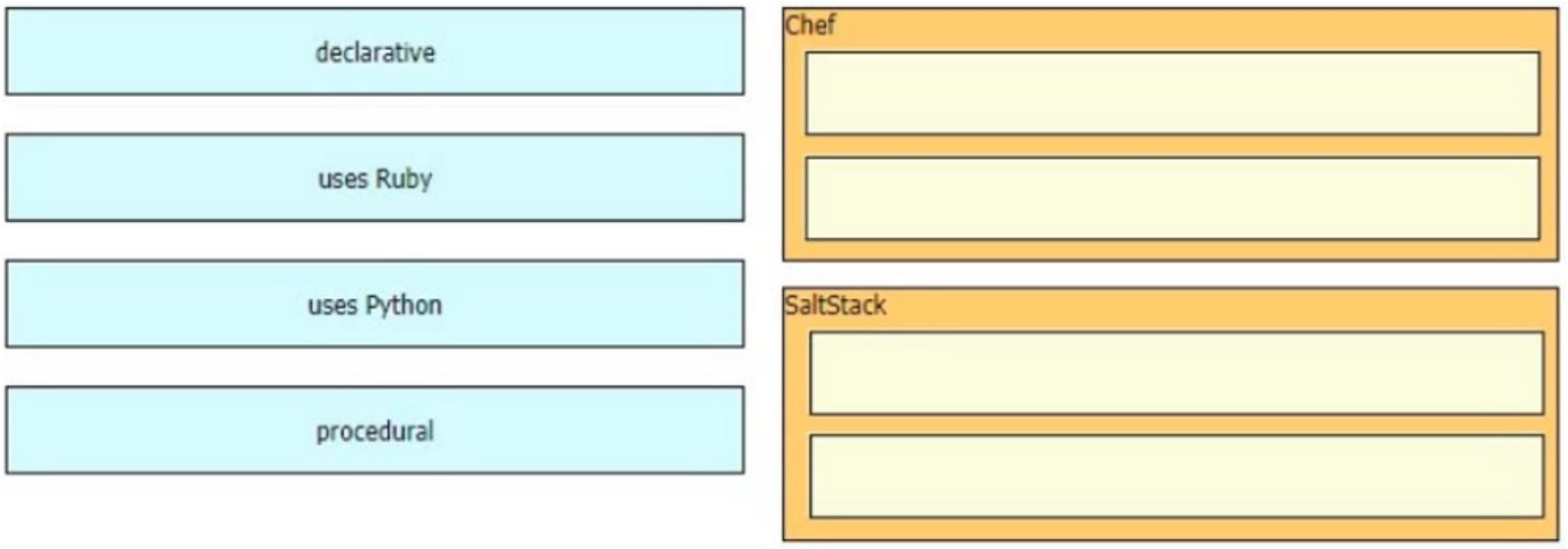
upvoted 4 times

Question #511 *Topic 1*

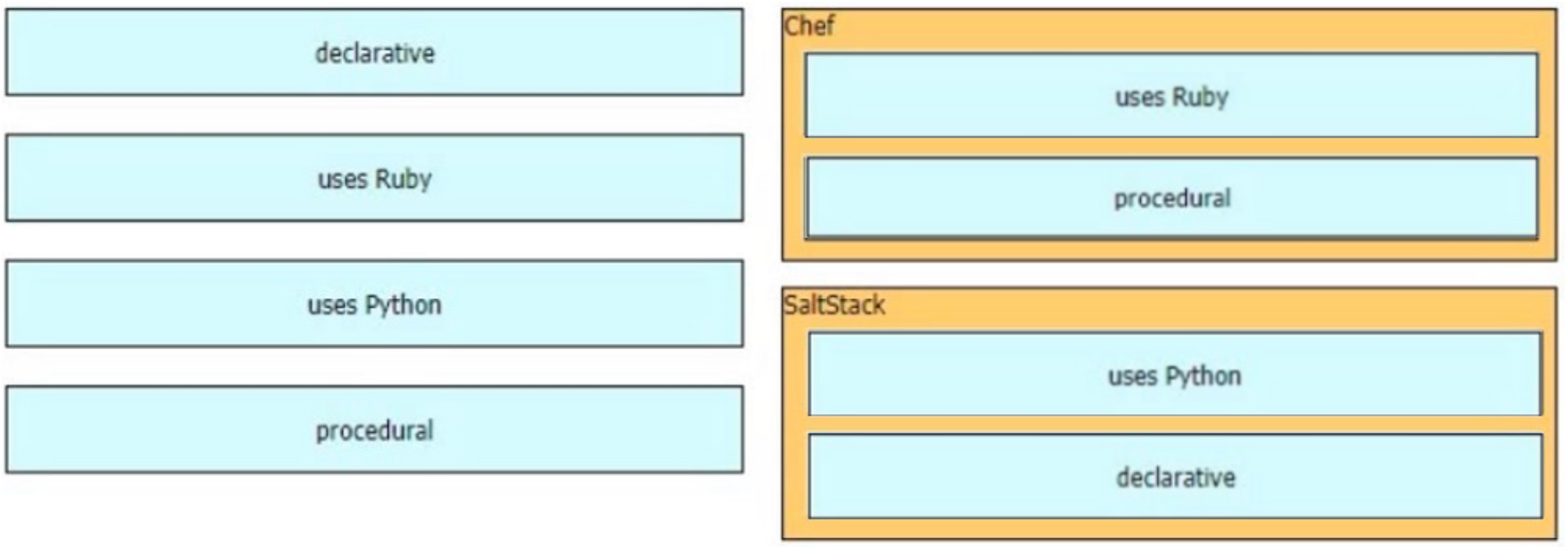
DRAG DROP -

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

Select and Place:



Correct Answer:



[Removed] 5 months ago

correct

upvoted 1 times

teikitiz 4 months, 4 weeks ago

It's one of those questions. Solution matches this link:
https://www.ibm.com/cloud/blog/chef-ansible-puppet-terraform

However, the encore examcram says explicitly Chef is declarative...

upvoted 2 times

[Removed] 4 months, 3 weeks ago

Holy hell, this test is a mess...
Thanks for correcting me.
But Saltstack is also declarative...
I hate Cisco for ham-fisting automation when they cannot bother doing proper questions around INTRODUCTION to programming. I'm not a programmer, but these programing questions are infuriating.

upvoted 6 times

Colmenarez 4 months ago

son de lo peos

upvoted 1 times

Muste 6 months, 1 week ago

the provided answers are correct
https://www.ibm.com/cloud/blog/chef-ansible-puppet-terraform#:~:text=There%20are%20a%20number%20of,achieve%20the%20desired%20end%20state.

upvoted 2 times

Nickplayany 7 months, 1 week ago

CHEF:

Ruby and declarative

SaltStack:

Python and procedural
upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago
look at question 374.

Chef communicates using the knife tool, and is procedural.
SaltStack is Declarative and communicates through SSH
upvoted 1 times

Nickplayany 7 months, 1 week ago
Well, I have been reading about it a lot. My conclusion is that both CHEF and SaltStack are DECLARATIVE. However, Chef does MORE Procedural config tasks than saltstack.

So my above answer is wrong
upvoted 2 times

Badger_27 8 months, 4 weeks ago
Just re-read the OCG - no mention of 'declarative' as a defining characteristic.
upvoted 3 times

x3rox 9 months, 1 week ago
A lot of conflicting information. I tried to review the official information about this topic:
hat is a Declarative Model Language:
this means a user describes the desired final state (for example, “this VLAN must be present” or “this route must be present”) rather than describing a series of steps to execute.

Chef
Use simple declarative definitions for common tasks or easily extend them to support the most unique environmental requirements.
SRC:https://www.chef.io/products/chef-infra

Chef, with its easy to implement, declarative, and configuration management capabilities, can aid in overcoming some of the challenges faced by IT Teams.
SRC: https://www.chef.io/webinars/managing-your-endpoint-state-as-code
upvoted 1 times

x3rox 9 months, 1 week ago
Chef is built around a couple simple concepts: achieving a desired state and a centralized modeling of IT infrastructure. Chef enables you to quickly manage almost any infrastructure. Chef is based on Ruby, uses a declarative intent-based model, is agent-based, and refers to its automation instructions as recipes.
SRC: CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram

Chef, another popular configuration management tool, follows much the same model as Puppet. Chef is based in Ruby, uses a declarative model, is agent based, and refers to the Chef automation instruction as recipes (groups of which are called cookbooks).
SRC: 31 Days Before Your CCNP and CCIE Enterprise Core Exam
upvoted 2 times

x3rox 9 months, 1 week ago
SALTSTACK

SaltStack supports both of the leading methodologies to define system configurations. Follow a declarative methodology using SaltStack’s powerful requisites system, or go imperative with SaltStacks built-in ordered execution.
SRC: https://docs.saltproject.io/en/getstarted/flexibility.html

You can use SaltStack’s declarative configuration language, YAML and Jinja, to define the desired State of the machine in a clear and concise way.
SRC: https://blogs.vmware.com/management/2023/02/getting-started-with-saltstack-config-working-with-reactors.html
upvoted 1 times

x3rox 9 months, 1 week ago
what a mess!!
upvoted 1 times

snarkymark 10 months ago
Answer is correct:
https://blog.gruntwork.io/why-we-use-terraform-and-not-chef-puppet-ansible-saltstack-or-cloudformation-7989dad2865c
upvoted 2 times

MO_2022 11 months ago
Answer is correct
Chef is procedural and Saltstack is declarative.
upvoted 3 times

Darude 1 year ago

Answer is correct
reference: https://www.ibm.com/cloud/blog/chef-ansible-puppet-terraform

upvoted 2 times

H3kerman 1 year ago

Chef and Ansible use a procedural style language where you write code that specifies, step-by-step, how to achieve the desired end state

upvoted 1 times

dougj 1 year, 1 month ago

Answer is wrong Chef is a declarative model

upvoted 1 times

bendarkel 1 year ago

The answer is correct. Stop misleading people.

upvoted 10 times

x3rox 9 months, 1 week ago

He is not misleading. There are conflicting information about this, but most likely Chef is Declarative based on the official website not blogs. Read my post from official sources. 1 point in the exam could make the difference in failing the test or succeeding.

upvoted 1 times

Just0808 1 year, 1 month ago

Answer is correct, seem who said wrong is intruder :) here

upvoted 4 times

Radwa_ 1 year, 1 month ago

The given answer is not correct.
Chef: Declarative
SaltStack: procedural

upvoted 2 times

civan 11 months ago

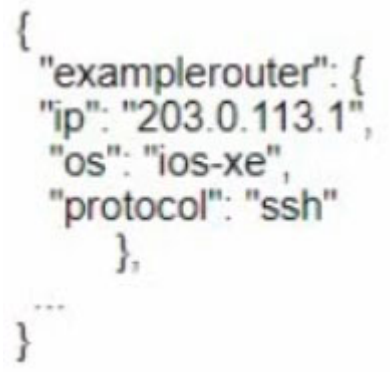
No, Chef is procedural and Saltstack is declarative.

https://www.ibm.com/cloud/blog/chef-ansible-puppet-terraform

upvoted 2 times

Question #512 *Topic 1*

An engineer must create a script to append and modify device entries in a JSON-formatted file. The script must work as follows:
☞ Until interrupted from the keyboard, the script reads in the hostname of a device, its management IP address operating system type, and CLI remote access protocol.
☞ After being interrupted, the script displays the entered entries and adds them to the JSON-formatted file, replacing existing entries whose hostname matches.
The contents of the JSON-formatted file are as follows:



Drag and drop the statements onto the blanks within the code to complete the script. Not all options are used.
Select and Place:

Correct Answer:

MO_2022 Highly Voted 11 months, 2 weeks ago

1. import json
2. while True:
3. except
4. File = open
5. File.close()

upvoted 22 times

Arnaud_R1 Highly Voted 1 year, 2 months ago

In that case, it should be File = open instead of File.open()
"File" is not defined in the script before, so no method can be applied to it. Also, the parenthesis after the blank field help us here.

upvoted 13 times

x3rox 10 months ago

Thank you mate!

upvoted 1 times

eojedad Most Recent 8 months, 2 weeks ago

definitly is File = open, compared to question 496 ...outfile = open(...)

upvoted 1 times

nushadu 11 months, 1 week ago

JSON Library in Python
Method >>>>>>>>> Description
dumps() >>>>>>>>> encoding to JSON objects
dump() >>>>>>>>> encoded string writing on file
loads() >>>>>>>>> Decode the JSON string
load() >>>>>>>>> Decode while JSON file read

upvoted 5 times

ccnptoppler34 1 year, 2 months ago

it should be File = open instead of File.open()

upvoted 9 times

Question #513 *Topic 1*

```
FastEthernet1/0/47 - Group 1 (version 2)
   State is Standby
      7 state changes, last state change 00:00:02
   Virtual IP address is 10.1.1.1
   Active virtual MAC address is 0000.0c9f.f001
      Local virtual MAC address is 0000.0c9f.f001 (v2 default)
   Hello time 3 sec, hold time 10 sec
      Next hello sent in 0.375 secs
   Authentication MD5, key-string "cisco"
   Preemption enabled, delay min 5 secs
   Active router is 10.1.1.2, priority 255 (expires in 9.396 sec)
   Standby router is local
   Priority 100 (default 100)
   IP redundancy name is "hsrp-Fa1/0/47-1" (default)
```

Refer to the exhibit. An engineer configures HSRP and enters the show standby command. Which two facts about the network environment are derived from the output? (Choose two.)

A. If the local device fails to receive a hello from the active router for more than 5 seconds, it becomes the active router.

B. If a router with a higher IP address and same HSRP priority as the active router becomes available that router becomes the new active router 5 seconds later.

C. The virtual IP address of the HSRP group is 10.1.1.1.

D. The hello and hold timers are set to custom values.

E. The local device has a higher priority setting than the active router.

Correct Answer: *BC*

Community vote distribution

BC (59%) AC (26%) CD (15%)

gibblock Highly Voted 7 months, 3 weeks ago

B. is ONLY valid if the "other" router has preemption enabled. How can anybody tell?
D. wrong
E. wrong

Correct answers
A. since the local router has preemption enabled with a minimum 5 sec. delay it becomes the active router.
C. Obviously the virtual IP is 10.1.1.1
upvoted 6 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago

Confirmed in CML A is the answer.

We do not have enough info for B to be accurate.

I killed the linke from R1 to R2 and R2 took over even with priority of 100 over 255. Simply because preempt is enabled on R2

Its easy for everyone here to talk and link articles, but have you guys actually labbed this stuff to find out if it practically works?

Too many book worms around here.

HSRP_R1(config-if)#do show standby
GigabitEthernet0/1 - Group 0 (version 2)
State is Standby
12 state changes, last state change 00:00:41
Virtual IP address is 10.10.1.1
Active virtual MAC address is 0000.0c9f.f000
Local virtual MAC address is 0000.0c9f.f000 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.048 secs
Preemption disabled

Active router is 10.10.1.3, priority 100 (expires in 9.872 sec)
MAC address is 5254.001e.efc3
Standby router is local
Priority 255 (configured 255)
Group name is "hsrp-Gi0/1-0" (default)

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Here is the #show standby command from R2

GigabitEthernet0/1 - Group 0 (version 2)
State is Active
7 state changes, last state change 00:01:34
Virtual IP address is 10.10.1.1
Active virtual MAC address is 0000.0c9f.f000
Local virtual MAC address is 0000.0c9f.f000 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.032 secs
Preemption enabled, delay min 5 secs
Active router is local
Standby router is 10.10.1.2, priority 255 (expires in 8.320 sec)
Priority 100 (default 100)
Group name is "hsrp-Gi0/1-0" (default)

upvoted 1 times

djedeen 3 months, 1 week ago

Selected Answer: BC

Not A: hold timer is 10 seconds (not 5 sec)

upvoted 1 times

Lungful 4 months ago

Selected Answer: BC

I do not think A can be correct because the router would not be considered down until the 10 second hold time has elapsed and only then would the 5 second preempt start. A mentions time after a missed hello not after a down state. B+C are what I would pick.

upvoted 2 times

danman32 4 months ago

B does seem to be the best 2nd answer but the "5 seconds later" is a problem because we don't know what the preempt settings are on the other routers. We can only assume all have preempt enabled with 5 second delay.

upvoted 2 times

alex711 4 months, 2 weeks ago

Selected Answer: BC

BC is correct

upvoted 2 times

CKL_SG 4 months, 3 weeks ago

Selected Answer: BC

HSRP uses two types of timers — hello and hold timers — to ensure redundancy among routers. The hello timer sends multicasts, or hello packets that broadcast status and priorities every three seconds. By default, if you don't tune in anything, the active and standby routers will say "hello" to each other once every three seconds. The hold timer tells the standby router when to take over. The standby router becomes active when it hasn't received a hello packet from the primary router in 10 seconds. So, worst case scenario, you've got 10 seconds before a standby router takes over and the timer settings can be lowered.
A- Are wrong because Standby router only take over after 10 sec not 5 sec base on default hello timer and hold timer

upvoted 2 times

tempaccount00001 4 months, 3 weeks ago

Selected Answer: BC

its deffinitely BC

upvoted 2 times

[Removed] 5 months, 2 weeks ago

Selected Answer: AC

Not enough information to deduce that B will be true. Preemption is required and that's not indicated.

upvoted 2 times

Entivo 5 months, 2 weeks ago

Selected Answer: AC

Its A and C

upvoted 1 times

Pilgrim5 7 months, 1 week ago

Selected Answer: AC

A seems correct. Why?

The Delay minimum quoted as 5 secs in the question means preempt delay.

The preempt delay means that, when the interface gets up it will detect that there is already an hsrp neighbour active. Thus, that active router will continue forward traffic, and this router will wait for configured time until it takes over the role.

If we don't wait, we will take over the active role immediate and that can be a problem if routing is not yet ready.

Also, if the other router is not detected, this router will take the active role immediate, and do not wait the configured time, and starts forward traffic as soon as routing is ready.
Source : https://community.cisco.com/t5/switching/hsrp-delay-minimum-amp-reload-question/td-p/3327186

C of course is right as seen from the output that the VIP is 10.1.1.1

upvoted 4 times

HungarianDish 7 months, 3 weeks ago

Only C) is valid right now. In order for B) to work, preemption needs to be enabled on the new device. We do not have that information about the new device. Preemption is not enabled by default in HSRP.

upvoted 3 times

Morticians 9 months, 2 weeks ago

Selected Answer: BC

The priority field is used to elect the active router and the standby router for the specific group. In the case of an equal priority, the router with the highest IP address for the respective group is elected as active. Furthermore, if there are more than two routers in the group, the second highest IP address determines the standby router and the other router/routers are in the listen state.

https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9281-3.html#q4

upvoted 2 times

[Removed] 5 months, 1 week ago

HSRP does not have preemption enabled by default. You can't infer that the new device will have that configuration as there is no indication of it. The only other best answer is A based on the information provided.

upvoted 1 times

kewokil120 10 months ago

Selected Answer: CD

Not b. You don’t know if other router will have preempt. Timers a default and vip is correct

upvoted 4 times

chefexam 9 months, 3 weeks ago

Timers are default, therefore Answer D is defenitely wrong.

upvoted 3 times

nushadu 11 months, 1 week ago

Selected Answer: BC

the rest choices are false (deduction method in the mathematics)

upvoted 2 times

Muste 6 months, 1 week ago

the priority of the shown router is 100 but the priority of the router who is active is 255 so think

upvoted 1 times

gibblock 7 months, 3 weeks ago

Your math "deduction" does not add up buddy.

upvoted 1 times

Japsurd 1 year ago

Hmm, B,C and D are true.

upvoted 1 times

Jebrony 11 months, 4 weeks ago

Dis NOT True.
Hello and hold timers are set to default value (3 & 10 sec). Hence, not custom value.

upvoted 8 times

iEpsilon 1 year, 1 month ago

Selected Answer: BC

Correct
https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9281-3.html#:~:text=The%20priority%20field,default%20of%20100.https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9281-3.html#:~:text=The%20priority%20field,default%20of%20100.

upvoted 3 times

Question #514 *Topic 1*

```
R1#show ip ospf interface Gi0/0
GigabitEthernet0/0 is up, line protocol is up
 Internet Address 172.20.0.1/24, Area 0, Attached via
Network Statement
 Process ID 1, RouterID 172.20.0.1, Network Type
BROADCAST, Cost: 1
 Topology-MTID    Cost    Disabled    Shutdown
Topology Name
       0           1         no          no
Base
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 172.20.0.1, Interface address
172.20.0.1
 No backup designated router on this network
 Timer intervals configured,Hello 10,Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
 Supports Link-local Signaling (LLS)
 Cisco NSF helper support enabled
 IETF NSF helper support enabled
 Index 1/1/1, flood queue length 0
 Next 0x0(0)/0x0(0)/0x0(0)
 Last flood scan length is 0, maximum is 0
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
```

```
R2#show ip ospf interface Gi0/0
GigabitEthernet0/0 is up, line protocol is up
 Internet Address 172.20.0.2/24, Area 0, Attached via
Network Statement
 Process ID 1, RouterID 172.20.0.2, Network Type
BROADCAST, Cost: 5
 Topology-MTID    Cost    Disabled    Shutdown
Topology Name
       0           5         no          no
Base
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 172.20.0.2, Interface address
172.20.0.2
 No backup designated router on this network
 Timer intervals configured,Hello 10,Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
 Supports Link-local Signaling (LLS)
 Cisco NSF helper support enabled
 IETF NSF helper support enabled
 Index 1/1/1, flood queue length 0
 Next 0x0(0)/0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 2
 Last flood scan time is 2 msec, maximum is 2 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
```

Refer to the exhibit. Cisco IOS routers R1 and R2 are interconnected using interface Gi0/0. Which configuration allows R1 and R2 to form an OSPF neighborship on interface Gi0/0?

A. R2(config)#interface Gi0/0 R2(config-if)#ip ospf cost 1

B. R1(config)#router ospf 1 R1(config-if)#network 172.20.0.0 0.0.0.255 area 1

C. R1(config)#router ospf 1 R1(config-router)#no passive-interface Gi0/0

D. R2(config)#router ospf 1 R2(config-router)#passive-interface Gi0/0

Correct Answer: *C*

Community vote distribution

C (100%)

HarwinderSekhon 5 months, 2 weeks ago

R1 output says ("No hellos, passive interface")

upvoted 1 times

bora4motion 1 year ago

Selected Answer: C

C is correct - Gi0/0 on R1 is not sending hellos on that interface.

upvoted 3 times

Mze 1 year ago

100%, answer is correct

upvoted 1 times

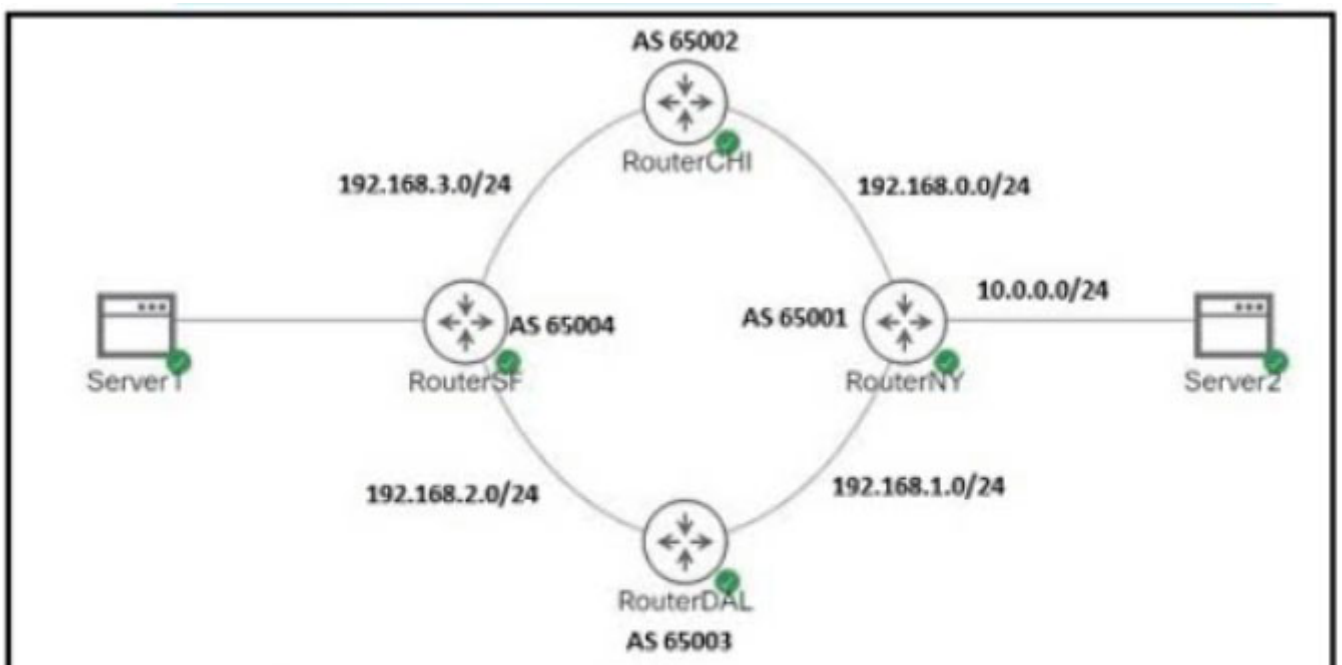
bendarkel 1 year ago

Selected Answer: C

Answer is correct.

upvoted 2 times

Question #515 *Topic 1*




```
RouterSF#show ip route 10.0.0.0
Routing entry for 10.0.0.0/24, 1 known subnets
B       10.0.0.0 [20/0] via 192.168.2.2, 00:03:23
RouterSF#
RouterSF#show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/24, version 8
Paths: (2 available, best #2, table default)
Multipath: eiBGP
  Advertised to update-groups:
     2
  Refresh Epoch 1
  65002 65001
    192.168.3.2 from 192.168.3.2 (192.168.3.2)
      Origin IGP, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
      Updated on Sep 22 2020 21:32:27 UTC
  Refresh Epoch 2
  65003 65001
    192.168.2.2 from 192.168.2.2 (192.168.2.2)
      Origin IGP, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
      Updated on Sep 22 2020 21:31:57 UTC
RouterSF#
```

Refer to the exhibit. After configuring the BGP network an engineer verifies that the path between Server1 and Server2 is functional. Why did RouterSF choose the route from RouterDAL instead of the route from RouterCHI?

A. BGP is not running on RouterCHI

B. There is a static route in RouterSF for 10.0.0.0/24

C. The route from RouterDAL has a lower MED

D. The Router-ID for Router DAL is lower than the Router-ID for RouterCHI

Correct Answer: *C*

Community vote distribution

D (100%)

djedeen 3 months, 2 weeks ago

Selected Answer: D

D: note the BGP router ID is shown in parens (192.168.3.2) vs (192.168.2.2). . .

upvoted 2 times

dudalykai 4 months, 2 weeks ago

When a NEW path is learned, and the new path has all identical path attributes, the CURRENT BEST path remains as "best". The idea is the current path is likely more stable than the path which was just learned. (oldest path)

When a CURRENT best path is forgotten/lost, then among the REMAINING paths, the next chosen "best" path is the one from the BGP speaker

with the best Router ID -- the age of the remaining paths are not considered.

The "prefer oldest path"only applies when a new path is learned, not when an best path is forgotten and the speaker is picking among remaining paths.
The answer should be the the oldest path is via RouterDAL
upvoted 2 times

Brandonkiaora 3 weeks ago
You are correct, the below path was first learned, and then the above path.
Oldest path method is not included in We Love Orange As Orange Mean Refreshment, so I understand why D is the answer here.
upvoted 1 times

bora4motion 1 year ago
Selected Answer: D
It's D. With default attribute values it really comes down to router id.
upvoted 3 times

ccnptoppler34 1 year, 2 months ago
Selected Answer: D
router ID answer D
upvoted 2 times

Caledonia 1 year, 2 months ago
Selected Answer: D
The answer is D
upvoted 1 times

Deu_Inder 1 year, 2 months ago
Selected Answer: D
The tie breaker here will be the router ID. Lower the better.
upvoted 2 times

siteoforigin 1 year, 2 months ago
Selected Answer: D
All things being the same, we see that DAL has the lower router ID. C does not make sense, as the med value is stripped when crossing AS's and is only useable for iBGP peers.
upvoted 1 times

bk989 7 months, 1 week ago
MED can be advertised from an outside AS to the AS to choose the path out. Like Localpref chooses the path out from within. In this context MED makes sense, but we don't have that information, so the next choice is lower RID, because it is assumed lower RID = more stable topology
upvoted 1 times

Deu_Inder 1 year, 2 months ago
I agree with the answer you chose, but regarding MED, you might be wrong. MED is non-transitive. But you can use it between ASes. Only, the AS which received the MED, cannot forward it to another AS.
upvoted 2 times

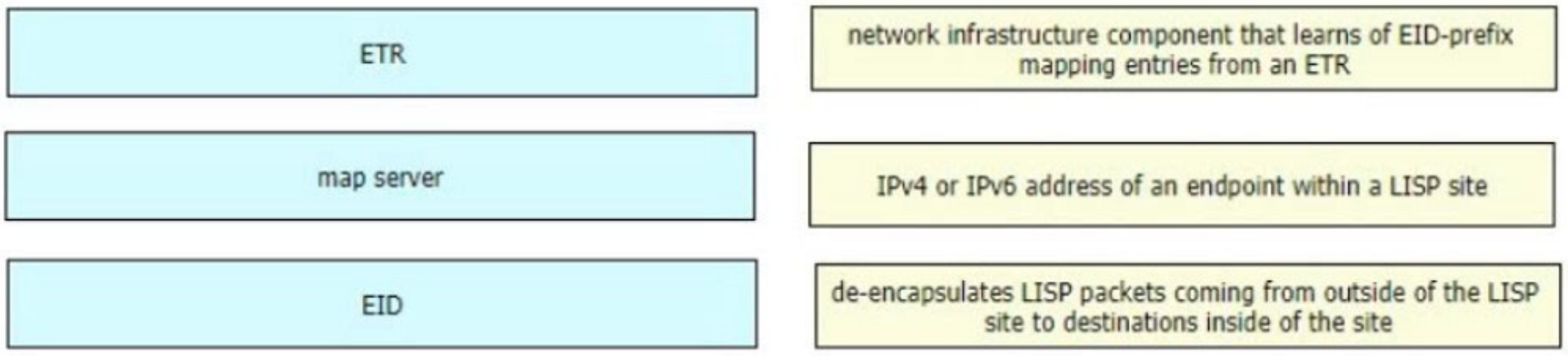
Lalane 1 year ago
I agreed with you, MED atribute can pass from AS to another (can be redistribute inside destination AS too) but no to can not cross a second one AS
upvoted 1 times

FelipePadilha 9 months, 4 weeks ago
MED has local meaning only (hence, its a Cisco attribute, not RFC attribute), its is LOCALPREF that can be redistribuited
upvoted 1 times

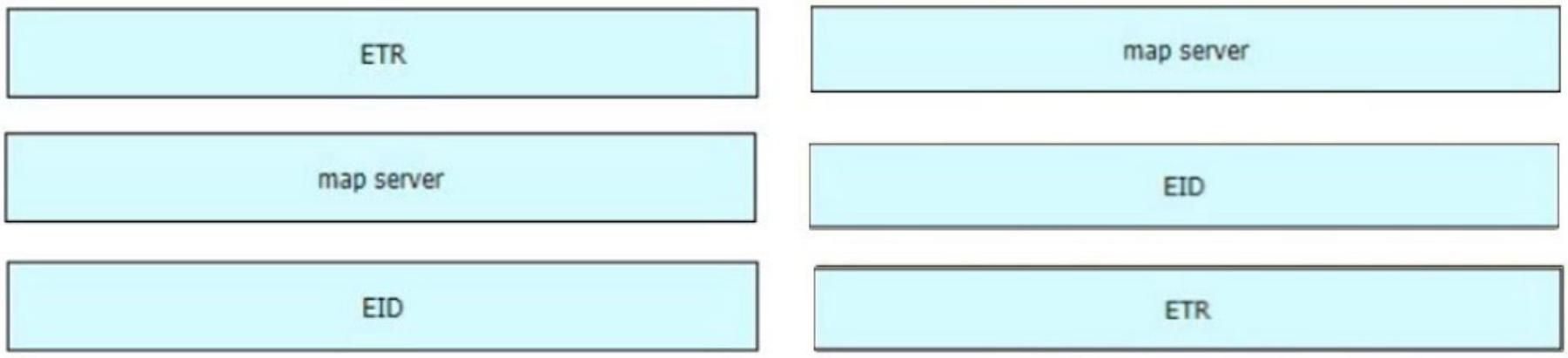
DRAG DROP -

Drag and drop the LISP components on the left to the correct description on the right.

Select and Place:



Correct Answer:



Radwa_ Highly Voted 1 year, 1 month ago

The given answer is correct.

upvoted 6 times

CCNPWILL Most Recent 1 month, 3 weeks ago

Given answer is correct. to clear confusion about EID and ETR:

Egress Tunnel Router (ETR): When a LISP-encapsulated packet arrives at the destination site, the ETR is responsible for de-encapsulating the packet. It extracts the original packet and forwards it to the destination host within the LISP site.

courtesy of ChatGPT.

upvoted 1 times

mgiuseppe86 2 months, 1 week ago

This answer is wrong. ETR should be "de-encapsulates LiSP packets from inside the site to destinations OUTSIDE of the site

upvoted 1 times

[Removed] 5 months ago

The given answer is correct.

upvoted 3 times

x3rox 10 months ago

If the packets are coming from outside the LISP site how is it possible to decapsulate something that is not LISP-enabled??

upvoted 4 times

PureInertiaCopy 3 months, 2 weeks ago

My thoughts exactly.

upvoted 1 times

```
Router#show access-lists
Extended IP access list 100
    10 permit ip 192.168.0.0 0.0.255.255 any
    20 permit ip 172.16.0.0 0.0.15.255 any
```

Refer to the exhibit. Which command set must be added to permit and log all traffic that comes from 172.20.10.1 in interface GigabitEthernet0/1 without impacting the functionality of the access list?

A.

```
Router(config)#access-list 100 permit ip host 172.20.10.1 any log
Router(config)#interface GigabitEthernet0/1
Router(config-if)#access-group 100 in
```

B.

```
Router(config)#access-list 100 seq 5 permit ip host 172.20.10.1 any log
Router(config)#interface GigabitEthernet0/1
Router(config-if)#access-group 100 in
```

C.

```
Router(config)#ip access-list extended 100
Router(config-ext-nacl)#5 permit ip 172.20.10.0 0.0.0.255 any log
Router(config)#interface GigabitEthernet0/1
Router(config-if)#access-group 100 in
```

D.

```
Router(config)#no access-list 100 permit ip 172.16.0.0 0.0.15.255 any
Router(config)#access-list 100 permit ip 172.16.0.0 0.0.15.255 any log
Router(config)#interface GigabitEthernet0/1
Router(config-if)#access-group 100 in
```

Correct Answer: *A*

[Removed] Highly Voted 5 months, 2 weeks ago

A

Two things to keep in mind. 1) the requirement of "WITHOUT impacting the functionality of the access list, and 2) the wildcard mask of ACE #20 does not overlap with the 172.20.10.1/32 therefore not affecting it
Another thing to note is that without the sequence keyword, the new ACE is added at the end of the list.

upvoted 5 times

rogi2023 5 months ago

very clear explanation.

upvoted 1 times

nushadu Highly Voted 11 months ago

A. tested again:
cisco_R3#show access-lists 123
Extended IP access list 123
5 permit ip host 1.1.1.1 any log
15 permit ip host 4.4.4.0 any log
cisco_R3#s runn | i 123
access-list 123 permit ip host 1.1.1.1 any log
access-list 123 permit ip host 4.4.4.0 any log

cisco_R3#
cisco_R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cisco_R3(config)#access-list 123 permit ip host 172.20.10.1 any log <<<<<<<<<<<<<<<<<
cisco_R3(config)#^Z
cisco_R3#
cisco_R3#s runn | i 123
access-list 123 permit ip host 1.1.1.1 any log
access-list 123 permit ip host 4.4.4.0 any log
access-list 123 permit ip host 172.20.10.1 any log <<<<<<<<<<<<<<<

cisco_R3#show access-lists 123
Extended IP access list 123
5 permit ip host 1.1.1.1 any log
15 permit ip host 4.4.4.0 any log

25 permit ip host 172.20.10.1 any log <<<<<<<<<<<<<<<<<<<<
cisco_R3#
upvoted 5 times

CCNPWILL Most Recent 1 month, 3 weeks ago
A is the correct answer. Been working with Cisco for a while I can just snipe correct syntax. idk what else to say.. Good luck folks. A is the correct answer.
upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago
People saying "B" do you have access to any network gear at all? or are you all book jockies? JFC. No wonder half the network admin pop sucks at their job, they have all these certs yet never touch a CLI

LAB THIS STUFF BEFORE YOU COMMENT

Answer is A
upvoted 1 times

alex711 4 months, 1 week ago
Sorry. my answer is wrong. C is not correct. But A is correct.
upvoted 2 times

alex711 4 months, 1 week ago
C is correct 100%
upvoted 1 times

foreignbishop 6 months, 1 week ago
"...without impacting the functionality of the access list." IMO, once you add 5 you are changing the operation of the existing ACL.
upvoted 3 times

AbandonedDonner 6 months, 3 weeks ago
Correct is answer C

Answer A cannot be correct, as if the entry is added without sequence number is placed at the end, so its processed last. If its processed last then the same traffic will be matched earlier by 172.16.0.0. 0.0.15.255 statement and in result log will never be generated !! And question specifically ask for log !

Correct is answer C as correctly position new entry before 172.16.0.0. 0.0.15.255 statement thus enable logging, while not altering the rest of the ACL as the 172.20.10.0 0.0.0.255 would be matched by later statement and permitted.
upvoted 3 times

Chuckzero 3 months ago
Not quite. The idea of a sequence number is to put the interesting traffic where you want it to be on the ACE. For example, if you have already permitted all traffic for a subnet and now wants to deny a single host from that subnet, then you will use sequence number to place it above the earlier permit statement, because ACL is processed from top-to-bottom. If you put the deny statement without a sequence number, it will append the ace at the bottom of the list, and it won't be effective for the purpose that you want to achieve.

Therefore A is the correct answer because 172.20.10.1 is not overlapping with 172.16.0.0, and the list will be appended below.

Chuckzero#sh ip access-lists
Extended IP access list 100
10 permit ip 192.168.0.0 0.0.255.255 any
20 permit ip 172.16.0.0 0.0.15.255 any
30 deny ip host 172.20.10.1 any
Chuckzero#
upvoted 1 times

byallmeans 6 months, 3 weeks ago
look at the wildcard carefully. 172.16.0.0. 0.0.15.255 doesn't overlap with 172.20.10.0 0.0.0.255. Answer is A.
upvoted 3 times

HungarianDish 8 months ago
Answer A) is correct. As Clauster writes "the question wants you to just permit the Interface, not the entire network". That is why A is better than C.
upvoted 3 times

MO_2022 11 months, 2 weeks ago
A is correct
upvoted 2 times

stationx 11 months, 3 weeks ago
A is correct
172.16.0.0 0.0.15.255 includes 172.16.0.0 - 172.16.15.255

Router(config)#do show access-list 100
Extended IP access list 100
10 permit ip 192.168.0.0 0.0.255.255 any
20 permit ip 172.16.0.0 0.0.15.255 any
Router(config)#access-list 100 permit ip host 172.20.10.1 any log

Router(config)#do show access-list 100
Extended IP access list 100
10 permit ip 192.168.0.0 0.0.255.255 any
20 permit ip 172.16.0.0 0.0.15.255 any
30 permit ip host 172.20.10.1 any log
Router(config)#

upvoted 3 times

nushadu 11 months, 3 weeks ago

A. extended ACL does not have seq keyword:
Router(config)#access-list ?
<1-99> IP standard access list
<100-199> IP extended access list
<1100-1199> Extended 48-bit MAC address access list
<1300-1999> IP standard access list (expanded range)
<200-299> Protocol type-code access list
<2000-2699> IP extended access list (expanded range)
<2700-2799> MPLS access list
<300-399> DECnet access list
<700-799> 48-bit MAC address access list
compiled Enable IP access-list compilation
dynamic-extended Extend the dynamic ACL absolute timer
rate-limit Simple rate-limit specific access list

Router(config)#access-list

upvoted 3 times

nushadu 11 months, 3 weeks ago

extended NAMED ACL has seq:
Router(config)#ip access-list extended MY_NAME ?
<cr>

Router(config)#ip access-list extended MY_NAME
Router(config-ext-nacl)#?
Ext Access List configuration commands:
<1-2147483647> Sequence Number
default Set a command to its defaults
deny Specify packets to reject
dynamic Specify a DYNAMIC list of PERMITs or DENYs
evaluate Evaluate an access list
exit Exit from access-list configuration mode
no Negate a command or set its defaults
permit Specify packets to forward
remark Access list entry comment

Router(config-ext-nacl)#

upvoted 1 times

nushadu 11 months, 3 weeks ago

Router(config-ext-nacl)#3 permit udp any host 8.8.8.8 eq 53 log
Router(config-ext-nacl)#do s access-l
Extended IP access list 100
10 permit ip 192.168.0.0 0.0.255.255 any
20 permit ip 172.16.0.0 0.0.15.255 any
30 permit ip host 172.20.10.1 any log
Extended IP access list MY_NAME
3 permit udp any host 8.8.8.8 eq domain log
10 deny ip any any log
Router(config-ext-nacl)#

upvoted 1 times

nushadu 11 months, 3 weeks ago

Router#show running-config | se
Router#show running-config | section acc
ip access-group 100 in
ip access-list extended MY_NAME
permit udp any host 8.8.8.8 eq domain log
deny ip any any log
access-list 100 permit ip 192.168.0.0 0.0.255.255 any
access-list 100 permit ip 172.16.0.0 0.0.15.255 any
access-list 100 permit ip host 172.20.10.1 any log
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#acc
Router(config)#access-list 100 ?
deny Specify packets to reject
dynamic Specify a DYNAMIC list of PERMITs or DENYs
permit Specify packets to forward
remark Access list entry comment

Router(config)#access-list 100

upvoted 1 times

nushadu 11 months, 3 weeks ago

technically "C" also can be right ...
Router(config)#ip access-list extended MY_NAME
Router(config-ext-nacl)#5 permit tcp any host 8.8.8.8 eq 53 log
Router(config-ext-nacl)#do s access-l
Extended IP access list 100
10 permit ip 192.168.0.0 0.0.255.255 any
20 permit ip 172.16.0.0 0.0.15.255 any
30 permit ip host 172.20.10.1 any log
Extended IP access list MY_NAME
3 permit udp any host 8.8.8.8 eq domain log
5 permit tcp any host 8.8.8.8 eq domain log
10 deny ip any any log
Router(config-ext-nacl)#

upvoted 1 times

nushadu 11 months, 3 weeks ago

in the end my reply is - A

Router(config)#ip access-list extended 100
Router(config-ext-nacl)#
Router(config-ext-nacl)#5 permit ip host 1.1.1.1 any log
Router(config-ext-nacl)#
Router(config-ext-nacl)#do s access-l
Extended IP access list 100
5 permit ip host 1.1.1.1 any log
10 permit ip 192.168.0.0 0.0.255.255 any
20 permit ip 172.16.0.0 0.0.15.255 any
30 permit ip host 172.20.10.1 any log
100 deny ip any any log
Extended IP access list MY_NAME
3 permit udp any host 8.8.8.8 eq domain log
5 permit tcp any host 8.8.8.8 eq domain log
10 deny ip any any log
Router(config-ext-nacl)#

upvoted 2 times

bora4motion 1 year ago

A is correct.
The syntax is wrong for B. You can't have everything on a single line.
(config)#access-list 100 seq 5
% Unrecognized command

Only if you use the syntax from A. C and D are not that specific so are out.

upvoted 4 times

Feliphus 11 months, 3 weeks ago

Disagree with you, if you don't indicate the exact position, it is added at the end of the ACL

upvoted 1 times

bora4motion 11 months, 2 weeks ago

Mate, you can't have the entire syntax from B on a single line.

upvoted 1 times

bora4motion 11 months, 2 weeks ago

Go ahead and test before stating something please.

upvoted 1 times

Feliphus 11 months, 3 weeks ago

For me, the C answer is the correct althouth I have to select a /24

upvoted 1 times

Clauster 8 months, 1 week ago

The only problem with your answer is that you are permitting the entire network, the question wants you to just permit the Interface, not the entire network, that's how they got you

upvoted 2 times

kalbos 1 year ago

B is correct. There is no syntax error.
without seq 5 there will be a match with 172.16.0.0/20

upvoted 1 times

[Removed] 5 months, 2 weeks ago

172.16.0.0/20 range is
172.16.0.1 to 172.16.15.254

upvoted 1 times

bora4motion 11 months, 4 weeks ago

well there is. you can't have all that stuff on a single line.

upvoted 1 times

mitosenoriko 1 year, 1 month ago

172.16.0.0/20 range is 172.16.0.1 - 172.16.15.254
so Answer A is Through seq 10 & 20.match　(going to be)seq 30 this.

upvoted 2 times

Deu_Inder 1 year, 2 months ago

A cannot be the answer. The config from A will get the line number 30 which will be executed after line 20 in the ACL 100. But the IP of the host 172.20.10.1 is already there in the line 20. So, this host will get treatment like others in line 20. Thus, line 30 will be ignored. We need to configure the special treatment to this host in a line prior to line 20.

upvoted 2 times

AhmadApmsET 1 year, 2 months ago

A is valid because 172.20.10.1 doesn't match with the 172.16.0.0 0.0.15.255, 172.20.10.1 doesn't fall within the 172.16.0.0/20 range, thus line 20 won't be disruptive and 172.16.20.1 will only match with line 30 when added.

upvoted 9 times

RREVECO 1 year, 2 months ago

A is the correct answer. laboratory validated

B has a syntax error

C indicates a network, not a host

D is disruptive

upvoted 2 times

jjeans 1 year ago

Where is the syntax error in B?
You mean "seq 5" ?

upvoted 1 times

bora4motion 1 year ago

yes - you can't have that there.

upvoted 1 times

Deu_Inder 1 year, 2 months ago

Did you also check if the logging count for the host is increasing for the ACL using 'sh access-list 100'?
I am sure it did not increase.

upvoted 1 times

```
R1#show ip interface brief | include 192.168.12
FastEthernet0/0     192.168.12.1    YES manual up                    up

R1#ping vrf CUST-A 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1#show ip arp 192.168.12.2
R1#
```

Refer to the exhibit. A network engineer checks connectivity between two routers. The engineer can ping the remote endpoint but cannot see an ARP entry. Why is there no ARP entry?

A. When VRFs are used, ARP protocol must be enabled in each VRF.

B. The ping command must be executed in the global routing table.

C. Interface FastEthernet0/0 is configured in VRF CUST-A, so the ARP entry is also in that VRF.

D. When VRFs are used, ARP protocol is disabled in the global routing table.

Correct Answer: *C*

Community vote distribution

C (100%)

nushadu 11 months, 3 weeks ago

cisco#show ip arp vrf ?
WORD VPN Routing/Forwarding instance name

cisco#show ip arp vrf

upvoted 2 times

nushadu 11 months, 1 week ago

cisco_R3#show ip arp vrf cust_1
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.1 - aabb.cc00.3000 ARPA Ethernet0/0.20
Internet 192.168.1.200 - aabb.cc00.3000 ARPA Ethernet0/0.20
cisco_R3#

upvoted 3 times

bora4motion 1 year ago

Selected Answer: C

LOL - C is correct

upvoted 2 times

Question #519 *Topic 1*

Which option must be used to support a WLC with an IPv6 management address and 100 Cisco Aironet 2800 Series access points that will use DHCP to register?

A. 43

B. 52

C. 60

D. 82

Correct Answer: *B*

Community vote distribution

B (86%) 14%

flash007 4 months, 1 week ago

43 is ipv4 dhcp this question talks about ipv6

upvoted 2 times

HarwinderSekhon 5 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

Doh247 8 months, 4 weeks ago

It's Option 52.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/IPV6_DG.html#pgfId-76725

upvoted 4 times

Brand 9 months, 3 weeks ago

Selected Answer: B

It's option 52 according to the document in the link.
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/17-1/configuration_guide/ip/b_171_ip_9400_cg/dhcpv6_options_support.html

upvoted 4 times

rafaelinho88 9 months, 3 weeks ago

Selected Answer: D

The option that must be used to support a WLC with an IPv6 management address and 100 Cisco Aironet 2800 Series access points that will use DHCP to register is DHCPv6 server with Option 82 support. This is because option 82 is required to provide the ability to assign IP addresses to devices based on their location within the network and to support the DHCP registration of Cisco Aironet access points.

upvoted 1 times

rogi2023 4 months, 1 week ago

52 in HEX = 82 dec HTH

upvoted 2 times

snarkymark 10 months ago

B is correct
https://insinuator.net/2016/02/dhcpv6-option-52-on-cisco-dhcpv6-server/

upvoted 2 times

Edwinmolinab 1 year ago

Selected Answer: B

Reference https://insinuator.net/2016/02/dhcpv6-option-52-on-cisco-dhcpv6-server/

upvoted 1 times

Joseph123 1 year, 2 months ago

Correct

upvoted 1 times

```
Router#sh access-list
Extended IP access list 100
    10 permit tcp any any eq telnet
Extended IP access list 101
    10 permit tcp any any eq 22
```

Refer to the exhibit. Which configuration set implements Control Plane Policing for SSH and Telnet?

A.

```
Router(config)#class-map type inspect match-all
Router(config-cmap)#match access-group 100
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP

Router(config-pmap)#class class-control
Router(config-pmap-c)#police 1000000 conform-action transmit
Router(config)#control-plane
Router(config-cp)#service-policy output CoPP
```

B.

```
Router(config)#class-map match-all class-control
Router(config-cmap)#match access-group 100
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP

Router(config-pmap)#class class-control
Router(config-pmap-c)#police 1000000 conform-action transmit
Router(config)#control-plane
Router(config-cp)#service-policy output CoPP
```

C.

```
Router(config)#class-map class-telnet
Router(config-cmap)#match access-group 100
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP

Router(config-pmap)#class class-telnet-ssh
Router(config-pmap-c)#police 1000000 conform-action transmit
Router(config)#control-plane
Router(config-cp)#service-policy input CoPP
```

D.

```
Router(config)#class-map match-any class-control
Router(config-cmap)#match access-group 100
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP

Router(config-pmap)#class class-control
Router(config-pmap-c)#police 1000000 conform-action transmit
Router(config)#control-plane
Router(config-cp)#service-policy input CoPP
```

Correct Answer: *A*

Caledonia Highly Voted 1 year, 2 months ago

The right answer is D

upvoted 25 times

onkel_andi Highly Voted 1 year, 1 month ago

Correct answer is D

upvoted 8 times

CCNPWILL Most Recent 1 month, 3 weeks ago

D is the correct answer folks.

upvoted 1 times

CKL_SG 4 months, 3 weeks ago

Answer is D

R8(config)#class-map type ?
control Configure a control policy class-map
inspect Configure Firewall Class Map
Inspect is to configure firewall class map

R8(config)#class-map ?
WORD class-map name
match-all Logical-AND all matching statements under this classmap
match-any Logical-OR all matching statements under this classmap

https://community.cisco.com/t5/switching/class-map-match-all-or-match-any-exact-difference/td-p/783620

match-all
(Optional) Matches all match criteria in the class map.

match-any
(Optional) Matches one or more match criteria.

upvoted 2 times

j8fx 5 months, 1 week ago

Definitely D

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

class map type-inspect is used in Zone Based firewall config for IOS.
D is the answer.

upvoted 1 times

massimp 5 months, 3 weeks ago

Don't know why i can't choose the answer here, but it is D for sure.

upvoted 1 times

olaniyijt 7 months, 2 weeks ago

D is the right answer

upvoted 2 times

xuanluo 7 months, 3 weeks ago

if u select A, the warning XXX type inspect is not allowed in policy-map copp of type default; if u select D, match-any means OR not AND
The B sounds better, because match-all means logical AND

upvoted 1 times

JackDRipper 7 months, 3 weeks ago

For answer B, every packet needs to be both telnet and SSH to go through CoPP, which is improbable, if not impossible.
D is correct. CoPP is triggered when either a telnet or SSH packet comes in, which is what I take the question is talking about.

upvoted 2 times

Cooldude89 9 months, 2 weeks ago

D is correct

upvoted 2 times

forccnp 11 months, 2 weeks ago

D is correct!!!!!

upvoted 2 times

MO_2022 11 months, 2 weeks ago

D is correct

upvoted 2 times

nushadu 11 months, 3 weeks ago

just tested, I do not know right answer ...
!
class-map match-any class-control
match access-group 101
!
policy-map CoPP
class class-control
police 1000000 conform-action transmit
!
access-list 101 permit tcp any any eq 22
!

control-plane
service-policy input CoPP
upvoted 1 times

Zizu007 1 year ago

A - Wrong, 'class-map type inspect' - incorrect.
B - Wrong, 'class-map match-all' cannot match a packet which is telnet and SSH at the same time.
C - Wrong, missing 'policy-map'
D - Correct.
upvoted 5 times

mgiuseppe86 2 months, 2 weeks ago

D is correct but C is not missing policy-map, its there but the class it's referencing does not exist. class-telnet-ssh does not exist

class-ssh and class-telnet do

its the wrong way to go about it
upvoted 1 times

mitosenoriko 1 year, 1 month ago

d is correct
upvoted 7 times

Question #521 *Topic 1*

A customer deploys a new wireless network to perform location-based services using Cisco DNA Spaces. The customer has a single WLC located on-premises in a secure data center. The security team does not want to expose the WLC to the public Internet. Which solution allows the customer to securely send RSSI updates to Cisco DNA Spaces?

A. Deploy a Cisco DNA Spaces connector as a VM

B. Perform tethering with Cisco DNA Center

C. Replace the WLC with a cloud-based controller

D. Implement Cisco Mobility Services Engine

Correct Answer: *A*

Chalmisco 1 month, 3 weeks ago

A Cisco DNA Spaces connector is a software application that can be deployed on a virtual machine (VM) in the customer's on-premises network. The connector acts as a secure intermediary between the WLC and Cisco DNA Spaces. It encrypts all traffic between the WLC and Cisco DNA Spaces, and it can be configured to use a variety of authentication and authorization mechanisms.
upvoted 2 times

HarwinderSekhon 5 months, 2 weeks ago

C - No because its cloud and customer dont want anything going out.
A looks like promising
answer.
upvoted 2 times

snarkymark 10 months ago

Cisco DNA Spaces is a cloud based service. However, you can deploy as a vm if needed.
"Cisco Spaces Connector can be deployed as a VM in OVA form factor, free of cost. "
upvoted 4 times

```
DSW2#sh spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    10
              Address     0013.80f9.8880
              Cost        2
              Port        9 (FastEthernet1/0/7)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4106   (priority 4096 sys-id-ext 10)
              Address     0018.7363.4300
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa1/0/7             Root FWD 2         128.9    P2p
Fa1/0/10            Desg FWD 4         128.12   P2p
Fa1/0/11            Desg FWD 2         128.13   P2p
Fa1/0/12            Desg FWD 2         128.14   P2p


DSW2#
*Mar  3 07:29:24.854: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/7
 with BPDU Guard enabled. Disabling port.
*Mar  3 07:29:24.854: %PM-4-ERR_DISABLE: bpduguard error detected on Fa1/0/7, put
 ting Fa1/0/7 in err-disable state
*Mar  3 07:29:24.879: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/7
 with BPDU Guard enabled. Disabling port.
*Mar  3 07:29:25.869: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
 t1/0/7, changed state to down
*Mar  3 07:29:26.884: %LINK-3-UPDOWN: Interface FastEthernet1/0/7, changed state
 to down
```

Refer to the exhibit. An engineer entered the command no spanning-tree bpduguard enable on interface Fa1/0/7. What is the effect of this command on
Fa1/0/7?

A. It remains in err-disabled state until the errdisable recovery cause failed-port-state command is entered in the global configuration mode

B. It remains in err-disabled state until the no shutdown command is entered in the interface configuration mode

C. It remains in err-disabled state until the shutdown/no shutdown command is entered in the interface configuration mode

D. It remains in err-disabled state until the spanning-tree portfast bpduguard disable command is entered in the interface configuration mode.

Correct Answer: *C*

Community vote distribution

C (100%)

HarwinderSekhon 5 months, 2 weeks ago

Selected Answer: C

C from old CCNA days and this is what I use at my workplace as well.

upvoted 1 times

nushadu 11 months, 1 week ago

Selected Answer: C

generally speaking, yes, it is true - the default behavior, but this setting is hidden from us:
sw2#show errdisable recovery
ErrDisable Reason Timer Status
----------------- --------------
arp-inspection Disabled
bpduguard Disabled
channel-misconfig (STP) Disabled
dhcp-rate-limit Disabled
dtp-flap Disabled
gbic-invalid Disabled

inline-power Disabled
l2ptguard Disabled
link-flap Disabled
mac-limit Disabled
link-monitor-failure Disabled
loopback Disabled
oam-remote-failure Disabled
pagp-flap Disabled
port-mode-failure Disabled
pppoe-ia-rate-limit Disabled
psecure-violation Disabled
security-violation Disabled
sfp-config-mismatch Disabled
storm-control Disabled
udld Disabled
unicast-flood Disabled
...
sw2#

upvoted 3 times

Question #523 *Topic 1*

Which design principle states that a user has no access by default to any resource, and unless a resource is explicitly granted, it should be denied?

A. least privilege

B. fail-safe defaults

C. economy of mechanism

D. complete mediation

Correct Answer: *B*

Community vote distribution

B (70%) A (30%)

Joseph123 Highly Voted 1 year, 2 months ago

The Principle of Fail-Safe Defaults states that, unless a subject is given explicit access to an object, it should be denied access to that object
upvoted 10 times

Entivo 4 months, 4 weeks ago

Fail safe defaults is a design philosophy where IF any device or process or system fails for whatsoever reason it will DEFAULT TO SAFE outcome. Principle of Least Privilege means applying a zero trust mindset and providing ONLY the required access that people need to do their jobs and nothing else.
upvoted 1 times

CKL_SG Most Recent 4 months, 3 weeks ago

Selected Answer: B

Clearly stated in below url

The principle of least privilege states that a subject should be given only those privileges that it needs in order to complete its task.

The principle of fail-safe defaults states that, unless a subject is given explicit access to an object, it should be denied access to that object.

https://www.informit.com/articles/article.aspx?p=30487&seqNum=2
upvoted 2 times

teikitiz 4 months, 4 weeks ago

Selected Answer: B

https://medium.com/strike-sh/rest-security-design-principles-434bd6ee57ea

Fail-Safe Defaults
A user's default access level to any resource in the system should be "denied" unless they have been granted a "permit" explicitly.
upvoted 1 times

Entivo 5 months, 2 weeks ago

Selected Answer: A

The answer is 100% A - admin please change.
upvoted 1 times

Clauster 8 months, 2 weeks ago

Selected Answer: B

Answer is B
No more arguing about this.
https://www.informit.com/articles/article.aspx?p=30487&seqNum=2#:~:text=The%20principle%20of%20fail-safe%20defaults%20states%20that%2C%20unless,is%20not%20explicitly%20granted%2C%20it%20should%20be%20denied.
upvoted 1 times

Asymptote 10 months, 3 weeks ago

Selected Answer: B

Least privilege means you can still access resources but with limited permission.
abviously A is not the answer.

B is the correct one.
upvoted 1 times

Entivo 5 months, 2 weeks ago

Wrong, The Principle of Least Privilege means that ALL access to denied UNLESS it is needed. Your answer is completely wrong.
upvoted 2 times

Asymptote 10 months, 3 weeks ago

obviously tyop .....

upvoted 1 times

civan 11 months ago

Selected Answer: B

While both A and B appear correct, the key words in the question seem to more closely match option B 'fail safe defaults' according to the CISA website

https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/failing-securely

https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege

upvoted 2 times

poy4242 11 months, 1 week ago

Selected Answer: A

it's from Zero-trust model, the least-privilege

upvoted 2 times

Question #524 *Topic 1*

A customer wants to connect a device to an autonomous Cisco AP configured as a WGB. The WGB is configured properly: however, it fails to associate to a
CAPWAP-enabled AP. Which change must be applied in the advanced WLAN settings to resolve this issue?

A. Enable Aironet IE.

B. Enable passive client.

C. Disable AAA override.

D. Disable FlexConnect local switching.

Correct Answer: *A*

Community vote distribution

A (100%)

Caledonia Highly Voted 1 year, 2 months ago

Selected Answer: A

• To enable the WGB to communicate with the lightweight access point, create a WLAN and make sure that Aironet IE is enabled.

upvoted 6 times

[Removed] Highly Voted 5 months ago

Selected Answer: A

A Workgroup Bridge (WGB) is a wireless client that serves as a non-root access point for wired clients. A WGB can associate to another access point that acts as a root access point, either in autonomous mode or in CAPWAP mode. A CAPWAP-enabled AP is an access point that is managed by a Wireless LAN Controller (WLC) using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol.

To resolve the issue of a WGB failing to associate to a CAPWAP-enabled AP, you need to enable Aironet IE in the advanced WLAN settings on the WLC. Aironet IE is a Cisco proprietary information element that contains additional information about the WLAN, such as the VLAN ID, QoS parameters, and load balancing. Aironet IE is required for WGB association because it helps the WGB to identify the correct WLAN and VLAN for its wired clients.

upvoted 5 times

HarwinderSekhon Most Recent 5 months, 2 weeks ago

To enable the WGB to communicate with the lightweight access point, create a WLAN and make sure that Aironet IE is enabled.

credit to siteoforigin for link -https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/workgroup_bridges.pdf

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

what the Fuc$ is WGB. I heard it very first time.

upvoted 5 times

CisR 5 months, 1 week ago

WGB threw me at first, but it is Workgroup Bridge

upvoted 2 times

Dv123456 4 months, 4 weeks ago

no such topic on the OG

upvoted 4 times

siteoforigin 1 year, 2 months ago

Selected Answer: A

Agree with A, 2nd page of this document:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/workgroup_bridges.pdf

• To enable the WGB to communicate with the lightweight access point, create a WLAN and make sure that Aironet IE is enabled.

upvoted 4 times

Question #525 *Topic 1*

By default, which virtual MAC address does HSRP group 32 use?

A. 04:19:01:05:2e:32

B. 05:5e:5c:ac:0c:32

C. 00:00:0c:07:ac:20

D. 00:5e:0c:07:ac:20

Correct Answer: *C*

Community vote distribution

C (100%)

H3kerman Highly Voted 1 year ago

Selected Answer: C

The virtual IP resolves to a virtual MAC address in the format 0000.0c07.acxx, xx being the group number in hexadecimal. For example, if you use group number 3, the last part of the MAC address is ac03.
32 is in binary 0010 0000 that's mean in HEX its 2 0

upvoted 5 times

nushadu Most Recent 11 months, 3 weeks ago

cisco(config-if)#do s ip int br | ex unass
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 10.0.0.1 YES manual up up

cisco(config-if)#do s stand
Ethernet0/0 - Group 32
State is Active
2 state changes, last state change 00:00:53
Virtual IP address is 10.0.0.254
Active virtual MAC address is 0000.0c07.ac20
Local virtual MAC address is 0000.0c07.ac20 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.720 secs
Preemption disabled
Active router is local
Standby router is unknown
Priority 100 (default 100)
Group name is "hsrp-Et0/0-32" (default)
cisco(config-if)#

upvoted 2 times

Question #526 *Topic 1*

Which two Cisco SD-WAN components exchange OMP information? (Choose two.)

A. WAN Edge

B. vBond

C. vManage

D. vAnalytics

E. vSmart

Correct Answer: *AE*

Community vote distribution

AE (100%)

H3kerman Highly Voted 1 year ago

Selected Answer: AE

OMP is the control protocol that is used to exchange routing, policy, and management information between the vSmart controllers and vEdge routers in the overlay network.

but shouldn't be vEdge instead of WAN Edge?

upvoted 8 times

teikitiz Most Recent 4 months, 4 weeks ago

Selected Answer: AE

From the ENCORE ExamCram book,
"Overlay Management Protocol (OMP): The OMP routing protocol has a similar structure to BGP and manages the SD-WAN overlay network. Its protocol runs between vSmart controllers and between vSmart controllers and WAN edge routers, where control plane information—such as route prefixes, next-hop routes, crypto keys, and policy information—is exchanged over a secure DTLS or TLS connection."

upvoted 2 times

AndreasThornus 11 months, 4 weeks ago

The provided answer is correct. I don't know if it is correct, I thought I would just jump on the bandwagon.

upvoted 4 times

yousif387 1 year ago

Selected Answer: AE

answer is correct

upvoted 1 times

Joseph123 1 year, 2 months ago

Provided answer is correct

upvoted 2 times

Question #527 *Topic 1*

What does the number in an NTP stratum level represent?

A. The number of hops it takes to reach the authoritative time source

B. The amount of offset between the device clock and true time

C. The number of hops it takes to reach the primary time server

D. The amount of drift between the device clock and true time

Correct Answer: *A*

Community vote distribution

A (100%)

nushadu 11 months, 1 week ago

Selected Answer: A

local Cisco the thrid in the chain and its server the second:
sw1#
sw1#show ntp status | i strat
Clock is synchronized, stratum 3, reference is 91.212.242.20
sw1#show ntp ass det | i strat
91.212.242.20 configured, ipv4, our_master, sane, valid, stratum 2
sw1#
sw1#show ntp ass

address ref clock st when poll reach delay offset disp
*~91.212.242.20 194.146.251.101 2 53 128 377 24.944 -2.181 3.274
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
sw1#

upvoted 3 times

Radwa_ 1 year, 1 month ago

Selected Answer: A

Given answer is correct.

upvoted 2 times

Question #528 *Topic 1*

Refer to the exhibit. Clients report that they cannot connect to this SSID using the provided PSK. Which action will resolve this issue?

A. Apply the correct interface to this WLAN

B. Apply the changes this SSID

C. Select the PSK under authentication key management

D. Define the correct Radio Policy.

Correct Answer: *C*

Community vote distribution

C (75%) A (19%) 6%

KOJJY Highly Voted 11 months, 3 weeks ago

Selected Answer: C

C is correct
https://www.youtube.com/watch?v=EjNCpxMr1rU

upvoted 7 times

RamazanLokov 6 months ago

Thanks a lot, you're right. Guys, just watch video. Correct answer C

upvoted 2 times

Soggyt74 Most Recent 3 months, 2 weeks ago

Selected Answer: C

For WPA2 personal mode, look under the Authentication Key Management section and check only the box next to PSK. You should then enter the pre-shared key string in the box next to PSK Format.

CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide page 564

upvoted 1 times

net_eng10021 6 months ago

Disaster of a question...I'm skipping it.

upvoted 4 times

BobbyFlash 4 months, 4 weeks ago

I absolutely agree.

upvoted 1 times

teikitiz 4 months, 4 weeks ago

don't. Look, the exhibit is set for dot1x, but question mentions pre shared key. Need to change to PSK

upvoted 3 times

lafrank 7 months ago

Selected Answer: A

"Modifications done under security tab will appear after applying the changes" Doesn't this mean that the dialog shows unapplied configuration ? That would suggest answer A, right ?

upvoted 1 times

eojedad 8 months, 4 weeks ago

C is the correct answer

upvoted 1 times

eojedad 8 months, 4 weeks ago

page 1202, 350-401-Official-Cert-Guide

upvoted 1 times

asiansensation 9 months, 2 weeks ago

Answer A is correct:

"Under the General tab, there are two important items:
Status: Click on the checkbox to enable the WLAN.
Interface: Select the dynamic interface we created for this VLAN.

upvoted 1 times

snarkymark 10 months ago

Agree with answer C
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116880-config-wpa2-psk-00.html#anc7

upvoted 4 times

bora4motion 1 year ago

Selected Answer: C

I'm going with C. As it stands it is configured for radius auth and must be changed to PSK.

upvoted 4 times

Gedson 12 months ago

Yes, it's C, it must be changed to psk

upvoted 2 times

Darude 1 year ago

Selected Answer: B

A = wrong ..it doesn matter witch interface because the authentication will still work it is local
see this:[WPA2][Auth(802.1X)] it should be [WPA2][PSK] and because they have received the password so the admin configured corectly the PSK but he have forgotten to APLY the change so B is the correct answer

upvoted 1 times

Darude 1 year ago

It is tricky. if you forget to apply it give you the same image but to re-apply you have to change to psk again which is C.

upvoted 1 times

Tacolicious 1 year ago

Selected Answer: A

It's using the management interface. Answer provided is correct

upvoted 1 times

winder 1 year ago

you mean Answer A is right or not?

upvoted 2 times

XDR 7 months, 2 weeks ago

Is not :)

upvoted 1 times

GeorgeFortiGate 1 year ago

Selected Answer: A

Correct is A

upvoted 1 times

Question #529 *Topic 1*

Which QoS queuing method transmits packets out of the interface in the order the packets arrive?

A. custom

B. weighted-fair

C. FIFO

D. priority

Correct Answer: *C*

Community vote distribution

C (100%)

eddgg 3 months, 3 weeks ago

Selected Answer: C

c is correct

upvoted 1 times

Lungful 3 months, 4 weeks ago

Selected Answer: C

C is correct, First In First Out

upvoted 1 times

bora4motion 1 year ago

Selected Answer: C

First In First Out

upvoted 3 times

Question #530 *Topic 1*

Which two results occur if Cisco DNA Center loses connectivity to devices in the SD-Access fabric? (Choose two.)

A. Users lose connectivity

B. Already connected users are unaffected but new users cannot connect

C. All devices reload after detecting loss of connection to Cisco DNA Center

D. User connectivity is unaffected

E. Cisco DNA Center is unable to collect monitoring data in Assurance

Correct Answer: *AE*

Community vote distribution

DE (91%) 6%

Clauster Highly Voted 8 months, 1 week ago

Selected Answer: DE

Guys let's use common sense, what solution costs 50 thousand dollars and it will make all devices point to it and if it fails your entire network fails ? think about it just from the logic common sense point of view and then answer. No devices will not lose connectivity if DNA Center goes down.

upvoted 9 times

rafaelinho88 Highly Voted 9 months, 3 weeks ago

Selected Answer: DE

If you have Cisco SD-Access implemented and DNA Center becomes unreachable then the wired and wireless network will continue to forward packets as usual. There will be no impact to network performance or behavior. Yes you will be able to SSH / telnet / console into switches and wireless network infrastructure as usual. For the period DNA Center is unreachable, Assurance data will be lost, and you will not be able to make configuration changes to the Cisco SD-Access network

upvoted 6 times

Indersingh Most Recent 6 months ago

correct answer is
D,E

upvoted 1 times

Leoveil 6 months, 3 weeks ago

no sure about D , because we don't know whether "user" means just "the already connected users" or both "new" and "already connected users" .
if "user" means both than the answer is BE
if "user" means just "already connected users " than the answer is DE

upvoted 1 times

rafaelinho88 9 months, 3 weeks ago

Selected Answer: CD

If you have Cisco SD-Access implemented and DNA Center becomes unreachable then the wired and wireless network will continue to forward packets as usual. There will be no impact to network performance or behavior. Yes you will be able to SSH / telnet / console into switches and wireless network infrastructure as usual. For the period DNA Center is unreachable, Assurance data will be lost, and you will not be able to make configuration changes to the Cisco SD-Access network

upvoted 1 times

rafaelinho88 9 months, 3 weeks ago

DE, sorry

upvoted 1 times

TSKARAN 10 months ago

If Cisco DNA Center loses connectivity to devices in the SD-Access fabric, it will affect both new and already connected users.

upvoted 1 times

TSKARAN 10 months ago

When Cisco DNA Center loses connectivity to devices in the SD-Access fabric, it can no longer communicate with the controllers that are responsible for managing user access and network policies. This means that new users will be unable to connect to the network, and existing users may experience disruptions in their connectivity.

The existing connected users may not be disconnected but their session may be affected by this loss of connectivity, for example:

They may experience a loss of network services, such as Internet access or access to specific resources.
They may experience a decrease in network performance.
They may be unable to authenticate to the network or access specific resources.

It is important to monitor the health of the Cisco DNA Center and the SD-Access fabric to ensure that connectivity is maintained and to quickly identify and resolve any issues that arise.

upvoted 1 times

bora4motion 1 year ago

Selected Answer: DE

DE 100%

upvoted 2 times

dougj 1 year, 1 month ago

Selected Answer: DE

DNAC is not required for correct operation of the network. It is only required for management control and monitoring

upvoted 4 times

kebkim 1 year, 2 months ago

DE

If you have Cisco SD-Access implemented and DNA Centre becomes unreachable then the wired and wireless network will continue to forward packets as usual. There will be no impact to network performance or behavior. Yes you will be able to SSH / telnet / console into switches and wireless network infra as usual. For the period DNA Centre is unreachable, Assurance data will be lost, and you will not be able to make configuration changes to the Cisco SD-Access network.

upvoted 3 times

Nonono 1 year, 2 months ago

Selected Answer: DE

This the correct answer

upvoted 3 times

RREVECO 1 year, 2 months ago

Selected Answer: DE

link: https://community.cisco.com/t5/cisco-digital-network-architecture-dna/dna-failure-mode/td-p/3841715
https://community.cisco.com/t5/cisco-digital-network-architecture-dna/dna-failure-mode/td-p/3841715

upvoted 3 times

Joseph123 1 year, 2 months ago

D,E is the answer

upvoted 1 times

jj970us 1 year, 2 months ago

Selected Answer: DE

If you have Cisco SD-Access implemented and DNA Center becomes unreachable then the wired and wireless network will continue to forward packets as usual.

upvoted 3 times

KZM 1 year, 2 months ago

The right answers are "D" and "E", I think.

upvoted 2 times

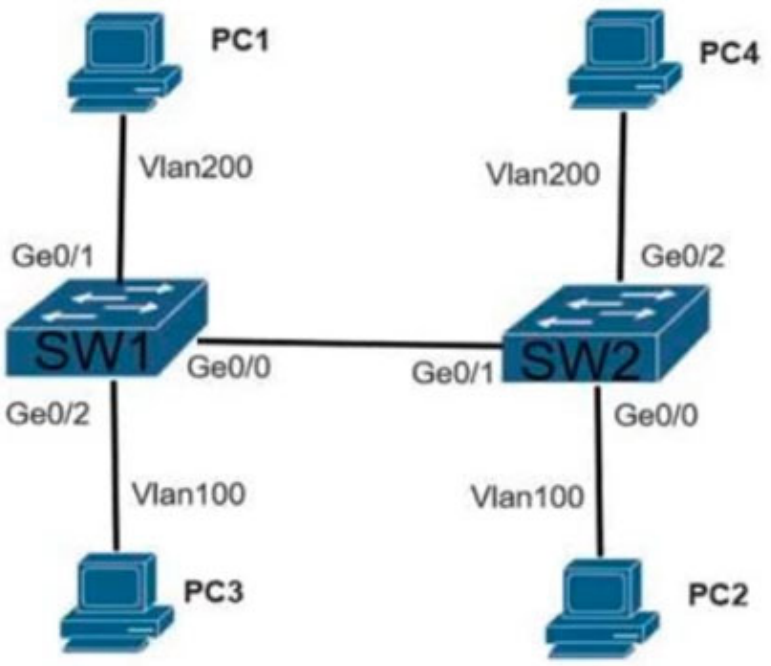
Ioannis34 1 year, 2 months ago

Selected Answer: BE

BE is the right answers.

upvoted 2 times

```
SW1# show interfaces gigabitethernet 0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (NATIVE)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
...output omitted...

SW2# show interfaces gigabitethernet 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (NATIVE)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
...output omitted...
```



Refer to the exhibit. The connection between SW1 and SW2 is not operational. Which two actions resolve the issue? (Choose two.)

A. configure switchport nonegotiate on SW1

B. configure switchport nonegotiate on SW2

C. configure switchport mode access on SW2

D. configure switchport mode trunk on SW2

E. configure switchport mode dynamic desirable on SW2

Correct Answer: *BE*

Community vote distribution

DE (37%) BD (30%) BE (26%) 2%

John13121 Highly Voted 11 months ago

I really see people with 0 xp in real working env.....
the the question asks which two actions - one OR the other... even if you exclude answers you end up with - dynamic desirable and static trunk...
stop misleading the people ...

upvoted 10 times

Jey117 9 months, 2 weeks ago

Take it easy Jimmy Neutron.

upvoted 10 times

tempaccount00001 4 months, 3 weeks ago

cheers megamind

upvoted 6 times

Cooldude89 9 months, 1 week ago

it's ok mr super intelligent

upvoted 10 times

JoeyT Highly Voted 8 months, 1 week ago

Look at SW1: it is dynamic auto AND also Negotiation off - no such thing!!!!!!!!
By default it is dynamic auto, then you can NOT disable negotiation. Unless you static it to trunk, then you can disable negotiation.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.

upvoted 8 times

[Removed] 5 months, 1 week ago

I tried to lab this. I can't get the configuration to match what the question is displaying. This question is dumb as hell.
upvoted 5 times

Dv123456 Most Recent 4 months, 1 week ago
if you set the switchport nonegotiate command you can't set switchport mode dynamic desirable /auto
upvoted 2 times

CKL_SG 4 months, 3 weeks ago
Selected Answer: BE
Test in GNS3

When switch port configure as negotiation auto
interface GigabitEthernet0/0
media-type rj45
negotiation auto
!
vIOS-L2-01(config-if)#do sh int g0/0 swi
Name: Gi0/0
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: down
Administrative Trunking Encapsulation: negotiate

When set to encapsulation dot1q, it refer to non negotiate in this question i believe
interface GigabitEthernet0/0
switchport trunk encapsulation dot1q
!
vIOS-L2-01#show int g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
upvoted 1 times

[Removed] 5 months ago
For me, there is only one correct answer is E. You can't define the mode as trunk without identifying the encapsulation as specifically either ISL or DOT1Q.
Configuring "nonegotiate" won't allow you to configure switch mode trunk, even if the question implies one or the other, B or D solve the issue.
The only way to get this trunk link to work is by configuring dynamic desireable on SW2.
I tried a lot of combinations, but non get me to the point where the exhibit shows
upvoted 1 times

Based_Engineer 5 months ago
On older IOS devices, that is true, but after version 15 of IOS (I believe), it is assumed that you want 802.1q encapsulation, so you no longer have to specify the encapsulation of a trunk link.
upvoted 3 times

RamazanLokov 6 months ago
Official cert: A static trunk port attempts to establish and negotiate a trunk port with a neighbor by default. However, the interface configuration command switchport nonegotiate prevents that port from forming a trunk port with a dynamic desirable or dynamic auto switch port.
So if you configure switchport mode trunk on SW2, trunk is up.
Correct answer DE
upvoted 1 times

Chiaretta 7 months, 1 week ago
Selected Answer: BD
B and D are the correct answer. If you disable the negotiation of the trunk with "switchport nonegotiate" commend non make sense the switchport mode dynamic desirable.
upvoted 1 times

Jack2002 8 months ago
Selected Answer: DE
I adree with the choices D & E
upvoted 2 times

dragonwise 8 months ago
Selected Answer: DE
ABC are absolutely wrong
DE are correct. even though only one of them can solve the problem
upvoted 1 times

rami_mma 8 months, 1 week ago
Selected Answer: BD
BD is correct

upvoted 1 times

Clauster 8 months, 2 weeks ago

Selected Answer: D

The answer is D and ONLY D.
I Truly believe choose two answers was not meant to be there.

upvoted 1 times

Clauster 8 months, 2 weeks ago

Sorry E

upvoted 1 times

HungarianDish 8 months, 2 weeks ago

Option E (configure switchport mode dynamic desirable on SW2) can only work if we enable DTP on SW1. This is not given as an option, thus, again I go with BD. Hopefully, there will be a more clear answer presented on the exam.

upvoted 3 times

HungarianDish 8 months, 2 weeks ago

I am testing these configs in CML, and the switch does not even take "nonegotiate" and "dynamic" configurations together. So, we should either enable DTP or hard code the trunk configuration with "switchport mode trunk". As "no switchport nonegotiate" is not listed as an option, we need to configure the trunk manually.

sw1(config-if)#switchport nonegotiate
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status on this interface: Gi0/0

upvoted 2 times

eojedad 8 months, 4 weeks ago

Selected Answer: BD

A - DTP is already shutdown in SW1
C - we want to form a trunk
E - DTP is shutdwon in SW1, how does SW2 negotiate the trunk?

B and D are the correct options

upvoted 2 times

olaniyijt 9 months ago

Answer is B and E

Dynamic Auto + Dynamic Auto != Trunk (No trunk formed)
Dynamic Auto + Dynamic Desirable = Trunk (Forms Trunk) - Means E is correct

For the second option, read this cisco press below:
switchport nonegotiate: Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

Switch 1 interface is already a trunk and Dynamic Auto so trunk forms!

https://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=8#:~:text=switchport%20nonegotiate%3A%20Prevents%20the%20interface,to%20establish%20a%20trunk%20link.

upvoted 3 times

Brand 9 months, 1 week ago

Selected Answer: DE

Both D and E can resolve this issue while the others may not be enough to fix it.

upvoted 2 times

bendarkel 9 months, 2 weeks ago

Selected Answer: BD

I'm going with B and D.

upvoted 1 times

Refer to the exhibit. A company has an internal wireless network with a hidden SSID and RADIUS-based client authentication for increased security. An employee attempts to manually add the company network to a laptop, but the laptop does not attempt to connect to the network. The regulatory domains of the access points and the laptop are identical. Which action resolves this issue?

A. Ensure that the "Connect even if this network is not broadcasting" option is selected.

B. Change the security type to WPA2-Personal AES.

C. Use the empty string as the hidden SSID network name.

D. Limit the enabled wireless channels on the laptop to the maximum channel range that is supported by the access points.

Correct Answer: *A*

Community vote distribution

A (100%)

[Removed] 2 months, 2 weeks ago

The worst questions are the ones where the answer is common sense but since they weren't ever discussed you think that it's gotta be a trick

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Apparently becoming an network engineer requires you to be a desktop windows admin now

upvoted 1 times

Dataset 3 months, 3 weeks ago

Selected Answer: A

the answer is correct

upvoted 1 times

Faridtnx 10 months, 2 weeks ago

Selected Answer: A

A is correct:
https://windowsreport.com/connect-hidden-wi-fi-network-windows-10/

upvoted 2 times

Question #533 *Topic 1*

How do the RIB and the FIB differ?

A. RIB is derived from the control plane, and the FIB is derived from the RIB.

B. FIB is derived from the control plane, and the RIB is derived from the data plane.

C. RIB contains the interface for a destination, and the FIB contains the next hop information.

D. FIB contains routes learned through a dynamic routing protocol and the RIB contains routes that are static or directly connected.

Correct Answer: *A*

Community vote distribution

A (100%)

Leon7942 6 months, 1 week ago

why not C?
Answer A is correct definitely, but is Answer C also correct as well?

upvoted 1 times

Rose66 10 months, 2 weeks ago

Selected Answer: A

RIB is derived from the control plane, it is not used for forwarding. Every protocol such as OSPF, EIGRP, BGP has its own RIB and select their best candidates to try to install to global RIB so that it can then be selected for forwarding. If this is implemented through totally separate RIBs or one big RIB with partitions I am not aware of.

FIB is used for forwarding, like Erick explained the information is derived from the RIB and from adjacency tables so that the packet can be rewritten with the correct encapsulation.
see https://learningnetwork.cisco.com/s/question/0D53i00000KssjfCAB/routing-rib-vs-fib

upvoted 1 times

Question #534 *Topic 1*

What does a YANG model provide?

A. standardized data structure independent of the transport protocols

B. creation of transport protocols and their interaction with the OS

C. user access to interact directly with the CLI of the device to receive or modify network configurations

D. standardized data structure that can be used only with NETCONF or RESTCONF transport protocols

Correct Answer: *D*

Community vote distribution

A (100%)

kebkim Highly Voted 1 year, 2 months ago

A?
YANG is a standards-based, extensible data modeling language that is used to model the configuration and operational state data, remote procedure calls (RPCs), and server event notifications of network devices. The NETMOD working group in the IETF originally designed YANG to model network management data and to provide a standard for the content layer of the Network Configuration Protocol (NETCONF) model. However, YANG is protocol independent, and YANG data models can be used independent of the transport or RPC protocol and can be converted into any encoding format supported by the network configuration protocol.

upvoted 6 times

jhonmeikel Most Recent 3 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

HarwinderSekhon 5 months ago

A because NETCONF and RESTCONF are not the only protocols as gRPC uses YANG as well.

upvoted 1 times

rami_mma 8 months, 1 week ago

Selected Answer: A

YANG is a standards-based

upvoted 1 times

Cooldude89 9 months, 3 weeks ago

A is correct
YANG is independent of the transport protocol

upvoted 2 times

poy4242 11 months, 1 week ago

Selected Answer: A

agree with A

upvoted 1 times

Dataset 11 months, 2 weeks ago

Selected Answer: A

A is the correct

upvoted 1 times

yousif387 1 year ago

Selected Answer: A

https://www.juniper.net/documentation/us/en/software/junos/netconf/topics/concept/netconf-yang-overview.html#:~:text=However%2C%20YANG%20is%20protocol%20independent,by%20the%20network%20configuration%20protocol.

upvoted 1 times

Abudi 1 year, 2 months ago

Selected Answer: A

A is correct

upvoted 3 times

jj970us 1 year, 2 months ago

Selected Answer: A

Reference: https://www.juniper.net/documentation/us/en/software/junos/netconf/topics/concept/netconf-yang-overview.html

upvoted 4 times

nushadu 11 months, 4 weeks ago

A. thanks for link - "However, YANG is protocol independent, and YANG data models can be used independent of the transport or RPC protocol and can be converted into any encoding format supported by the network configuration protocol."

upvoted 2 times

Question #535 *Topic 1*

A system must validate access rights to all its resources and must not rely on a cached permission matrix. If the access level to a given resource is revoked but is not reflected in the permission matrix, the security is violated. Which term refers to this REST security design principle?

A. economy of mechanism

B. complete mediation

C. separation of privilege

D. least common mechanism

Correct Answer: *B*

Community vote distribution

B (100%)

Cer_Pit Highly Voted 1 year ago

Selected Answer: B

B is correct.

Complete Mediation: A system should validate access rights to all its resources to ensure that they're allowed and should not rely on the cached permission matrix. If the access level to a given resource is being revoked, but that isn't reflected in the permission matrix, it would violate the security.
https://restfulapi.net/security-essentials/

upvoted 5 times

kewokil120 Most Recent 10 months, 3 weeks ago

Selected Answer: B

B is right.

upvoted 2 times

kebkim 1 year, 2 months ago

B.
Complete Mediation: A system should validate access rights to all its resources to ensure that they're allowed and should not rely on the cached permission matrix. If the access level to a given resource is being revoked, but that isn't reflected in the permission matrix, it would violate the security.

upvoted 2 times

Joseph123 1 year, 2 months ago

Correct

upvoted 2 times

Question #536 *Topic 1*

```
monitor session 11 type erspan-source
source interface GigabitEthernet3
destination
erspan-id 12
ip address 10.10.10.10
origin ip address 10.100.10.10
```

Refer to the exhibit. Which command set completes the ERSPAN session configuration?

A. monitor session 11 type erspan-destination destination interface GigabitEthemet4 source erspan-id 11 ip address 10.10.10.10

B. monitor session 12 type erspan-destination destination interface GigabitEthernet4 source erspan-id 12 ip address 10.10.10.10

C. monitor session 11 type erspan-destination destination interface GigabitEthernet4 source erspan-id 12 ip address 10.100.10.10

D. monitor session 12 type erspan-destination destination interface GigabitEthernet4 source erspan-id 11 ip address 10.10.10.10

Correct Answer: *C*

Community vote distribution

B (90%) 10%

HungarianDish Highly Voted 9 months, 3 weeks ago

Selected Answer: B

https://www.networkstraining.com/how-to-configure-cisco-span-rspan-erspan/

The flow ID (erspan-id) must be the same on both devices (to identify the ERSPAN traffic).

Under erspan-source, the destination IP is the IP where we want to send the traffic (e.g. the machine with an analyzer).
The origin IP address is the source of the traffic to be monitored.

Under erspan-destination, the source IP address is the same as the destination IP address of the corresponding source session.

The session IDs (#monitor session ...) don't have to match for the source session and end session.

upvoted 8 times

TSKARAN Highly Voted 10 months ago

Selected Answer: B

```
R1(config)#monitor session 1 type erspan-source
R1(config-mon-erspan-src)#source interface GigabitEthernet 2 rx
R1(config-mon-erspan-src)#no shutdown
R1(config-mon-erspan-src)#destination
R1(config-mon-erspan-src-dst)#erspan-id 100
R1(config-mon-erspan-src-dst)#ip address 172.16.2.200
R1(config-mon-erspan-src-dst)#origin ip address 172.16.12.1

R2(config)#monitor session 1 type erspan-destination
R2(config-mon-erspan-dst)#no shutdown
R2(config-mon-erspan-dst)#destination interface GigabitEthernet 2
R2(config-mon-erspan-dst)#source
R2(config-mon-erspan-dst-src)#erspan-id 100
R2(config-mon-erspan-dst-src)#ip address 172.16.2.200
```

upvoted 7 times

HungarianDish 9 months, 3 weeks ago

From:
https://networklessons.com/cisco/ccie-routing-switching-written/erspan

upvoted 2 times

ihateciscoreally Most Recent 4 months ago

of course not covered in OCG. the more questions im looking at i think OCG is kind of sabotage.

upvoted 3 times

CKL_SG 4 months, 3 weeks ago

Selected Answer: B

Other sample of Erspan configuration

```
Router1(config)#monitor session 1 type erspan-source
Router1(config-mon-erspan-src)# description SOURCE
Router1(config-mon-erspan-src)#source interface GigabitEthernet0/0/1 rx
```

Router1(config-mon-erspan-src)#no shutdown
Router1(config-mon-erspan-src)#
Router1(config-mon-erspan-src)#destination
Router1(config-mon-erspan-src-dst)#erspan-id 10
Router1(config-mon-erspan-src-dst)#ip address 172.16.30.254
Router1(config-mon-erspan-src-dst)#origin ip address 172.16.20.10

Router2(config)#monitor session 1 type erspan-destination
Router2(config-mon-erspan-dst)#description DESTINATION
Router2(config-mon-erspan-dst)#no shutdown
Router2(config-mon-erspan-dst)#destination interface GigabitEthernet0/0/1
Router2(config-mon-erspan-dst)#source
Router2(config-mon-erspan-dst-src)#erspan-id 10
Router2(config-mon-erspan-dst-src)#ip address 172.16.30.254

https://study-ccnp.com/erspan-encapsulated-remote-span-explained/#:~:text=ERSPAN%20Configuration&text=To%20configure%20the%20destination%2C%20enter,be%20sent%20to%20be%20analyzed.

upvoted 2 times

[Removed] 4 months, 4 weeks ago

Selected Answer: C

ERSPAN has two main devices, the source device from which the mirrored traffic will be originated from, and the destination device where the packet analyzer tool is connected and for which the mirrored packets will be forwarded two. And these devices create a tunnel between each other to encapsulate the mirrored traffic across a layer 3 network.

>ERSPAN Source Device needs to configure the following:

--> 1) Define the Monitor Session and the type of ERSPAN (Source)
monitor session <id> type erspan-source
--> 2) Define the Source Interface or VLAN. Where the mirrored traffic originates from
source interface <interface> or source vlan <vlan-id>
--> 2a) Enter Destination configuration mode and:
destination
--> 3) Define the ERSPAN ID (THIS MUST MATCH ON BOTH DEVICES)
erspan id <id>
--> 4) Define the Destination IP address. This is the remote device's address
ip address <address>
-->5) Define the Origin IP address that connects the other end of the ERSPAN tunnel
origin ip address <address>

Continued...

upvoted 2 times

[Removed] 4 months, 4 weeks ago

Shoot I missclicked and chose the Wrong Answer by accident, its B

upvoted 1 times

[Removed] 4 months, 4 weeks ago

>ERSPAN Destination Device needs to configure the following:

--> 1) Define the Monitor Session and the type of ERSPAN (Destination)
monitor session <id> type erspan-destination
--> 2) Define the Destination Interface Where the mirrored traffic will be forwarded to
destination interface <interface>
--> 2a) Enter SOURCE configuration mode and:
source
--> 3) Define the ERSPAN ID (THIS MUST MATCH ON BOTH DEVICES)
erspan id <id>
--> 4) Define the SOURCE IP address. This is the remote device's ORIGIN IP address
ip address <address>

upvoted 1 times

teikitiz 4 months, 4 weeks ago

the destination IP and erspan-id must match. It's B.

upvoted 1 times

Splashisthegreatestmovie 5 months, 2 weeks ago

Help me out on this one please. I'm hung up with the monitor session command 11 having to match. Why is this wrong?

upvoted 1 times

olaniyijt 7 months, 2 weeks ago

Answer is B

upvoted 1 times

dragonwise 8 months ago

A.
monitor session 11 type erspan-destination
destination interface GigabitEthemet4
source erspan-id 11
ip address 10.10.10.10

B.
monitor session 12 type erspan-destination
destination interface GigabitEthernet4
source erspan-id 12
ip address 10.10.10.10

C.
monitor session 11 type erspan-destination
destination interface GigabitEthernet4
source erspan-id 12
ip address 10.100.10.10

D.
monitor session 12 type erspan-destination
destination interface GigabitEthernet4
source erspan-id 11
ip address 10.10.10.10
upvoted 3 times

John13121 10 months, 3 weeks ago
It is B, Refer to question 569.
upvoted 1 times

Darude 1 year ago
Selected Answer: B
correct answer is B - the source IP of erspan-destination is local IP(or erspan-source destination IP)
reference:https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/system_mgmt/503_u2_2/Cisco_Nexus_3000_system_mgmt_config_gd_503_U2_2_chapter14.pdf
upvoted 2 times

Darude 1 year ago
sorry NOT "or" IT IS erspan-source destination IP
upvoted 1 times

iGlitch 1 year ago
Selected Answer: B
It looks suspicious, but trust me it's B.
upvoted 3 times

mitosenoriko 1 year ago
Selected Answer: C
given answer is correct.
because..
first
complete sentences

A.
Router(config)# monitor session 11 type erspan-destination
Router(config-erspan-dst)# destination interface GigabitEthemet4
Router(config-erspan-dst)# source
Router(config-erspan-dst-src)# erspan-id 11
Router(config-erspan-dst-src)# ip address 10.10.10.10 << not source(origin) address

C.
Router(config)# monitor session 11 type erspan-destination
Router(config-erspan-dst)# destination interface GigabitEthernet4
Router(config)# source
Router(config-erspan-dst-src)# erspan-id 12
Router(config-erspan-dst-src)# ip address 10.100.10.10 << source(origin) address
upvoted 1 times

mitosenoriko 1 year ago
second.
ERSPAN configure example(source)

Router(config)# monitor session 3 type erspan-source
Router(config-mon-erspan-src)# source interface gigabitethernet 4/1
Router(config-mon-erspan-src)# destination
Router(config-mon-erspan-src-dst)# ip address 10.1.1.1
Router(config-mon-erspan-src-dst)# origin ip address 10.2.2.2
Router(config-mon-erspan-src-dst)# erspan-id 101

ERSPAN configure example(destination)
Router(config)# monitor session 3 type erspan-destination
Router(config-erspan-dst)# destination interface gigabitethernet 2/1
Router(config-erspan-dst)# source
Router(config-erspan-dst-src)# ip address 10.1.1.1
Router(config-erspan-dst-src)# erspan-id 101

upvoted 1 times

dogdoglee 1 year ago

from your example can find answer is B
Router(config-mon-erspan-src-dst)# ip address 10.1.1.1
Router(config-mon-erspan-src-dst)# origin ip address 10.2.2.2

Router(config-erspan-dst-src)# ip address 10.1.1.1 <- not origin ip 10.2.2.2

upvoted 3 times

melkij17 1 year, 2 months ago

B is correct.
Configuration happens on two different routers, so ERSPAN - ID must match (this gives us B and C). Under Destination section we have IP address which is analysers IP 10.10.10.10, so under Source section IP address must be same 10.10.10.10 (analysers IP)

upvoted 4 times

jdholmes423 1 year, 2 months ago

Selected Answer: B

I also agree that B is the answer.

upvoted 4 times

Lukaszaw 1 year, 2 months ago

B is correct

upvoted 2 times

Deu_Inder 1 year, 2 months ago

Agreed.

upvoted 1 times

Question #537 *Topic 1*

"HTTP/1.1 204 No Content" is returned when the curl -i -X DELETE command is issued. Which situation has occurred?

A. The command succeeded in deleting the object.

B. The object was located at the URI, but it could not be deleted

C. The object could not be located at the URI path.

D. The URI was invalid.

Correct Answer: *A*

kebkim Highly Voted 1 year, 2 months ago

A.
The HTTP 204 No Content success status response code indicates that a request has succeeded, but that the client doesn't need to navigate away from its current page.

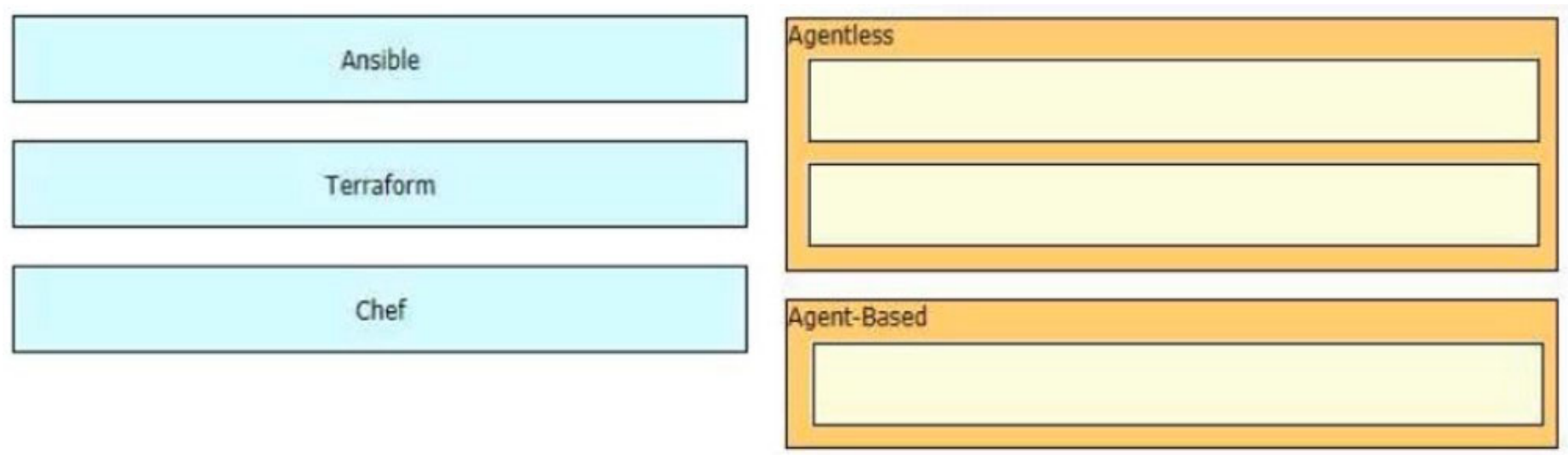
upvoted 10 times

Question #538 *Topic 1*

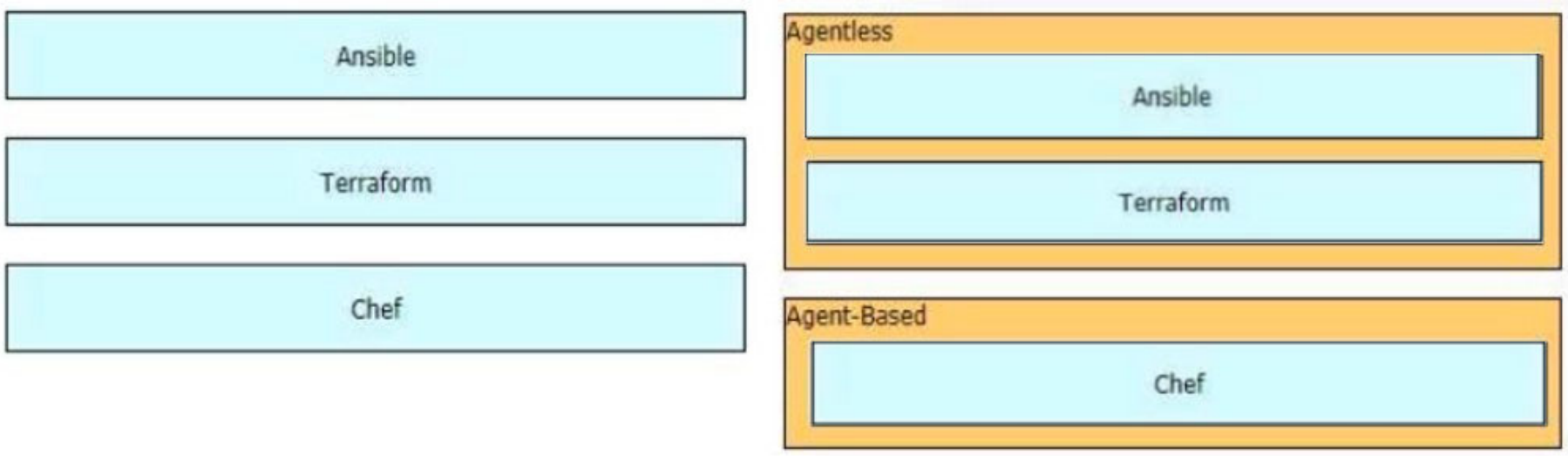
DRAG DROP -

Drag and drop the tools from the left onto the agent types on the right.

Select and Place:



Correct Answer:



Dataset 3 months, 3 weeks ago

thats correct!
Regards

upvoted 2 times

snarkymark 9 months, 4 weeks ago

Agree on answer.
https://niveussolutions.com/chef-vs-terraform-vs-ansible-comparison/#:~:text=Chef%20and%20Ansible%20are%20configuration,hand%20is%20a%20provisioning%20tool.

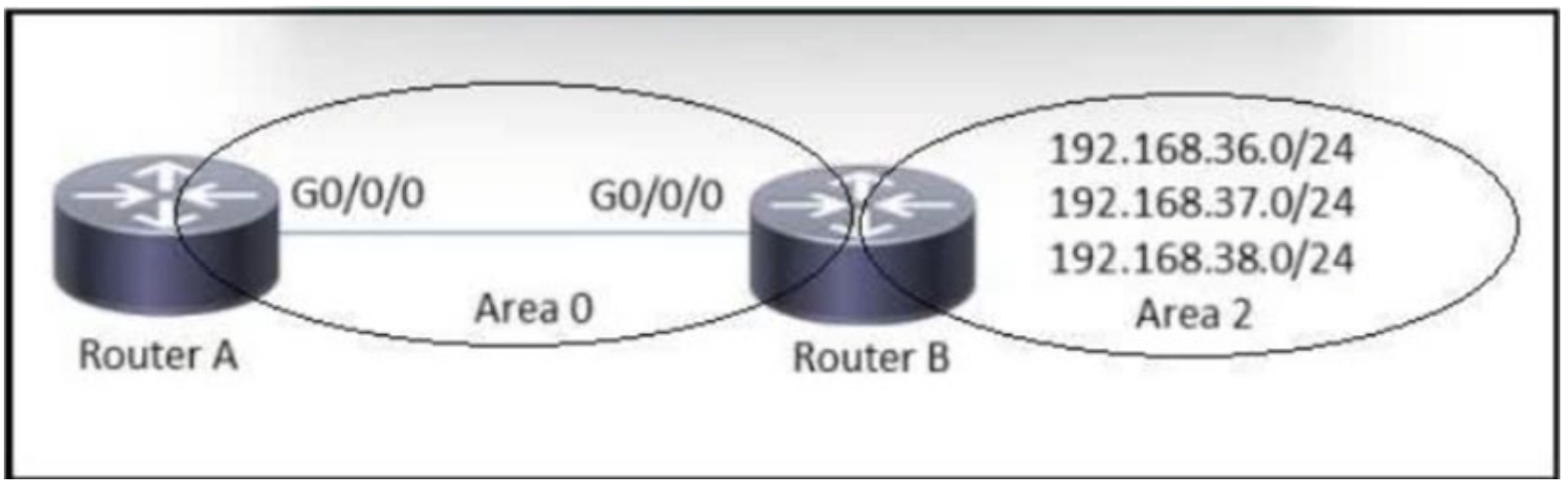
upvoted 4 times

bora4motion 1 year ago

Provided answer is correct.
Terraform is infrastructure as code.
Ansible relies on SSH.

upvoted 4 times

Question #539 *Topic 1*



Refer to the exhibit. Which configuration is required to summarize the Area 2 networks that are advertised to Area 0?

A. RouterB(config)# router ospf 1 RouterB(config-router)# area 2 range 192.168.36.0 255.255.252.0

B. RouterB(config)# router ospf 1 RouterB(config-router)# network 192.168.38.0 255.255.255.0

C. RouterB(config)# router ospf 1 RouterB(config-router)# network 192.168.38.0 255.255.252.0

D. RouterB(config)# router ospf 1 RouterB(config-router)# area 2 range 192.168.36.0 255.255.255.0

Correct Answer: *A*

Community vote distribution

A (100%)

mgiuseppe86 2 months, 2 weeks ago

This is really a subnetting question. Nothing really to do with OSPF if you think about what the question is asking you.

It wants you to summarize 3 /24s

B only covers one /24.. what about the other two networks? WRONG
C is getting somewhere with a /22 but the wrong network ID is listed. 38.0 in a /22 is a client IP, not a network IP
D is like B, it only covers the first /24 and not the entire /22 we need to include all 3 /24s

A is the only answer that works. in a /22, 192.168.36.0 is a network IP that covers up to 192.168.39.255

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

its always area you are summarizing from. In this case we are summerzing area 2 routes and check aggregated (Supernet) Mask.

upvoted 1 times

nushadu 11 months, 1 week ago

Selected Answer: A

this is ABR (area 0 & 22) :
cisco_R3(config-router)#area 22 range 55.0.0.0 255.255.192.0
cisco_R3(config-router)#
cisco_R3(config-router)#do s runn | s router ospf
router ospf 1
router-id 3.3.3.3
auto-cost reference-bandwidth 1000
area 22 range 55.0.0.0 255.255.192.0
area 22 filter-list prefix PL_3 in
passive-interface default
no passive-interface Ethernet0/0.10
no passive-interface Ethernet0/0.50
network 0.0.0.0 255.255.255.255 area 0
bfd all-interfaces
cisco_R3(config-router)#

upvoted 2 times

nushadu 11 months, 1 week ago

far-end in the area 0 - netw mask has been changed + debug;
cisco_R2#show ip route ospf
55.0.0.0/24 is subnetted, 1 subnets
O IA 55.0.0.0 [110/201] via 192.168.255.3, 00:07:30, Ethernet0/0.10
cisco_R2#
cisco_R2#
*Dec 23 15:27:11.674: RT: updating ospf 55.0.0.0/18 (0x0) :
via 192.168.255.3 Et0/0.10 0 1048578

*Dec 23 15:27:11.674: RT: network 55.0.0.0 is now variably masked
*Dec 23 15:27:11.674: RT: add 55.0.0.0/18 via 192.168.255.3, ospf metric [110/201]
*Dec 23 15:27:11.674: RT: updating ospf 10.111.10.0/30 (0x0) :
via 192.168.255.3 Et0/0.10 0 1048578

*Dec 23 15:27:11.674: RT: rib update return code: 17
*Dec 23 15:27:11.679: RT: del 55.0.0.0 via 192.168.255.3, ospf metric [110/201]
*Dec 23 15:27:11.679: RT: delete subnet route to 55.0.0.0/24
cisco_R2#
cisco_R2#show ip route ospf

55.0.0.0/18 is subnetted, 1 subnets
O IA 55.0.0.0 [110/201] via 192.168.255.3, 00:02:09, Ethernet0/0.10
cisco_R2#

upvoted 1 times

nushadu 11 months ago

+ you'll see this summary route on the ABR, it will reject all traffic that does not match more specific route in this range (everything in range 55.0.0.0/18 -> Null0 except 55.0.0.0/24)

cisco_R3#show ip route ospf | b Ga
Gateway of last resort is 2.2.2.2 to network 0.0.0.0

55.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O 55.0.0.0/18 is a summary, 00:07:13, Null0 <<<<<<<<<<<<<<<<<<< reject
O 55.0.0.0/24 [110/101] via 10.111.10.2, 00:07:13, Ethernet0/0.50 <<<<<<<<< except this
cisco_R3#

upvoted 1 times

bendarkel 1 year ago

Selected Answer: A

Provided answer is correct.

upvoted 2 times

Question #540 *Topic 1*

Based on the router's API output in JSON format below, which Python code will display the value of the "role" key?

```
{
    "response": [{
            "family": "Routers",
            "macAddress": "00:c8:8b:80:bb:00",
            "hostname": "BorderA",
            "role": "BORDER ROUTER",
            "lastUpdateTime": 1577420806077,
            "serialNumber": "FXS8799Q1SE",
            "softwareVersion": "16.3.2",
            "upTime": "5 days, 9:22:32:17",
            "lastUpdated": "2021-03-05 23:30:37"
    }]
}
```

A.

```
json_data = json.loads(response.text)
print(json_data['response']['family']['role'])
```

B.

```
json_data = response.json()
print(json_data['response'][0]['role'])
```

C.

```
json_data = response.json()
print(json_data['response'][family]['role'])
```

D.

```
json_data = json.loads(response.text)
print(json_data[response][0][role])
```

Correct Answer: *B*

HarwinderSekhon 5 months, 2 weeks ago

D is missing " " and response has list [] and you numbers 0, 1, 2 etc to reference list index.
B is the answer.

upvoted 1 times

shellder 10 months ago

Answer is B.
response.json() returns a JSON object of the result (if the result was written in JSON format, if not it raises an error). Python requests are generally used to fetch the content from a particular resource URI. Whenever we make a request to a specified URI through Python, it returns a response object. Now, this response object would be used to access certain features such as content, headers, etc. This article revolves around how to check the response.json() out of a response object. It is one of the most used methods in the requests module.

upvoted 2 times

poy4242 11 months, 1 week ago

B and D are valid. json.loads(r.text) or r.json() both return the same DIC type...

upvoted 1 times

poy4242 11 months, 1 week ago

B is the good one D is missing the escape caracter '

upvoted 3 times

nushadu 11 months, 3 weeks ago

Parse JSON - Convert from JSON to Python
If you have a JSON string, you can parse it by using the json.loads() method.
The result will be a Python dictionary.

upvoted 1 times

nushadu 11 months, 3 weeks ago

D.
x = {'response': [{
"name": "John",
"age": 30,
"city": "New York"}]
}
print(x['response'][0]['age'])

==
result is 30
upvoted 1 times

nushadu 11 months ago
so sorry, D.
upvoted 1 times

nushadu 11 months ago
shit happens - B. is correct, sorry for flood, or just remove all my comments here!
upvoted 1 times

Gedson 11 months, 3 weeks ago
La B es correcta,
upvoted 4 times

ricaela10 11 months, 3 weeks ago
based on other sites,
answer is D
upvoted 2 times

Question #541 *Topic 1*

What is the recommended minimum SNR for voice applications on wireless networks?

A. 10

B. 15

C. 20

D. 25

Correct Answer: *D*

Community vote distribution

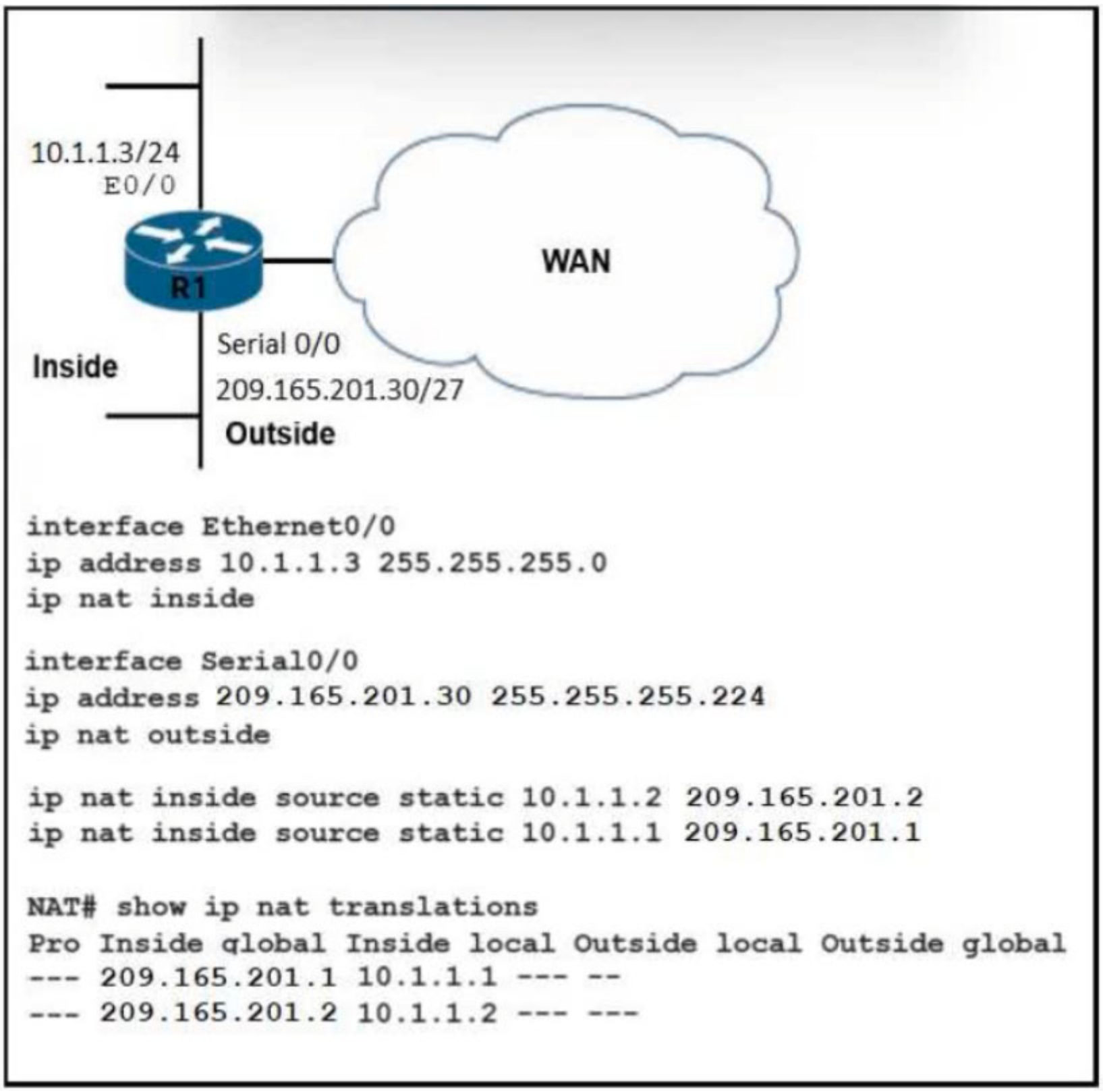
D (100%)

kebkim Highly Voted 1 year, 2 months ago
D.
Generally, a signal with an SNR value of 20 dB or more is recommended for data networks where as an SNR value of 25 dB or more is recommended for networks that use voice applications.
upvoted 9 times

HungarianDish Most Recent 9 months, 3 weeks ago
Selected Answer: D
https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength
upvoted 2 times

Raipen24 1 year ago
answer is correct
upvoted 3 times

Question #542 *Topic 1*



Refer to the exhibit. What are two results of the NAT configuration? (Choose two.)

A. Packets with a destination of 200.1.1.1 are translated to 10.1.1.1 or .2, respectively.

B. A packet that is sent to 200 1.1.1 from 10.1.1.1 is translated to 209.165.201.1 on R1.

C. R1 is performing NAT for inside addresses and outside address.

D. R1 looks at the destination IP address of packets entering S0/0 and destined for inside hosts.

E. R1 processes packets entering E0/0 and S0/0 by examining the source IP address.

Correct Answer: *BC*

Community vote distribution

BD (72%) BC (28%)

snarkymark Highly Voted 9 months, 4 weeks ago

I am leaning towards BD. Here is the problem with C.
The wording says outside. Technically the "209" address is considered inside global. So, in those terms it would not be outside.
https://ipwithease.com/nat-understanding-local-global-inside-and-outside-addresses/

upvoted 6 times

djedeen Most Recent 3 months, 1 week ago

Selected Answer: BD

R1 is only NATing the inside IPs to the outside.

upvoted 1 times

myhdtv6 4 months, 1 week ago

Guys anybody can help, how come 200.1.1.1 came from ?????
upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

f you have to ask this question, you should be studying for CCNA or Network+ or go learn how the internet works first before you shame us all and get your CCNP working jobs you dont deserve.

Anyone who is at this level understands when questions like this come up, we are expected to analyze everything and realize the concepts.

We are NATing addresses to connect to the internet, presumably,, so its asking us how packets are sent to a public IP (200.1.1.1 in this example). We are expected to understand that once we NAT to our ISP IP (209.167.201.30/27) that we can theoretically route to any other public IP Space thereonafter (hence the WAN Cloud).

Cisco does create ridiculous questions usually but this is a pretty decent one.
upvoted 2 times

PureInertiaCopy 3 months, 1 week ago

If client 10.1.1.1 or 10.1.1.2 on the inside network are reaching out to a server on the outside with any global IP address, then they will be translated.

Let's pretend 200.1.1.1 is a youtube server. Then client 10.1.1.1 will be translated to 209.169.201.1, in order to reach out to it.
upvoted 2 times

ando2023 5 months, 2 weeks ago

I feel its B and C. With static one to one NAT, traffic can originate from either the internal or external side. There does not need to be a specific line for NAT one to one from the external to the internal. In the real world. you would have a firewall rules if necessary to block the inbound connection.
upvoted 1 times

Papins 6 months, 3 weeks ago

Who is 200.1.1.1 btw? i'll go with CD
upvoted 2 times

mgiuseppe86 2 months, 2 weeks ago

I
mgiuseppe86 0 minutes ago Awaiting moderator approval
f you have to ask this question, you should be studying for CCNA or Network+ or go learn how the internet works first before you shame us all and get your CCNP working jobs you dont deserve.

Anyone who is at this level understands when questions like this come up, we are expected to analyze everything and realize the concepts.

We are NATing addresses to connect to the internet, presumably,, so its asking us how packets are sent to a public IP (200.1.1.1 in this example). We are expected to understand that once we NAT to our ISP IP (209.167.201.30/27) that we can theoretically route to any other public IP Space thereonafter (hence the WAN Cloud).

Cisco does create ridiculous questions usually but this is a pretty decent one.
upvoted 1 times

byallmeans 6 months, 4 weeks ago

Selected Answer: BC

given answer is correct. Static one-to-one NAT is bidirectional.
D - is very vague when it mentions inside address, almost as if it's trying to say the original destination address it's looking at as traffic enters S0/0 interface is the internal address, which would be wrong.
upvoted 2 times

x3rox 10 months ago

Selected Answer: BD

This is the Correct answers: BD
A: is DEAD wrong
*B: Because there is a 1:1 mapping so that 10.1.1.1 is translated to 209.169.201.1 to any destination.
C: WRONG because the command was ip nat "inside",it's just that the initial traffic from the outside it's staticly
set in the nat table but it's only "Natting" for inside addreses.
to those outside local addresses are translated to internal ip.
*D:is RIGHT since "initial traffic" on S0/0 needs to look at the destination "outside Local"
E: WRONG R1 look at the destination for S0/0 for "initiating traffic" in order to match the outside local to inside local AND source when initial traffic is from the inside - So it's wrong in saying that it will look at destination for both.
upvoted 3 times

x3rox 10 months ago

More on C: to do natting for the outside the command would be "ip nat outside"
upvoted 3 times

HungarianDish 10 months, 2 weeks ago

Selected Answer: BD

In this case, NAT translates the inside local IP address to the inside global IP address.
On the return traffic, the destination inside global IP address gets translated back to the inside local IP address.

Based on the picture, there aren't any outside address translations involved in this scenario.

(Even though, the traffic flows between the inside and outside interfaces of R1.)

Source:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3548/sw/interfaces/b_N3548_Interfaces_Config_503_A1/b_N3548_Interfaces_Config_503_A1_chapter_0101.pdf

Thus, I go with B,D (however, D describes a general function of the router).
upvoted 2 times

kewokil120 10 months, 3 weeks ago

Selected Answer: BD

BD is right.
upvoted 2 times

M_B 10 months, 3 weeks ago

The best answer must always be chosen- the router is not doing NAT for outside addresses as per translations table so C is incorrect. A and E are definitely incorrect. That leaves D which is a function performed by the router, so that is the best response for the question
upvoted 1 times

nushadu 11 months, 1 week ago

Selected Answer: BC

B. A packet that is sent to 200 1.1.1 from 10.1.1.1 is translated to 209.165.201.1 on R1.
C. R1 is performing NAT for inside addresses and outside address.
both answers related to STATIC NAT ONE_TO_ONE, it works on both directions (inbound\outbound), and it does not matter from WHERE IP Packed has arrived (LAN or WAN)
NAT will be performed in any way, just google and read it (nat one to one)

>D. R1 looks at the destination IP address of packets entering S0/0 and destined for inside hosts.
it can not be true because R1 itself is the last hop\destination in the trace (wan IP) i.e. arrived packets to this both NAT PUBLIC IP will be translated to RFC1918 and vice versa.
Enjoi!))
upvoted 1 times

H3kerman 1 year ago

Selected Answer: BD

there is no outside entry in translations table
upvoted 1 times

yousif387 1 year ago

Selected Answer: BD

BD is correct
upvoted 1 times

Darude 1 year ago

Selected Answer: BD

correct answer is B, D C=wrong because it describe PAT adress translation "many to one"
reference: https://www.netsetup.it/cisco/78-configurazione-nat-router-cisco
upvoted 2 times

iGlitch 1 year ago

Selected Answer: BD

B and D are correct.
upvoted 1 times

i_am 1 year, 1 month ago

B and D would be correct. C is not correct as there is no translation for outside addresses.
upvoted 2 times

onkel_andi 1 year, 1 month ago

And where do we see the traffic translation to 200 1.1.1
upvoted 2 times

mgiuseppe86 2 months, 2 weeks ago

If you have to ask this question, you should be studying for CCNA or Network+ or go learn how the internet works first before you shame us all and get your CCNP working jobs you dont deserve.

Anyone who is at this level understands when questions like this come up, we are expected to analyze everything and realize the concepts.

We are NATing addresses to connect to the internet, so it asking us how to route to a public IP (200.1.1.1 in this example). We are expected to understand that once we NAT to our ISP IP (209.167.201.30/27) that we can route to any other public IP Space thereonafter.

Cisco does create ridiculous questions usually but this is a pretty decent one.
upvoted 1 times

x3rox 9 months, 1 week ago

This IP is irrelevant, it's just to confuse you. 200.1.1.1 it's just a general IP destination, It could've been 8.8.8.8 and the result is the same.

upvoted 1 times

Question #543 *Topic 1*

A network engineer must configure a switch to allow remote access for all feasible protocols Only a password must be requested for device authentication and all idle sessions must be terminated in 30 minutes. Which configuration must be applied?

A. line vty 0 15 password cisco transport input telnet ssh exec-timeout 30 0

B. line vty 0 15 password cisco transport input all exec-timeout 0 30

C. username cisco privilege 15 cisco line vty 0 15 transport input telnet ssh login local exec-timeout 0 30

D. line console 0 password cisco exec-timeout 30 0

Correct Answer: *B*

Community vote distribution

A (100%)

jj970us Highly Voted 1 year, 2 months ago

Selected Answer: A

exec-timeout minutes [seconds]
upvoted 11 times

Deu_Inder 1 year, 2 months ago

A does not fulfil the requirement of allowing all feasible protocols. It only allows ssh and telnet.
upvoted 2 times

mgiuseppe86 2 months, 2 weeks ago

> A does not fulfl the requreiment of allow all feasible protocols

This statement right here just proved to me you have ZERO real-world experience

Tell me what other feasible protocols, other than SSH and Telnet are available for VTY?
upvoted 1 times

Pilgrim5 7 months ago

You're right but look at the exec-timeout command.

It's wrong on B, so it makes A the most reasonable choice even if A just specifies just telnet and SSH only
upvoted 1 times

ronin 1 year, 2 months ago

Router(config-line)# exec-timeout 3 30
In the example configuration above, exec-timeout is set with 3 minutes and 30

https://study-ccnp.com/cisco-exec-timeout-absolute-timeout-commands/#:~:text=The%20Cisco%20'exec%2Dtimeout'%20command%20sets%20a%20specific%20time,run%20before%20it%20will%20time out.
upvoted 1 times

Caledonia Highly Voted 1 year, 2 months ago

Selected Answer: A

A is the answer. I don't know any other remote session apart from SSH and Telnet.
upvoted 6 times

HarwinderSekhon 5 months, 2 weeks ago

transport input ?
all All protocols
lapb-ta LAPB Terminal Adapter
lat DEC LAT protocol
mop DEC MOP Remote Console Protocol
none No protocols
pad X.3 PAD
rlogin Unix rlogin protocol
ssh TCP/IP SSH protocol
telnet TCP/IP Telnet protocol
udptn UDPTN async via UDP protocol
v120 Async over ISDN
upvoted 2 times

Splashisthegreatestmovie 5 months, 2 weeks ago

There's no way in 2023 that anything but telnet or ssh is feasible and it's questionable that telnet still qualifies as feasible. We can actually still configure DLCIs but there's no way we can expect it work.

upvoted 1 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago

Selected Answer: A

A is the absolute 1000% answer

Only a password? CHECK (password cisco)
Terminated in 30 minutes? CHECK (30 0)
ALLOW ALL FEASIBLE PROTOCOLS? CHECK CHECK CHECK - SSH AND TELNET ARE THE ONLY PROTOCOLS AVAILABLE, SO BECAUSE BOTH ARE THERE, IT TECHNICALLY MEANS ALL ARE ALLOWED

Tell me what other feasible protocols, other than SSH and Telnet are available for VTY?

upvoted 1 times

pc_evans 2 months, 2 weeks ago

A is wrong because you need a username and password to connect via SSH so login local is requrired.

B is wrong because of incorrect exec-timeout
C has wrong exec-timeout value.
D. uses the console line

How do you create a ssh session without using login local or AAA?

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

Selected Answer: A

Vague question cisco.
exec-timeout 30 0
exec-timeout 0 30 means time out after 0 minutes and 30 seconds.
A is right answer kinda exec-timeout timing wise but it does not cover all porotocols such as -
Router(config-line)#transport input ?
all All protocols
lapb-ta LAPB Terminal Adapter
lat DEC LAT protocol
mop DEC MOP Remote Console Protocol
none No protocols
pad X.3 PAD
rlogin Unix rlogin protocol
ssh TCP/IP SSH protocol
telnet TCP/IP Telnet protocol
udptn UDPTN async via UDP protocol
v120 Async over ISDN

upvoted 2 times

ando2023 5 months, 2 weeks ago

Selected Answer: A

I intially thought B, but the times are out for the Exec-Timeout, so the only option really then is A. I don't like how they ask for "all feasible protocols". They are making a trick question, so you have to hope that they mean SSH and Telnet when they said "all feasible protocols"

upvoted 1 times

Papins 6 months, 3 weeks ago

Provided answer is correct B, question didn't mention to allow only ssh & telnet.

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

This statement right here just proved to me you have ZERO real-world experience

Tell me what other feasible protocols, other than SSH and Telnet are available for VTY?

upvoted 1 times

Papins 6 months, 3 weeks ago

exec-timeout MINUTES SECONDS - Apology although it not mention about ssh & telnet but the is 30minutes was the one of the question indicator.

upvoted 1 times

Vlad_Is_Love_ua 9 months, 1 week ago

Selected Answer: A

Router(config-line)#exec
Router(config-line)#exec-timeout ?
<0-35791> Timeout in minutes
Router(config-line)#exec-timeout 30 ?
<0-2147483> Timeout in seconds
<cr>
Router(config-line)#exec-timeout 30

upvoted 2 times

snarkymark 9 months, 4 weeks ago

A is correct.
transport input telnet ssh , this is correct format.
exec-timeout 30 0 , this is correct format, 30 mins
upvoted 1 times

HenokFU 10 months ago
correct answer shall be A...first 0 means minutes ...requested is 30 minutes
upvoted 1 times

M_B 10 months, 3 weeks ago
"login" command missing from A but it is the best answer- not necessarily complete - Timeout is incorrect for B and C. D has no protocols so this cannot work
upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago
login is not needed. did you read the question? it says just the password must be requested.
upvoted 1 times

John13121 10 months, 3 weeks ago
stop posting wrong answers... Answer is A...

Switch(config-line)#exec-timeout ?
<0-35791> Timeout in minutes
upvoted 1 times

H3kerman 1 year ago
Selected Answer: A
B would be good for ALL protocols, but timer is 0 minutes 30 seconds, so fue to this A is correct - 30 minutes 0 seconds...
upvoted 2 times

mgiuseppe86 2 months, 2 weeks ago
This statement right here just proved to me you have ZERO real-world experience

Tell me what other feasible protocols, other than SSH and Telnet are available for VTY?

A IS the absolute answer, SSH and TElnet are the ONLY protocols. and because both a re there, it means ALL are allowed.

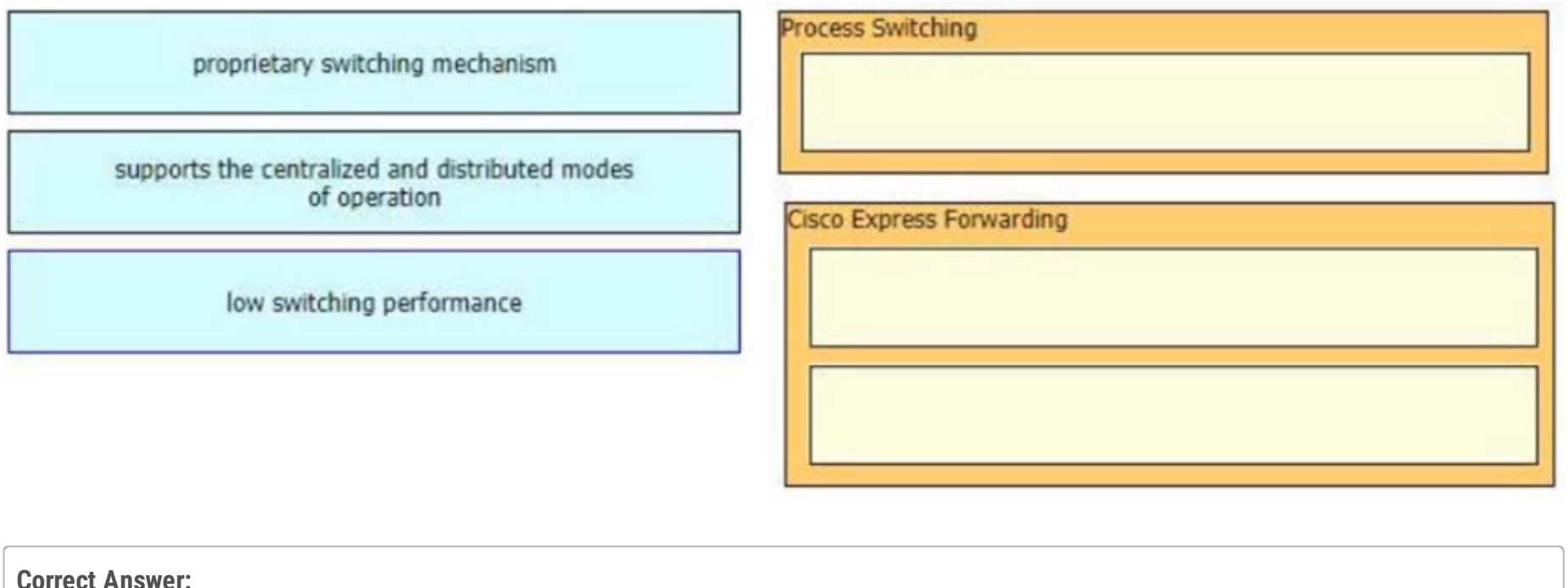
JFC
upvoted 1 times

yousif387 1 year ago
Selected Answer: A
first minute then seconds
upvoted 1 times

DRAG DROP -

Drag and drop the characteristics from the left onto the switching architectures on the right.

Select and Place:



Correct Answer:

TheDazzler Highly Voted 10 months, 2 weeks ago

Given answer is correct:
https://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html

upvoted 7 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago

Remember boys and girls, when Cisco insults other technologies, it's usually ones that are not standard

LOW SWITCHING PERFORMANCE? Cisco would never dare talk bad about their own product, so it must be "Process Switching"

Cisco Express Forwarding Is ThE BeSt

upvoted 4 times

tempaccount00001 4 months, 3 weeks ago

correct

upvoted 1 times

```
SW1#show cdp neighbors | include Local|0/1
Device ID       Local Intrfce     Holdtme    Capability  Platform  Port ID
SW2             Fas 0/1           131        R S  WS-C3750- Fas 0/1

SW1#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On

SW2#show cdp neighbors | include Local|0/1
Device ID       Local Intrfce     Holdtme    Capability  Platform  Port ID
SW1             Fas 0/1           142        R S  WS-C3750- Fas 0/1

SW2#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
```

Refer to the exhibit. An engineer configures a trunk between SW1 and SW2 but tagged packets are not passing. Which action fixes the issue?

A. Configure SW1 with dynamic auto mode on interface FastEthernet0/1.

B. Configure the native VLAN to be the same VLAN on both switches on interface FastEthernet0/1.

C. Configure SW2 with encapsulation dot1q on interface FastEthernet0/1.

D. Configure FastEthernet0/1 on both switches for static trunking.

Correct Answer: *C*

Community vote distribution

C (87%) 13%

CCNPWILL 1 month, 3 weeks ago

Selected Answer: C

C .. ISL and DOT1Q trunking issue.

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Selected Answer: C

SW2 is ISL, SW1 is dot1q.

Nothing else needs to be discussed.

upvoted 2 times

Burik 5 months, 2 weeks ago

Selected Answer: C

The exhibit is from two interfaces configured with non-matching trunking encapsulations, so they are not forming a trunk, as per Operational Mode: static access. In this condition, issuing a switchport mode trunk on both switches as per answer D will just have the effect of blocking the port on SW2 because of inconsistent port type. Change the encapsulation to dot1q on SW2 and the trunk will form.

Just lab it as follows to reproduce the problem.

SW1

interface Fa0/1
switchport trunk encapsulation dot1q

SW2

interface Fa0/1
switchport trunk encapsulation isl

upvoted 1 times

Brand 9 months, 3 weeks ago

Just can't believe how much time and effort we're putting to figure out how a "thing" that is not the valid configuration anymore. I mean who is using "negotiation" on trunks? If it's going to be a trunk, it's "configured" as trunk. Can't really believe...

upvoted 2 times

Leoveil 10 months ago

Selected Answer: C

C is right
D trunk will come up but spaning tree will block the port , will be no communication between devices behind the switches due to the tagging protocols mismatch

upvoted 2 times

markymark874 10 months, 3 weeks ago

Selected Answer: C

Desirable + desirable = trunk.
Isl + dot1q = fail

upvoted 2 times

milovnik1 11 months, 3 weeks ago

Selected Answer: C

C is correct, "static trunking" won't help unless the encapsulation protocol is matching on both sides

upvoted 2 times

nushadu 11 months, 4 weeks ago

Selected Answer: D

D. no doubt, current status is access

upvoted 1 times

bora4motion 11 months, 4 weeks ago

it's C. only one switch must be changed, not both.

upvoted 1 times

nushadu 10 months, 3 weeks ago

see from the picture on both sides:
==
OPERATIONAL MODE: STATIC ACCESS
==
this is why the trunk does not work ...

upvoted 1 times

nushadu 10 months, 3 weeks ago

BTW maybe "C" also working scenario, I do not know

upvoted 1 times

Burik 5 months, 2 weeks ago

The output shows static access because the trunk has not formed. The only working scenario is C. With D, the port on SW2 will be blocked for inconsistent port type.

upvoted 1 times

forccnp 12 months ago

Selected Answer: D

i think D should be the correct answer

upvoted 1 times

bora4motion 1 year ago

Selected Answer: C

C is correct, change from isl to .1q

upvoted 3 times

Question #546 *Topic 1*

When does a Cisco StackWise primary switch lose its role?

A. when a switch with a higher priority is added to the stack

B. when a stack member fails

C. when the priority value of a stack member is changed to a higher value

D. when the stack primary is reset

Correct Answer: *D*

Community vote distribution

D (74%) A (26%)

Jason233 Highly Voted 1 year, 2 months ago

Selected Answer: D

Active and Standby Switch Election and Reelection

All stack members are eligible to be the active switch or the standby switch. If the active switch becomes unavailable, the standby switch becomes the active switch.

An active switch retains its role unless one of these events occurs:

The switch stack is reset.

The active switch is removed from the switch stack.

The active switch is reset or powered off.

The active switch fails.

The switch stack membership is increased by adding powered-on standalone switches or switch stacks.

The active switch is elected or reelected based on one of these factors and in the order listed:

The switch that is currently the active switch.

The switch with the highest stack member priority value

upvoted 7 times

BryCR 1 year, 1 month ago

Jason, it seems based on this answer could be also A and D

upvoted 6 times

bora4motion Highly Voted 1 year ago

Selected Answer: D

even if you change the priority or add a higher priority member to the stack you still have to reboot the stack to change the election, so the correct answer is D.

upvoted 6 times

djedeen Most Recent 3 months, 1 week ago

Selected Answer: D

No preemption so now active change without the primary getting reset.

upvoted 1 times

KingCon 3 months, 4 weeks ago

Selected Answer: A

As per Cisco documentation:

Note: If you reset the stack primary, it would reset the whole stack.

Which means that the original stack primary would more than likely be elected as the primary again.

To add a switch, as a primary, to a stack, complete these steps:

Change the priority value of the switch to be added to a value greater than the highest priority of the stack.
With the new switch powered on, connect the StackWise ports of the switch to the stack.
The election for the stack primary occurs, and the new switch is elected as the primary since it has the highest priority value.
The members of the previous stack reboot themselves to join the new stack.

So D could be true, but I believe based on the documentation that A is the best answer.

upvoted 1 times

WereAllinThisTogether 4 months, 2 weeks ago

B. When a stack member fails.

In a Cisco StackWise stack, the StackWise primary switch is the designated master switch that handles certain control plane functions and provides stack-wide coordination. If the StackWise primary switch fails or becomes unreachable, the stack will automatically elect a new StackWise primary switch from the remaining stack members. This ensures the continuity and resilience of the stack operation.

Therefore, option B is the correct answer. The StackWise primary switch loses its role when a stack member fails.

upvoted 1 times

jeffro9898 4 months, 3 weeks ago

If you reset/reboot only the primary switch in a switch stack, then, during the time that the primary switch is rebooting, the remaining switches in the stack will need to elect a new primary switch, which would most likely be the switch that is acting as the standby switch.

upvoted 1 times

ando2023 5 months, 2 weeks ago

Selected Answer: A

I am having trouble with the answer D, everyone seems to prefer it but by resetting the stack, the same master could be re-elected, resulting in no changes. A definitely makes the current master/active switch lose its master role. A reboot may happen to certain models when a higher priority switch is added to the stack. Why are Cisco putting in so many tricky questions, it all depends on certain circumstances. In this case, I go with A.

upvoted 1 times

teikitiz 4 months, 4 weeks ago

Adding a new member with higher priority is definitive. The current active will lose that role indefinitely. In D, after the reboot, the active will resume its role after reelection. I believe it's A too, but it's one of those questions...

upvoted 1 times

HungarianDish 8 months ago

Selected Answer: A

Let's see what happens after A and after D.
A. when a switch with a higher priority is added to the stack
=> election is triggered, and the stack member with the higher priority becomes the new primary

D. when the stack primary is reset
=> election is triggered, and the current stack primary gets to be reelected

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/71925-cat3750-create-switch-stks.html#anc16
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/ha_stack_manager/configuration_guide/b_hastck_3se_3850_cg/b_hastck_3se_3850_cg_chapter_010.html

The primary is only change after answer A), otherwise the current primary retains its role.

upvoted 1 times

mikhailov_ivan90 10 months ago

Selected Answer: A

I think it should be A, based on https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/71925-cat3750-create-switch-stks.html#anc16
So, in D by default when it is reseted it meand that election will be and there is a chance for the primary be elected again or not, but if you add a new node with higher priority it means 2 things:
1)it will be rebooted anyway
2)based on priority value the new memeber will be primary

upvoted 2 times

jucevabe 1 year, 2 months ago

Thank you Jason

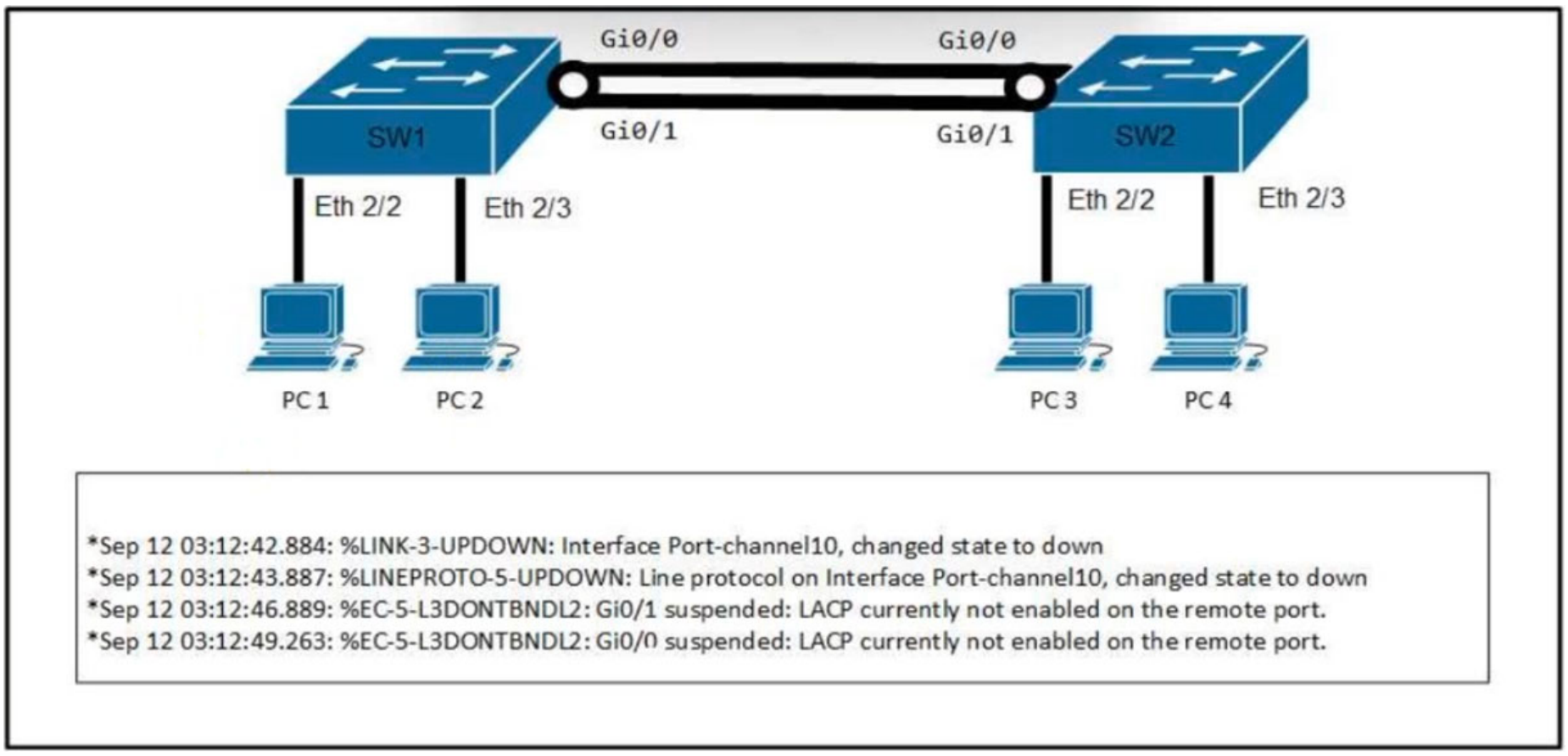
upvoted 2 times

jucevabe 1 year, 2 months ago

answer C

upvoted 1 times

Question #547 *Topic 1*



Refer to the exhibit. A network engineer troubleshoots an issue with the port channel between SW1 and SW2. Which command resolves the issue?

A. SW2(config-if)#switchport mode trunk

B. SW1(config-if)#channel-group 10 mode active

C. SW1(config-if)#channel-group 10 mode desirable

D. SW2(config-if)#channel-group 10 mode on

Correct Answer: *B*

Community vote distribution

B (100%)

CCNPWILL 1 month, 3 weeks ago

B is correct. LACP active on both sides all 4 ports.

upvoted 1 times

nushadu 11 months, 3 weeks ago

I cathed this log, it looks "B" is good but i need peer to check it anyway
sw1#show logging | include LACP
*Dec 12 19:14:33.154: %EC-5-L3DONTBNDL2: Et0/0 suspended: LACP currently not enabled on the remote port.
sw1#sh running-config interface port-channel 1
Building configuration...

Current configuration : 66 bytes
!
interface Port-channel1
ip address 10.0.0.2 255.255.255.0
end

sw1#sh running-config int e0/0
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet0/0
description "UPLINK"
no switchport
no ip address
channel-group 1 mode active
end
sw1#

upvoted 1 times

bora4motion 1 year ago

Selected Answer: B

B is correct for LACP.
upvoted 1 times

Dataset 1 year ago
the trunkig protocol is LACP...so the only option are "active" or "passive"
Regards
upvoted 2 times

jackr76 8 months, 2 weeks ago
Active, Passive or On
upvoted 1 times

melkij17 1 year, 2 months ago
LACP protocol - so Active or Passive
upvoted 1 times

shubhambala 1 year, 2 months ago
why not C?
upvoted 3 times

Dataset 1 year ago
Hi, because "desirable" is for use with PAGP (Cisco propietary protocl)
Regards
upvoted 1 times

Symirnian 9 months ago
But if the other switch is understood working in PAGP as here, shouldn't we solve the issue by changing ourself to PAGP? As C does.?
upvoted 3 times

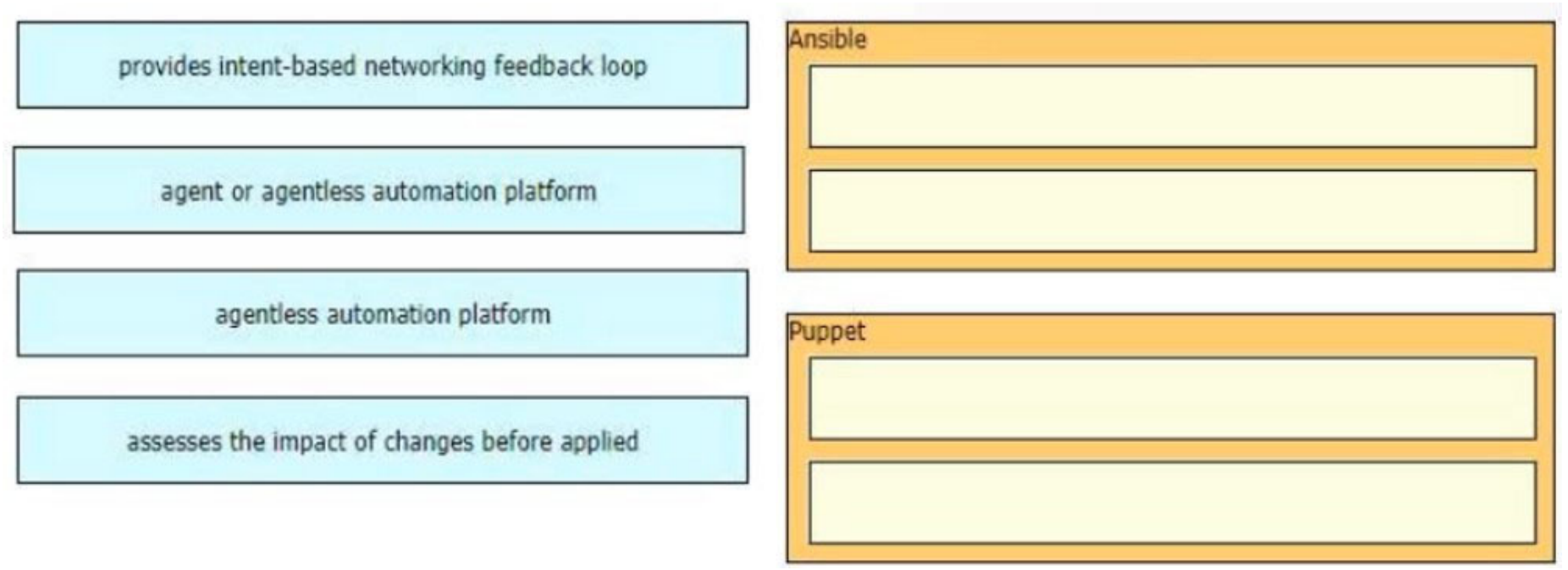
byallmeans 6 months, 4 weeks ago
it's not saying the other end is running PAgP, it's just saying it's not running LACP. Might not be running neither for what we know.
upvoted 2 times

Question #548 *Topic 1*

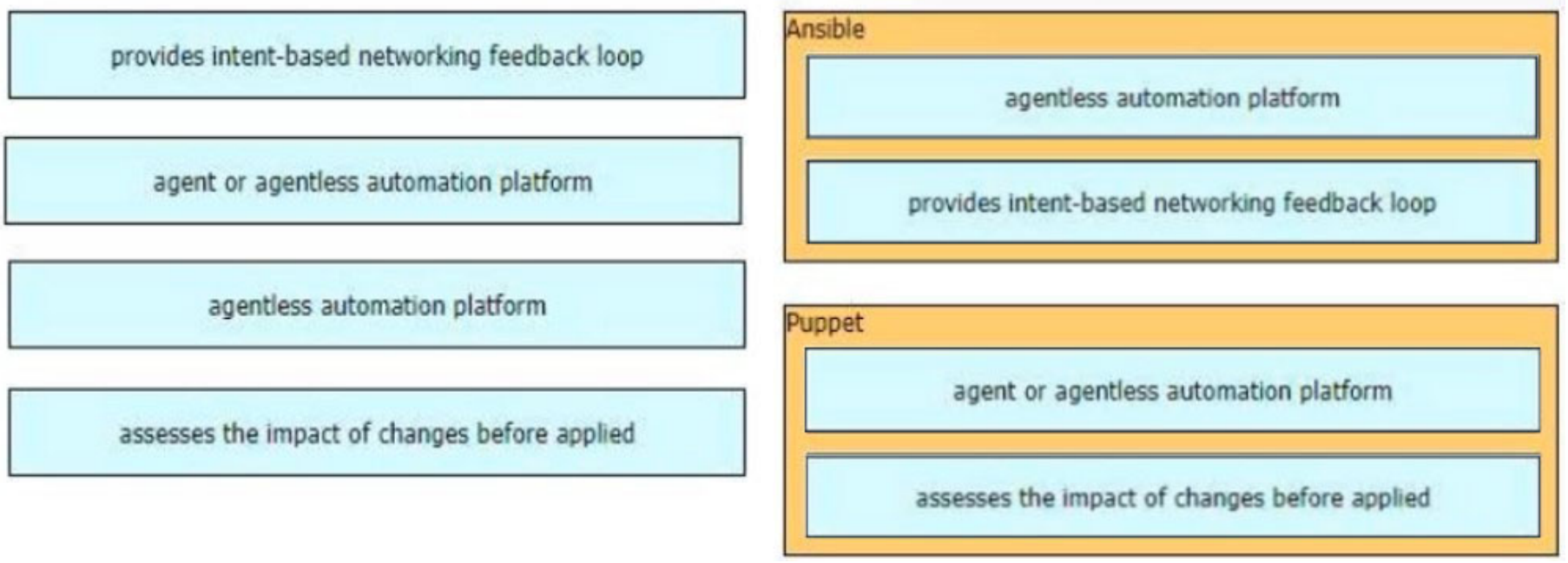
DRAG DROP -

Drag and drop the automation characteristics from the left onto the appropriate tools on the right.

Select and Place:



Correct Answer:



MO_2022 Highly Voted 11 months, 1 week ago

Ansible
+ assesses the impact of changes before applied
+ agentless automation platform

upvoted 15 times

Rose66 10 months, 2 weeks ago

Most Ansible modules check whether the desired final state has already been achieved, and exit without performing any actions if that state has been achieved, so that repeating the task does not change the final state. Modules that behave this way are often called 'idempotent.' Whether you run a playbook once, or multiple times, the outcome should be the same. However, not all playbooks and not all modules behave this way. If you are unsure, test your playbooks in a sandbox environment before running them multiple times in production. (Source: https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_intro.html).... I think you are right

upvoted 4 times

[Removed] Most Recent 3 months, 2 weeks ago

The answer is correct.
https://www.puppet.com/blog/ansible-vs-puppet

Visibility
Ansible Controller (formerly Tower) offers a visual user interface to schedule and run tasks. However, both reporting and historical auditing capabilities are not included, which makes it difficult to preview the impact of new code.

Puppet's interface was built with viewing, managing, and monitoring in mind. Impact Analysis (available in Continuous Delivery for Puppet Enterprise) will parse changes to your existing code, adding additional visibility.

upvoted 1 times

mdawg 9 months, 3 weeks ago

ansible-playbook provides a --check option, which enables Ansible check mode. In this mode, Ansible runs through your playbook and reports what it would do, but makes no actual changes. This allows you to validate your code before applying it for real, providing several benefits including:

allowing you to catch syntax errors in your code
allowing you to validate the changes that Ansible intends to make, to ensure they match your expectations
Additionally, you can also pass --diff. With this option, for each task that Ansible detects changes will be necessary, Ansible will output the difference between the current state and the changes it intends to make.

https://www.clockworknet.com/blog/2020/06/05/mastering-ansible-check-mode/

upvoted 2 times

snarkymark 9 months, 4 weeks ago

I believe answer is correct. This explains features of puppet.
https://www.globenewswire.com/news-release/2019/05/02/1815333/0/en/Puppet-s-Latest-Release-Offers-Organizations-a-One-Stop-Shop-for-Infrastructure-Automation.html

upvoted 2 times

HungarianDish 10 months, 2 weeks ago

Intent-based feedback loops seem to be more appropriate with Puppet:
Feedback loops must be maintained to ensure that any issues picked up along the stream are reported back to the right area for remediation.
Configuration management tools, including Puppet, support some of these critical tasks.

https://www.techtarget.com/searchitoperations/tip/What-is-the-Puppet-configuration-management-tool-and-how-does-it-work

upvoted 2 times

AndreasThornus 11 months, 3 weeks ago

I believe the given answer is correct based on this article:
http://jedelman.com/home/intent-based-network-automation-with-ansible/

upvoted 3 times

Question #549 *Topic 1*

How do stratum levels relate to the distance from a time source?

A. Stratum 0 devices are connected directly to an authoritative time source.

B. Stratum 1 devices are connected directly to an authoritative time source.

C. Stratum 15 devices are connected directly to an authoritative time source.

D. Stratum 15 devices are an authoritative time source.

Correct Answer: *B*

Community vote distribution

B (100%)

CCNPWILL 1 month, 3 weeks ago

Yes. Straum 0 IS the authoritative time source. Straum 1 is directly connective to the authoritative source, 0 ... Answer is B. Given answer is correct.

upvoted 1 times

Dataset 10 months ago

Selected Answer: B

correct, stratum 0 is the attomic watch
Regards

upvoted 1 times

Xerath 11 months, 2 weeks ago

Selected Answer: B

Provided answer is correct, because "stratum 0" is the authoritative time source.

upvoted 2 times

Question #550 *Topic 1*

A customer has a wireless network deployed within a multi-tenant building. The network provides client access, location-based services and is monitored using
Cisco DNA Center. The security department wants to locate and track malicious devices based on threat signatures. Which feature is required for this solution?

A. malicious rogue rules on Cisco DNA Center

B. malicious rogue rules on the WLC

C. Cisco aWIPS policies on the WLC

D. Cisco aWIPS policies on Cisco DNA Center

Correct Answer: *B*

Community vote distribution

D (80%) C (20%)

Caledonia Highly Voted 1 year, 2 months ago

The answer is D.

As the aWIPS functionality is integrated into Cisco DNA Center, the aWIPS can configure and monitor WIPS policies and alarms and report threats.

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-1-2/quick-start-guide/b_rogue_management_qsg_2_1_2/b_rogue_management_qsg_1_4_chapter_00.html

upvoted 7 times

Deu_Inder Highly Voted 1 year, 2 months ago

Selected Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-1-2/quick-start-guide/b_rogue_management_qsg_2_1_2/b_rogue_management_qsg_1_4_chapter_00.html

upvoted 5 times

Asombrosso Most Recent 2 months, 4 weeks ago

Selected Answer: D

Cisco Advanced Wireless Intrusion Prevention System (aWIPS) and Rogue Management is a complete wireless security solution that uses the Cisco DNA Center and Cisco Catalyst infrastructure to detect, locate, mitigate, and contain wired and wireless rogues and threats at Layers 1 through 3. Integration of aWIPS into the WLAN infrastructure offers cost and operational efficiencies delivered by using a single infrastructure for both aWIPS and WLAN services.

upvoted 1 times

network_gig 1 year, 1 month ago

Confusing question. aWIPS can be configured on both WLC and DNA Center.

upvoted 1 times

Titini 1 year, 2 months ago

Selected Answer: D

D is the answer

upvoted 2 times

jj970us 1 year, 2 months ago

Selected Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/config-guide/b_wl_17_11_cg/b_wl_17_11_cg_chapter_010001100.html

upvoted 2 times

x3rox 10 months ago

Wrong, The question states: The network provides client access, location-based services and is monitored "using Cisco DNA Center" - So the feature must be related to DNA,

From the shared guide here:
Because the Cisco Adaptive Wireless Intrusion Prevention System (aWIPS) is integrated with Cisco DNA Center, you can monitor the aWIPS signatures within the Rogue and aWIPS dashboard.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-1-2/quick-start-guide/b_rogue_management_qsg_2_1_2/b_rogue_management_qsg_1_4_chapter_00.html#:~:text=Intrusion%20Prevention%20System%20(-,aWIPS,-)%20is%20integrated%20with

upvoted 3 times

Question #551 *Topic 1*

In a Cisco SD-Access wireless environment, which device is responsible for hosting the anycast gateway?

A. fusion router

B. control plane node

C. fabric border node

D. fabric edge node

Correct Answer: *D*

Community vote distribution

D (100%)

Deu_Inder Highly Voted 1 year, 2 months ago

Selected Answer: D

Given answer is correct. See below:
"..... Inter-VLAN traffic is attracted to the edge node because the AnyCast gateway for the end hosts resides there." Here is the link:
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

upvoted 5 times

Vlad_Is_Love_ua Most Recent 9 months, 1 week ago

Inter-VLAN traffic is attracted to the edge node because the AnyCast gateway for the end hosts resides there. When a host connected to extended node sends traffic to destinations in the same VN connected to or through other fabric edge nodes, segmentation and policy is enforced through VLAN to SGT mappings on the fabric edge node.

upvoted 1 times

snarkymark 9 months, 4 weeks ago

Agree with D,
https://www.routeprotocol.com/sd-access-fabric-edge-nodes/

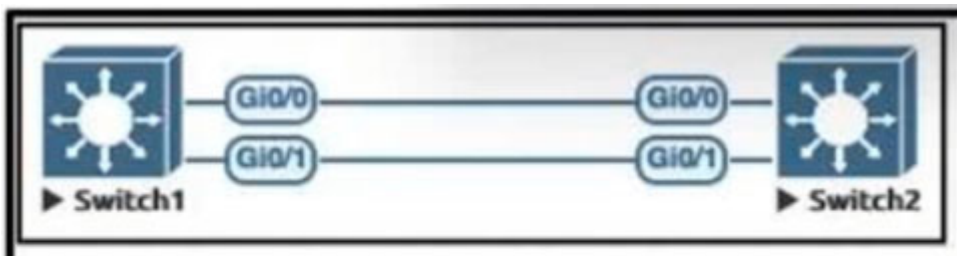
upvoted 2 times

Titini 1 year, 2 months ago

D, agree with Deu

upvoted 2 times

Question #552 *Topic 1*




```
Switch1#show run interface Gi0/0
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
 channel-group 1 mode active
end

Switch1#show run interface Gi0/1
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
 channel-group 1 mode passive
end
```

```
Switch2#show run interface Gi0/0
!
interface GigabitEthernet0/0
 negotiation auto
 channel-group 1 mode active
end

Switch2#show run interface Gi0/1
!
interface GigabitEthernet0/1
 negotiation auto
 channel-group 1 mode passive
end
```

Refer to the exhibit. The port channel between the switches does not work as expected. Which action resolves the issue?

A. Interface Gi0/1 on Switch1 must be configured as desirable.

B. Trunking must be enabled on both interfaces on Switch2.

C. Interface Gi0/0 on Switch2 must be configured as passive.

D. Interface Gi0/1 on Switch2 must be configured as active.

Correct Answer: *D*

Community vote distribution

D (79%) B (21%)

AndreasThornus Highly Voted 11 months, 3 weeks ago

Selected Answer: D

I believe the given answer is correct after running this through a lab.

SW2 in "auto" mode picks up on the fact that it's connections to SW1 are trunks and appears to form trunk based on negotiation as per the output below.

Port Mode Encapsulation Status Native vlan
Po1 auto n-802.1q trunking 1

The port channel does actually come up but with only one member, Gi0/0 on each side. Setting the port channel mode on SW2-Gi0/1 to active (LACP), the port is bundled into the port channel and everything works as expected. Therefore, I believe the answer to be D.

upvoted 13 times

Zikosheka Highly Voted 1 year, 1 month ago

Selected Answer: B

Stupid question but I think it's B - when you configure etherChannel, the config has to match on both ends.
another thing to note is that 0/1 is set to passive on both ends and therefore it will not form etherchannel.
As you can see SW-2 is not set to trunk

upvoted 6 times

bendarkel 9 months, 2 weeks ago

Both interfaces on SW2 are running DTP, so with the remote interfaces being hardcoded as "Trunks" means DTP still runs in the background and causes SW2 interfaces to negotiate trunking.

upvoted 2 times

CCNPWILL Most Recent 1 month, 3 weeks ago

Selected Answer: D

Both links need to be active for the LACP port channel to become active. B is a good contender... but D is the correct answer.

upvoted 1 times

Haidary 2 months, 2 weeks ago

D is correct
Passive and Passive cant form a trunk

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Labbed in CML

D is the answer.

SW2(config)#int g0/1
SW2(config-if)#channel-group 1 mode passive
SW2(config-if)#do show etherchan sum

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+---
1 Po1(SU) LACP Gi0/0(P) Gi0/1(w)

After applying command in D

SW2(config-if)#channel-group 1 mode active
*Sep 12 14:13:08.444: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
SW2(config-if)#do show etherchan sum

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+---
1 Po1(SU) LACP Gi0/0(P) Gi0/1(P)

upvoted 1 times

Asombrosso 2 months, 4 weeks ago

Selected Answer: D

...does not work as expected!

upvoted 1 times

CKL_SG 4 months, 3 weeks ago

Selected Answer: D

Tested in GNS3
D is correct answer

upvoted 2 times

FerroForce 7 months ago

Selected Answer: D

The answer is D

upvoted 1 times

Cooldude89 9 months, 2 weeks ago

Selected Answer: D

Was thinking same along the lines with Andreas in the comments

upvoted 1 times

bendarkel 9 months, 2 weeks ago

Selected Answer: D

D is the correct answer.

upvoted 1 times

Brand 9 months, 3 weeks ago

This is a very stupid scenario and a question out of this stupidity but the very first action to make this awfully configured port-channel work is to set one end of gig 0/1 as active.
upvoted 2 times

Nickplayany 9 months, 4 weeks ago

Selected Answer: D

D... active passive...
upvoted 1 times

markymark874 10 months, 3 weeks ago

Selected Answer: D

D is correct
upvoted 1 times

temphurricane1091 11 months, 2 weeks ago

It is B. A port-channel would form with 1 active member, which we would have here regardless of gi0/1. SW2 is not trunking so a port channel will not form
upvoted 1 times

MO_2022 11 months, 2 weeks ago

Selected Answer: D

D for sure
upvoted 2 times

MO_2022 11 months, 2 weeks ago

D for sure
upvoted 3 times

nushadu 11 months, 3 weeks ago

D for sure, sw1 conf:

interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport mode trunk

interface Ethernet0/1
description to_e0/1_SW2
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
channel-group 2 mode passive
upvoted 2 times

nushadu 11 months, 3 weeks ago

sw2:

sw2#show running-config | section inter
vlan internal allocation policy ascending
interface Port-channel2
switchport
switchport trunk encapsulation dot1q
switchport mode trunk

interface Ethernet0/1
description to_e0/1_SW1
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
channel-group 2 mode active
upvoted 1 times

nushadu 11 months, 3 weeks ago

from sw2 perspective his peer sw1 in Passive mode (SP code in the Flags output):

sw2#show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode

Channel group 2 neighbors

Partner's information:

LACP port Admin Oper Port Port
Port Flags Priority Dev ID Age key Key Number State
Et0/1 SP 32768 aabb.cc00.1000 22s 0x0 0x2 0x2 0x3C
sw2#

upvoted 1 times

nushadu 11 months, 3 weeks ago

sw1
sw1#show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode

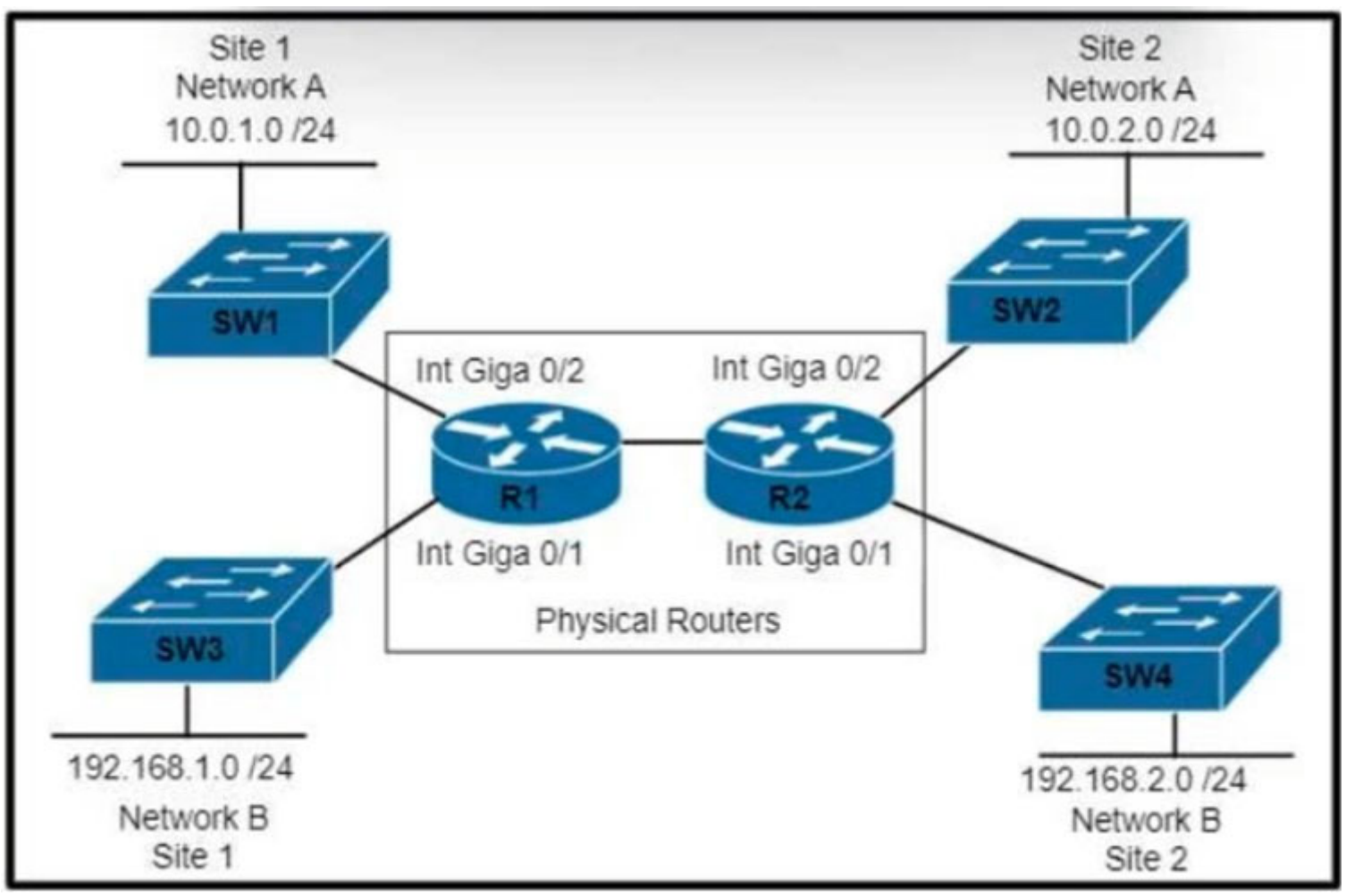
Channel group 2 neighbors

Partner's information:

LACP port Admin Oper Port Port
Port Flags Priority Dev ID Age key Key Number State
Et0/1 SA 32768 aabb.cc00.4000 25s 0x0 0x2 0x2 0x3D
sw1#

upvoted 1 times

Question #553 *Topic 1*



Refer to the exhibit. Which set of commands is required to configure and verify the VRF for Site 1 Network A on router R1?

A. R1#ip routing R1#(config)#ip vrf 100 R1#(config-vrf)#rd 100:1 R1#(config-vrf)# address family ipv4 ! R1(config)#interface Gi0/2 R1(config-if)#ip address 10.0.1.1 255.255.255.0 R1#show ip route

B. R1#ip routing R1#(config)#ip vrf 100 ! R1(config)#interface Gi0/2 R1(config-if)#ip address 10.0.1.1 255.255.255.0 R1#showip route

C. R1#ip routing R1#(config)#ip vrf 100 ! R1(config)#interface Gi0/2 R1(config-if)#ip vrf forwarding 100 R1(config-if)#ip address 10.0.1.1 255.255.255.0 R1#show ip vrf

D. R1#ip routing R1#(config)#ip vrf 100 ! R1(config)#interface Gi0/2 R1(config-if)#ip address 10.0.1.1 255.255.255.0 R1#show ip vrf

Correct Answer: *C*

Community vote distribution

C (100%)

myhdtv6 4 months, 1 week ago

Guys, one trick I learned from VRF Questions and answers and from Labs..
that in VRF we always give IP address after the VRF command, I mean later command of VRF should be IP address.
If you give the IP address before and then give VRF, then IP addresses will get removed.

upvoted 1 times

BobbyFlash 4 months, 4 weeks ago

One of the discarding tricks is the command needed to verify the VRF. I remember that show ip vrf command is the one we need in these cases.

upvoted 1 times

dragonwise 8 months ago

C is correct because it's the only option where they assigned the VRF to an interface

upvoted 2 times

dragonwise 8 months ago

A.
R1#ip routing
R1#(config)#ip vrf 100
R1#(config-vrf)#rd 100:1
R1#(config-vrf)# address family ipv4 !
R1(config)#interface Gi0/2
R1(config-if)#ip address 10.0.1.1 255.255.255.0
R1#show ip route

B.
R1#ip routing
R1#(config)#ip vrf 100 !

R1(config)#interface Gi0/2
R1(config-if)#ip address 10.0.1.1 255.255.255.0
R1#showip route

C.
R1#ip routing
R1#(config)#ip vrf 100 !
R1(config)#interface Gi0/2
R1(config-if)#ip vrf forwarding 100
R1(config-if)#ip address 10.0.1.1 255.255.255.0
R1#show ip vrf

D.
R1#ip routing
R1#(config)#ip vrf 100 !
R1(config)#interface Gi0/2
R1(config-if)#ip address 10.0.1.1 255.255.255.0
R1#show ip vrf

upvoted 2 times

nushadu 11 months, 1 week ago

Selected Answer: C

cisco_R3#show ip vrf
Name Default RD Interfaces
RED 1:1
cust_1 11:11 Et0/0.20
cust_2 22:22 Et0/0.30
cisco_R3#show runn int Et0/0.20
!
interface Ethernet0/0.20
encapsulation dot1Q 20
ip vrf forwarding cust_1
ip address 192.168.1.200 255.255.255.0 secondary
ip address 192.168.1.1 255.255.255.0
end

cisco_R3#show runn | s vrf
!
ip vrf cust_1
rd 11:11
import ipv4 unicast map cust_2_to_cust_1

upvoted 2 times

bora4motion 1 year ago

Selected Answer: C

C looks somewhat OK but all options are weird.

upvoted 3 times

Dataset 1 year ago

Selected Answer: C

correct, the only that contains "vrf fowarding"

upvoted 1 times

amadeu 1 year, 1 month ago

Answer is C.

upvoted 1 times

Question #554 *Topic 1*

How does Protocol Independent Multicast function?

A. In sparse mode, it establishes neighbor adjacencies and sends hello messages at 5-second intervals.

B. It uses the multicast routing table to perform the multicast forwarding function.

C. It uses unicast routing information to perform the multicast forwarding function.

D. It uses broadcast routing information to perform the multicast forwarding function.

Correct Answer: *C*

Community vote distribution

C (100%)

HarwinderSekhon 5 months, 2 weeks ago

If you know RPF failure topic, then you know it uses Unicast.

upvoted 1 times

rafaelinho88 9 months, 3 weeks ago

Selected Answer: C

Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers

upvoted 4 times

bendarkel 1 year ago

Selected Answer: C

Given answer is correct. PIM relies on IGP for forward.

upvoted 2 times

iEpsilon 1 year, 1 month ago

Provided answer is correct
https://en.wikipedia.org/wiki/Protocol_Independent_Multicast#:~:text=PIM%20is%20not%20dependent%20on%20a%20specific%20unicast%20routing%20protocol%3B%20it%20can%20make%20use%20of%20any%20unicast%20routing%20protocol%20in%20use%20on%20the%20network.%20PIM%20does%20not%20build%20its%20own%20routing%20tables.%20PIM%20uses%20the%20unicast%20routing%20table%20for%20reverse%2Dpath%20forwarding.

upvoted 3 times

Question #555 *Topic 1*

Which VXLAN component is used to encapsulate and decapsulate Ethernet frames?

A. VNI

B. GRE

C. VTEP

D. EVPN

Correct Answer: *C*

Alberht Highly Voted 1 year, 2 months ago

VTEP (Virtual Tunnel Endpoint) - This is the device that does the encapsulation and de-encapsulation.

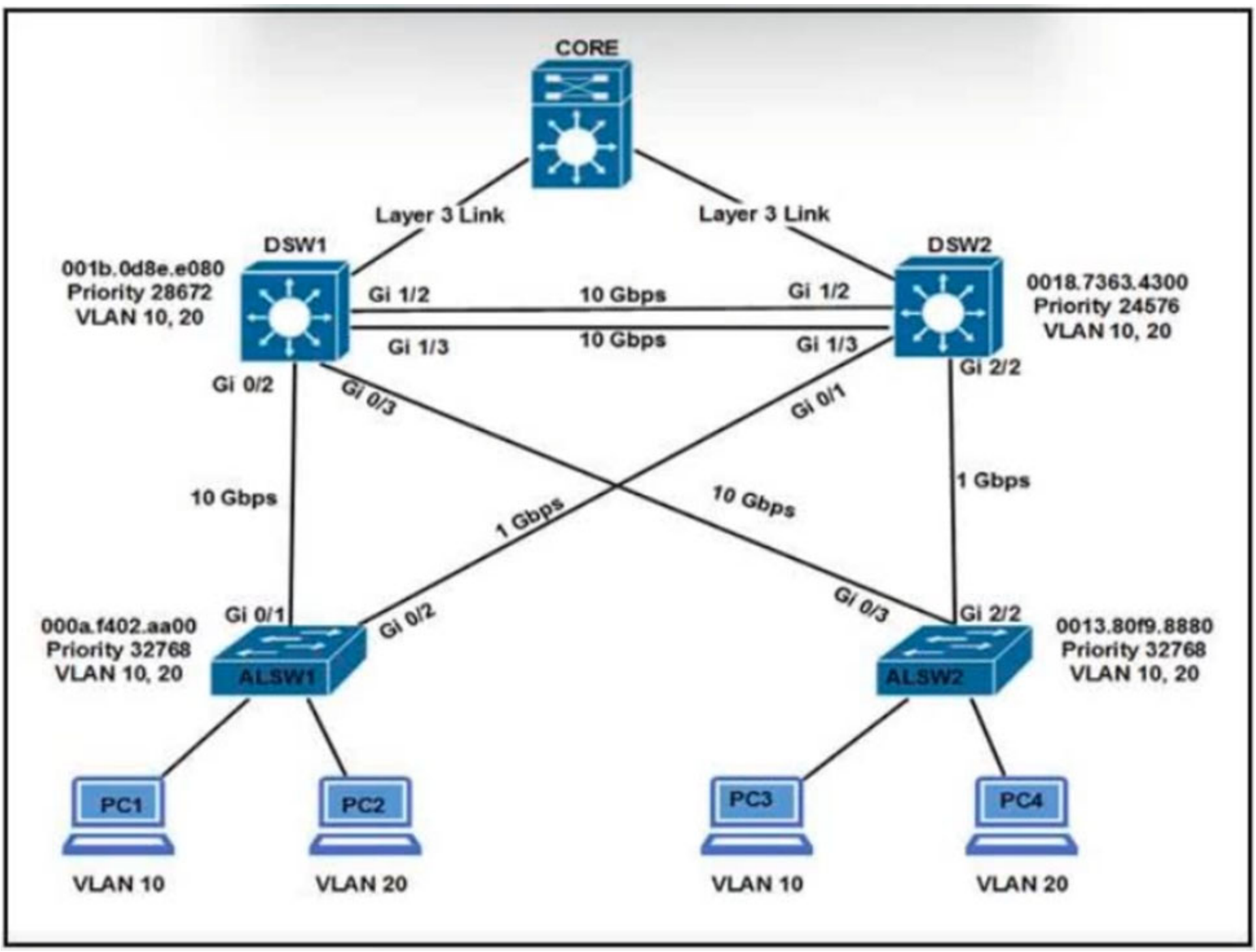
upvoted 5 times

CCNPWILL Most Recent 1 month, 3 weeks ago

Seen this question multiple times in this course.. gotta know this! VTEP ois correct.

upvoted 1 times

Question #556 *Topic 1*



Refer to the exhibit. Assuming all links are functional, which path does PC1 take to reach DSW1?

A. PC1 goes from ALSW1 to DSW2 to CORE to DSW1.

B. PC1 goes from ALSW1 to DSW2 to ALSW2 to DSW1.

C. PC1 goes from ALSW1 to DSW2 to DSW1.

D. PC1 goes from ALSW1 to DSW1.

Correct Answer: *D*

Community vote distribution

C (83%) D (17%)

tckoon Highly Voted 1 year, 1 month ago

Selected Answer: C

Path cost from ALSW1 to root bridge(DSW2) via DSW1 is 2 + 2 = cost of 4. (10gbps+10Gbps)
Path cost from ALSW1 to root bridge(DSW2) is 4 = cost of 4. (1Gbps)
Therefore the patch cost equal and DSW2 is root bridge Therefore it will via Gi0/2.

Answer is C.

IF let say the question change the ALSW1 to DSW2 Gi0/2 interface to 100Mbps (cost=19) , the answer will be different.
ALSW1 to DSW2 will be blocked.
Answer will be D.

upvoted 14 times

chegii Highly Voted 9 months, 3 weeks ago

Selected Answer: C

STP Rule 1—All ports of the root switch must be in forwarding mode.
DSW2 is root because it has lowest priority 24576.
Therefore, ALSW1 will block port Gi0/1
The path will be PC1 to ALSW1 to DSW2 to DSW1

upvoted 8 times

Alondrix 3 weeks, 6 days ago

True, but forwarding ports on the root switch would be misleading if considered alone. Path cost is considered by the downstream switch based on the received BPDU, not at the root.

upvoted 1 times

rami_mma Most Recent 8 months, 1 week ago

Selected Answer: C

"spanning-tree pathcost method long" command is very important to answer this question.

upvoted 1 times

[Removed] 5 months, 1 week ago

Yeah... I got this answer wrong because I assumed otherwise. But we are supposed to know that short method is the default.

SW-1#show spanning-tree pathcost method
Spanning tree default pathcost method used is short

upvoted 1 times

owenshinobi 8 months, 1 week ago

I'm no sure but.
NOTE

The original IEEE specification did not account for links faster than 1 Gbps. Specifically, 1 Gbps links were assigned a port cost of 1, 100 Mbps link a cost of 10, and 10 Mbps links a cost of 100. Any link faster than 1 Gbps (i.e., 10 GE) was automatically assigned the same port cost of 1 Gbps links (i.e., port cost of 1).

refer link: https://www.ciscopress.com/articles/article.asp?p=2832407&seqNum=4#:~:text=The%20default%20port%20cost%20is,a%20port%20cost%20of%20100.

upvoted 1 times

rafaelinho88 9 months, 3 weeks ago

Selected Answer: C

In the topology above, we see DSW2 has lowest priority 24576 so it is the root bridge for VLAN 10 so surely all traffic for this VLAN must go through it. All of DSW2 ports must be in forwarding state. And:
+ The direct link between DSW1 and ALSW1 is blocked by STP.
+ The direct link between DSW1 and ALSW2 is also blocked by STP.
Therefore PC1 must go via this path: PC1 -> ALSW1 -> DSW2 -> DSW1

upvoted 4 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: C

C. is the answer.
But NOT directly because DSW2 is root bridge. It does not matter, if ALSW1 is directly connected to the root bridge or not. The best path to the root is choosen and this has nothing to do with direct connection.

When a switch has several ways to the root bridge, the port is chosen based on
- The cost of the port (in this case both times 4, so it is equal)
- port priority (also equal, as no info given)
- switch ID (MAC)

Because DSW2 has a lower MAC, the path via Gi0/2 is chosen.

upvoted 4 times

Leoveil 6 months, 2 weeks ago

well explained , well done

upvoted 1 times

kewokil120 11 months, 1 week ago

Selected Answer: C

not sure why people are putting D due to Root Bridge Priority.

upvoted 2 times

StefanOT2 10 months, 2 weeks ago

Because the Path to the Root Bridge and Root Bridge Priority are 2 different things.

upvoted 1 times

nushadu 11 months, 1 week ago

Selected Answer: C

ALSW1 to DSW2 [ROOT] to DSW1

upvoted 1 times

nushadu 11 months, 3 weeks ago

C. this question about root priority, lower priority is root switch stp:

sw2#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee
Root ID Priority 32769
Address aabb.cc00.1000
Cost 100
Port 65 (Port-channel2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address aabb.cc00.4000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 100 128.1 Shr
Et0/2 Desg FWD 100 128.3 Shr
Et0/3 Desg FWD 100 128.4 Shr
Po2 Root FWD 100 128.65 Shr
sw2#

upvoted 1 times

nushadu 11 months, 3 weeks ago

priority has been changed:
sw2(config)#spanning-tree vlan 1 priority 24000
% Bridge Priority must be in increments of 4096.
% Allowed values are:
0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440
sw2(config)#spanning-tree vlan 1 priority 24576

upvoted 1 times

nushadu 11 months, 3 weeks ago

now it is root for vlan1

sw2(config)#do s spann

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 24577
Address aabb.cc00.4000
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24577 (priority 24576 sys-id-ext 1)
Address aabb.cc00.4000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 100 128.1 Shr
Et0/2 Desg FWD 100 128.3 Shr
Et0/3 Desg FWD 100 128.4 Shr
Po2 Desg FWD 100 128.65 Shr

sw2(config)#^Z
sw2#sh

upvoted 1 times

nushadu 11 months, 4 weeks ago

Selected Answer: C

DSW2 is root stp switch (it has low priority), so all traffic goes over it

upvoted 1 times

bora4motion 1 year ago

Selected Answer: C

I'm going with C.

upvoted 1 times

onkel_andi 1 year, 1 month ago

Selected Answer: C

Packets always goes to the root bridge first.

upvoted 1 times

yousif387 1 year ago

not mandatory, if the port is in FWD state it will check the MAC address based on that it will FWD the frame

upvoted 2 times

ivokol 1 year, 1 month ago

Selected Answer: C

PC1-ALSW1-DSW2-DSW1

upvoted 1 times

VergilP 1 year, 2 months ago

Selected Answer: C

I'm going for C

In the topology above, we see DSW2 has lowest priority 24576 so it is the root bridge for VLAN 10 so surely all traffic for this VLAN must go through it. All of DSW2 ports must be in forwarding state. And:

+ The direct link between DSW1 and ALSW1 is blocked by STP.
+ The direct link between DSW1 and ALSW2 is also blocked by STP.

Therefore PC1 must go via this path: PC1 -> ALSW1 -> DSW2 -> DSW1.

upvoted 2 times

Joseph123 1 year, 2 months ago

Selected Answer: D

Saw this question on the real exam

upvoted 3 times

Deu_Inder 1 year, 2 months ago

And Gi0/2 on ALSW1 will be blocked.

upvoted 2 times

Deu_Inder 1 year, 2 months ago

Selected Answer: D

DSW2 is the root bridge. ALSW1 has two paths to DSW2: a direct path and via DSW1. ALSW1 needs to decide which path has less cost.
Both the paths have the same cost. Direct path has a cost of 4 since the link is 1GB. The path thru DSW1 has the cost 2 + 2 = 4 as the cost of a 10GB link is 2. So, path costs are equal. Now, my understanding would be: since the port Gi0/1 is smaller than Gi0/2, Gi0/1 will be chosen as root port. And thus the path to root bridge for ALSW1 will be thru DSW1.

upvoted 5 times

onkel_andi 1 year, 1 month ago

The Packet goes always to the root bridge first

upvoted 2 times

rogi2023 4 months, 4 weeks ago

Yes, but following the principle: 1-lowest Roothpath cost; IF equal than 2-lowest Sender BID, If that is equal; 3-lower received portID in BPDU. HTH

upvoted 1 times

Summo 1 year, 1 month ago

we have two equal cost paths, tie breaking rules in this scenario. Here they are,

1. Lowest Sending Bridge ID
2. Lowest Port Priority (of sender)
3. Lowest Interface number (of sender)

upvoted 6 times

Question #557 *Topic 1*

By default, which virtual MAC address does HSRP group 22 use?

A. c0:41:99:98:06:16

B. 00:00:0c:07:ac:16

C. 00:00:0c:07:ac:22

D. c0:07:0c:ac:00:22

Correct Answer: *B*

Community vote distribution

B (81%) C (19%)

mellohello Highly Voted 9 months, 1 week ago

Selected Answer: B

22 in binary = 0001 0110
0001 = 1
0110 = 6
put both numbers together -> 16

upvoted 8 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago

22 = 00010110 = 0001|0110 = 1|6 = 16

upvoted 1 times

jrquissak 2 months, 3 weeks ago

Selected Answer: B

B
22 in HEX = 16

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

how do you calculate decimal to hex in exam?

upvoted 1 times

connorm 3 months ago

Think Binary for HSRP - split the last octet into two:
.128 .64 .32 .16 | .8 .4 .2 .1
0 0 0 1 0 1 1 0
Now make the number 16 out of Binary starting from the right to left^
Add the 2 numbers together from each slice of the octet you get 16

upvoted 1 times

nushadu 11 months, 4 weeks ago

Selected Answer: B

hex 16 == (16x1) + 6 == 22

upvoted 2 times

Caradum 1 year ago

Selected Answer: B

100% B, as many explained before.
The MAC address is in HEX. This question was asked in this specific way to lure you in the trap.

upvoted 1 times

Cer_Pit 1 year ago

Selected Answer: B

B is correct.
22 is 16 in HEX (0001 0110)

upvoted 1 times

Amoako 1 year, 1 month ago

Answer is B as MAC address is in HEX and 22 in HEX is 16

upvoted 1 times

Lapegues 1 year, 1 month ago

HSRP v1 uses the virtual MAC address of 0000.0c07.acxx where xx represent the group number. when replacing the 2 last digits xx with 22 we getting: 00.00.0c.07.ac.22. That's means "C" is the correct answer.

upvoted 1 times

dougj 1 year, 1 month ago

The number is in HEX not decimal. 22 = (2 x 16) + (2 x 1) = 34. Answer is B (1x16)+(6x1)=22

upvoted 1 times

diamant 1 year ago

Conver hex to des
https://www.rapidtables.com/convert/number/hex-to-decimal.html
$(16)_{16} = (1 \times 16^1) + (6 \times 16^0) = (22)_{10}$

upvoted 2 times

onkel_andi 1 year, 1 month ago

Selected Answer: B

The last 2 digits are the group in HEX. So Group 22 in HEX is 16.

upvoted 4 times

iEpsilon 1 year, 1 month ago

Selected Answer: C

The last 2 digits in the mac address represent the group number so "C" is the correct answer

upvoted 2 times

onkel_andi 1 year, 1 month ago

So 22 in Hex is 22 ?

upvoted 3 times

shubhambala 1 year, 2 months ago

Selected Answer: C

C should be the ans

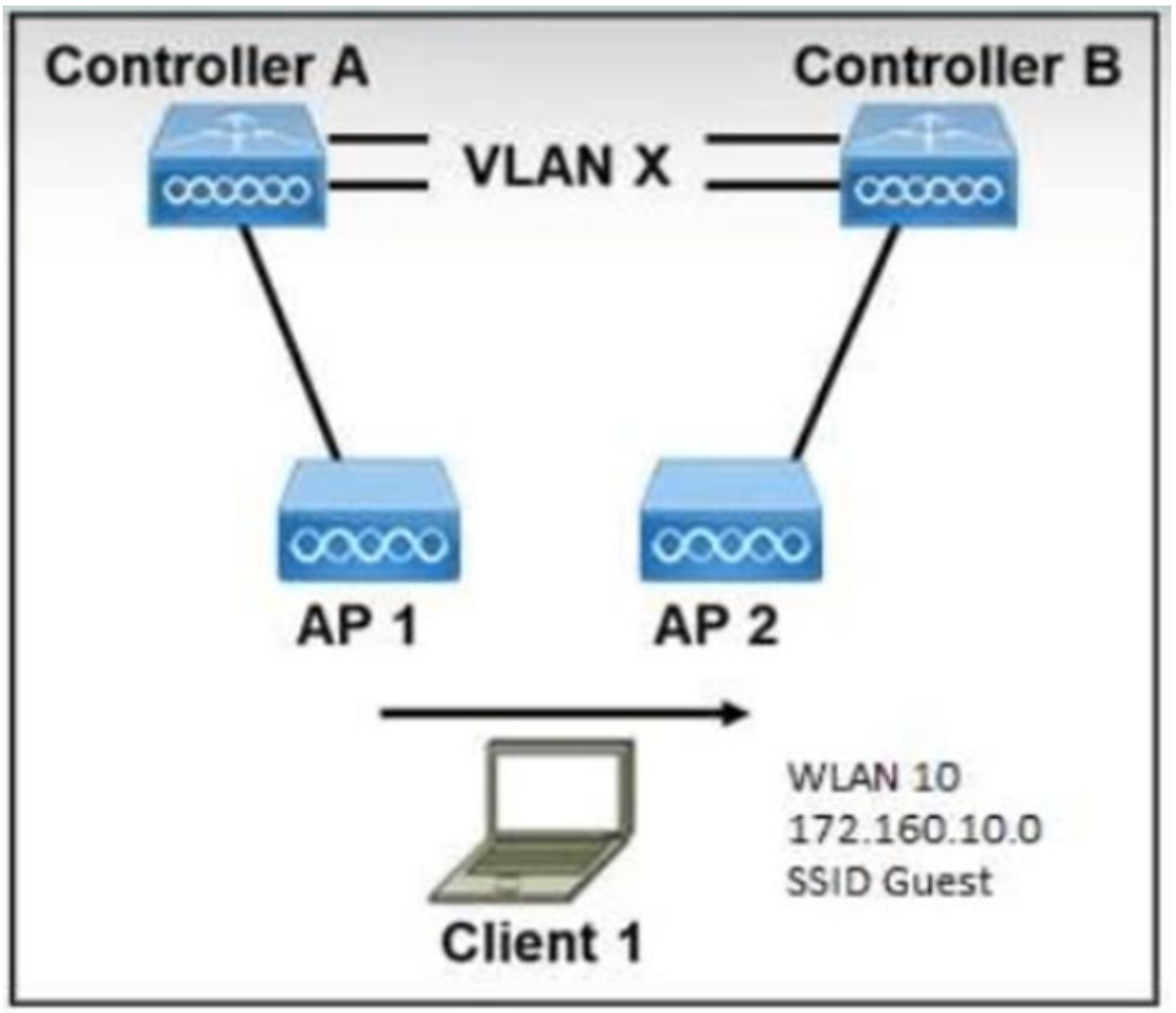
upvoted 2 times

Joseph123 1 year, 1 month ago

Nope :)

upvoted 2 times

Question #558 *Topic 1*



Refer to the exhibit. Both controllers are in the same mobility group. Which result occurs when client 1 roams between APs that are registered to different controllers in the same WLAN?

A. The client database entry moves from controller A to controller B

B. A CAPWAP tunnel is created between controller A and controller B

C. Client 1 uses an EoIP tunnel to contact controller A

D. Client 1 contacts controller B by using an EoIP tunnel

Correct Answer: *A*

Community vote distribution

A (100%)

rafaelinho88 9 months, 3 weeks ago

Selected Answer: A

This is called Inter Controller-L2 Roaming. Inter-Controller (normally layer 2) roaming occurs when a client roam between two APs registered to two different controllers, where each controller has an interface in the client subnet. In this instance, controllers exchange mobility control messages (over UDP port 16666) and the client database entry is moved from the original controller to the new controller.

upvoted 3 times

snarkymark 9 months, 4 weeks ago

A is correct,
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_010011010.pdf

upvoted 2 times

Bigbongos 10 months ago

B. A CAPWAP tunnel is created between controller A and controller B.

When a client roams between access points that are registered to different controllers in the same WLAN, a CAPWAP (Control And Provisioning of Wireless Access Points) tunnel is established between the controllers to allow for seamless roaming. This allows the client to maintain its connection without interruption as it moves between APs, and allows the controllers to keep track of the client's location and status in the network.

upvoted 2 times

Cer_Pit 1 year ago

Selected Answer: A

A is correct, if this is Intercontroller Layer 2 Roaming (the client database entry is moved to the new controller).
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/overview.html

upvoted 2 times

Question #559 *Topic 1*

Where in Cisco DNA Center is documentation of each API call organized by its functional area?

A. Developer Toolkit

B. platform management

C. platform bundles

D. Runtime Dashboard

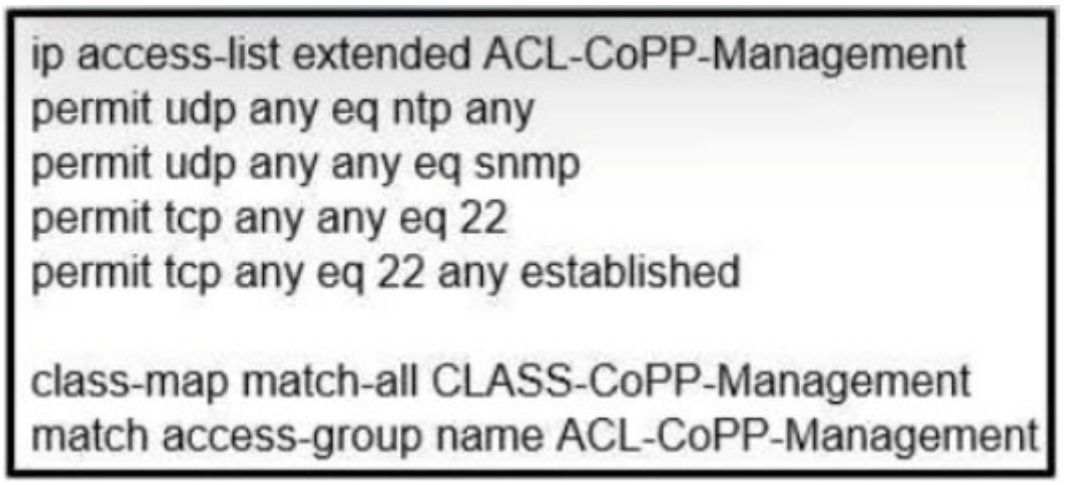
Correct Answer: *A*

kebkim Highly Voted 1 year, 2 months ago

A.
The Developer Toolkit provides documentation about each API call, organized according to functional areas of the Intent API in Cisco DNA center.

upvoted 7 times

Question #560 *Topic 1*



Refer to the exhibit. An engineer must protect the CPU of the router from high rates of NTP, SNMP, and SSH traffic. Which two configurations must be applied to drop these types of traffic when it continuously exceeds 320 kbps? (Choose two.)

A. R1(config-pmap)#class CLASS-CoPP-Management R1(config-pmap-c)#police 32 conform-action transmit exceed-action drop violate-action transmit

B. R1(config)#policy-map POLICY-CoPP R1(config-pmap)#class CLASS-CoPP-Management R1(config-pmap-c)#police 320000 conform-action transmit exceed-action drop violate-action drop

C. R1(config)#policy-map POLICY-CoPP R1(config-pmap)#class CLASS-CoPP-Management R1(config-pmap-c)#police 320000 conform-action transmit exceed-action transmit violate-action drop

D. R1(config)#control-plane R1(config-cp)# service-policy output POLICY-CoPP

E. R1(config)#control-plane R1(config-cp)# service-policy input POLICY-CoPP

Correct Answer: *BE*

Community vote distribution

CE (83%) BE (17%)

HungarianDish Highly Voted 10 months, 2 weeks ago

Selected Answer: CE

https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/cpp.html
exceed-action action: Specifies the action to take on packets that exceed the rate limit
violate-action action: Specifies the action to take on packets that continuously exceed the police rate limit.
"continuously exceeds" -> Hence, option C,E.

upvoted 11 times

net_eng10021 6 months ago

Excellent post.

upvoted 1 times

Haidary Most Recent 2 months, 2 weeks ago

BE
Should be the correct answers

upvoted 1 times

dragonwise 8 months ago

A.
R1(config-pmap)#class CLASS-CoPP-Management
R1(config-pmap-c)#police 32 conform-action transmit exceed-action drop violate-action transmit

B.
R1(config)#policy-map POLICY-CoPP
R1(config-pmap)#class CLASS-CoPP-Management
R1(config-pmap-c)#police 320000 conform-action transmit exceed-action drop violate-action drop

C.
R1(config)#policy-map POLICY-CoPP
R1(config-pmap)#class CLASS-CoPP-Management
R1(config-pmap-c)#police 320000 conform-action transmit exceed-action transmit violate-action drop

D.
R1(config)#control-plane
R1(config-cp)# service-policy output POLICY-CoPP

E.

R1(config)#control-plane
R1(config-cp)# service-policy input POLICY-CoPP
upvoted 4 times

rami_mma 8 months, 1 week ago

Selected Answer: CE

consider "when it continuously exceeds", the word continuously mean there could be some extra buffer, but the extra buffer is limited.
upvoted 2 times

Rose66 10 months, 2 weeks ago

Selected Answer: BE

With B.:
When the traffic rate is below 320 Kbps the conform-action is to transmit the packet, when it exceeds 128 Kbps we will drop the packet.

violate-action specifies the action to take on packets that violate the normal and maximum burst sizes (default normal burst size is 1500 bytes; maximum burst size in bytes depends on the platform) >> in our case drop for B and C. >>> It's not asking for bursts it's asking for continious....
upvoted 2 times

nushadu 11 months, 3 weeks ago

not sure but CE my choise;
cisco(config-pmap-c)#police 320000 conform-action transmit exceed-action tra
cisco(config-pmap-c)#$00 conform-action transmit exceed-action transmit ?
violate-action action when rate is greater than conform + exceed burst
<cr>
cisco(config-pmap-c)#$00 conform-action transmit exceed-action transmit v
cisco(config-pmap-c)#$-action transmit exceed-action transmit violate-action ?
drop drop packet
upvoted 1 times

iEpsilon 1 year ago

Selected Answer: CE

I'll go with C and E because the question mentions "continuously". so we have to configure MQOS in such a way that it can transmit spikes in these traffic here and there but not always.. feel free to correct me if I am wrong.
upvoted 1 times

Huntkey 1 year ago

Selected Answer: CE

"continuously" would imply that occasionally exceeding 320kbps is ok. "exceed drop" will not allow it to ever go above it.
upvoted 2 times

testcom680 1 year ago

Selected Answer: BE

going with B since no PIR rates are mentioned in any of the answers also.
upvoted 2 times

Youssefmetry 12 months ago

Nothing mentioned about marking down the exceeding allowed traffic either
upvoted 2 times

Deu_Inder 1 year, 2 months ago

Not sure if the answer is BE or CE. The phrase in the question to watch for is: "continuously exceed". Does the phrase mean violate?
upvoted 2 times

bendarkel 9 months, 2 weeks ago

Continuously exceeding leads to violation. The answer is CE.
upvoted 1 times

jj970us 1 year, 2 months ago

Selected Answer: CE

Reference: https://www.ccexpert.us/qos-implementing/dual-token-bucket-single-rate-classbased-policing-cont.html
upvoted 3 times

Alberht 1 year, 2 months ago

The question only refers to a conform CIR of 320Kbps, no PIR is mentioned so are you just assuming this is a dual bucket?
upvoted 2 times

Question #561 *Topic 1*

Which free application has the ability to make REST calls against Cisco DNA Center?

A. API Explorer

B. REST Explorer

C. Postman

D. Mozilla

Correct Answer: *C*
Reference:
https://developer.cisco.com/docs/dna-center/#!getting-started

kebkim Highly Voted 1 year, 2 months ago
Postman (a freely available application) is to make REST calls against a Cisco DNA Center appliance.
upvoted 6 times

CCNPWILL Most Recent 1 month, 3 weeks ago
Agreed. I have this tool personally and I did not pay a single penny for it. Postman is the correct answer.
upvoted 1 times

Question #562 *Topic 1*

If AP power level is increased from 25 mW to 100 mW, what is the power difference in dBm?

A. 6 dBm

B. 14 dBm

C. 17 dBm

D. 20 dBm

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/23231-powervalues-23231.html

Community vote distribution

A (100%)

FrameRelay Highly Voted 1 year, 1 month ago

Selected Answer: A

or the easiest calculation is using the laws of 3s covered in the book. A value of 3dB means that the power value of interest is double the reference value.

upvoted 8 times

H3kerman 1 year ago

explanation: 25x2=50 that's 3db gain 50x2=100, that's another 3db. 3+3=6db

upvoted 12 times

kebkim Highly Voted 1 year, 2 months ago

10*log(100) - 10*log(25) = 20dbm - 14dbm = 6dbm

upvoted 6 times

Nova911 5 months, 2 weeks ago

Yes, t think so

upvoted 1 times

Feliphus 11 months, 3 weeks ago

then, 6 db

upvoted 1 times

Nova911 Most Recent 5 months, 2 weeks ago

Selected Answer: A

100 mW = 20 dBm
25 mW = 14 dBm
= 20 dBm - 14 dBm = 6 dBm

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/23231-powervalues-23231.html

upvoted 1 times

AhcMez 8 months, 4 weeks ago

Selected Answer: A

6 dbm
Power Change dB Value
= 0 dB
× 2 +3 dB
/ 2 −3 dB
× 10 +10 dB
/ 10 −10 dB

upvoted 1 times

Bigbongos 10 months ago

C. 17 dBm

The power level of an AP can be measured in watts (W) or milliwatts (mW). To convert from mW to dBm, you can use the formula: dBm = 10 * log10 (mW).

If we increase the AP power level from 25 mW to 100 mW, we can calculate the power difference in dBm as follows:
100mW = 0.1W
100mW = 10 * log10 (0.1W) = 10 * (-1) = -10 dBm
25mW = 0.025W

25mW = 10 * log10 (0.025W) = 10 * (-2.602) = -26.02 dBm

Power difference = -10 dBm - (-26.02 dBm) = -10 dBm + 26.02 dBm = 16.02 dBm or approximately 17dBm

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

You did all this math and you were wrong. im not sure where you failed..

10x100log is 20
10x25log is 14
subtract that and you have 6dBm

upvoted 1 times

Question #563 *Topic 1*

What is the result when an active route processor fails in a design that combines NSF with SSO?

A. The standby route processor temporarily forwards packets until route convergence is complete.

B. An NSF-aware device immediately updates the standby route processor RIB without churning the network.

C. An NSF-capable device immediately updates the standby route processor RIB without churning the network.

D. The standby route processor immediately takes control and forwards packets along known routes

Correct Answer: *D*

Reference:

https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/stck_mgr_ha/b_166_nsf_sso_9400_cg.html

Community vote distribution

D (100%)

snarkymark 9 months, 4 weeks ago

Perhaps it the word temporary in answer A that is the issue.

upvoted 1 times

snarkymark 9 months, 4 weeks ago

To me, both A and D can be correct.
So, it is immediate, but there is convergence going on too.
Cisco NSF with SSO allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover.

NSF works with SSO to minimize the amount of time that a Layer 3 network is unavailable following an active device election by continuing to forward IP packets. Reconvergence of Layer 3 routing protocols (BGP, OSPFv2, and EIGRP) is transparent to the user and happens automatically in the background. Routing protocols recover routing information from neighbor devices and rebuild the Cisco Express Forwarding table.

upvoted 2 times

MJane 11 months ago

Selected Answer: D

D
Cisco Nonstop Forwarding does not maintain a continuously active control plane during switchover.
Instead, the forwarding plane uses known routes while the routing protocol information is being restored after switchover

https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd801dc5e2.html

upvoted 4 times

Darude 1 year ago

Selected Answer: D

answer is correct
reference:
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_01100110.pdf

upvoted 2 times

```
<rpc-reply> [0, 1] required
  <ok> [0, 1] required
  <data> [0, 1] required
  <rpc-error> [0, 1] required
    <error-type>[0, 1] required
    <error-tag> [0, 1] required
    <error-severity> [0, 1] required
    <error-app-tag> [0, 1] required
    <error-path> [0, 1] required
    <error-message> [0, 1] required
    <error-info> [0, 1] required
      <bad-attribute> [0, 1] required
      <bad-element> [0, 1] required
      <ok-element> [0, 1] required
      <err-element> [0, 1] required
      <noop-element> [0, 1] required
      <bad-namespace> [0, 1] required
      <session-id> [0, 1] required
```

Refer to the exhibit. Which command is required to verify NETCONF capability reply messages?

A. show netconf rpc-reply

B. show netconf | section rpc-reply

C. show netconf schema | section rpc-reply

D. show netconf xml rpc-reply

Correct Answer: *C*

Community vote distribution

C (100%)

nushadu Highly Voted 11 months, 3 weeks ago

C.

```
cisco#show netconf schema | section rpc-reply
<rpc-reply> [0, 1] required
<ok> [0, 1] required
<data> [0, 1] required
<rpc-error> [0, 1] required
<error-type> [0, 1] required
<error-tag> [0, 1] required
<error-severity> [0, 1] required
<error-app-tag> [0, 1] required
<error-path> [0, 1] required
<error-message> [0, 1] required
<error-info> [0, 1] required
<bad-attribute> [0, 1] required
<bad-element> [0, 1] required
<ok-element> [0, 1] required
<err-element> [0, 1] required
<noop-element> [0, 1] required
<bad-namespace> [0, 1] required
<session-id> [0, 1] required

cisco#
```

upvoted 5 times

CCNPWILL 1 month, 3 weeks ago

Excellent and indisputable data.

upvoted 1 times

net_eng10021 Most Recent 6 months ago

Selected Answer: C

router#show netconf ?

counters <omitted>
schema <omitted>
session <omitted>

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Dont you come around here showing us your labbing wizardry and showing us real answers. Around here we just read blogs and theorize from OCG text!!!!

upvoted 2 times

kebkim 1 year, 2 months ago

c.
The output of the show netconf schema command displays the element structure for a NETCONF request and the resulting reply. This schema can be used to construct proper NETCONF requests and parse the resulting replies.

upvoted 1 times

Deu_Inder 1 year, 2 months ago

Selected Answer: C

Given answer is correct.

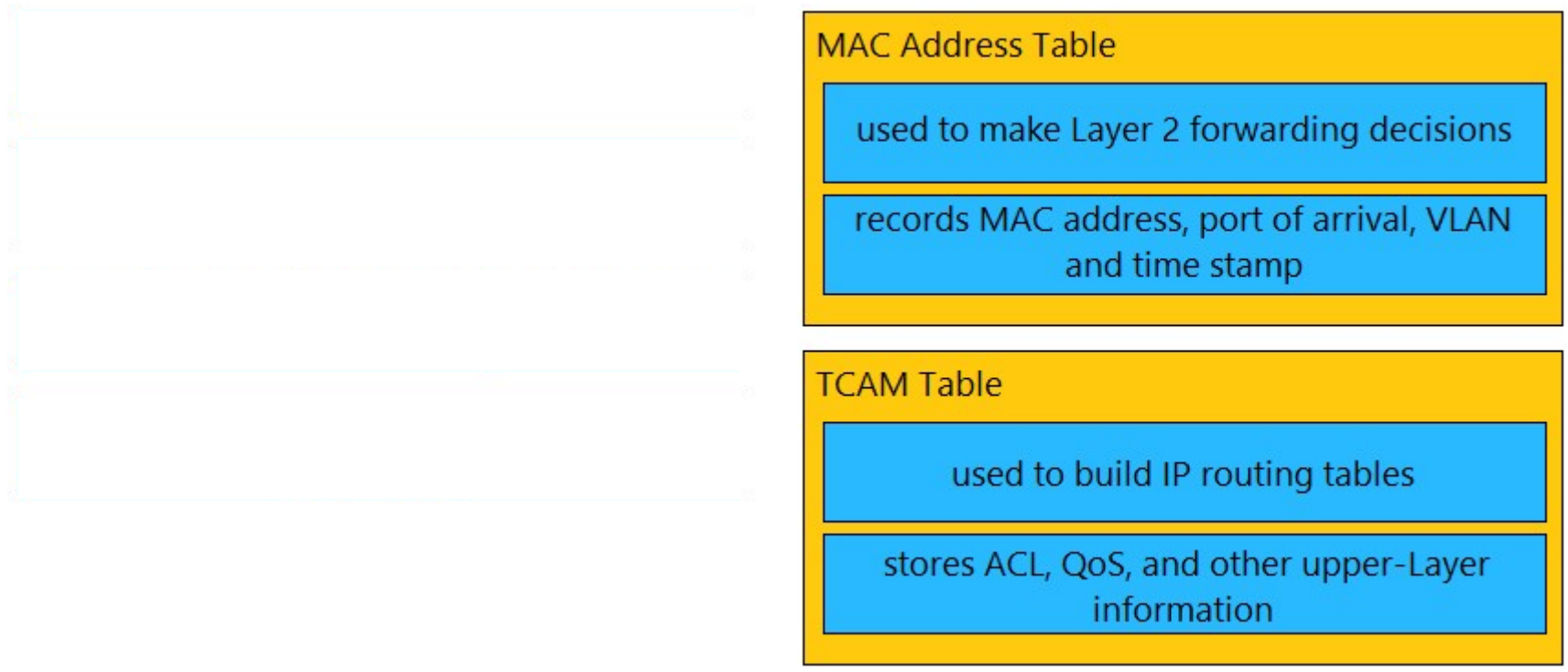
upvoted 1 times

DRAG DROP -

Drag and drop the characteristics from the left to the table types on the right.

Select and Place:

Correct Answer:



StefanOT2 Highly Voted 10 months, 2 weeks ago

The given answer is correct

upvoted 6 times

CCNPWILL Most Recent 1 month, 3 weeks ago

Given answers are right. i co sign on the answer given :D

upvoted 1 times

tempaccount00001 4 months, 3 weeks ago

correct

upvoted 1 times

Dataset 7 months ago

Is correct!

upvoted 1 times

Question #566 *Topic 1*

Which A record type should be configured for access points to resolve the IP address of @ wireless LAN controller using ONS?

A. CISCO.CONTROLLER localdomain

B. CISCO.CAPWAP.CONTROLLER localdomain

C. CISCO-CONTROLLER localdomain

D. CISCO-CAPWAP-CONTROLLER.localdomain

Correct Answer: *D*

Community vote distribution

D (100%)

StefanOT2 Highly Voted 10 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 6 times

samitherider Most Recent 2 months, 4 weeks ago

Answer is correct

upvoted 1 times

drgreen 6 months, 2 weeks ago

obvious typos in the question, should be: a wireless LAN controller using DNS?

upvoted 4 times

mgiuseppe86 2 months, 2 weeks ago

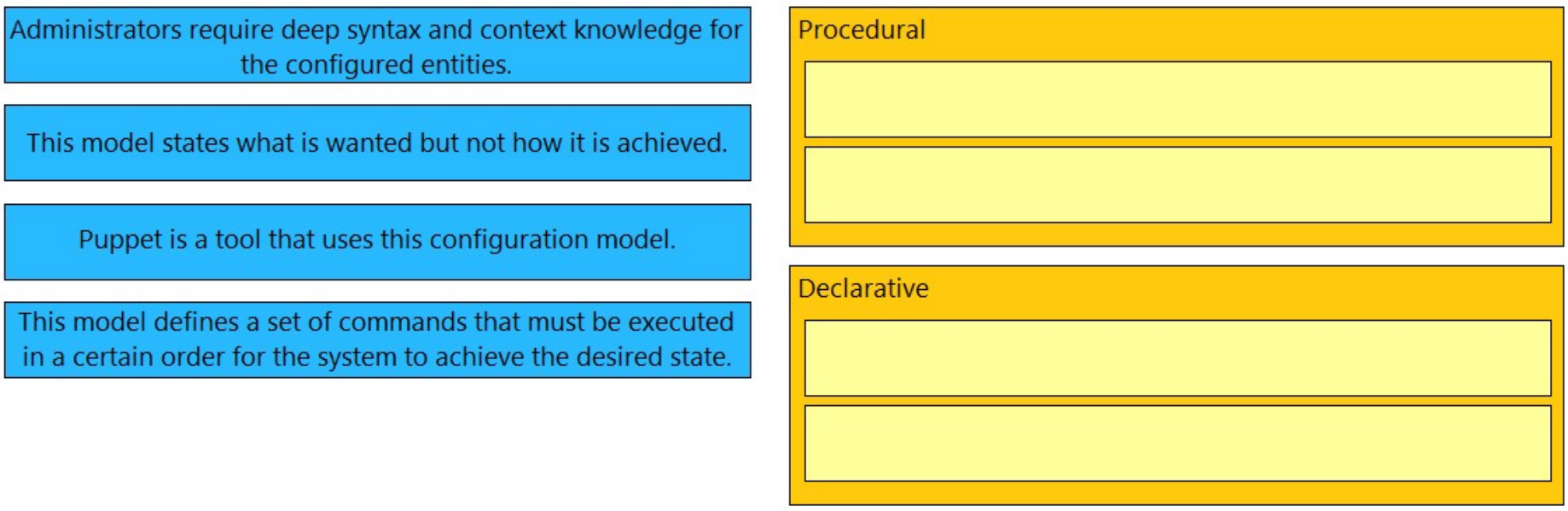
Yes but remember. These questions were ripped from the real exams in countries where test centers allow their students to cheat and usually in these countries, English is not their first language.

upvoted 2 times

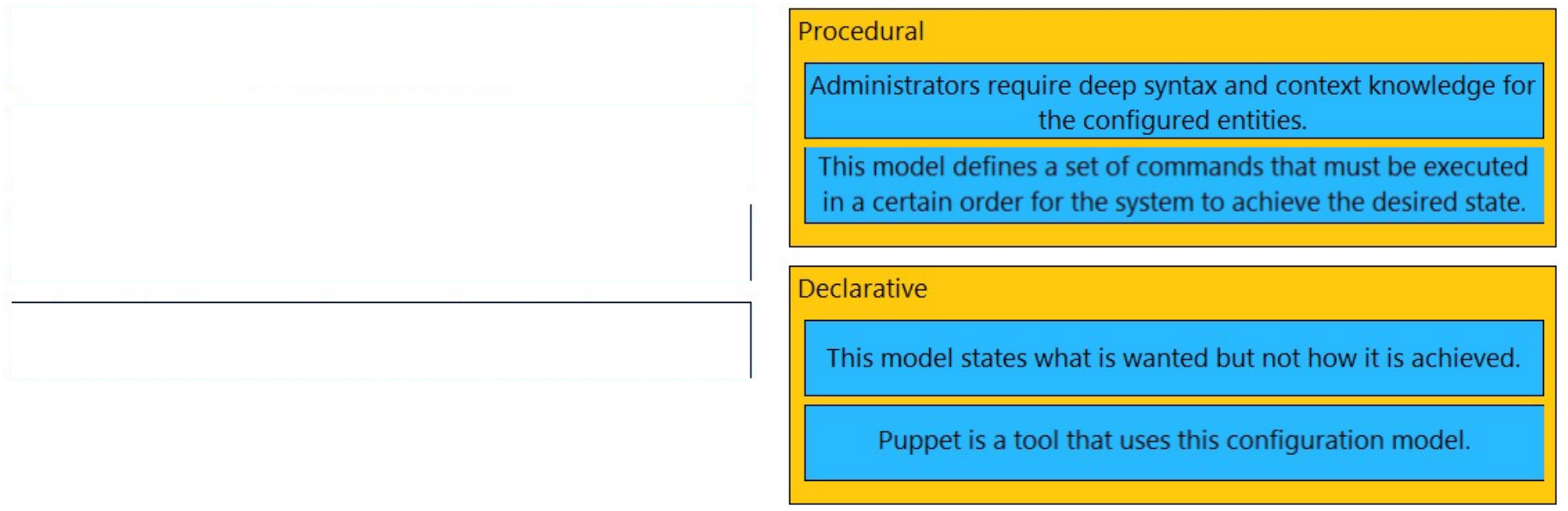
DRAG DROP -

Drag and drop the characteristics from the left onto the configuration models on the right.

Select and Place:



Correct Answer:



mgiuseppe86 2 months, 2 weeks ago

All you need to do is understand English to know Declarative without context assumes you declare what you want

and Precedural means you follow a precedure.....

upvoted 2 times

[Removed] 4 months, 4 weeks ago

Given answer looks correct

upvoted 1 times

net_eng10021 6 months ago

https://www.puppet.com/docs/puppet/7/puppet_language.html

You'll use Puppet's declarative language to describe the desired state of your system.

upvoted 1 times

StefanOT2 10 months, 2 weeks ago

The given answer is correct

upvoted 2 times

Question #568 *Topic 1*

Which activity requires access to Cisco DNA Center CLI?

A. provisioning a wireless LAN controller

B. creating a configuration template

C. upgrading the Cisco DNA Center software

D. graceful shutdown of Cisco DNA Center

Correct Answer: *D*

Community vote distribution

D (100%)

snarkymark 9 months, 2 weeks ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/ha_guide/b_cisco_dna_center_ha_guide_2_1_2.html

upvoted 2 times

Bigbongos 10 months ago

b is correct

upvoted 1 times

CCNPWILL 1 month, 3 weeks ago

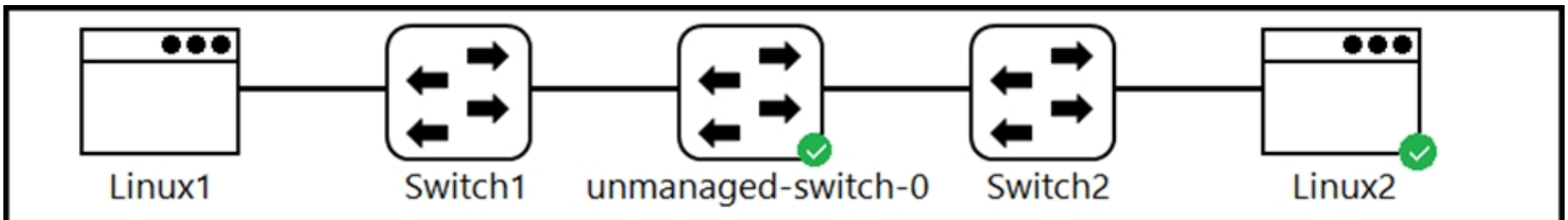
Stop guessing ESPECIALLY without backing your answer with some sort of credenible facts or links. We pay for GOOD information... remember that.

upvoted 1 times

chefexam 9 months, 3 weeks ago

Definitely not, D must be correct. The other options are available in GUI (just Google them)

upvoted 2 times




```
Switch1#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet1           192.168.1.1     YES manual up                    up
GigabitEthernet2           172.16.40.10    YES manual administratively down down
Loopback0                  172.16.10.10    YES manual up                    up

Switch2#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet1           192.168.1.2     YES manual up                    up
GigabitEthernet2           172.16.20.10    YES manual up                    up
Loopback0                  10.10.10.10     YES manual up                    up

Switch1(config)#monitor session 1 type erspan-scurce
Switch1(config-mon-erspan-src)#source interface gigabitethernet1
Switch1(config-mon-erspan-src)#destination
Switch1(config-mon-erspan-src-dst)#erspan-id 110
Switch1(config-mon-erspan-src-dst)#ip address 10.10.10.10
Switch1(config-mon-erspan-src-dst)#origin ip address 172.16.10.10

Switch2(config)#monitor session 1 type erspan-destination
Switch2(config-mon-erspan-dst)#destination interface Gigabitethernet2
Switch2(config-mon-erspan-dst)#source
Switch2(config-mon-erspan-dst-src)#
Switch2(config-men-erspan-dst-src)#ip address 10.10.10.10
```

Refer to the exhibit. An engineer must configure an ERSPAN tunnel that mirrors traffic from Linux1 on Switch1 to Linux2 on Switch2. Which command must be added to the destination configuration to enable the ERSPAN tunnel?

A. (config-mon-erspan-dst-src)# erspan-id 172.16.10.10

B. (config mon erspan-dst-src)# erspan-id 110

C. (config-mon-erspan-dst-src)# no shut

D. (config-mon-erspan-dst-src)# origin ip address 172.16.10.10

Correct Answer: *B*

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xe-3s/lanswitch-xe-3s-book/lnsw-conf-erspan.html

Community vote distribution

B (100%)

bendarkel Highly Voted 1 year ago

Selected Answer: B

Given answer is correct.

upvoted 5 times

[Removed] Most Recent 4 months, 4 weeks ago

Selected Answer: B

The ERSPAN ID is required to match on both the source and destination devices of the ERSPAN tunnel

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

https://youtu.be/RHXbeyYvRp0

upvoted 1 times

nli 6 months, 3 weeks ago

ID needs to be the same

upvoted 1 times

x3rox 10 months ago

I think this question is wrong. The destination address is pointing to sw2 loop back when it's suppose to be the Linux box. Shutdown is not configured either.

upvoted 2 times

sam6996 4 months, 3 weeks ago

origin address is the source of the GRE tunnel used to encapsulate traffic in ERSPAN, and yeah you're right the no shut command needs to be configured to start the monitoring session. see https://networklessons.com/cisco/ccie-routing-switching-written/erspan. So I think your right this question is a little off.

upvoted 1 times

Question #570 *Topic 1*

What are two characteristics of Cisco SD-Access elements? (Choose two.)

A. The border node is required for communication between fabric and nonfabric devices.

B. Traffic within the fabric always goes through the control plane node.

C. Fabric endpoints are connected directly to the border node.

D. The control plane node has the full RLOC-to-EID mapping database.

E. The border node has the full RLOC-to-EID mapping database.

Correct Answer: *AD*

Community vote distribution

AD (100%)

Dataset 10 months ago

Selected Answer: AD

the answer is correct
Regards

upvoted 3 times

HungarianDish 10 months, 1 week ago

Selected Answer: AD

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#Border_Node

The fabric border nodes serve as the gateway between the SD-Access fabric site and the networks external to the fabric.

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#Control_Plane_Node

The control plane node enables the following functions:
Host tracking database — a central repository of Endpoint ID to Routing Locator (EID-to-RLOC) bindings

upvoted 4 times

Question #571 *Topic 1*

When is an external antenna used inside a building?

A. only when using Mobility Express

B. only when using 2.4 GHz

C. when it provides the required coverage

D. only when using 5 GHz

Correct Answer: *C*

AndreasThornus 11 months, 3 weeks ago

Think coverage being required in a warehouse.

upvoted 2 times

mitosenoriko 1 year, 1 month ago

Answer C
not only "A" "B" "C"
also Mobility Express use External Antena.

upvoted 1 times

Question #572 *Topic 1*

```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.2    4        65002       0       0        1    0    0 00:00:15 Idle
R1#show ip interface brief | include 192.168.12
FastEthernet0/0            192.168.12.1    YES NVRAM  up                    up

R2#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 65002
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.1    4        65001       0       0        1    0    0 00:01:00 Idle (Admin)
R2#show ip interface brief | include 192.168.12
Ethernet0/0                192.168.12.2    YES NVRAM  up                    up
R2#ping 192.168.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Refer to the exhibit. R1 and R2 are directly connected, but the BGP session does not establish. Which action must be taken to build an eBGP session?

A. Configure no neighbor 192.168.12.1 shutdown under R2 BGP process.

B. Configure neighbor 2.2.2.2 remote-as 65002 under R1 BGP process.

C. Configure ip route 1.1.1.1 0.0.0.0 192.168.12.1 on R2.

D. Configure neighbor 192.168.12.1 activate under R2 BGP process.

Correct Answer: *A*

Reference:
https://www.noction.com/blog/debug-bgp-states#:~:text=Idle%20(Admin)%20means%20that%20the,!&text=This%20is%20a%20good%20way,BGP%20section%20of%20the%20configuration

Community vote distribution

A (100%)

nushadu 11 months, 3 weeks ago

A. for sure;
cisco(config-router)#
cisco(config-router)#do s bgp summ
BGP router identifier 10.0.0.1, local AS number 777
BGP table version is 1, main routing table version 1

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
77.7.7.7 4 555 0 0 1 0 0 never Idle (Admin)
cisco(config-router)#do s runn | sec bgp
router bgp 777
bgp log-neighbor-changes
neighbor 77.7.7.7 remote-as 555
neighbor 77.7.7.7 shutdown
cisco(config-router)#

upvoted 2 times

nushadu 11 months, 3 weeks ago

cisco(config-router)#
cisco(config-router)#no neighbor 77.7.7.7 shutdown
cisco(config-router)#do s bgp summ
BGP router identifier 10.0.0.1, local AS number 777
BGP table version is 1, main routing table version 1

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd

77.7.7.7 4 555 0 0 1 0 0 never Idle
cisco(config-router)#

upvoted 2 times

bendarkel 1 year ago

Selected Answer: A

Given answer is correct.

upvoted 1 times

Dataset 1 year ago

why not D ?

upvoted 1 times

bendarkel 1 year ago

Because if you look at the show ip bgp summary output on R2, it clearly shows neighbor 192.168.12.1 is admin down. That means under R2 BGP process, neighbor 192.168.12.1 has been shut down.

upvoted 9 times

Dataset 7 months ago

u r right , thanks!
Regards

upvoted 1 times

Question #573 *Topic 1*

A company requires a wireless solution to support its main office and multiple branch locations. All sites have local Internet connections and a link to the main office for corporate connectivity. The branch offices are managed centrally. Which solution should the company choose?

A. Cisco DNA Spaces

B. Cisco Unified Wireless Network

C. Cisco Mobility Express

D. Cisco Catalyst switch with embedded controller

Correct Answer: *A*

Community vote distribution

B (100%)

Jason233 Highly Voted 1 year, 2 months ago

Selected Answer: B

Spaces is for location services etc not a wireless solution.
Centrally managed corp and branch offices gives you a clue

upvoted 8 times

olaniyijt Most Recent 8 months, 4 weeks ago

Admin, answer is B, Please correct it.

upvoted 3 times

snarkymark 9 months, 2 weeks ago

Selected Answer: B

https://www.cisco.com/web/AP/wireless/pdf/overview.pdf

upvoted 2 times

Kasia1992 10 months ago

Selected Answer: B

B is the only option that makes sense

upvoted 2 times

kewokil120 11 months, 1 week ago

Selected Answer: B

The only solution here is B

upvoted 2 times

bora4motion 1 year ago

Selected Answer: B

B with a pair of 5520s or 9800s in SSO.

upvoted 2 times

Dataset 1 year ago

Selected Answer: B

B is corretc

upvoted 2 times

Edwinmolinab 1 year ago

Given answer is correct https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spaces-config/dnaspaces-configuration-guide/m_wireless.html

upvoted 1 times

network_gig 1 year, 1 month ago

Selected Answer: B

The only solution here is B. The rest are part of different solutions.

upvoted 1 times

onkel_andi 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

Question #574 *Topic 1*

Which QoS feature uses the IP Precedence bits in the ToS field of the IP packet header to partition traffic into different priority levels?

A. marking

B. shaping

C. policing

D. classification

Correct Answer: *A*

Community vote distribution

A (64%) D (36%)

msstanick Highly Voted 5 months, 1 week ago

Selected Answer: A

It is tricky and actually stupid (Cisco style I guess...) as classification and marking go together and one is useless without another.

The traffic needs to be classified first so it could ba marked.

The IPP bits are actually used to mark something which is in line with Cisco's Cert Guide official flashcard: "ToS: An 8 bit field where only the first 3 bits, referred to as IP Precedence (IPP), are used for marking, and the rest of the bits are unused."

upvoted 6 times

djedeen Most Recent 3 months, 2 weeks ago

Selected Answer: A

Marker—Set the DSCP field based on the traffic profile.

upvoted 1 times

Colmenarez 4 months ago

Selected Answer: A

The ToS field is an 8-bit field where only the first 3 bits of the ToS field, referred to as
IP Precedence (IPP), ARE USED FOR MARING, and the rest of the bits are unused. IPP values,
which range from 0 to 7, ALLOW THE TRAFFIC TO BE PARTITIONED IN UP TO SIX USABLE CLASSES OF SERVICES; IPP 6 and 7 are reserved for internal network use.

OCG Page 371

upvoted 2 times

Entivo 4 months, 4 weeks ago

Selected Answer: A

Marking is the answer according to Cisco Official Cert Guide page 371 where it shows in Figure 14-3 ToS field containing IP Precedence and DiffServ fields.

upvoted 1 times

HarwinderSekhon 4 months, 4 weeks ago

Selected Answer: A

group traffic - Classification
Identify - Marking
A

upvoted 3 times

Splashisthegreatestmovie 5 months, 2 weeks ago

I think it's D. In the question the action is a discrimination of the already marked packet. This discrimination is the process of classification.

upvoted 2 times

jubrilak 5 months, 2 weeks ago

Correct Answer is A. Marking means that we set the TOS (Type of Service) byte with an IP Precedence value or DSCP value.
https://networklessons.com/quality-of-service/qos-marking-cisco-ios-router

While classification is how we look at the traffic that is running through our router and identify (classify) it so we know to which application it belongs. That's what classification is about. https://networklessons.com/quality-of-service/qos-classification-cisco-ios-router

upvoted 1 times

jubrilak 5 months, 2 weeks ago

Correct Answer is A. Marking means that we set the TOS (Type of Service) byte with an IP Precedence value or DSCP value.
https://networklessons.com/quality-of-service/qos-marking-cisco-ios-router

upvoted 1 times

Mani9Don 5 months, 4 weeks ago

Selected Answer: A

defo marking

upvoted 1 times

net_eng10021 6 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book/classification_oview.html

How the IP Precedence Bits Are Used to Classify Packets

You use the three IP Precedence bits in the ToS field of the IP header to specify CoS assignment for each packet. You can partition traffic into a maximum of six classes and then use policy maps and extended access lists to define network policies for congestion handling and bandwidth allocation for each class.

upvoted 1 times

foreignbishop 6 months, 1 week ago

Selected Answer: D

Section 24 of Cisco ENCOR online learning lists CoS, ToS, DSCP, Class Selector, and TID under the section "Classification". IPP is in the ToS.

upvoted 1 times

MMaris018 7 months ago

Selected Answer: D

it says uses IPP bits to partition traffic into different priority levels. So the answer must be D. Classification.

A is not correct because when we say Marking. It alters the packets to classify the traffic.

upvoted 2 times

cockito 7 months ago

Traffic policers and traffic shapers rely on packet classification features, such as IP precedence, to select packets (or traffic flows) traversing a router or interface for different types of QoS service

upvoted 1 times

Chiaretta 7 months ago

Selected Answer: A

A is the correct answer

upvoted 1 times

olaniyijt 7 months, 2 weeks ago

"into different PRIORITY LEVELS"

upvoted 1 times

Sarmed_abidali 7 months, 2 weeks ago

Agreed, so the answer is shaping ?

upvoted 1 times

Sarmed_abidali 7 months, 2 weeks ago

Nah, it must be D

upvoted 1 times

JackDRipper 7 months, 3 weeks ago

Selected Answer: D

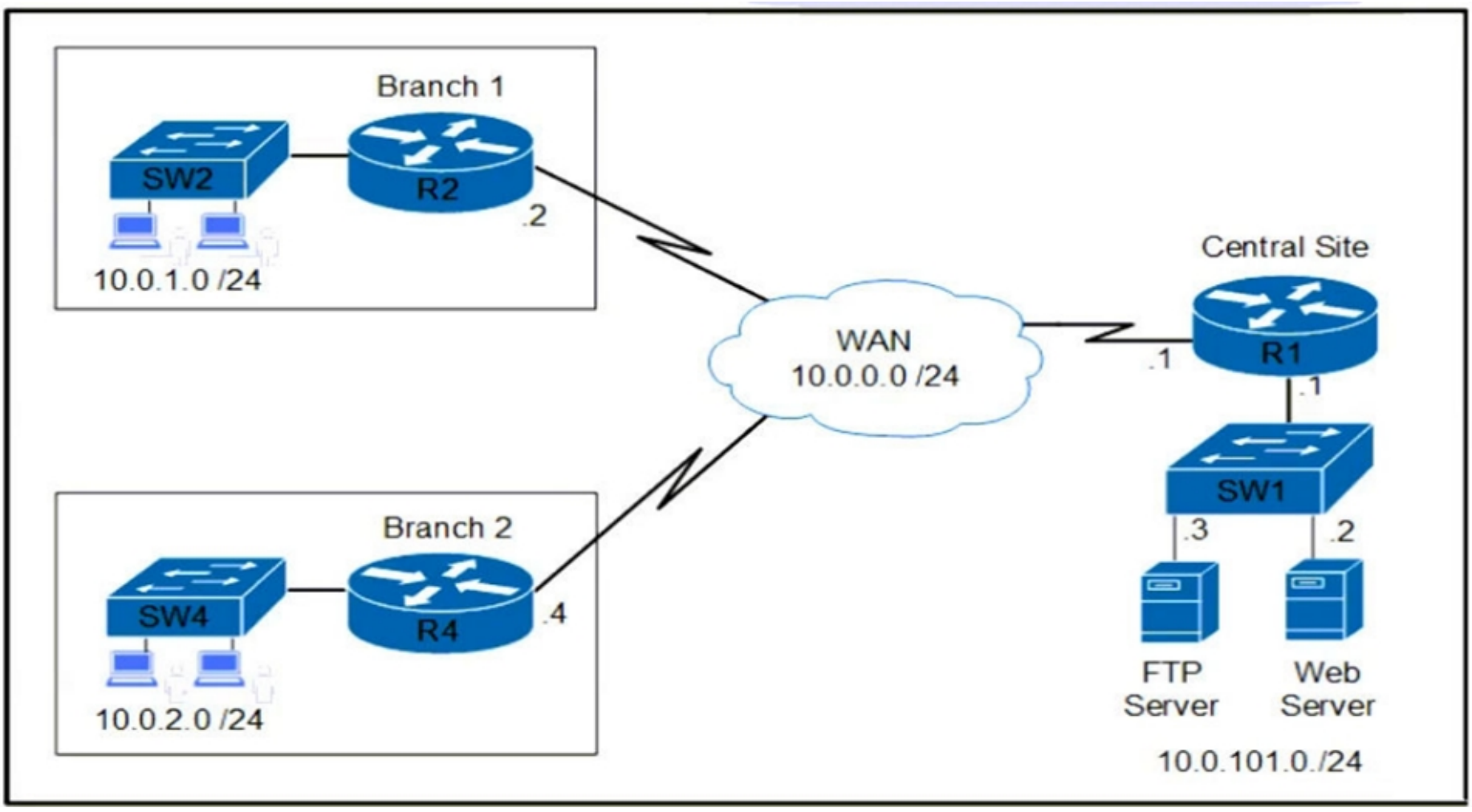
I'm with Team D.
Granted that the question is vague. The word "uses" can be made to mean to "manipulate" (as with Marking) but can also mean to "read" or "utilize" what bits are stored in there (as is appropriate for Classification).

upvoted 2 times

dragonwise 7 months, 4 weeks ago

A is correct. Why?
because: Marking refers to the process of setting a value in a packet header to indicate its priority or treatment within the network

upvoted 2 times



Refer to the exhibit. Which two commands are required on router R1 to block FTP and allow all other traffic from the Branch 2 network? (Choose two.)

A. access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data access-list 101 permit ip any any

B. access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data access-list 101 permit ip any any

C. interface GigabitEthernet0/0 ip address 10.0.0.1 255.255.255.252 ip access-group 101 out

D. access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp access-list 101 permit ip any any

E. interface GigabitEthernet0/0 ip address 10.0.101.1 255.255.255.252 ip access-group 101 in

Correct Answer: *BD*

Community vote distribution

AC (54%) DE (41%) 2%

dragonwise Highly Voted 7 months, 4 weeks ago

A.
access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp
access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data
access-list 101 permit ip any any

B.
access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data
access-list 101 permit ip any any

C.
interface GigabitEthernet0/0
ip address 10.0.0.1 255.255.255.252
ip access-group 101 out

D.
access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp
access-list 101 permit ip any any
E.
interface GigabitEthernet0/0
ip address 10.0.101.1 255.255.255.252
ip access-group 101 in

upvoted 9 times

HungarianDish Highly Voted 10 months, 1 week ago

Selected Answer: AC

I suspect errors in the provided options. I would expect to see options like these based on the topology:
C. interface GigabitEthernet0/0 ip address 10.0.101.1 255.255.255.0 ip access-group 101 out <<< applied for traffic leaving R1 on LAN facing interface
E. interface interface Serial 0/0/0 ip address 10.0.0.1 255.255.255.0 ip access-group 101 in <<< applied for traffic coming to R1 on WAN facing interface

upvoted 8 times

sergiosolotrabajo Most Recent 1 week, 3 days ago

Guys just pass this question go to the next one. Most suitable answers are B and D. C and E are wrong, bad mask and bad in/out configuration, so we cannot even select answer A. We have to think as the ACL was already apply, and then B and D.

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

Those of you saying This question is fucked. None of the subnet masks of the interface IPs match the network of the servers in the diagram. /22 vs /24. So there must be a typo here in the answers. Barring that, the proper method is IN. as we are putting an ACL on traffic coming INTO R1. A B and D are strange. A and D definitely are answers, A just provides a little extra security for FTP, B is only half right. So all we know is, definitely B and C are WRONG.

upvoted 1 times

djedeen 3 months, 2 weeks ago

Selected Answer: AC

A) need to block both FTP ports, and Gig intf must be towards the switch (not a WAN intf) so the direction is out.

upvoted 1 times

JochenStacker 3 months, 3 weeks ago

Selected Answer: AC

I'm voting first for A because it denies both FTP ports and is the only sane answer.
My second vote goes for option C. Interface Gig 0/0 MUST be the interface facing SW1. Because the other interface has to be a serial interface as per the squiggly line and the cloud marked "WAN". This option applies access list 101 in an outward direction from R1 towards SW1 and therefore makes sense.

upvoted 1 times

alex711 3 months, 4 weeks ago

Selected Answer: DE

Voting for DE

https://community.cisco.com/t5/other-network-architecture-subjects/acl-to-block-ftp-servers/td-p/72508

upvoted 1 times

Manvek 4 months ago

Selected Answer: BD

I go with the provided answer with this one as the most correct.

C and D - Wrong, they would filter traffic coming from the server and not from the host. The ACL options configure the host as the source, so it will not work.

A - Wrong, After discarding C and E, all others configuration are about configuring the ACL. Choosing A will make B and D redundant. It is technically correct, but I will discard it just because the question ask for two answers, not one.

B - C: Each one block one of the two ports used by FTP. They are part of the configuration one needs to apply in order to block the FTP traffic. We will need to assume that the ACL is already applied to the correct port and we are just adding the indexes.

Certainly an awful question, but from all possible answers combination, B and D seems the most correct.

upvoted 1 times

[Removed] 5 months ago

The exhibit does not show what interface is what...

upvoted 5 times

HarwinderSekhon 5 months, 2 weeks ago

Selected Answer: AC

A and C
A because you need to block port 20, and 21 and C is because that traffic should go out of gi0/0 according to IP scheme so request with port 20 and 21 tcp will be blocked.

upvoted 1 times

dudalykai 4 months, 2 weeks ago

ftp ports 20 and 21 are going to different directions... 21 from client to ftp, 20 from ftp to client, there is no logic to your explanation...

upvoted 1 times

Burik 5 months, 2 weeks ago

This question doesn't make any sense as no combination of answers provided is correct, none match the exhbit. I'd say we can safely ignore it as it's 100% a bad dump and of all the internet it appears only here.

upvoted 6 times

net_eng10021 6 months ago

Another disaster of a question....seems to be error laden.
upvoted 4 times

Chiaretta 7 months ago

This question is crazy, answer A is correct if applied in IN on R1, B is correct if applied in IN on R1, D is correct if applied in IN on R1, C is applied in OUT and the subnet mask is wrong, E is applied in IN and the subnet mask is wrong.
upvoted 1 times

JackDRipper 7 months, 3 weeks ago

Only A appears to be feasible.
Neither C or E is correct: Subnet masks as well as the ACL direction are wrong. If the IP address on C and E were exchanged and the mask corrected, then it's gotta be E.
upvoted 2 times

rami_mma 8 months, 1 week ago

Selected Answer: DE

if we change the ip address in option E to "10.0.0.1" the answer should be DE.
Otherwise the question can not be solved.
upvoted 4 times

olaniyijt 8 months, 4 weeks ago

Question says to Block FTP (port21) and not FTP-Data (port 20).

Due to the question, I will rule out the answers blocking FTP data which are A and B.

C has the wrong subnet mask. The subnet mask for 10.0.0.0 is /24. C in the option is a /30. So that's wrong too. Also, the access-group should be applied inbound and not outbound.

E also has a wrong mask. The mask for the 10.0.101.0 subnet is /24, and not /30. So E is also wrong.

That leaves us with D being the only correct answer.

The answers need fixing. There seems to be only one correct answer. I am open to correction please.
upvoted 2 times

x3rox 10 months ago

Selected Answer: AC

This is the correct answer:
*A: Correct. Because we need to block both ftp (21) and ftp-data (20) - Although by block the control port I don't see why one would need the other port, but Cisco documentation recommends both: Here: shorturl.at/rEOS7

B: Wrong because only block ftp-data (20) and we need both according to Cisco references.

*C: Correct. Although the image won't show which side is the port G0/0, and we know that extended ACL SHOULD be place as close as possible to the source (WAN) the other option has incorrect Mask, so this would be the best option. Out to the LAN.
See: shorturl.at/mIJTZ

D Wrong, because only blocks control FTP (21)

E. Wrong mask.
upvoted 4 times

Burik 5 months, 2 weeks ago

How is C correct? ip address 10.0.0.1 255.255.255.252 of option C doesn't match the mask in the exhibit
upvoted 1 times

x3rox 10 months ago

* Moreover. FTP uses two modes active and passive. Passive FTP is when the ftp-data port 20 is NOT used at all but instead the client request an IP address and port which is used by the client to open a data connection bypassing the need for port 20. In Active FTP is the client who opens port 20 for the server to connect - and that is in the other direction, so blocking port 20 won't have any effect.. FTP - What a mess!!
upvoted 1 times

x3rox 10 months ago

Active mode: Client is the one opening the ftp-data (20) - ACL won't have effect unless we also do ACL in the opposite direction.
Passive Mode: port ftp-data (20) is NOT used.
upvoted 1 times

Question #576 *Topic 1*

A company recently decided to use RESTCONF instead of NETCONF, and many of their NETCONF scripts contain the operation <edit-config> (operation="create"). Which RESTCONF operation must be used to replace these statements?

A. PUT

B. CREATE

C. GET

D. POST

Correct Answer: *B*

Community vote distribution

D (100%)

Ado_68 Highly Voted 1 year ago

RESTCONF NETCONF
GET <get>, <get-config>
POST <edit-config> (operation=”create”)
PUT <edit-config> (operation=”create/replace”)
Selected Answer D
PATCH <edit-config> (operation=”merge”)
DELETE <edit-config> (operation=”delete”)

upvoted 9 times

PALURDIN Highly Voted 1 year, 2 months ago

Selected Answer: D

RESTCONF does not have CREATE method.

upvoted 8 times

aaabattery 8 months, 1 week ago

https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/101x/programmability/cisco-nexus-9000-series-nx-os-programmability-guide-release-101x/m-n9k-agent-restconf-101x.pdf

upvoted 1 times

asusarla Most Recent 4 months, 1 week ago

imo, I'm going with PUT...the keyword in the question says "replace"
PUT: (Create or Replace) Request:
If the specified command is not present on the device, the POST request creates it ; however, if it is already present in the running configuration, the command will be replaced by this request

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/171/b_171_programmability_cg/restconf_protocol.html#id_125840

upvoted 1 times

Alondrix 3 weeks, 6 days ago

You are interpreting as replacing information on the device. The question is asking to replace the NETCONF command with the RESTCONF command.

upvoted 1 times

CisR 5 months, 1 week ago

It could be A or D.
A if they mean use RESTCONF to replace the text in the NETCONF script (therefore a PUT as that is the replace operator, you are replacing some text with something else)
D if they mean reword the NETCONF script by some means to do the same thing as it did before, which was a 'create' (and therefore a POST)

upvoted 1 times

Bluntedcase 5 months, 2 weeks ago

I think it's A. Here from Cisco:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/171/b_171_programmability_cg/restconf_protocol.html#id_125840

"PUT: (Create or Replace) Request:
If the specified command is not present on the device, the POST request creates it ; however, if it is already present in the running configuration, the command will be replaced by this request."

upvoted 1 times

Bluntedcase 5 months, 2 weeks ago

I've realised my mistake.... of course it's a new command in order to replace the CREATE from NETCONF. That's why POST would be correct, imo

upvoted 1 times

net_eng10021 6 months ago

Why would A not work?

PUT <edit-config> (operation="create/replace")

upvoted 1 times

MO_2022 11 months, 2 weeks ago

Selected Answer: D

POST <edit-config> (operation="create")

upvoted 2 times

BryCR 1 year, 1 month ago

Has to be POST D
https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/101x/programmability/cisco-nexus-9000-series-nx-os-programmability-guide-release-101x/m-n9k-agent-restconf-101x.pdf

upvoted 1 times

doron1122 1 year, 1 month ago

why no A ?
PUT: This method creates or replaces the target resource.

upvoted 3 times

net_eng10021 6 months ago

I'm wondering the same thing...why not A?

PUT <edit-config> (operation="create/replace")

upvoted 2 times

doron1122 1 year, 1 month ago

https://www.ipspace.net/kb/CiscoAutomation/070-netconf.html

upvoted 1 times

jj970us 1 year, 2 months ago

Selected Answer: D

POST: This method creates a data resource or invokes an operations resource.

upvoted 3 times

Question #577 *Topic 1*

An engineer is configuring RADIUS-Based Authentication with EAP MS-CHAPv2 is configured on a client device. Which outer method protocol must be configured on the ISE to support this authentication type?

A. LDAP

B. EAP-FAST

C. EAP-TLS

D. PEAP

Correct Answer: *C*

Community vote distribution

D (100%)

kebkim Highly Voted 1 year, 2 months ago

D.

If you use EAP-MSCHAPv2, it means that your clients doesn't need to have a certificate, but your authentication server (NPS) has a certificate. Passwords from the clients are send using hashes to the authentication server. To protect these password hashes being send over the network, you can use PEAP which act as a TLS/SSL tunnel to protect the authentication traffic.

upvoted 11 times

aaabattery 8 months, 1 week ago

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/201044-802-1x-authentication-with-PEAP-ISE-2-1.html

upvoted 2 times

Quesocat Highly Voted 11 months, 1 week ago

Selected Answer: D

EAP Methods That Use Cisco ISE Server Certificate for Authentication
-PEAP/EAP-MS-CHAPv2
-PEAP/EAP-GTC
-EAP-FAST/EAP-MS-CHAPv2
-EAP-FAST/EAP-GTC
https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_0100000.html

upvoted 5 times

JoeyT 8 months, 2 weeks ago

so why C (EAP-FAST) wrong???

upvoted 1 times

Dan_T_P 5 days, 1 hour ago

i think because it asks for an "outer" method so would be EAP or PEAP. i think EAP-FAST may count as inner method (based on EAP). Theory only, and ready to be corrected, but makes sense to me.

upvoted 1 times

roonly Most Recent 4 months ago

Selected Answer: D

correct answer is D

upvoted 1 times

bob_135 5 months ago

Selected Answer: D

Not EAP-TLS definitely.

PEAP uses a digital certificate to authenticate the authentication server, but clients need to authenticate themselves through MSCHAPv2 or 2GTC.

EAP-TLS goes one step further and requires a certificate on the authentication server and a certificate on every client. The authentication server and supplicant authenticate each other using these certificates.

Once authentication is successful, encryption key material is exchanged through the TLS tunnel.

EAP-TLS is the most secure method for wireless authentication but can be challenging to implement:

You need a Public Key Infrastructure (PKI) to generate certificates.
You need to enroll certificates to your clients.
When an attacker steals a client device, you need to revoke the certificate.

upvoted 3 times

aaabattery 8 months, 1 week ago

Selected Answer: D

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/201044-802-1x-authentication-with-PEAP-ISE-2-1.html

upvoted 2 times

Edwinmolinab 1 year ago

Given answer is correct https://community.cisco.com/t5/network-access-control/ise-with-ldap-using-peap-or-mschapv2/td-p/3540023

upvoted 1 times

tckoon 1 year, 1 month ago

Selected Answer: D

correct answer D

upvoted 4 times

jj970us 1 year, 2 months ago

Selected Answer: D

Reference: https://social.technet.microsoft.com/Forums/Lync/en-US/7962d24d-7aa2-4413-97da-4f03793f2405/very-confused-on-authenciation-concepts-eap-peap-eapmschapv2-?forum=winserversecurity

upvoted 3 times

Question #578 *Topic 1*

An engineer must protect the password for the VTY lines against over-the-shoulder attacks. Which configuration should be applied?

A. line vty 0 15 password XD822j

B. service password-encryption

C. username netadmin secret 7 $1$42J31k98867Pyh4QzwXyZ4

D. username netadmin secret 9 9vFpMf8elb4RVV8$seZ/bDA

Correct Answer: *B*

Community vote distribution

B (82%) D (18%)

Burik 5 months, 2 weeks ago

Selected Answer: B

This is referring to the password under the VTY lines, meaning that we are using the password command under line vty 0 15, and to protect that password from over-the-shoulder attacks when we issue a show run we have to use service password-encryption. This is also in Question #721, where the only correct answer is service password-encryption as well.

upvoted 3 times

Cesar12345 6 months, 1 week ago

Selected Answer: B

https://www.oreilly.com/library/view/hardening-cisco-routers/0596001665/ch04.html

upvoted 1 times

Nickplayany 8 months, 4 weeks ago

Selected Answer: B

It´s the B... Read CCNA if you need more details about it...

upvoted 1 times

sinaghozati 9 months, 3 weeks ago

B - When you use the "service password-encryption" command, any clear-text passwords that are set using the "line vty 0 15 password" command or similar commands will be encrypted. This means that when you look at the configuration file or monitor the console, you will not see the actual password, but rather an encrypted representation of it.

upvoted 2 times

snarkymark 9 months, 4 weeks ago

Going with B,
The question asks "protect the password for the VTY". So taking specifically from the VTY config point of view. The VTY password will be encrypted when service password-encryption. The question is not asking about username and password, IMO

upvoted 2 times

eff3 10 months ago

Selected Answer: D

I go for D - Type 9 is the bp and I don't use cleartext
https://community.cisco.com/t5/networking-knowledge-base/understanding-the-differences-between-the-cisco-password-secret/ta-p/3163238

upvoted 1 times

Rose66 10 months, 2 weeks ago

Selected Answer: B

over-the-shoulder can be also when you enter show running.....

upvoted 3 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: D

I go for D. The password is already entered hashed and therefore protected also while the Engineers is typing the command.
C is not recommended due to weak hashing. B. is hashing the password after is was typed in clear text.

upvoted 1 times

nushadu 11 months, 3 weeks ago

Selected Answer: B

cisco(config)#username test privilege 15 password test777
cisco(config)#do s running-config | include user
username test privilege 15 password 0 test777

cisco(config)#service password-encryption

cisco(config)#do s running-config | include user
username test privilege 15 password 7 044F0E151B761B19
cisco(config)#
cisco(config)#do wr
Building configuration...
[OK]
cisco(config)#

upvoted 1 times

StefanOT2 10 months, 2 weeks ago

Where was the "over-the-shoulder-protection" while you typed in the password in clear text?

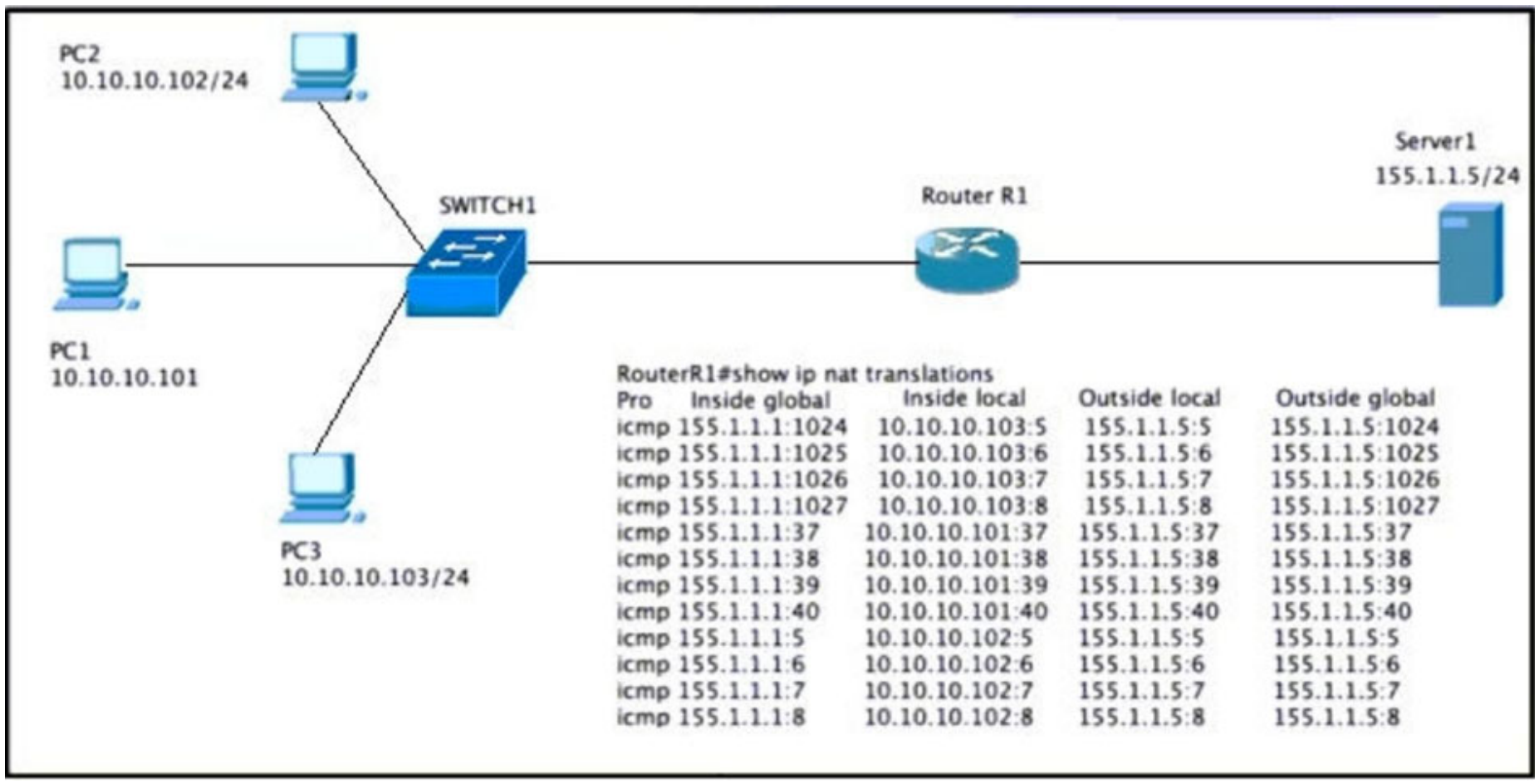
upvoted 1 times

Burik 5 months, 2 weeks ago

This question is asking how to protect the password for the VTY lines, meaning that you have the password command directly under the VTY lines. No username is used. And to protect that password from over-the-shoulder attacks, you have to use service password encryption.

upvoted 1 times

Question #579 *Topic 1*



Refer to the exhibit. Hosts FC1, PC2; and PC3 must access resources on Server1. An engineer configures NAT on Router R1 to enable the communication and enters the show command to verify operation. Which IP address is used by the hosts when they communicate globally to Server1?

A. random addresses in the 155.1.1.0/24 range

B. 155.1.1.1

C. their own address in the 10.10.10.0/24 range

D. 155.1.1.5

Correct Answer: *D*

Community vote distribution

B (69%) D (31%)

mikhailov_ivan90 Highly Voted 10 months, 1 week ago

Selected Answer: D

Read the question word by word again. They asked "Which IP address is used by the HOSTS when they communicate globally to Server1?" Hosts are these 3 PCs, and they use only the server public (global) IP, they don't need to know anything about what is going on on the router. The answer is D

upvoted 7 times

jackr76 8 months, 1 week ago

The server has 155.1.1.5, no cummunication would be possible then...

upvoted 2 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago

Selected Answer: B

Not sure what the debate here is.

Server 1 is 155.1.1.5

the 10.10.10.0/24 network NATs to 155.1.1.1 which then connects to 155.1.1.5...
The question asks which IP address is USED BY THE HOSTS when they communicate

A lot of you need to learn to read the question

upvoted 1 times

HarwinderSekhon 5 months, 2 weeks ago

Selected Answer: B

Poor wording, they are trying to say inside global IP.

upvoted 2 times

Burik 5 months, 2 weeks ago

This question is so badly worded that even C would apply in this case. I'm confident this isn't even an actual exam question as it's in no other dump on the whole internet.

upvoted 2 times

net_eng10021 6 months ago

Wording is awful and it's ambiguous. Exactly how a good engineer does NOT communicate a problem or question.

upvoted 2 times

keesu 7 months ago

Selected Answer: D

GLOBALLY by HOSTS
155.1.1.5

upvoted 1 times

rami_mma 8 months, 1 week ago

Selected Answer: B

B is correct

upvoted 2 times

Clauster 8 months, 1 week ago

Selected Answer: B

Ok let me decipher this for you guys:
"Which IP address is used" "by the hosts" (This has to me 155.1.1.1, it cannot be 155.1.1.5 because Inside Hosts are unable to translate to Remote Routers) "WHEN" (The word WHEN is also a given point) they communicate globally to Server1? (They communicate globally with the Inside Global Address to reach the Outside Global Address.

I really hope this helps you

upvoted 2 times

bendarkel 9 months, 2 weeks ago

Selected Answer: B

The inside Global address (155.1.1.1)

upvoted 4 times

snarkymark 9 months, 4 weeks ago

As usual the wording is horrible, and is how you look at it. Going with D

upvoted 2 times

net_eng10021 6 months ago

Wording is awful and it's ambiguous. Exactly how a good engineer does NOT communicate a problem or question.

upvoted 1 times

snarkymark 9 months, 2 weeks ago

After looking at this again. I am now choosing B

upvoted 1 times

Dataset 10 months ago

Selected Answer: D

The answer is D
read carefully..."wich ip uses GLOBALLY the hosts..."
Regards

upvoted 2 times

Dataset 7 months ago

sorry , the correct is B

upvoted 1 times

markymark874 10 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 2 times

MO_2022 11 months, 2 weeks ago

Selected Answer: B

B for sure

upvoted 2 times

bora4motion 11 months, 2 weeks ago

This is from a host perspective. I thing the answer is d.

upvoted 1 times

nushadu 11 months, 3 weeks ago

B.
cisco#show runn | section int

interface Ethernet0/0
ip address 10.0.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
standby 32 ip 10.0.0.254
interface Ethernet0/1
description WAN_test
ip address 10.10.10.1 255.255.255.252
ip nat outside
ip virtual-reassembly in

upvoted 1 times

nushadu 11 months, 3 weeks ago

cisco#show runn | section nat
ip nat inside
ip nat outside
ip nat inside source static 10.0.0.1 10.10.10.1 extendable
cisco#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 10.10.10.1 10.0.0.1 --- ---
cisco#

upvoted 1 times

Dataset 1 year ago

Selected Answer: B

Its B for me

upvoted 1 times

yousif387 1 year ago

Selected Answer: B

from inside host perspective the global address is 15.1.1.1

upvoted 2 times

Question #580 *Topic 1*

Using the EIRP formula, what parameter is subtracted to determine the EIRP value?

A. transmitter power

B. antenna cable loss

C. antenna gain

D. signal-to-noise ratio

Correct Answer: *C*

Community vote distribution

B (100%)

JochenStacker 3 months, 3 weeks ago

Selected Answer: B

EIRP = Tx Power + Tx Antenna – Tx Cable

upvoted 1 times

Entivo 5 months, 2 weeks ago

Selected Answer: B

EIRP = Output Power - Cable Loss + Antenna Gain

upvoted 2 times

AhcMez 8 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 3 times

snarkymark 9 months, 2 weeks ago

Selected Answer: B

https://www.everythingrf.com/rf-calculators/eirp-effective-isotropic-radiated-power

upvoted 1 times

Kasia1992 10 months ago

Selected Answer: B

B is correct

upvoted 2 times

markymark874 10 months, 3 weeks ago

Selected Answer: B

B is correct

Eirp=output power +antenna gain - cable loss

upvoted 4 times

Dataset 1 year ago

Selected Answer: B

Gain cant be loss..is a (+) in the summatory
Cable loss in effect ,,is a (-)
So , the corretc is

upvoted 2 times

ils9100 1 year, 1 month ago

Has to be - B, lets consider an example
Output power of the transmitter is 27, Cable loss is 12 and Antenna Gain is 45.
EIRP = 27 - 12 (Cable loss) + 45
= 15 + 45
= 60

upvoted 2 times

JamPauGalBag 1 year, 1 month ago

Selected Answer: B

EIRP = + (plus) Gain - (minus) Loss

upvoted 3 times

Jason233 1 year, 2 months ago

Selected Answer: B

E.I.R.P. = transmitter power (dBm) + antenna gain (dBi) – cable attenuation (dB) – connector attenuation (dB)

upvoted 2 times

siteoforigin 1 year, 2 months ago

Selected Answer: B

Antenna Cable loss agreed, page 496 in ENCOR study guide

upvoted 2 times

Deu_Inder 1 year, 2 months ago

Selected Answer: B

Cable loss needs to be subtracted.

upvoted 3 times

PALURDIN 1 year, 2 months ago

Selected Answer: B

Antenna cable loss is substracted

upvoted 2 times

Question #581 *Topic 1*

What is one main REST security design principle?

A. separation of privilege

B. password hashing

C. confidential algorithms

D. OAuth

Correct Answer: *A*

Community vote distribution

A (100%)

Alberht 1 year, 2 months ago

Selected Answer: A

https://medium.com/strike-sh/rest-security-design-principles-434bd6ee57ea

upvoted 4 times

```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 65001
<output omitted>
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.50.2    4        65002      10       9        5    0    0 00:04:56        2

R1#show ip bgp 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 2
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  65002
    192.168.50.2 from 192.168.50.2 (172.20.0.2)
      Origin IGP, metric 0, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0

 <CONFIGURATION CHANGE MADE>

R1#show ip bgp 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 6
Paths: (1 available, best #1, table default, RIB-failure(17))
  Not advertised to any peer
  Refresh Epoch 1
  65002
    192.168.50.2 from 192.168.50.2 (172.20.0.2)
      Origin IGP, metric 0, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
```

Refer to the exhibit. R1 has a BGP neighborship with a directly connected router on interface Gi0/0. Which command set is applied between the iterations of show ip bgp 2.2.2.2?

A. R1(config)#no ip route 192.168.50.2 255.255.255.255 Gi0/0

B. R1(config)#ip route 2.2.2.2 255.255.255.255 192.168.50.2

C. R1(config)#router bgp 65002 R1(config-router)#neighbor 192.168.50.2 shutdown

D. R1(config)#router bgp 65001 R1(config-router)#neighbor 192.168.50.2 shutdown

Correct Answer: *B*

Community vote distribution

B (100%)

emanc93 Highly Voted 1 year, 1 month ago

BGP rib failure from 'show ip bgp' indicates that a route learned from a neighbor where a lower administrative distance (from a static, or other IGP) has already been installed into the routing table, thus the BGP route has failed to install into the IP routing table (RIB) because it has been trumped by the lower admin distance route.

static route has lower AD thus the bgp route is failing to install

upvoted 19 times

nushadu 11 months, 4 weeks ago

yes, agree

upvoted 1 times

djedeen Most Recent 3 months, 2 weeks ago

Selected Answer: B

Step 3. If the Routing Table already has the same prefix/prefix-length entry with a lower Administrative Distance (AD) as seen in show ip bgp, BGP marks the route received with RIB-Failure.

upvoted 1 times

dragonwise 7 months, 4 weeks ago

A.
R1(config)#no ip route 192.168.50.2 255.255.255.255 Gi0/0

B.
R1(config)#ip route 2.2.2.2 255.255.255.255 192.168.50.2

C.
R1(config)#router bgp 65002
R1(config-router)#neighbor 192.168.50.2 shutdown

D.
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 shutdown

upvoted 2 times

nushadu 11 months, 1 week ago

Selected Answer: B

cisco_R3#show bgp 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 16
Paths: (2 available, best #1, table default)
Advertised to update-groups:
4
Refresh Epoch 1
2
192.168.255.22 from 192.168.255.22 (2.2.2.2)
Origin incomplete, metric 0, localpref 101, valid, external, best
rx pathid: 0, tx pathid: 0x0
Refresh Epoch 1
2, (received-only)
192.168.255.22 from 192.168.255.22 (2.2.2.2)
Origin incomplete, metric 0, localpref 100, valid, external
rx pathid: 0, tx pathid: 0

cisco_R3#show ip ro 2.2.2.2
Routing entry for 2.2.2.2/32
Known via "bgp 3", distance 20, metric 0
Tag 2, type external
Last update from 192.168.255.22 00:01:59 ago
Routing Descriptor Blocks:
* 192.168.255.22, from 192.168.255.22, 00:01:59 ago
Route metric is 0, traffic share count is 1
AS Hops 1
Route tag 2
MPLS label: none

cisco_R3(config)#ip route 2.2.2.2 255.255.255.255 192.168.255.22 11

upvoted 1 times

nushadu 11 months, 1 week ago

cisco_R3(config)#do s ip bgp 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 20
Paths: (2 available, best #1, table default, RIB-failure(17)) <<<<<<<<<<<<<<<<<<<<<< after static route
Advertised to update-groups:
4
Refresh Epoch 1
2
192.168.255.22 from 192.168.255.22 (2.2.2.2)
Origin incomplete, metric 0, localpref 101, valid, external, best
rx pathid: 0, tx pathid: 0x0
Refresh Epoch 1
2, (received-only)
192.168.255.22 from 192.168.255.22 (2.2.2.2)
Origin incomplete, metric 0, localpref 100, valid, external
rx pathid: 0, tx pathid: 0
cisco_R3(config)#
cisco_R3(config)#
cisco_R3(config)#do s ip rou 2.2.2.2
Routing entry for 2.2.2.2/32
Known via "static", distance 11, metric 0 <<<<<<<<<<<<<<<<<<<<
Routing Descriptor Blocks:
* 192.168.255.22
Route metric is 0, traffic share count is 1
cisco_R3(config)#

upvoted 2 times

nushadu 11 months, 1 week ago

cisco_R3(config)#do s ip rou sta

Gateway of last resort is 2.2.2.2 to network 0.0.0.0

2.0.0.0/32 is subnetted, 1 subnets
S 2.2.2.2 [11/0] via 192.168.255.22

cisco_R3(config)#
cisco_R3(config)#
cisco_R3(config)#ip route 2.2.2.2 255.255.255.255 192.168.255.22 250
cisco_R3(config)#
cisco_R3(config)#
cisco_R3(config)#do s ip rou sta

S* 0.0.0.0/0 [1/0] via 2.2.2.2
172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S 172.16.1.0/24 is directly connected, Ethernet0/0.30
S 192.168.1.0/24 is directly connected, Ethernet0/0.20

cisco_R3(config)#do s ip rou bg

2.0.0.0/32 is subnetted, 1 subnets
B 2.2.2.2 [20/0] via 192.168.255.22, 00:00:09 <<<<<<<<<<<<<<<<

cisco_R3(config)#

upvoted 1 times

nushadu 11 months, 3 weeks ago

Selected Answer: B

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/213286-understand-bgp-rib-failure-and-the-bgp-s.html

upvoted 2 times

Deu_Inder 1 year, 2 months ago

B seems to be the right answer.
See: https://bradhedlund.com/notes/bgp/#:~:text=BGP%20rib%20failure%20from%20'show,trumped%20by%20the%20lower%20admin

upvoted 4 times

siteoforigin 1 year, 2 months ago

Agreed, Cisco doc on it here as well:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/213286-understand-bgp-rib-failure-and-the-bgp-s.html

upvoted 3 times

Question #583 *Topic 1*

After a redundant route processor failure occurs on a Layer 3 device, which mechanism allows for packets to be forwarded from a neighboring router based on the most recent tables?

A. BFD

B. RP failover

C. NSF

D. RPVST+

Correct Answer: *C*

Community vote distribution

C (100%)

KZM Highly Voted 1 year ago

Cisco Nonstop Forwarding (NSF) works with the Stateful Switchover (SSO) feature to minimize the amount of time a network is unavailable to users following a switchover. The main objective of NSF SSO is to continue forwarding IP packets following a Route Processor (RP) switchover.

upvoted 5 times

snarkymark Most Recent 9 months, 2 weeks ago

Selected Answer: C

https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/stck_mgr_ha/b_166_nsf_sso_9400_cg.html

upvoted 2 times

Japsurd 1 year, 2 months ago

Selected Answer: C

It's NSF https://www.youtube.com/watch?v=Dm-3UxiKPtc

upvoted 3 times

By default, which virtual MAC address does HSRP group 15 use?

A. c0:42:31:98:86:0f

B. 05:af:1c:0f:ac:15

C. 00:00:0c:07:ac:0f

D. 05:5e:ac:07:0c:0f

Correct Answer: *C*

Community vote distribution

C (100%)

mgiuseppe86 2 months, 2 weeks ago

15 = 00001111 = 0000|1111 = 0|15 = 0F

upvoted 1 times

eddgg 3 months, 3 weeks ago

Selected Answer: C

c is the answer

upvoted 1 times

mellohello 9 months, 1 week ago

Selected Answer: C

A - 10
B - 11
C = 12
D = 13
E = 14
F = 15

upvoted 3 times

nushadu 11 months, 3 weeks ago

Selected Answer: C

interface Ethernet0/0.100
encapsulation dot1Q 100
ip address 10.0.111.1 255.255.255.0
standby 15 ip 10.0.111.254
!

cisco(config-subif)#do s stand

Ethernet0/0.100 - Group 15
State is Speak
Virtual IP address is 10.0.111.254
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac0f (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.200 secs
Preemption disabled
Active router is unknown
Standby router is unknown

upvoted 4 times

Question #585 *Topic 1*

An engineer must provide wireless coverage in a square office. The engineer has only one AP and believes that it should be placed it in the middle of the room.
Which antenna type should the engineer use?

A. directional

B. polarized

C. omnidirectional

D. Yagi

Correct Answer: *C*

Community vote distribution

C (100%)

Dataset 8 months ago

Selected Answer: C

HI!
C is correct
Regards

upvoted 2 times

snarkymark 9 months, 4 weeks ago

C is correct,
https://www.waveform.com/pages/antennas-and-antenna-placement

upvoted 2 times

Question #586 *Topic 1*

Which technology reduces the implementation of STP and leverages both unicast and multicast?

A. VLAN

B. VPC

C. VXLAN

D. VSS

Correct Answer: *D*

Community vote distribution

C (81%) D (19%)

Darude Highly Voted 1 year ago

Selected Answer: C

correct answer is C
reference:
https://www.cisco.com/c/en/us/support/docs/switches/nexus-9000-series-switches/118978-config-vxlan-00.html#anc7
and
https://blogs.cisco.com/datacenter/detecting-and-mitigating-loops-in-vxlan-networks

upvoted 5 times

StefanOT2 Highly Voted 10 months, 2 weeks ago

Selected Answer: C

C makes most sense. VXLAN is leveraging multicast to flood broadcast. And STP is normally no longer needed.
D. can reduces STP, but I don't see the multicast link...

upvoted 5 times

djedeen Most Recent 3 months, 2 weeks ago

Selected Answer: C

VXLAN, multicast used to flood L2 traffic such as ARP. VXLAN eliminates the need for a spanning tree, using a MAC over IP/UDP solution. So, within the VXLAN no STP, reducing it overall in the entire network ...

upvoted 1 times

rogue_user 4 months, 2 weeks ago

Selected Answer: C

To me it's VXLAN. Key word is "leverages". VSS doesn't make use of either.

upvoted 3 times

msstanick 5 months, 1 week ago

Selected Answer: D

Well, I am going with D because the question is about "reducing" the STP while VXLAN eliminates it at all. MC is supported by both I believe. As always - who knows what Cisco had in mind?

upvoted 1 times

Chiaretta 7 months ago

Selected Answer: D

D is correct VSS stack two remote switch in one

upvoted 1 times

CiscoTheHorse 7 months, 1 week ago

Hi All, I think D. How does VXLAN prevent a packet from looping?

upvoted 1 times

Chiaretta 8 months ago

Selected Answer: D

D is correct.
Virtual switching system VSS, stack 2 core switchs in one virtual reducing the needs of STP

upvoted 2 times

snarkymark 9 months, 2 weeks ago

Selected Answer: C

https://www.nakivo.com/blog/vxlan-vmware-basics/

upvoted 1 times

Huntkey 1 year ago

Selected Answer: C

Does VSS leverage multicast? Or in other words, does it need multicast for VSS to function? I doubt it. VXLAN does though. It can use multicast to handle BUM traffic.

upvoted 2 times

jdholmes423 1 year, 2 months ago

The root of the STP should always be the VSS:
https://community.cisco.com/t5/switching/spanning-tree-and-vss-recommended-best-practice/td-p/3213837

upvoted 1 times

Deu_Inder 1 year, 2 months ago

VXLAN also eliminates STP and uses multicast.

upvoted 1 times

AndreasThornus 11 months, 2 weeks ago

Careful - it says "reduce STP", not eliminate.

upvoted 2 times

onkel_andi 1 year, 1 month ago

No, so if you implement VXLAN in LAN, are there fewer STP Instances? With VSS, yes.

upvoted 1 times

StefanOT2 10 months, 2 weeks ago

usually you don't need any STP any more with VXLAN implemented

upvoted 1 times

Typovy 12 months ago

Ofcourse yes because VXLAN underlay is routed based and do not use STP....

upvoted 1 times

Question #587 *Topic 1*

A customer has recently implemented a new wireless infrastructure using WLC-5520s at a site directly next to a large commercial airport. Users report that they intermittently lose Wi-Fi connectivity, and troubleshooting reveals it is due to frequent channel changes. Which two actions fix this issue? (Choose two.)

A. Enable DFS channels because they are immune to radar interference.

B. Restore the DCA default settings because this automatically avoids channel interference.

C. Remove UNII-2 and Extended UNII-2 channels from the 5 Ghz channel list.

D. Disable DFS channels to prevent interference with Doppler radar.

E. Configure channels on the UNII-2 and the Extended UNII-2 sub-bands of the 5 Ghz band only.

Correct Answer: *CD*

Community vote distribution

CD (100%)

kebkim Highly Voted 1 year, 2 months ago

DFS is Dynamic Frequency Selection, which is a function of using 5 GHz Wi-Fi frequencies that are generally reserved for radar. Because the 2.4Ghz band is free of radar, the DFS rules only apply to the 5.250 – 5.725 Ghz band.
UNII-2 (5.250-5.350 GHz and 5.470-5.725 GHz) shared with radar systems. Therefore, APs operating on UNII-2 channels are required to use Dynamic Frequency Selection (DFS) to avoid interfering with radar signals.

upvoted 6 times

Badger_27 Most Recent 8 months, 2 weeks ago

Really..really?

upvoted 4 times

Dv123456 4 months, 4 weeks ago

I haven't see DFS in the official cert guide

upvoted 2 times

ihateciscoreally 3 months ago

man you talking about DFS not being covered in OCG, but its not the problem xD problem is that they are asking about high level wireless, its not topic for ENCOR.

upvoted 1 times

sinaghozati 9 months, 3 weeks ago

C and D

upvoted 2 times

x3rox 10 months ago

From Source: If you want to use the UNI II band DFS channels, don't have your site near an airport! If you have newer....
https://blog.iptel.com.au/wifi-and-the-problem-with-radar#:~:text=If%20you%20want%20to%20use%20the%20UNI%20II%20band%20DFS%20channels%2C%20don%27t%20have%20your%20site%20near%20an%20airport!%20If%20you%20have%20newer

upvoted 1 times

bora4motion 1 year ago

Selected Answer: CD

DFS channels are actually extended UNII-2 and 3. To me the answer is C and D. Disable DFS as that will stop taking the radios down to scan for a free channel and stop using UNI2.

upvoted 2 times

winder 1 year ago

my understanding of this is for answer A is "DFS channels because they are immune to radar interference" , they aren't immune. believe the question mentioned channel keeps changing is due to DFS, so the provided answer is right
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/213882-radar-detection-in-dynamic-frequency-sel.html

upvoted 1 times

tckoon 1 year, 2 months ago

This mean answers are A & C ?

upvoted 2 times

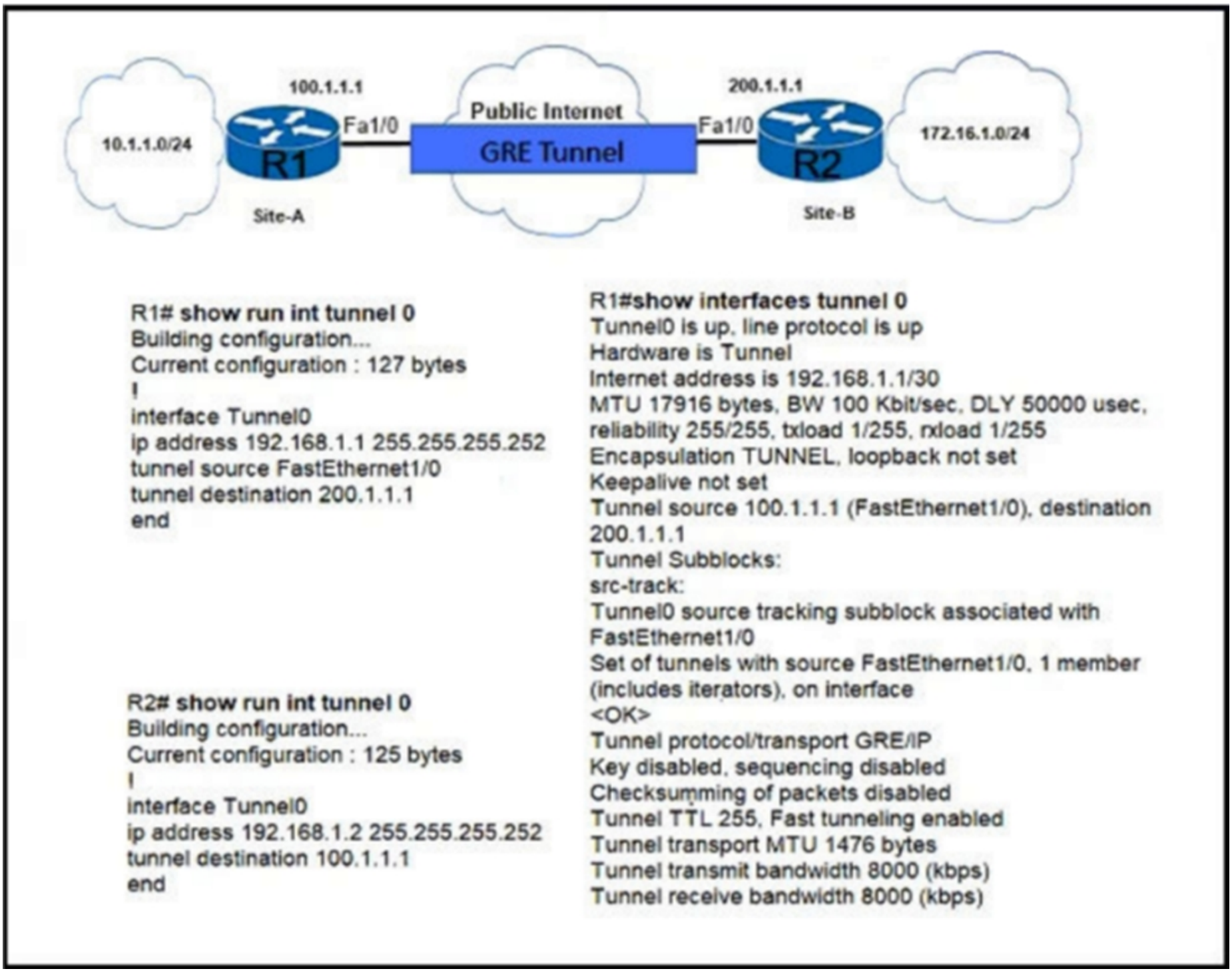
Nassir76 4 months, 3 weeks ago

apologies I accidently upvoted you response. I meant to say it could not be A because the question states that there is frequent channel change. We need to stop that by disabling DFS,

upvoted 2 times

Question #588 *Topic 1*

Refer to the exhibit.



Which GRE tunnel configuration command is missing on R2?

A. tunnel source 172.16.1.0

B. tunnel source 200.1.1.1

C. tunnel destination 200.1.1.1

D. tunnel source 192.168.1.2

Correct Answer: *B*

Community vote distribution

B (100%)

jhonmeikel 3 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

snarkymark 9 months, 4 weeks ago

B is correct
https://community.cisco.com/t5/networking-knowledge-base/how-to-configure-a-gre-tunnel/ta-p/3131970#toc-hId--1446104265

upvoted 3 times

Question #589 *Topic 1*

The Gig0/0 interface of two routers is directly connected with a 1G Ethernet link. Which configuration must be applied to the interface of both routers to establish an OSPF adjacency without maintaining a DR/BDR relationship?

A. interface Gig0/0 ip ospf network non-broadcast

B. interface Gig0/0 ip ospf network point-to-multipoint

C. interface Gig0/0 ip ospf network point-to-point

D. interface Gig0/0 ip ospf network broadcast

Correct Answer: *C*

Community vote distribution

C (100%)

nushadu 11 months, 1 week ago

Selected Answer: C

cisco_R3#show run int e0/0.50
Building configuration...

Current configuration : 189 bytes
!
interface Ethernet0/0.50
encapsulation dot1Q 50
ip address 10.111.10.1 255.255.255.252
ip ospf network point-to-point <<<<<<<<<<<<<<<<<<<
ip ospf 1 area 22
bfd interval 999 min_rx 999 multiplier 3
end

cisco_R3#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
192.168.255.2 1 FULL/DROTHER 00:00:33 192.168.255.2 Ethernet0/0.10
200.200.200.200 1 FULL/DR 00:00:34 192.168.255.22 Ethernet0/0.10
5.5.5.5 0 FULL/ - 00:00:34 10.111.10.2 Ethernet0/0.50 <<<<<<<<<<<<<<<<<
cisco_R3#

upvoted 3 times

Xerath 11 months, 2 weeks ago

Selected Answer: C

Provided answer is correct.

upvoted 2 times

Question #590 *Topic 1*

Refer to the exhibit.

```
R1#show running-config interface fa0/0
Building configuration...

Current configuration : 192 bytes
!
interface FastEthernet0/0
 ip address 192.168.3.5 255.255.255.0
 duplex full
 vrrp 1 ip 192.168.3.1
 vrrp 1 priority 110
 vrrp 1 authentication text cisco
 vrrp 1 track 20 decrement 20
end

R1#show running-config | include track 20
track 20 ip route 10.10.1.1 255.255.255.255 reachability
```

```
R2#show running-config interface fa0/0
Building configuration...

Current configuration : 141 bytes
!
interface FastEthernet0/0
 ip address 192.168.3.2 255.255.255.0
 duplex full
 vrrp 1 ip 192.168.3.1
 vrrp 1 authentication text cisco
end
```

An engineer configures VRRP and issues the show commands to verify operation. What does the engineer confirm about VRRP group 1 from the output?

A. Communication between VRRP members is encrypted using MD5.

B. There is no route to 10.10.1.1/32 in R2's routing table.

C. R1 is primary if 10.10.1.1/32 is in its routing table.

D. If R1 reboots, R2 becomes the primary virtual router until R2 reboots.

Correct Answer: *C*

Community vote distribution

C (67%) B (27%) 7%

[Removed] 5 months, 1 week ago

Selected Answer: C

answer makes sense.
A- Wrong, its cleartext
B- Wrong, not enough information to infer this
C- Correct, if there is reachability to the network 10.10.1.1/32, R1's priority is default 100, which is equal to R2's priority of default 100, so what is the next tie breaker? the higher IP address, R1 wins, and with VRRP having preempt enabled by default, R1 becomes the Master.
D- Wrong

upvoted 2 times

teikitiz 4 months, 3 weeks ago

R1's prio is 110. When the tracked object fails, the prio is decremented by 20, lowering it below R2's default prio, 100. But C says when the route is installed (meaning reachable), so R1's prio remains 110, and master. Still C, nevertheless.

upvoted 2 times

echipbk 10 months, 3 weeks ago

Selected Answer: C

C is the correct answer

upvoted 2 times

kewokil120 10 months, 4 weeks ago

Selected Answer: C

R1 tracks a /32 network and remove vrrp priority if the /32 goes away.

upvoted 1 times

John13121 11 months ago

It is NOT D, Why ? Because preemption is enabled by default. Which means that if R1 reboots -> R2 will become primary and when R1 reboot is finished will take the role again because of the default preemption ! -> C seems right.

upvoted 4 times

nushadu 11 months, 1 week ago

Selected Answer: C

cisco_R3(config-subif)#do s runn interface Ethernet0/0.40
!
interface Ethernet0/0.40
encapsulation dot1Q 40
ip address 172.16.13.2 255.255.255.0
vrrp 10 ip 172.16.13.254
vrrp 10 track 4 decrement 20
end

cisco_R3(config-subif)#do s track 4
Track 4
IP route 5.5.5.55 255.255.255.255 reachability
Reachability is Down (no ip route)
1 change, last change 00:04:13
First-hop interface is unknown
Tracked by:
VRRP Ethernet0/0.40 10

cisco_R3(config-subif)#do s vrrp
Ethernet0/0.40 - Group 10
State is Master
Virtual IP address is 172.16.13.254
Virtual MAC address is 0000.5e00.010a
Advertisement interval is 1.000 sec
Preemption enabled <<<<<<<<<< by default, so it'll become MASTER after high priority
Priority is 80
Track object 4 state Down decrement 20
Master Router is 172.16.13.2 (local), priority is 80
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec

cisco_R3(config-subif)#

upvoted 1 times

nushadu 11 months, 1 week ago

cisco_R3(config-subif)#
*Dec 23 20:51:51.008: %TRACK-6-STATE: 4 ip route 5.5.5.55/32 reachability Down -> Up
cisco_R3(config-subif)#
cisco_R3(config-subif)#do s track 4
Track 4
IP route 5.5.5.55 255.255.255.255 reachability
Reachability is Up (BGP)
2 changes, last change 00:00:41
First-hop interface is Ethernet0/0.10
Tracked by:
VRRP Ethernet0/0.40 10
cisco_R3(config-subif)#do s vrrp
Ethernet0/0.40 - Group 10
State is Master
Virtual IP address is 172.16.13.254
Virtual MAC address is 0000.5e00.010a
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Track object 4 state Up decrement 20
Master Router is 172.16.13.2 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec

upvoted 1 times

nushadu 11 months, 1 week ago

cisco_R3(config-subif)#
cisco_R3(config-subif)#do s ip ro 5.5.5.55
Routing entry for 5.5.5.55/32
Known via "bgp 3", distance 20, metric 0
Tag 5, type external
Last update from 192.168.255.55 00:01:21 ago
Routing Descriptor Blocks:

* 192.168.255.55, from 192.168.255.55, 00:01:21 ago
Route metric is 0, traffic share count is 1
AS Hops 4
Route tag 5
MPLS label: none
cisco_R3(config-subif)#

upvoted 1 times

nushadu 11 months, 3 weeks ago

tricky question, I hate it ...
D. is true anyway,
C. is unclear, let's say what happens if this route flaps? after that R2 will be master anyway cos no feature PREEMPTION is configured on R1... right?

upvoted 2 times

Xerath 11 months, 2 weeks ago

Preemption is enabled by default in VRRP, Answer "C" is correct.

upvoted 1 times

KOJJY 11 months, 3 weeks ago

Selected Answer: C

i think that is close answer

upvoted 1 times

Inzo 11 months, 4 weeks ago

Selected Answer: D

I believe D is correct because preemption is enabled in VRRP by default.
The answer C says " if 10.10.1.1/32 is in its routing table." if this route is statically configured it will still be there disregarding its reachability.

upvoted 1 times

Feliphus 11 months, 3 weeks ago

Look close the D answer: . If R1 reboots, R2 becomes the primary virtual router until R2 reboots. (R2 reboots !)

upvoted 1 times

tinoe 1 year, 1 month ago

Selected Answer: C

C is correct because of the tracking feature. Exhibit speaks nothing about availability of routes, so we can not tell which routes are available or not available.

upvoted 2 times

onkel_andi 1 year, 1 month ago

Selected Answer: C

Provides answer is correct. R1 is primary if 10.10.1.1/32 is in its routing table. -> because of track 20 command

upvoted 1 times

melkij17 1 year, 2 months ago

A believe it is C. By ''sh run int fa0/0'' command we are not able to tell if route is in routing table or not. On router 1 is configured IP SLA which is tracking reachability to 10.10.1.1 - so if this route is unavailable, routers 1 priority decrements and it becomes Secondary, but if the route is reachable it will stay Primary because of its 110 priority.

upvoted 4 times

Wooker 1 year, 2 months ago

Selected Answer: B

Answer: B

upvoted 1 times

Wooker 1 year, 2 months ago

Sorry is D

upvoted 1 times

civan 11 months ago

Not D; VRRP has preempt on by default, so R1 will take back over as primary when it can.

Answer is C

upvoted 1 times

jdholmes423 1 year, 2 months ago

Selected Answer: B

I believe B is true.

upvoted 3 times

H3kerman 1 year ago

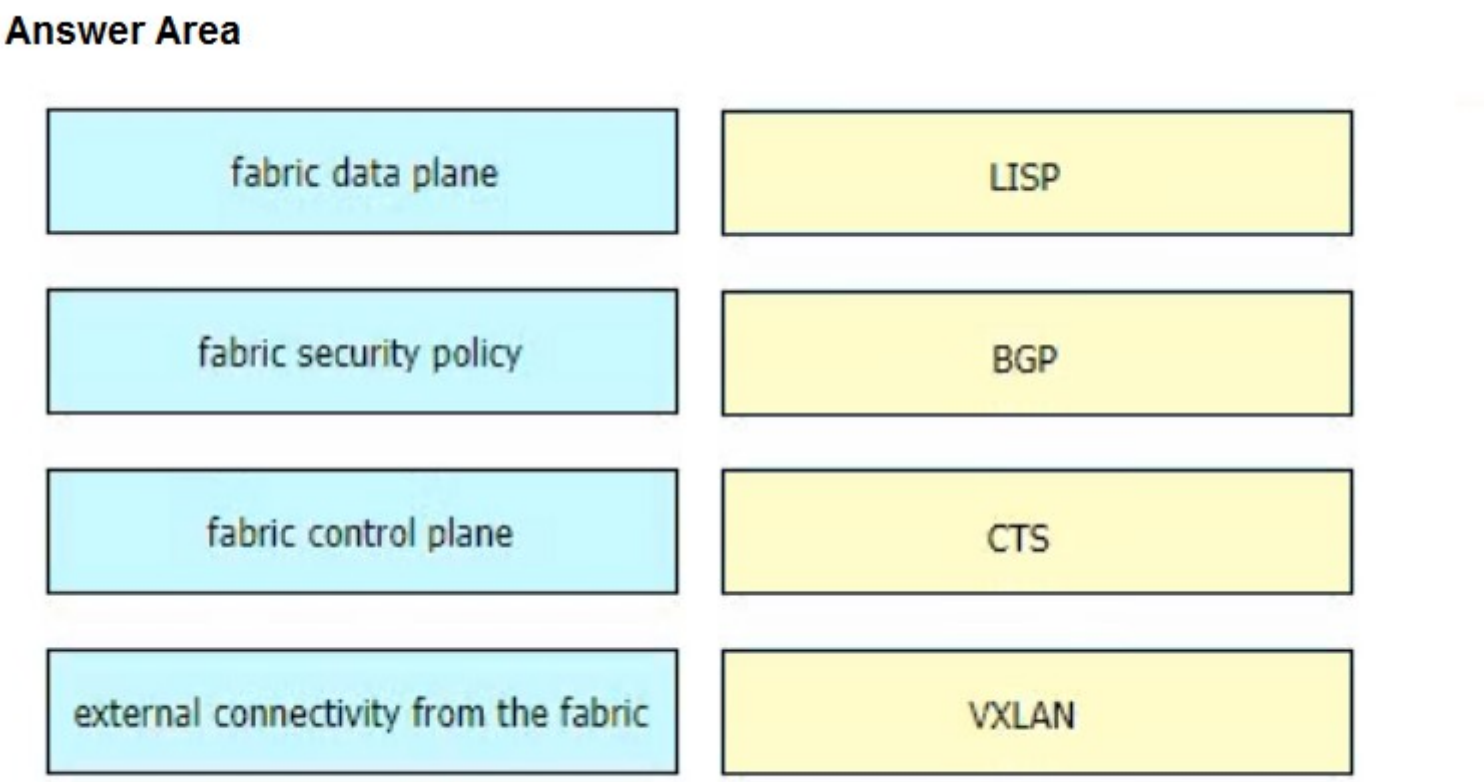
there was no output regarding routing table, so you can't say if yes or no

upvoted 3 times

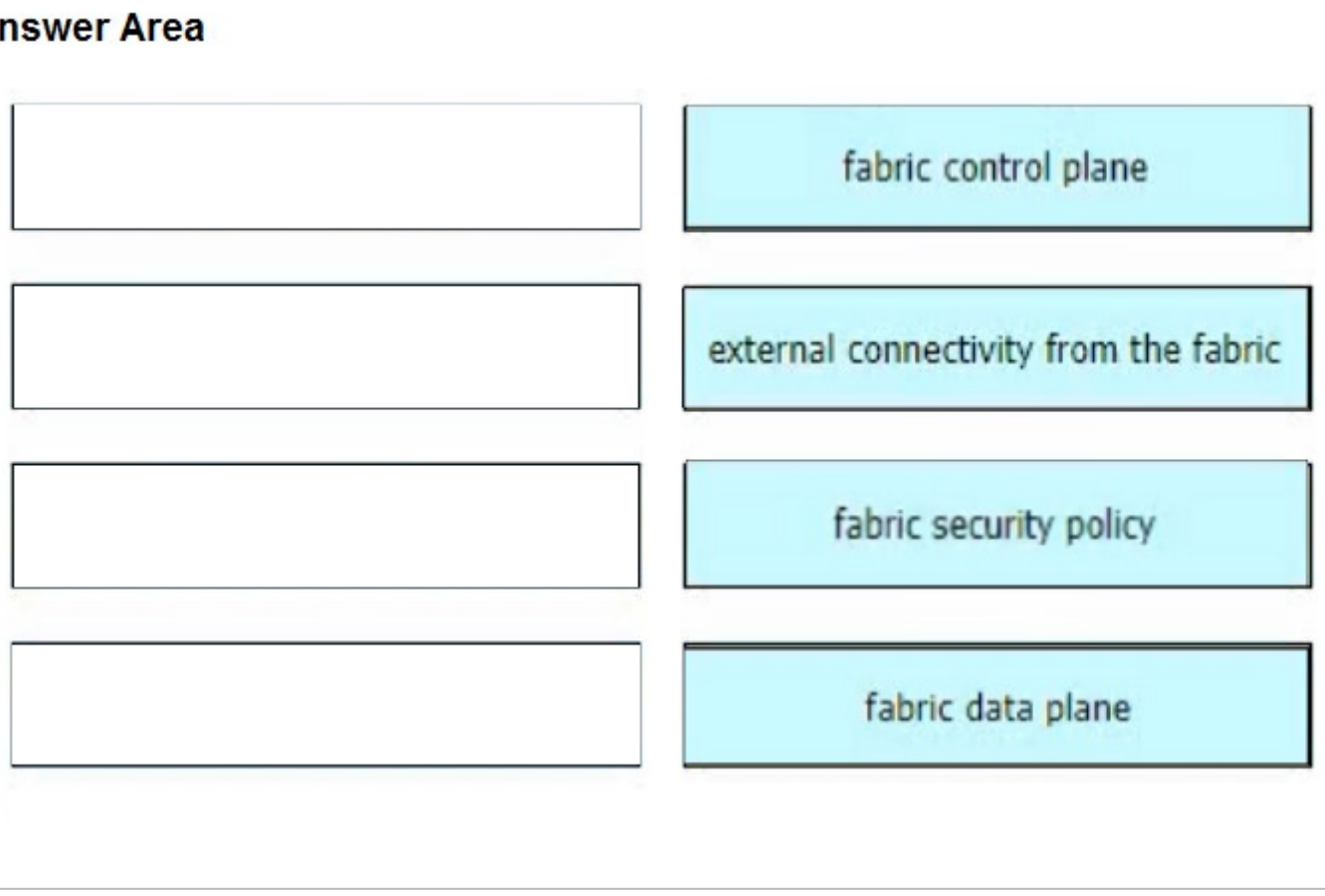
DRAG DROP -

Drag and drop the Cisco SD-Access solution areas from the left onto the protocols they use on the right.

Select and Place:



Correct Answer:



Huntkey Highly Voted 1 year ago

Control Plane – LISP
Data Plane – VXLAN
Security - Cisco TrustSec or CTS
External connection - BGP
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

upvoted 9 times

bora4motion Highly Voted 11 months, 2 weeks ago

The presented solution is correct.

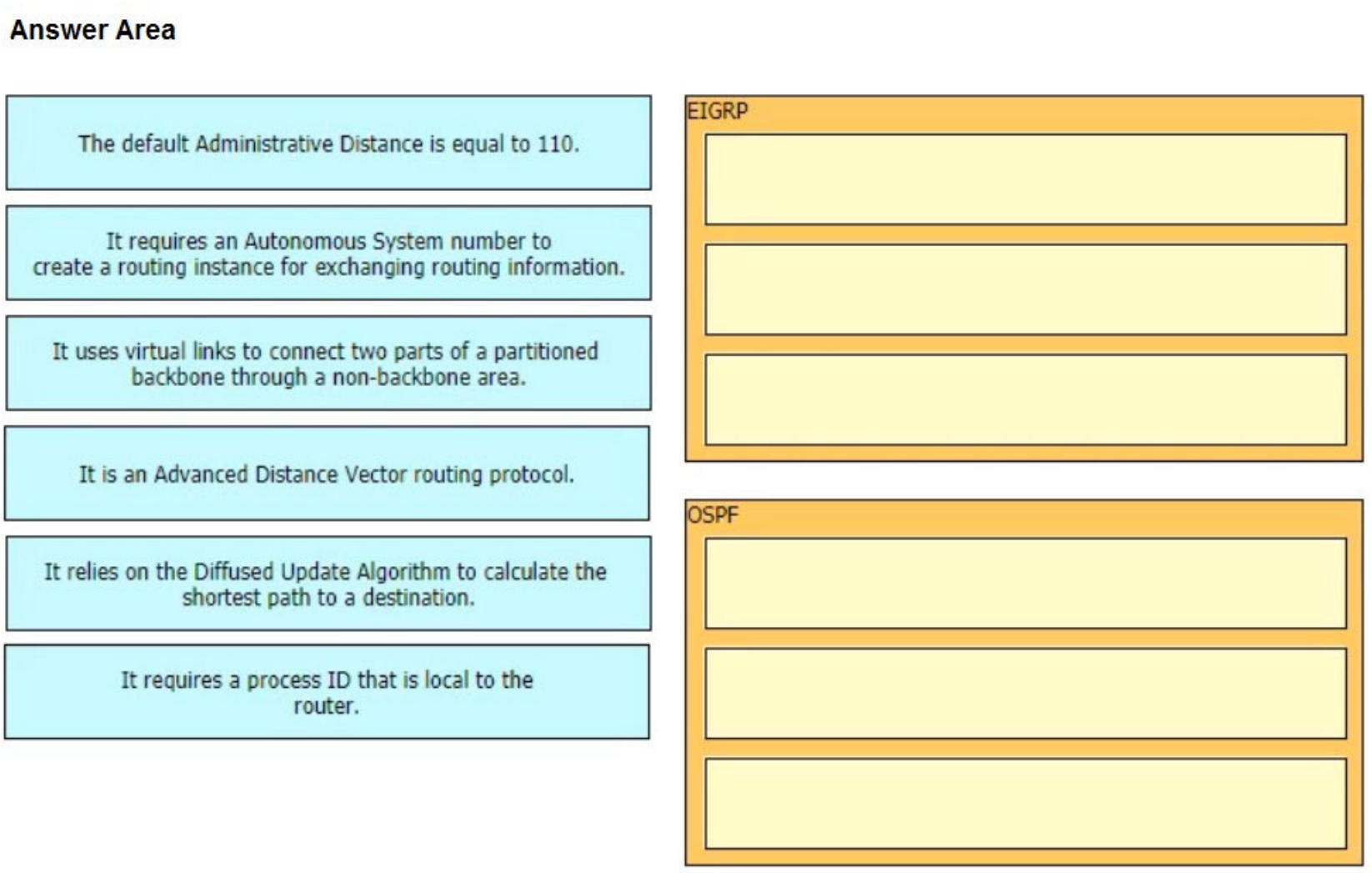
upvoted 5 times

Question #592 *Topic 1*

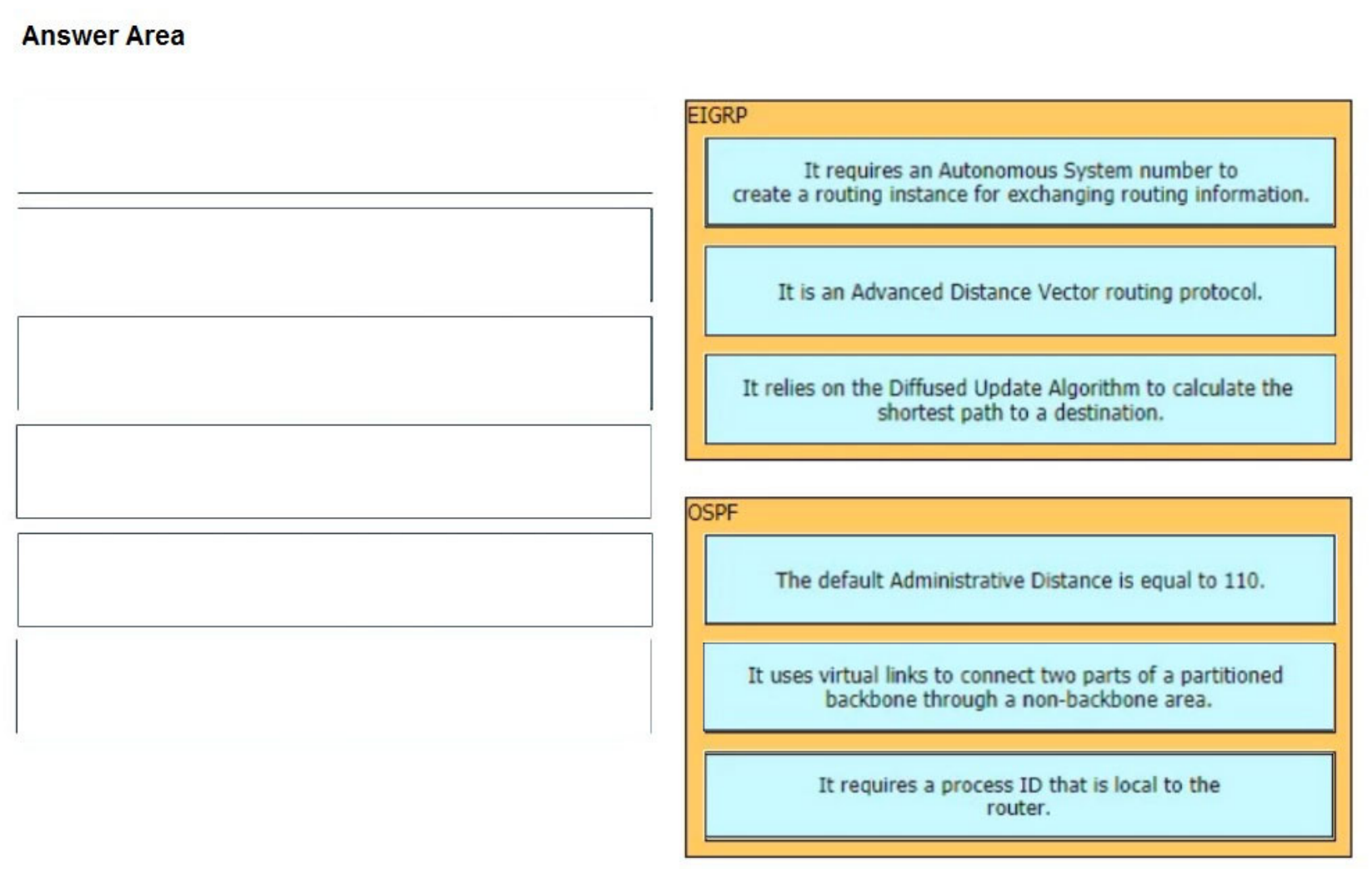
DRAG DROP -

Drag and drop the characteristics from the left onto the routing protocols they describe on the right.

Select and Place:



Correct Answer:



eddgg 3 months, 4 weeks ago

correct answer

upvoted 1 times

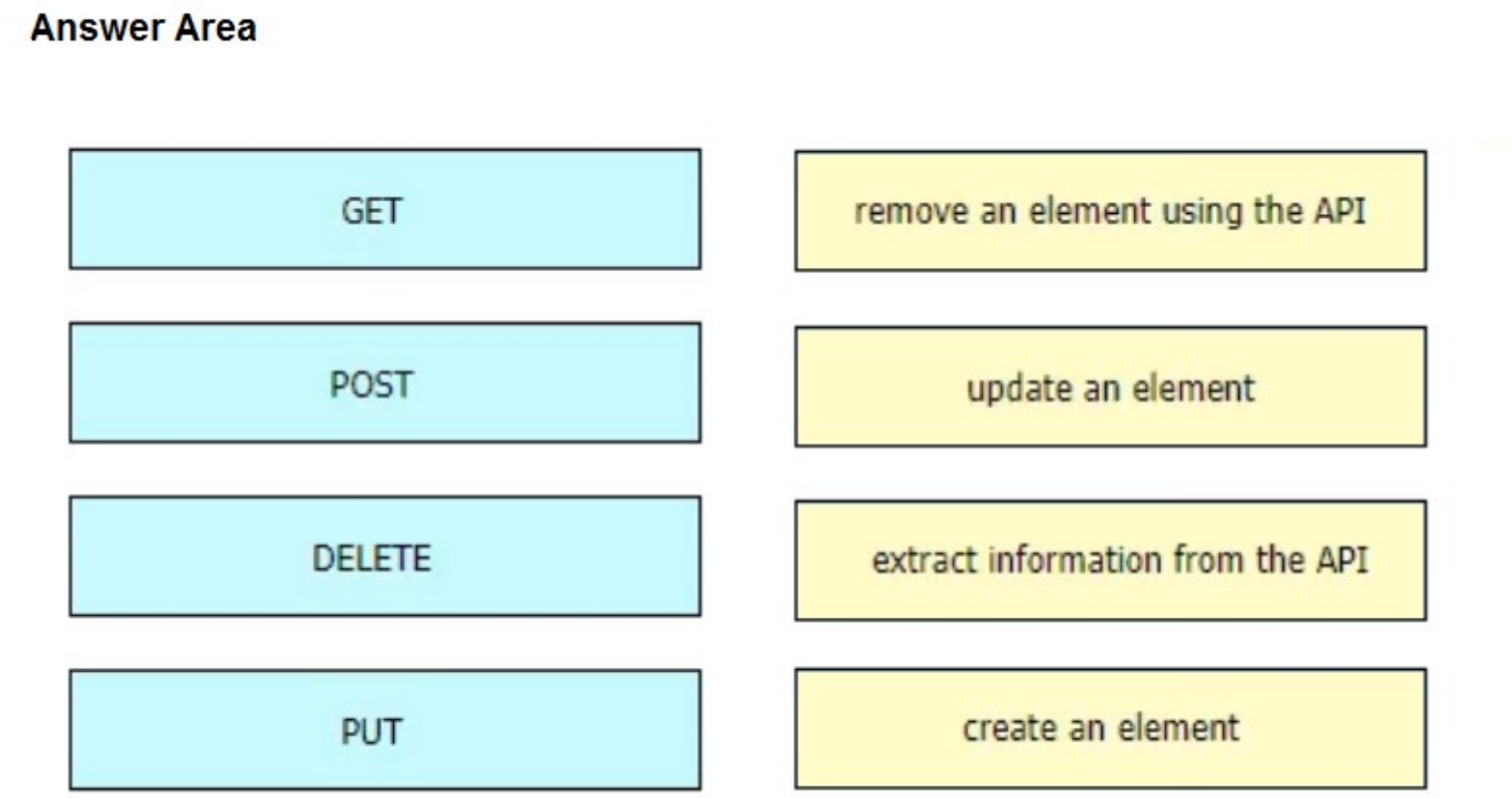
snarkymark 9 months, 4 weeks ago

Correct
https://community.fs.com/blog/eigrp-vs-ospf-differences.html

upvoted 4 times

Question #593 *Topic 1*

DRAG DROP -
An engineer is working with the Cisco DNA Center API. Drag and drop the methods from the left onto the actions that they are used for on the right.
Select and Place:



Correct Answer:

pepgua Highly Voted 1 year, 2 months ago
PUT - update a resource (like adding a new resource to existing one)
POST - create a NEW resource
Provided answer is correct.
upvoted 7 times

Entivo Most Recent 5 months, 2 weeks ago
According to W3, POST and PUT do the same thing. https://www.w3schools.com/tags/ref_httpmethods.asp
upvoted 1 times

Entivo 5 months, 2 weeks ago
although this seems to be slightly different in the context of REST where the PUT method is used when we want to overwrite an existing resource or create a resource. On the other hand, the POST method helps to create a subordinate resource under a collection of resources.
upvoted 1 times

Pilgrim5 7 months ago

Provided Answer is correct 💯

Delete - Remove an element using the API.
Put - Update an element.
Get - Extract information from the API.
Post - Create an element.

upvoted 4 times

Cooldude89 9 months, 2 weeks ago

Given Answer is correct
Del , put ,get,post

upvoted 3 times

MO_2022 11 months, 1 week ago

+ remove an element using the API: DELETE
+ extract information from the API: GET
+ update an element: PUT
+ create an element: POST

upvoted 2 times

Arnaud_R1 1 year, 2 months ago

PUT is used to create an element, POST is used to update

upvoted 1 times

jdholmes423 1 year, 2 months ago

the opposite is true:
https://restfulapi.net/rest-put-vs-post/

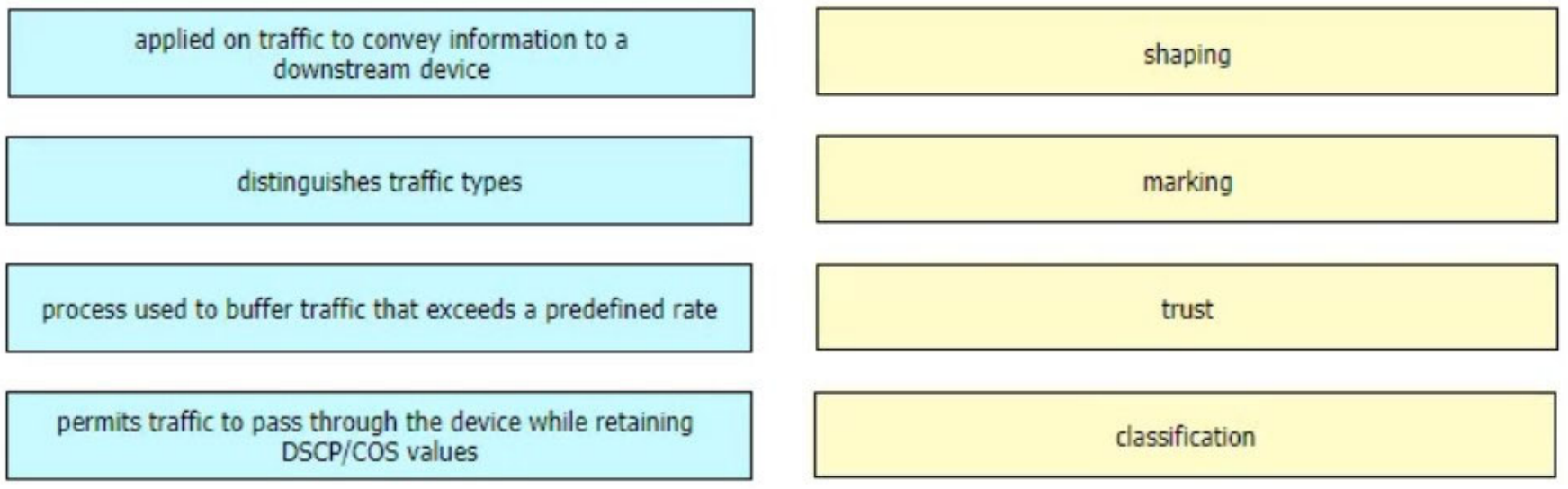
upvoted 11 times

DRAG DROP -

Drag and drop the characteristics from the left onto the QoS components they describe on the right.

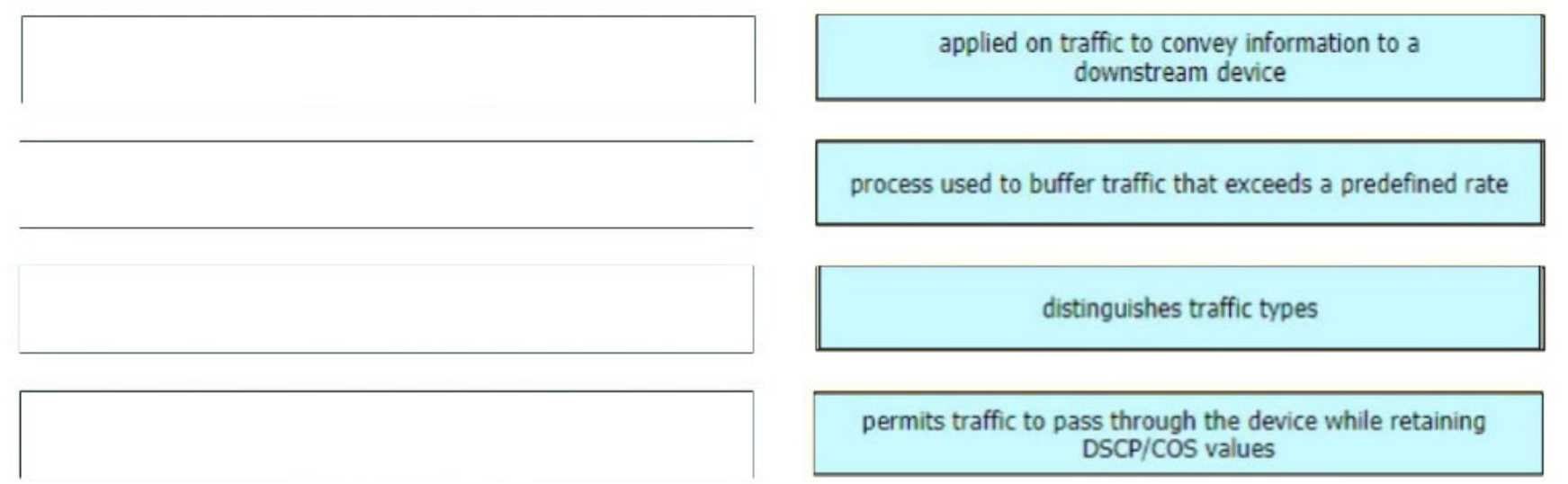
Select and Place:

Answer Area



Correct Answer:

Answer Area



siteoforigin Highly Voted 1 year, 2 months ago

Given Answer is Incorrect.

Shaping - Process used to buffer traffic
Marking - Applied on traffic to convey information to downstream device
Trust - Permits DSCP / CoS values on traffic
Classification - Distinguishes Traffic Types

upvoted 93 times

jdholmes423 1 year, 2 months ago

Agreed.

upvoted 7 times

TSKARAN Highly Voted 10 months, 3 weeks ago

WRONG ANSWER PROVIDED

CORRECT ANSWER
Shaping > Process used to buffer traffic
Marking > Applied on traffic to convey information to downstream device
Trust > Permits DSCP / CoS values on traffic
Classification > Distinguishes Traffic Types

upvoted 8 times

eddgg Most Recent 3 months, 4 weeks ago

incorrect answer

upvoted 1 times

myhdtv6 4 months, 1 week ago

Answers are incorrect

Shaping - Process used to buffer traffic
Marking - Applied on traffic to convey information to downstream device
Trust - Permits DSCP / CoS values on traffic
Classification - Distinguishes Traffic Types

should be like above

upvoted 1 times

MO_2022 11 months, 2 weeks ago

Shaping - Process used to buffer traffic
Marking - Applied on traffic to convey information to downstream device
Trust - Permits DSCP / CoS values on traffic
Classification - Distinguishes Traffic Types

upvoted 4 times

```
CPE# debug ip nat

*Jun 28 19:14:41.463: NAT: Entry assigned id 11
*Jun 28 19:14:41.463: NAT*: s=10.0.1.1->198.51.100.5, d=203.0.113.8 [59922]NAT: dyn flow info
download suppressed for flow 11
*Jun 28 19:14:41.463: NAT*: s=203.0.113.8, d=198.51.100.5->10.0.1.1 [53790]NAT: dyn flow info
download suppressed for flow 11
[...]
*Jun 28 19:14:46.147: NAT: Entry assigned id 13
*Jun 28 19:14:46.147: NAT*: s=10.0.2.1->198.51.100.6, d=203.0.113.8 [60095]NAT: dyn flow info
download suppressed for flow 13
*Jun 28 19:14:46.148: NAT*: s=203.0.113.8, d=198.51.100.6->10.0.2.1 [32109]NAT: dyn flow info
download suppressed for flow 13
[...]
*Jun 28 19:14:50.462: %IPNAT-4-ADDR_ALLOC_FAILURE: Address allocation failed for 10.0.3.1,
pool NAT might be exhausted
*Jun 28 19:14:50.462: NAT: translation failed (A), dropping packet s=10.0.3.1 d=203.0.113.8

CPE# show ip nat translation
Pro Inside global     Inside local   Outside local      Outside global
tcp 198.51.100.5:61082 10.0.1.1:61082  203.0.113.8:23     203.0.113.8:23
--- 198.51.100.5       10.0.1.1        ---                ---
tcp 198.51.100.6:15350 10.0.2.1:15350  203.0.113.8:23     203.0.113.8:23
--- 198.51.100.6       10.0.2.1        ---                ---

CPE# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 234  Misses: 0
CEF Translated packets: 234, CEF Punted packets: 7
Expired translations: 2
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT pool NAT refcount 4
 pool NAT: id 1, netmask 255.255.255.0
    start 198.51.100.5 end 198.51.100.6
    type generic, total addresses 2, allocated 2 (100%), misses 7
nat-limit statistics:
 max entry: max allowed 0, used 0, missed 0
Outside global interfaces count: 1
```

Refer to the exhibit. An administrator troubleshoots intermittent connectivity from internal hosts to an external public server. Some internal hosts can connect to the server while others receive an ICMP Host Unreachable message, and these hosts change over time. What is the cause of this issue?

A. The NAT ACL and NAT pool share the same name.

B. The translation does not use address overloading.

C. The NAT ACL does not match all internal hosts.

D. The NAT pool netmask is excessively wide.

Correct Answer: *B*

Community vote distribution

B (100%)

snarkymark 9 months, 2 weeks ago

Selected Answer: B

Since only 2 NATs in pool, and more then 2 are needed. Then overloading may be the best NAT choice.

upvoted 2 times

Question #596 *Topic 1*

What is the function of the LISP map resolver?

A. to connect a site to the LISP-capable part of a core network publish the EID-to-RLOC mappings for the site, and respond to map-request messages

B. to advertise routable non-LISP traffic from one address family to LISP sites in a different address family

C. to send traffic to non-LISP sites when connected to a service provider that does not accept nonroutable EIDs as packet sources

D. to decapsulate map-request messages from ITRs and forward the messages to the MS

Correct Answer: *D*

Community vote distribution

D (100%)

Tacolicious Highly Voted 1 year ago

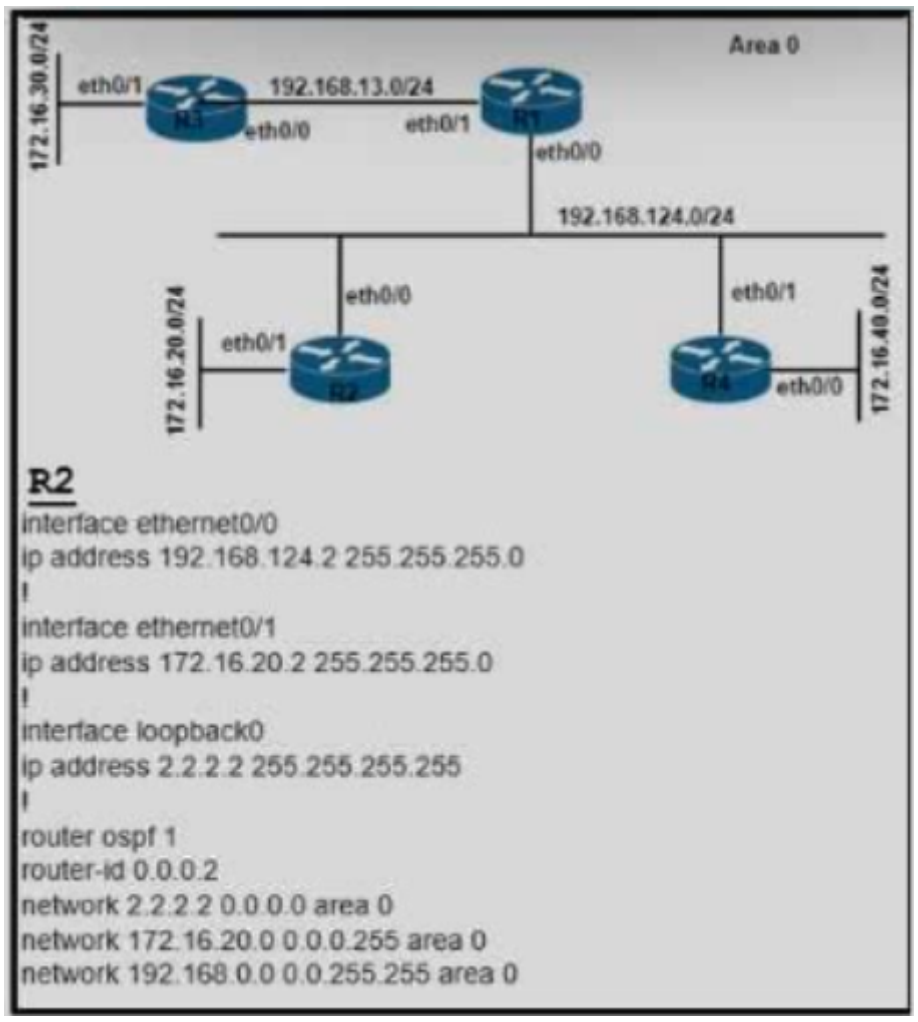
Selected Answer: D

Like an MS, a LISP MR connects to the ALT. The function of the LISP MR is to accept encapsulated Map-Request messages from ingress tunnel routers (ITRs), decapsulate those messages, and then forward the messages to the MS responsible for the egress tunnel routers (ETRs) that are authoritative for the requested EIDs.

When an MR is implemented concurrently with an MS in a private mapping system deployment, the concurrent MS forwards the encapsulated Map-Request messages to the authoritative ETRs. When a LISP ALT is present in the deployment, the MR forwards the Map-Request messages directly over the ALT to the MS responsible for the ETRs that are authoritative for the requested EIDs. An MR also sends Negative Map-Replies to ITRs in response to queries for non-LISP addresses.
source: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html#GUID-89BB8D34-63BF-43DE-8743-5572D357CDB3

upvoted 5 times

Question #597 *Topic 1*



Refer to the exhibit. An attacker can advertise OSPF fake routes from 172.16.20.0 network to the OSPF domain and black hole traffic. Which action must be taken to avoid this attack and still be able to advertise this subnet into OSPF?

A. Configure 172.16.20.0 as a stub network.

B. Configure graceful restart on the 172.16.20.0 interface.

C. Configure a passive interface on R2 toward 172.16.20.0.

D. Apply a policy to filter OSPF packets on R2.

Correct Answer: *D*

Community vote distribution

C (100%)

Brand Highly Voted 9 months, 3 weeks ago

Selected Answer: C

The question itself is the definition of "passive interface"

upvoted 6 times

CCNPWILL Most Recent 1 month, 3 weeks ago

Selected Answer: C

C. Gimme question.

upvoted 1 times

snarkymark 9 months, 3 weeks ago

Agree C,
https://study-ccna.com/ospf-passive-interface/#:~:text=The%20%27passive%2Dinterface%27%20command,interface%20is%20to%20increase%20security.

upvoted 2 times

civan 11 months ago

Selected Answer: C

C. Passive interface means R2 won't form neighbor relationships out that interface, and therefore can't learn routes via that subnet

upvoted 3 times

AndreasThornus 11 months, 3 weeks ago

We labbed this in EVE-NG and setting the interface facing 172.16.20.0/24 does indeed mean this network remains in OSPF but any relationship between a router on that subnet will fail to establish.

C is correct.

upvoted 2 times

milovnik1 11 months, 3 weeks ago

Selected Answer: C

I choose C

upvoted 1 times

forccnp 11 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 2 times

shoo83 1 year ago

agree with passive interface
I choose C

upvoted 2 times

Dataset 1 year ago

Selected Answer: C

i think is C

upvoted 1 times

Darude 1 year ago

Selected Answer: C

reference:
https://networklessons.com/ospf/ospf-passive-interface

upvoted 1 times

testcom680 1 year ago

Selected Answer: C

i choose C

upvoted 1 times

```
DSW2#sh spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID     Priority    4106
              Address     0018.7363.4300
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4106  (priority 4096 sys-id-ext 20)
              Address     0018.7363.4300
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa1/0/7             Desg FWD 2         128.9    P2p Peer(STP)
Fa1/0/10            Desg FWD 4         128.12   P2p Peer(STP)
Fa1/0/11            Desg FWD 2         128.13   P2p Peer(STP)
Fa1/0/12            Desg FWD 2         128.14   P2p Peer(STP)
```

Refer to the exhibit. What is the result when a switch that is running PVST+ is added to this network?

A. Both switches operate in the PVST+ mode.

B. Spanning tree is disabled automatically on the network.

C. Both switches operate in the Rapid PVST+ mode.

D. DSW2 operates in Rapid PVST + and the new switch operates in PVST+.

Correct Answer: *D*

Community vote distribution

D (87%) 13%

HungarianDish Highly Voted 10 months, 1 week ago

Selected Answer: D

This seems to be a frequent topic in cisco forums.
DSW2 is not going to switch to PVST+ mode, only the affected interfaces are going to adjust their behavior to the old style PVST+ device.

The output shows that DSW2 runs "protocol rstp" i.e. cisco rapid-pvst+,
whereas the new switch (connected to DSW2) runs PVST+. Hence we see "P2p Peer(STP)" under "Type".

Source: https://ccie2012.wordpress.com/2011/12/27/what-p2p-peerstp-means-in-the-show-spanning-tree-output/

"The RPVST+ switch should detect that the other switch is running PVST+ by the incoming BPDUs.
It would then revert to sending 802.1D BPDUs on that interface and rely on timers instead of synchronization."

Source: https://community.cisco.com/t5/switching/rstp-rapid-pvst-compatibility/td-p/2400863

"An RSTP bridge that receives an STP BPDU know that it's connected to a legacy device and start sending STP BPDUs itself.
This mechanism will happen on a per-vlan basis with Cisco PVST/Rapid-PVST."

Source: https://community.cisco.com/t5/switching/mix-pvst-and-rstp/td-p/1345045

upvoted 8 times

tom_novotny Highly Voted 11 months, 3 weeks ago

I think it is A = the RSTP one downgrades to PVST+ so both run PVST+ now.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-3/configuration_guide/lyr2/b_173_lyr2_9500_cg/configuring_spanning_tree_protocol.html#spanning-tree-interoperability-backward-compatibility

upvoted 7 times

bendarkel Most Recent 9 months, 2 weeks ago

Selected Answer: D

D is the correct answer. Rapid PVST+ is backwards compatible with PVST.

upvoted 1 times

MO_2022 11 months, 1 week ago

Selected Answer: D

From the output we see DSW2 is running in RSTP mode (in fact Rapid PVST+ mode as Cisco does not support RSTP alone). When a new switch running PVST+ mode is added to the topology, they keep running the old STP instances as RSTP (in fact Rapid PVST+) is compatible with PVST+.

upvoted 3 times

dnjJ56 11 months, 1 week ago

Selected Answer: A

Tested in LAB.
Just on that shared interface both switches run PVST+.
Switch runs RSTP on other interfaces.

upvoted 1 times

nushadu 11 months, 1 week ago

Selected Answer: D

sw1#show spanning-tree vlan 10 detail | i compat
VLAN0010 is executing the rstp compatible Spanning Tree protocol
sw1#
!!!!!!!!!! sw1 [Rapid PVST +] <---> sw2 [PVST +]
sw2#show spanning-tree vlan 10 detail | i compat
VLAN0010 is executing the ieee compatible Spanning Tree protocol
sw2#

upvoted 1 times

nushadu 11 months, 3 weeks ago

D. looks true, but not sure ...

sw1#
sw1#sh runn | include spann
spanning-tree mode pvst
spanning-tree extend system-id
sw1#
sw1#show spanning-tree

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 24577
Address aabb.cc00.4000
Cost 100
Port 66 (Port-channel2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address aabb.cc00.1000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/3 Desg FWD 100 128.4 Shr
Po2 Root FWD 100 128.66 Shr

upvoted 1 times

nushadu 11 months, 3 weeks ago

sw2 is root and RPVST mode:

sw2#show spanning-tree

VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 24577
Address aabb.cc00.4000
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24577 (priority 24576 sys-id-ext 1)
Address aabb.cc00.4000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Et0/0 Desg FWD 100 128.1 Shr
Et0/2 Desg FWD 100 128.3 Shr
Et0/3 Desg FWD 100 128.4 Shr
Po2 Desg FWD 100 128.65 Shr Peer(STP)

sw2#sh runn | include spann
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
sw2#

upvoted 1 times

bora4motion 11 months, 3 weeks ago

Selected Answer: A

A looks OK to me.

upvoted 1 times

bora4motion 11 months, 2 weeks ago

So I say A because as I know STP will negotiate and run the slowest version running between the two switches,

upvoted 1 times

Question #599 *Topic 1*

Which protocol is responsible for data plane forwarding in a Cisco SD-Access deployment?

A. IS-IS

B. OSPF

C. VXLAN

D. LISP

Correct Answer: *C*

Community vote distribution

C (100%)

GeorgeFortiGate 10 months ago

Selected Answer: C

The control plane is based on Locator/ID Separation Protocol (LISP), the data plane is based on Virtual Extensible LAN (VXLAN), the policy plane is based on Cisco TrustSec and the management plane is enabled and powered by Cisco DNA
Center.

upvoted 3 times

Question #600 *Topic 1*

```
import requests
import json

url='https://switchIP.foo.com/ins'
switchuser='username'
switchpassword='password123'

myheaders={'content-type':'application/json-rpc'}
payload=[
 {
  "jsonrpc": "2.0",
  "method": "cli",
  "params": {
   "cmd": "show clock",
   "version": 1
  },
  "id": 1
 }
]
response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword), verify=False).json()
```

Refer to the exhibit. Which Python code parses the response and prints "18:32:21.474 UTC Sun Mar 10 2019"?

A. print(response['result'][0]('simple_time'])

B. print(response['result']['body']('simple_time'])

C. print(response['body']['simple_time'])

D. print(response['jsonrpc']['body']['simple_time'])

Correct Answer: *B*

Community vote distribution

B (100%)

nushadu Highly Voted 11 months, 1 week ago

Jesus, why does Cisco ask for programming language skills?

upvoted 28 times

Asymptote 10 months, 3 weeks ago

becasue it is almost the end of the 350-401,
there will be lot more programming question in the coming new CCNP CORE this Fall maybe.

upvoted 6 times

Alondrix 3 weeks, 6 days ago

And, because the days of the CLI network engineer are coming to an end. We have no choice, learn the new skills or you will age yourself out of the market.

upvoted 1 times

MJane Highly Voted 11 months ago

it's not even programming language skills, it's to learn by heart their API, WHO does that?

upvoted 18 times

adamzet33 Most Recent 2 weeks, 5 days ago

print(response['result']['body']['simple_time']), with corrected parenthesis

upvoted 1 times

eww_cybr 4 months, 3 weeks ago

Selected Answer: B

{
"jsonrpc": "2.0",
"result": {
"body": {
"simple_time": "12:31:02.686 UTC Wed Jul 10 2019\n",
"time_source": "NTP"
}
}

upvoted 3 times

Alondrix 3 weeks, 6 days ago

Is this to imply the format of the payload in the comment is wrong and should be replaced with this? I think 'yes', but no context to this post. There is no 'simple_time' to parse in the posted file. Your answer would make more sense as the result to parse.

upvoted 1 times

[Removed] 4 months, 4 weeks ago

This question is dumb.... This is suppose to be a Cisco Network Professional, not a Programmer. This should be in the DevCore.

upvoted 3 times

mgiuseppe86 2 months, 2 weeks ago

A lot of questions in this test are dumb. Gone are the days of a route/switch/tshoot jocky. Welcome to Cloud, WiFi, JSON, API

The art of core networking is becoming lost.

upvoted 1 times

dragonwise 7 months, 4 weeks ago

I don't know man. I think this question should be in 350-901 DEVCOR exam

upvoted 3 times

SheldonC 10 months, 2 weeks ago

@M_B
The Options are altered. The option that should be there is:
#. print(response['result']['body']['simple_time'])

upvoted 4 times

M_B 10 months, 3 weeks ago

I am not a python expert, but A and B seem to have bad syntax as the number of brackets, open and close, do not match. Based on the post by ZiZu007, I would say the answer is D

upvoted 2 times

Zizu007 1 year ago

Selected Answer: B

B is almost 100% correct, should be
response['result']['body']['simple_time']
{
"jsonrpc": "2.0",
"result": {
"body": {
"simple_time": "17:53:49.435 UTC Tue Nov 22 2022\n",
"time_source": "NTP"
}
},
"id": 1
}

upvoted 9 times

Question #601 *Topic 1*

```
switch > enable
switch # configure terminal
switch(config)# interface GigabitEthernet 1/10
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 10,20,30
switch(config-if)# exit
switch (config)# monitor session 1 type erspan-source
 switch(config-mon-erspan-src)# description source1
 switch(config-mon-erspan-src)# source vlan 10
 switch(config-mon-erspan-src)# source vlan 20
 switch(config-mon-erspan-src)# filter vlan 30
 switch(config-mon-erspan-src)# destination
 switch(config-mon-erspan-src-dst)# erspan-id 100
 switch(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
 switch(config-mon-erspan-src-dst)# ip prec 5
 switch(config-mon-erspan-src-dst)# ip ttl 32
 switch(config-mon-erspan-src-dst)# mtu 1500
 switch(config-mon-erspan-src-dst)# ip address 10.10.0.1
 switch(config-mon-erspan-src-dst)# vrf 1
 switch(config-mon-erspan-src-dst)# no shutdown
 switch(config-mon-erspan-src-dst)# end
```

Refer to the exhibit. An engineer configures the trunk and proceeds to configure an ESPAN session to monitor VLANs 10, 20, and 30. Which command must be added to complete this configuration?

A. Device(config-mon-erspan-src-dst)# no vrf 1

B. Device(config-mon-erspan-src)# no filter vlan 30

C. Device(config-mon-erspan-src-dst)# mtu 1460

D. Device(config-mon-erspan-src-dst}# erspan-id 6

Correct Answer: *A*

Community vote distribution

B (100%)

Huntkey Highly Voted 1 year ago

Selected Answer: B

You cannot include source VLANs and filter VLANs in the same session
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-5/configuration_guide/nmgmt/b_165_nmgmt_3850_cg/b_165_nmgmt_3850_cg_chapter_0111.pdf

upvoted 9 times

rogue_user Most Recent 4 months, 2 weeks ago

Selected Answer: B

B is best since you can't mix "source VLAN" and "filter VLAN", but it also requires "source vlan 30" after you remove "filter". SMH Cisco.

upvoted 4 times

Symirnian 9 months ago

I think question is mistyped. It claims to VLANs 10, 20 and filter out 30. Then the answer changes to no VRF 1, right?

upvoted 2 times

snarkymark 9 months, 3 weeks ago

Agree B,
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/nmgmt/b_166_nmgmt_9400_cg/b_166_nmgmt_9400_cg_chapter_01000.pdf

upvoted 1 times

iEpsilon 1 year ago

Selected Answer: B

".....An engineer configures the trunk and proceeds to configure an ESPAN session to monitor VLANs 10, 20, and 30"

upvoted 2 times

testcom680 1 year ago

Selected Answer: B

I'll go for B since vlan 30 is supposed to be monitored

upvoted 4 times

Question #602 *Topic 1*

An administrator is configuring NETCONF using the following XML string. What must the administrator end the request with?

<?xml version="1.0" encoding="UTF-8" ?>
<rpc message-id="9.0">

A. </rpc>]]>]]>

B. <rpc message-id="9.0"><notification-off/>

C. </rpc-reply>

D. </rpc>

Correct Answer: *A*

Community vote distribution

A (100%)

Darude Highly Voted 1 year ago

Selected Answer: A

Provided answer is correct:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cns/configuration/xe-16/cns-xe-16-book/cns-netconf.html

upvoted 11 times

HarwinderSekhon Highly Voted 5 months, 2 weeks ago

Thanks @Darude for the link.
"All NETCONF requests must end with]]>]]> which denotes an end to the request. Until the]]>]]> sequence is sent, the device will not process the request."

upvoted 6 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago

This question will make me a better Network Administrator when architecting and building routers and switches

F off Cisco

upvoted 4 times

Question #603 *Topic 1*

Which Python snippet should be used to store the devices data structure in a JSON file?

```
import json
Devices = {'Switches': [{'name': 'AccSw1',
                         'ip': '2001:db8:4308:3884:3::1'},
                         {'name': 'AccSw2',
                         'ip':'2001:db8:12b1:31a7:fffe::2'}],
           'Routers': [{'name': 'CE1', 'ip': '2001:db8:31ac:a97a:8::1'},
                         {'name': 'CE2', 'ip': '2001:db8:7ac8:9ab7::2'}
                         ]
}
```

A.
```
OutFile = open("devices.json", "w")
json.dump(Devices, OutFile)
OutFile.close()
```

B.
```
OutFile = open("devices.json", "w")
OutFile.write(str(Devices))
OutFile.close()
```

C.
```
with open("devices.json", "w") as OutFile:
  json.dumps(Devices)
```

D.
```
with open("devices.json", "w") as OutFile:
  Devices = json.load(OutFile)
```

Correct Answer: *C*

Community vote distribution

A (84%) Other

Darude Highly Voted 1 year ago

Selected Answer: A

reference:
https://www.section.io/engineering-education/storing-data-in-python-using-json-module/

upvoted 11 times

andresga20 Most Recent 3 months, 1 week ago

Selected Answer: A

Tested all 4 of them on Visual Studio Code:
A: works, right answer
B: does not work properly, it just copies the data without making sure the formatting is good for json files
C: creates an empty file
D: errors out, the syntax is not right

upvoted 1 times

dapardo 3 months, 2 weeks ago

Selected Answer: A

I will go with A considering the differences between json.dump and json.dumps https://www.geeksforgeeks.org/python-difference-between-json-dump-and-json-dumps/

upvoted 1 times

eddgg 3 months, 3 weeks ago

Selected Answer: A

the main difference is that outfile.write(str(devices)) writes the string representation of the data directly to the file, while outfile.dump(devices, outfile) uses serialization to write the data in a specific format (e.g., JSON, YAML) to the file, preserving its original data structure and types

upvoted 1 times

teikitiz 4 months, 2 weeks ago

Selected Answer: A

"Devices" is already a dict, which prompts dump as the tool to write a file.

upvoted 1 times

msstanick 5 months, 2 weeks ago

Selected Answer: B

I got it tested - the correct one is B.

Explanation
A: Incorrect, there is no such a thing like json.dumb - there is a missing 's' -> dumbs
B: Correct, worked fine on my py script. str(Devices) is doig the same thing as json.dumbs in this case - it is casting dict to str type

C: Incorrect, the outcomes are not put into a file. It would have worked if it was OutFile.write(json.dumbs(Devices))
D: Incorrect, not only are we not putting anything into a file but it is also trting to change dicto to a dict which would cause an error
upvoted 2 times

Burik 5 months ago

Actually both json.dump() and json.dumps() are valid Python methods, only slightly different.

https://www.geeksforgeeks.org/json-dump-in-python/
https://www.geeksforgeeks.org/json-dumps-in-python/

Thing is, in the version of this question as shown here, both A and B will work. An alternative dump of this question shows A as wrong because it says OutFile.Close(), with an uppercase C, which is not a valid Python method.

If you've been using json.dumb [lol?] of course it will throw an error because it doesn't exist as a method.
upvoted 1 times

snarkymark 9 months, 3 weeks ago

Choosing A.
https://www.section.io/engineering-education/storing-data-in-python-using-json-module/
upvoted 2 times

mask_n_sorrow 10 months, 2 weeks ago

Selected Answer: C

Option A didn't work as you can see
>>> import json
>>> devices = {'switch':'blah',
... 'router':'ddd'
... }
>>> outfile = open("devices.json",w)
Traceback (most recent call last):
File "<stdin>", line 1, in <module>
NameError: name 'w' is not defined
>>> with open("devices.json","w") as outfile:
... json.dumps(devices)
File "<stdin>", line 2
json.dumps(devices)
^
IndentationError: expected an indented block
>>> with open("devices.json","w") as outfile:
... json.dumps(devices)
...
'{"switch": "blah", "router": "ddd"}'
>>>
upvoted 1 times

ImFran 10 months, 1 week ago

in your test """ >>> outfile = open("devices.json",w) """ you forgot to put quotation marks around w...
upvoted 2 times

nushadu 10 months, 3 weeks ago

Guys, what version of Python they used in the scripts?
upvoted 1 times

milovnik1 11 months, 3 weeks ago

Selected Answer: A

A is correct, the same configuration can be found in multiple examples here:
https://www.geeksforgeeks.org/json-dump-in-python/
upvoted 3 times

dancott 12 months ago

Selected Answer: C

https://www.section.io/engineering-education/storing-data-in-python-using-json-module/#:~:text=Using%20json.,-dumps()&text=dumps()%20can%20be%20used,object%20into%20a%20JSON%20string.&text=dumps(data)-,The%20json.,be%20converted%20into%20JSON%20string.
upvoted 1 times

testcom680 1 year ago

Selected Answer: A

I'll go for A
upvoted 3 times

Question #604 *Topic 1*

A large campus network has deployed two wireless LAN controllers to manage the wireless network WLC1 and WLC2 have been configured as mobility peers. A client device roams from AP1 on WLC1 to AP2 on WLC2, but the controller's client interfaces are on different VLANs. How do the wireless LAN controllers handle the inter-subnet roaming?

A. WLC1 marks the client with an anchor entry in its own database. The database entry is copied to the new controller and marked with a foreign entry on WLC2.

B. WLC2 marks the client with an anchor entry in its own database. The database entry is copied to the new controller and marked with a foreign entry on WLC1.

C. WLC1 marks the client with a foreign entry in its own database. The database entry is copied to the new controller and marked with an anchor entry on WLC2.

D. WLC2 marks the client with a foreign entry in its own database. The database entry is copied to the new controller and marked with an anchor entry on WLC1.

Correct Answer: *B*

Community vote distribution

A (100%)

Darude Highly Voted 1 year ago

Selected Answer: A

Inter-subnet roaming is similar to inter-controller roaming in that the controllers exchange mobility messages on the client roam. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains transparent to the wireless client, and the client maintains its original IP address.
reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-3/configuration/guide/b_cg73/b_wlc-cg_chapter_01111.html

upvoted 8 times

HarwinderSekhon Most Recent 5 months, 2 weeks ago

Selected Answer: A

A is the correct answer

upvoted 1 times

mohammaduzzalmollah 8 months, 4 weeks ago

A is the correct answer

upvoted 1 times

asiansensation 9 months, 2 weeks ago

A is the correct answer

upvoted 1 times

Ciscopass 1 year ago

Selected Answer: A

A is the correct answer

upvoted 1 times

iEpsilon 1 year ago

Selected Answer: A

A is the correct answer

upvoted 1 times

testcom680 1 year ago

Selected Answer: A

I pick A too

upvoted 1 times

Tacolicious 1 year ago

Selected Answer: A

https://rscciew.wordpress.com/2014/07/10/layer-3-inter-controller-roaming/

answer seems to be A

upvoted 2 times

Question #605 *Topic 1*

By default, which virtual MAC address does HSRP group 25 use?

A. 04:30:83:88:4c:19

B. 00:00:0c:07:ac:25

C. 05:5c:5e:ac:0c:25

D. 00:00:0c:07:ac:19

Correct Answer: *B*

Community vote distribution

D (100%)

mgiuseppe86 2 months, 2 weeks ago

25 = 00011001 = 0001|1001 = 19

upvoted 3 times

SemStrond 4 months, 3 weeks ago

Selected Answer: D

Correct D

upvoted 2 times

bullett00th 8 months, 1 week ago

Selected Answer: D

25 in HEX is 19 - so D is correct.

upvoted 1 times

Vlad_Is_Love_ua 8 months, 3 weeks ago

Selected Answer: D

Vlan100 - Group 25
State is Listen
5 state changes, last state change 00:08:37
Virtual IP address is 192.168.1.201
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0C07.AC19 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.180 secs
Preemption disabled
Active router is unknown
Standby router is unknown
Priority 100 (default 100)
Group name is hsrp-Vl1-25 (default)

upvoted 2 times

mellohello 9 months, 1 week ago

Selected Answer: D

25 = 0001 1001
0001 = 1
1001 = 9
by adding both numbers togehter we will get 19.

upvoted 2 times

Vlad_Is_Love_ua 9 months, 3 weeks ago

Selected Answer: D

The IP address and the corresponding MAC address of the virtual router are maintained in the ARP table of the active router in an HSRP group.

The HSRP MAC address is in the following format: 0000.0c07.acXX, where XX is the HSRP group number converted from decimal to hexadecimal. Clients utilize this MAC address to forward data.

R2(config)# interface ethernet 0/1
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)# standby 1 ip 192.168.1.1

R1# show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.1 - 0000.0c07.ac01 ARPA Ethernet0/1
Internet 192.168.1.2 - aabb.cc01.ba10 ARPA Ethernet0/1
Internet 192.168.1.3 50 aabb.cc01.bb10 ARPA Ethernet0/1

Internet 192.168.2.1 - aabb.cc01.ba00 ARPA Ethernet0/0
Internet 192.168.2.2 51 aabb.cc01.bc00 ARPA Ethernet0/0

upvoted 1 times

ricaela10 11 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

Dataset 1 year ago

Selected Answer: D

D is corretc
19 in hex is 25
Regards

upvoted 2 times

Dataset 1 year ago

sorry
19hex = 26 dec

upvoted 1 times

Dataset 1 year ago

25 jajajajajaja

upvoted 1 times

diamant 1 year ago

https://www.rapidtables.com/convert/number/hex-to-decimal.html
$(19)_{16} = (1 \times 16^1) + (9 \times 16^0) = (25)_{10}$

upvoted 2 times

testcom680 1 year ago

Selected Answer: D

same, going with D

upvoted 3 times

scarface35 1 year ago

Selected Answer: D

The correct answer is D

upvoted 3 times

Redzero07 1 year ago

Selected Answer: D

The correct answer is D

upvoted 3 times

Question #606 *Topic 1*

In a Cisco Catalyst switch equipped with two supervisor modules an administrator must temporarily remove the active supervisor from the chassis to perform hardware maintenance on it. Which mechanism ensures that the active supervisor removal is not disruptive to the network operation?

A. VRRP

B. HSRP

C. NSF/NSR

D. SSO

Correct Answer: *D*

Community vote distribution

D (70%) C (30%)

Adnan5252 3 months ago

What cisco thinks ...i mean asking half Questions with no reference if you want us say SSO you should mention layer 2 And if you want us to say NSR And NSf so mention in the Question meaning what they are trying to doing i dont know ....confusing at exam who ever make this exhibet need to be fired ...

upvoted 2 times

djedeen 3 months, 2 weeks ago

Selected Answer: D

SSO .....

upvoted 1 times

rogue_user 4 months, 2 weeks ago

Selected Answer: D

SSO since you can you it gracefully and you won't need NSF/NSR for that which are required only when RE fails abruptly

upvoted 1 times

rogue_user 4 months, 2 weeks ago

key word is "removal" not fault

upvoted 1 times

[Removed] 4 months, 4 weeks ago

Selected Answer: C

Which mechanism ensures that the active supervisor removal is not disruptive to the NETWORK operation?

Cisco is about semantics. it specifically asks about the NETWORK operation, which should immediately put your engineer brains thinking routing protocols.

SSO is a feature that allows a Standby RP taking over the and prevent some problems, but LAYER 3 disruption is not one of them. In fact, the OCG specifically says that during the switchover, the "routing protocol adjacency" flaps and "clears the route table", this then causes the CEF entries to be purged and at that point "traffic is no longer routed until routes are re-learned"

To avoid this situation, NSF/NSR needs to be enabled, this allows the router to "maintain the CEF entries for a short duration and continue forwarding packets through an RP failure until the control plane recovers".

The answer is C) NSF/NSR

upvoted 2 times

Chiaretta 7 months ago

Selected Answer: D

Statefull Switch Over is the right answer. SSO

upvoted 3 times

ttl2000 4 months, 3 weeks ago

need NSR to be non-disruptive

upvoted 2 times

rogue_user 4 months, 2 weeks ago

not if you do it gracefully

upvoted 1 times

XDR 7 months, 1 week ago

Selected Answer: C

C and D are OK, but the technology which minimizes downtime is NSF.

upvoted 1 times

Chiaretta 8 months ago

Selected Answer: D

D is correct

upvoted 2 times

JackDRipper 8 months, 1 week ago

Selected Answer: D

Both C and D could be correct answers. But, gun to my head, I'm going with D. SSO is the fundamental technology that allows this. NSF requires SSO.

upvoted 4 times

snarkymark 9 months, 3 weeks ago

Again, the problem is the wording of the question, IMO. If you need L3 to continue to function without interruption, then you need NSF/NSR. Really its C and D. https://www.routeprotocol.com/stateful-switchover/

upvoted 3 times

landgar 10 months ago

Selected Answer: C

C. NSF provides layer 3 redundancy. SSO only synchronization and layer 2 redundancy.
https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/stck_mgr_ha/b_166_nsf_sso_9400_cg.html#concept_gds_jmy_31b

upvoted 3 times

Nickplayany 11 months ago

Selected Answer: D

SSO is the answer, we have similar question before....

upvoted 3 times

dogdoglee 12 months ago

Selected Answer: D

D. remove the active supervisor from the chassis

upvoted 3 times

Huntkey 1 year ago

Selected Answer: C

Sso will take over the control plane but adjacency could drop and packers could be lost. NSF is to prevent disruption I think

upvoted 1 times

kalbos 1 year ago

Selected Answer: D

SSOenables the standby RP to take over if the active RP fails
I'll go with D

upvoted 2 times

Darude 1 year ago

Selected Answer: C

I go with C. NSF= non stop forwarding NSR = non stop routing SSO is layer2 only it will drop all layer 3 connections.

reference:
https://www.ciscopress.com/articles/article.asp?p=1395746&seqNum=2
https://www.ciscopress.com/articles/article.asp?p=1395746&seqNum=2

upvoted 1 times

Darude 1 year ago

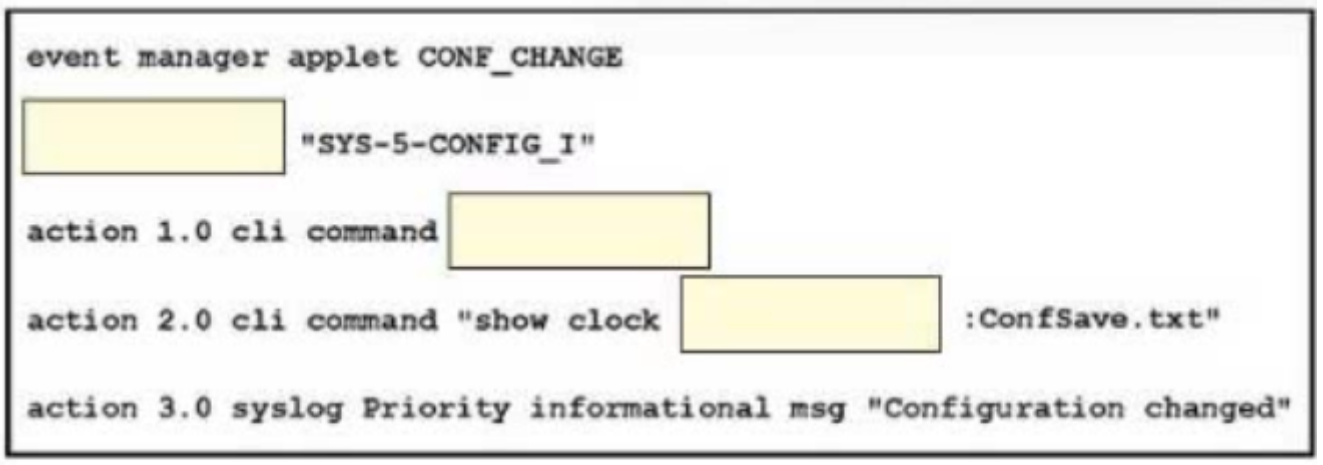
Sorry guys correct answer is D because NSF goes allways with SSO.
reference: https://community.cisco.com/t5/switching/difference-between-nsf-and-sso/td-p/2262550

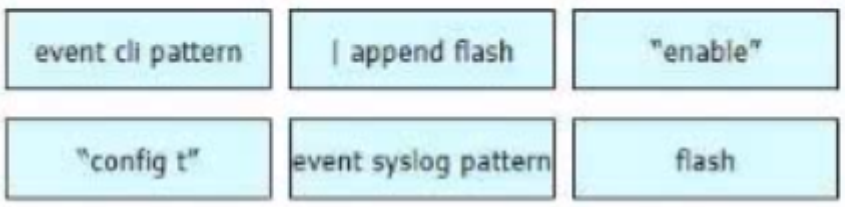
upvoted 5 times

Question #607 *Topic 1*

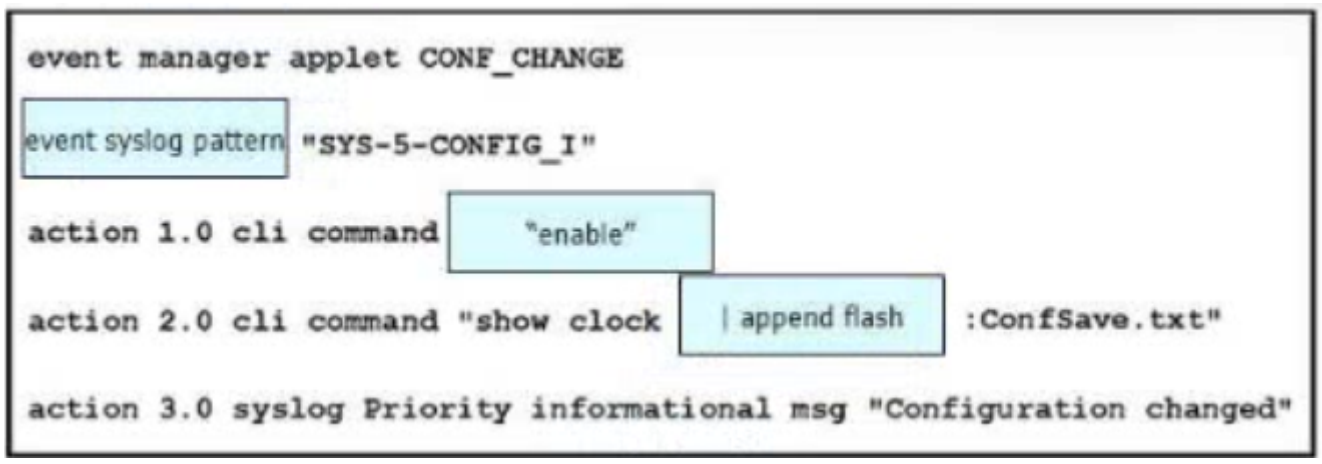
DRAG DROP -

Drag and drop the snippets onto the blanks within the code to create an EEM script that adds an entry to a locally stored text file with a timestamp when a configuration change is made. Not all options are used.





Correct Answer:



nushadu Highly Voted 11 months, 2 weeks ago

yes, technically it works:
!
event manager applet CONF_CHANGE
event syslog pattern "SYS-5-CONFIG_I"
action 1.0 cli command "enable"
action 2.0 cli command "show clock | append flash:confsave.txt"
action 3.0 syslog priority informational msg "Configuration changed"
!

upvoted 9 times

papagussepi Most Recent 4 months, 1 week ago

As it says add an entry when a configuration change is made, should the second answer be "config t" instead on "enable".

upvoted 4 times

Zizu007 1 year ago

provided answer is correct.

upvoted 4 times

AndreasThornus 11 months, 3 weeks ago

Thanks

upvoted 3 times

Question #608 *Topic 1*

Which function does a fabric AP perform in a Cisco SD-Access deployment?

A. It updates wireless clients' locations in the fabric.

B. It connects wireless clients to the fabric.

C. It manages wireless clients' membership information in the fabric.

D. It configures security policies down to wireless clients in the fabric.

Correct Answer: *B*

Community vote distribution

B (100%)

CCNPWILL 1 month, 3 weeks ago

B .. no derp.

upvoted 1 times

snarkymark 9 months ago

Selected Answer: B

https://www.routeprotocol.com/sd-access-fabric-wireless-controller-wlc/

upvoted 1 times

ihateciscoreally 4 months ago

question is about AP, not WLC

upvoted 1 times

Question #609 *Topic 1*

```
flow monitor FLOW-MONITOR-1
 record netflow ipv6 original-input
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet 0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
!
```

Refer to the exhibit. What is the effect of introducing the sampler feature into the Flexible NetFlow configuration on the router?

A. NetFlow updates to the collector are sent 50% less frequently.

B. Every second IPv4 packet is forwarded to the collector for inspection.

C. CPU and memory utilization are reduced when compared with what is required for full NetFlow.

D. The resolution of sampling data increases, but it requires more performance from the router.

Correct Answer: *C*

Community vote distribution

C (69%) A (31%)

AndreasThornus Highly Voted 11 months, 3 weeks ago

Selected Answer: C

"Flow sampling reduces the CPU overhead of analyzing traffic with Flexible NetFlow by reducing the number of packets that are analyzed."

Taken from:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/xe-3se/3850/use-fnflow-redce-cpu.html

upvoted 6 times

eddgg Most Recent 3 months, 3 weeks ago

Selected Answer: C

i will choose c

upvoted 1 times

byallmeans 6 months, 4 weeks ago

Why not B?

upvoted 1 times

wd457 6 months, 1 week ago

Interface uses IPv6 not IPv4.

upvoted 4 times

nushadu 11 months, 2 weeks ago

C. correct, on ISP core PE use 1:1000 or 1:5000 sampling to detect DDOS attacks for Arbor collectors.
A. is wrong because the router sends flow when the current flow is finished (you can think TCP session) or when the session is UP but the flow timer is expired - the router sends every 10 min. flow data to the collector by default ...

upvoted 2 times

iGlitch 1 year ago

Selected Answer: C

C is the answer, it's about what record the router is analyzing and not about what is been sent to the collector.

upvoted 2 times

testcom680 1 year ago

Selected Answer: A

I'll pick A

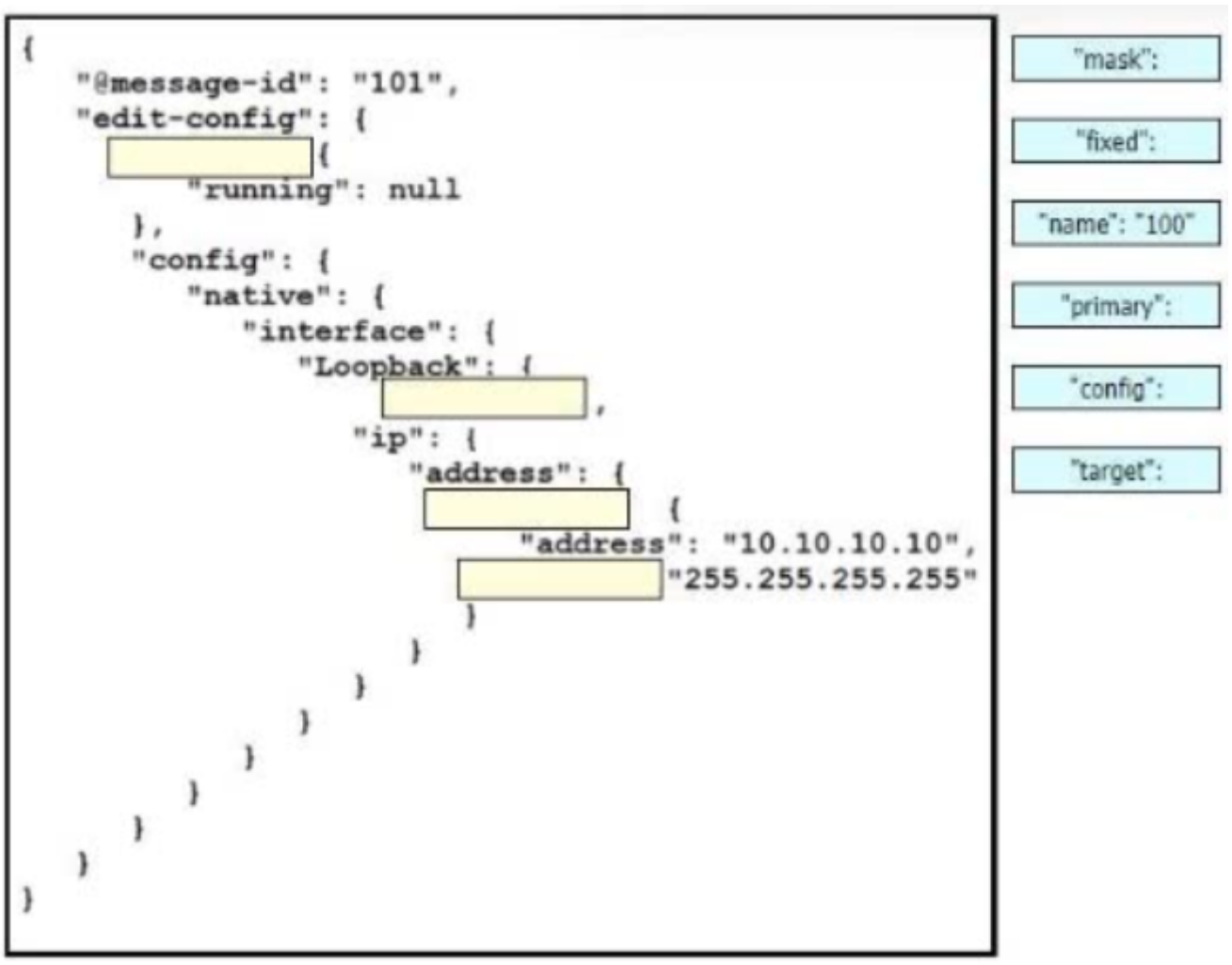
upvoted 4 times

Question #610 *Topic 1*

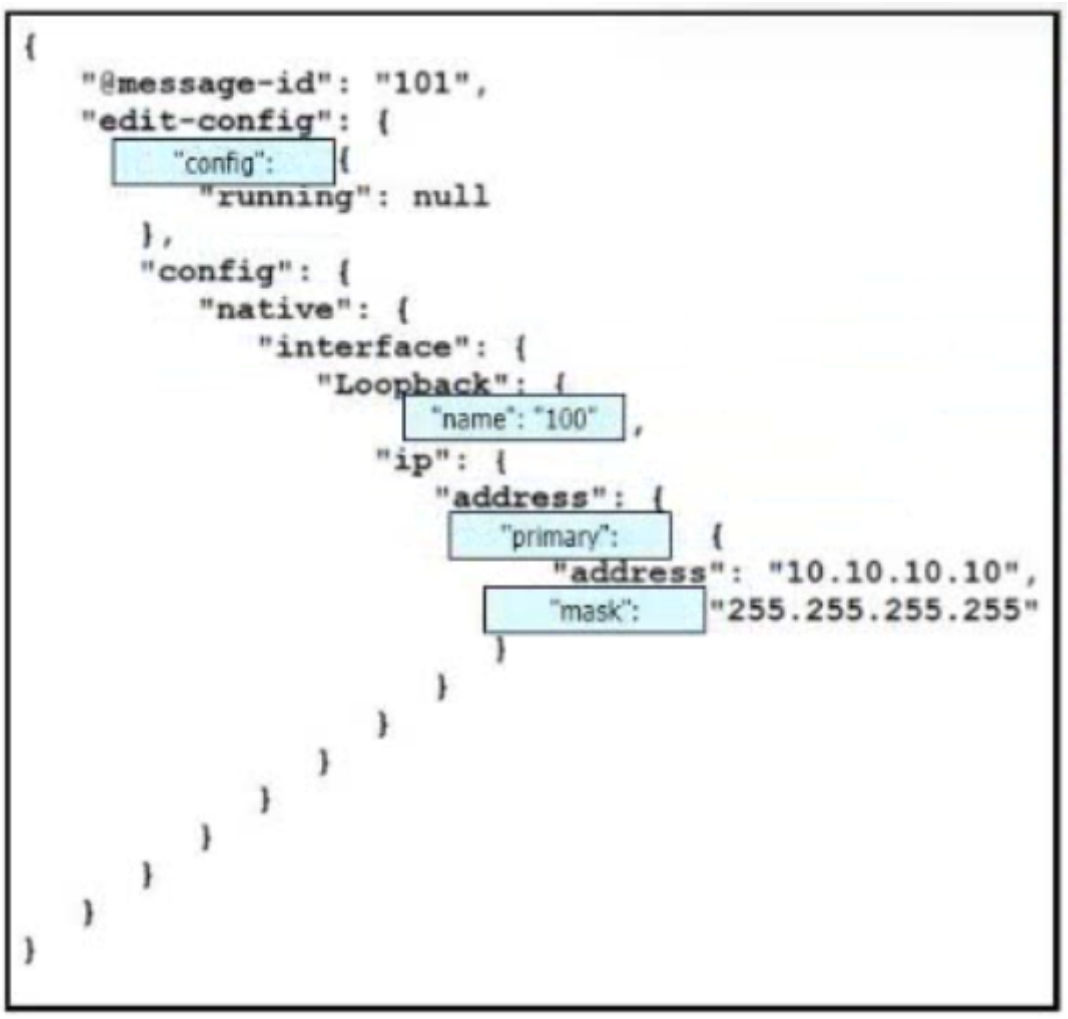
DRAG DROP

-

Drag and drop the snippets onto the blanks within the code to construct a script that configures a loopback interface with an IP address. Not all options are used.



Correct Answer:



iGlitch Highly Voted 1 year ago

Wrong, should be:
1 - target.
2- name:100.
3- primary.
4- mask.

upvoted 48 times

mmt1mmt1 Most Recent 5 months, 1 week ago

Can someone provide an explanation please?
Which one is correct, the official one, or the one what iGlitch provided?

upvoted 1 times

jubrilak 5 months, 1 week ago

iGlitch is correct.2. "target": Specifies the target datastore for the configuration change. In this example, we target the "running" datastore.

{
"edit-config": {
"target": {
"running": {}
},
"config": {
"native": {
"interface": {
"Loopback": {
"name": "0",
"ip": {
"address": {
"primary": {
"address": "192.168.0.1",
"mask": "255.255.255.0"
} }}}}}}}

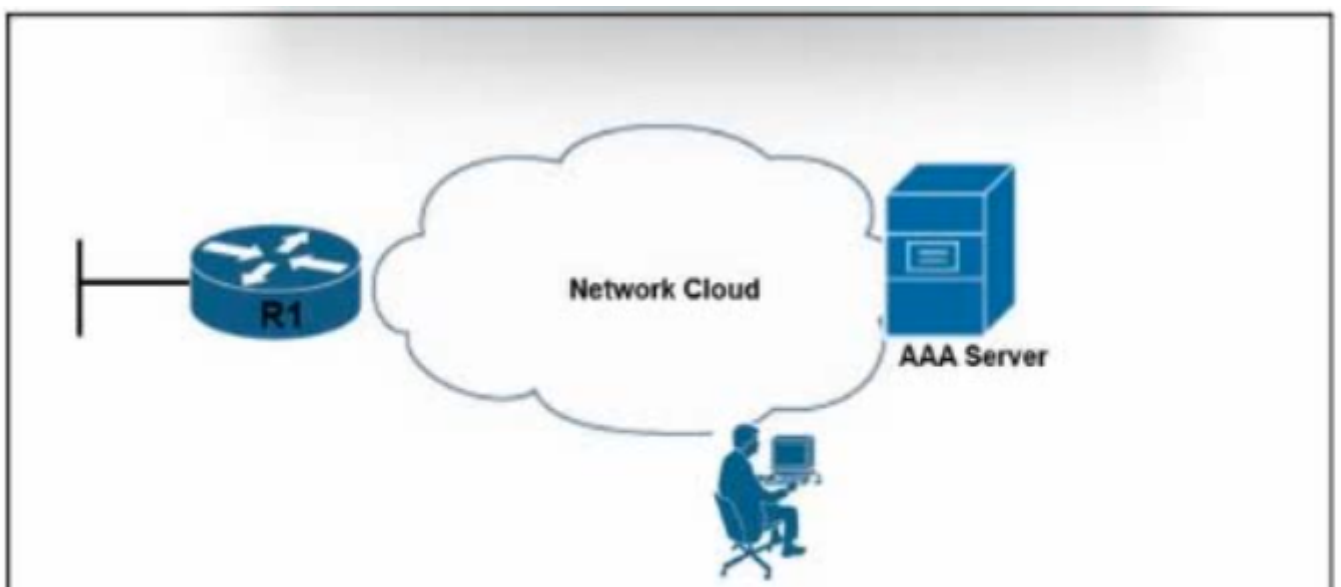
upvoted 4 times

[Removed] 4 months, 4 weeks ago

thank you, I appreciate you taking time to explain. I dont know why people do not rebuke further than "WRONG!"

upvoted 1 times

Question #611 *Topic 1*




```
Router1$ ssh -s admin@192.168.20.3 -p 830 netconf
admin@192.168.20.3's password: cisco123

<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
<capability>urn:ietf:params:netconf:base:1.1</capability>
<capability>urn:ietf:params:netconf:capability:writable-
running:1.0</capability>
<capability>urn:ietf:params:netconf:capability:xpath:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.1</capability>
<capability>urn:ietf:params:netconf:capability:rollback-on-
error:1.0</capability
--snip--
</capabilities>
<session-id>2870</session-id></ hello>]]>]]>

Use < ^C > to exit
```

A. R1# aaa new-model
aaa authorization exec default local
enable aaa admin privilege 15

B. R1#username admin privilege 15
aaa authorization exec default local
netconf-yang

C. R1#netconf-yang
username admin privilege 15 secret cisco123
aaa new-model
aaa authorization exec default local

D. R1# username admin privilege 15
aaa authorization exec default local

Correct Answer: *B*

Community vote distribution

C (100%)

MO_2022 Highly Voted 11 months, 2 weeks ago

An engineer tries to log in to router R1. Which configuration enables a successful login?

upvoted 27 times

JochenStacker 3 months, 3 weeks ago

Can confirm this from another dump.

upvoted 2 times

iEpsilon Highly Voted 1 year ago

Selected Answer: C

Provided answer is not correct, because you cannot use "aaa" unless you create aaa new-model.
https://www.cisco.com/c/en/us/support/docs/storage-networking/management/200933-YANG-NETCONF-Configuration-Validation.html#:~:text=Configure-,1.%20Basic%20Configuration%20of%20a%20Catalyst%203850%20Running%20IOS%2DXE%2016.3.3%20Software%20to%20Support%20NETCONF/YANG%20Data%20Modeling,-3850%2D1%23

upvoted 15 times

AndreasThornus 11 months, 3 weeks ago

The link here is excellent but to my mind suggests D assuming we are using a minimal config, you can configure AAA to use a local database as per the text below. This matches D.

"If it is desired to enable AAA (authentication, authorization, and accounting) by configuring "aaa new-model" then this configuration is also required at a minimum. You can also expand this to use AAA with a TACACS+ or RADIUS configuration but this is beyond the scope of this example.

aaa new-model
aaa authorization exec default local ----------> Required for NETCONF-SSH connectivity and edit-config op"

upvoted 1 times

Tacolicious 1 year ago

Don't know what the question is, but the example is taken from your link and the config of C seems to line up with Step 1, so i'm inclined to agree with you.

upvoted 1 times

CCNPWILL Most Recent 1 month, 3 weeks ago

You see netconf/XML output and the only answer choice dealing with netconf yang is C ... Gimme question guys.

upvoted 1 times

djedeen 3 months, 1 week ago

Selected Answer: C

C:
global cmd 'netconf-yang' is required for NETCONF/YANG support, good description at the link:
https://networkop.co.uk/blog/2017/01/25/netconf-intro/

upvoted 1 times

Vip44000 6 months ago

The moderator should take acton to fix wrong answers.
We didn't payed for so many wrong answers in this dump

upvoted 11 times

Cesar12345 6 months ago

Selected Answer: C

https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html#anc15 says that until aaa-new model is used other aaa commands are hidden.

upvoted 1 times

dancott 11 months, 3 weeks ago

Looks like the question is missing?

upvoted 5 times

Tacolicious 1 year ago

Selected Answer: C

I think it's C, See iEpsilon's comment

upvoted 2 times

```
ip sla 100
 udp-echo 10.10.10.15 6336
 frequency 30
```

Refer to the exhibit. An engineer has configured an IP SLA for UDP echos. Which command is needed to start the IP SLA to lest every 30 seconds and continue until stopped?

A. ip sla schedule 100 life forever

B. ip sla schedule 30 start-time now life forever

C. ip sla schedule 100 start-time now life 30

D. ip sla schedule 100 start-time now life forever

Correct Answer: *C*

Community vote distribution

D (100%)

Huntkey Highly Voted 1 year ago

Selected Answer: D

Frequency 30 already sends it every 30 seconds

upvoted 11 times

Hosein Most Recent 5 months, 1 week ago

Selected Answer: D

already set to send every 30sec

upvoted 1 times

Burik 5 months, 3 weeks ago

Selected Answer: D

Why the proper answer to this question hasn't been updated in 6 months?

upvoted 4 times

Splashisthegreatestmovie 5 months, 2 weeks ago

because they already have your money. At least we have the comments. The comments are gold

upvoted 8 times

JochenStacker 3 months, 3 weeks ago

Quite frankly the content here is very good for the money you pay.
You want the most accurate and up to date dumps?
Then don't be a cheapskate and go to SPOTO and pay them 400 bucks.

upvoted 1 times

CCNPWILL 1 month, 3 weeks ago

If they got the CCIE LAB then its worth the 400....

upvoted 1 times

adrian0792 5 months, 4 weeks ago

D. ip sla schedule 100 start-time now life forever
Is correct

upvoted 1 times

Clauster 8 months, 3 weeks ago

Selected Answer: D

Answer is 100% D
Moderator please update.

upvoted 2 times

nushadu 11 months, 2 weeks ago

D.
cisco#sh runn | section ip sla
ip sla 1

udp-echo 10.10.10.15 6336
frequency 30
ip sla schedule 1 life forever start-time now
cisco#
cisco#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID Type Destination Stats Return Last
(ms) Code Run
---
*1 udp-echo 10.10.10.15 - No connecti 25 seconds ag
on o
cisco#

upvoted 3 times

AndreasThornus 11 months, 3 weeks ago

Selected Answer: D

Confirmed on the CLI that there is no mention of frequency in the scheduler statement. It's when you want it to start, i.e. "now" and how long you want it to live - "forever".

upvoted 4 times

Tacolicious 1 year ago

Selected Answer: D

C is incorrect: https://www.cisco.com/c/en/us/td/docs/ios/ipsla/command/reference/sla_book/sla_02.html

(Optional) Specifies the number of seconds the IP SLAs operations will actively collect information. The default is 3600 (one hour).

it has to be D, because B references the wrong SLA, and A doesn't actually start it

upvoted 2 times

iGlitch 1 year ago

Selected Answer: D

100% the answer is D.

upvoted 2 times

Ciscopass 1 year ago

Selected Answer: D

I would pick D

upvoted 2 times

Question #613 *Topic 1*

What is the calculation that is used to measure the radiated power of a signal after it has gone through the radio, antenna cable, and antenna?

A. mW

B. ERIP

C. dBm

D. dBi

Correct Answer: *B*

Community vote distribution

B (100%)

Dataset Highly Voted 1 year ago

Selected Answer: B

Correct but Its EIRP (Effective Isotroppic Radiated Power)
Regards

upvoted 9 times

MO_2022 Most Recent 11 months, 2 weeks ago

Correct but Its EIRP

upvoted 3 times

Question #614 *Topic 1*

Which Quality of Service (QoS) mechanism is used to identify traffic flow and to use DSCP, IP Precedence values, and MPLS EXP bits to create different priority levels?

A. Policing

B. Marking

C. Queueing

D. Classification

Correct Answer: *D*

Community vote distribution

D (49%) B (44%) 7%

Pilgrim5 Highly Voted 6 months, 3 weeks ago

Selected Answer: D

I go with D because the key sentence here is "to create different priority levels?"

Yes marking adds bits to packets inorder to identify them, however it doesn't create different priority levels.

upvoted 5 times

dragonwise Highly Voted 7 months, 4 weeks ago

Selected Answer: B

Answer is B
When we talk about DSCP, IPP and packet headers, then it's marking

But, when we talk about traffic nature, and categories like S/D IP addresses, and port number, then it's classification

upvoted 5 times

byallmeans 6 months, 4 weeks ago

It specifically says "identify", so most likely classification.
If it was saying "sets" or "marks" - that would be marking.

D seems to be the correct answer

upvoted 1 times

CCNPWILL Most Recent 1 month, 3 weeks ago

Selected Answer: D

Classification. D

Because my gut got me through multiple exams already.

upvoted 1 times

Soggyt74 3 months, 2 weeks ago

Selected Answer: B

Packet marking is a QoS mechanism that colors a packet by changing a field within a packet or a frame header with a traffic descriptor so it is distinguished from other packets during the application of other QoS mechanisms (such as re-marking, policing, queuing, or congestion avoidance).

Packet classification is a QoS mechanism responsible for distinguishing between different traffic streams. It uses traffic descriptors to categorize an IP packet within a specific class. Packet classification should take place at the network edge, as close to the source of the traffic as possible. Once an IP packet is classified, packets can then be marked/re-marked, queued, policed, shaped, or any combination of these and other actions.

CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide page 368-369

upvoted 1 times

jhonmeikel 3 months, 3 weeks ago

Selected Answer: B

classification is the process of grouping traffic flows together, while marking is the process of identifying individual packets within those traffic flows.
Classification is the process of identifying traffic flows based on their characteristics, such as their source and destination addresses, their port numbers, and their type of traffic. This allows network administrators to group traffic flows together so that they can be treated differently by the network.
Marking is the process of adding a label to packets that identifies the traffic flow to which they belong. This label is used by the network to

determine how the packet should be treated. For example, a packet that is marked with a high priority label will be forwarded ahead of packets that are marked with a lower priority label.

upvoted 1 times

andyforreg 4 months, 2 weeks ago

Selected Answer: B

Marking

upvoted 1 times

rogue_user 4 months, 2 weeks ago

Selected Answer: D

To me identify=classification

upvoted 2 times

Entivo 4 months, 4 weeks ago

Selected Answer: B

The answer is 100% marking according to Cisco OCG page 369.

upvoted 1 times

HarwinderSekhon 5 months ago

Selected Answer: D

"identify traffic flow and to use DSCP, IP Precedence values"

upvoted 2 times

Burik 5 months, 2 weeks ago

"Network devices use classification to identify IP traffic as belonging to a specific class."
OCG p368

upvoted 2 times

bk989 7 months, 1 week ago

page 368 of Encor OCG says it is classification.

upvoted 2 times

MJane 7 months, 2 weeks ago

Selected Answer: D

classification identifies.

upvoted 4 times

jackr76 8 months, 1 week ago

Selected Answer: B

Packet Marking (Marking Network Traffic)--Packet marking allows you to differentiate packets by designating them different identifying values. For example, you can mark packets by setting the IP Precedence bits or the IP differentiated services code point (DSCP) in the type of service (ToS) byte.

upvoted 2 times

eojedad 8 months, 3 weeks ago

Selected Answer: B

marking

upvoted 2 times

mellohello 9 months, 1 week ago

Selected Answer: D

Classification

upvoted 1 times

snarkymark 9 months, 3 weeks ago

Classification is distinguishing what kind of traffic is it.
Marking, is setting or changing it.
Read the dos Rose66 provides link to.

upvoted 1 times

snarkymark 9 months, 3 weeks ago

So, agree, D

upvoted 1 times

landgar 10 months ago

Selected Answer: D

D: traffic classification based on their QoS (IP TOS, MPLS EXP), to put it in several buffers with different treatment

upvoted 1 times

Question #615 *Topic 1*

What are two valid modes that Cisco Express Forwarding can operate in? (Choose two.)

A. Central CEF mode

B. Dense CEF mode

C. Sparse CEF mode

D. Distributed CEF mode

E. Routed CEF mode

Correct Answer: *AD*

Community vote distribution

AD (100%)

Tacolicious Highly Voted 1 year ago

Selected Answer: AD

CEF can be enabled in one of two modes:

Central CEF mode - When CEF mode is enabled, the CEF FIB and adjacency tables reside on the route processor, and the route processor performs the express forwarding. You can use CEF mode when line cards are not available for CEF switching, or when you need to use features not compatible with distributed CEF switching.

Distributed CEF (dCEF) mode - When dCEF is enabled, line cards maintain identical copies of the FIB and adjacency tables. The line cards can perform the express forwarding by themselves, and this relieves the main processor - Gigabit Route Processor (GRP) - of involvement in the switching operation. This is the only switching method available on the Cisco 12000 Series Router.

https://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html

upvoted 17 times

ConqiD 2 weeks, 4 days ago

Excellent explanation, thank you!

upvoted 1 times

Question #616 *Topic 1*

You need to weigh the pros and cons of deploying a premise-based data center versus using a cloud-based data center deployment. What is an advantage of using a premise-based solution? (Choose two.)

A. Lower application latency for end users

B. Easily scalable

C. Lower capital costs

D. Reduced deployment times

E. Increased control over the environment

Correct Answer: *AE*

Community vote distribution

AE (100%)

Ira 3 months, 3 weeks ago

AE is correct

upvoted 1 times

Tacolicious 1 year ago

Selected Answer: AE

AE sounds like the only two correct-ish answers in this one, but A is kinda debatable since especially with Work from home culture / VPN's, it doesn't really matter anymore since you'd always connect either to on-prem, or to a cloud environment.

upvoted 4 times

AndreasThornus 11 months, 3 weeks ago

I believe you are correct. Every other On-Prem vs Cloud deployment question in the deck refers to On-Premise being lower latency and control over the hardware/security.

upvoted 1 times

Question #617 *Topic 1*

Which Quality of Service (QoS) mechanism allows for the creation of multiple levels of QoS policy, providing a more granular degree of traffic management?

A. Policing

B. H-QoS

C. Congestion avoidance

D. Dual Policy

Correct Answer: *B*

Community vote distribution

B (100%)

AndreasThornus Highly Voted 11 months, 3 weeks ago

Selected Answer: B

Hierarchical QoS allows you to specify QoS behavior at multiple policy levels, which provides a high degree of granularity in traffic management. A hierarchical policy is a QoS model that enables you to specify QoS behavior at multiple levels of hierarchy.

From: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-2/qos/configuration/guide/qc42hqos.html#wp1236859

upvoted 8 times

Huntkey Most Recent 1 year ago

Selected Answer: B

Hierarchical QoS (H-QoS)

upvoted 3 times

Question #618 *Topic 1*

Which Quality of Service (QoS) mechanism allows the network administrator to control the maximum rate of traffic received or sent on a given interface?

A. Policing

B. Marking

C. Queueing

D. Classification

Correct Answer: *A*

Community vote distribution

A (100%)

mgiuseppe86 2 months, 2 weeks ago

Selected Answer: A

Finally, a QoS answer everyone can agree on. unlike question 615.

upvoted 1 times

Jebrony 11 months, 3 weeks ago

Selected Answer: A

Traffic Policing

In general, traffic policing allows you to control the maximum rate of traffic sent or received on an interface and to partition a network into multiple priority levels or class of service (CoS).

upvoted 2 times

Question #619 *Topic 1*

Refer to the following two images regarding QoS Traffic Shaping and Traffic Policing:

Image A:

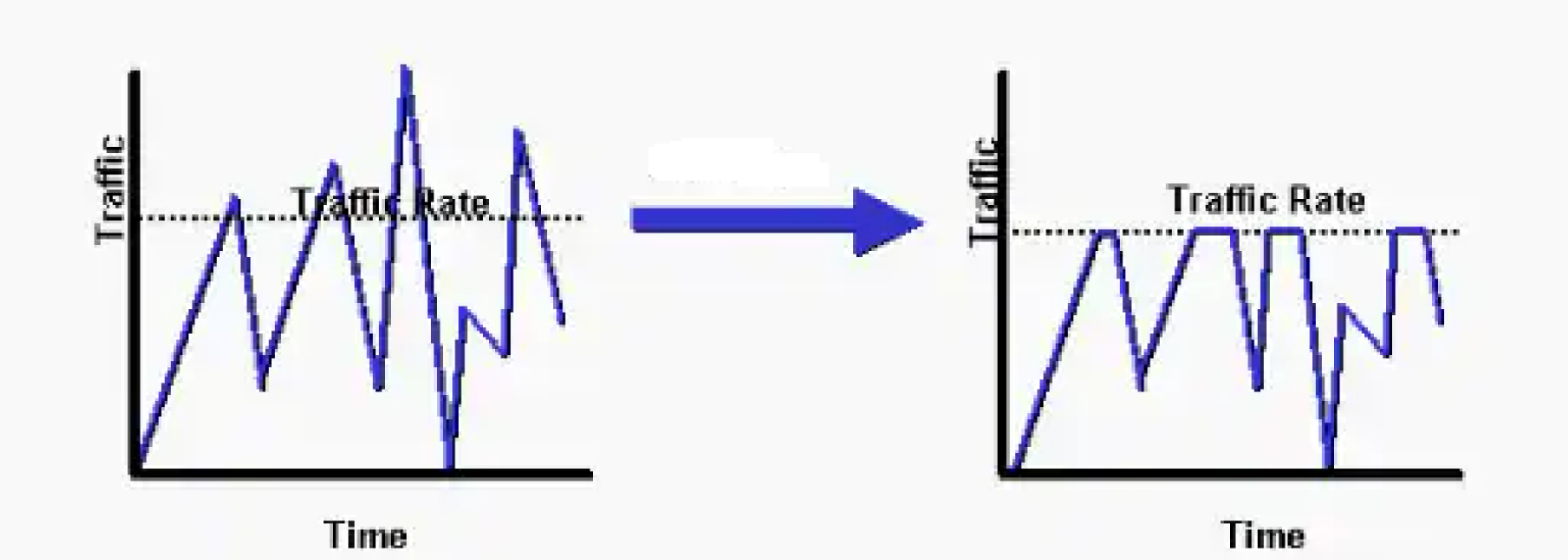
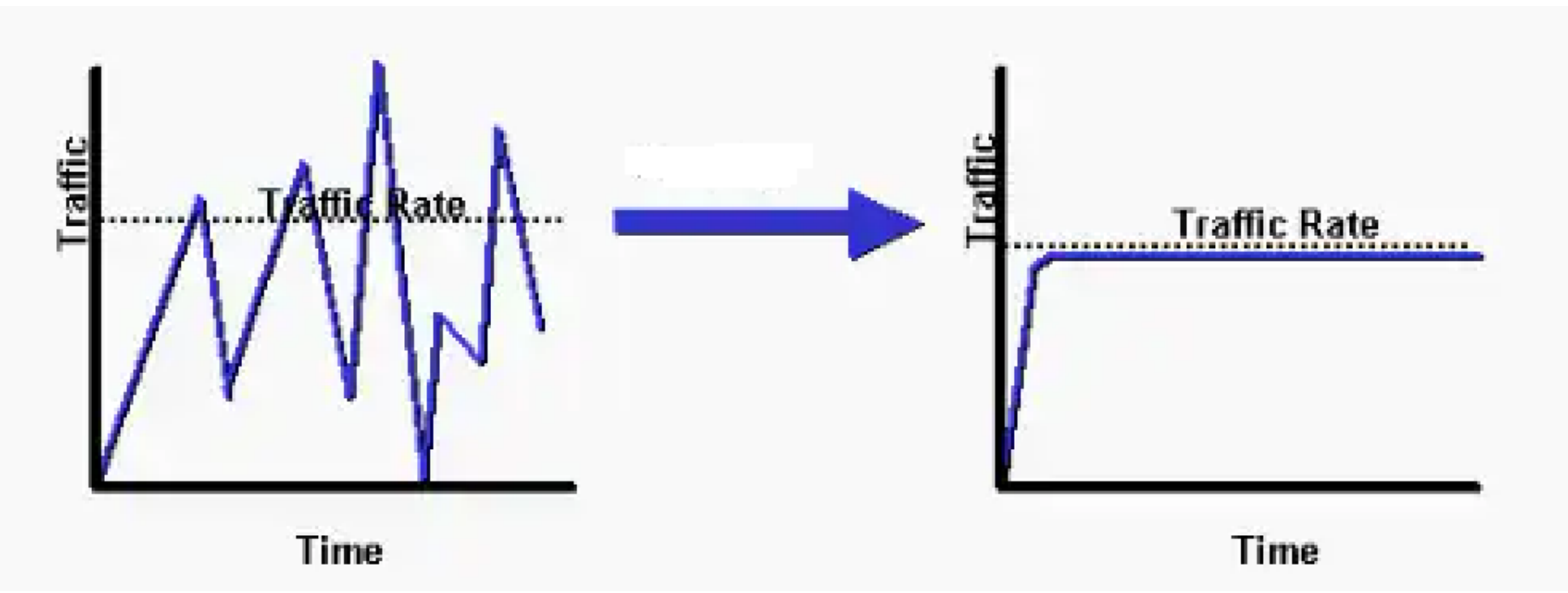


Image B:



Based on the images, which of the following are true? (Choose two.)

A. Image A depicts the result of Traffic Shaping

B. Image A depicts the result of Traffic Policing

C. Image B depicts the result of Traffic Shaping

D. Image B depicts the result of Traffic Policing

Correct Answer: *BC*

Community vote distribution

BC (100%)

Cooldude89 9 months, 2 weeks ago

Selected Answer: BC

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

upvoted 2 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: BC

B and C are fine
Shaping always uses Buffers, while Policing drops packets.
upvoted 3 times

Ioannis34 10 months, 4 weeks ago

Selected Answer: BC

BC are correct
upvoted 1 times

Darude 1 year ago

Selected Answer: BC

correct
reference:https://www.cisco.com/c/it_it/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html
upvoted 2 times

Tacolicious 1 year ago

Selected Answer: BC

Answers provided are correct
upvoted 1 times

Question #620 *Topic 1*

In a Cisco SD-Access fabric architecture, which of the following are valid device roles (Choose three.)

A. Control Plane Node

B. Access routing device

C. Edge Node

D. Border Node

E. Distributed Node

Correct Answer: *ACD*

snarkymark 9 months, 3 weeks ago

ACD Correct,
https://www.cisco.com/c/dam/m/hr_hr/training-events/2019/cisco-connect/pdf/VH-Cisco-SD-Access-Connecting.pdf
upvoted 4 times

Question #621 *Topic 1*

Which of the following are valid statements when configuring Nonstop Forwarding (NSF) with Stateful Switchover (SSO) on a Cisco device? (Choose two.)

A. supports multicast routing protocols

B. Supports IPv4 and IPv6

C. Nonstop Forwarding requires SSO to also be configured

D. HSRP is not supported with NSF/SSO

E. Improper implementation of NSF/SSO can result in routing loops

Correct Answer: *CD*

Community vote distribution

CD (100%)

Huntkey Highly Voted 1 year ago

Selected Answer: CD

NSF capability is supported for IPv4 routing protocols only. NSF capability is not supported for IPv6 routing protocols.
NSF does not support IP Multicast Routing, as it is not SSO-aware.
You must configure SSO in order to use NSF with any supported protocol.
The Hot Standby Routing Protocol (HSRP) is not supported with NSF SSO. Do not use HSRP with NSF SSO.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/stck_mgr_ha/b_166_nsf_sso_9400_cg.html

upvoted 14 times

TSKARAN Highly Voted 10 months, 3 weeks ago

Restrictions for Cisco Nonstop Forwarding with Stateful Switchover
The following are restrictions for configuring NSF with SSO:

NSF capability is supported for IPv4 routing protocols only. NSF capability is not supported for IPv6 routing protocols.

NSF does not support IP Multicast Routing, as it is not SSO-aware.

For NSF operation, you must have SSO configured on the device.

All Layer 3 neighboring devices must be an NSF helper or NSF-capable to support graceful restart capability.

For IETF, all neighboring devices must be running an NSF-aware software image.

The Hot Standby Routing Protocol (HSRP) is not supported with NSF SSO. Do not use HSRP with NSF SSO.

An NSF-aware device cannot support two NSF-capable peers performing an NSF restart operation at the same time. However, both neighbors can reestablish peering sessions after the NSF restart operation is complete.

For SSO operation, ensure that both active and standby devices run the same version of the Cisco IOS XE image. If the active and standby devices are operating different images, SSO failover might cause an outage.

upvoted 6 times

Question #622 *Topic 1*

In a Cisco SD-Access wireless network, which device is used as an entry and exit point in and out of the fabric?

A. fabric edge node

B. control plane node

C. fabric border node

D. fabric access points

Correct Answer: *C*

Community vote distribution

C (64%) D (33%) %

cjk3 Highly Voted 11 months, 1 week ago

Selected Answer: C

See slide 12.
Answer C - Border Node
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2825.pdf

upvoted 9 times

ImFran 9 months ago

Seems to be wrong. The question says "SD-access wireless" . The right document is : https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf and the answer D

upvoted 5 times

PKamato 7 months, 1 week ago

ehm.. the document states "• There are two types of fabric border nodes: border and default border nodes. Both types provide the fundamental routing entry
and exit point for all data traffic going into or out of the fabric overlay, as well as for VN and/or group-based policy enforcement (for traffic outside the fabric)" so it's C

upvoted 4 times

mellohello 9 months, 1 week ago

Thanks.

upvoted 1 times

Clauster Highly Voted 8 months, 1 week ago

Selected Answer: C

SUPER Confusing question but i will decipher it for you:
The answer is 100% C and here's why:

Here is a question for you:
What is one fact about Cisco SD-Access wireless network infrastructure deployments?
A. The access point is part of the fabric overlay. < Correct
B. The wireless client is part of the fabric overlay.
C. The access point is part of the fabric underlay.
D. The WLC is part of the fabric underlay

So this means Wireless Clients ARE NOT PART OF THE Wireless FABRIC. So if they are not part of the Fabric which Device do they use to enter the Fabric ? = (The AP). Which device do they use to Exit the Fabric ? It cannot be the AP because they use it to enter it. (The only device that a client can use to exit the Fabric is a Border Router)
You're welcome :)

upvoted 7 times

NewLife77 3 months ago

The WLC is part of the underlay but the AP is part of the overlay.

upvoted 1 times

NewLife77 Most Recent 3 months ago

Selected Answer: D

The question specifically uses the work wireless. Thats a hint.

upvoted 1 times

NewLife77 3 months ago

The question specifically uses the word "wireless" thus the answer is access point.

upvoted 2 times

djedeen 3 months, 1 week ago

Selected Answer: C

c: A fabric border node is required to allow traffic to egress and ingress the fabric site
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.pdf

upvoted 1 times

andyforreg 4 months, 2 weeks ago

Selected Answer: C

Border Node - 100%

upvoted 1 times

helmerpach 5 months, 2 weeks ago

my answer: C

upvoted 2 times

JackyChon 6 months, 3 weeks ago

Selected Answer: C

In a Cisco SD-Access wireless network, the device that serves as an entry and exit point in and out of the fabric is called a Border Node (BN). The Border Node is responsible for connecting the SD-Access fabric to external networks, such as the Internet or other non-fabric networks.

upvoted 1 times

Clauster 8 months ago

Selected Answer: C

Answer is C.
Answer can be found here:
https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf
On Page 7

upvoted 1 times

Clauster 8 months, 3 weeks ago

Selected Answer: D

In an SD-Access Wireless Deployment the Access Points are part of the Fabric, so the second traffic hits the AP you are already in the Fabric, when traffic goes from Network to the Client it traverses the AP as an exit point into the client. In and Out. Answer is D

upvoted 1 times

snarkymark 9 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/sda_fabric_troubleshooting/b_cisco_sda_fabric_troubleshooting_guide.html

upvoted 1 times

snarkymark 9 months ago

Meant to select C, sprry my bad.

upvoted 1 times

snarkymark 9 months, 2 weeks ago

Selected Answer: C

https://community.cisco.com/t5/networking-knowledge-base/guide-to-choosing-sd-access-sda-border-roles-in-cisco-dnac-1-3/ta-p/3889472

upvoted 1 times

laeppli 9 months, 4 weeks ago

"out of the fabric" is key. Another simple question with a sneaky wording

upvoted 2 times

eff3 10 months ago

Selected Answer: C

As per usual wording I go with C. Because an EIP has access to the fabric and a Border-Node is the entry

upvoted 1 times

Kasia1992 10 months ago

Selected Answer: C

I understand how some people may say AP is entry point to the fabric for wireless users but in no way it is the exit point from the fabric for wireless users. Answer should be Border Node. Same as for wired traffic.

upvoted 1 times

landgar 10 months ago

Selected Answer: C

• There are two types of fabric border nodes: border and default border nodes. Both types provide the fundamental routing entry and exit point for all data traffic going into or out of the fabric overlay, as well as for VN and/or group-based policy enforcement (for traffic outside the fabric).

upvoted 2 times

TSKARAN 10 months, 3 weeks ago

Given answer is correct; C
fabric border nodes
There are two types of fabric border nodes: border and default border nodes. Both types provide the fundamental routing entry and exit point for all data traffic going into or out of the fabric overlay, as well as for VN and/or group-based policy enforcement (for traffic outside the fabric).

upvoted 2 times

Question #623 *Topic 1*

The Overlay Management Protocol (OMP) is used as the control plane protocol and forms peers between the VSmart Controller and the SD-WAN edge devices. OMP is responsible for advertising which three types of routes in the SD-WAN network? (Choose three.)

A. OMP routes

B. TLOCs

C. MP-BGP

D. LISP routes

E. Service routes

Correct Answer: *ABE*

Community vote distribution

ABE (100%)

CCNPWILL 1 month, 3 weeks ago

Given answers are correct.

upvoted 1 times

Vlad_Is_Love_ua 9 months, 3 weeks ago

Selected Answer: ABE

TLOC routes advertise TLOCs connected to the WAN transports, along with an extra set of attributes such as TLOC private and public IP addresses, carrier, preference, site ID, tag, weight, and encryption key information.

Service routes represent services (firewall, IPS, application optimization, and so on) that are connected to the Cisco WAN Edge local-site network and are available for other sites for use with service insertion. In addition, these routes include originator System IP, TLOC, and VPN-IDs; the VPN labels are sent in this update type to tell the Cisco vSmart controllers which VPNs are serviced at a remote site.

upvoted 3 times

Vlad_Is_Love_ua 9 months, 3 weeks ago

Selected Answer: ABE

OMP advertises three types of routes from Cisco WAN routers to Cisco vSmart controllers:

OMP routes, or vRoutes, are prefixes that are learned from the local site, or service side, of a Cisco WAN Edge router. The prefixes are originated as static or connected routes, or from within the OSPF, BGP, or EIGRP protocol, and redistributed into OMP so they can be carried across the overlay. OMP routes advertise attributes such as transport location (TLOC) information, which is similar to a BGP next-hop IP address for the route, and other attributes such as origin, origin metric, originator, preference, site ID, tag, and VPN. An OMP route is only installed in the forwarding table if the TLOC to which it points is active.

upvoted 3 times

Huntkey 1 year ago

The answer is correct
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/control-policies.html

upvoted 4 times

shoo83 1 year ago

given answer is correct
https://www.lookingpoint.com/blog/cisco-sd-wan-omp

upvoted 3 times

Question #624 *Topic 1*

Which of the following are the three components of the three-tier hierarchical networking model used in the classical Cisco networks design? (Choose three.)

A. Distribution

B. Core

D. Access

E. Leaf

F. Spine

Correct Answer: *ABC*

Community vote distribution

ABD (100%)

bora4motion Highly Voted 1 year ago

Selected Answer: ABD

Lol - c is missing.

upvoted 15 times

CCNPWILL Most Recent 1 month, 3 weeks ago

Easy gimme question... There is another similar question on the exam so be sure to read the entire question before just trying to snipe the answer by memory..

upvoted 1 times

cj_kuo 3 months, 4 weeks ago

Selected Answer: ABD

Core, Distribution, Access were correct answer.

upvoted 1 times

Burik 5 months, 2 weeks ago

Admins, please fix these questions.. too many mistakes

upvoted 3 times

ricaela10 11 months, 3 weeks ago

CORE
DISTRIBUTION
ACCESS
:)

upvoted 2 times

Dataset 1 year ago

CORE-DIST-ACC
Regards

upvoted 1 times

Question #625 *Topic 1*

Which of the following are the two components of the two-tier modern data center design? (Choose two.)

A. Distribution

B. Core

D. Access

E. Leaf

F. Spine

Correct Answer: *EF*

Community vote distribution

Niam77 Highly Voted 1 year ago

Selected Answer: EF

provided answer is correct because the question is in modern data center not a classical networkd design

upvoted 7 times

CCNPWILL Most Recent 1 month, 3 weeks ago

Correct.. LEAF + SPINE is for DATA CENTER... Classic campus is Access/Core. READ CAREFULLY.

upvoted 1 times

mdawg 9 months, 3 weeks ago

weird because when i think of two tier i think of collapsed core :(

upvoted 3 times

Nickplayany 10 months, 4 weeks ago

Selected Answer: EF

It is leaf and spine

upvoted 4 times

bora4motion 11 months, 3 weeks ago

leaf spine . lol.

upvoted 1 times

Dataset 1 year ago

Selected Answer: BD

I think is B and D
two tier is colapsed CORE (CORE+DISTRIBUTION, like three tier but together at the same level) and Access
Regards

upvoted 1 times

dogdoglee 12 months ago

BD is three tier (CS , DS , AS)
EF is correct
https://www.wwt.com/article/comparing-two-tier-three-tier-data-center-networks

upvoted 2 times

Question #626 *Topic 1*

In a Cisco SD-WAN network, which VPN Identifier is reserved for carrying out-of-band network management traffic?

A. VPN 0

B. VPN 1

C. VPN 512

D. VPN 514

Correct Answer: *C*

Community vote distribution

C (100%)

Tacolicious Highly Voted 1 year ago

Selected Answer: C

VPN 0—Transport VPN, which carries control traffic via the configured WAN transport interfaces. Initially, VPN 0 contains all of a device's interfaces except for the management interface, and all interfaces are disabled.
VPN 512—Management VPN, which carries out-of-band network management traffic among the Viptela devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all vEdge routers except for vEdge 100. For controller devices, by default, VPN 512 is not configured.
VPNs 1 through 511, and 513 through 65530—VPNs on vEdge routers for service-side data traffic.

https://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html

upvoted 10 times

iGlitch Most Recent 1 year ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/configure-interfaces.html

upvoted 3 times

Question #627 *Topic 1*

In a Cisco SD-WAN network, which VPN Identifier is reserved as the transport VPN, carrying control traffic?

A. VPN 0

B. VPN 1

C. VPN 512

D. VPN 514

Correct Answer: *A*

Community vote distribution

A (100%)

Tacolicious 1 year ago

Selected Answer: A

VPN 0—Transport VPN, which carries control traffic via the configured WAN transport interfaces. Initially, VPN 0 contains all of a device's interfaces except for the management interface, and all interfaces are disabled.
VPN 512—Management VPN, which carries out-of-band network management traffic among the Viptela devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all vEdge routers except for vEdge 100. For controller devices, by default, VPN 512 is not configured.
VPNs 1 through 511, and 513 through 65530—VPNs on vEdge routers for service-side data traffic.

https://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html

upvoted 4 times

iGlitch 1 year ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/configure-interfaces.html

upvoted 2 times

Question #628 *Topic 1*

Which Cisco SD-WAN component acts as a single pane of glass for management and offers centralized fault, performance, accounting, and configuration management?

A. vBond

B. vEdge

C. vSmart

D. vManage

Correct Answer: *D*

Community vote distribution

D (100%)

CCNPWILL 1 month, 3 weeks ago

Selected Answer: D

Correct answer is given. D

upvoted 1 times

andyforreg 4 months, 2 weeks ago

glass for management - > vManage)))

upvoted 1 times

snarkymark 9 months, 3 weeks ago

Agree, answer is D
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf

upvoted 1 times

nj1999 10 months, 3 weeks ago

https://www.cbtnuggets.com/it-training/cisco/sd-wan-vmanage

upvoted 1 times

Question #629 *Topic 1*

You need to implement a First Hop Redundancy Protocol (FHRP) in a dual stack (IPv4 and IPV6) environment that utilizes devices from multiple different vendors. Which protocol best meets these needs?

A. HSRP

B. GLBP

C. VRRPv1

D. VRRPv2

Correct Answer: *D*

Community vote distribution

D (89%) 11%

landgar Highly Voted 10 months ago

Selected Answer: D

No answer is correct. VRRP is vendor agnostic, but only version 3 provides IPv6 FHRP

upvoted 6 times

halinhit2208 Most Recent 1 month, 3 weeks ago

No answer is correct.
There are currently two versions of VRRP:
■ VRRPv2: Supports IPv4
■ VRRPv3: Supports IPv4 and IPv6
Refer: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

upvoted 1 times

felix_simon 5 months, 1 week ago

B
GLBP support IPV6. VRRP not support IPV6

upvoted 2 times

mgiuseppe86 2 months, 2 weeks ago

GLBP is Cisco only. So that is wrong. It says utilizes devices from multiple different vendors.

upvoted 1 times

MO_2022 11 months, 2 weeks ago

VRRP version 3

upvoted 1 times

nushadu 11 months, 2 weeks ago

no correct answer in the choices, MUST be VRRPv3
==
cisco(config)#fhrp version vrrp ?
v2 Legacy VRRP - VRRPv2 for IPv4
v3 Unified VRRP - VRRPv3 for IPv4 and IPv6
cisco(config)#fhrp version vrrp v2

cisco(config)#interface ethernet 0/0.10
cisco(config-subif)#vrrp ?
<1-255> Group number

cisco(config-subif)#vrrp 1 ?
authentication Authentication
description Group specific description
ip Enable Virtual Router Redundancy Protocol (VRRP) for IP
preempt Enable preemption of lower priority Master
priority Priority of this VRRP group
shutdown Disable VRRP Configuration
timers Set the VRRP timers
track Event Tracking
cisco(config-subif)#exit

upvoted 2 times

nushadu 11 months, 2 weeks ago

swap to vrrp_ver3:
==
cisco(config)#fhrp version vrrp v3

cisco(config)#interface ethernet 0/0.10
cisco(config-subif)#vrrp 1 ?
address-family Address family of the group

cisco(config-subif)#vrrp 1 address-family ?
ipv4 ipv4 Address family
ipv6 ipv6 Address family

cisco(config-subif)#vrrp 1 address-family
upvoted 1 times

bora4motion 1 year ago

Selected Answer: D

You have to go with VRRP as the protocol must be vendor agnostic.
upvoted 2 times

Tacolicious 1 year ago

Selected Answer: B

None of these? VRRP3, but that answer is not provided. GLBP has ipv6 functionality I think but I can't find anything about GLBP running a dual stack. Because of that i'll probably choose GLBP because the other ones sound more wrong to me
upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

GLBP is Cisco only. So that is wrong. It says utilizes devices from multiple different vendors.
upvoted 1 times

bora4motion 1 year ago

You have to go with VRRP as the protocol must be vendor agnostic. - It's D.
upvoted 1 times

Question #630 *Topic 1*

A wireless client roams from one Access Point to another Access Point using a different switch in a Cisco SD-Access network. If only a single Wireless Lan Controller in involved, what roaming methods is being used?

A. L3 roaming

B. inter-xTR

C. auto anchor

D. bridged roaming

Correct Answer: *B*

Community vote distribution

B (100%)

Darude Highly Voted 1 year ago

Selected Answer: B

answer is correct:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html
upvoted 11 times

well123 9 months ago

correct. That link explains it under SDA roaming
upvoted 2 times

Bigbongos Most Recent 10 months ago

A. L3 Roaming is being used when a wireless client roams from one Access Point to another Access Point using a different switch in a Cisco SD-Access network and only a single Wireless Lan Controller is involved.
upvoted 1 times

byallmeans 6 months, 4 weeks ago

Non-sense. Correct answer is B as per link shared by Darude.
upvoted 2 times

Question #631 *Topic 1*

In a Cisco SD-Access network where VXLAN is used for encapsulating data packets, what is the minimum MTU setting that devices should be configured with?

A. 1492

B. 1500

C. 1518

D. 1550

Correct Answer: *D*

Community vote distribution

D (100%)

Tacolicious Highly Voted 1 year ago

Selected Answer: D

If the underlay uses 1500 then the overlay needs to use at least 1550 for the 50 extra used for VXLAN overhead

upvoted 5 times

Darude Most Recent 1 year ago

Selected Answer: D

Correct
reference: https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/103x/configuration/vxlan/cisco-nexus-9000-series-nx-os-vxlan-configuration-guide-release-103x/m_configuring_vxlan_93x.html

upvoted 4 times

Question #632 *Topic 1*

Which Cisco Locator/ID Separation Protocol (LISP) device receives packets from remote site facing devices and either decapsulates the LISP packets or routes them natively?

A. ITR

B. ETR

C. MS

D. MR

Correct Answer: *A*

Community vote distribution

B (80%) A (20%)

kewokil120 Highly Voted 10 months, 3 weeks ago

Selected Answer: B

Decap = ETR
Encap = ITR

Answer is B

upvoted 12 times

Manvek Most Recent 4 months ago

Selected Answer: B

LISP Site Edge Devices
• ITR-Ingress Tunnel Router is deployed as a CE device. It receives packets from site-facing interfaces, and either encapsulates packets to remote LISP sites or natively forwards packets to non-LISP sites.
• ETR-Egress Tunnel Router is deployed as a CE device. It receives packets from core-facing interfaces and either decapsulates LISP packets or natively delivers non-LISP packets to local EIDs at the site.

Both ETR and ITR receive packets and natively forward them, so the question's key part is " receives packets from remote site facing devices". If the packets are coming from a remote site, it means they are coming from the network core. Thus, by definition, the answer is ETR.

upvoted 2 times

andyforreg 4 months, 2 weeks ago

Selected Answer: A

I think ITR

upvoted 1 times

HarwinderSekhon 5 months ago

When I hear Decapsulate, its ETR.
Encap -ITR. MS and MR not route natively, they just respond to requests.

upvoted 1 times

foreignbishop 6 months, 1 week ago

Selected Answer: A

I think there is a type in this question... This is directly from the OnDemandLearning that costs $1000.00

Ingress tunnel router (ITR): An ITR is a LISP site edge device that receives packets from site-facing interfaces (internal hosts) and encapsulates them to remote LISP sites, or natively forwards them to non-LISP sites.

Egress tunnel router (ETR): An ETR is a LISP site edge device that receives packets from core-facing interfaces (the transport infrastructure), de-encapsulates LISP packets, and delivers them to local EIDs at the site.

While B may look right, the ETR doesn't forward anything natively. While A may NOT look right, it DOES forward things natively. I think the question is supposed to say "encapsulates" as both A and B are wrong without that fix.

upvoted 4 times

aaabattery 8 months, 1 week ago

Selected Answer: B

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/locator-id-separation-protocol-lisp/datasheet_c78-576698.html

upvoted 3 times

snarkymark 9 months, 2 weeks ago

So, here is the question.
Which Cisco Locator/ID Separation Protocol (LISP) device receives packets from remote site facing devices and either decapsulates the LISP packets or routes them natively?

ITR-Ingress Tunnel Router is deployed as a CE device. It receives packets from site-facing interfaces, and either encapsulates packets to remote LISP sites or natively forwards packets to non-LISP sites.

• ETR-Egress Tunnel Router is deployed as a CE device. It receives packets from core-facing interfaces and either decapsulates LISP packets or natively delivers non-LISP packets to local EIDs at the site.

Is it me, or do neither of these fit?

upvoted 4 times

Cooldude89 9 months, 2 weeks ago

very snarky question
closest answer is B

upvoted 1 times

landgar 10 months ago

Selected Answer: B

ETR: decapsulates LISP packets:
https://networklessons.com/cisco/ccnp-encor-350-401/cisco-locator-id-separation-protocol-lisp

upvoted 3 times

mikhailov_ivan90 10 months ago

Selected Answer: B

I am for B, because there are 2 key words in the question "recieves" and "decapsulates" , it's all about ETR only. ITR sends and ecapsulates (recieves from IP side only)

upvoted 2 times

Rose66 10 months, 2 weeks ago

Selected Answer: B

ETR-Egress Tunnel Router is deployed as a CE device. It receives packets from core-facing interfaces and either decapsulates LISP packets or natively delivers non-LISP packets to local EIDs at the site.

upvoted 3 times

markymark874 10 months, 2 weeks ago

Selected Answer: A

A is the answer direction of flow is out to in
Etr is in to external. John13121 is correct.

upvoted 1 times

John13121 10 months, 3 weeks ago

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/locator-id-separation-protocol-lisp/datasheet_c78-576698.html

i was also for B until I read this article ... it is A....

upvoted 3 times

Nickplayany 7 months, 4 weeks ago

The one you provided literally says the answer is B ETR :)

upvoted 1 times

civan 11 months ago

Selected Answer: B

I think this is B - ETR:

From the question - which device "receives packets from remote site facing devices" and "decapsulates the LISP packets"

From https://www.ciscopress.com/articles/article.asp?p=2992605

An ITR (option A) "encapsulates them to the remote LISP site", which seems to be the opposite of what the question is asking

upvoted 2 times

bendarkel 11 months, 3 weeks ago

Selected Answer: A

Provided answer is correct.

upvoted 2 times

reza88 11 months, 3 weeks ago

Answer s correct.
"An ITR is a LISP site edge device that receives packets from
site-facing interfaces (internal hosts) and encapsulates them to remote LISP sites or natively
forwards them to non-LISP sites. An ITR is responsible for finding EID-to-RLOC mappings
for all traffic destined for LISP-capable sites. When it receives a packet destined for an EID,
it first looks for the EID in its mapping cache."

upvoted 4 times

Xerath 12 months ago

Provided answer is correct "A", reference: https://www.ciscopress.com/articles/article.asp?p=2992605

upvoted 1 times

Tacolicious 1 year ago

Selected Answer: B

shouldn't it be the ETR? Since the ITR encapsulates internal LISP going outwards?

upvoted 2 times

Question #633 *Topic 1*

Which of the following statements regarding the use of Bidirectional Forwarding Detection (BFD) in a Cisco SD-WAN environment are true?

A. BFD cannot be disabled on SD-WAN routers.

B. OSPFv3 is not supported with BFD.

C. In addition to link failure detection, it is also used to measure loss and latency used by application aware routing.

D. Is not typically enabled for OMP.

E. Does not support BGP.

Correct Answer: *AC*

Community vote distribution

AC (100%)

Tacolicious Highly Voted 1 year ago

Selected Answer: AC

Answer provided is correct:

Runs on SD-WAN tunnel to detect failures in the overlay tunnel

Is enabled by default and cannot be disabled

Is typically enabled for OMP

Besides link failures, it also measures latency, loss, and other link statistics used by application-aware routing

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-bfd-for-routing-protocols.html#Cisco_Concept.dita_26cf6354-cce5-4799-b140-f518adc78a40

upvoted 7 times

Question #634 *Topic 1*

Which of the following statements are true regarding the Link Management Protocol (LMP) when used in the Cisco Stackwise virtual link? (Choose two.)

A. It determines the switch priority.

B. It negotiates the version of the virtual header

C. It verifies link integrity via bidirectional forwarding

D. It performs auto discovery of other active Stackwise switches

Correct Answer: *BC*

Community vote distribution

BC (100%)

Tacolicious Highly Voted 1 year ago

Selected Answer: BC

Answer provided is correct:

The Link Management Protocol (LMP) is activated on each link of the StackWise Virtual link as soon as it is brought up online. The LMP performs the following functions:

● Verifies link integrity by establishing bidirectional traffic forwarding, and rejects any unidirectional links

● Exchanges periodic hellos to monitor and maintain the health of the links

● Negotiates the version of StackWise Virtual header between the switches StackWise Virtual link role resolution

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html

upvoted 8 times

djedeen Most Recent 3 months, 1 week ago

Selected Answer: BC

the other protocol besides LMP is SDP (StackWise Discovery Protocol) used for the following:
- Determines whether the hardware and software versions allow a Cisco StackWise Virtual domain to be formed
- Determines which switch will become the active virtual switch and which will become the standby virtual switch from a control-plane perspective

upvoted 1 times

Colmenarez 4 months ago

Selected Answer: BC

LMP is not even found in the OCG

upvoted 2 times

Question #635 *Topic 1*

You have configured router R1 with multiple VRF's in order to support multiple customer VPN networks. If you wanted to see the best path for the 10.2.1.0.24 route in VRF Green, what command would you use?

A. show ip route vrf Green 10.2.1.0

B. show ip route 10.2.1.0 vrf Green

C. show route all 10.2.1.0

D. show ip route 10.2.1.0 Green

Correct Answer: *A*

Community vote distribution

A (100%)

Burik 5 months, 2 weeks ago

Give me a break, this is a question from the preparation of the ENARSI exam, not even an actual exam question from any certification. Since when Cisco refers to the exam candidate as "you"? And it's VRFs, not VRF's. Delete this question.

upvoted 1 times

nushadu 11 months, 2 weeks ago

cisco#show ip vrf
Name Default RD Interfaces
RED 1:1 Lo0
cisco#show ip route vrf RED | b Gate
Gateway of last resort is not set

10.0.0.0/32 is subnetted, 1 subnets
C 10.0.0.1 is directly connected, Loopback0
cisco#
A. is true

upvoted 3 times

bora4motion 1 year ago

Selected Answer: A

a is correct
#show ip route vrf mgmt 10.100.10.1
% IP routing table vrf mgmt does not exist

upvoted 3 times

Question #636 *Topic 1*

Which of the following are benefits from implementing the use of VXLAN's in a network? (Choose two)

A. Increased scalability since VXLAN extends the IF field to 24 bits, providing up to 16 million unique ID values.

B. Makes the implementation of Spanning Tree more efficient.

C. Can be used to replace layer 3 routing protocols and increase routing efficiency at layer 2.

D. Supports Equal Cost Multi-pathing (ECMP) so that load balancing over multiple links can be used.

Correct Answer: *AD*

Community vote distribution

AD (100%)

Tadese 2 months, 2 weeks ago

The answer correct AD (ECMP).reference:https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nxos/vxlan/configuration/guide/b_NX-OS_VXLAN_Configuration_Guide/overview.pdf

upvoted 1 times

Manvek 4 months ago

Selected Answer: AD

Provided answer are correct

upvoted 1 times

Darude 1 year ago

Selected Answer: AD

provided answer is correct.
VXLAN is a MAC in IP/UDP(MAC-in-UDP) encapsulation technique with a 24-bit segment identifier in the form of a VXLAN ID. The larger VXLAN ID allows LAN segments to scale to 16 million in a cloud network. In addition, the IP/UDP encapsulation allows each LAN segment to be extended across existing Layer 3 networks making use of Layer 3 equal-cost multipath (ECMP).

reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/vxlan/configuration/guide/b_NX-OS_VXLAN_Configuration_Guide/overview.pdf

upvoted 3 times

Question #637 *Topic 1*

Which component of TCP defines the maximum packet size that a host interface is able to accept on ingress?

A. MTU

B. PATH MTU

C. Window size

D. MRU

Correct Answer: *D*

Community vote distribution

D (50%) C (43%) 7%

iGlitch Highly Voted 1 year ago

Selected Answer: D

A maximum transmission unit (MTU) is the largest length of a packet that can be transmitted out of an interface toward a destination. maximum receive unit (MRU) is the largest packet size that an interface can receive, so it's an ingress interface parameter.

https://www.networkers-online.com/p/understand-mtu-and-mru-the-full-story

upvoted 13 times

snarkymark 9 months, 3 weeks ago

Agree, and if you read this MRU can be configured differently. Not sure anyone does, but it is an option.

upvoted 2 times

JackDRipper Highly Voted 8 months ago

Selected Answer: C

"...component of TCP..." - Has to be TCP window size. That's about the only thing TCP has that can influence how much data the ingress interface on the far-side can accept before sending back and ack.

upvoted 5 times

Adnan5252 3 months ago

no window size is only when send an acknowledge and its not to determine one single mtu because he can receive multiple mtu and then window size send an acknowledgment

upvoted 1 times

dudalykai 3 months, 1 week ago

100% true

upvoted 1 times

Soggyt74 Most Recent 3 months, 2 weeks ago

Selected Answer: D

A maximum transmission unit (MTU) is the largest length of a packet that can be transmitted out of an interface toward a destination. Maximum Receive Unit (MRU) is the largest packet size that an interface can receive, so it's an ingress interface parameter.

https://www.networkers-online.com/p/understand-mtu-and-mru-the-full-story

upvoted 1 times

Colmenarez 3 months, 3 weeks ago

Selected Answer: C

C is correct.

upvoted 1 times

NLFluke 4 months, 1 week ago

Selected Answer: C

C - For sure, the question says "component of TCP". The devices will negotiate a window size that both can handle.

Congestion occurs when the interface has to transmit more data than it can handle.
It's queue(s) will hit a limit and packets will be dropped.

https://networklessons.com/cisco/ccie-routing-switching-written/tcp-window-size-scaling

upvoted 1 times

CKL_SG 4 months, 3 weeks ago

Selected Answer: D

MRU?

On the other hand maximum receive unit (MRU) is the largest packet size that an interface can receive, so it's an ingress interface parameter. In most of the cases MRU equals MTU but it's not a requirement. You can configure different values for both MTU and MRU to achieve some benefits.

upvoted 1 times

Entivo 5 months, 1 week ago

Selected Answer: C

The question specifically asks "which component of TCP". If you go and look up TCP you will see that there are no parts of a TCP PDU for MTU/MRU, as these are set in layer 2 in the ethernet frame. Window Size is the way TCP controls flow, so the answer has to be C. The lesson here is - don't ask a question about TCP (layer 4) and then expect an answer about another layer. Stupid question.

upvoted 4 times

lafrank 7 months, 2 weeks ago

This is actually a wrongly worded question which is totally mixing networking units.
TCP is L4, packet is for L3 and interface capability is more of an L2 term.
https://i.stack.imgur.com/6dKkj.gif

upvoted 5 times

Pcatt 8 months, 2 weeks ago

TCP L4, MTU L2 naswer C

upvoted 1 times

TSKARAN 10 months, 3 weeks ago

Typically, the MTU and MRU sizes for a particular network are the same values. For example, Ethernet networks have an MTU/MRU of 1500 bytes

The question is about MRU - the largest packet size that an interface can receive in ingress.
So D is the correct answer.

upvoted 1 times

kewokil120 10 months, 3 weeks ago

Selected Answer: A

MTU = Max Trans Unit. MRU linked to MTU

upvoted 1 times

MJane 11 months ago

Selected Answer: C

the window size indicates the size of the receive buffer

upvoted 2 times

bora4motion 1 year ago

Tricky one, I'm still debating between A and D, tending to incline towards D - just because of the wording of the question.

upvoted 1 times

Tacolicious 1 year ago

Selected Answer: A

MTU and MRU are linked, so by changing the mtu you'd also change the mru. I'm going for A for this question

upvoted 1 times

Question #638 *Topic 1*

Which of the following are examples of Type 2 hypervisors? (Choose three.)

A. VMware ESXi

B. Oracle VirtualBox

C. Oracle Solaris Zones

D. Microsoft Hyper-V

E. Microsoft Virtual PC

Correct Answer: *BCE*

Community vote distribution

BCE (100%)

mmhawish 10 months, 2 weeks ago

Selected Answer: BCE

A few examples of Type 1 hypervisors are Citrix/Xen Server, VMware ESXi and Microsoft Hyper-V.

upvoted 4 times

KOJJY 11 months, 2 weeks ago

Selected Answer: BCE

correct

upvoted 2 times

Quentin_ 11 months, 4 weeks ago

ADE is correct

upvoted 1 times

Quentin_ 11 months, 4 weeks ago

sorry, I meant BDE

upvoted 1 times

Inzo 11 months, 4 weeks ago

ESXi and HyperV are type 1 hypervisors.

upvoted 1 times

Question #639 *Topic 1*

EIRP (Effective Isotropic Radiated Power) is the actual amount of signal leaving the antenna. It is a measurement value in db and is based on which three components? (Choose three.)

A. Transmit Power

B. RSSI

C. Cable Loss

D. Antenna Gain

E. SNR

Correct Answer: *ACD*

Community vote distribution

ACD (100%)

jrquissak 3 months ago

Selected Answer: ACD

provided answer is correct.

upvoted 1 times

CKL_SG 5 months ago

Selected Answer: ACD

EIRP (Effective Isotropic Radiated Power)
EIRP (Effective Isotropic Radiated Power) is the actual amount of signal leaving the antenna and is a value measured in db and is based on 3 values:
a) Transmit Power (dBm)
b) Cable Loss (dB)
c) Antenna Gain (dBi)

https://community.cisco.com/t5/wireless-mobility-knowledge-base/snr-rssi-eirp-and-free-space-path-loss/ta-p/3128478#toc-hId-1040688787

upvoted 1 times

Darude 1 year ago

Selected Answer: ACD

provided answer is correct.
The radiated (transmitted) power is rated in either dBm or W. Power that comes off an antenna is measured as effective isotropic radiated power (EIRP). EIRP is the value that regulatory agencies, such as the FCC or European Telecommunications Standards Institute (ETSI), use to determine and measure power limits in applications such as 2.4-GHz or 5-GHz wireless equipment. In order to calculate EIRP, add the transmitter power (in dBm) to the antenna gain (in dBi) and subtract any cable losses (in dB).

reference:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/23231-powervalues-23231.html

upvoted 4 times

Question #640 *Topic 1*

A switch is attached to router R1 on its gig 0/0 interface. Fort security reasons, you want to prevent R1 from sending OSPF hellos to the switch. Which command should be enabled to accomplish this?

A. R1(config-router)#ip ospf hello disable

B. R1(config-router)#ip ospf hello-interval 0

C. R1(config)#passive-interface Gig 0/0

D. R1(config-router)#passive-interface Gig 0/0

Correct Answer: *D*

Community vote distribution

D (100%)

nushadu Highly Voted 11 months, 2 weeks ago

Selected Answer: D

cisco(config-router)#passive-interface ethernet 0/0.10

upvoted 6 times

djedeen Most Recent 2 weeks, 1 day ago

Selected Answer: D

config#'router ospf 1' will move to submenu with prompt config-router#

upvoted 1 times

jrquissak 3 months ago

Selected Answer: D

provided answer is correct.

upvoted 1 times

Question #641 *Topic 1*

What are some of the key differences between HSRPv1 and HSRPv2? (Choose two.)

A. HSRPv1 uses the multicast address of 224.0.0.102 while HSRPv2 uses 225.0.0.2.

B. HSRP uses a group range of 0-255, while HSRP uses a group range of 0-4095.

C. HSRPv1 uses seconds based timers, while HSRPv2 uses milliseconds based timers.

D. HSRPv1 provides support for IPv6, while HSRPv2 supports IPv4 only.

Correct Answer: *BC*

Community vote distribution

BC (100%)

iGlitch Highly Voted 1 year ago

Selected Answer: BC

B - should be HSRPv1, HSRPv2

upvoted 6 times

Nickplayany Highly Voted 9 months, 3 weeks ago

Selected Answer: BC

Admin please fix the answer B.

B. HSRPv1 uses a group range of 0-255, while HSRPv2 uses a group range of 0-4095.

upvoted 6 times

foreignbishop Most Recent 6 months, 1 week ago

HSRPv1 DOES support msec timers, but that leaves 1 answer correct and it's asking for 2.

upvoted 1 times

T_Cos 11 months, 1 week ago

Answers B and C

upvoted 3 times

nushadu 11 months, 2 weeks ago

Selected Answer: BC

https://learningnetwork.cisco.com/s/question/0D53i00000Kt11hCAB/reg-hsrp-v1-vs-hsrp-v2

upvoted 1 times

Question #642 *Topic 1*

Which of the following are valid Port Aggregation Protocol (PAgP) modes? (Choose two.)

A. On

B. Active

C. Passive

D. Auto

E. Desirable

Correct Answer: *DE*

Community vote distribution

DE (100%)

danman32 Highly Voted 5 months, 1 week ago

How I am remembering auto/desirable for PaGP vs active/passive for LACP is that auto/desirable is also DTP options, which can be thought of (or perhaps is) Cisco proprietary

upvoted 5 times

[Removed] Most Recent 5 months, 2 weeks ago

Selected Answer: DE

correct

upvoted 1 times

T_Cos 11 months, 1 week ago

Modes PaGP: Auto and Desirable, LACP: Active and Passive, On: Forced

upvoted 4 times

Question #643 *Topic 1*

Which of the following are true statements regarding the Virtual Router Redundancy Protocol (VRRP) feature? (Choose two.)

A. Pre-emption is enabled by default

B. The router priority is a configurable value from 0-4095

C. MD5 authentication is supported with VRRP

D. Secondary IP addresses are supported with VRRP

E. VRRP can only be used with Cisco devices

Correct Answer: *AD*

Community vote distribution

AD (55%) CD (27%) AC (18%)

[Removed] Highly Voted 5 months, 1 week ago

ACD are correct.

VRRP supports md5 authentication
R1(config-if)#vrrp 1 authentication ?
WORD Plain text authentication string
md5 Use MD5 authentication
text Plain text authentication

VRRP supports secondary IP address
R1(config-if)#vrrp 1 ip 192.168.1.250 ?
secondary Specify an additional VRRP address for this group
<cr>

and VRRP has preempt enabled by default.

upvoted 7 times

Manvek 4 months ago

Option C is wrong. Authentication was revoked from VRRP with RFC 3768 and RFC 5798. Even though Cisco still support authentication for VRRP, the protocol itself does not. A 3rd party device may not supported as it is not required in the standard.

https://datatracker.ietf.org/doc/html/rfc5798
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html#GUID-B1CB24C0-2526-4790-A701-0105FDA69FC8

upvoted 2 times

Jasper Most Recent 1 week, 5 days ago

AD is correct: according GPT Chat:
Regarding the use of Message Digest Algorithm 5 (MD5) authentication with VRRP, it's important to note that VRRP itself does not have built-in support for MD5 authentication. VRRP provides a basic authentication mechanism through a simple plaintext password.

upvoted 1 times

Evreni 1 month ago

Selected Answer: AD

AD: are correct
C: is not because MD5 i supported only in VRRP-E (extended)

upvoted 1 times

Manvek 4 months ago

Selected Answer: AD

A - Correct. Preemption is enabled by default on VRRP.
B - Wrong. The priority goes from 0 - 255.
C - Wrong. Authentication was revoked from VRRP with RFC 3768 and RFC 5798. Even though Cisco still support authentication for VRRP, the protocol itself does not. A 3rd party device may not supported as it is not required in the standard.
D - Correct. As stated by others VRRP can manage multiple addresses, including secondary addresses.
E- Wrong. VRRP is an open standard

upvoted 2 times

Hosein 5 months, 1 week ago

Selected Answer: AD

obvious answers are A and D,

upvoted 1 times

[Removed] 5 months, 1 week ago

If you are familiar with VRRP, you would know that VRRP supports MD5 authentication, it also supports Secondary IP address, and Preempt is enabled by default.
The question should say to "choose all that apply" instead of choose only two.
upvoted 1 times

Entivo 5 months, 1 week ago

A and D are true but so is C, so there are 3 correct answers here!!
upvoted 1 times

Bluntedcase 5 months, 2 weeks ago

For me it's A&D too.
Here from Cisco:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html#GUID-25707FA6-F3D5-4726-9E03-62112630F329

"By default, a preemptive scheme is enabled whereby a higher priority virtual router backup that becomes available takes over for the virtual router backup that was elected to become virtual router master. You can disable this preemptive scheme using the no vrrp preempt command."

"The virtual router can manage multiple IP addresses, including secondary IP addresses." Therefore, if you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.
upvoted 1 times

Bluntedcase 5 months, 2 weeks ago

According to the same page aboce, C would also be valid:

"You can configure VRRP text authentication, authentication using a simple MD5 key string, or MD5 key chains for authentication."
upvoted 2 times

Cesar12345 5 months, 2 weeks ago

Selected Answer: AD

MD5 seems to be not allowed on all Cisco devices https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/unicast/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Unicast_Routing_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_Unicast_Routing_Configuration_Guide_7x_chapter_010011.pdf
upvoted 1 times

foreignbishop 6 months, 1 week ago

Interesting as the labs in the online training have you configure VRRP with authentication but it's not recommended. Since I needed to do it as part of the official training course for ENCOR on Cisco's online training, I'll go with MD5. Preempt is enabled by default.
upvoted 1 times

gibblock 7 months, 3 weeks ago

B. wrong, since <1-254> Priority level
D. wrong, the virtual IP can be a configured interface IP but not a secondary address/es
E. wrong

Right answers
A. show vrrp "Preemption enabled" pre-emption obviously a typo
C. vrrp 100 authentication ?
WORD Plain text authentication string
md5 Use MD5 authentication
text Plain text authentication
upvoted 2 times

JackDRipper 8 months, 1 week ago

Must be a bonus question. To me, ACD are correct choices. "Pre-empt" and "Preempt" exactly means the same thing in English. But I concede that only the latter form of the spelling is the acceptable IOS command.
upvoted 1 times

JackDRipper 7 months, 2 weeks ago

I think this question is looking for three answers:
A, C, and D are all features of VRRP: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html#GUID-3A5601DB-95A3-48EE-9F46-ECB746E820FC
upvoted 2 times

eojedad 8 months, 2 weeks ago

Selected Answer: CD

C and D are correct answer.
pre-emption doesn't exist....a tricky option
upvoted 2 times

snarkymark 9 months, 3 weeks ago

If I go by this Cisco documentation, then A and D are correct.
https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/addr_serv/configuration/guide/ic40crs1book_chapter10.html
upvoted 1 times

StefanOT2 10 months, 2 weeks ago

Selected Answer: AD

A and D are correct. C (MD5 Auth) is not supported on all Cisco devices.
upvoted 3 times

John13121 10 months, 3 weeks ago
the answers are right read the question carefully there is a difference between:
preemption and pre-emption
upvoted 1 times

poy4242 11 months, 1 week ago
Selected Answer: AD
Interesting fact :
First RFC 2338 says MD5 is a feature, but the last version 5798 of the RFC says "VRRP for IPvX does not currently include any type of authentication." (same satement is in RFC 3768)
So A and D for me
upvoted 4 times

Quesocat 11 months, 1 week ago
This one is interesting as A, C and D all seem to be true for me.
A - Page 409 on the OCG states 'VRRP enables preemption by default. Also stated on cisco's VRRP Router Priority and Preemption section: "By default, a preemptive scheme is enabled whereby a higher priority virtual router backup that becomes available takes over for the virtual router backup that was elected to become virtual router master." https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html#GUID-25707FA6-F3D5-4726-9E03-62112630F329

C and D show as listed under the options for configuration here: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html#GUID-3931AB2F-738A-4BE6-B06E-E46AB30A33FA
upvoted 1 times

Question #644 *Topic 1*

You want to securely implement the Network Time Protocol (NTP) on your network. What two mechanisms are available to secure NTP? (Choose two.)

A. IPSec communication

B. MD5 authentication keys

C. Role based access control (RBAC)

D. access-group configuration

Correct Answer: *BD*

Community vote distribution

BD (100%)

nushadu Highly Voted 11 months, 2 weeks ago
Selected Answer: BD
cisco(config)#ntp ?
access-group Control NTP access
allow Allow processing of packets
authenticate Authenticate time sources
authentication-key Authentication key for trusted time sources
upvoted 5 times

bora4motion Most Recent 1 year ago
Selected Answer: BD
BD is correct
upvoted 4 times

Question #645 *Topic 1*

Which Cisco EIGRP K-values are set to zero by default? (Choose three.)

A. Bandwidth

B. Load

C. Total Delay

D. Reliability

E. MTU

Correct Answer: *BDE*

Community vote distribution

BDE (100%)

due 2 months, 4 weeks ago

Selected Answer: BDE

Big Dog Realy Love Me
1 0 1 0 0

0= Delay , Reliability , MTU

upvoted 2 times

bora4motion 1 year ago

Selected Answer: BDE

BDE is correct, the other ones are 1.

upvoted 2 times

Darude 1 year ago

Selected Answer: BDE

provided answer is correct

reference: https://ipwithease.com/eigrp-k-values/
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-s/ire-15-s-book/ire-wid-met.html

upvoted 3 times

Question #646 *Topic 1*

What are the four stages of obtaining an IP address lease from a DHCP server?

A. Discover, Offer, Release, Renew

B. Discover, Obtain, Request, Renew

C. Determine, Obtain, Release, Acknowledge

D. Discover, Offer, Request, Acknowledge

Correct Answer: *D*

Community vote distribution

D (100%)

robi1020 Highly Voted 11 months ago

tu to do tu DORA tu to do tu DORA ola :D

upvoted 7 times

jackr76 6 months, 1 week ago

C is DORA too...

upvoted 1 times

Din04 Most Recent 9 hours, 57 minutes ago

Selected Answer: D

DORA - feels like muscle memory to me

upvoted 1 times

[Removed] 5 months ago

Selected Answer: D

DORA is the correct answer

upvoted 1 times

danman32 5 months, 1 week ago

Most of us know DORA. Looks like Cisco knows we use that accronym as well so they trick us with answer C.

upvoted 2 times

Dataset 6 months, 4 weeks ago

"DETERMINE" jajajajajjajaaj
DORA...we love you

upvoted 1 times

Mze 1 year ago

DORA is the correct answer. D , is correct.

upvoted 4 times

bora4motion 1 year ago

good ol' DORA

upvoted 4 times

Question #647 *Topic 1*

A new multicast server is being added to an existing PIM Sparse mode network. Which device in this network must the new server register with before its multicast traffic can be dispersed throughout the network?

A. IGMP Querier

B. Local PIM router

C. Local IGMP switch

D. Rendezvous Point (RP)

Correct Answer: *D*

Community vote distribution

D (100%)

felix_simon 5 months ago

D
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-tech-oview.html
When hosts join a multicast group, the directly connected routers send PIM Join messages toward the RP.

upvoted 2 times

Darude 1 year ago

Selected Answer: D

provided answer is correct

reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-9/configuration_guide/sys_mgmt/b_169_ip_mcast_rtng_3850_cg/ip_multicast_optimization__optimizing_pim_sparse_mode_in_a_large_ip_multicast_deployment.html

upvoted 3 times

Question #648 *Topic 1*

You want to create a policy that allows all TCP traffic in the port range of 20 to 110, except for telnet traffic, which should be dropped. Which of the following access control lists will accomplish this?

A. deny tcp any any eq 22
permit tcp any any gt 20 lt 110

B. permit tcp any any range 22 443
deny tcp any any eq 23

C. deny tcp any any eq 23
permit tcp any any

D. deny tcp any any eq 23
permit tcp any any range 20 110

Correct Answer: *D*

Community vote distribution

D (100%)

CCNPWILL 1 month, 3 weeks ago

Selected Answer: D

Correct. Deny unwanted port first. Then permit is the next statement. D..
EZ

upvoted 1 times

[Removed] 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

nushadu 11 months, 2 weeks ago

D. looks good but cisco IOS swapped numbers to port names:
Extended IP access list Q_648
20 deny tcp any any eq telnet
40 permit tcp any any range ftp-data pop3
==
original cmd:
cisco(config-ext-nacl)#40 permit tcp any any range 20 110

upvoted 2 times

nushadu 11 months, 1 week ago

++
cisco_R3#show running-config | section access
...
ip access-list extended Q_648
deny tcp any any eq telnet
permit tcp any any range ftp-data pop3

upvoted 1 times

iGlitch 1 year ago

Selected Answer: D

D is correct, for the policy map to MATCH an entry we should use 'permit' otherwise use 'deny'.

upvoted 4 times

AndreasThornus 11 months, 3 weeks ago

The question doesn't specifically refer to a policy-map, just says policy.

upvoted 1 times

Question #649 *Topic 1*

In a Cisco SD-Access network architecture, what is the role of the Fabric Edge Node?

A. It manages endpoint to device relationships

B. It connects external layer 3 networks to the SDA fabric

C. It connects wired endpoints to the SDA fabric

D. It connects wireless endpoints to the SDA fabric

Correct Answer: *C*

Community vote distribution

C (100%)

ConqiD 1 week, 2 days ago

Edge Node Design:
In SD-Access, fabric edge nodes represent the access layer in a two or three-tier hierarchy. The access layer is the edge of the campus. It is the place where end devices attach to the wired portion of the campus network. The edge nodes also represent the place where devices that extend the network connectivity out one more layer connect. These include devices such as IP phones, access points, and extended nodes.

upvoted 1 times

TheDazzler 10 months, 1 week ago

Selected Answer: C

Answer shown is correct.
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

upvoted 3 times

Question #650 *Topic 1*

Which of the following are features typically only found in a Next Generation (NextGen) firewall? (Choose two.)

A. Network Address Translation (NAT)

B. Secure remote access VPN (RA VPN)

C. Deep packet inspection

D. reputation based malware detection

E. IPSec site-to-site VPN

Correct Answer: *CD*

Community vote distribution

CD (100%)

nushadu 11 months, 2 weeks ago

Selected Answer: CD

Agree with provided answers, basically NGFW it is application control on layer 7 OSI, like skype, facebook games, icq, etc.

upvoted 3 times

iGlitch 1 year ago

Selected Answer: CD

Provided answers are correct.

upvoted 1 times

Question #651 *Topic 1*

JSON web tokens (JWT) are used to secure JSON based communications. Which of the following fields make up a JWT? (Choose three.)

A. Header

B. Trailer

C. Payload

D. Sequence number

E. Signature

Correct Answer: *ACE*

Community vote distribution

ACE (100%)

Darude Highly Voted 1 year ago

Selected Answer: ACE

provided answer is correct

reference: https://jwt.io/introduction

upvoted 5 times

ihateciscoreally Most Recent 3 months, 2 weeks ago

questions about fields on CCNP - no comment

upvoted 1 times

Vlad_Is_Love_ua 9 months, 1 week ago

Selected Answer: ACE

A JWT (JSON Web Token) is comprised of three parts:

Header: A JSON object that describes the type of token and the cryptographic algorithm used to secure it. It typically consists of two fields: "alg" for algorithm and "typ" for type.

Payload: A JSON object that contains the claims (statements) about the user or system that the token represents. The claims can include user ID, name, email, role, and any other relevant information. The payload may also contain additional custom claims, and the entire payload is typically encrypted using the algorithm specified in the header.

Signature: A hash that is used to verify the authenticity of the token. The signature is computed by combining the encoded header, the encoded payload, and a secret key known only to the issuer, using the algorithm specified in the header.

Together, these three components make up a JWT, which is typically used for authentication and authorization in web applications and APIs.

upvoted 1 times

Vlad_Is_Love_ua 9 months, 1 week ago

A JWT (JSON Web Token) is comprised of three parts:

Header: A JSON object that describes the type of token and the cryptographic algorithm used to secure it. It typically consists of two fields: "alg" for algorithm and "typ" for type.

Payload: A JSON object that contains the claims (statements) about the user or system that the token represents. The claims can include user ID, name, email, role, and any other relevant information. The payload may also contain additional custom claims, and the entire payload is typically encrypted using the algorithm specified in the header.

Signature: A hash that is used to verify the authenticity of the token. The signature is computed by combining the encoded header, the encoded payload, and a secret key known only to the issuer, using the algorithm specified in the header.

Together, these three components make up a JWT, which is typically used for authentication and authorization in web applications and APIs.

upvoted 1 times

Question #652 *Topic 1*

Ansible is being used in a network for configuration and management automation. Which of the following are true statements regarding Ansible? (Choose two.)

A. Requires an agent on the end device.

B. Utilizes the concept of playbooks to execute the configuration.

C. Uses a pull model, where the end devices pull configuration files from the Ansible server.

D. Utilizes SSH.

Correct Answer: *BD*

Community vote distribution

BD (100%)

felix_simon 5 months ago

BD
https://docs.ansible.com/ansible/latest/network/getting_started/first_playbook.html
upvoted 1 times

mellohello 9 months ago

Ansible is a push model and is based on SSH.
upvoted 1 times

snarkymark 9 months, 3 weeks ago

Selected Answer: BD

https://www.devopsschool.com/blog/what-are-the-key-features-and-specific-roles-of-ansible/
upvoted 1 times

Darude 1 year ago

Selected Answer: BD

provided answer is correct:

Playbooks
https://docs.ansible.com/ansible-core/devel/getting_started/basic_concepts.html

SSH
https://docs.ansible.com/ansible-core/devel/getting_started/index.html
upvoted 3 times

Question #653 *Topic 1*

In a Cisco Software Defined Networking (SDN) architecture, what is used to describe the API communication between the SDN controller and the network elements (routers and switches) that it manages?

A. Southbound API

B. Northbound API

C. Westbound API

D. Eastbound API.

Correct Answer: *A*

Community vote distribution

A (100%)

TheDazzler 10 months, 1 week ago

Selected Answer: A

Provided answer is correct.
https://www.cisco.com/c/en_uk/solutions/software-defined-networking/overview.html#~services

upvoted 3 times

Question #654 *Topic 1*

In a Cisco VXLAN based network, which of the following best describes the main function of a VXLAN Tunnel Endpoint (VTEP)?

A. A device that performs VXLAN encapsulation and decapsulation.

B. It is a 24 bit segment ID that defines the broadcast domain.

C. It is the Logical interface where the encapsulation and de-encapsulation occurs.

D. It is a device that performs tunneling using GRE.

Correct Answer: *A*

Community vote distribution

A (100%)

romario22 1 month ago

No way. The correct answer is C

upvoted 1 times

samitherider 2 months, 4 weeks ago

I have an issue for it being called a Device... VTEP is a logical Tunnel that encapsulates the VXLAN

upvoted 2 times

bora4motion 1 year ago

Selected Answer: A

a is correct

upvoted 3 times

Darude 1 year ago

Selected Answer: A

provided answer is correct
VTEP (Virtual Tunnel Endpoint) - This is the device that does the encapsulation and de-encapsulation.

reference:https://www.cisco.com/c/en/us/support/docs/switches/nexus-9000-series-switches/118978-config-vxlan-00.html

upvoted 3 times

Question #655 *Topic 1*

Two Cisco switches are logically configured as a single switch using Cisco Stackwise technology. This will result in virtually combining which two planes? (Choose two.)

A. Data Plane

B. Control Plane

C. Forwarding Plane

D. Management Plane

E. Bearer Plane

Correct Answer: *BD*

Community vote distribution

BD (100%)

Darude 1 year ago

Selected Answer: BD

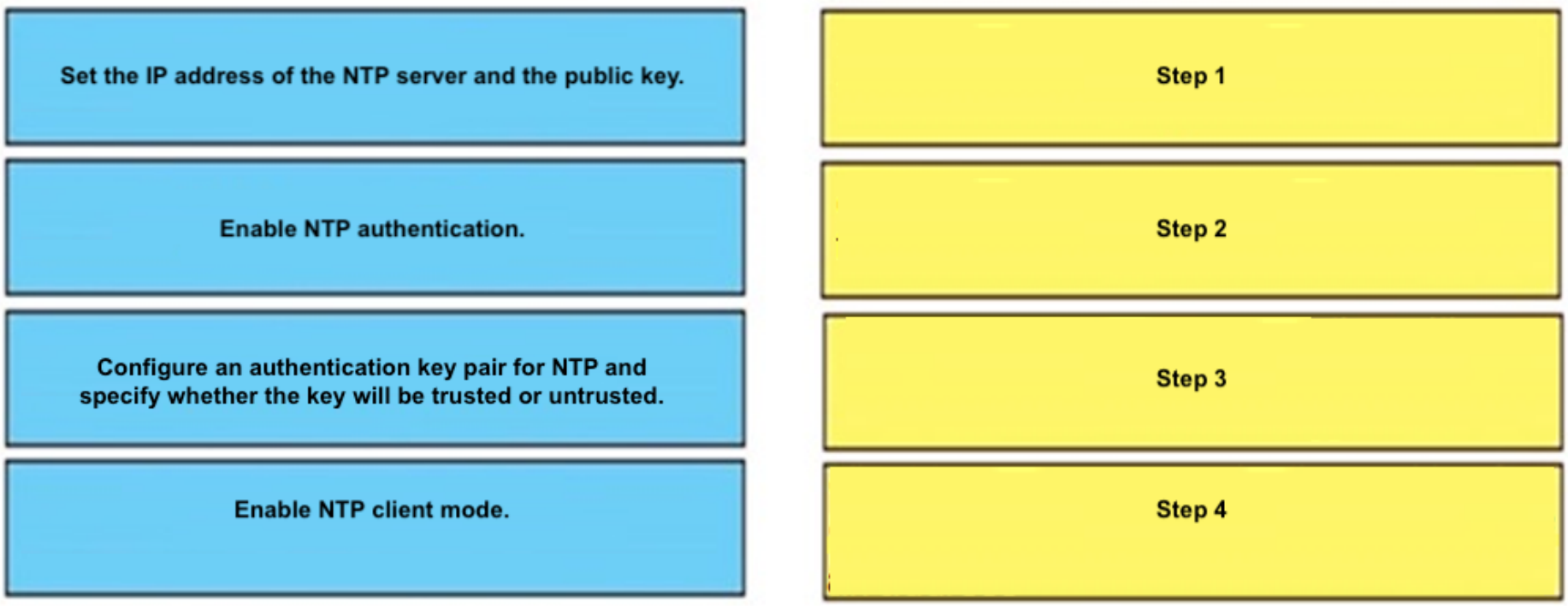
provided answer is correct.

StackWise Virtual (SV) combines two switches into a single logical network entity from the network control plane and management perspectives.
reference:https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html

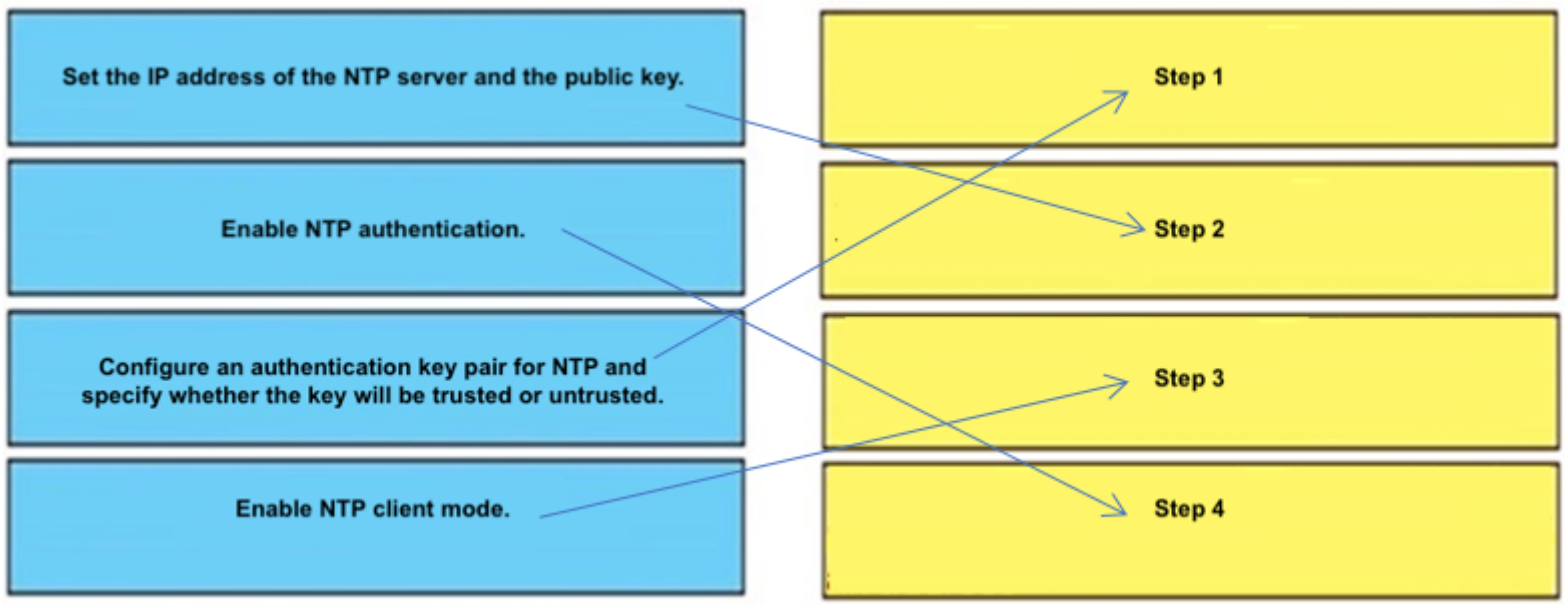
upvoted 3 times

DRAG DROP -

Please drag and drop the options provided in the left to configure NTP in client mode.



Correct Answer:



Darude Highly Voted 1 year ago

answer is correct:
reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html#wp1021234

upvoted 8 times

AndreasThornus Highly Voted 11 months, 3 weeks ago

This question appears to cover NTP configuration from the dark dark days of CATOS based on the articles provided!

upvoted 8 times

Opreis Most Recent 8 months, 4 weeks ago

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html

upvoted 3 times

Tacolicious 1 year ago

Answer is correct:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html#wp1019984

upvoted 5 times

Question #657 *Topic 1*

Please select the correct option that shows the correct combination for the Type 1 Hypervisor.

A. Hardware; Hypervisor; Guest OS

B. Hardware; Host OS; Hypervisor; Guest OS

C. Host OS; Hypervisor; Guest OS

D. Hardware; Host OS; Guest OS

Correct Answer: *A*

Community vote distribution

A (100%)

snarkymark 9 months, 3 weeks ago

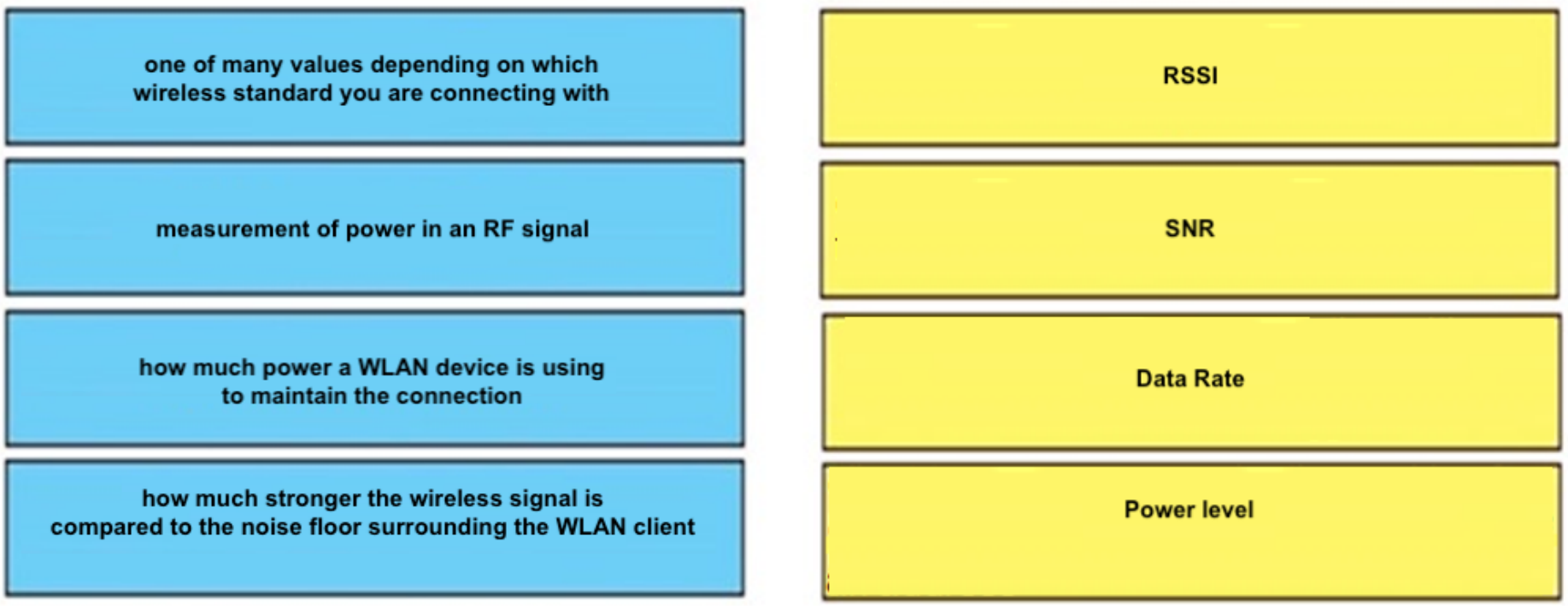
Selected Answer: A

https://www.techtarget.com/searchitoperations/tip/Whats-the-difference-between-Type-1-vs-Type-2-hypervisor

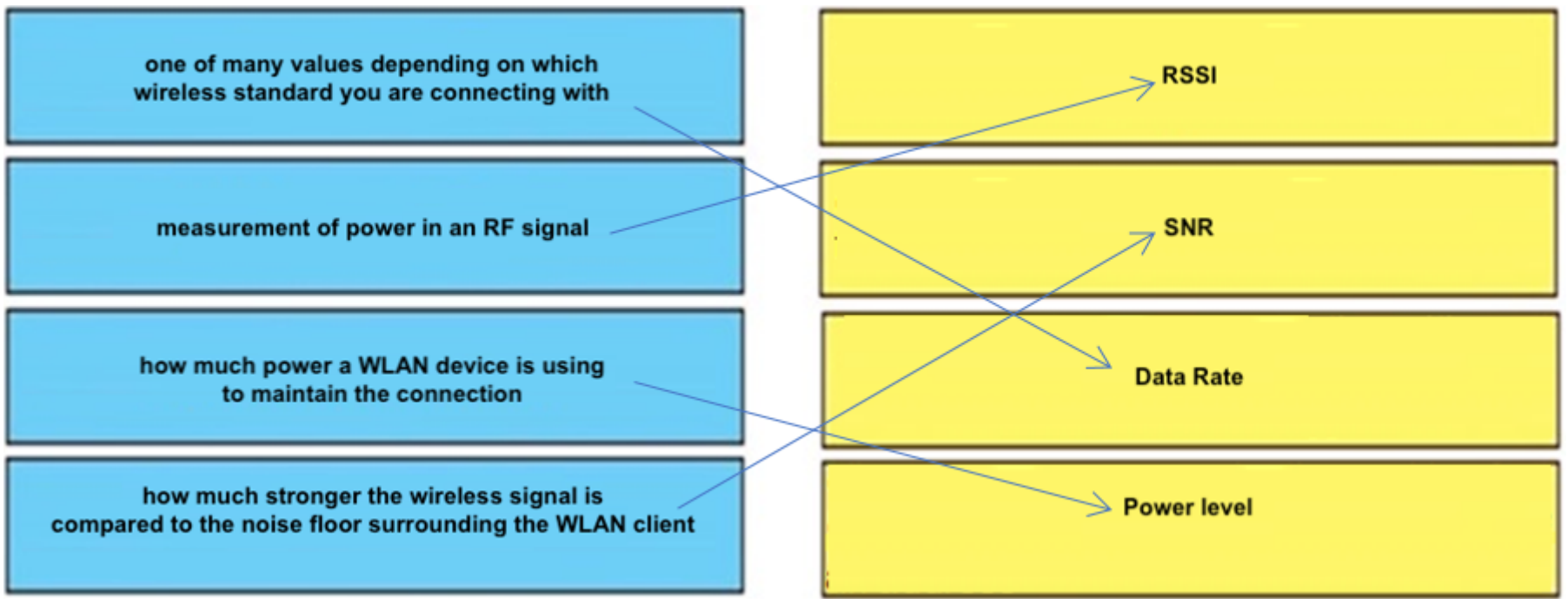
upvoted 1 times

DRAG DROP -

Drag and drop the definitions on the left to their respective technological names on the right.



Correct Answer:



TheDazzler Highly Voted 10 months, 1 week ago

Provided answer is correct.
https://ccie-or-null.net/2011/01/24/understanding-a-wi-fi-connection/

upvoted 9 times

jrquissak Most Recent 3 months ago

RSSI = for Received Signal Strength Indicator, and measures how well a client device can hear (receive) a signal
SNR = Signal-to-Noise Ratio is a ratio based value that evaluates your signal based on the noise being seen
Data Rate = Data Rate is defined as the amount of data transmitted during a specified time period over a network
Power level = The signal strength is the wireless signal power level received by the wireless client. Strong signal strength results in more reliable connections and higher speeds

upvoted 1 times

Question #659 *Topic 1*

Select the prerequisites for configuring LISP from the below options. (Choose two.)

A. Determine the type of LISP deployment you intend to deploy

B. One can directly deploy LISP without determining the type.

C. LISP configuration requires the datak9 license.

D. LISP configuration requires the advanced ip services license.

Correct Answer: *AC*

Community vote distribution

AC (92%) 8%

AndreasThornus Highly Voted 11 months, 3 weeks ago

Selected Answer: AC

From the article below:

Before you can configure Locator/ID Separation Protocol (LISP), you will need to determine the type of LISP deployment you intend to deploy. The LISP deployment defines the necessary functionality of LISP devices, which, in turn, determines the hardware, software, and additional support from LISP mapping services and proxy services that are required to complete the deployment.

LISP configuration requires the datak9 license.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html

upvoted 8 times

jhonmeikel Most Recent 3 months, 3 weeks ago

Selected Answer: AD

A - D

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/locator-id-separation-protocol-lisp/datasheet_c78-576698.html

upvoted 1 times

T_Cos 11 months, 1 week ago

Excellent

upvoted 1 times

iGlitch 1 year ago

Selected Answer: AC

Provided answers are correct.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html#GUID-CE94D60C-573B-40FA-916B-01810FCEF0FB

upvoted 3 times

Question #660 *Topic 1*

Select the benefits of implementing Cisco DNA Center. (Choose all that apply.)

A. Simplified management

B. Automatic VPN tunnelling

C. One click Configuration

D. Policy Driven Provisioning

E. Ensure Network & Appliance performance

Correct Answer: *ADE*

Community vote distribution

ADE (100%)

Gabiche Highly Voted 9 months, 2 weeks ago

What about one click configuration (you only have to click to provision devices, you can have templates to automate configuration, etc.), meaning every configuration is doing with clicking now.
Agree with the 3 other answers also.

upvoted 6 times

bora4motion Most Recent 1 year ago

Selected Answer: ADE

ADE seems OK with me

upvoted 1 times

iGlitch 1 year ago

Selected Answer: ADE

Provided answers are correct.

https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-so-cte-en.html#Benefits

upvoted 4 times

Question #661 *Topic 1*

A network administrator need to configure Netflow on the devices in his network. He has Source IP Address, Destination IP Address, Source Port number & Destination port number. What additional information do he need to configure Netflow.

A. Layer 3 Protocol type

B. Encryption type

C. ToS (Type of Service) byte

D. Input Logical Interface

E. Hashing Algorithm

F. Transform-set details

Correct Answer: *ACD*

Community vote distribution

ACD (100%)

iGlitch Highly Voted 1 year ago

Selected Answer: ACD

Missing the (choose three), but provided answers are correct.

"
NetFlow Flows Key Fields

A network flow is identified as a unidirectional stream of packets between a given source and destination--both are defined by a network-layer IP address and by transport-layer source and destination port numbers. Specifically, a flow is identified as the combination of the following key fields:

Source IP address

Destination IP address

Source port number

Destination port number

Layer 3 protocol type

Type of service (ToS)

Input logical interface
"

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/get-start-cfg-nflow.html#GUID-BE3FF8D7-C298-4C34-95DE-1CA27DB651EF

upvoted 11 times

Vlad_Is_Love_ua Most Recent 9 months, 3 weeks ago

Selected Answer: ACD

Traditionally, an IP flow is based on a set of five to seven IP packet attributes:

IP source address

IP destination address

Source port

Destination port

Layer 3 protocol type

CoS

Router or switch interface

upvoted 1 times

Question #662 *Topic 1*

A network administrator is configuring a configuration management tool for some network devices that does not support agent. Select what option will you pick from the below options to successfully configure configuration management tool for that device.

A. Agent based Configuration

B. Agent Less Configuration

C. Proxy-agent Configuration

D. None of the above

Correct Answer: *C*

Community vote distribution

B (74%) C (21%) 5%

CCNPWILL 1 month, 3 weeks ago

Selected Answer: B

Trying not to think too hard.. Going for B.

Also, ChatGPT also thinks B.

upvoted 2 times

mgiuseppe86 2 months, 2 weeks ago

Selected Answer: B

The grammar is horrible.

Yes the question does state "some network devices that do not support an agent." but that is what the question is referring to, the question is not asking to find a common management tool for all devices, just the ones that do not support an agent... I am going with B on this one based on the last part of the question alone "What option will you pick... for THAT device?"

upvoted 1 times

teikitiz 4 months, 2 weeks ago

Selected Answer: C

Yet another one of those... Only some of the devices don't support agents, which means overall an agent based management solution has been devised. To continue to use this agent based solution on non-capable devices, a proxy-agent workaround needs to be implemented. My perspective, only.

upvoted 2 times

felix_simon 5 months ago

C

The question is how to configure proxy tools when proxy is not supported, so it can only be the proxy of the agent.

upvoted 1 times

Splashisthegreatestmovie 5 months, 2 weeks ago

The first problem with this question is the grammar. It reads like it was written by a seconder grader. The english problems in this question should make it invalid.

upvoted 1 times

mgiuseppe86 2 months, 2 weeks ago

have you spoken to Cisco TAC Before? Yeah? So these questions arent far off.

upvoted 1 times

Clauster 8 months, 3 weeks ago

Selected Answer: D

Answer is D,
None of those are Configuration Management Tools. It's like saying what type of protocol supports Unequal Load Balancing, will the answer be Advanced Distance Vector ? No

upvoted 1 times

Uzzi1222 9 months, 1 week ago

Selected Answer: B

Proxy-agent configuration: This type of configuration does not require an agent on every device, but it does require some type of “process” or “worker” to communicate with the master server and the remote device.

upvoted 2 times

Burik 5 months, 2 weeks ago

You voted B and provided explanation for C.. huh?

upvoted 1 times

Nickplayany 9 months, 3 weeks ago

Selected Answer: C

It´s soooo snicky question - ``some network devices``

Proxy-agent configuration: This type of configuration does not require an agent on every device

C it is :(

upvoted 2 times

snarkymark 9 months, 3 weeks ago

Well, C, can work too.
https://www.ciscopress.com/articles/article.asp?p=3100057&seqNum=3

upvoted 1 times

snarkymark 9 months, 3 weeks ago

So, looking at the question again, I think I may lean towards C. Since the question states "some" devices may not support agents. In that case you can use puppet with a proxy for those devices and puppet with an agent for those devices that support agents

upvoted 2 times

AndreasThornus 11 months, 3 weeks ago

B B B B and again, B.

Just in case you weren't sure, it's B.

upvoted 4 times

BertWhipple 10 months, 1 week ago

Is it B then? ;-)

upvoted 1 times

Zikosheka 11 months, 3 weeks ago

Selected Answer: B

I think it's B

upvoted 1 times

forccnp 1 year ago

Selected Answer: B

It's BBBBB

upvoted 4 times

iGlitch 1 year ago

Selected Answer: B

Surly it's 'Agentless' ?

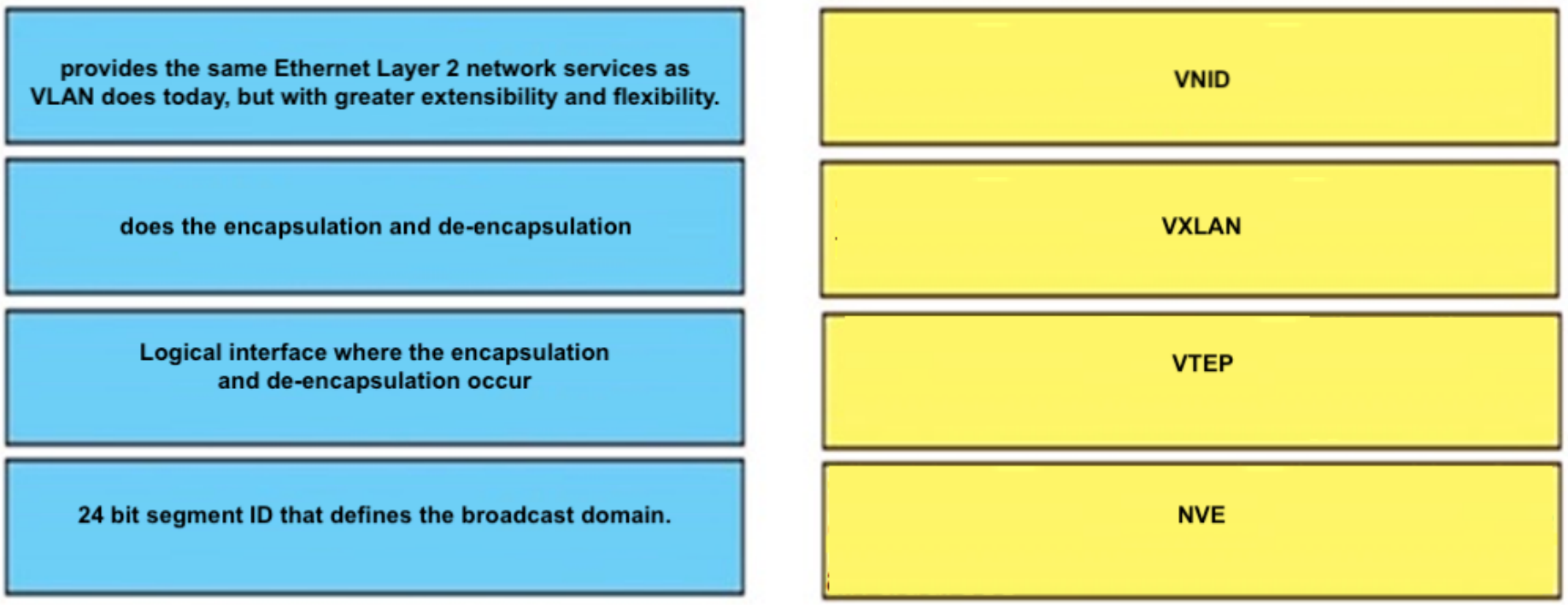
upvoted 4 times

Question #663 *Topic 1*

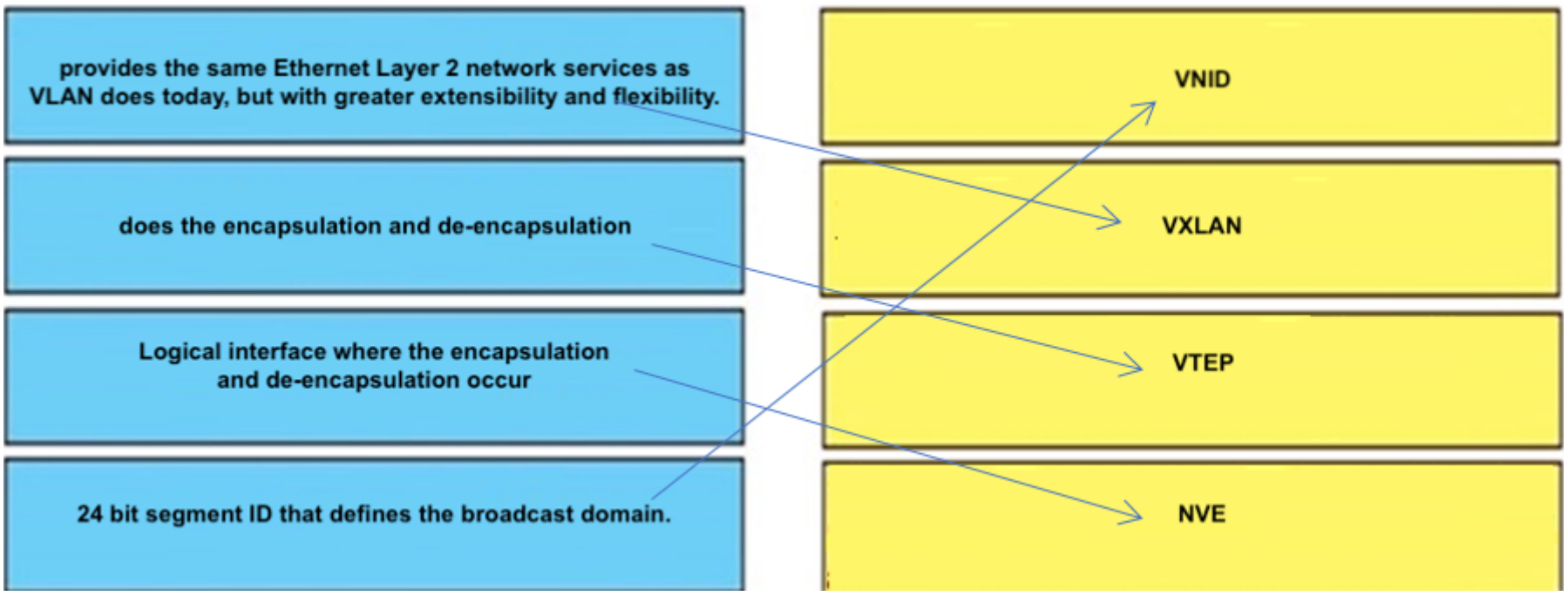
DRAG DROP

-

Drag and drop the definitions in the left to their respective Terminology in the right.



Correct Answer:



PeterTheCheater Highly Voted 1 year ago

correct
Terminology
VXLAN (Virtual Extensible LAN) - The technology that provides the same Ethernet Layer 2 network services as VLAN does today, but with greater extensibility and flexibility.

VNID (Vxlan Network Identifier) - 24 bit segment ID that defines the broadcast domain. Interchangeable with "VXLAN Segment ID".

VTEP (Virtual Tunnel Endpoint) - This is the device that does the encapsulation and de-encapsulation.

NVE (Network Virtual Interface) - Logical interface where the encapsulation and de-encapsulation occur.

upvoted 10 times

Asymptote 10 months, 3 weeks ago

Reference:
https://www.cisco.com/c/en/us/support/docs/switches/nexus-9000-series-switches/118978-config-vxlan-00.html#:~:text=VXLAN%20(Virtual%20Extensible,de%2Dencapsulation%20occur.

upvoted 1 times

Question #664 *Topic 1*

Select the devices from the below options that can be fart of Cisco SDWAN Solution. (Choose two.)

A. ISR 2900

B. ASR 1000

C. IR8300

D. FTD 1120

E. ASR 9000

Correct Answer: *BC*

Community vote distribution

BC (100%)

jzzmth Highly Voted 11 months ago

This ones tricky, I wasn't aware Cisco supported fart protocols....

upvoted 37 times

HarLikon 3 months ago

HAHAHA

upvoted 1 times

well123 9 months, 2 weeks ago

lol :)...

upvoted 1 times

x3rox 10 months ago

hah...

upvoted 1 times

x3rox Highly Voted 10 months ago

so we are suppose to know ALL the models that support SDA to be a CCNP. ¯_(ツ)_/¯

upvoted 15 times

mgiuseppe86 2 months, 2 weeks ago

Didnt you know, networking isnt about networking anymore.

upvoted 2 times

HarwinderSekhon 5 months, 2 weeks ago

you have to about sales too. New CCNP is not just about networking, its also to turn you into sales.

upvoted 3 times

c946f3e Most Recent 6 months, 2 weeks ago

i think it is a typo, it should be 'Part', then it makes more sense

Select the devices from the below options that can be Part of Cisco SDWAN Solution.

upvoted 3 times

rtfgvb 6 months, 2 weeks ago

I can’t find any information about Fart protocols, maybe something Cisco proprietary and secret ;)

upvoted 3 times

Dataset 8 months ago

Fart is a noisy protocol...and stinks
JAJAJJAJ
Regards

upvoted 4 times

BobbyFlash 4 months, 2 weeks ago

hahaha

upvoted 1 times

Cooldude89 9 months, 2 weeks ago

Selected Answer: BC

ASR FART 1000 and 1r8300 , wait ,i for to add fart IR FART 830

upvoted 1 times

Jey117 9 months, 2 weeks ago

Fart LOLOLOOOOOOOOOOOOOOOOOOOOOOOOOOOOOL xD

upvoted 1 times

AndreasThornus 11 months, 3 weeks ago

Selected Answer: BC

ASR1000
IR8300

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/compatibility/sdwan-device-compatibility.html

upvoted 4 times

AndreasThornus 11 months, 3 weeks ago

Never was a question more appropriately asked! :)

upvoted 3 times

Ioannis34 11 months ago

hahahaah...indeed!

upvoted 2 times

Darude 1 year ago

Selected Answer: BC

answer is correct:
reference:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/compatibility/sdwan-device-compatibility.html#device-compat-ir8300rugged

upvoted 2 times

Question #665 *Topic 1*

What is the purpose of the weight attribute in an EID-to-RLOC mapping?

A. It determines the administrative distance of LISP generated routes in the RIB.

B. It indicates the load-balancing ratio between ETRs of the same priority.

C. It indicates the preference for using LISP over native IP connectivity.

D. It identifies the preferred RLOC address family.

Correct Answer: *B*

Community vote distribution

B (100%)

[Removed] 4 months, 3 weeks ago

Selected Answer: B

Load balance between multiple EID-To-RLOCs

This document has more information, scroll down to Usage Guidelines

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/command/ip-lisp-cr-book/ip-lisp-cr-book_chapter_01010.html

upvoted 1 times

snarkymark 9 months, 2 weeks ago

Selected Answer: B

http://www.watersprings.org/pub/id/draft-ietf-lisp-rfc6830bis-32.html
hen multiple RLOC have the same 'Priority' then the 'Weight' states how to load balance traffic among them. The value of the 'Weight' represents the relative weight of the total packets that match the maping entry.

upvoted 2 times

Nickplayany 9 months, 2 weeks ago

Selected Answer: B

Probably B

In the LISP context, for each RLOC mapped to an EID, the mapping system provides a priority and a weight [4]. When several RLOCs have the same priority, the LISP traffic is split among the different RLOCs in proportion to their weight. This makes possible to control the traffic that enters a site by tuning the RLOCs sent to different sources and also by changing their priorities and weights.

upvoted 1 times

Question #666 *Topic 1*

A network engineer is designing a QoS policy for voice and video applications. Which software queuing feature provides strict-priority servicing?

A. Class-Based Weighted Fair Queuing

B. Low Latency Queuing

C. Link Fragmentation

D. Automatic QoS

Correct Answer: *B*

Community vote distribution

B (100%)

snarkymark 9 months, 2 weeks ago

Selected Answer: B

https://en.wikipedia.org/wiki/Low-latency_queuing
Low-latency queuing (LLQ) is a feature developed by Cisco to bring strict priority queuing (PQ) to class-based weighted fair queuing (CBWFQ). LLQ allows delay-sensitive data (such as voice) to be given preferential treatment over other traffic by letting the data to be dequeued and sent first.

upvoted 3 times

Question #667 *Topic 1*

Which characteristic applies to a traditional WAN solution but not to a Cisco SD-WAN solution?

A. lengthy installation times

B. centralized reachability, security, and application policies

C. low complexity and increased overall solution scale

D. operates over DTLS/TLS authenticated and secured tunnels

Correct Answer: *A*

Community vote distribution

A (80%) B (20%)

ihateciscoreally 3 months, 2 weeks ago

you can answer this question without even knowing thing about SD-WAN. this question is boasting about cisco technologies, only answer A seems to be pejorative so it would apply to standard SD-WAN, not GODLIKE CISCO SD-WAN SOLUTION.

upvoted 1 times

Lungful 3 months, 3 weeks ago

Selected Answer: A

I think A because B is listed as an SD-WAN characteristic on https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html#~benefits
"A single, centralized, cloud-delivered management dashboard for configuration and management of WAN, cloud, and security"

upvoted 1 times

andyforreg 4 months, 2 weeks ago

Selected Answer: B

It can be B

upvoted 1 times

felix_simon 5 months ago

B
https://www.geeksforgeeks.org/difference-between-traditional-wan-and-sd-wan/
Security: Traditional WANs are typically highly secure, as they use dedicated circuits and leased lines to ensure data confidentiality and integrity.
Reliability: Traditional WANs offer reliable connectivity, as they use dedicated circuits that are typically highly available and have low latency.
Control: Traditional WANs offer complete control over network traffic, allowing organizations to prioritize certain types of traffic over others and configure routing policies as needed.

upvoted 1 times

felix_simon 5 months ago

B
traditional WAN solution with centralized reachability, security, and application policies

upvoted 1 times

Nayef20233 5 months, 2 weeks ago

this is really strange , look at this question from dumps i have:
what is a characteristic of a traditional WAN?
A low complexity and high overall solution scale.
B centralized reachability,security, and application policies.
C operates over DTLS and TLS authenticated and secure tunnel.
D unified data plane and control plane.

and they put B as a correct answer , suprise !!!

upvoted 2 times

Brandonkiaora 3 weeks, 5 days ago

Shouldn't this be D, as the traditional WAN has a unified data plane and control plane; and the SD-WAN has a separate data plane and control plane?

upvoted 1 times

examtopicsacct 5 months, 3 weeks ago

Cisco flex question

upvoted 2 times

byallmeans 6 months, 4 weeks ago

from my personal experience Cisco's SD-WAN solution can be a real sh!t show and ends up taking more time than traditional WAN. But obviously that's not the answer they're looking for :)

upvoted 3 times

HarwinderSekhon 5 months, 2 weeks ago

agree. CCNP is created by Sales people lol.

upvoted 2 times

snarkymark 9 months, 2 weeks ago

Selected Answer: A

https://sase.vmware.com/sd-wan/sd-wan-vs-traditional-wan

upvoted 3 times

Question #668 *Topic 1*

What is a characteristic of traffic shaping?

A. drops out-of-profile packets

B. causes TCP retransmits when packets are dropped

C. can be applied in both traffic directions

D. queues out-of-profile packets until the buffer is full

Correct Answer: *D*

Community vote distribution

D (100%)

felix_simon 5 months ago

D
https://avinetworks.com/glossary/traffic-shaping/
Transitioning from a high speed interface to a low speed interface can cause egress blocking: tail drop or packet loss in the outgoing queue. Prevent this issue by configuring egress traffic shaping to ensure all packets are eventually sent, at least until the buffer fills.

upvoted 1 times

bk989 7 months, 1 week ago

Another consideration is that queueing packets up to be sent later—traffic shaping—can only ever apply to outbound traffic. True inbound traffic shaping does not exist, because inbound traffic is the realm of traffic policing.
https://avinetworks.com/glossary/traffic-shaping/#:~:text=Another%20consideration%20is%20that%20queueing,the%20realm%20of%20traffic%20policing.

upvoted 1 times

snarkymark 9 months, 2 weeks ago

Selected Answer: D

https://www.ccexpert.us/qos-implementing/policing-vs-shaping.html

upvoted 2 times

well123 9 months, 2 weeks ago

Selected Answer: D

Answer is correct

upvoted 1 times

Question #669 *Topic 1*

What is a characteristic of para-virtualization?

A. Para-virtualization allows the host hardware to be directly accessed.

B. Para-virtualization guest servers are unaware of one another.

C. Para-virtualization lacks support for containers.

D. Para-virtualization allows direct access between the guest OS and the hypervisor.

Correct Answer: *D*

Community vote distribution

D (100%)

shefo1 2 weeks, 2 days ago

in where OCG describe the para-virtualization ??

upvoted 1 times

felix_simon 5 months ago

D
https://en.wikipedia.org/wiki/Paravirtualization
By allowing the guest operating system to indicate its intent to the hypervisor, each can cooperate to obtain better performance when running in a virtual machine.

upvoted 1 times

snarkymark 9 months, 2 weeks ago

Selected Answer: D

https://blackberry.qnx.com/en/ultimate-guides/automotive-hypervisor/paravirtualization

upvoted 1 times

well123 9 months, 2 weeks ago

Selected Answer: D

correct answer

upvoted 2 times

Nickplayany 9 months, 2 weeks ago

Selected Answer: D

Paravirtualization is a type of virtualization where software instructions from the guest operating system running inside a virtual machine can use “hypercalls” that communicate directly with the hypervisor.

upvoted 4 times

Question #670 *Topic 1*

What is a Type 2 hypervisor?

A. installed as an application on an already installed operating system

B. also referred to as a “bare metal hypervisor” because it sits directly on the physical server

C. runs directly on a physical server and includes its own operating system

D. supports over-allocation of physical resources

Correct Answer: *A*

Community vote distribution

A (100%)

snarkymark 9 months, 2 weeks ago

Selected Answer: A

https://www.hitechnectar.com/blogs/hypervisor-type-1-vs-type-2/

upvoted 1 times

well123 9 months, 2 weeks ago

Selected Answer: A

Correct answer

upvoted 1 times

Question #671 *Topic 1*

What is a characteristic of a Type 1 hypervisor?

A. It is referred to as a hosted hypervisor.

B. It is completely independent of the operating system.

C. Problems in the base operating system can affect the entire system.

D. It is installed on an operating system and supports other operating systems above it.

Correct Answer: *B*

Community vote distribution

B (83%) D (17%)

pmmg 7 months, 4 weeks ago

Selected Answer: B

should be completely independent of an underlying operating system.

upvoted 3 times

bendarkel 9 months, 1 week ago

Selected Answer: B

B is the correct answer.

upvoted 3 times

snarkymark 9 months, 2 weeks ago

Selected Answer: B

B seems to be the closest that makes sense, even though do not like the wording.

upvoted 4 times

well123 9 months, 2 weeks ago

Selected Answer: D

correct

upvoted 2 times

CCNPWILL 1 month, 3 weeks ago

You memorized the wrong question. The exam asks for both type.1 and type 2. be careful EVERYTHING before answering questions. We pay for GOOD information, remember. if you arent sure. say that when you comment.

upvoted 1 times

CCNPWILL 1 month, 3 weeks ago

Read everything*

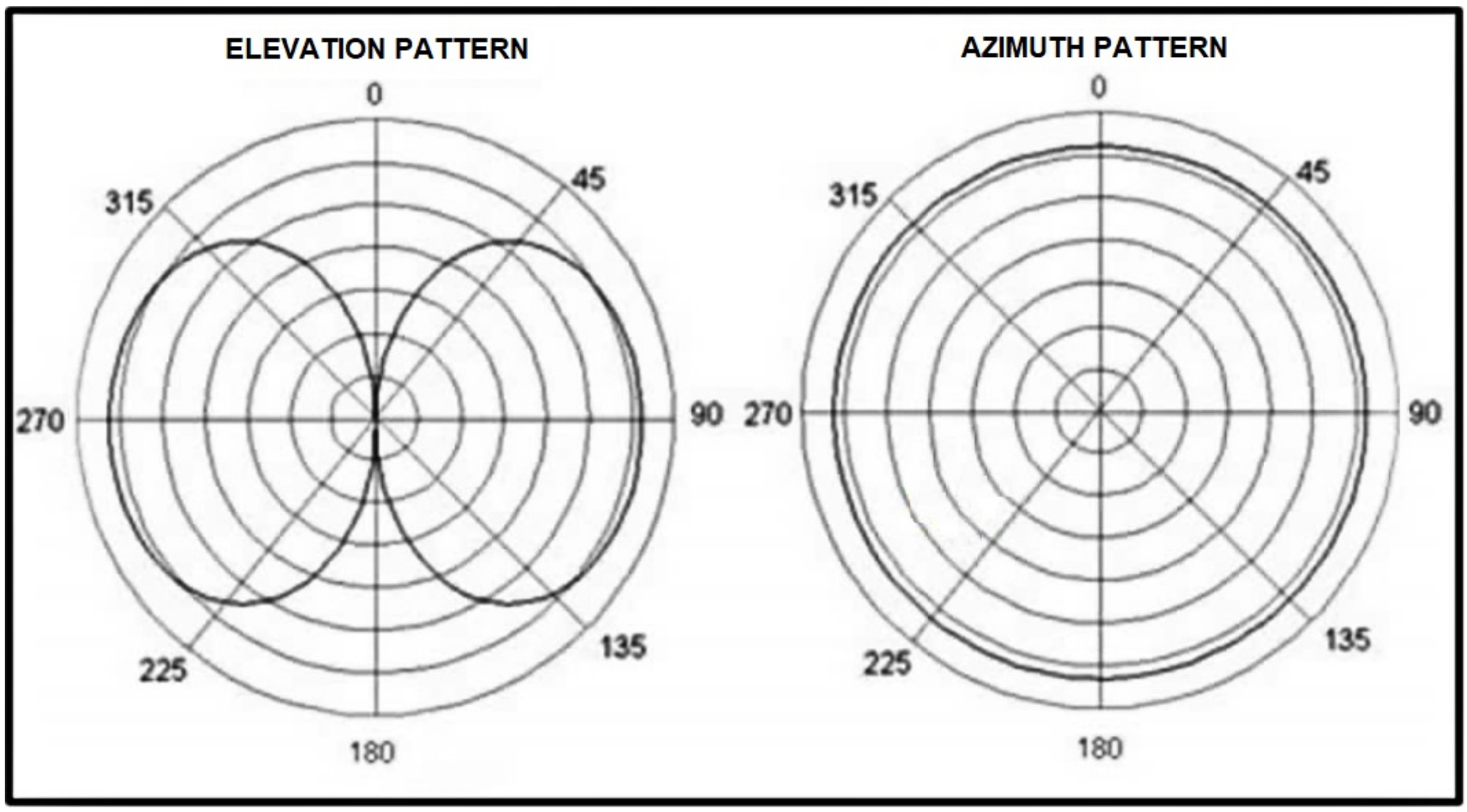
upvoted 1 times

well123 9 months, 2 weeks ago

typo it is B

upvoted 3 times

Refer to the exhibit.



Which antenna emits this radiation pattern?

A. omnidirectional

B. RP-TNC

C. dish

D. Yagi

Correct Answer: *A*

Community vote distribution

A (100%)

Entivo 4 months, 4 weeks ago

Looks like Dipole to me.

upvoted 3 times

NLFluke 4 months ago

And it is, because it's categorized as a common type of omnidirectional antenna:

https://study-ccnp.com/directional-antenna-vs-omnidirectional-antenna/

upvoted 2 times

snarkymark 9 months, 2 weeks ago

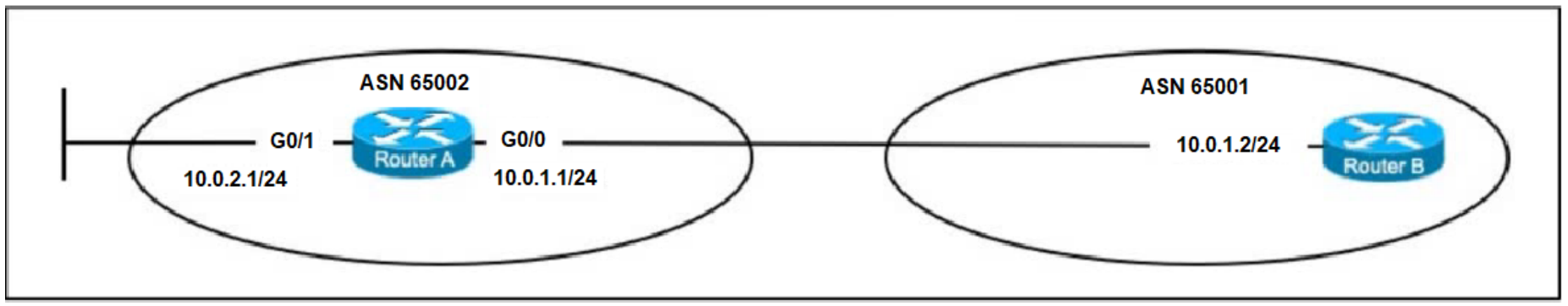
Selected Answer: A

https://www.mpantenna.com/omnidirectional-antenna-radiation-patterns/

upvoted 3 times

Question #673 *Topic 1*

Refer to the exhibit.



A. router bgp 65002
neighbor 10.0.1.2 remote-as 65002
network 10.0.2.0 255.255.255.0

B. router bgp 65001
neighbor 10.0.1.2 remote-as 65002
redistribute static

C. router bgp 65001
neighbor 10.0.1.2 remote-as 65002
network 10.0.1.0 255.255.255.0

D. router bgp 65001
neighbor 10.0.1.2 remote-as 65002
network 10.0.2.0 255.255.255.0

Correct Answer: *D*

Community vote distribution

D (100%)

snarkymark Highly Voted 9 months, 2 weeks ago

Unless I am missing something here, none of these are right. Let me know if I am missing something.

upvoted 14 times

M2013 Most Recent 2 months, 3 weeks ago

The questin is confusing me. as I understand the configuration should be done on router A not B.
an engineer must configure a BGP neighborship to Router B on router A. the network that is connected to G0/1 on router A must be advertised to router B. which configuration should be applied

upvoted 1 times

TroyMcLure 5 months ago

Selected Answer: D

The wording of the question is mising. It should have been as follows:
"An engineer must configure an eBGP neighborship to Router B on Router A. The network that is connected to G0/1 on Router A must be advertised to Router B. Which configuration should be applied?"
That makes D the correct answer, even though the keyword "mask" is missing from the network statement.

upvoted 2 times

HarwinderSekhon 5 months ago

remote as IP is wrong.
D is not correct either

upvoted 2 times

TroyMcLure 3 months, 3 weeks ago

The AS numbers are clearly inverted.
Router A belongs to AS 65001 and Router B belongs to AS 65002.
Considering that, the best option is D.

upvoted 1 times

Leoveil 5 months, 2 weeks ago

let assume that Router A is AS65001(because .1 on interface 0/0 and g0/1) and Router B in AS65002,
answer B would be correct if redistribute connected rather than static

upvoted 1 times

Splashisthegreatestmovie 5 months, 3 weeks ago
this is why people use test dumps!
upvoted 4 times

Papins 6 months, 2 weeks ago
what is the question? the provided answer also is wrong? it could be C if my understanding on the diagram provided is correct :)
upvoted 1 times

Papins 6 months, 2 weeks ago
sory.. i misread it C also is wrong... none of them is correct.
upvoted 2 times

SAMAKEMM 6 months, 3 weeks ago
none of them is correct
upvoted 2 times

owenshinobi 7 months ago
What the question !!!
No question, no correct answer.
upvoted 3 times

Dataset 8 months ago
Hi !
Admin, please fix the diagram...
Regards
upvoted 2 times

Shansab 8 months ago
The diagram is not correct
upvoted 1 times

MJane 8 months, 3 weeks ago
is also missing the mask keyword, so ABD not correct as of now
upvoted 1 times

bendarkel 9 months, 1 week ago
No question, no correct answer.
upvoted 3 times

Cooldude89 9 months, 2 weeks ago
Please fix this Admin ?
upvoted 2 times

Jey117 9 months, 2 weeks ago
Admin fix it.

It doesn´t even include the question and the answer makes no sense at all to guess it.
upvoted 2 times

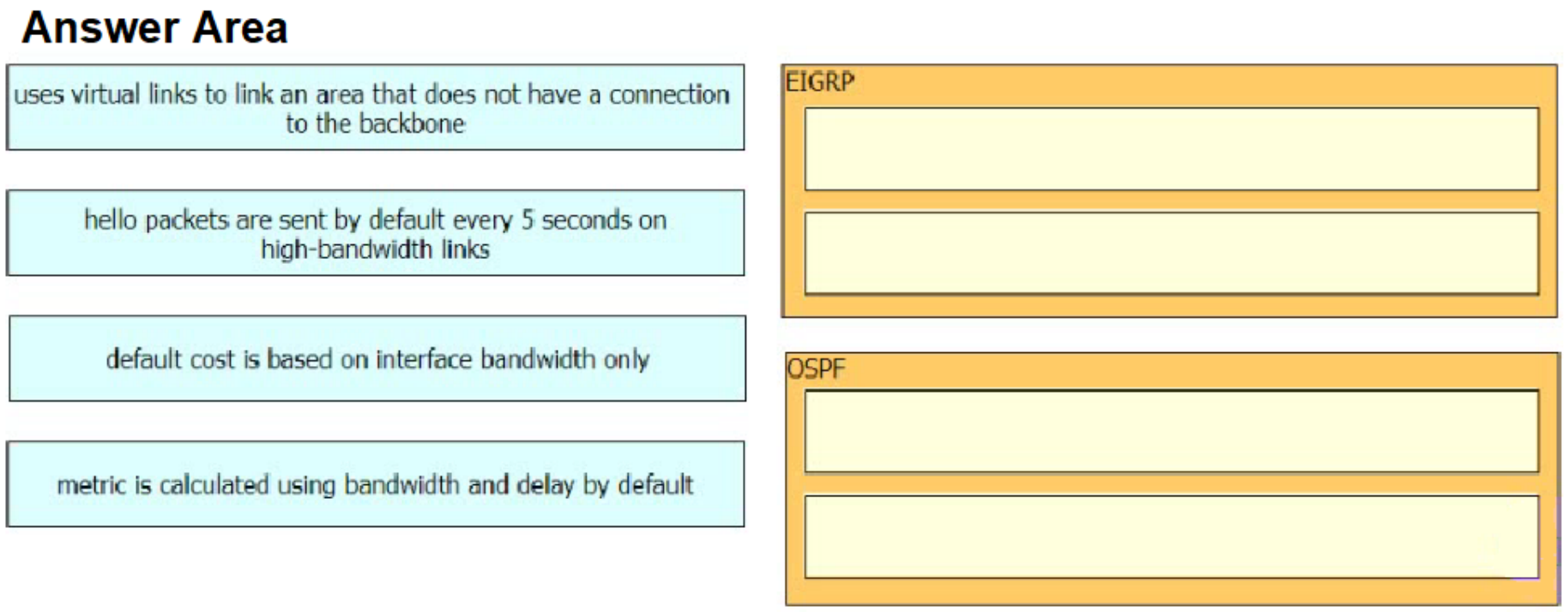
well123 9 months, 2 weeks ago
probably the diagram isn't correct
AS should be interchanged for D to be correct!
upvoted 1 times

well123 9 months, 2 weeks ago
ip addresses should be interchanged not AS
upvoted 1 times

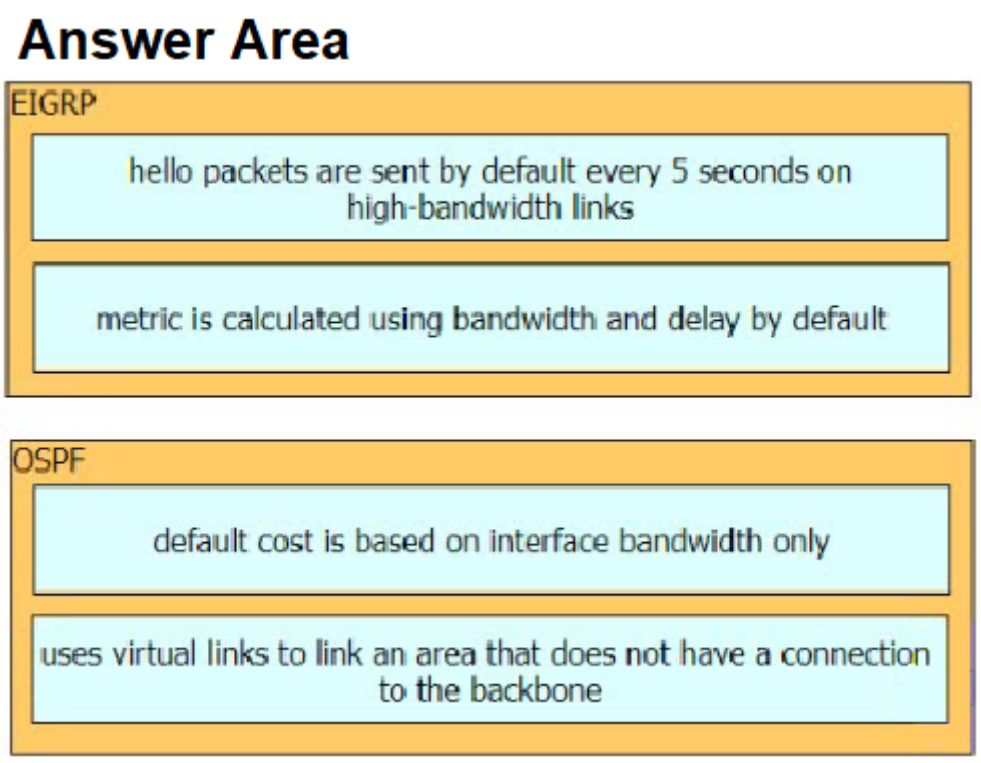
DRAG DROP

-

Drag and drop the characteristics from the left onto the routing protocols they describe on the right.



Correct Answer:



snarkymark 9 months, 2 weeks ago

Correct:
EIGRP: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html

OSPF: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

upvoted 4 times

Question #675 *Topic 1*

What are two best practices when designing a campus Layer 3 infrastructure? (Choose two.)

A. Configure passive-interface on nontransit links.

B. Implement security features at the core.

C. Summarize routes from the aggregation layer toward the core layer.

D. Tune Cisco Express Forwarding load balancing hash for ECMP routing.

E. Summarize from the access layer toward the aggregation layer.

Correct Answer: *CD*

Community vote distribution

CD (53%) AC (47%)

Burik 4 months, 2 weeks ago

Selected Answer: CD

We should not implement security features at the core as it would reduce the speed in this layer -> Answer B is not correct.

It is a recommended practice to configure summarization in a large network from the distribution layers toward the core. Implementing summarization at the distribution layer optimizes the convergence process -> Answer C is correct while answer E is not correct.

Reference: https://www.ccexpert.us/network-design/route-summarization.html

Also in the above link, it is recommended to configure "Passive Interfaces for IGP at the Access Layer", not "nontransit links" which makes answer A to be not correct.

"As a best practice for ECMP-based Layer 3 networks, Cisco recommends fine-tuning Cisco Express Forwarding load balancing to include Layer 3 and Layer 4 tuple inclusion to compute and derive the first phase of the optimal forwarding decision process between two upstream Layer 3 MEC interfaces." -> Answer D is correct.

Reference: https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_enterprise_campus_infrastructure_design_guide.pdf

upvoted 2 times

rogue_user 4 months, 2 weeks ago

Selected Answer: AC

D is a catch since fine tuning ECMP hash is not required, you just need to have it in place.
https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_enterprise_campus_infrastructure_design_guide.pdf
Nowhere in the guide you can find "fine tune" part.

upvoted 1 times

sam6996 4 months, 2 weeks ago

"As a best practice for ECMP-based Layer 3 networks, Cisco recommends fine-tuning Cisco Express Forwarding load balancing to include Layer 3 and Layer 4 tuple inclusion to compute and derive the first phase of the optimal forwarding decision process between two upstream Layer 3 MEC interfaces." this is under the General Routing Recommendations and Equal Cost Multipath Routing Best practices.

upvoted 1 times

[Removed] 4 months, 3 weeks ago

Selected Answer: CD

CD are correct
https://www.ciscopress.com/articles/article.asp?p=1315434&seqNum=3

upvoted 2 times

felix_simon 5 months ago

CD
https://www.ciscopress.com/articles/article.asp?p=1315434&seqNum=3
A. C is implemented in the routing protocol design, but configuring the passive interface for A requires manual operation on the port, so it is not the best method.

upvoted 1 times

bob_135 5 months, 1 week ago

Selected Answer: CD

As a best practice for ECMP-based Layer 3 networks, Cisco recommends fine-tuning Cisco Express Forwarding load balancing to include Layer 3 and Layer 4 tuple inclusion to compute and derive the first phase of the optimal forwarding decision process between two upstream Layer 3 MEC interfaces.

upvoted 1 times

yuusui 7 months ago

Selected Answer: CD

C, D is correct.
https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKCRS-2031.pdf

A is incorrect. "Only peer on links that you intend to use as transit" cisco said.
In pdf p42, the link are used for L2 transit but configured passive-interface.

upvoted 2 times

HungarianDish 8 months, 1 week ago

Based on these A,C, and D are all true:
https://www.ciscopress.com/articles/article.asp?p=1315434&seqNum=3

https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_enterprise_campus_infrastructure_design_guide.pdf

upvoted 1 times

Badger_27 8 months, 3 weeks ago

Selected Answer: AC

Could be A,C or D - hopefully Cisco give credit for all three in the exam.
https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_enterprise_campus_infrastructure_design_guide.pdf

upvoted 3 times

DavideDL 8 months, 4 weeks ago

Selected Answer: AC

https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_enterprise_campus_infrastructure_design_guide.pdf

Block OSPF neighbor processing with passive-mode configuration on physical or logical interfaces connected to non-EIGRP devices in the network, such as PCs, wireless LAN controllers,
and so on. This best practice helps reduce CPU utilization and secures the network with unprotected OSPF
adjacencies with untrusted devices

I think A,C could be the correct answer.

upvoted 3 times

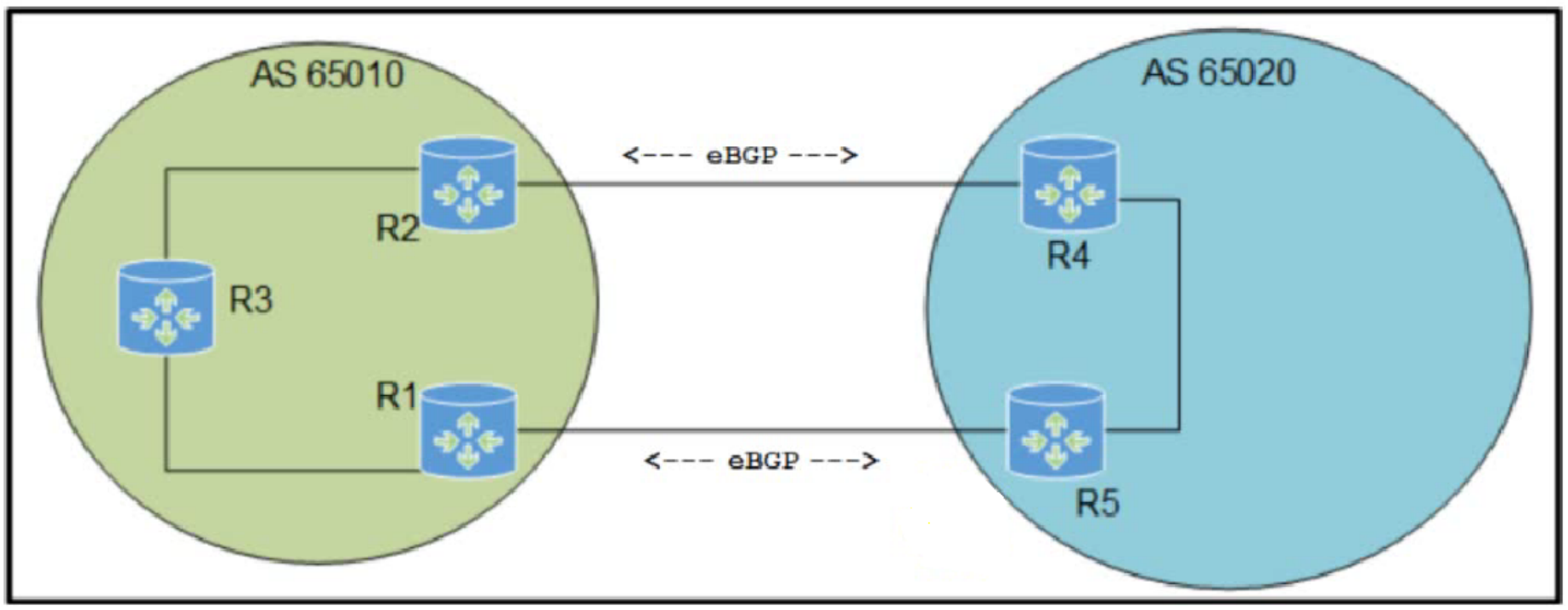
snarkymark 9 months, 2 weeks ago

Selected Answer: CD

agree with C D.
https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_enterprise_campus_infrastructure_design_guide.pdf

upvoted 1 times

Refer to the exhibit.



Which configuration must be applied to ensure that the preferred path for traffic from AS 65010 toward AS 65020 uses the R2 to R4 path?

A. R4(config)# router bgp 65020 -
R4(config-router)# bgp default local-preference 300

R5(config)# router bgp 65020 -
R5(config-router)# bgp default local-preference 200

B. R2(config)# router bgp 65010 -
R2(config-router)# bgp default local-preference 300

R1(config)# router bgp 65010 -
R1(config-router)# bgp default local-preference 200

C. R2(config)# router bgp 65010 -
R2(config-router)# bgp default local-preference 200

R1(config)# router bgp 65010 -
R1(config-router)# bgp default local-preference 300

D. R4(config)# router bgp 65020 -
R4(config-router)# bgp default local-preference 200

R5(config)# router bgp 65020 -
R5(config-router)# bgp default local-preference 300

Correct Answer: *B*

Community vote distribution

B (100%)

PureInertiaCopy 3 months, 1 week ago
What wouldn't A work?
upvoted 1 times

Din04 8 hours, 22 minutes ago
local preference attribute is local to the AS. it will not transcend to remote AS, thus will not influence their route decisions.
upvoted 1 times

PureInertiaCopy 3 months, 1 week ago
Oh... "Local" Preference. Literally.
upvoted 1 times

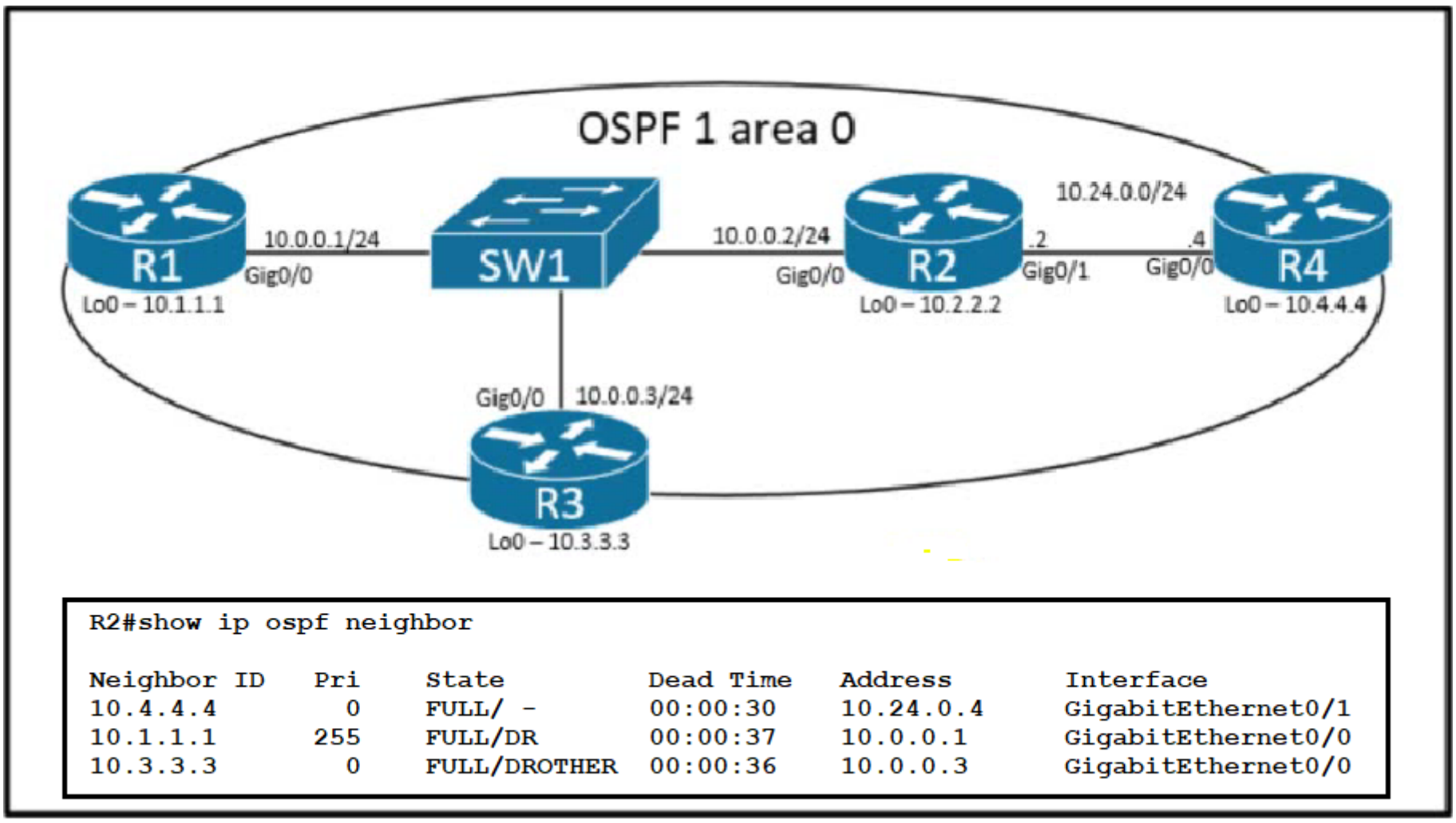
snarkymark 9 months, 2 weeks ago

Selected Answer: B

Agree with B.
https://ipwithease.com/bgp-local-preference-attribute/

upvoted 3 times

Refer to the exhibit.




```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.4.4.4          0   FULL/ -         00:00:30    10.24.0.4       GigabitEthernet0/1
10.1.1.1        255   FULL/DR         00:00:37    10.0.0.1        GigabitEthernet0/0
10.3.3.3          0   FULL/DROTHER    00:00:36    10.0.0.3        GigabitEthernet0/0
```

An engineer must reduce the number of Type 1 and Type 2 LSAs that are advertised to R4 within OSPF area 0. Which configuration must be applied?

A. R1# conf t -

Router(config)# router ospf 1 -
Router(config-router)# prefix-suppression

B. R4# conf t -

Router(config)# router ospf 1 -
Router(config-router)# summary-address 10.0.0.0 255.255.255.0

C. R2# conf t -
Router(config)# interface Gig0/0
Router(config-router)# ip ospf prefix-suppression

D. R2# conf t -

Router(config)# int Gig0/0 -
Router(config-if)# ip summary-address 10.0.0.0 255.255.255.0

Correct Answer: *A*

Community vote distribution

A (61%) C (39%)

snarkymark Highly Voted 9 months, 2 weeks ago

I would think prefix suppression would be better if placed on R2 on the interface facing R4.
Being applied globally on R1 won't suppress routes from other routers to R4. Like to see what others think.
https://itskillbuilding.com/networking/network/ospf/ospf-prefix-suppression/

upvoted 8 times

djedeen Most Recent 3 months, 1 week ago

Selected Answer: A

Going with A. There are 2 approaches for prefix suppression, global mode configuration and interface mode configuration. The global config (option A) only requires the config shown, interface level suppression would need to be applied on multiple interfaces for the same effect.
upvoted 1 times

alex711 3 months, 3 weeks ago

Selected Answer: C

I testet it on gns3. It is C.
upvoted 1 times

jubrilak 4 months, 1 week ago

The corect answer is A. Why?
1) The suppression for each transit subnet is effected by the DR for that link
2) Only advertised transit link prefixes are affected, hence the prefixes to be suppressed is only the 10.0.0.0/24 prefix, because 10.24.0.0/24 prefix is a connected prefix to R4.
3) Simply implementing the prefix suppression on R1, will suppress 10.0.0.0/24 prefix in the FIB of R4
4) If you implement ip ospf prefix suppression on R2, it won't suppress the 10.0.0.0/24 prefix on R4, because it is not the DR for that segment.
upvoted 3 times

rogue_user 4 months, 2 weeks ago

Selected Answer: C

If you apply A it will have effect in opposite direction as well
upvoted 1 times

nikramor 4 months, 3 weeks ago

Selected Answer: A

I simulated this topology and the correct answer is A.
Only prefix-suppression on R1(DR) under router ospf 1 is needed.
You can enable prefix suppression on links between R1-R2 and it would work like a charm.
But on this question i'd choose A
upvoted 4 times

ajeetnagdev 5 months ago

A is correct. Type 2 – Network LSA: Network LSAs are generated by the DR. Router R1 is DR.
upvoted 3 times

felix_simon 5 months ago

C
If A is selected, type 1 and type 3LSA announcements between R1 and R3 will be suppressed, which is not true.
upvoted 1 times

massimp 5 months, 2 weeks ago

Selected Answer: A

C should be the most correct, unless the interface is wrong (must be gi0/1). So A is the most correct.
upvoted 2 times

foreignbishop 6 months, 1 week ago

Selected Answer: C

R1 may be the DR in the segment but NOT the entire area. Therefore, the P2P link communication between 2 and 4 would be different regarding LSA advertisements. Therefore, I think C is correct.
upvoted 1 times

ALOVEVIKS 6 months, 2 weeks ago

Selected Answer: A

OSPF prefix-suppression is a useful feature in order to reduce the number of Link State Advertisement (LSA) that are flooded within an area. In an OSPF area which has multiple transit links between hosts and actual communication is between the hosts. There is no need to advertise the transit link LSAs to all the routers. You can only advertise the LSAs related to end hosts. By default, OSPF advertises all the LSAs that include the transit link LSAs.

OSPF prefix-suppression feature helps to overcome this behavior and reduces the number of Type 1(router) and Type 2(network) LSAs advertised.

This feature can be enabled globally on a router or on per interfaces basis.

OSPF prefix-suppression helps in faster Shortest Path First (SPF) calculation due to less number of prefixes in the database (DB). OSPF Type 3, Type 4, Type 5, or Type 7 LSAs are not suppressed.
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/213404-open-shortest-path-first-prefix-suppress.html
upvoted 2 times

HungarianDish 8 months, 1 week ago

Selected Answer: C

I would say C, but on the correct interface. R2 gig0/1.
https://community.cisco.com/t5/networking-knowledge-base/ospf-prefix-suppression/ta-p/3293724
upvoted 3 times

HungarianDish 8 months, 1 week ago

I think that none of the listed answers are correct. I would apply it on R2 gig0/1 (facing R4). NOT on R2 gig0/0.

There is a point-to-point link btw R2-R4. It means that no LSA type 2 is generated! Prefix-supression reduces type1 and type 3 on point-to-point, and it is recommended to apply also on point-to-point.

upvoted 2 times

jackr76 8 months, 1 week ago

Selected Answer: C

See snarkymark

upvoted 1 times

Symirnian 8 months, 2 weeks ago

R1 is seen as the DR for OSPF. So prefix suppress command in DR is useful for all broadcasts in the area? If I am wrong please correct.

upvoted 1 times

bendarkel 9 months, 1 week ago

In the case of routers R1, R2, R3, it should be configured on each OSPF interface attached to that Ethernet segment. Simply put, you cannot just configure OSPF prefix-suppression on one side.

upvoted 2 times

Jeff555566 9 months, 1 week ago

It looks like prefix suppression needs to be put on all of the routers, not just one of them.

upvoted 2 times

Question #678 *Topic 1*

An engineer is connected to a Cisco router through a Telnet session. Which command must be issued to view the logging messages from the current session as soon as they are generated by the router?

A. logging host

B. terminal monitor

C. service timestamps log uptime

D. logging buffer

Correct Answer: *B*

Community vote distribution

B (100%)

Cooldude89 9 months, 2 weeks ago

Selected Answer: B

Good Old Term mon

upvoted 2 times

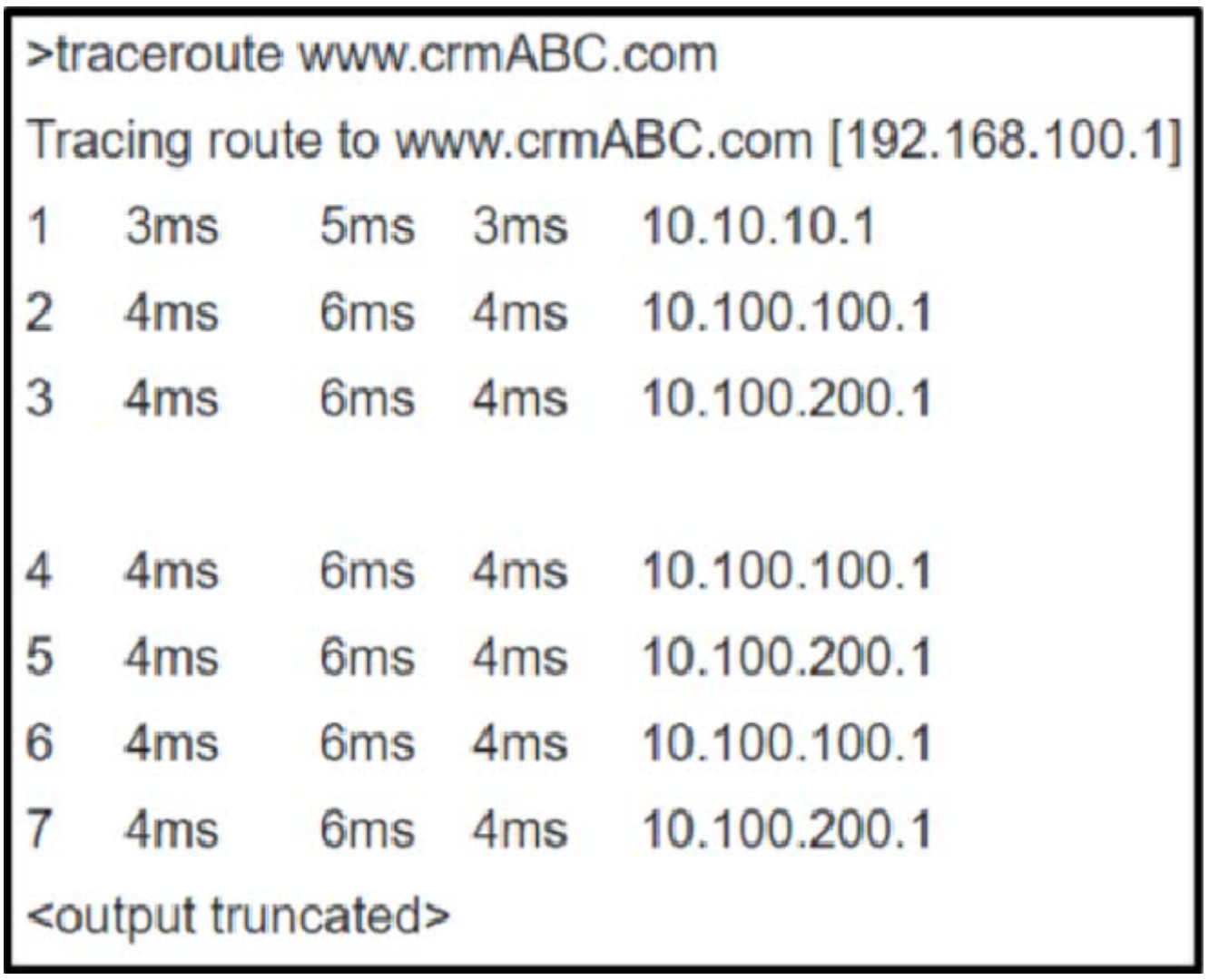
snarkymark 9 months, 2 weeks ago

Selected Answer: B

correct.

upvoted 1 times

Refer to the exhibit.



Users cannot reach the web server at 192.168.100.1. What is the root cause for the failure?

A. The server is attempting to load balance between links 10.100.100.1 and 10.100.200.1.

B. There is a loop in the path to the server.

C. The gateway cannot translate the server domain name.

D. The server is out of service.

Correct Answer: *B*

Community vote distribution

B (100%)

Ira 3 months, 3 weeks ago

Given answer is 100% correct

upvoted 1 times

bendarkel 9 months, 1 week ago

Selected Answer: B

There's a loop between 10.100.100.1 and 10.100.200.1

upvoted 3 times

snarkymark 9 months, 2 weeks ago

Selected Answer: B

https://superuser.com/questions/204709/what-does-this-tracert-output-mean-hovering-between-two-ip-addresses

upvoted 3 times

Question #680 *Topic 1*

What is one method for achieving REST API security?

A. using a combination of XML encryption and XML signatures

B. using HTTPS and TLS encryption

C. using a MDS hash to verify the integrity

D. using built-in protocols known as Web Services Security

Correct Answer: *B*

Community vote distribution

B (100%)

snarkymark 9 months, 2 weeks ago

Selected Answer: B

https://stackoverflow.blog/2021/10/06/best-practices-for-authentication-and-authorization-for-rest-apis/

upvoted 1 times

Question #681 *Topic 1*

What is a benefit of using segmentation with TrustSec?

A. Integrity checks prevent data from being modified in transit.

B. Packets sent between endpoints on a LAN are encrypted using symmetric key cryptography.

C. Security group tags enable network segmentation.

D. Firewall rules are streamlined by using business-level profiles.

Correct Answer: *D*

Community vote distribution

D (89%) 11%

Symirnian Highly Voted 9 months ago

There are 2 correct answers I think C and D.
Security Group Tagging transforms segmentation by simplifying administration:
• Security group tags allow organizations to segment their networks without having to redesign to accommodate more VLANs and subnets.
• Firewall rules are dramatically streamlined by using an intuitive business-level profile method.
upvoted 5 times

djedeen Most Recent 4 days, 23 hours ago

Selected Answer: D

D: benefit, as C is more about how it works.
upvoted 1 times

aglalp 1 month, 2 weeks ago

Answer: C

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec_pci_validation.pdf
upvoted 1 times

Calica 2 months, 3 weeks ago

Answer: C TrustSec, which stands for Trustworthy Security, is a Cisco technology that helps organizations implement network segmentation and access control policies. One of the benefits of using TrustSec is that it relies on security group tags (SGTs) to enable network segmentation. SGTs are used to classify and label network traffic based on various attributes, such as user identity, device type, or location. These labels are then used to enforce access control policies and segment the network, ensuring that only authorized users and devices can access specific resources or segments of the network. This helps improve network security and reduce the risk of unauthorized access or lateral movement by attackers.
upvoted 1 times

Ray_Dell 3 months, 2 weeks ago

Key word is "benefit". Answer D
upvoted 1 times

ihateciscoreally 3 months, 2 weeks ago

Segmentation is other words is boundary for clients' traffic (where clients' traffic can go and where can't go). Answer C is correct, but D is more correct (more details). Thus, correct answer is D.
upvoted 1 times

[Removed] 4 months, 3 weeks ago

Selected Answer: D

I've changed my mind, I think D is the best answer
upvoted 1 times

[Removed] 5 months ago

Selected Answer: C

choice between C & D
upvoted 1 times

DavideDL 8 months, 2 weeks ago

Selected Answer: D

It's a difficult choice between C & D , in my opnion D is more focus on the "benefit" than C
upvoted 3 times

x3rox 9 months, 1 week ago

Selected Answer: D

D -
* Firewall rules are dramatically streamlined by using an intuitive business-level profile method

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec_pci_validation.pdf
upvoted 2 times

Alondrix 1 month, 2 weeks ago

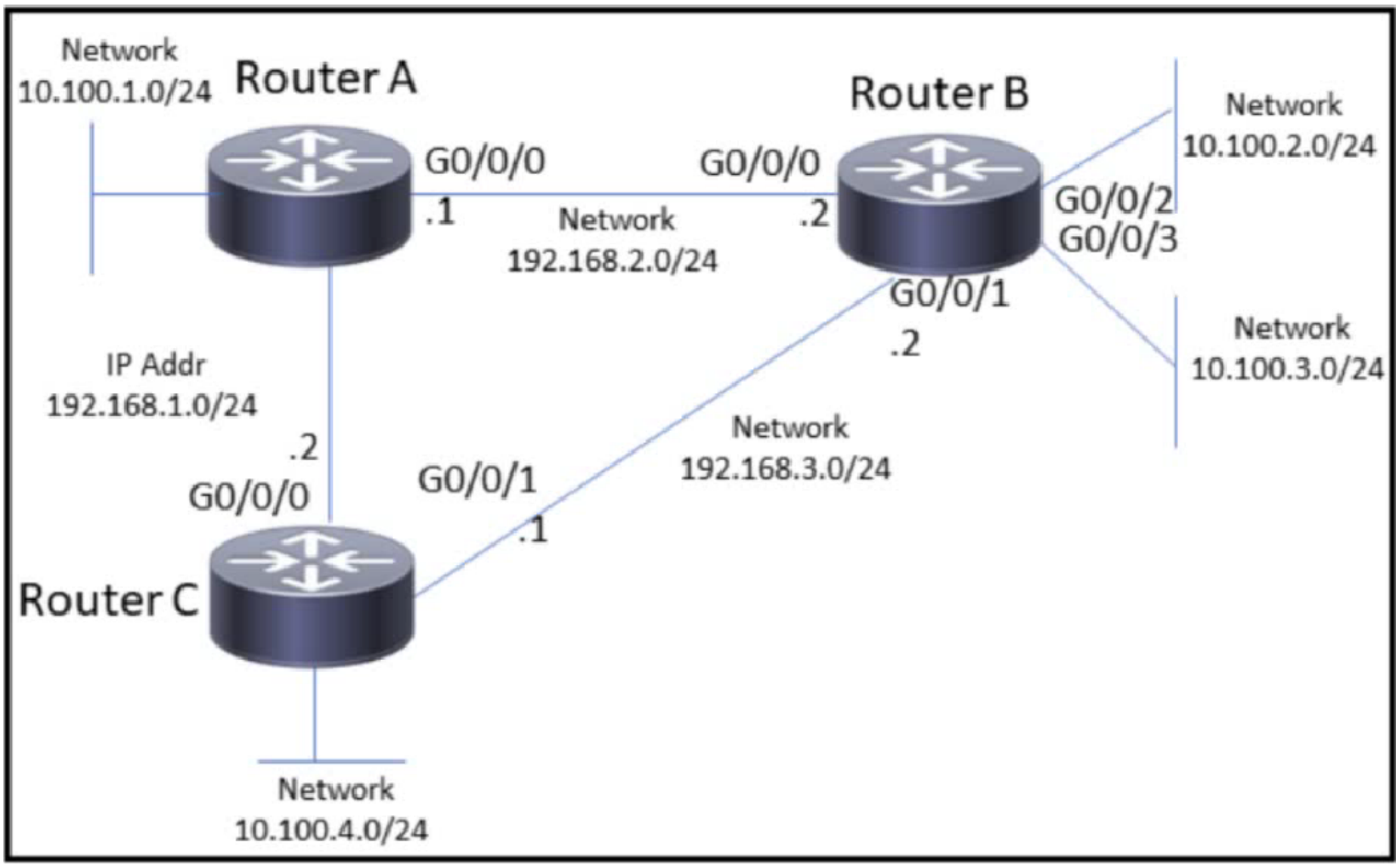
Good reference, but it shows:
Security group tags allow organizations to segment their networks without having to redesign to accommodate more VLANs and subnets.
• Firewall rules are dramatically streamlined by using an intuitive business-level profile method.
Seems both C and D are correct.
upvoted 1 times

snarkymark 9 months, 2 weeks ago

Selected Answer: D

https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-726831.pdf
upvoted 1 times

Refer to the exhibit.



A network administrator must configure router B to allow traffic only from network 10.100.2.0 to networks outside of router B. Which configuration must be applied?

A. RouterB(config)# access-list 101 permit ip 10.100.2.0 0.0.0.255 any
RouterB(config)# access-list 101 deny any

RouterB(config)# int g0/0/0 -
RouterB(config-if)# ip access-group 101 out

B. RouterB(config)# access-list 101 permit ip 10.100.3.0 0.0.0.255 any
RouterB(config)# access-list 101 deny any

RouterB(config)# int g0/0/0 -
RouterB(config-if)# ip access-group 101 out

RouterB(config)# int g0/0/1 -
RouterB(config-if)# ip access-group 101 out

C. RouterB(config)# access-list 101 permit ip 10.100.2.0 0.0.0.255 any
RouterB(config)# access-list 101 deny any

RouterB(config)# int g0/0/2 -
RouterB(config-if)# ip access-group 101 in

D. RouterB(config)# access-list 101 permit ip 10.100.2.0 0.0.0.255 any

RouterB(config)# int g0/0/0 -
RouterB(config-if)# ip access-group 101 out

RouterB(config)# int g0/0/1 -
RouterB(config-if)# ip access-group 101 out

Correct Answer: *D*

Community vote distribution

D (86%) 14%

well123 Highly Voted 9 months, 2 weeks ago

Selected Answer: D

A: Not ok, missing to apply ACL on int g0/0/1
B: Not ok, permits 10.100.3.0 (wrong)
C: not ok, applied ACL on wrong interface
D: OK, correct answer

upvoted 9 times

Colmenarez Most Recent 3 months, 4 weeks ago

Selected Answer: C

hmmm what about interface gi 0/0/3?

upvoted 2 times

teikitiz 4 months, 2 weeks ago

Selected Answer: D

C looked ok, but the ACL's deny component should be "deny ip any any". D's ACL carries the explicit deny, so it's correct

upvoted 3 times

x3rox 9 months, 1 week ago

A - WRONG. destination is missing an 'any' and it only affect traffic to 1 external network.
B - WRONG. wrong network souce and missing 'any' and only affect traffic to 1 external network.
C - WRONG. Select the best interface for this scenario, however, it's missing an 'any'; it it only had this missing any, would've been the best choice.
D - Correct. Correct network sources, implicit deny takes care of the rest. Interfaces are ok in the out direction.

upvoted 4 times

Question #683 *Topic 1*

How is traffic classified when using Cisco TrustSec technology?

A. with the IP address

B. with the VLAN

C. with the security group tag

D. with the MAC address

Correct Answer: *C*

Community vote distribution

C (100%)

CCNPWILL 1 month, 3 weeks ago

Selected Answer: C

C is correct. no brainer.

upvoted 1 times

well123 9 months, 2 weeks ago

Selected Answer: C

correct answer is C

upvoted 2 times

snarkymark 9 months, 2 weeks ago

https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-726831.pdf

upvoted 1 times

DRAG DROP
-

Drag and drop the code snippets from the bottom onto the blanks in the code to construct a request that configures a deny rule on an access list.

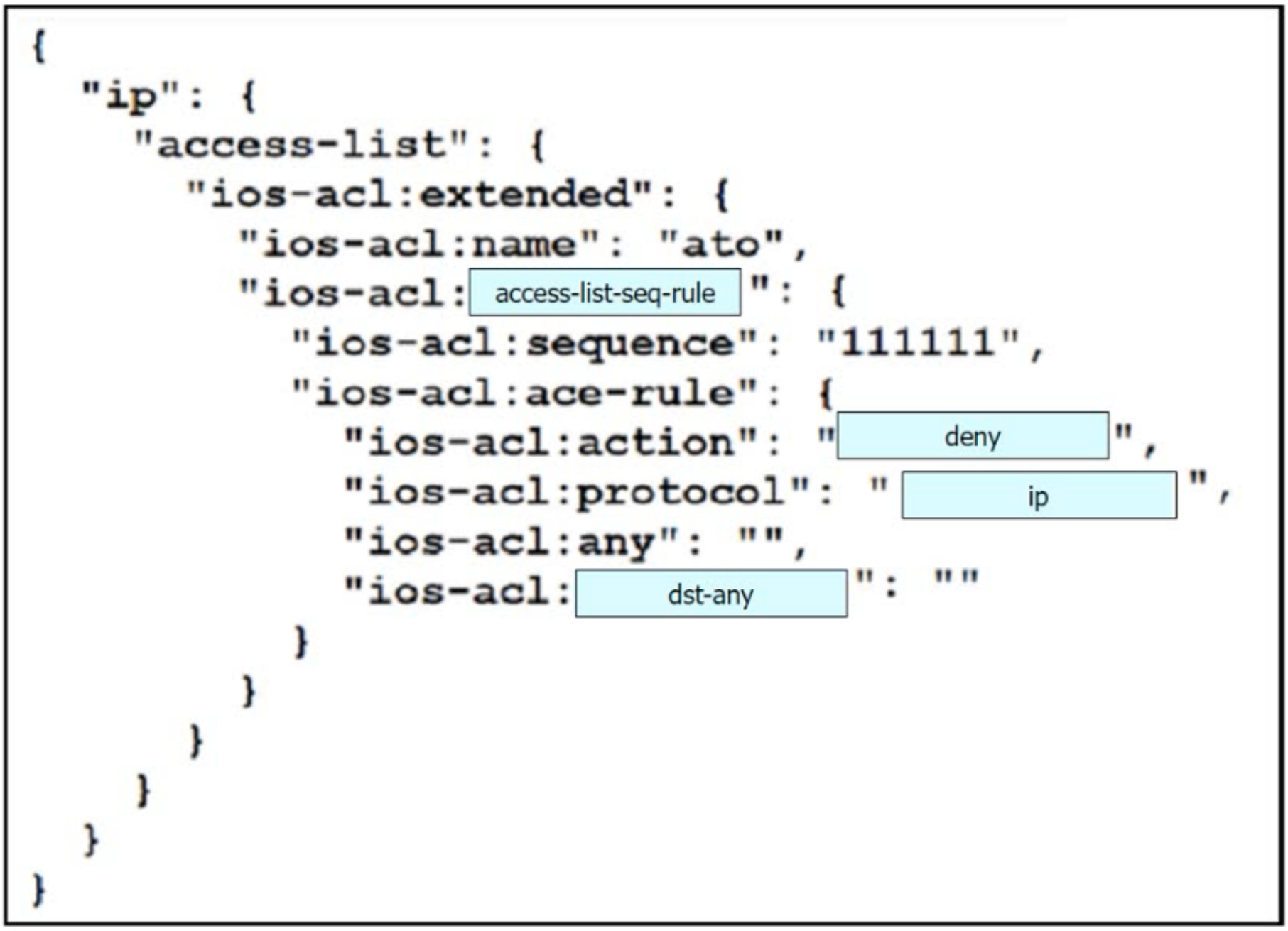
Answer Area

```
{
  "ip": {
    "access-list": {
      "ios-acl:extended": {
        "ios-acl:name": "ato",
        "ios-acl:[                ]": {
          "ios-acl:sequence": "111111",
          "ios-acl:ace-rule": {
            "ios-acl:action": "[                ]",
            "ios-acl:protocol": "[                ]",
            "ios-acl:any": "",
            "ios-acl:[                ]": ""
          }
        }
      }
    }
  }
}
```

deny | access-list-seq-rule | dst-any | ip

Correct Answer:

Answer Area



jackr76 Highly Voted 8 months, 1 week ago

Of all of these type of questions the most easy one

upvoted 6 times

tempaccount00001 4 months, 3 weeks ago

maybe for you, these are particularly hard for me, but others are super easy which people are arguing over.

upvoted 1 times

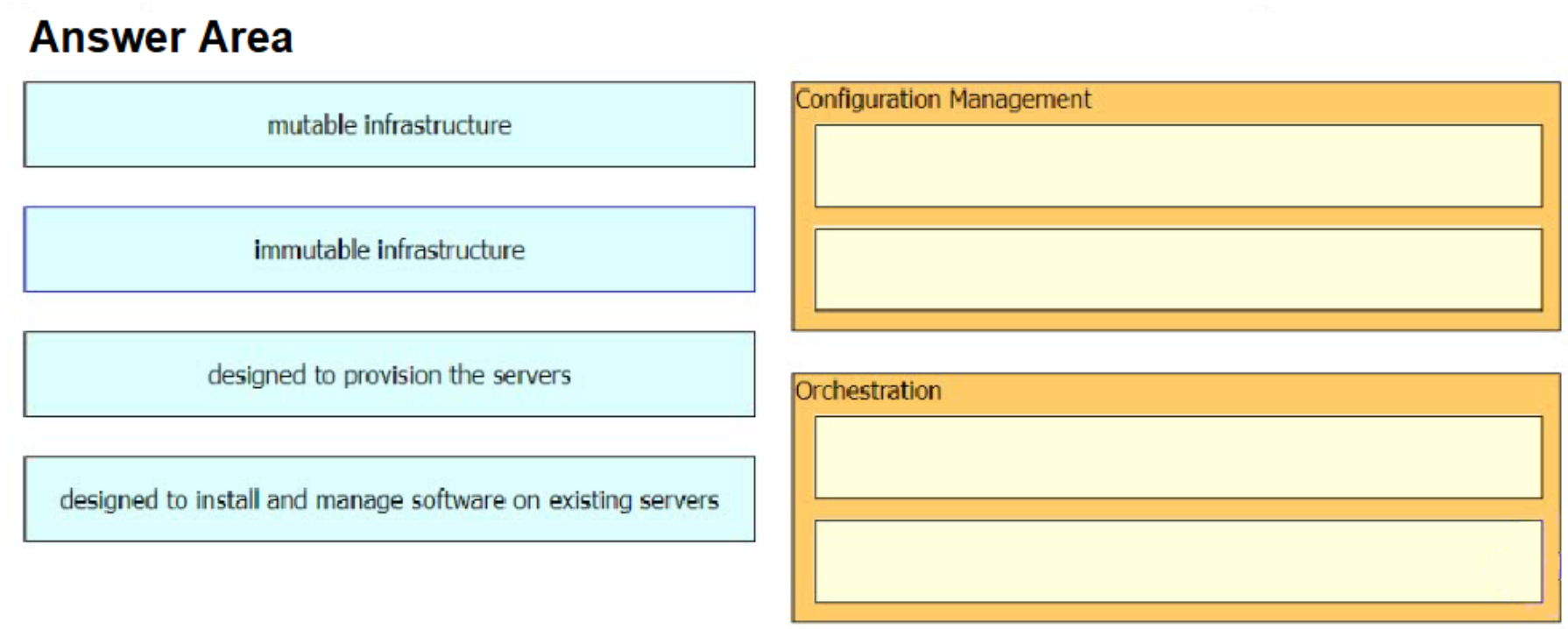
well123 Highly Voted 9 months, 2 weeks ago

correct answer

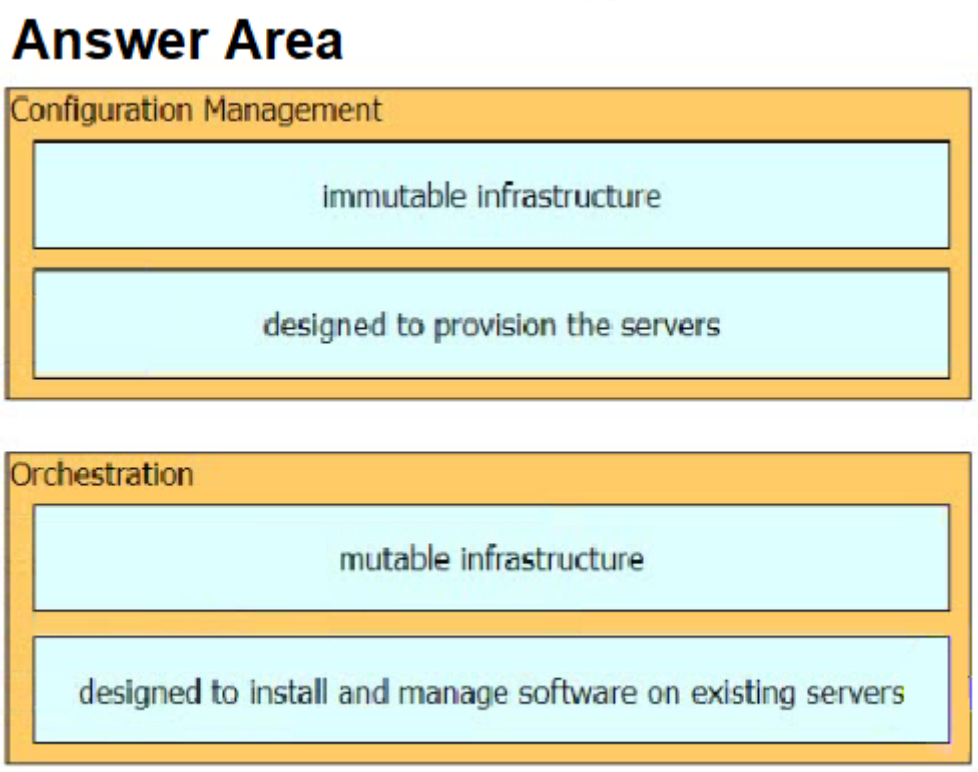
upvoted 5 times

DRAG DROP
-

Drag and drop the characteristics from the left onto the orchestration tool classifications on the right.



Correct Answer:



DavideDL Highly Voted 8 months, 2 weeks ago

According to:
https://www.ibm.com/cloud/blog/chef-ansible-puppet-terraform
and
https://blog.gruntwork.io/why-we-use-terraform-and-not-chef-puppet-ansible-saltstack-or-cloudformation-7989dad2865c#b264

They write about:
Configuration management tools such as Chef, Puppet, and Ansible typically default to a mutable infrastructure paradigm.

and

Generally, Ansible, Puppet, SaltStack, and Chef are considered to be configuration management (CM) tools and were created to install and manage software on existing server instances

So I would say:

Configuration Management Tool
- mutable infrastructure
- design to install and manage softwareon existing servers

My 0,02 cents

upvoted 14 times

JackDRipper Highly Voted 7 months, 3 weeks ago

My vote. I don't have a link to prove it, but it does make a lot of sense.

Configuration Management:
- Mutable
- Designed to install and manage software on existing servers

Orchestration:
- Immutable
- Designed to provision the servers

upvoted 7 times

Hosein Most Recent 5 months, 1 week ago

Mutable infrastructure refers to infrastructure that can be modified or changed after it is provisioned. In mutable infrastructure, configuration management tools are commonly employed to automate and manage the configuration, deployment, and maintenance of the infrastructure components. These tools help ensure consistency, enforce desired configurations, and facilitate updates or changes to the infrastructure over time.

For immutable infrastructure, while the focus is on building and deploying new instances rather than modifying existing ones, orchestration tools can still play a role. In this context, orchestration tools are often used to automate the creation, deployment, and scaling of immutable infrastructure instances. These tools enable the streamlined provisioning of pre-configured and consistent instances, ensuring the rapid deployment of identical infrastructure components.
So,
Configuration Management:
- Mutable
- Designed to install and manage software on existing servers

Orchestration:
- Immutable
- Designed to provision the servers

upvoted 4 times

Dv123456 4 months, 3 weeks ago

In the end i don't know why configuration management should be linked to immutable infrastructure

upvoted 1 times

Leoveil 9 months, 1 week ago

should be other way round

upvoted 3 times

x3rox 9 months, 1 week ago

Incorrect:
Orchestration
....In this blog we'll discuss Terraform's paradigm of immutable deployment

Configuration Management
.....We will also demonstrate how Ansible – with its mutable approach to managing infrastructure and applications – masterfully manages configuration management and application software provisioning for initial and ongoing deployments.
....*Configuration management tools such as Chef, Puppet, and Ansible typically default to a mutable infrastructure paradigm.

https://blogs.cisco.com/developer/choosingtools01

upvoted 1 times

snarkymark 9 months, 2 weeks ago

Correct

upvoted 1 times

snarkymark 9 months ago

thx for the correction

upvoted 1 times

Refer to the exhibit.

```
import requests

### The authentication part is omitted for brevity purposes

URL = "https://dnac/dna/intent/api/v1/topology/vlan/vlan-names"
VlanNames = requests.get(URL, headers=Header).json()
print(VlanNames)
```

```
{'response': ['Vlan1', 'Vlan3002', 'Vlan3003', 'Vlan1023', 'Vlan2046', 'Vlan3009', 'Vlan3999'], 'version': '1.0'}
```

How should the programmer access the list of VLANs that were received via the API call?

A. VlanNames[‘response’]

B. VlanNames[0]

C. VlanNames[‘Vlan1’]

D. list(VlanNames)

Correct Answer: *D*

Community vote distribution

A (100%)

Vlad_Is_Love_ua Highly Voted 9 months ago

Selected Answer: A

```
>>> VlanNames = {'response':['vlan1','vlan2','vlan3'],'version':'1.0'}
>>> VlanNames['response']
['vlan1', 'vlan2', 'vlan3']
```

upvoted 9 times

msstanick Most Recent 5 months, 1 week ago

Selected Answer: A

As stated by Vlad already it is A. I got it labbed with Cisco's sandbox.

```
url1 = "https://sandboxdnac.cisco.com/dna/intent/api/v1/topology/vlan/vlan-names"
VlanNames = requests.get(url=url1, headers=headers, verify=False).json()
print("\n\n",VlanNames['response'])

['Vlan1', 'Vlan101']
Process finished with exit code 0
```

upvoted 1 times

Question #687 *Topic 1*

An EEM applet contains this command:
event snmp oid 1.3.6.1.4.3.8.0.5.8.7.1.3 get-type next entry-op gt entry-val 80 poll-interval 8

What is the result of the command?

A. An SNMP event is generated when the value equals 80% for eight polling cycles.

B. An SNMP event is generated when the value is greater than 80% for eight polling cycles.

C. An SNMP event is generated when the value reaches 80%.

D. An SNMP variable is monitored and an action is triggered when the value exceeds 80%.

Correct Answer: *D*

Community vote distribution

D (100%)

NewLife77 3 months ago

I think the correct answer is B.

upvoted 3 times

snarkymark 9 months, 2 weeks ago

Selected Answer: D

Similar command for cpu utilization.

upvoted 1 times

Question #688 *Topic 1*

Refer to the exhibit.

```
import sqlite3
a= sqlite3.connect('/home/sdwan-lab/user.sqlite3')
b= a.cursor()
c= "select user from monitor_branch where loopbackip='" + str(ip[i]) + "'"
d= b.execute(c)
e= b.fetchall()
usr= str(e[0])
usr= usr.replace("('","")
usr= usr.replace("',)","")
```

What does this Python script do?

A. enters the TACACS+ username for a specific IP address

B. reads the username for a specific IP address from a light database

C. writes the username for a specific IP address into a light database

D. enters the RADIUS username for a specific IP address

Correct Answer: *B*

Community vote distribution

B (100%)

jackr76 Highly Voted 8 months, 1 week ago

WTF is this a Cisco or SQL exam

upvoted 12 times

Dre876 2 months, 3 weeks ago

tell me about it!

upvoted 1 times

ando2023 5 months, 2 weeks ago

I've recertified my ccnp since 2013 a few times, but now Cisco all of a sudden is going off in such a different direction. Switching and routing is now such a small part of the overall requirements.

upvoted 6 times

dragonwise 7 months, 3 weeks ago

They think we're not worthy of the certificate if we do answer this question

upvoted 2 times

mgiuseppe86 2 months, 2 weeks ago

Thats my biggest gripe with the new CCNP. It's all BS Cloud/WiFi/Automation.

WHAT HAPPENED TO REAL LAYER 1 2 3 NETWORKING

upvoted 2 times

Badger_27 Highly Voted 8 months, 3 weeks ago

WTF are they serious?

upvoted 6 times

zogerixty 8 months, 2 weeks ago

Can't understand?

upvoted 1 times

Badger_27 8 months, 2 weeks ago

No- how are you supposed to if you don't regularly use Python and the SQLite module?

upvoted 2 times

mgiuseppe86 Most Recent 2 months, 2 weeks ago

doesn the usr.replace string write the username back to the DB once it selects it from the table monitor_Branch?

upvoted 1 times

djedeen 3 months, 1 week ago

Selected Answer: B

B: good link here for similar queries from sqlite3 DB.
https://pyneng.readthedocs.io/en/latest/book/25_db/sqlite3_fetch.html

upvoted 1 times

HungarianDish 8 months, 1 week ago

Selected Answer: B

B seems to be correct, because data only needs to be read from the DB, and not altered.

https://www.google.com/amp/s/www.geeksforgeeks.org/how-to-list-tables-using-sqlite3-in-python/amp/

upvoted 1 times

Cooldude89 9 months, 1 week ago

no clue ...
didn't see this coming , not in OCG

upvoted 3 times

Question #689 *Topic 1*

Refer to the exhibit.

```
for x in range(6):
   print(x)
```

What is output by this code?

A. 0 5

B. 0 1 2 3 4 5

C. 0 1 2 3 4

D. (0,5)

Correct Answer: *B*

Community vote distribution

B (100%)

adamzet33 2 weeks, 5 days ago

Selected Answer: B

I knew answer to this, i am a programmer now.

upvoted 2 times

snarkymark 9 months, 2 weeks ago

Selected Answer: B

https://www.learnpython.org/en/Loops

upvoted 3 times

Question #690 *Topic 1*

Which statement describes the Cisco SD-Access plane functionality for fabric-enabled wireless?

A. The control plane traffic is sent to the WLC through VXLAN, and the data plane traffic is sent to the WLC through CAPWAP tunnels.

B. Control plane traffic and data plane traffic are sent to the WLC through CAPWAP tunnels.

C. The control plane traffic is sent to the WLC through CAPWAP tunnels, and the data plane traffic is sent from the AP to the fabric edge switch through VXLAN.

D. Control plane traffic and data plane traffic are sent to the WLC through VXLAN.

Correct Answer: *C*

Community vote distribution

C (100%)

RocketS17 Highly Voted 8 months, 4 weeks ago

Selected Answer: C

"In SD-Access Wireless, the control plane is centralized. This means that, as with Cisco Unified Wireless Network, a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel is maintained between APs and WLC. The main difference is that in SDAccess Wireless, the data plane is distributed using a Virtual Extensible LAN (VXLAN) directly from the fabric-enabled APs."
https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf

upvoted 7 times

Question #691 *Topic 1*

A company hires a network architect to design a new OTT wireless solution within a Cisco SD-Access Fabric wired network. The architect wants to register access points to the WLC to centrally switch the traffic. Which AP mode must the design include?

A. local

B. bridge

C. FlexConnect

D. fabric

Correct Answer: *A*

Community vote distribution

A (100%)

HarwinderSekhon 5 months, 2 weeks ago

Selected Answer: A

OOT- Wireless is Not part of Fabiric and runs overlay.
Flexconnect - Local swithcing (Question focous on central switching)
So only A is left

upvoted 1 times

byallmeans 6 months, 4 weeks ago

Why A? Centrally means Flexconnect, not local right?

upvoted 2 times

bk989 6 months, 2 weeks ago

local is the default, FlexConnect is option to locally switch on the AP itself, notably used at branch locations where there still should be a connection to WLC at data center/core

upvoted 1 times

snarkymark 8 months, 4 weeks ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html

upvoted 2 times

Question #692 *Topic 1*

Which two methods are used to interconnect two Cisco SD-Access Fabric sites? (Choose two.)

A. SD-Access transit

B. fabric interconnect

C. wireless transit

D. IP-based transit

E. SAN transit

Correct Answer: *AD*

Community vote distribution

AD (100%)

Opreis 8 months, 3 weeks ago

Selected Answer: AD

IP transit: Uses a regular IP network to connect to an external network or to connect two or more fabric sites. It leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites.

SD-Access transit: Uses LISP/VxLAN encapsulation to connect two fabric sites. The SD-Access transit area may be defined as a portion of the fabric that has its own control plane nodes, but does not have edge or border nodes. However, it can work with a fabric that has an external border. With an SD-Access transit, an end-to-end policy plane is maintained using SGT group tags.

upvoted 3 times

Brian9296 9 months ago

Selected Answer: AD

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2815.pdf

upvoted 2 times

Question #693 *Topic 1*

What is a characteristic of Cisco SD-WAN?

A. uses unique per-device feature templates

B. requires manual secure tunnel configuration

C. uses control plane connections between routers

D. operates over DTLS/TLS authenticated and secured tunnels

Correct Answer: *D*

Community vote distribution

D (100%)

CCNPWILL 2 months ago

D is correct. Do not let A confuse you. You can recycle the same device template so it doesnt have to be unique per say.

upvoted 1 times

felix_simon 4 months, 4 weeks ago

D

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-sol-overview-cte-en.html

Cisco Catalyst SD-WAN offers integrated security, including full-stack multilayer security capabilities on the premises and in the cloud.

upvoted 1 times

snarkymark 8 months, 4 weeks ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book.pdf

upvoted 1 times

Question #694 *Topic 1*

What is the centralized control policy in a Cisco SD-WAN deployment?

A. set of statements that defines how routing is performed

B. set of rules that governs nodes authentication within the cloud

C. list of ordered statements that define user access policies

D. list of enabled services for all nodes within the cloud

Correct Answer: *A*

Community vote distribution

A (100%)

CCNPWILL 2 months ago

Selected Answer: A

A is correct. Dont get confused with data policy, C.

Answer is A.

upvoted 1 times

snarkymark 8 months, 4 weeks ago

Selected Answer: A

https://www.networkacademy.io/ccie-enterprise/sdwan/what-is-a-centralized-control-policy

upvoted 2 times

Question #695 *Topic 1*

Which function is performed by vSmart in the Cisco SD-WAN architecture?

A. aggregation and distribution of VPN routing information

B. execution of localized policies

C. facilitation of NAT detection and traversal

D. redistribution between OMP and other routing protocols

Correct Answer: *B*

Community vote distribution

A (60%) D (25%) B (15%)

Asombrosso 3 months ago

Selected Answer: A

A. vSmart
B. vManage
C. vBond
D. vEdge

upvoted 2 times

WereAllinThisTogether 4 months, 2 weeks ago

In the Cisco SD-WAN architecture, the vSmart controller acts as the centralized brain of the network. It is responsible for aggregating and distributing VPN (Virtual Private Network) routing information across the SD-WAN fabric. The vSmart controller uses the Overlay Management Protocol (OMP) to exchange routing information with the edge routers (vEdge routers) in the SD-WAN network. It collects information about network reachability, network policies, and security requirements from the vEdge routers and distributes this information to ensure efficient and optimized routing throughout the network.

upvoted 4 times

sam6996 4 months, 2 weeks ago

Selected Answer: A

I think the vEdges are the ones that redistribute the routes into OMP, the vSmart just learns the routes and advertises it to other vEdges, so I would go with A, I could be wrong. But Iim using this as a reference and if you ctrl f redistribute you can see its configured on the vEdges section, https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html

upvoted 1 times

Dv123456 4 months, 3 weeks ago

Selected Answer: D

The answer is D here is an explicative source
https://www.thenetworkdna.com/2021/02/cisco-viptela-sd-wan-vsmart-as-control.html#:~:text=OMP%2D%20Overlay%20Management,using%20OMP%20updates.

upvoted 1 times

felix_simon 4 months, 4 weeks ago

D
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html
The major components of the Cisco vSmart Controller are:
Control plane connections; OMP (Overlay Management Protocol); Authentication; Key reflection and rekeying; Policy engine; Netconf and CLI

upvoted 1 times

Mani9Don 5 months, 4 weeks ago

Selected Answer: D

I still go with D

upvoted 1 times

pmmg 7 months, 4 weeks ago

Selected Answer: A

Seems like A to me.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html

Each Cisco vSmart Controller establishes and maintains a control plane connection with each edge router in the overlay network. Each connection, which runs as a DTLS tunnel, is established after device authentication succeeds, and it carries the encrypted payload between the Cisco vSmart Controller and the edge router. This payload consists of route information necessary for the Cisco vSmart Controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the Edge routers.

upvoted 2 times

pmmg 7 months, 4 weeks ago

Sorry, looking at the wrong question. I think this one is D

OMP (Overlay Management Protocol): The OMP protocol is a routing protocol similar to BGP that manages the Cisco SD-WAN overlay network. OMP runs inside DTLS control plane connections and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the Cisco vSmart Controller and the edge routers and carries only control plane information. The Cisco vSmart Controller processes the routes and advertises reachability information learned from these routes to other edge routers in the overlay network.

upvoted 1 times

HungarianDish 8 months, 1 week ago

Selected Answer: A

After some further reading, I need to vote for A, because D seems to belong to vEdges. Distribution of VPN routing information clearly is a function of the vSmart. (A)
However, OMP route redistribution (D) is done by vEdges:
"two WAN edge routers doing route redistribution between the Cisco Overlay Management Protocol (OMP) and any site-local routing protocol running on the service side"
"By default, the vEdges automatically redistribute the following route types that they learn from site-local peers into OMP: Connected, Static, OSPF/OSPFv3 intra-area, OSPF/OSPFv3 inter-area"
https://www.networkacademy.io/ccie-enterprise/sdwan/omp-redistribution-loop-prevention

upvoted 3 times

HungarianDish 8 months, 1 week ago

According to these documents, both A and D seem to be correct:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html
"All site-local routes are populated on the vEdge routers. Distributed these routes to the other vEdge routers this is done through the Cisco vSmart Controller, via OMP. If you are using BGP or if there are OSPF external LSAs, allow OMP to redistribute the BGP routes. Re-advertise OMP routes into BGP or OSPF."

https://www.networkacademy.io/ccie-enterprise/sdwan/what-is-a-centralized-control-policy
"VPN Membership policies are used to control the distribution of routing information for specific VPNs to a list of sites."
Based on the diagram, vSmart is responsible for managing OMP and VPN in the SD-WAN fabric.

upvoted 1 times

jackr76 8 months, 1 week ago

Selected Answer: B

As an optional step, you can create control and data plane policies on the Cisco vSmart Controller and push them to the vEdge routers.

Shouldn't this then be answer B?
A aggregation & distribution (in vSmart)
and not
B execution of localized policies (in vEdge)

upvoted 2 times

jackr76 8 months, 1 week ago

SORRY A (bad system no edit)

upvoted 1 times

Clauster 8 months, 1 week ago

Selected Answer: B

Guys be careful, question 440 and this one are exactly the same and on both questions it states the correct answer, this must be the answer, please find the information here:

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html#cisco-vsmart-controller

upvoted 1 times

Asombrosso 3 months ago

Localized policy refers to a policy that is provisioned locally through the CLI on devices, or through a Cisco SD-WAN Manager device template. vManage pushes the policy to all reachable Cisco SD-WAN Controllers in the network.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/localized-policy.html#Cisco_Concept.dita_d90ce142-5a9a-463c-acf3-a33dc486d53c.

So itsn't B!

upvoted 1 times

jackr76 8 months, 1 week ago

in your link:
As an optional step, you can create control and data plane policies on the Cisco vSmart Controller and push them to the vEdge routers.

Shouldn't this then be answer B?
A aggregation & distribution (in vSmart)
and not
B execution of localized policies (in vEdge)

upvoted 1 times

jackr76 8 months, 1 week ago

SORRY A (bad system no edit)

upvoted 1 times

Symirnian 8 months, 2 weeks ago

Selected Answer: D

I prefer D as I know vSmart is managing routing. OMP is the control protocol that is used to exchange routing, policy, and management information between the vSmart controllers and vEdge routers in the overlay network. It is enabled by default, so after you start up the vSmart controllers and vEdge routers, it is not necessary to explicitly configure or enable OMP.

upvoted 3 times

daezee 8 months, 4 weeks ago

Selected Answer: A

Think its A too

The Cisco SD-WAN policy design provides a clear separation between centralized and localized policy. In short, centralized policy is provisioned on the centralized Cisco vSmart Controllers in the overlay network, and the localized policy is provisioned on Cisco vEdge devices,

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2815.pdf

upvoted 2 times

snarkymark 8 months, 4 weeks ago

agree A.
https://www.networkacademy.io/ccie-enterprise/sdwan/what-is-a-centralized-control-policy

upvoted 1 times

snarkymark 8 months, 4 weeks ago

Sorry, I meant to say, I believe it is D
Each vEdge device sends all site-local prefixes, tlocs, and service routes toward the controller using all established DTLS control connections.
The vSmart controller accepts all incoming OMP routes (omp, tloc, or service) and stores them in the respective route tables per VPN.
The vSmart then redistributes all learned routes to all WAN edge devices. This results in a full-mesh overlay fabric and full IP reachability between all nodes.
Each vEdge device continually sends route updates.
The vSmart updates its routing table based on each update and advertises any routing

upvoted 3 times

Brian9296 9 months ago

Selected Answer: A

Strongly think that answer is A

upvoted 2 times

mellohello 9 months ago

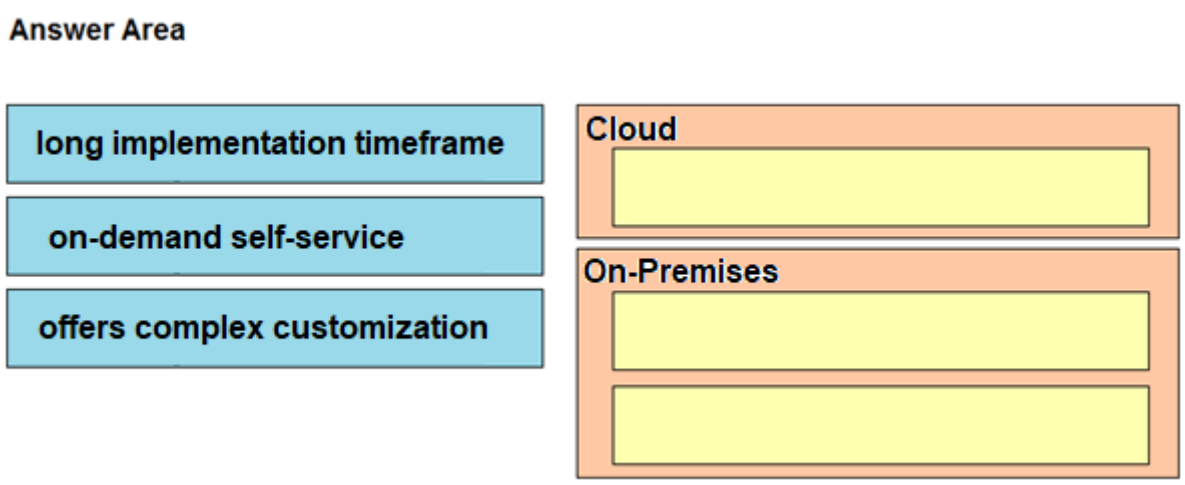
I think it is inncorrect. It should be A?

upvoted 1 times

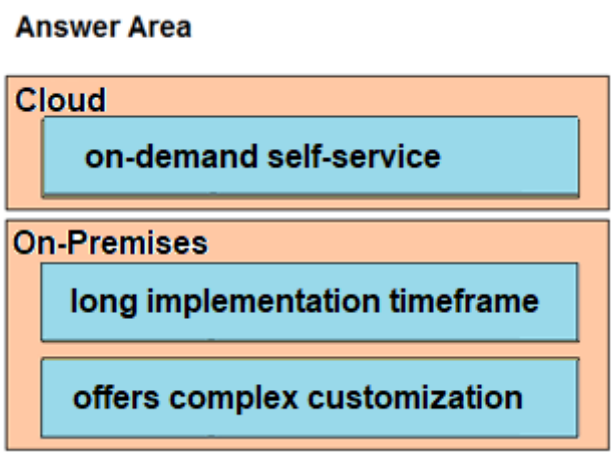
Question #696 *Topic 1*

DRAG DROP
-

Drag and drop the characteristics from the left onto the deployment models on the right.



Correct Answer:



CCNPWILL 2 months ago
CorrectomunDo
upvoted 1 times

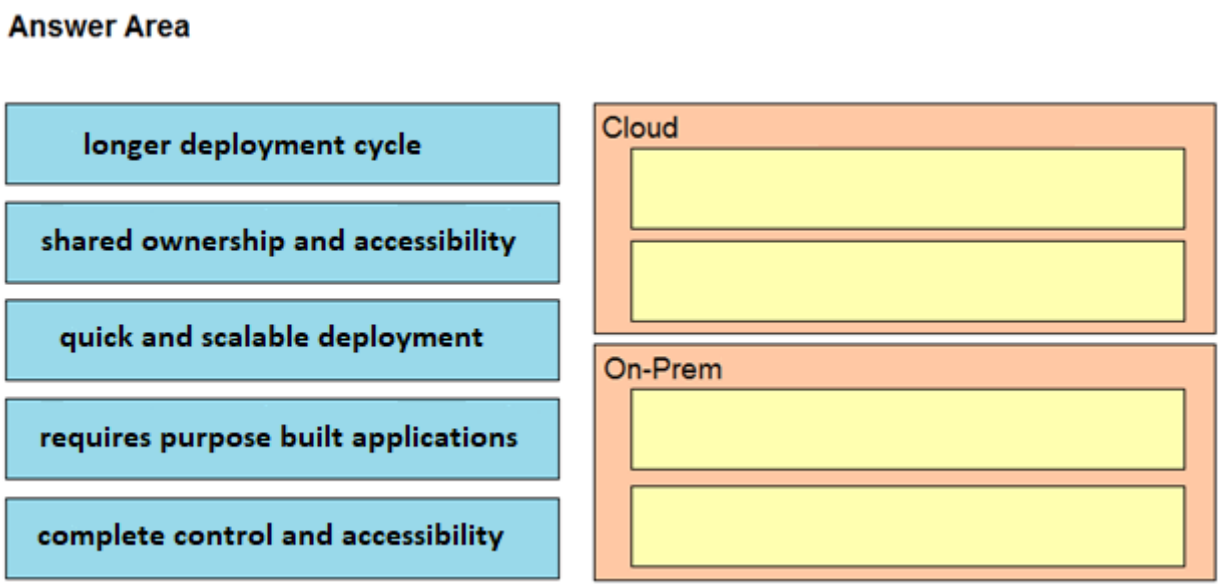
Ira 3 months, 3 weeks ago
answer is correct
upvoted 1 times

cuda74 8 months, 3 weeks ago
I think answer it's correct.
upvoted 3 times

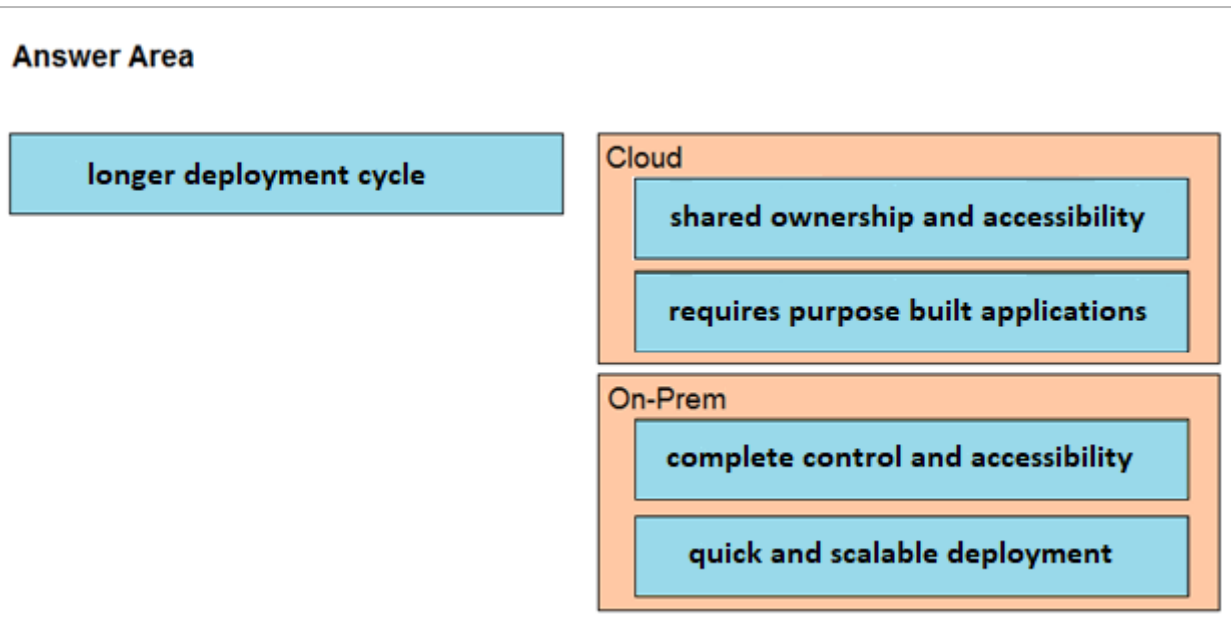
Question #697 *Topic 1*

DRAG DROP
-

Drag and drop the characteristics from the left onto the deployment models on the right. Not all options are used.



Correct Answer:



Nickplayany Highly Voted 8 months, 4 weeks ago

I think it should be

Cloud:
Shared ownership and accessibility
Quick and scalable deployment

On-Prem:

Longer depolyment cycle
Complete control and accessibility

upvoted 46 times

Symirnian Highly Voted 9 months ago

Requires purpose built applications should be out. It is necessary for both I think.

upvoted 8 times

Question #698 *Topic 1*

How do cloud deployments compare to on-premises deployments?

A. Cloud deployments provide a better user experience across world regions, whereas on-premises deployments depend upon region-specific conditions.

B. Cloud deployments mandate a secure architecture, whereas on-premises deployments are inherently unsecure.

C. Cloud deployments must include automation infrastructure, whereas on-premises deployments often lack the ability for automation.

D. Cloud deployments are inherently unsecure, whereas a secure architecture is mandatory for on-premises deployments.

Correct Answer: *C*

Community vote distribution

A (90%) 10%

djedeen 4 months ago

Selected Answer: A

A .....

upvoted 1 times

Dataset 8 months ago

Selected Answer: A

The answer is A
Regards

upvoted 2 times

jackr76 8 months, 1 week ago

Selected Answer: A

A for me

upvoted 2 times

Symirnian 8 months, 2 weeks ago

Selected Answer: A

A is clear and true for me

upvoted 2 times

DavideDL 8 months, 3 weeks ago

Selected Answer: A

I think A sounds bettter

Easily deploy your application in multiple regions around the world with just a few clicks. This means you can provide lower latency and a better experience for your customers at minimal cost.
https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html

upvoted 2 times

MJane 8 months, 3 weeks ago

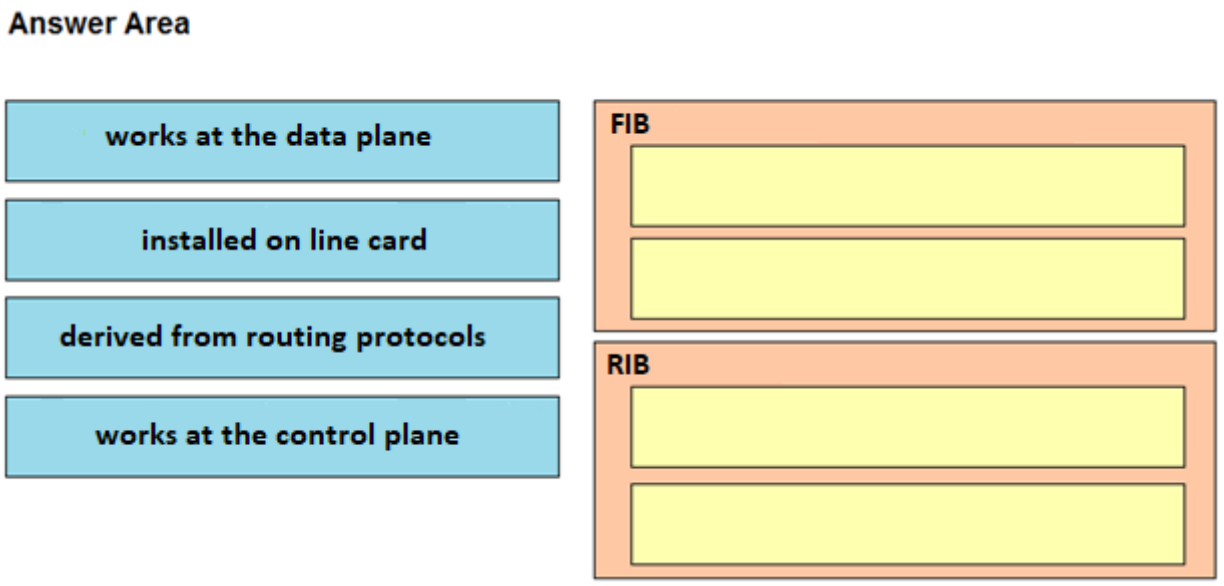
Selected Answer: D

i vote for D here. i find more on that subject when talking about the diff.

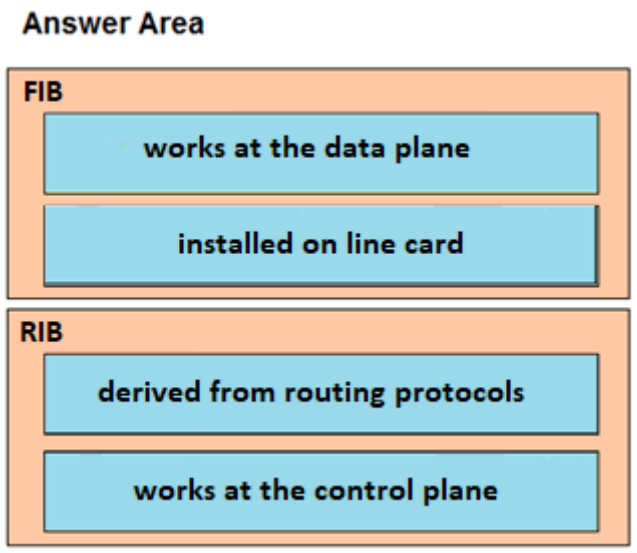
upvoted 1 times

DRAG DROP
-

Drag and drop the characteristics from the left onto the architectures on the right.



Correct Answer:



snarkymark Highly Voted 8 months, 4 weeks ago
Correct, https://networkdirection.net/articles/network-theory/controlanddataplane/
upvoted 5 times

tempaccount00001 Most Recent 4 months, 3 weeks ago
yup, correct
upvoted 2 times

Question #700 *Topic 1*

When voice services are deployed over a wireless environment, which service must be disabled to ensure the quality of calls?

A. priority queuing

B. dynamic transmit power control

C. aggressive load balancing

D. Fastlane

Correct Answer: *A*

Community vote distribution

C (100%)

Asombrosso 3 months ago

Selected Answer: C

deffinetly its C

upvoted 1 times

djedeen 4 months ago

Selected Answer: C

C per the links and text below

upvoted 1 times

WereAllinThisTogether 4 months, 2 weeks ago

C. Aggressive load balancing.

When deploying voice services over a wireless environment, it is important to ensure the quality of calls. Aggressive load balancing should be disabled to achieve this. Aggressive load balancing is a feature that dynamically moves clients between access points to balance the load and optimize network performance. However, in the context of voice services, it can cause disruptions and call quality issues.

upvoted 2 times

Clauster 8 months, 3 weeks ago

Selected Answer: C

Answer is C

Another wrong answer.

upvoted 3 times

snarkymark 8 months, 4 weeks ago

Selected Answer: C

http://what-when-how.com/deploying-and-troubleshooting-cisco-wireless-lan-controllers/configuration-cisco-wireless-lan-controllers/

upvoted 3 times

Nickplayany 8 months, 4 weeks ago

Selected Answer: C

C is the answer

upvoted 1 times

Brian9296 9 months ago

Selected Answer: C

The answer should be C

upvoted 1 times

mellohello 9 months ago

I think it should be C.

upvoted 1 times

DavideDL 9 months ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/advanced_wireless_tuning.html

You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

upvoted 4 times

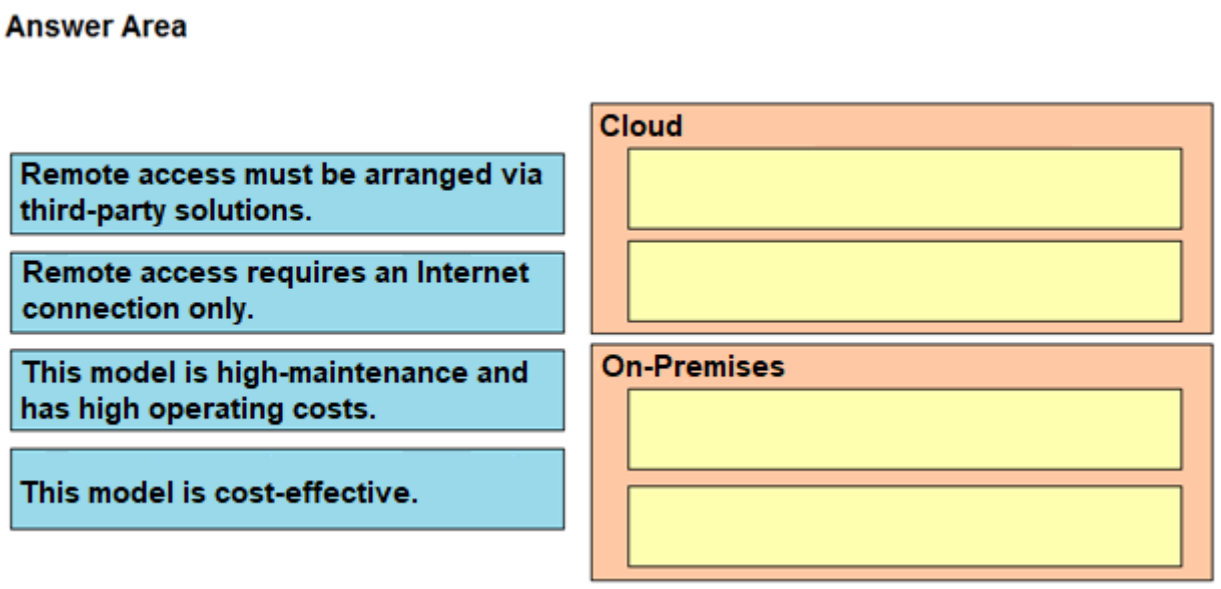
Custom View Settings

Question #701 *Topic 1*

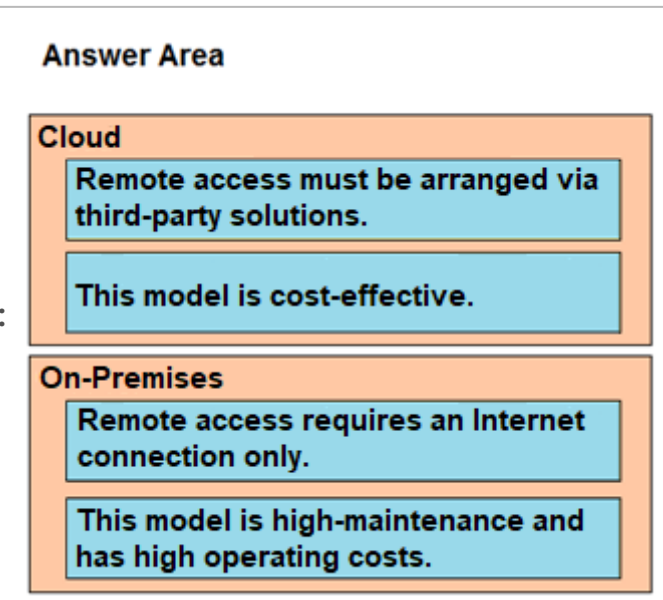
DRAG DROP

-

Drag and drop the characteristics from the left onto the deployment models on the right.



Correct Answer:



JackDRipper Highly Voted 9 months, 2 weeks ago

I believe the answer should be...

Cloud:
Remote access requires an internet connection only
This model is cost-effective

On-Prem:
Remote access must be arranged via third-party solutions
This model is high-maintenance and has high operating costs

upvoted 26 times

Brian9296 Highly Voted 10 months, 2 weeks ago

i think the answer is wrong, Cloud remote access only required an internet connection while on-prem remote access required 3rd party software

upvoted 18 times

mgiuseppe86 Most Recent 3 months, 4 weeks ago

I would argue Cloud is Cost Effective because of how much Amazon and Microsoft charge for cloud licensning.

However realistically, in this case you need to think outside the box.

For on Prem, you need to pay for the building itself, the infrastructure around housing a datacenter: cooling, power, electricians, plumbers, racks, cabling, network equipment, licenses, etc

so yes, cloud is "cost-effective" that it takes nothing but a credit card online to buy a service. but what they can charge you may have you rethinking going cloud at all.

upvoted 1 times

Dataset 4 months ago

Hi!
Admin , please fix the answers
CLOUD:
Remote access requires an internet connection only
This model is cost-effective

ON-PREMISES:
Remote access must be arranged via third-party solutions
This model is high-maintenance and has high operating costs

thanks!
Best regards

upvoted 1 times

Dv123456 5 months, 3 weeks ago

Probably for cisco is correct but it's undisputed that the on-prem deployment has higher capEx costs and cloud deployment has higher operational cost (az-900)

https://www.parallels.com/blogs/ras/cloud-vs-on-premises-costs/#:~:text=High%20operating%20costs

upvoted 1 times

Nickplayany 10 months, 1 week ago

I think is WRONG

Correct below:

Cloud:
Remote access must be arranged via third-party solutions
Remote access requires an Internet connection only

On-Premises:
This model is cost-effective
This model is high-maintenance and has high operating costs

upvoted 4 times

wyleebb 7 months, 3 weeks ago

How do you say cost effective and high maintenance on the same item?

upvoted 2 times

Symirnian 10 months, 1 week ago

Why many of the answers are wrong? We are paying for this :) I burned my brain.

upvoted 7 times

Asombrosso 4 months, 1 week ago

I'm curious who decides the correct answer? and how?

upvoted 1 times

Question #702 *Topic 1*

What is an OVF?

A. a package that is similar to an IMG and that contains an OVA file used to build a virtual machine

B. an alternative form of an ISO that is used to install the base operating system of a virtual machine

C. the third step in a P2V migration

D. a package of files that is used to describe a virtual machine or virtual appliance

Correct Answer: *A*

Community vote distribution

D (100%)

Clauster Highly Voted 10 months, 1 week ago

Why are all answers wrong on this exam ? At some point Moderator needs to start fixing it, i understand 1 out of 50 but i been finding tons of wrong answers.

upvoted 10 times

mgiuseppe86 3 months, 4 weeks ago

I feel the last 150 questions (650-800) have been phoned in. I think people start dropping off the deep end this deep into the dump

upvoted 2 times

ando2023 6 months, 3 weeks ago

I notice on the main 350-401 page there are a lot of comments saying to "Look at the comments". IE, dont trust the answer provided. I have noticed this too, nearly every second question is wrong and you have to go on what is most voted.

upvoted 4 times

jackr76 9 months, 3 weeks ago

Indeed! Why pay for wrong information

upvoted 5 times

snarkymark 10 months ago

Yes, Agree

upvoted 3 times

Nickplayany Highly Voted 10 months, 1 week ago

Selected Answer: D

D. a package of files that is used to describe a virtual machine or virtual appliance

upvoted 6 times

Asombrosso Most Recent 4 months, 1 week ago

Selected Answer: D

but itsn't a package of files! its a single XML file.

upvoted 1 times

Asombrosso 4 months, 1 week ago

Correction:
In addition to the OVF descriptor(XML), the OVF package will typically contain one or more disk images, and optionally certificate files and other auxiliary files.

The entire directory can be distributed as an Open Virtual Appliance (OVA) package, which is a tar archive file with the OVF directory inside.

upvoted 1 times

DavideDL 10 months, 1 week ago

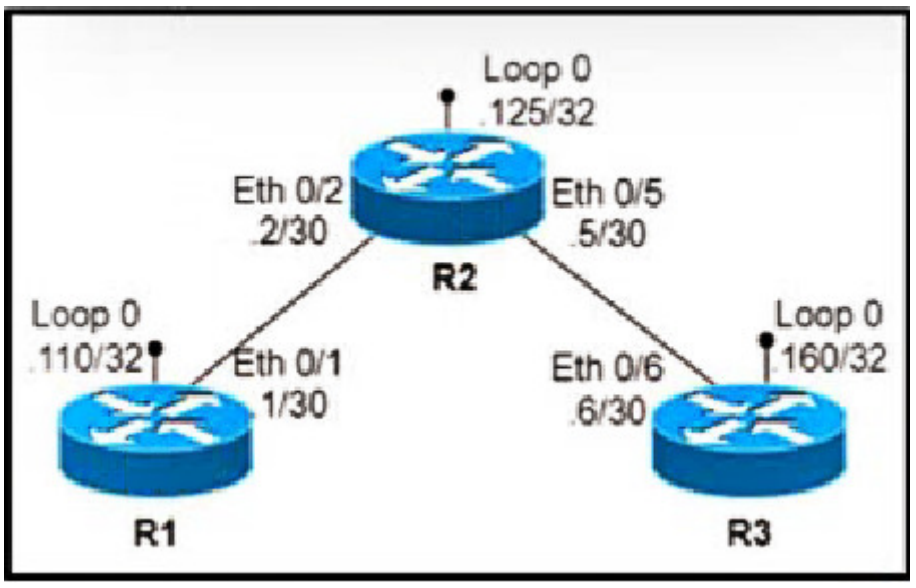
Selected Answer: D

https://spin.atomicobject.com/2013/06/03/ovf-virtual-machine/#:~:text=Most%20commonly%2C%20an%20OVF%20file,on%20such%20a%20disk%20image.

Most commonly, an OVF file is used to describe a single virtual machine or virtual appliance. It can contain information about the format of a virtual disk image file as well as a description of the virtual hardware that should be emulated to run the OS or application contained on such a disk image.

upvoted 5 times

Refer to the exhibit.



An engineer configures routing between all routers and must build a configuration to connect R1 to R3 via a GRE tunnel. Which configuration must be applied?

A. R1 -
interface Tunnel1
ip address 1.1.1.13 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.110

R3 -
interface Tunnel
ip address 1.1.1.31 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.160

B. R1 -
interface Tunnel1
ip address 1.1.1.13 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.160

R3 -
interface Tunnel1
ip address 1.1.1.31 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.110

C. R1 -
interface Tunnel2
ip address 1.1.1.12 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.125

R2 -
interface Tunnel1
ip address 1.1.1.125 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.110
interface Tunnel3

ip address 1.1.1.125 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.160

R3 -
interface Tunnel2
ip address 1.1.1.32 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.125

D. R1 -
interface Tunnel1
ip address 1.1.1.13 255.255.255.0
tunnel source Loopback0
tunnel destination x-y.z.110

R3 -
interface Tunnel1
ip address 1.1.1.31 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.125

Correct Answer: *B*

Community vote distribution

B (100%)

mgiuseppe86 3 months, 4 weeks ago

This is the absolutely worst fucking diagram i have ever seen.

upvoted 3 times

NLFluke 5 months, 2 weeks ago

A - Wrong - Tunnel destination is itself
B - Correct - Since the question says "An engineer configures routing between all routers" we must assume the Loopbacks are being advertised, so we can use them as source / destination.
C - Wrong - Doesn't make sense since we have a tunnel from R1 to R2
D - Wrong - Tunnel destination is itself

upvoted 2 times

tempaccount00001 6 months, 1 week ago

what the f is this, all interface IPs are wrong...

upvoted 3 times

mgiuseppe86 3 months, 4 weeks ago

Yep its pretty bad.

upvoted 1 times

Opreis 10 months, 1 week ago

Selected Answer: B

Correct

upvoted 4 times

Question #704 *Topic 1*

Which function does a virtual switch provide?

A. RAID storage for virtual machines

B. connectivity between virtual machines

C. CPU context switching for multitasking between virtual machines

D. emulation of power for virtual machines

Correct Answer: *B*

Community vote distribution

B (100%)

NikosTsironis 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

ando2023 6 months, 3 weeks ago

B is correct. In VMware its called a vSwitch and connects different VM's together.

upvoted 2 times

Question #705 *Topic 1*

Which device is responsible for finding EID-to-RLOC mapping when traffic is sent to a LISP-capable site?

A. map resolver

B. egress tunnel router

C. map server

D. ingress tunnel router

Correct Answer: *C*

Community vote distribution

D (93%) 7%

Quentin_ Highly Voted 9 months, 4 weeks ago

Selected Answer: D

An ITR is responsible for finding EID-to-RLOC mappings for all traffic destined for LISP-capable sites.
When the ITR receives a packet destined for an EID, it first looks for the EID in its mapping cache. If the ITR finds a match, it encapsulates the packet inside a LISP header with one of its RLOCs as the IP source address and one of the RLOCs from the mapping cache entry as the IP destination. The ITR then routes the packet normally.

upvoted 6 times

Asombrosso Most Recent 4 months, 1 week ago

Selected Answer: D

An ITR is responsible for finding EID-to-RLOC mappings for all traffic destined for LISP-capable sites.

upvoted 1 times

ihateciscoreally 5 months ago

another broken question, one word changes question's whole meaning.

upvoted 2 times

Networkfate 5 months, 3 weeks ago

An ETR connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to Map-Request messages, and decapsulates and delivers LISP-encapsulated user data to end systems at the site

upvoted 1 times

Networkfate 5 months, 3 weeks ago

An ITR is responsible for finding EID-to-RLOC mappings for all traffic destined for LISP-capable sites.
When the ITR receives a packet destined for an EID, it first looks for the EID in its mapping cache
Answer is ETR keyword"publish"

upvoted 1 times

Lungful 5 months ago

I assume you mean the answer is ITR due to "finding" and the line above is just a typo.

upvoted 1 times

Networkfate 5 months, 3 weeks ago

Publish means ; ETR
Finding means: ITR

upvoted 4 times

Symirnian 9 months, 3 weeks ago

Selected Answer: D

Responsible means to search for RLOC and route the traffic in time. So D.

upvoted 2 times

Clauster 10 months, 1 week ago

Selected Answer: D

Answer is D
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/15-mt/irl-15-mt-book/irl-overview.pdf

Thank god for discussions or I will fail lol

upvoted 3 times

Badger_27 10 months, 1 week ago

Selected Answer: D

D - read the working of the question.
upvoted 1 times

Opreis 10 months, 1 week ago

Selected Answer: D

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.pdf
upvoted 1 times

Nickplayany 10 months, 1 week ago

Selected Answer: C

Map server: This is a network device that learns EID-to-prefix mapping entries from an ETR and stores them in a local EID-to-RLOC mapping database.

I think C is correct
upvoted 1 times

Nickplayany 9 months, 1 week ago

D is the correct my bad. I totally misunderstood this.
upvoted 1 times

MikeyPher 10 months, 1 week ago

I think the answer is D.
An ITR is responsible for finding EID-to-RLOC mappings for all traffic destined for LISP-capable sites
upvoted 1 times

snarkymark 10 months, 1 week ago

Agree D,
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/15-sy/irl-15-sy-book/irl-overview.pdf
upvoted 1 times

Question #706 *Topic 1*

In which way are EIGRP and OSPF similar?

A. They both support unequal-cost load balancing.

B. They both support MD5 authentication for routing updates.

C. They both support autosummarization.

D. They have similar CPU usage, scalability, and network convergence times.

Correct Answer: *B*

Community vote distribution

B (89%) 11%

Asombrosso 4 months, 1 week ago

Selected Answer: B

They both DONT support autosummarization in similar way

upvoted 1 times

djedeen 4 months, 2 weeks ago

Selected Answer: B

Correct = B.
D is incorrect per: 'EIGRP vs OSPF: CPU Usage.OSPF maintains the complete information about the routers in its area. Each time there is a change within the area, all routers need to re-sync their database, which makes it more CPU intensive. EIGRP, on the other hand, has triggered and incremental updates and will not send all the information about the network rather just the information that has changed will be shared.'

upvoted 1 times

Mani9Don 7 months, 1 week ago

Selected Answer: D

100% D is the right answer.

EIGRP supports MD5 but not for routing updates

upvoted 1 times

b7c04a1 1 month, 1 week ago

"The IP Enhanced IGRP Route Authentication feature provides MD5 authentication of routing updates from
the EIGRP routing protocol."
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-s/ire-15-s-book/ire-rte-auth.pdf

upvoted 1 times

danman32 6 months, 3 weeks ago

OSPF is much more resource intensive, hence it was designed with areas to reduce the information needed to be processed.

upvoted 1 times

jackr76 9 months, 3 weeks ago

Selected Answer: B

MD5 EIGRP
https://networklessons.com/eigrp/how-to-configure-eigrp-authentication

MD5 OSPF
https://networklessons.com/ospf/how-to-configure-ospf-md5-authentication

upvoted 3 times

snarkymark 10 months, 1 week ago

Selected Answer: B

https://community.fs.com/blog/eigrp-vs-ospf-differences.html

upvoted 3 times

jackr76 9 months, 3 weeks ago

no MD5 on that page

upvoted 1 times

snarkymark 8 months, 2 weeks ago

use process of elimination

upvoted 2 times

Question #707 *Topic 1*

Which option works with a DHCP server to return at least one WLAN management interface IP address during the discovery phase and is dependent upon the VCI of the AP?

A. Option 15

B. Option 43

C. Option 125

D. Option 42

Correct Answer: *B*

Community vote distribution

B (100%)

eddgg 5 months, 1 week ago

Selected Answer: B

i am sending my answer

upvoted 1 times

eddgg 5 months, 1 week ago

The option that works with a DHCP server to return at least one WLAN (Wireless Local Area Network) management interface IP address during the discovery phase and is dependent upon the Vendor Class Identifier (VCI) of the Access Point (AP) is called the "Vendor Specific Information" option (Option 43).

upvoted 1 times

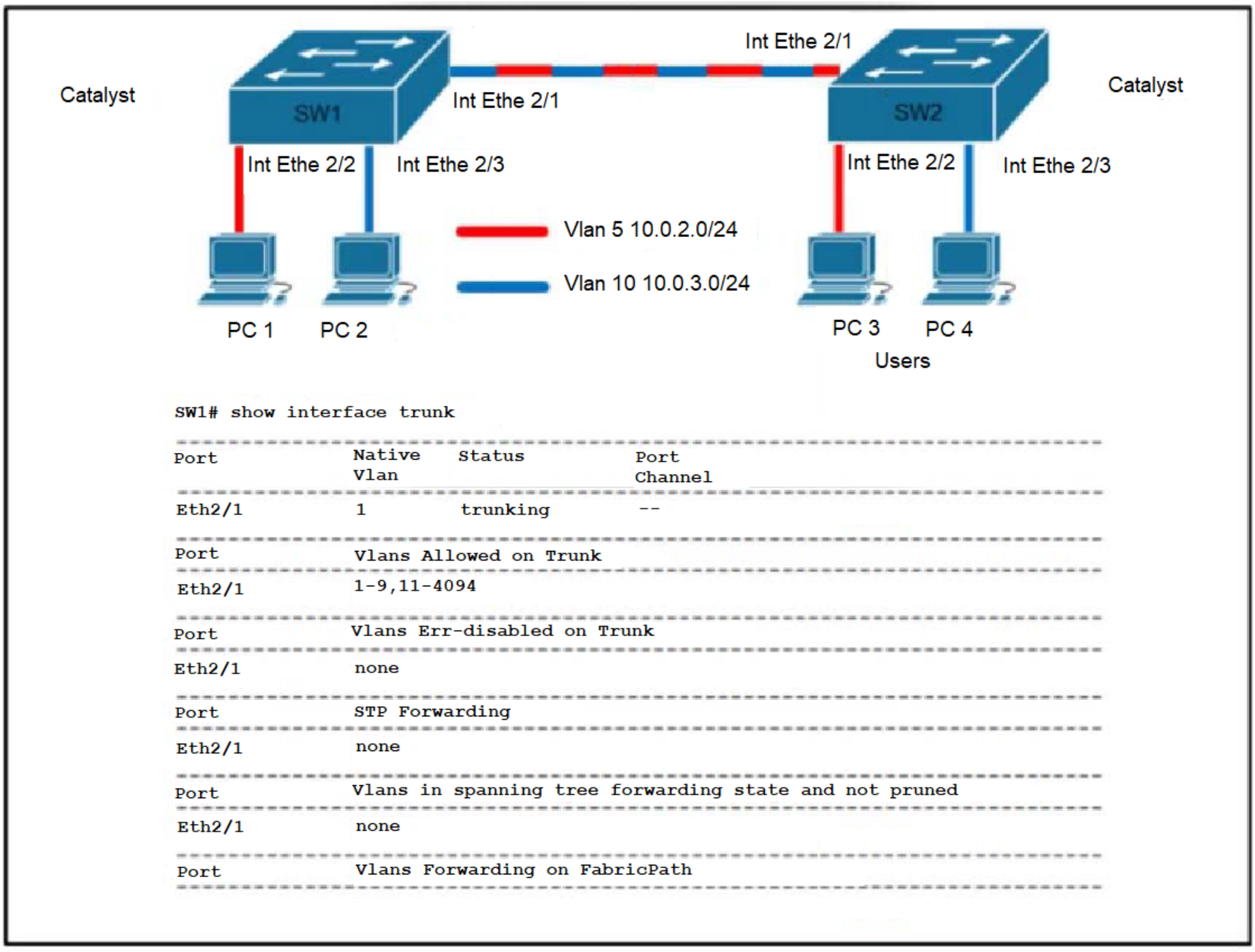
snarkymark 10 months, 1 week ago

Selected Answer: B

Correct

upvoted 2 times

Refer to the exhibit.




```
SW1# show interface trunk
--------------------------------------------------------------------------------
Port            Native  Status        Port
                Vlan                  Channel
--------------------------------------------------------------------------------
Eth2/1          1       trunking      --
--------------------------------------------------------------------------------
Port            Vlans Allowed on Trunk
--------------------------------------------------------------------------------
Eth2/1          1-9,11-4094
--------------------------------------------------------------------------------
Port            Vlans Err-disabled on Trunk
--------------------------------------------------------------------------------
Eth2/1          none
--------------------------------------------------------------------------------
Port            STP Forwarding
--------------------------------------------------------------------------------
Eth2/1          none
--------------------------------------------------------------------------------
Port            Vlans in spanning tree forwarding state and not pruned
--------------------------------------------------------------------------------
Eth2/1          none
--------------------------------------------------------------------------------
Port            Vlans Forwarding on FabricPath
--------------------------------------------------------------------------------
```

PC 2 cannot communicate with PC 4. Which configuration resolves this issue?

A. SW1(config)# interface Gigabitethernet 2/1
SW1(config-if)# switchport mode trunk

B. SW1(config)# interface Gigabitethernet 2/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10

C. SW1(config)# interface Gigabitethernet 2/1
SW1(config-if)# switchport trunk allowed vlan add 10

D. SW1(config)# interface Gigabitethernet 2/1
SW1(config-if)# switchport vlan mapping 10 10

Correct Answer: *C*

Community vote distribution

C (100%)

CCNPWILL 3 months, 1 week ago

Selected Answer: C

C. Obviously.

upvoted 1 times

danman32 6 months, 3 weeks ago

Strange that VLAN 5 is not listed in section "in spanning tree and not pruned". After all, it is allowed.

upvoted 1 times

nerdymarwa 9 months, 2 weeks ago

Correct but the interfaces mentioned are incorrect :)

upvoted 2 times

snarkymark 10 months, 1 week ago

Selected Answer: C

Correct

upvoted 1 times

Question #709 *Topic 1*

A customer has 20 stores located throughout a city. Each store has a single Cisco AP managed by a central WLC. The customer wants to gather analytics for users in each store. Which technique supports these requirements?

A. angle of arrival

B. presence

C. trilateration

D. hyperlocation

Correct Answer: *D*

Community vote distribution

B (71%) D (29%)

djedeen 5 months, 2 weeks ago

Selected Answer: B

B:
The Cisco Connected Mobile Experiences (Cisco CMX) Presence Analytics service enables organizations with small deployments, even those with only one or two access points (APs), to use the wireless technology to study customer behavior.

upvoted 1 times

Clauster 9 months, 2 weeks ago

Selected Answer: D

Giving Props to the Moderator here, I am going to start digging on these answers, this one is D here it is straight from Cisco

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/Halo-DG/b_hyperlocation-deployment-guide.html

upvoted 4 times

JackDRipper 9 months, 2 weeks ago

Wrong. Problem states that each store has only one (1) AP. Hyperlocation requires multiple APs to work.

If you read further down, you'll find this:
"A general rule of thumb is to have 3 or 4 access points that are within line of sight of the device at a distance of less than 70 feet."

upvoted 3 times

jackr76 9 months, 3 weeks ago

Selected Answer: B

As all say B

upvoted 2 times

Doh247 10 months, 1 week ago

Selected Answer: B

Single AP per Store. The question is asking about analytic data. Presence is the best fit.

upvoted 2 times

snarkymark 10 months, 1 week ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-4/cmx_config/b_cg_cmx104/the_cisco_cmx_presence_analytics_service.html

upvoted 3 times

Brian9296 10 months, 2 weeks ago

Selected Answer: B

Answer should be B

As Hyperlocation is meant for user location tracing, while the answer asking for analytic data of user, so should be Presence

upvoted 2 times

Brian9296 10 months, 2 weeks ago

Answer should be B

As Hyperlocation is meant for user location tracing, while the answer asking for analytic data of user, so should be Presence

upvoted 2 times

Question #710 *Topic 1*

Refer to the exhibit.

```
*Sep 16 09:13:40:974: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non
trunk GigabitEthernet0/0 VLAN0001.
*Sep 16 09:13:40:977: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet0/0
on VLAN0001. Inconsistent port type.
```

Two switches are interconnected using interface GigabitEthernet0/0 on both sides. While configuring one of the switches, a network engineer receives the logging message. Which action resolves this issue?

A. Block VLAN1 on the trunk interface GigabitEthernet0/0.

B. Configure interface GigabitEthernet0/0 as an access port.

C. Configure interface GigabitEthernet0/0 as a trunk port.

D. Shutdown interface GigabitEthemet0/0 and bring it back up.

Correct Answer: *B*

Community vote distribution

C (93%) 7%

Aldebeer 1 month, 3 weeks ago

it must be defiantly a trunk port!

upvoted 1 times

CCNPWILL 3 months, 1 week ago

Two switches together... means you need trunk ports on both.. that resolves the issue, no if and or buts about it. any justifications for other answers means you need to go study more. This is fundamental.

upvoted 1 times

mgiuseppe86 3 months, 4 weeks ago

Who the F chose B? Are you high?

Why would you want BPDUs sent on an access port?

Yes C is the answer, but you also have to remove bpduguard on the port and shut/no shut to bring it back up. so D is also an answer but only after you do C first.

upvoted 2 times

Asombrosso 4 months, 1 week ago

Selected Answer: C

GigabitEthernet0/0

upvoted 1 times

eddgg 5 months, 1 week ago

Selected Answer: C

c, it must be trunk to solve it

upvoted 1 times

djedeen 5 months, 2 weeks ago

C .....

upvoted 1 times

BobbyFlash 5 months, 3 weeks ago

C'mon Admin...

upvoted 1 times

Burik 6 months, 4 weeks ago

It's obviously C.

The NON TRUNK G0/0 port on our switch is receving a TRUNK DOT1Q BPDU from the switch at the other end of the link. G0/0 on our switch is an Access port in VLAN 1. The port on the switch at the other end of the link is a trunk port. So the fix is to configure G0/0 on our switch as TRUNK.

Admins, please fix the answer.

upvoted 1 times

Chiaretta 9 months ago

this is a stupid question because it ask to fix problem but don't say how. I think the answer is correct because it dont talk of vlan.
If you need only one vlan the answer is correct.

upvoted 1 times

bullett00th 9 months, 3 weeks ago

Selected Answer: C

B is causing the issue. C is resolves it.

upvoted 4 times

Leoveil 9 months, 4 weeks ago

B is the cause of the issue. C to resolve it

upvoted 3 times

Clauster 10 months, 1 week ago

Selected Answer: B

The answer is 100% B here's why
On the Output Switch we received that error code, the Error code CLEARLY states that we received a NON_TRUNK and that we received a BPDU from an 802.1Q on our Trunk Interface g0/0 which means we are set to Trunk.

You can't set to Trunk again because we are already set to trunk, if we switchport mode access the link will become operational.

upvoted 1 times

Clauster 10 months, 1 week ago

My Apologies answer is C

upvoted 2 times

cuda74 10 months, 1 week ago

Selected Answer: C

Port will be configured as trunk.

upvoted 2 times

Badger_27 10 months, 1 week ago

Selected Answer: C

C would resolve the problem but you would also need to shut/no shut the interface?

upvoted 2 times

NLFluke 5 months, 2 weeks ago

The interface is not in err-disabled mode so no bounce needed.
The interface will show a status of 'BKN' and a type of 'P2p *TYPE_Inc', you can also verify that with the command: show spanning-tree inconsistentports.

upvoted 1 times

verbose_bronzes 10 months, 1 week ago

Selected Answer: C

C is the answer

upvoted 1 times

snarkymark 10 months, 1 week ago

Selected Answer: C

You would think!?

upvoted 2 times

Brian9296 10 months, 1 week ago

The question stated that G0/0 is interconnection link between 2 switch. So i think the answer should be C. Trunk link

upvoted 3 times

Question #711 *Topic 1*

By default, which virtual MAC address does HSRP group 12 use?

A. 00:00:0c:07:ac:0c

B. 00:05:5e:00:0c:12

C. 00:5e:0c:07:ac:12

D. 05:43:84:57:29:2c

Correct Answer: *A*

Community vote distribution

A (100%)

mgiuseppe86 3 months, 4 weeks ago

12 = 00001100 = 0000|1100 = 0|12 = 0C

upvoted 1 times

RamazanLokov 7 months, 2 weeks ago

Selected Answer: A

correct

upvoted 1 times

bullett00th 9 months, 3 weeks ago

Selected Answer: A

Correct

upvoted 1 times

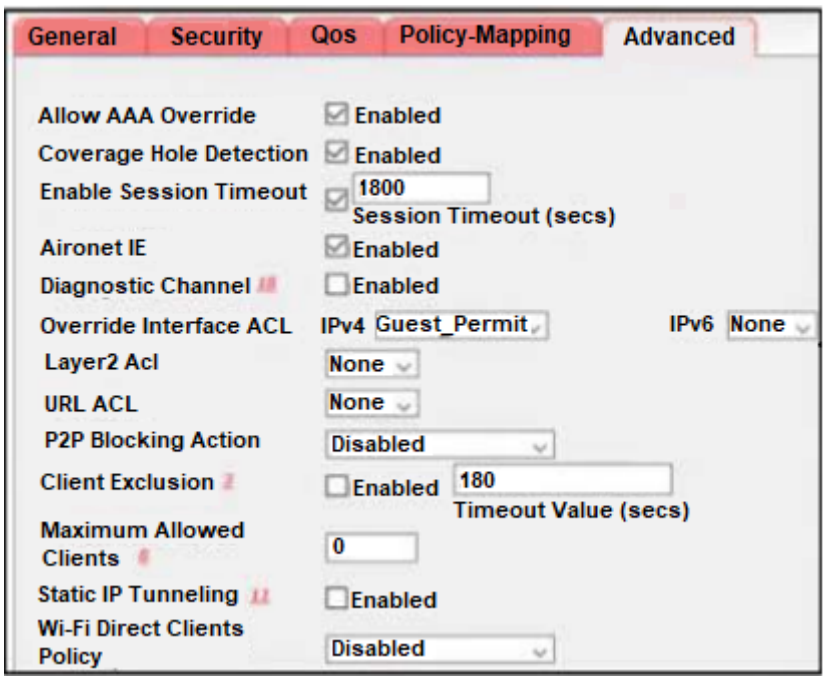
snarkymark 10 months, 1 week ago

Selected Answer: A

correct

upvoted 1 times

Refer to the exhibit.



An engineer configures a new WLAN that will be used for secure communications; however, wireless clients report that they are able to communicate with each other. Which action resolves this issue?

A. Enable Client Exclusions.

B. Enable P2P Blocking.

C. Disable Aironet IE.

D. Enable Wi-Fi Direct Client Policy.

Correct Answer: *A*

Community vote distribution

B (100%)

Brian9296 Highly Voted 10 months, 2 weeks ago

Selected Answer: B

The answer is B. Enable P2P Blocking.

upvoted 9 times

kinezi Most Recent 4 months ago

Selected Answer: B

B is correct

upvoted 1 times

ermanzan 6 months, 3 weeks ago

Selected Answer: B

Definitively, B is the correct answer. P2P Blocking is the mechanism to block communications between host in the same SSID

upvoted 4 times

funmax 7 months ago

Selected Answer: B

B is correct

upvoted 3 times

ClPo 8 months, 3 weeks ago

Selected Answer: B

B of course. Amazing what answers the "exports" pick as suggested answer

upvoted 3 times

Clauster 10 months, 1 week ago

Selected Answer: B

The Answer IS NOT A
Client exclusions only matter for when client authenticates, it has nothing to do with Secure Communication.

More info on Client Exclusions:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_01001011.pdf

The Anwer is B
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_01001011.pdf

upvoted 3 times

kalachuh 10 months, 1 week ago

Answer is B. P2P Blocking.

upvoted 3 times

Opreis 10 months, 1 week ago

Selected Answer: B

https://www.kareemccie.com/2018/06/what-is-peer-2-peer-blocking-in-cisco.html#:~:text=%2D%2D%3E%20Peer%202%20Peer%20blocking,it%20only%20blocks%20unicast%20traffic.

upvoted 1 times

Nickplayany 10 months, 1 week ago

Selected Answer: B

Enable P2P Blocking.

upvoted 3 times

Question #713 *Topic 1*

Refer to the exhibit.

```
vlan 222
 remote-span
!
vlan 223
 remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

What happens to access interfaces where VLAN 222 is assigned?

A. STP BPDU guard is enabled.

B. A description "RSPAN" is added.

C. They are placed into an inactive state.

D. They cannot provide PoE.

Correct Answer: *C*

Community vote distribution

C (100%)

shefo1 2 months, 2 weeks ago

Selected Answer: C

Because VLAN 222 is an RSPAN VLAN, any access interfaces that are assigned to VLAN 222 will be placed into an inactive state. This means that they will not forward any traffic, except for traffic that is specifically destined for the switch.

upvoted 2 times

Opreis 10 months, 1 week ago

After the system is on, a SPAN or RSPAN destination session remains inactive until the destination port is operational. An RSPAN source session remains inactive until any of the source ports are operational or the RSPAN VLAN becomes active.

upvoted 3 times

snarkymark 10 months, 1 week ago

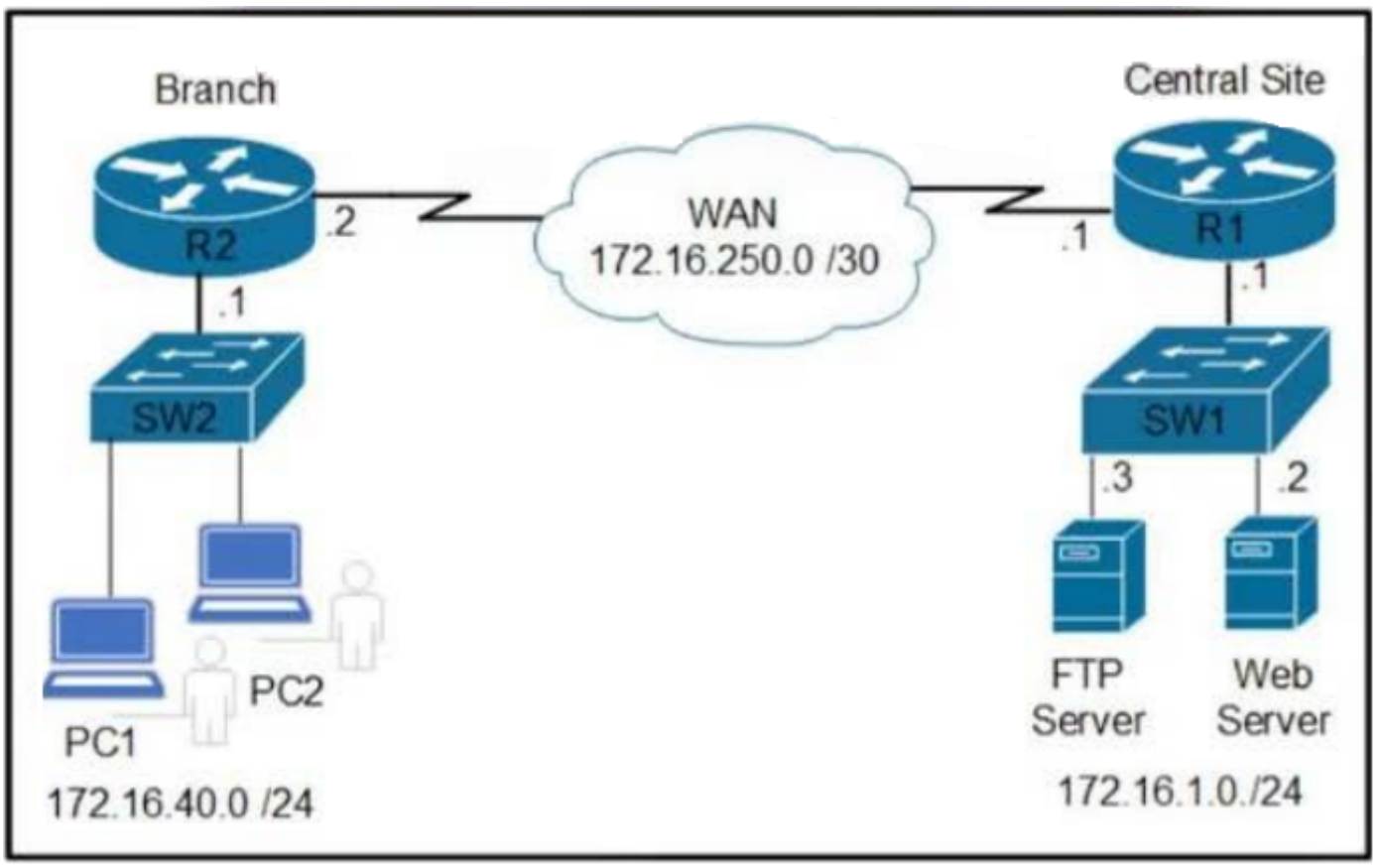
Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/span.html#wp1022030

upvoted 2 times

Question #714 *Topic 1*

Refer to the exhibit.



Which command is required to validate that an IP SLA configuration matches the traffic between the branch office and the central site?

A. R1# show ip sla group schedule

B. R1# show ip route

C. R1# show ip sla configuration

D. R1# show ip sla statistics

Correct Answer: *C*

Community vote distribution

D (79%) C (21%)

Jeff555566 Highly Voted 9 months, 3 weeks ago

Selected Answer: D

Question says to "validate" that the configuration matches the traffic - D, sh ip sla statistics has the counters that show the "matched" traffic.

upvoted 7 times

eearmani Most Recent 1 week, 3 days ago

Selected Answer: C

to validate the configuration
BRCC-LAN-B#show ip sla configuration
IP SLAs Infrastructure Engine-II
Entry number: 10
Owner:
Tag:
Type of operation to perform: icmp-echo
Target address/Source address: 1.1.1.1/11.11.11.11
Operation timeout (milliseconds): 3000
Type Of Service parameters: 0x0

upvoted 1 times

CCNPWILL 3 months, 1 week ago

Selected Answer: D

The answer is D. lab ouput provided int he discussions already.

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: C

Router# show ip sla configuration 3

Entry number: 3

Owner:
Tag:
Type of operation: echo
Target address/Source address: 1.1.1.1/0.0.0.0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Vrf Name:
Request size (ARR data portion): 28
Verify data: No
Schedule:
Next Scheduled Start Time: Start Time already passed
Group Scheduled: False
Operation frequency (seconds): 60
Life/Entry Ageout (seconds): Forever/never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 5
Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Enhanced History:

upvoted 1 times

Asombrosso 4 months, 1 week ago

Router# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200 OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707

upvoted 1 times

Asombrosso 4 months, 1 week ago

When the IP SLA operation is scheduled, it can be verified with the show ip sla configuration command. Example 24-55 illustrates the configuration steps to schedule the IP SLA 1 operation with a start time of now and a lifetime of forever. This example also shows the verification that it is running and configured properly.
OCG

upvoted 1 times

Asombrosso 4 months, 1 week ago

my fault, It should be D, "matches the traffic"

DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707

upvoted 1 times

olaniyijt 8 months, 3 weeks ago

C is more correct. It shows configuration.
Statistics shows counters. Successes and Failures.

"Which command is required to validate that an IP SLA configuration"

upvoted 1 times

olaniyijt 8 months, 3 weeks ago

"Which command is required to validate that an IP SLA configuration matches the traffic".

To validate, you need to check if the SLA is successful or failing and that's "sh ip sla statistics". Please ignore my first comment, D is correct

upvoted 5 times

Clauster 10 months, 1 week ago

Selected Answer: C

Correct answer is C
Information can be found here

https://www.cisco.com/c/en/us/td/docs/ios/ipsla/command/reference/sla_book/sla_04.html
upvoted 2 times

snarkymark 10 months ago

Agree, "configuration" provides better info then "stat
upvoted 2 times

kalachuh 10 months, 1 week ago

show ip sla statisic
upvoted 1 times

Nickplayany 10 months, 1 week ago

Selected Answer: D

show ip sla statistics
upvoted 3 times

Brian9296 10 months, 2 weeks ago

Selected Answer: D

The answer is D. R1# show ip sla statistics
upvoted 4 times

Question #715 *Topic 1*

Refer to the exhibit.

```
hostname Cat3850
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 ip address 198.51.100.214 255.255.255.0
 no shutdown
!
ip route vrf Mgmt-vrf 0.0.0.0 0.0.0.0 198.51.100.1
```

The administrator must extend the configuration of the switch to perform remote logging using syslog according to these requirements:
• syslog server: 203.0.113.11 reachable through Gi0/0
• initial message severity: notifications
• message transport: reliable

Which two commands must be added to the configuration to accomplish this goal? (Choose two.)

A. logging monitor notifications

B. logging host 203.0.113.11 vrf Mgmt-vrf transport tcp

C. logging source-Interface GigabitEthernet0/0 vrf Mgmt-vrf

D. logging trap notifications

E. logging host 203.0.113.11 vrf Mgmt-vrf

Correct Answer: *BE*

Community vote distribution

BD (56%) BC (24%) 12% 4%

eww_cybr Highly Voted 6 months, 1 week ago

Selected Answer: BD

This question applies to Catalyst 3850 SWITCH.
Answer is BD not BC.

logging host 203.0.113.11 vrf Mgmt-vrf transport tcp - changed from udp to tcp
logging trap notifications - change from informational to notification/notice

logging source-Interface GigabitEthernet0/0 vrf Mgmt-vrf - will be used by default. Gig0/0 will most probably be the only interface on the switch in VRF mgmt hence no need to configure this one.

upvoted 5 times

eearmani Most Recent 1 month ago

Selected Answer: DE

Configure logging to the syslog server with VRF
logging 192.168.1.1 vrf mngt

Set logging severity level (e.g., informational)
logging trap informational

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: BD

By default, syslog servers receive informational messages (level 6)

upvoted 1 times

Asombrosso 4 months, 1 week ago

When the IP SLA operation is scheduled, it can be verified with the show ip sla configuration command. Example 24-55 illustrates the configuration steps to schedule the IP SLA 1 operation with a start time of now and a lifetime of forever. This example also shows the verification that it is running and configured

properly.
OCG
upvoted 1 times

djedeen 4 months, 2 weeks ago

Selected Answer: BC

Has to be B and C because [D] is not needed, as default logging trap level is notifications.
Command Default
Syslog messages at level 0 to level 6 are generated, but will only be sent to a remote host if the logging host command is configured.
[0 | emergencies]—System is unusable
[1 | alerts]—Immediate action needed
[2 | critical]—Critical conditions
[3 | errors]—Error conditions
[4 | warnings]—Warning conditions
[5 | notifications]—Normal but significant conditions
[6 | informational]—Informational messages
[7 | debugging]—Debugging messages
upvoted 1 times

Manvek 5 months, 1 week ago

Selected Answer: BE

B: there we configure the syslog and specify the vrf and the protocol to be tcp.
D: The requirement is for the lowest severity to be Notification.

Regarding the requirement that the syslog needs to be reachable through interface G0/0. The interface is already part of the VRF and there is a default route pointing to the subnet of the interface. The server needs to be reachable "through that interface" not "only through that interface"
upvoted 1 times

Manvek 5 months, 1 week ago

Answer BD, no BE.
upvoted 1 times

rogi2023 6 months ago

Selected Answer: BD

it says "initial message severity: notifications" the default is informational so we have to choose D. B is clear
upvoted 2 times

eww_cybr 6 months, 1 week ago

Selected Answer: BC

This question applies to Catalyst 3850 SWITCH.

logging host 203.0.113.11 vrf Mgmt-vrf transport tcp - changed from udp to tcp
logging trap notifications - change from informational to notification/notice

logging source-Interface GigabitEthernet0/0 vrf Mgmt-vrf - will be used by default. Gig0/0 will most probably be the only interface on the switch in VRF mgmt hence no need to configure this one.
upvoted 2 times

CKL_SG 6 months, 1 week ago

Selected Answer: DE

Configuring VRF Aware System Message Logging on a Routing Device
Perform this task to configure the VRF Aware System Message Logging feature on a routing device. This allows the sending of logging messages that can be used to monitor and troubleshoot network traffic connected through VRF instances.

Prerequisites
You must perform the following tasks before you perform this task:

•Configuring a VRF on a Routing Device

•Associating a VRF with an Interface

SUMMARY STEPS
1. enable

2. configure terminal

3. logging host {ip-address | hostname} [vrf vrf-name]

4. logging trap level

5. logging facility facility-type

6. logging buffered [buffer-size | severity-level]

7. end
upvoted 2 times

[Removed] 6 months, 2 weeks ago

Selected Answer: BC

I have to agree with other users.
I tried different scenarios, one where the router is directly connected to the Syslog server, and one where the router was two hops away from the server.
If you don't specify the source interface, it will utilize the one for egress traffic towards the default route.

upvoted 1 times

danman32 6 months, 3 weeks ago

Answer BC
The default trap level (Trap being what goes to syslog server) is informational, so answer D is not necessary.
Answer A doesn't affect what goes to the syslog server, only what goes to terminal sessions (Telnet/SSH)
So that leaves two of B, C and E.
You need to specify TCP as the transport, so you need B, and that crosses out E since E is same as B but without TCP
So all you have left to go with B is C to specify the source interface.

Someone on Cisco community asked a similar question with regards to sending sylog through the the management interface:
https://community.cisco.com/t5/network-management/logging-through-the-management-interface/td-p/3071828

Reply said to specify the VRF when specifying the source interface.
The OP then replied he also had to specify the VRF when specifying the host.

upvoted 2 times

Splashisthegreatestmovie 6 months, 4 weeks ago

the question is asking us to ensure that send packets through G0/0. The only way to do that is to use the logging source-interface command

upvoted 1 times

ClPo 8 months, 3 weeks ago

I'd say B and D, but how can an expert come to "BE"?

upvoted 1 times

jackr76 9 months, 3 weeks ago

If it's sa hard to get it right here... how to do in the actual exam?

upvoted 4 times

Clauster 10 months, 1 week ago

Selected Answer: AE

Answers are 100% A and E i am backing up my information here
For Answer A: https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html

For Answer E: https://www.cisco.com/c/en/us/td/docs/ios/12_2sr/12_2sra/feature/guide/srvrfslg.html

You're welcome

upvoted 1 times

snarkymark 10 months ago

disagree, logging monitor level = Limits messages logged to the terminal lines.
logging trap level = Limits messages logged to the syslog servers.

So D for logs to syslog servers. And B for host IP and thru mgmt-vrf

upvoted 5 times

asiansensation 10 months, 1 week ago

B and D for sure

upvoted 1 times

Brian9296 10 months, 1 week ago

Selected Answer: BD

i think B and D is more likely the answer

upvoted 3 times

Question #716 *Topic 1*

Which two prerequisites must be met before Cisco DNA Center can provision device? (Choose two.)

A. Cisco DNA Center must have the software image for he provisioned device in its image repository.

B. The provisioned device must be put into bootloader mode.

C. The provisioned device must be configured with CLI and SNMP credentials that are known to Cisco DNA Center.

D. Cisco DNA Center must have IP connectivity to the provisioned device.

E. The provisioned device must recognize Cisco DNA Center as its LLDP neighbor.

Correct Answer: *CE*

Community vote distribution

CD (95%) 5%

Tadese 3 months, 3 weeks ago

Definitely CD is the correct answer

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: CD

definately Itsn't E: cuz CDP is not mentioned

upvoted 1 times

sam6996 5 months, 4 weeks ago

Selected Answer: CD

"The prerequisites of DNAC being able to manage devices are:

DNAC must have:

SSH access
Privilege level 15
SNMP access
SNMPv2c read at a minimum"

https://zartmann.dk/dnac-provision-what-it-does-to-your-devices/

upvoted 3 times

rtfgvb 8 months, 1 week ago

Selected Answer: CD

D It's necessary

upvoted 4 times

Chiaretta 8 months, 2 weeks ago

Selected Answer: CD

C and D

upvoted 2 times

Clauster 10 months, 1 week ago

Selected Answer: CD

Out of all of the answers the only 100% sure answer is C and then the common sense one is D
Feel free to check out more information on the following link:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-2/user_guide/b_cisco_dna_center_ug_2_2_2/b_cisco_dna_center_ug_2_2_2_chapter_01101.html

upvoted 4 times

asiansensation 10 months, 1 week ago

C and D definitely

upvoted 2 times

Opreis 10 months, 1 week ago

Selected Answer: CE

Provided answers are correct

upvoted 1 times

belisarius 10 months ago

It can't be E, because it would mean that ALL the devices must be L2 adjacent to the DNA Center. I know, that DNA Center can provision CDP and LLDP adjacent devices, but that is not a requirement for provisioning.

upvoted 4 times

blindz0rs 10 months, 2 weeks ago

Selected Answer: CD

It can't provision if it can't reach it.

upvoted 4 times

Question #717 *Topic 1*

In Cisco DNA Center, what is used to publish events and notifications to a third-party product such as IPAM?

A. intent API

B. southbound SDK

C. integration API

D. RESTful API

Correct Answer: *B*

Community vote distribution

C (76%) D (21%)

MJane Highly Voted 10 months ago

Selected Answer: C

https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitive-advantage

Westbound—Integration APIs
Cisco DNA Center platform can power end-to-end IT processes across the value chain by integrating various domains such as ITSM, IPAM, and reporting. By leveraging the REST-based Integration Adapter APIs, bi-directional interfaces can be built to allow the exchange of contextual information between Cisco DNA Center and the external, third-party IT systems. The westbound APIs provide the capability to publish the network data, events and notifications to the external systems and consume information in Cisco DNA Center from the connected systems.

upvoted 11 times

Tadese Most Recent 2 weeks, 4 days ago

Selected Answer: C

Westbound—Integration APIs
Cisco DNA Center platform can power end-to-end IT processes across the value chain by integrating various domains such as ITSM, IPAM, and reporting. By leveraging the REST-based Integration Adapter APIs, bi-directional interfaces can be built to allow the exchange of contextual information between Cisco DNA Center and the external, third-party IT systems. The westbound APIs provide the capability to publish the network data, events and notifications to the external systems and consume information in Cisco DNA Center from the connected systems.

upvoted 1 times

due 4 months, 1 week ago

Selected Answer: C

REST API: Refers to any API that follows some principles of REST but may not adhere strictly to all of them.

RESTful API: A specific type of REST API that strictly adheres to all the constraints and principles of REST, providing a clean and consistent design.

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: C

For ITSM, IPAM - Integration API (Westbound)

upvoted 1 times

Cesar12345 7 months, 1 week ago

Selected Answer: C

https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/intent-api-northbound

upvoted 2 times

Indersingh 8 months ago

Selected Answer: C

correct answer is C
https://developer.cisco.com/dnacenter/integrationapis/

D says RESTful API not REST API

upvoted 2 times

Pilgrim5 8 months, 1 week ago

Selected Answer: C

Going with C

https://developer.cisco.com/dnacenter/integrationapis/#:~:text=The%20APIs%20provide%20the%20capability,Center%20from%20the%20connected%20systems.

upvoted 2 times

PKamato 8 months, 2 weeks ago

Selected Answer: D

https://developer.cisco.com/docs/dna-center/#!ipam-api-introduction/cisco-dna-center---ip-address-management-provider-integration

upvoted 2 times

Dataset 9 months, 1 week ago

Selected Answer: C

" to a third-party product ..."
Answer is C
Regards

upvoted 2 times

Nickplayany 9 months, 3 weeks ago

Selected Answer: C

Looks like it´s C

https://developer.cisco.com/dnacenter/integrationapis/

The APIs provide the capability to publish the network data, events and notifications to the external systems and as well, consume information in Cisco DNA Center from the connected systems.

upvoted 3 times

habibmangal 9 months, 4 weeks ago

if you dont know please dont comment, why you are confusing us !

upvoted 2 times

Vlad_Is_Love_ua 10 months ago

Selected Answer: B

SDKs allow management to be extended to network devices of third-party vendors to offer support for diverse environments. These southbound SDKs allow for the creation of device packs that allow Cisco DNA Center to recognize and manage previously unknown devices. In their first iteration, these SDKs support level one operations such as discovery, inventory, topology, availability, and health scores.

upvoted 1 times

Clauster 10 months, 1 week ago

Selected Answer: D

Answer is D

upvoted 2 times

asiansensation 10 months, 1 week ago

The answer is C

upvoted 1 times

daezee 10 months, 1 week ago

Selected Answer: D

D- REST API

Two third party integration modules are included in Cisco DNA Center, as shipped,
one for IPAM Provider Infoblox and one for Bluecat.
Other IPAM Providers may be configured for use with Cisco DNA Center by providing an IPAM Provider REST API service that meets the Cisco DNA Center IPAM Provider specification.

upvoted 4 times

PKamato 8 months, 2 weeks ago

https://developer.cisco.com/docs/dna-center/#!ipam-api-introduction/cisco-dna-center---ip-address-management-provider-integration

upvoted 1 times

makarov_vg 10 months, 1 week ago

https://developer.cisco.com/docs/dna-center/#!ipam-api-introduction/cisco-dna-center---ip-address-management-provider-integration

IPAM Provider Integration Requirements
- Cisco IPAM Provider must provide the complete Cisco IPAM Provider REST API including error handling, as described by this guide.

Answer D

upvoted 3 times

Brian9296 10 months, 1 week ago

Selected Answer: C

it should be C, its consider westbound integration API

upvoted 4 times

Question #718 *Topic 1*

Router R1 must be configured as a UDP responder on port 6336. Which configuration accomplishes this task?

A. (config)#ip sla responder udp-echo ipaddress 10.10.10.1 port 6336

B. (config)#ip sla responder udp-echo ipv4 10.10.10.1 port 6336

C. (config)#ip sla responder ipaddress 10.10.10.1 port 6336

D. (config-if)#ip sla responder udp-port ipaddress 10.10.10.1 port 6336

Correct Answer: *A*

Community vote distribution

A (100%)

eearmani 1 week, 3 days ago

Selected Answer: A

LAN-B(config)#ip sla responder udp-echo ipaddress 1.1.1.1 port 6336

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: A

ip sla responder udp-echo ipaddress [ip-address] port [port] vrf [vrf]

upvoted 2 times

mellohello 10 months, 1 week ago

Correct...

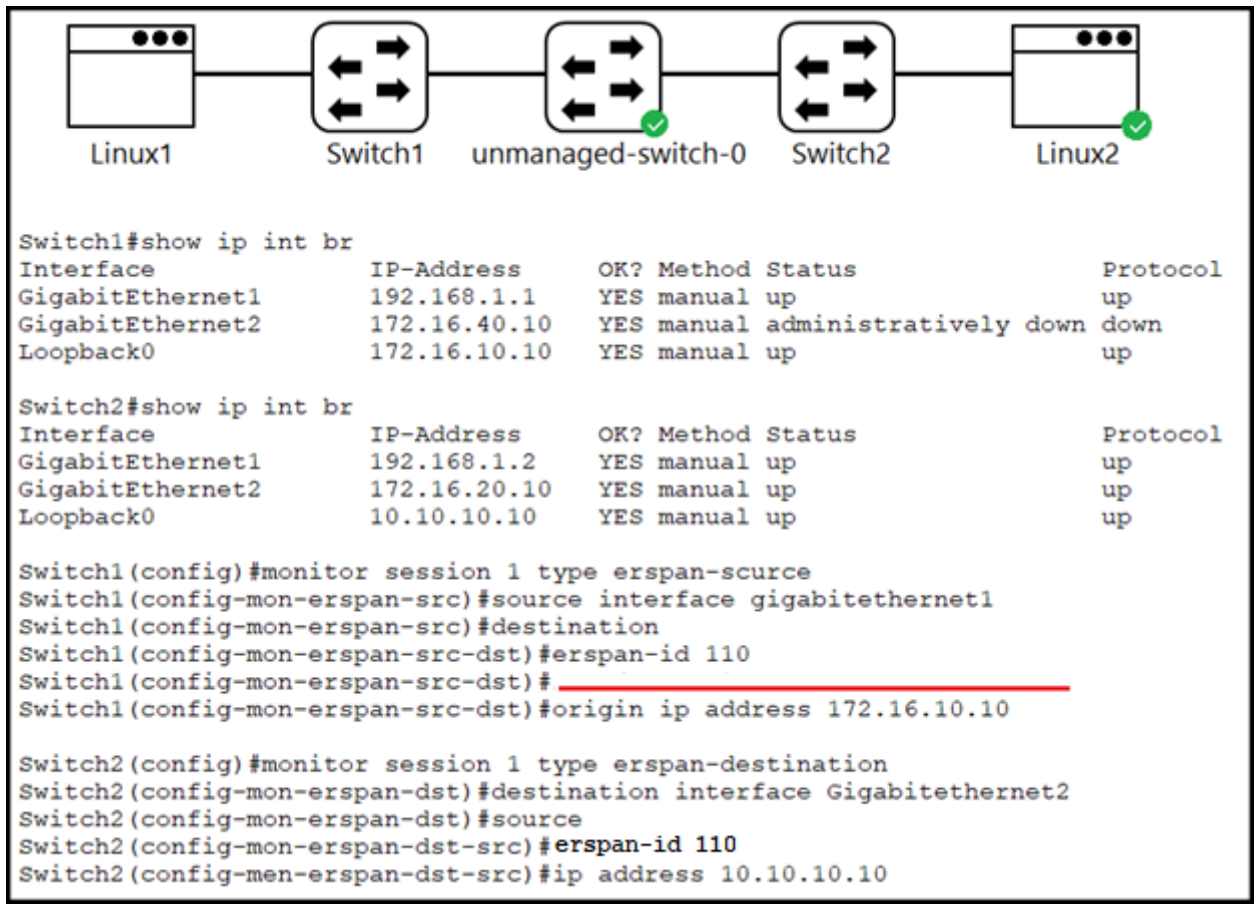
upvoted 1 times

Sa134 10 months, 1 week ago

A

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/xe-3s/sla-xe-3s-book/sla_udp_echo.pdf

upvoted 3 times



Refer to the exhibit. An engineer must configure an ERSPAN tunnel that mirrors traffic from Linux1 on Switch1 to Linux2 on Switch2. Which command must be added to the destination configuration to enable the ERSPAN tunnel?

A. (config-mon-erspan-src-dst)# no shut

B. (config-mon-erspan-src-dst)# traffic bidirectional

C. (config-mon-erspan-src-dst)# monitor session 1 activate

D. (config-mon-erspan-src-dst)# ip address 10.10.10.10

Correct Answer: *D*

Community vote distribution

D (100%)

Asombrosso 4 months, 1 week ago

Selected Answer: D

destination IP is mandatory

upvoted 2 times

Doh247 10 months ago

Correct.
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-3/configuration_guide/b_163_consolidated_3850_cg/b_163_consolidated_3850_cg_chapter_01001010.pdf

upvoted 2 times

snarkymark 10 months ago

Selected Answer: D

Agree with selected answer.

upvoted 2 times

Question #720 *Topic 1*

Refer to the exhibit.

```
Router#show running-config | include aaa
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
aaa session-id common
```

Which configuration enables fallback to local authentication and authorization when no TACACS+ server is available?

A. Router(config)# aaa fallback local

B. Router(config)# aaa authentication login FALLBACK local
Router(config)# aaa authorization exec FALLBACK local

C. Router(config)# aaa authentication login default local
Router(config)# aaa authorization exec default local

D. Router(config)# aaa authentication login default group tacacs+ local
Router(config)# aaa authorization exec default group tacacs+ local

Correct Answer: *D*

Community vote distribution

D (100%)

snarkymark Highly Voted 10 months ago

Selected Answer: D

https://ipwithease.com/understanding-aaa-configuration/

upvoted 9 times

raajj354 Most Recent 2 weeks, 1 day ago

Selected Answer: D

D is correct. Look for the text "default group" to distinguish the answer if you can't remember!

upvoted 1 times

CCNPWILL 3 months, 1 week ago

D is correct.

upvoted 1 times

felix_simon 5 months, 4 weeks ago

D

https://www.packetswitch.co.uk/cisco-tacacs-example-with-ise/

upvoted 2 times

mellohello 10 months, 1 week ago

I think it should be B? Im not sure.

upvoted 1 times

Question #721 *Topic 1*

Which configuration protects the password for the VTY lines against over-the-shoulder attacks?

A. line vty 0 15
password 2FpM7f82!

B. username admin secret 7 6j809J23kpp438337113N7%e$

C. line vty 0 4
password 2FpM7f82!

D. service password-encryption

Correct Answer: *D*

Community vote distribution

D (100%)

CCNPWILL 3 months, 1 week ago

Selected Answer: D

Yup yup

upvoted 2 times

[Removed] 6 months, 2 weeks ago

Selected Answer: D

agreed

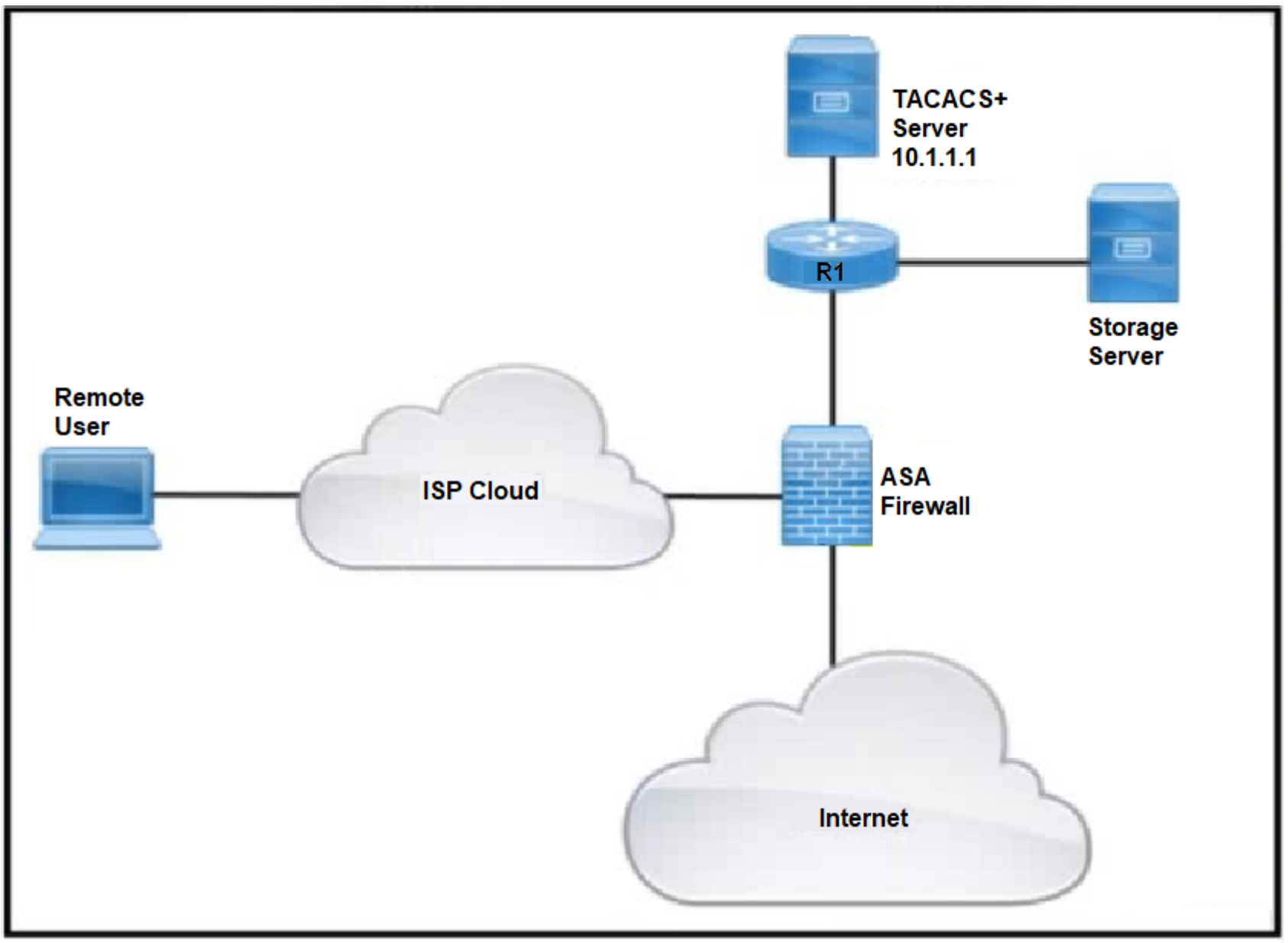
upvoted 2 times

Opreis 10 months, 1 week ago

correct

upvoted 4 times

Refer to the exhibit.



Remote users cannot access the Internet but can upload files to the storage server. Which configuration must be applied to allow Internet access?

A. ciscoasa(config)# access-list MAIL_AUTH extended permit udp any any eq http ciscoasa(config)# aaa authentication listener http outside redirect

B. ciscoasa(config)# access-list MAIL_AUTH extended permit tcp any any eq www ciscoasa(config)# aaa authentication listener http inside redirect

C. ciscoasa(config)# access-list MAIL_AUTH extended permit tcp any any eq http ciscoasa(config)# aaa authentication listener http inside port 43

D. ciscoasa(config)# access-list HTTP_AUTH extended permit udp any any eq http ciscoasa(config)# aaa authentication listener http outside port 43

Correct Answer: *B*

Community vote distribution

B (100%)

HarwinderSekhon Highly Voted 6 months, 2 weeks ago

Fuck you cisco

upvoted 20 times

monoki Highly Voted 10 months ago

Where did the Cisco exams gone? Can't find any in the site anymore.

upvoted 15 times

Asombrosso Most Recent 4 months, 1 week ago

Selected Answer: B

By a process of elimination

upvoted 1 times

dragonwise 9 months, 1 week ago

A.
ciscoasa(config)# access-list MAIL_AUTH extended permit udp any any eq http
ciscoasa(config)# aaa authentication listener http outside redirect

B.
ciscoasa(config)# access-list MAIL_AUTH extended permit tcp any any eq www
ciscoasa(config)# aaa authentication listener http inside redirect

C.
ciscoasa(config)# access-list MAIL_AUTH extended permit tcp any any eq http
ciscoasa(config)# aaa authentication listener http inside port 43

D.
ciscoasa(config)# access-list HTTP_AUTH extended permit udp any any eq http
ciscoasa(config)# aaa authentication listener http outside port 43

upvoted 5 times

JackDRipper 9 months, 2 weeks ago

Selected Answer: B

See: https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/fwaaa.html

upvoted 2 times

Jeff555566 9 months, 3 weeks ago

Selected Answer: B

B is the only one that makes any sense - eq www is correct to allow tcp port 80.

upvoted 4 times

htz0000 10 months ago

i'm in the same state
> Where did the Cisco exams gone? Can't find any in the site anymore.

upvoted 2 times

kalachuh 10 months ago

so all the AAA in different appliance are covered?

upvoted 1 times

MOES1349 10 months ago

I didn't see ASA in the ENCOR, but if this question came up on the exam and it made me think, don't expect it

upvoted 2 times

Badger_27 10 months, 1 week ago

ASA configs now in the Encor exam?

upvoted 2 times

Question #723 *Topic 1*

Refer to the exhibit.

Extended access-list 100 is configured on interface GigabitEthernet 0/0 in an inbound direction, but it does not have the expected behavior of allowing only packets to or from 192.168.0.0/16. Which command set properly configures the access list?

A. R1(config)#no access-list 100 deny ip any any

B. R1(config)#no access-list 100 seq 10
R1(config)#access-list 100 seq 40 deny ip any any

C. R1(config)#ip access-list extended 100
R1(config-ext-nacl)#5 permit ip any any

D. R1(config)#ip access-list extended 100
R1(config-ext-nacl)#no 10

Correct Answer: *D*

Community vote distribution

D (100%)

raajj354 2 weeks, 1 day ago

Can someone explain seq 30? Please.

upvoted 1 times

CCNPWILL 3 months, 1 week ago

D is correct. its short hand but its correct.

upvoted 1 times

yqpmateo 4 months, 1 week ago

no access-list 100 seq 10, will delete the entire access-list 100 !!!! you need to enter under the access list configuration and run a no command for the sequence you want to delete.

upvoted 1 times

djedeen 5 months, 2 weeks ago

Selected Answer: D

Note: At the end of each access list there is an explicit deny all statement, so the second ACL statement wasn't really necessary. After applying an access list, every traffic not explicitly permited will be denied.

upvoted 1 times

djedeen 5 months, 2 weeks ago

Meaning - no deny everything else needed, just the first two permit statements (20 and 30).

upvoted 2 times

Cryptoking112211 6 months, 1 week ago

The correct answer is B
you need to move the deny rule to the bottom of the list as the question says to only allow the subnet to and from.

upvoted 2 times

Pilgrim5 8 months, 1 week ago

Selected Answer: D

D makes sense because the 10 statement won't allow ip packets from the 192.168.0.0 subnet or any other subnet pass through

upvoted 2 times

snarkymark 10 months ago

Selected Answer: D

correct

upvoted 2 times

Question #724 *Topic 1*

Which security measure mitigates a man-in-the-middle attack of a REST API?

A. password hash

B. SSL certificates

C. nonrepudiation feature

D. biometric authentication

Correct Answer: *B*

Community vote distribution

B (100%)

CCNPWILL 3 months, 1 week ago

Selected Answer: B

B is correct.

upvoted 1 times

Pilgrim5 8 months, 1 week ago

Selected Answer: B

B is correct. Using SSL and TLS goes a long way in securing Restful APIs and preventing man in the middle attacks

https://blog.restcase.com/rest-apis-how-to-handle-man-in-the-middle-security-threat/

upvoted 1 times

snarkymark 10 months ago

Selected Answer: B

https://blog.restcase.com/rest-apis-how-to-handle-man-in-the-middle-security-threat/

upvoted 1 times

Question #725 *Topic 1*

A wireless administrator must create a new web authentication corporate SSID that will be using ISE as the external RADIUS server. The guest VLAN must be specified after the authentication completes. Which action must be performed to allow the ISE server to specify the guest VLAN?

A. Enable AAA Override.

B. Enable Network Access Control State.

C. Set AAA Policy name.

D. Set RADIUS Profiling.

Correct Answer: *D*

Community vote distribution

A (93%) 7%

Clauster Highly Voted 10 months, 1 week ago

Selected Answer: A

The Answer is A
AAA Override

Here's the Link: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/217043-configure-dynamic-vlan-assignment-with-c.html#anc18

Yet another incorrect answer, it would be amazing if they fix this as some people will fail the exam if they solely go by the answers provided by examtopics

upvoted 7 times

danman32 6 months, 3 weeks ago

Perhaps that's the point, has you study rather than blind memorization

upvoted 6 times

djedeen Most Recent 4 months, 2 weeks ago

Selected Answer: A

A - AAA Override
From the Advance tab, enable the Allow AAA Override check box to override the WLC configuration when the RADIUS server returns the attributes needed to place the client on the proper VLAN as shown in the image

upvoted 1 times

felix_simon 5 months, 4 weeks ago

A
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_aaa_override.pdf
On the controller, enable the Allow AAA Override configuration parameter using the GUI or CLI. Enabling this parameter allows the controller to accept the attributes returned by the RADIUS server. The controller then applies these attributes to its clients.

upvoted 1 times

CKL_SG 6 months, 1 week ago

Selected Answer: D

Maybe question answer for d have typo, question seem to be about cisco ise related ise profiling can be use to assign vlan for guest specific

Using ISE Profiling Services to classify devices allows ISE to apply different policies to a non-authenticating endpoint such as a printer or IP phone using MAB, or to apply a different policy to an authenticated employee when connecting using a personal workstation versus a corporate workstation

https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456

upvoted 1 times

bob_135 6 months, 1 week ago

AAA override is on WLC. Radius Profiling is on ISE?

upvoted 1 times

funmax 7 months ago

Selected Answer: A

Please correct.

upvoted 1 times

ClPo 8 months, 3 weeks ago

Selected Answer: A

Please fix

upvoted 1 times

HungarianDish 9 months, 2 weeks ago

Selected Answer: A

I agree. Enable AAA Override... "to apply VLAN tagging to individual clients based on the returned RADIUS attributes from the AAA server."
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_aaa_override.pdf

upvoted 1 times

asiansensation 10 months, 1 week ago

the answer is A

upvoted 1 times

mellohello 10 months, 1 week ago

Selected Answer: A

Enable AAA Override. Correct me if im wrong!

upvoted 3 times

Question #726 *Topic 1*

An engineer must configure an EXEC authorization list that first checks a AAA server then a local username. If both methods fail, the user is denied. Which configuration should be applied?

A. aaa authorization exec default local group radius none

B. aaa authorization exec default group radius local none

C. aaa authorization exec default group radius local

D. aaa authorization exec default local group tacacs+

Correct Answer: *C*

Community vote distribution

C (88%) 13%

darkspawn117 2 months, 2 weeks ago

Selected Answer: C

A. aaa authorization exec default local group radius none
-wrong because it checks local first
B. aaa authorization exec default group radius local none
-WRONG, it checks everything in the correct order, but "none" doesn;t require any
C. aaa authorization exec default group radius local
-CORRECT, the only correct order that only allows what we want
D. aaa authorization exec default local group tacacs+
-WRONG, for same reason as A

upvoted 2 times

CCNPWILL 3 months, 1 week ago

Selected Answer: C

C is correct.

upvoted 2 times

nike01163 3 months, 4 weeks ago

Selected Answer: B

Given answer did not denied when first 2 methods failed.

upvoted 1 times

snarkymark 10 months ago

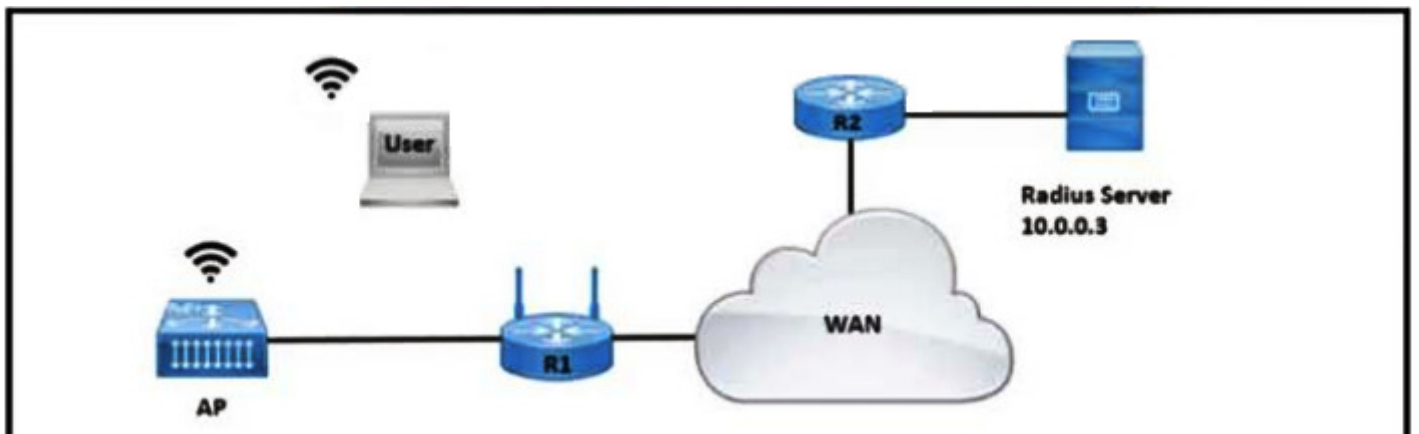
Selected Answer: C

https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html#anc25

upvoted 3 times

Question #727 *Topic 1*

Refer to the exhibit.




```
AP(config)# aaa group server radius rad_auth
AP(config-sg-radius)# server 10.0.0.3 auth-port 1645 acct-port 1646
AP(config)# aaa new-model
AP(config)# aaa authentication login eap_methods group rad_auth
AP(config)# radius-server host 10.0.0.3 auth-port 1645 acct-port 1646 key
labap1200
AP(config)# interface dot11radio 0
AP(config-if)# ssid labap1200
AP(config-if-ssid)# encryption mode wep mandatory
```

A company requires that all wireless users authenticate using dynamic key generation. Which configuration must be applied?

A. AP(config-if-ssid)# authentication open eap eap_methods

B. AP(config-if-ssid)# authentication dynamic open wep_dynamic

C. AP(config-if-ssid)# authentication dynamic wep wep_methods

D. AP(config-if-ssid)# authentication open wep wep_methods

Correct Answer: *D*

Community vote distribution

A (100%)

Clauster Highly Voted 10 months, 1 week ago

Selected Answer: A

After several minutes researching the answer is A. Here's the documentation that clearly states it:
https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html#:~:text=This%20authentication%20type%20provides%20the%20highest%20level%20of,authentication%20and%20derive%20a%20dynamic%20unicast%20WEP%20key.

Also here's answer from other Exams with the same question correct answer

https://exam-files.com/cisco/350-401/implementing%20cisco%20enterprise%20network%20core%20technologies%20%28350-401%20encor%29.certdumps.350-401.2022-03-01.1e.498q.vcex/

MODERATOR PLEASE FIX WHEN POSSIBLE>

upvoted 8 times

PureInertiaCopy 4 months, 3 weeks ago

Chat GPT seems to think it is B

A company requires that all wireless users authenticate using dynamic key generation. Which configuration must be applied?

A. AP(config-if-ssid)# authentication open eap eap_methods
B. AP(config-if-ssid)# authentication dynamic open wep_dynamic
C. AP(config-if-ssid)# authentication dynamic wep wep_methods
D. AP(config-if-ssid)# authentication open wep wep_methods

upvoted 1 times

PureInertiaCopy 4 months, 3 weeks ago

The correct configuration for dynamic key generation in this scenario is:

B. AP(config-if-ssid)# authentication dynamic open wep_dynamic

Explanation:
Dynamic key generation typically involves using a protocol like WEP (Wired Equivalent Privacy) with dynamic keys that are generated and changed frequently. In this context, "authentication dynamic open wep_dynamic" would likely enable dynamic key generation using the WEP protocol.

Option A mentions EAP methods, which are typically used for more advanced and secure authentication methods like WPA/WPA2, not WEP.

Option C is similar to Option A and is not typically used for dynamic key generation.

Option D mentions WEP, but it doesn't specify dynamic key generation, and it's not recommended to use static WEP keys due to security vulnerabilities.

So, the most appropriate option is B: AP(config-if-ssid)# authentication dynamic open wep_dynamic.

upvoted 1 times

PureInertiaCopy 4 months, 3 weeks ago

I apologize for the confusion. If the correct answer is indeed A, let me explain:

A. AP(config-if-ssid)# authentication open eap eap_methods

This configuration suggests using EAP (Extensible Authentication Protocol) for authentication with dynamic key generation. EAP is a more secure and flexible authentication protocol compared to WEP. EAP can be used in conjunction with other security protocols like WPA/WPA2 to provide stronger security for wireless networks.

In this context, "authentication open eap eap_methods" would set up the SSID to use EAP authentication methods with dynamic key generation.

Thank you for providing the correct information, and I appreciate your understanding.

upvoted 1 times

Asombrosso Most Recent 4 months, 1 week ago

Selected Answer: A

authenticate

upvoted 1 times

ihateciscoreally 4 months, 4 weeks ago

more questions not covered in OCG and blueprint! yay!

upvoted 1 times

Colmenarez 5 months, 2 weeks ago

this is NOT an ENCORE exam question

upvoted 2 times

ihateciscoreally 4 months, 4 weeks ago

just remember answer, there is no other way around

upvoted 2 times

rogue_user 6 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/15-3-3/configuration/guide/cg15-3-3/cg15-3-3-chap10-cipherwep.html

There is no such option as "open wep", only "open eap"

upvoted 2 times

asiansensation 10 months, 1 week ago

the answer is A

upvoted 2 times

ImFran 10 months, 1 week ago

When your SSID authentication mechanism uses Extensible Authentication Protocol (EAP) with 802.1x authentication (and without WPA v1 or WPA v2 support), dynamic WEP keys can be generated for each wireless user. Dynamic WEP keys are more secure than static, or unchanging, WEP keys. If an intruder passively receives enough packets encrypted by the same WEP key, the intruder can perform a calculation to learn the key and use it to join your network. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/access_point/15-3-3/configuration/guide/cg15-3-3/cg15-3-3-chap10-cipherwep.html

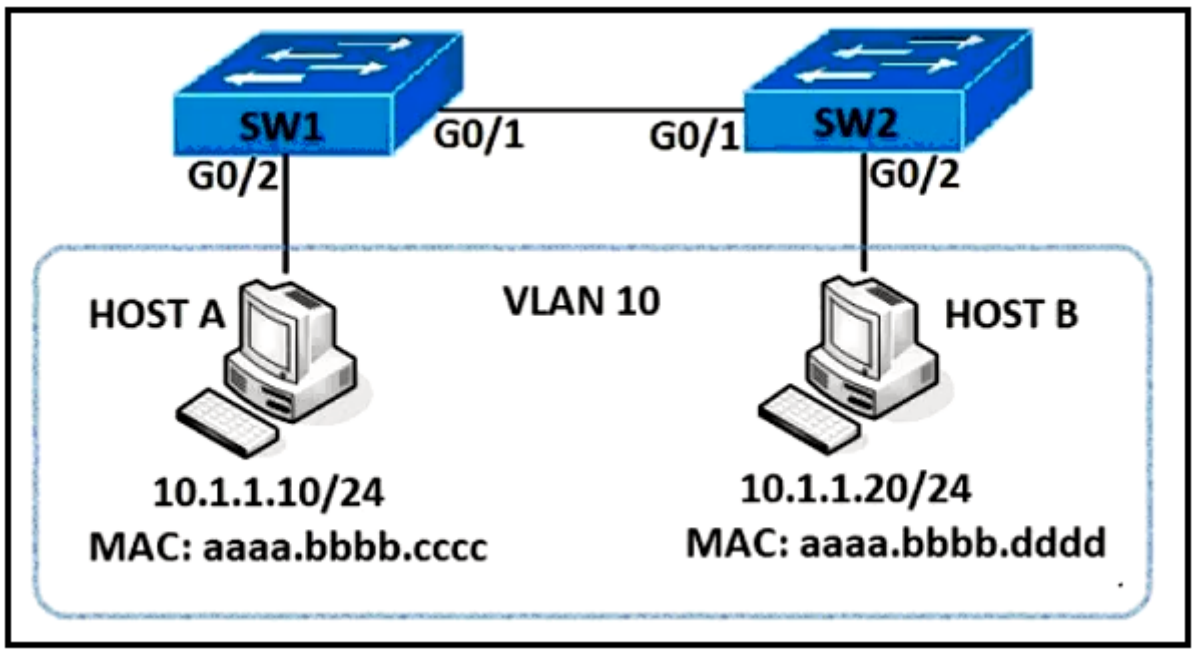
upvoted 3 times

Sa134 10 months, 1 week ago

Selected Answer: A

https://www.cisco.com/c/en/us/support/docs/wireless/aironet-1100-series/44844-leapserver.html

upvoted 3 times



Refer to the exhibit. An engineer must deny HTTP traffic from host A to host B while allowing all other communication between the hosts. Which command set accomplishes this task?

A. SW1(config)# mac access-list extended HOST-A-B
SW1(config-ext-macl)# permit host aaaa.bbbb.cccc aaaa.bbbb.dddd

SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# deny tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# vlan access-map DROP-MAC 10
SW1(config-access-map)# match mac address HOST-A-B
SW1(config-access-map)# action drop
SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop

SW1(config)# vlan filter HOST-A-B vlan 10

B. SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# deny tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# permit ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop
SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)# action forward

SW1(config)# vlan filter HOST-A-B vlan 10

C. SW1(config)# mac access-list extended HOST-A-B
SW1(config-ext-macl)# permit host aaaa.bbbb.cccc aaaa.bbbb.dddd

SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# permit tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# vlan access-map DROP-MAC 10
SW1(config-access-map)# match mac address HOST-A-B
SW1(config-access-map)# action forward

SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop

SW1(config)# vlan filter HOST-A-B vlan 10

Correct Answer: *B*

Community vote distribution

B (100%)

HungarianDish Highly Voted 9 months, 2 weeks ago

Selected Answer: B

MAC Access-Lists is irrelevant here. B seems to be the closest answer, however, it is not right in that form. This should work:

SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# permit tcp host 10.1.1.10 host 10.1.1.20 eq www
SW1(config)# vlan access-map DROP-MAC 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop
SW1(config)# vlan access-map DROP-MAC 20
SW1(config-access-map)# action forward
SW1(config-access-map)# exit
SW1(config)# vlan filter DROP-MAC vlan 10

https://www.networkstraining.com/vlan-access-map-example-configuration/

upvoted 9 times

Clauster 9 months, 2 weeks ago

This is correct

upvoted 1 times

HungarianDish 9 months, 2 weeks ago

Tested in CML, and it worked. MAC access-list is only for L2 (for example arp), ip access-list is for L3, so that is what we need here. Both can be matched under vlan ACL, however, MAC access-list is rarely used in this combination.

upvoted 1 times

MJane Highly Voted 10 months ago

None of the 3 are correct

upvoted 6 times

Asombrosso Most Recent 4 months, 1 week ago

I vote for D, the missing one.

upvoted 1 times

Manvek 5 months, 1 week ago

There seems to be an option missing. So I vote for D, the missing one.
Here you can find the complete question with all answers.
https://www.braindump2go.com/free-online-pdf/350-401-PDF-Dumps(409-433).pdf

upvoted 2 times

edajede 7 months, 1 week ago

I dont like the deny ip access list in option B. It should be permit for both cases and then decided about the drop in the access-map. I think C is correct.

upvoted 2 times

edajede 7 months, 1 week ago

hmm, sorry, the problem in C is, that the mac address communication in the access-map is at the first place, so it will avoid the http check

upvoted 2 times

Question #729 *Topic 1*

A network engineer wants to configure console access to a router without using AAA so that the privileged exec mode is entered directly after a user provides the correct login credentials. Which action achieves this goal?

A. Configure a RADIUS or TACACS+ server and use it to send the privilege level.

B. Configure login authentication privileged on line con 0.

C. Configure privilege level 15 on line con 0.

D. Configure a local username with privilege level 15.

Correct Answer: *B*

Community vote distribution

C (73%) D (27%)

asiansensation Highly Voted 10 months, 1 week ago

Answer is C

upvoted 9 times

HungarianDish Highly Voted 9 months, 3 weeks ago

Selected Answer: C

D only works if "login local" is added under "line con 0". We need to tell the device to use the local user database for authentication. C achieves the goal.

https://www.n-study.com/en/cisco-basic/login-privilege-exec/

upvoted 6 times

Manvek Most Recent 5 months, 1 week ago

Selected Answer: C

C. Using the command "privilege level 15" under line console 0 will guarantee exec privileges as soon as we log in through that port. From there, the authentication can be done either by a username/password combination or just a console password.

upvoted 1 times

Colmenarez 5 months, 2 weeks ago

Selected Answer: D

D is the only way

upvoted 1 times

Colmenarez 5 months, 1 week ago

Im wrong, is C

upvoted 1 times

HarwinderSekhon 6 months, 2 weeks ago

Selected Answer: D

D seems like answer to me. C will assign privilege 15 to all authenticated users (user can be authenticated via AAA as well as local database). Question want you to bypass AAA involvement. Option D is assigning privilege level 15 and creating Local user.

upvoted 1 times

Burik 7 months, 1 week ago

Selected Answer: C

The only way to enter the privileged exec mode right away without using AAA is to use the "privilege level 15" command. In this case the credentials mentioned in the question is just the password you enter under line con 0.

D is wrong because it implies using AAA and the question explicitly says not to.

upvoted 2 times

XDR 8 months, 2 weeks ago

Selected Answer: C

It's C.
Answer D uses AAA

upvoted 4 times

JackDRipper 9 months, 2 weeks ago

Selected Answer: C

It says "without using AAA", so it has to be using the password configured on line con 0, plus the "privilege level 15" command so entering said password would immediately put you on privileged mode.

upvoted 4 times

jackr76 9 months, 3 weeks ago

Selected Answer: C

C C C yes

upvoted 2 times

Clauster 9 months, 3 weeks ago

Selected Answer: D

Answer is D

upvoted 1 times

Jeff555566 9 months, 3 weeks ago

Correct me if I am wrong but it seems to me that both C and D will accomplish this?

upvoted 1 times

Quentin_ 10 months ago

Selected Answer: D

it's D

upvoted 2 times

Badger_27 10 months ago

Selected Answer: D

Surely its D? Create a local user with priveledge 15?

upvoted 2 times

Question #730 *Topic 1*

Refer to the exhibit.

```
for x in range(5):
   print(x)
```

What is output by this code?

A. 0 5

B. 0 1 2 3 4 5

C. 0 1 2 3 4

D. (0,5)

Correct Answer: *C*

Community vote distribution

C (100%)

sergiosolotrabajo 4 weeks ago

Guys this is for you, hope it is useful for your Encor exam:

a = 1
b = 1

print(a+b)

What is the print result? xD

upvoted 1 times

Nathan_ 6 months, 3 weeks ago

Answer is C:
for x in range(5) :
print (x)

for testing python scrips on output you can check this link https://www.programiz.com/python-programming/online-compiler/

upvoted 1 times

snarkymark 10 months ago

Selected Answer: C

https://www.learnpython.org/en/Loops

upvoted 3 times

Question #731 *Topic 1*

What is one benefit of implementing a data modeling language?

A. use XML style of data formatting

B. interoperability to allow unlimited implementations

C. machine-oriented logic and language-facilitated processing

D. conceptual representation makes interpretation simple

Correct Answer: *C*

Community vote distribution

D (100%)

Nickplayany Highly Voted 9 months, 3 weeks ago

Selected Answer: D

I found the answer also to a not so network page! Check this out: https://www.indeed.com/career-advice/career-development/data-modeling

D: Data modeling allows you to conceptually represent the data and the association between data objects and rules.

upvoted 5 times

Asombrosso Most Recent 4 months, 1 week ago

Selected Answer: D

Data modeling concepts are rendered as easy-to-read visual representations, such as simple graphs, that label data types and the relationships between them using jargon-free, real-world terms such as customers, suppliers, vendors, and products

upvoted 1 times

mellohello 8 months, 2 weeks ago

Selected Answer: D

I will choose D

upvoted 1 times

Shansab 9 months, 2 weeks ago

Selected Answer: D

D is the correct Answer.

upvoted 1 times

snarkymark 10 months ago

Selected Answer: D

https://powerbi.microsoft.com/en-us/what-are-the-advantages-of-data-modeling-tools/

upvoted 3 times

asiansensation 10 months, 1 week ago

the answer is D

upvoted 1 times

Question #732 *Topic 1*

Refer to the exhibit.

```
from ncclient import manager

with manager.connect(host=host,port=830,username=user,hostkey_verify=False) as m:
  c = m.get_config(source='running').data_xml
  with open("%s.xml" % host,'w') as f:
    f.write(c)
```

What is generated by the script?

A. the router processes

B. the cdp neighbors

C. the routing table

D. the running configuration

Correct Answer: *D*

Community vote distribution

D (100%)

snarkymark Highly Voted 10 months ago

Selected Answer: D

https://github.com/ncclient/ncclient

upvoted 5 times

Question #733 *Topic 1*

What is a benefit of YANG modules?

A. tightly coupled models with encoding to improve performance

B. easier multivendor interoperability provided by common or industry models

C. avoidance of ecosystem fragmentation by having fixed modules that cannot be changed

D. single protocol and model coupling to simplify maintenance and support

Correct Answer: *B*

Community vote distribution

B (100%)

AdamoNetworko 20 hours, 44 minutes ago

B. Easier multivendor interoperability provided by common or industry models stands out as a significant benefit of YANG modules.

They facilitate interoperability between devices from different vendors by providing standardized and commonly accepted data models.

upvoted 1 times

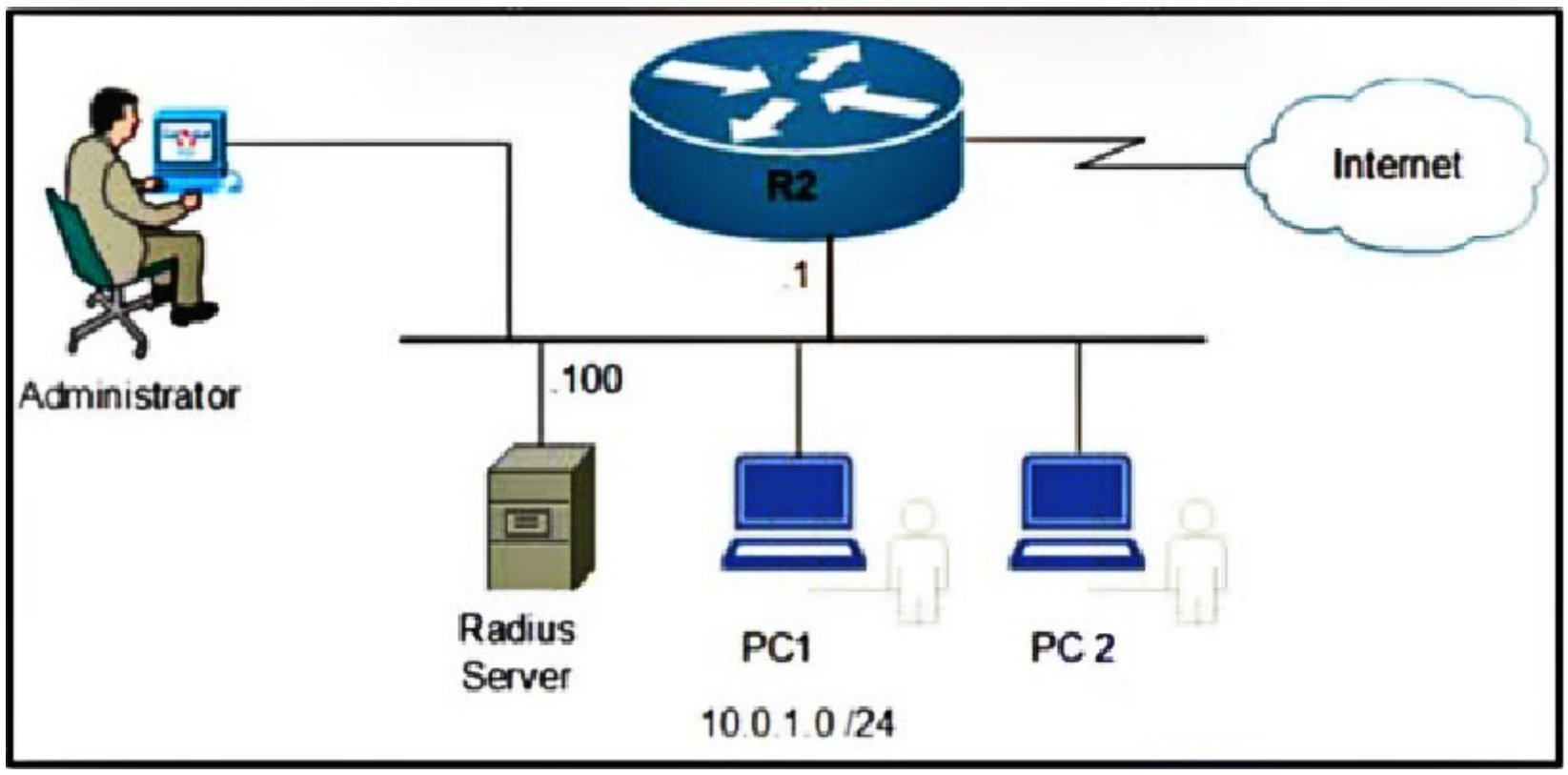
snarkymark 10 months ago

Selected Answer: B

https://blog.aviatnetworks.com/whats-the-big-deal-about-netconf-yang/

upvoted 3 times

Refer to the exhibit.



An engineer must save the configuration of router R2 using the NETCONF protocol. Which script must be used?

A.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
  <cisco-ia:save-config xmlns:cisco-ia="http://cisco.com/yang/cisco-ia"/>
</rpc>
```

B.

```
<?xml version="1.0" encoding="utf-8"?>
 <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
  <get>
   <filter type="subtree">
    <ncm:netconf-state xmlns:ncm="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">
     <ncm:capabilities/>
    </ncm:netconf-state>
   </filter>
  </get>
 </rpc>
```

C.

```
<?xml version="1.0" encoding="utf-8"?>
 <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
    <cisco-ia:sync-from xmlns:cisco-ia="http://cisco.com/yang/cisco-ia"></cisco-ia:sync-from>
 </rpc>
```

D.

```
<?xml version="1.0" encoding="utf-8"?>
 <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
    <cisco-ia:reset xmlns:cisco-ia="http://cisco.com/yang/cisco-ia">
    <cisco-ia:reinitialize>true</cisco-ia:reinitialize>
  </cisco-ia:reset>
 </rpc>
```

Correct Answer: *A*

Community vote distribution

A (100%)

snarkymark Highly Voted 10 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/support/docs/storage-networking/management/200933-YANG-NETCONF-Configuration-Validation.html

upvoted 5 times

Badger_27 Highly Voted 10 months, 1 week ago

Think its A is its the only command that's specifying the config.

upvoted 5 times

due Most Recent 4 months, 2 weeks ago

Selected Answer: A

cisco-ia:save-config: Saves the current device configuration.
cisco-ia:reset: Reverts the configuration to a baseline or initial state.
cisco-ia:sync-from: Synchronizes the device configuration with a reference source.

upvoted 2 times

HarwinderSekhon 6 months, 2 weeks ago

GPT - <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
<cisco-ia:save-config xmlns:cisco-ia="http://cisco.com/yang/cisco-ia"/>
</rpc>

upvoted 1 times

Question #735 *Topic 1*

Which language defines the structure or modeling of data for NETCONF and RESTCONF?

A. YAML

B. XML

C. JSON

D. YANG

Correct Answer: *C*

Community vote distribution

D (100%)

Symirnian Highly Voted 10 months, 1 week ago

YANG in my opinion...

upvoted 7 times

Asombrosso Most Recent 4 months, 1 week ago

Selected Answer: D

The YANG data modeling language (comes with a number of built-in data types), being protocol independent, can then be converted into any encoding format, e.g. XML or JSON.

upvoted 1 times

ClPo 8 months, 3 weeks ago

Selected Answer: D

I wonder how the 'experts' have suggested C here.

upvoted 1 times

Shansab 9 months, 2 weeks ago

Selected Answer: D

YANG is correct.

upvoted 2 times

Symirnian 9 months, 3 weeks ago

In CBTNUGGETS there is an phrase; (So the answer might be XML too?)
-While NETCONF uses XML encoding only, RESTCONF supports both JSON and XML
https://www.cbtnuggets.com/blog/certifications/cisco/ccnp-enterprise-what-are-yang-netconf-restconf

upvoted 1 times

massimp 6 months, 4 weeks ago

if you read carefully it ask for the "language that defines the structure or modeling of NETCONF" that is not XML, but YANG. Its' not asking about language encoding.

habibmangal 9 months, 4 weeks ago

Selected Answer: D

https://study-ccna.com/model-driven-programmability-netconf-restconf/

upvoted 1 times

snarkymark 10 months ago

Selected Answer: D

https://info.support.huawei.com/info-finder/encyclopedia/en/YANG.html

upvoted 1 times

Clauster 10 months ago

Selected Answer: D

Answer is D

upvoted 2 times

Clauster 10 months, 1 week ago

Selected Answer: D

The Answer is D
https://developer.cisco.com/docs/nso/guides/#!the-yang-data-modeling-language/the-yang-data-modeling-language

upvoted 2 times

AhcMez 10 months, 1 week ago

Selected Answer: D

correct is D

upvoted 2 times

Refer to the exhibit.

```
def main():
    print("The answer is " + str(magic(5)))

def magic(num):
    try:
        answer = num + 2 * 10
    except:
        answer = 100
    return answer

main()
```

What is displayed when the code is run?

A. The answer is 100

B. The answer is 5

C. The answer is 25

D. The answer is 70

Correct Answer: *A*

Community vote distribution

C (100%)

kmb192006 Highly Voted 8 months, 3 weeks ago

Selected Answer: C

If num is not a number then the method will throw out exception then the answer will be 100, for example putting a character "a" in to method - magic("a")

But the main() method has statically defined the num as 5 - magic(5), which will never throw out an exception. answer should always be num + 2 * 10, which is 25 in this program

So the answer is C

upvoted 9 times

Leoveil 6 months, 3 weeks ago

good explanation thanks

upvoted 3 times

Tadese Most Recent 2 weeks, 5 days ago

Selected Answer: C

def main():
print("The answer is" +str(magic(5)))
def magic(num):
try:
answer=num+2*10
except:
answer=100
return answer
main()
Output is 25

upvoted 1 times

Entivo 6 months, 3 weeks ago

Selected Answer: C

It is C - I just tried it at programiz.com

It adds the number (in this case, 5) to the calculated value of 2*10 (which is 20), hence 25.
upvoted 1 times

net_eng10021 7 months, 3 weeks ago
C

```
def main():
print(str(magic(5)))
def magic(num):
try:
answer = num+2*10
except:
answer = 100

return answer

main()
```
upvoted 1 times

net_eng10021 7 months, 3 weeks ago
Ran the above code and it does return 25
upvoted 1 times

Farida_Fathi 8 months, 3 weeks ago
Selected Answer: C
Selected Answer: C
upvoted 1 times

Rman0059 9 months, 2 weeks ago
Selected Answer: C
choose C
upvoted 1 times

RayZheng 9 months, 3 weeks ago
Selected Answer: C
The answer should be C
upvoted 1 times

Nickplayany 10 months, 1 week ago
Selected Answer: C
answer = num + 2 * 10
5 + 20
upvoted 2 times

makarov_vg 10 months, 1 week ago
Answer C
https://www.programiz.com/python-programming/online-compiler/

```
def main():
print (str(magic(5)))
def magic(num):
try:
answer = num + 2 * 10
except:
answer = 100
return answer

main()
```
upvoted 2 times

XDR 8 months, 2 weeks ago
Yes. The input could be a string.
upvoted 1 times

Symirnian 10 months, 1 week ago
Answer is 25, why is there an exception here otherwise?
upvoted 1 times

XDR 8 months, 2 weeks ago
Yes. The input could be a string.
upvoted 1 times

Question #737 *Topic 1*

What is the purpose of an integration API in Cisco DNA Center?

A. Obtain information about clients, sites, and topology from Cisco DNA Center.

B. Enable external systems to take actions in response to an event.

C. Allow the platform into approval chains in ITSM.

D. Enable discovery and control of the network by using HTTPS verbs.

Correct Answer: *B*

Community vote distribution

C (77%) B (23%)

HungarianDish Highly Voted 9 months, 2 weeks ago

Selected Answer: C

https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/integration-api-westbound

upvoted 5 times

Symirnian Highly Voted 9 months, 3 weeks ago

Selected Answer: B

B is also covering C but more general. C is more specific. I prefer B

upvoted 5 times

XDR 8 months, 2 weeks ago

Me too

upvoted 2 times

NikosTsironis Most Recent 4 weeks ago

Selected Answer: C

https://developer.cisco.com/docs/dna-center/#!overview/integration-api-westbound

If you are using an ITSM system that supports this reference architecture, then the Cisco DNA Center platform can integrate with your system.

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: C

Integration API (Westbound)
Integration capabilities are part of Westbound interfaces. To meet the need to scale and accelerate operations in modern data centers, IT operators require intelligent, end-to-end work flows built with open APIs. The Cisco DNA Center platform provides mechanisms for integrating Cisco DNA Assurance workflows and data with third-party IT Service Management (ITSM) solutions.

upvoted 2 times

PureInertiaCopy 4 months, 3 weeks ago

Chat GPT:

What is the purpose of an integration API in Cisco DNA Center?

A. Obtain information about clients, sites, and topology from Cisco DNA Center.
B. Enable external systems to take actions in response to an event.
C. Allow the platform into approval chains in ITSM.
D. Enable discovery and control of the network by using HTTPS verbs.

upvoted 1 times

PureInertiaCopy 4 months, 3 weeks ago

The purpose of an integration API in Cisco DNA Center is:

B. Enable external systems to take actions in response to an event.

Integration APIs in Cisco DNA Center allow external systems to interact with and integrate with the DNA Center platform. They enable external applications, tools, or systems to programmatically access and control various aspects of network management, configuration, and monitoring within the Cisco DNA Center environment. These APIs facilitate automation, orchestration, and integration with other IT tools and systems.

While the other options (A, C, and D) may have relevance to Cisco DNA Center's capabilities, the primary purpose of integration APIs is to enable external systems to take actions and interact with Cisco DNA Center in response to events and requirements.

upvoted 1 times

HarwinderSekhon 6 months, 2 weeks ago

Selected Answer: C

A - Northbound API
B- East Bound API
C- WestBound
D- SouthBound
C is answer

upvoted 2 times

Splashisthegreatestmovie 7 months ago

I really think it's B. C describes a specific action while B defines the function

upvoted 1 times

Jack2002 9 months ago

Selected Answer: C

C is correct, it is part of integration API in DNA Center westbound

upvoted 3 times

Rman0059 9 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 2 times

Nickplayany 9 months, 3 weeks ago

Selected Answer: C

C is correct

https://developer.cisco.com/dnacenter/integrationapis/

upvoted 1 times

asiansensation 9 months, 3 weeks ago

C is the answer

upvoted 1 times

snarkymark 10 months ago

Selected Answer: C

Inof in link provided by ImFran

upvoted 1 times

HungarianDish 9 months, 3 weeks ago

I read the document, and I agree.

upvoted 1 times

ImFran 10 months, 1 week ago

https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/integration-api-westbound

upvoted 2 times

Question #738 *Topic 1*

Refer to the exhibit.

```
list = [1, 2, 3, 4]
list[3] = 10
print(list)
```

What is the value of the variable list after the code is run?

A. [1, 2, 10]

B. [1, 2, 3, 10]

C. [1, 2, 10, 4]

D. [1, 10,10,10]

Correct Answer: *C*

Community vote distribution

Vlad_Is_Love_ua Highly Voted 10 months ago

Selected Answer: B

After the code is run, the value of the variable list will be [1, 2, 3, 10].

The code creates a list containing the values [1, 2, 3, 4]. Then, it modifies the fourth element of the list (which has an index of 3, since Python uses 0-indexing) by setting it equal to 10 using the assignment operator (=). Finally, it prints the resulting list using the print() function.

So, the output of the print statement will be [1, 2, 3, 10], indicating that the fourth element of the list has been successfully modified.

upvoted 13 times

makarov_vg Highly Voted 10 months, 1 week ago

https://www.programiz.com/python-programming/online-compiler/
list = [1, 2, 3, 4]
list[3] = 10
print(list)

Answer B

upvoted 8 times

bullett00th 9 months, 3 weeks ago

Anser B
Thanks for the Link. The result is [1, 2, 3, 10]

upvoted 1 times

rsmachado 10 months, 1 week ago

Thanks for the link. It clearly gives the right answer which is B.

upvoted 1 times

Tadese Most Recent 2 weeks ago

Selected Answer: B

Test on python
list = [1, 2, 3, 4]

list[3] = 10

print(list)

[1, 2, 3, 10]

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: B

starts fr. 0

upvoted 1 times

Wissammawas 6 months ago

Selected Answer: B

Answer B

upvoted 1 times

net_eng10021 7 months, 3 weeks ago

B is answer...

pytcharm python console output...

list=[1,2,3,4]
list[3]=10
print(list)
[1, 2, 3, 10]

upvoted 1 times

ClPo 8 months, 3 weeks ago

Selected Answer: B

Even if an expert doesn't know python, running the code will show that it's B. Python list index starts at 0.

upvoted 1 times

Shansab 9 months, 2 weeks ago

Selected Answer: B

B. [1, 2, 3, 10] is correct.

upvoted 1 times

rsmachado 10 months, 1 week ago

Selected Answer: B

Answer B

upvoted 1 times

Nickplayany 10 months, 1 week ago

Selected Answer: B

1,2,3,10

upvoted 1 times

Symirnian 10 months, 1 week ago

B. [1, 2, 3, 10] I think.

upvoted 3 times

Question #739 *Topic 1*

What is one difference between SaltStack and Ansible?

A. SaltStack uses the Ansible agent on the box, whereas Ansible uses a Telnet server on the box.

B. SaltStack uses an API proxy agent to program Cisco boxes in agent mode, whereas Ansible uses a Telnet connection.

C. SaltStack uses SSH to interact with Cisco devices, whereas Ansible uses an event bus.

D. SaltStack is agent based, whereas Ansible is agentless.

Correct Answer: *C*

Community vote distribution

D (100%)

jackr76 Highly Voted 9 months, 3 weeks ago

Selected Answer: D

I pay for GOOD information

upvoted 5 times

Asombrosso Most Recent 4 months, 1 week ago

Selected Answer: D

only Ansible is agentless

upvoted 1 times

ClPo 8 months, 3 weeks ago

Selected Answer: D

As usual: trust the discussion, not the experts. This site would already improve a lot if there was a link from question to discussion.

upvoted 3 times

nikramor 9 months, 1 week ago

Selected Answer: D

The answer is D

upvoted 2 times

Dataset 9 months, 2 weeks ago

The answer is D
Regards

upvoted 1 times

bullett00th 9 months, 3 weeks ago

Selected Answer: D

ADMIN - Fix this. Why so many wrong answers here?

upvoted 4 times

RocketS17 9 months, 3 weeks ago

Selected Answer: D

Ansible is agentless and uses SSH.

upvoted 2 times

snarkymark 10 months ago

Selected Answer: D

https://phoenixnap.com/kb/saltstack-vs-ansible

upvoted 3 times

Nickplayany 10 months, 1 week ago

Selected Answer: D

Read Question #379 if you want.

It´s D the correct answer

upvoted 1 times

mellohello 10 months, 1 week ago

Selected Answer: D

D is the correct answer.

upvoted 3 times

Question #740 *Topic 1*

Which signal strength and noise values meet the minimum SNR for voice networks?

A. signal strength -66 dBm, noise 90 dBm

B. signal strength -67 dBm, noise 91 dBm

C. signal strength -68 dBm, noise 89 dBm

D. signal strength -69 dBm, noise 94 dBm

Correct Answer: *B*

Community vote distribution

D (100%)

Nickplayany Highly Voted 9 months, 4 weeks ago

Selected Answer: D

The correct is D

Check below:

Generally, a signal with an SNR value of 20 dB or more is recommended for data networks where as an SNR value of 25 dB or more is recommended for networks that use voice applications.

A. signal strength -66 dBm, noise 90 dBm=24dB
B. signal strength -67 dBm, noise 91 dBm=24dB
C. signal strength -68 dBm, noise 89 dBm=21dB
D. signal strength -69 dBm, noise 94 dBm=25dB <- Correct

upvoted 12 times

bullett00th 9 months, 3 weeks ago

Totally agree - min. 25dB - I choose also D

upvoted 3 times

eearmani Most Recent 1 month ago

The minimum recommended wireless signal strength for voice applications is -67 dBm and the minimum SNR is 25 dB.

upvoted 1 times

Vadkorte 4 months ago

None of these choices are correct -
"The minimum recommended wireless signal strength for voice applications is -67 dBm and the minimum SNR is 25 dB."
https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html

upvoted 2 times

Asombrosso 4 months, 1 week ago

Selected Answer: D

actually, none of the answers are correctly represented

upvoted 2 times

HarwinderSekhon 6 months, 2 weeks ago

-25 For Voice
-20 for anything else.

upvoted 2 times

Burik 7 months ago

Selected Answer: D

None of the answers are correct, they should be as follows:

A. signal strength -66 dBm, noise -90 dBm
B. signal strength -67 dBm, noise -91 dBm
C. signal strength -68 dBm, noise -89 dBm
D. signal strength -69 dBm, noise -94 dBm

Even if fixed, the answer is D and not B, as -69 -(-94) = 25 which is the recommended SNR for voice applications.

upvoted 3 times

RamazanLokov 7 months, 2 weeks ago

wrong answers, minus forgotten for noise value

upvoted 2 times

felix_simon 8 months, 1 week ago

B
https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html
"The minimum recommended wireless signal strength for voice applications is -67 dBm and the minimum SNR is 25 dB."

upvoted 1 times

danman32 6 months, 3 weeks ago

I just re-read the question. They're only interested in the SNR meeting minimum requirement, so answer is definitely D as it is the only answer that meets the minimum SNR, even if it doesn't meet industry signal strength requirement

upvoted 1 times

danman32 6 months, 3 weeks ago

B fits the signal strength requirement, but not the SNR requirement.
SNR for B is 24 (-91-(-67)) = 24
So really none of the answers fit.
A & B fit the minimum strength requirement
But only D fits the SNR minimum requirement but not the strength requirement.

upvoted 2 times

Humb13g0d 9 months, 3 weeks ago

Selected Answer: D

D is the correct answer.

upvoted 1 times

DavideDL 10 months ago

Selected Answer: D

Generally, a signal with an SNR value of 20 dB or more is recommended for data networks where as an SNR value of 25 dB or more is recommended for networks that use voice applications

https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength#:~:text=Generally%2C%20a%20signal%20with%20an,networks%20that%20use%20voice%20applications.

upvoted 2 times

snarkymark 10 months ago

Selected Answer: D

Believe correct answer is D, 25

upvoted 2 times

Question #741 *Topic 1*

A customer requires their wireless network to be fully functional, even if the wireless controller fails. Which wireless design supports these requirements?

A. FlexConnect

B. mesh

C. centralized

D. embedded

Correct Answer: *A*

Community vote distribution

A (100%)

snarkymark Highly Voted 10 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html

upvoted 5 times

due Most Recent 4 months, 2 weeks ago

Selected Answer: A

FlexConnect: Provides local functionality even without the central controller with local mode and for remote or branch office deployments.
Mesh: Creates a wireless backhaul network using access points as relays.
Centralized: Access points rely heavily on a central controller for management and data forwarding.
Embedded: Access points have built-in controller functionality to enhance resiliency.

upvoted 3 times

Question #742 *Topic 1*

Which two conditions occur when the primary route processor fails on a switch that is using dual route processors with stateful switchover? (Choose two.)

A. Data forwarding can continue along known paths until routing protocol information is restored.

B. Data forwarding is stopped until the routing protocols reconverge after the switchover.

C. The standby route processor is fully initialized and state information is maintained.

D. User sessions are immediately recreated on the new active route processor.

E. The standby route processor initialization is started when the primary router processor fails.

Correct Answer: *AC*

Community vote distribution

AC (80%) 10% 10%

sam6996 5 months, 3 weeks ago

Selected Answer: AC

A and C
from the 2nd edition OCG under SSO and NFS section, "During a switchover, the standby RP takes over as the new active RP. The new active RP uses the SSO learnt checkpoint information and keeps the interfaces on the router from flapping and the router and/or line cards from reloading, however, SSO doesn't checkpoint any Layer 3 control plane information about any neighbor router, and due to this, the existing routing protocol adjacencies go down and begin to reestablish. During this time, since the FIB was checkpointed by NSF, the data plane is not affected by the Layer 3 control plane going down and traffic continues to be forwarded while the routing protocol adjacencies reestablish. After routing convergence is complete, the FIB is updated with new routing or topology information from the RIB if necessary."

upvoted 3 times

sam6996 5 months, 3 weeks ago

also it states "SSO/NSF is not a configurable feature; it is enabled by default when SSO is enabled, this means that any NSF command or keyword found in the documentation or the command line, is referring to Graceful Restart." meaning when you enable SSO you also enable NSF is what it seems. so I go with AC

upvoted 1 times

CHERIFNDIAYE 7 months, 1 week ago

Selected Answer: AC

Correct answer is AC

upvoted 2 times

siyamak 7 months, 1 week ago

Selected Answer: BC

BC is the right answer

upvoted 1 times

kmb192006 8 months, 3 weeks ago

I am doubting the answer should be AC or BC...

A requires NSF which cannot be simply done with SSO. Without NSF the CEF entries are purged and routing table is cleared. Routing protocols need time to relearn and rebuild routing table on the standby processor, which B seems describing more precisely.

E is not correct because processor initialization is done when activating SSO, the bulk synchronization initializes standby processor. After SSO startup completes there will be only regular checkpoints to perform increment synchronization to standby processor.

Any thought?

upvoted 1 times

danman32 6 months, 3 weeks ago

Question didn't mention SSO or NSF, only that the sync is stateful, which to me would imply NSF is in play.

upvoted 1 times

Based_Engineer 6 months, 1 week ago

Stateful switchover = SSO

upvoted 2 times

dragonwise 9 months, 1 week ago

Selected Answer: CE

C is correct because the standby route processor is fully initialized and maintains the state information of the system. This ensures that there is no loss of state information during the switchover process, and the system continues to function normally without interruption.

E is correct because the initialization of the standby route processor begins as soon as the primary route processor fails. This ensures that the standby route processor is fully operational and can take over the duties of the primary route processor seamlessly.

upvoted 1 times

danman32 6 months, 3 weeks ago

E can't be right because if the standby initializes, it could not be stateful. It would be starting from scratch.

upvoted 1 times

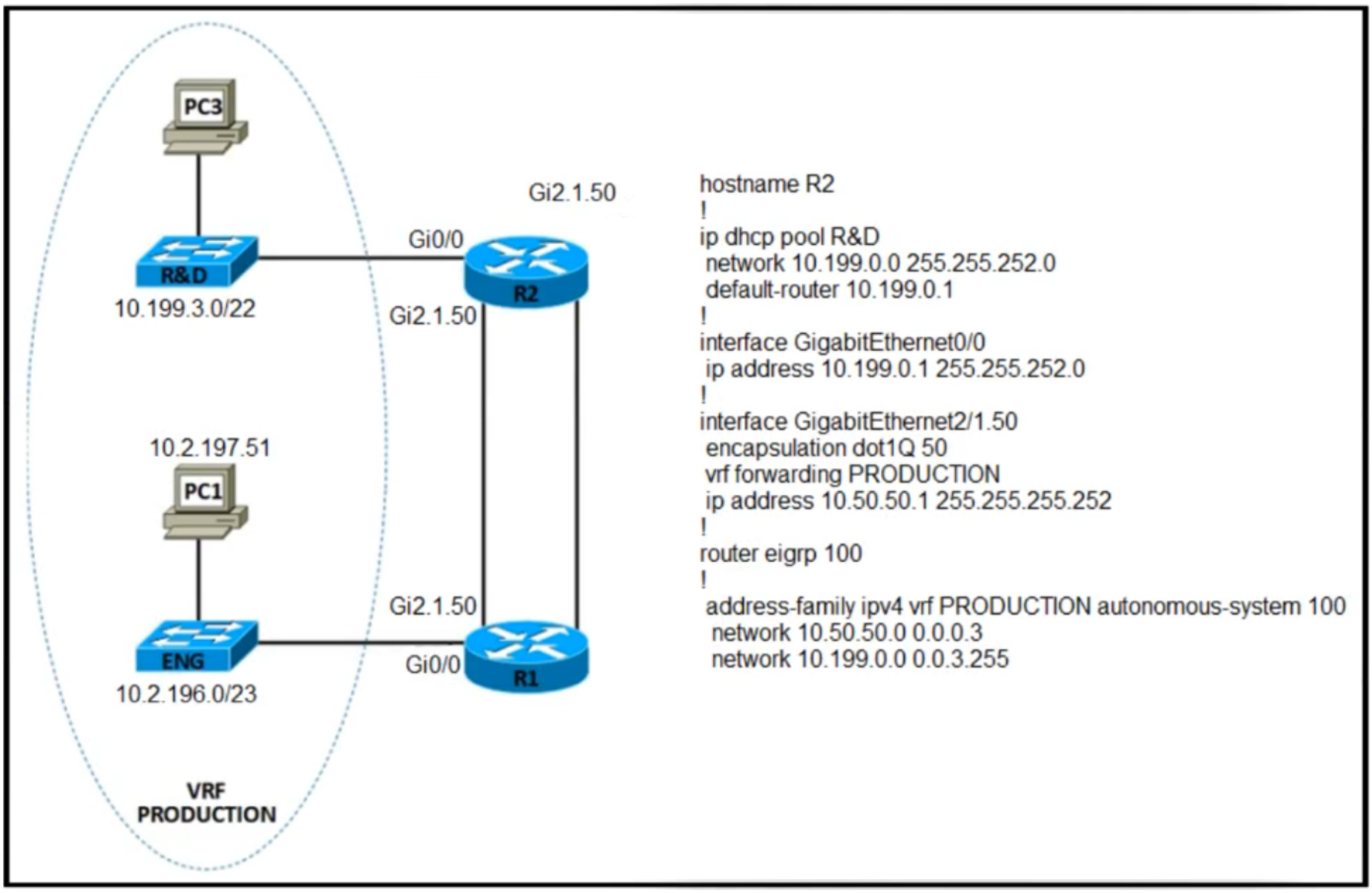
snarkymark 10 months ago

Selected Answer: AC

https://content.cisco.com/chapter.sjs?uri=%2Fsearchable%2Fchapter%2Fwww.cisco.com%2Fcontent%2Fen%2Fus%2Ftd%2Fdocs%2Fswitches%2Flan%2Fcatalyst6500%2Fios%2F15-4SY%2Fconfig_guide%2Fsup2T%2F15_4_sy_swcg_2T%2Fstateful_switchover.html.xml#56839

upvoted 3 times

Refer to the exhibit.



Which configuration must be added to R2 to enable PC3 to obtain a DHCP address and successfully ping PC1?

A. Router(config)# vrf definition PRODUCTION
Router(config-vrf)# address-family ipv4

Router(config)# interface GigabitEthernet 0/0
Router(config-if)# vrf forwarding PRODUCTION
Router(config-if)# ip address 10.199.0.1 255.255.252.0

Router(config)# ip dhcp pool R&D
Router(dhcp-config)# vrf PRODUCTION

B. Router(config)# vrf definition PRODUCTION

Router(config-vrf)# rd 1:100 -

Router(config)# router eigrp 100
Router(config-rtr)# redistribute vrf PRODUCTION

C. Router(config)# vrf definition PRODUCTION
Router(config-vrf)# vnet tag 100

Router(config)# interface GigabitEthernet 0/0

Router(config-if)# vnet trunk -

D. Router(config)# vrf definition PRODUCTION

Router(config-vrf)# rd 1:100 -
Router(config-vrf)# address-family ipv4

Router(config)# router eigrp 100
Router(config-rtr)# route-target export 1:100

Correct Answer: *A*

Community vote distribution

A (100%)

HarwinderSekhon 6 months, 2 weeks ago

currently gi0/0 is not part of VRF.
A does that.

upvoted 2 times

HungarianDish 9 months, 3 weeks ago

Selected Answer: A

https://community.cisco.com/t5/routing/dhcp-pool-and-vrf/td-p/4487651

upvoted 2 times

Symirnian 9 months, 3 weeks ago

Selected Answer: A

A is reasonable

upvoted 2 times

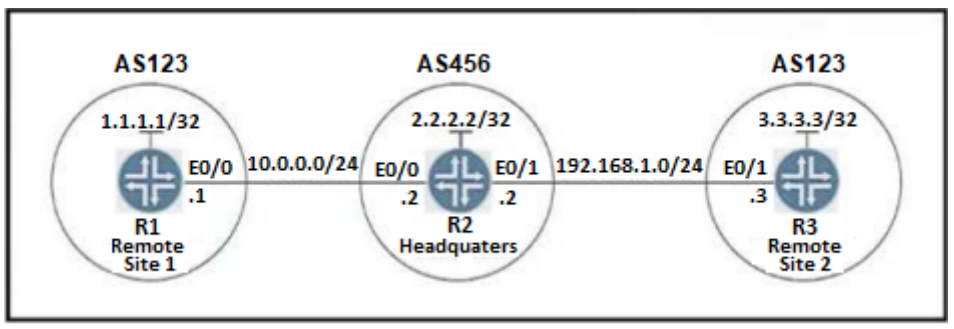
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

Topology
-

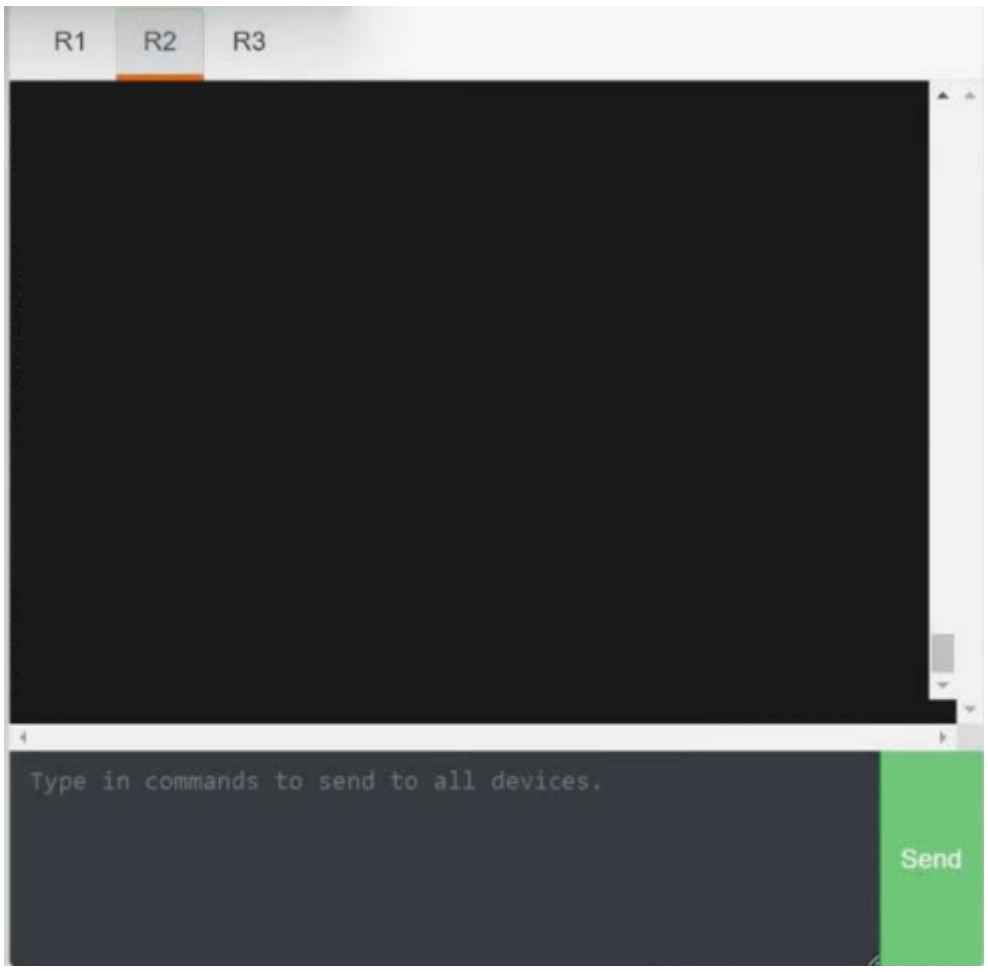


Tasks
-

BGP connectivity exists between Headquarters and both remote sites, however Remote Site 1 cannot communicate with Remote Site 2. Configure BGP according to the topology to achieve these goals:

1. Configure R2 under the BGP process to provide reachability between Remote Site 1 and Remote Site 2. No configuration changes are permitted on R1 or R3.

2. Ensure that the /32 networks at Remote Site 1 and Remote Site 2 can ping each other.



Correct Answer:

R2

Router BGP 456
Network 10.0.0.0 255.255.255.0
Network 192.168.1.0 255.255.255.0
Network 2.2.2.2 255.255.255.255
Neighbor 10.0.0.1 remote-as 123
Neighbor 192.168.1.3 remote-as 123
Neighbor 10.0.0.1 as-override
Neighbor 192.168.1.3 as-override

kleno Highly Voted 5 months, 1 week ago

the same today, please consider thet as-override (for R2 config) also available only under router bgp ### > address-family ipv4 configuration mode

upvoted 5 times

sledgey121 Most Recent 2 weeks, 1 day ago

If the question said configure R1 and R3 then allowas-in would be correct. Because the question says configure 'only' R2, as-override in the correct answer.

upvoted 1 times

b7c04a1 1 month, 1 week ago

I did this lab and the provider's answer is correct. It can use "redistribute connected" instead "network command" in bgp also.

R2#show run | sec router.bgp
router bgp 456
bgp log-neighbor-changes
redistribute connected
neighbor 10.0.0.1 remote-as 123
neighbor 10.0.0.1 as-override
neighbor 192.168.1.3 remote-as 123
neighbor 192.168.1.3 as-override

R1#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R3#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
upvoted 3 times

sergiosolotrabajo 1 day, 19 hours ago
redistribute connected is a dangerous command if not secured other way, careful
upvoted 1 times

Din04 1 month, 1 week ago
I haven't used allowas-in and as-override in production. I read documents about this command, but are these necessary on this lab?
upvoted 1 times

sergiosolotrabajo 2 months, 3 weeks ago
Guys just saying, I did the exam yesterday and Cisco changed all simulations with the new ENCOR v1.1. Neither 744, 745, 746, 747, 751, 752, 754, 773, 798 or 801. I recommend you to wait till ExamTopics people has uploaded the new ones. Just not fair, from v1.0 to v1.1 changing the whole exam, thanks Cisco.
upvoted 4 times

Wazerface 1 week, 1 day ago
I passed the updated exam less than 2 weeks ago.
And as Din04 said it most of the Simulations here are not in the current exam. (Well i did not get any of them but one)
Out of the 4 simulations that I had to complete i only got the GRE + Ipsec simulation.
This material is great if you want to find and work on your weakness but dont expect to have the exact same questions.
upvoted 1 times

Wazerface 1 week, 1 day ago
I meant sergiosolotrabajo
upvoted 1 times

Evreni 2 months, 3 weeks ago
did you pass it
upvoted 2 times

connorm 3 months, 3 weeks ago
R2 config question, Lab in EVE NG - below works
R2#show run | sec router
router bgp 456
bgp log-neighbor-changes
neighbor 10.0.0.1 remote-as 123
neighbor 192.168.1.1 remote-as 123
!
address-family ipv4
network 1.1.1.1 mask 255.255.255.255
network 2.2.2.2 mask 255.255.255.255
network 3.3.3.3 mask 255.255.255.255
neighbor 10.0.0.1 activate
neighbor 10.0.0.1 as-override
neighbor 192.168.1.1 activate
neighbor 192.168.1.1 as-override
exit-address-family

can ping /32 from both R1 / R3
upvoted 2 times

[Removed] 6 months ago
I got the lab to configure R1 and R3
The solution was to configure "allowas-in" under the router bgp ### > address-family ipv4 configuration mode
upvoted 3 times

[Removed] 6 months ago
It took me a while to find the command, but luckily, this one was one of the few commands that cisco has a proper description for.
upvoted 2 times

Wissammawas 6 months ago
can you please write the whole Answer for R1 and R3? (the all Command, which you wrote in the exam)
upvoted 1 times

123robinsong 5 months, 4 weeks ago
I did it on GNS3 with the allowas-in and it worked. not sure if this is what the simulation iteem is asking for tho.
R1#
router bgp 123
neighbor 10.0.0.2 remote-as 456
address-family ipv4
network 1.1.1.1 mask 255.255.255.255
network 10.0.0.0 mask 255.255.255.0
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 allowas-in

R3#

router bgp 123
neighbor 192.168.1.2 remote-as 456
address-family ipv4
network 3.3.3.3 mask 255.255.255.255
network 192.168.1.0
neighbor 192.168.1.2 activate
neighbor 192.168.1.2 allowas-in

upvoted 6 times

teikitiz 5 months, 4 weeks ago

Please note that this is for the case of R1 and R3 to be configured. It's not the required answer to this lab. Here's for R1, R3 is similar.
R1#sh run | sect bgp
router bgp 123
bgp log-neighbor-changes
neighbor 10.0.0.2 remote-as 456
!
address-family ipv4
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 allowas-in
no auto-summary
no synchronization
network 1.1.1.1 mask 255.255.255.255
exit-address-family
R1#

upvoted 3 times

teikitiz 5 months, 4 weeks ago

Only noticed tempaccount00001's reply now, below.

upvoted 1 times

SHONA1 3 months, 3 weeks ago

Same I had that LAB, like you mentioned I had to use the # address-family ipv4. Thanks for the heads up mate.

upvoted 1 times

edajede 6 months, 1 week ago

Very similar lab in today's exam.
Topology was the same, but I couldn't modify R2, but R1 and R3. I didn't have a clue how to resolve it. Anyone knows?

upvoted 2 times

Cryptoking112211 6 months, 1 week ago

Hi - the Sim you are referring to is where you need to configure R1 and R3 and need to allow-as-in under the bgp IPv4 address family

upvoted 1 times

tempaccount00001 6 months, 1 week ago

The "allowas-in" feature is configured on the neighbour not on the bgp ipv4 address family.

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/112236-allowas-in-bgp-config-example.html

If in the exam you need to configure R1 and R3 you would do this:

R1:
router bgp 123
neighbour 10.0.0.2 remote-as 456
neighbour 10.0.0.2 allowas-in
network 10.0.0.0 255.255.255.0
network 1.1.1.1 255.255.255.255

R3:
router bgp 123
neighbour 192.168.1.2 remote-as 456
neighbour 192.168.1.2 allowas-in
network 192.168.1.0 255.255.255.0
network 3.3.3.3 255.255.255.255

then you would test:
R1:
ping 1.1.1.1 source 3.3.3.3

or from R3:
ping 3.3.3.3 source 1.1.1.1

upvoted 7 times

Cryptoking112211 6 months ago

it depends on the IOS, IOS XE will not allow you to do the command you mentioned and it will need to be configured under the address family configuration mode. i have lab'ed it up. id say you will need to check in the exam if IPv4 address family has been configured or not and take it from there

upvoted 1 times

bier132 5 months, 2 weeks ago

i also "lab'ed it up" with IOS-XE.
It is working for me.

R1#show run | s r b
router bgp 123
bgp log-neighbor-changes
network 1.1.1.1 mask 255.255.255.255
neighbor 10.0.0.2 remote-as 456
neighbor 10.0.0.2 allowas-in
R1#sho
R1#show ver
R1#show version
Cisco IOS XE Software, Version 17.03.04a
Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.4a, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Tue 20-Jul-21 04:59 by mcpre

upvoted 2 times

[Removed] 6 months, 1 week ago

the given answer is correct with the exception that they forgot to add the 'mask' keyword when defining the networks

upvoted 4 times

helmerpach 6 months, 2 weeks ago

I just took the exam, the interfaces are already configured. Therefore, the answer given by the administrator is the correct one

upvoted 3 times

danman32 6 months, 2 weeks ago

What gets me is that as-override didn't seem to be in the scope of ENCOR (certainly not in the official Cisco cert guide), particularly if vpnv4 and MPLS needs (or originally needed) to be part of the equation.

upvoted 1 times

danman32 6 months, 1 week ago

I'm wondering if the intent of the test simulation is to test you on using policy-map to modify the AS as R2 sends it out to R1 and R3. That would get around the controversy if as-override would work in real-world without VRF4.
After all, route manipulation using policy-map IS in the cert study guide.

upvoted 1 times

danman32 6 months, 1 week ago

Then again, if you go by the cert guide, there's only "set as-path prepend"
That won't work because you'll still have the unwanted AS in the path.
So I guess you can only use as-override.
There is a "set as-prepend replace" but again beyond the scope of the cert guide. Seems to be a relatively new command addition to IOS.

upvoted 1 times

mellohello 8 months, 1 week ago

R:1
Router(config)#int lo0
Router(config-if)#ip add 1.1.1.1 255.255.255.255
Router(config-if)#end

Router# conf t
Router (config)# int e0/0
Router (config)# ip add 10.0.0.1 255.255.255.0
Router (config)# no shut
Router (config)# end
Router#wr

Router# conf t
Router(config) router bgp 123
Router(config-router) network 1.1.1.1 mask 255.255.255.255
Router(config-router) neighbor 10.0.0.2 remote-as 456
Router(config-router) end
Router#wr

upvoted 1 times

mellohello 8 months, 1 week ago

R3:
Router(config)#int lo0
Router(config-if)#ip add 3.3.3.3 255.255.255.255
Router(config-if)#end

Router# conf t
Router (config)# int e0/1
Router (config)# ip add 192.168.1.3 255.255.255.0
Router (config)# no shut
Router (config)# end
Router#wr

Router# conf t
Router(config) router bgp 123
Router(config-router) network 3.3.3.3 mask 255.255.255.255
Router(config-router) neighbor 192.162.1.2 remote-as 456
Router(config-router) end
Router#wr

upvoted 1 times

mellohello 8 months, 1 week ago

R2:
Router(config)#int lo0
Router(config-if)#ip add 2.2.2.2 255.255.255.255
Router(config-if)#end

Router# conf t
Router (config)# int e0/0
Router (config)# ip add 10.0.0.2 255.255.255.0
Router (config)# no shut
Router (config)# end
Router#wr

Router# conf t
Router (config)# int e0/1
Router (config)# ip add 192.168.1.2 255.255.255.0
Router (config)# no shut
Router (config)# end
Router#wr

Router# conf t
Router(config) router bgp 456
Router(config-router) network 2.2.2.2 mask 255.255.255.255
Router(config-router) network 10.0.0.0 mask 255.255.255.0
Router(config-router) network 192.168.1.0 mask 255.255.255.0
Router(config-router) neighbor 10.0.0.1 remote-as 123
Router(config-router) neighbor 192.168.1.3 remote-as 123
Router(config-router) neighbor 10.0.0.1 as-override
Router(config-router) neighbor 192.168.1.3 as-override
Router(config-router) end
Router#wr

upvoted 2 times

dereknatsu 8 months ago

just wondering, guys
There is no conf change permitted on R1 and R3 as question specify
So if you configure VRF, RD, things like that, means R1 and R3 need to be done so
not sure because question has not publish conf for R1 and R3,
So, maybe check R1 R3 in the exam if you have this question then go from there
I will have exam 31May, if this question will popup, I be back let you guys know

upvoted 3 times

helmerpach 6 months, 3 weeks ago

como te fue en el examen

upvoted 1 times

hollowdew1211 8 months, 2 weeks ago

On R2:
!define vrf and export + import
ip vrf AS
rd 1:1
route-target export 1:1
route-target import 1:1
interface Loopback0
ip vrf forwarding AS
ip address 2.2.2.2 255.255.255.255
!
interface Ethernet0/0
ip vrf forwarding AS
ip address 10.0.0.2 255.255.255.0
half-duplex
!
interface Ethernet1/0
ip vrf forwarding AS
ip address 192.168.1.2 255.255.255.0
half-duplex
!
router bgp 456
bgp log-neighbor-changes
network 2.2.2.2 mask 255.255.255.255
!
address-family ipv4 vrf AS
neighbor 10.0.0.1 remote-as 123
neighbor 10.0.0.1 activate

neighbor 10.0.0.1 as-override
neighbor 192.168.1.3 remote-as 123
neighbor 192.168.1.3 activate
neighbor 192.168.1.3 as-override
no auto-summary
no synchronization
network 2.2.2.2 mask 255.255.255.255
exit-address-family
!

upvoted 2 times

Jeff555566 9 months, 2 weeks ago

I had an opportunity to model this with the Cisco tool. It appears that the given answer is correct. I was able to issue the as-override command under the bgp statement without using a vrf. It must have to do with the newer versions of ios.

upvoted 2 times

JackDRipper 8 months, 3 weeks ago

Apologies.... what Cisco tool?

upvoted 1 times

HungarianDish 9 months, 1 week ago

Yes, you are right. It also works without a VRF. I also confirmed it with a new test for the peace of my mind.

upvoted 1 times

Jeff555566 9 months, 3 weeks ago

I tried to set this up in GNS3 and was not successful in configuring the example. It seems as if the word "mask" is missing in the network statements between the IP and the mask. As HungarianDish mentioned, it looks like the as-override command only works inside of a VRF. I am certainly far from an expert though, I wonder how much vrf configuration is actually on the exam.

upvoted 1 times

Nickplayany 9 months, 3 weeks ago

Probably if you can check the configuration of the R1 and R3 you will get the answer.

upvoted 2 times

HungarianDish 9 months, 3 weeks ago

R2 (provide edge)
R2#show bgp vpnv4 unicast vrf MYVRF summary | b Neighbor
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.0.0.1 4 123 15 21 10 0 0 00:09:49 2
192.168.1.3 4 123 28 30 10 0 0 00:21:52 2
R2#

upvoted 1 times

HungarianDish 9 months, 3 weeks ago

Results from R1, R3 (customer edges). R2 (provider edge) replaced AS 123 with its own AS, AS 456 in the advertisements. (Simple "find-and-replace-all" mechanism.)

R1#sh ip bgp | b Network
Network Next Hop Metric LocPrf Weight Path
*> 1.1.1.1/32 0.0.0.0 0 32768 i
*> 3.3.3.3/32 10.0.0.2 0 456 456 i
* 10.0.0.0/24 10.0.0.2 0 0 456 i
*> 0.0.0.0 0 32768 i
*> 192.168.1.0 10.0.0.2 0 0 456 i
R1#

R3#sh ip bgp | b Network
Network Next Hop Metric LocPrf Weight Path
*> 1.1.1.1/32 192.168.1.2 0 456 456 i
*> 3.3.3.3/32 0.0.0.0 0 32768 i
*> 10.0.0.0/24 192.168.1.2 0 0 456 i
* 192.168.1.0 192.168.1.2 0 0 456 i
*> 0.0.0.0 0 32768 i
R3#

upvoted 1 times

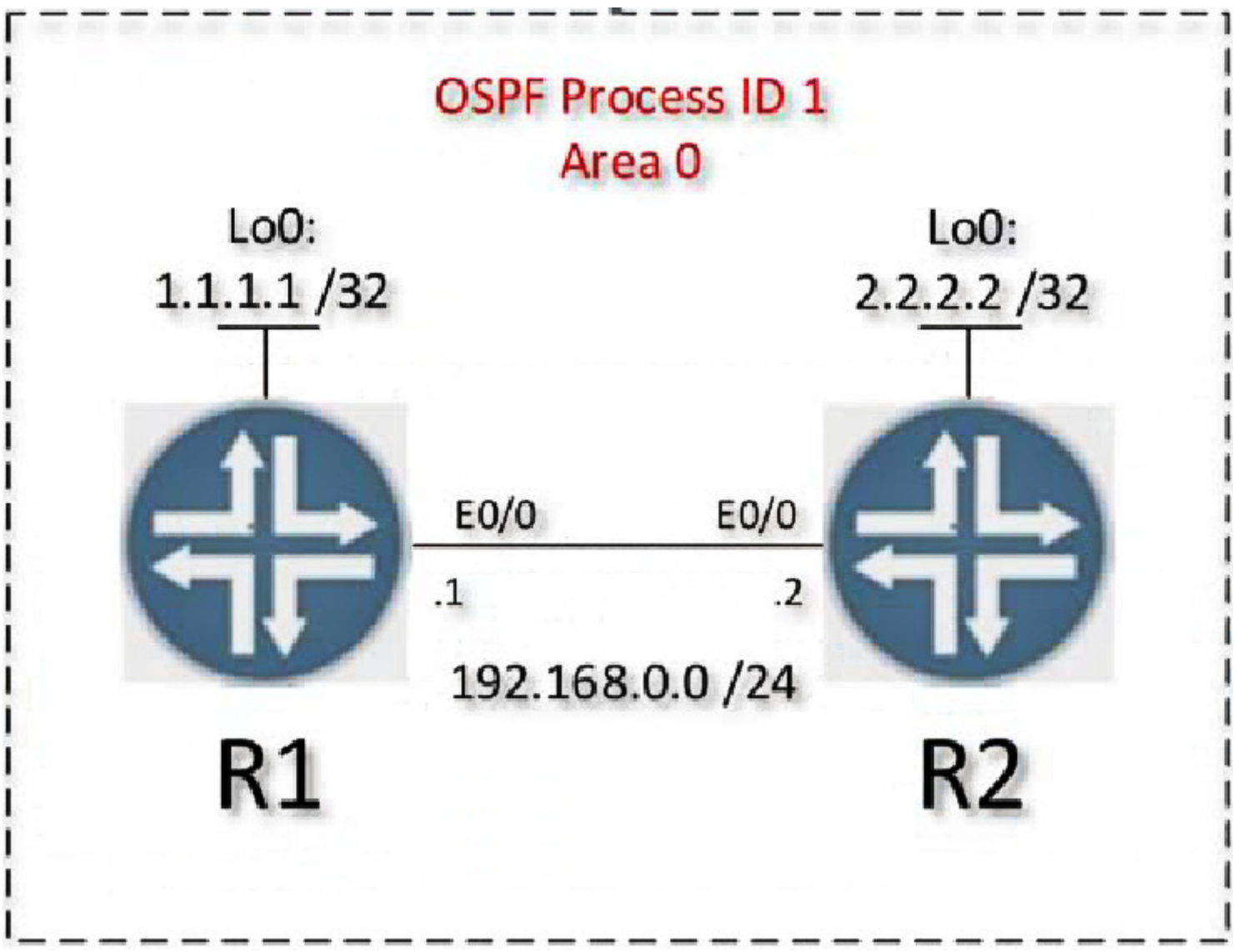
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

Topology
-

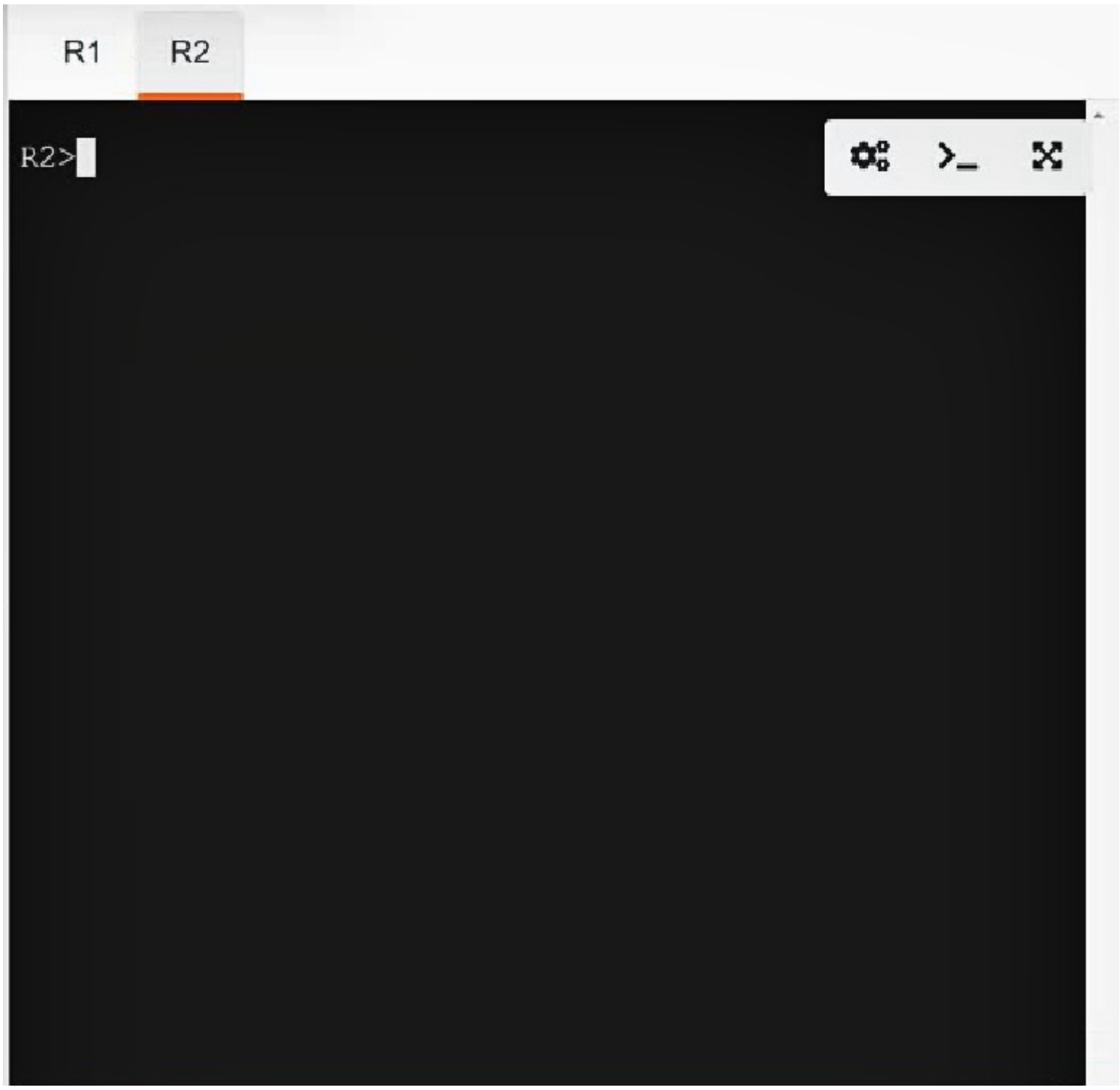


Tasks
-

Configure OSPF on both routers according to the topology to achieve these goals:

1. Ensure that all networks are advertised between the routers without using the “network” statement under the “router ospf” configuration section.
2. Configure a single command on both routers to ensure:
• The DR/BDR election does not occur on the link between the OSPF neighbors.

• No extra OSPF host routes are generated.



R1
Router ospf 1
Int loop0
ip ospf 1 area 0
int et0/0
ip ospf 1 area 0
ip ospf network point-to-point
Copy run start

Correct Answer:

R2
Router ospf 1
int loop0
ip ospf 1 area 0
int et0/0
ip ospf 1 area 0
ip ospf network point-to-point
Copy run start

asjose1 Highly Voted 6 months, 1 week ago

On R1
interface loopback 0
ip ospf 1 area 0
interface e0/0
ip ospf 1 area 0
ip ospf network-type point-to-point

On R2
interface loopback 0

ip ospf 1 area 0
interface e0/0
ip ospf 1 area 0
ip ospf network-type point-to-point
upvoted 5 times

mgiuseppe86 Most Recent 3 months, 4 weeks ago

So guys, the answer is in the question

"2. Configure a single command on both routers to ensure:"

a SINGLE command... what single command accomplishes both of those tasks?
ip ospf network-type point-to-point

and that's it.
upvoted 1 times

bier132 5 months, 2 weeks ago

• No extra OSPF host routes are generated.
What does it mean?

We can prevent DR/BDR election by configuring the Ethernet link to OSPF type point-to-point OR point-to-mulitpoint.
If you choose point-to-mulitpoint for whatever reason, OSPF will create a extra host route for every multipoint neighbor in that segment.
Just choose point-to-point and you accomplish both tasks (no DR/BDR - no extra host route).

Tested with IOS-XE 17.3.4a in GNS3
upvoted 4 times

[Removed] 6 months, 2 weeks ago

To me, the answer seems correct.
On R1 and R2, configure the ospf process under the interfaces

R1/R2
interface loopback 0
ip ospf 1 area 0
interface e0/0
ip ospf 1 area 0
ip ospf network-type point-to-point

The confusing part could be the last statement "no extra ospf host routes are generated"
I'm not sure what they mean by this, but the suggestion to configure OSPF with passive interface default doesn't fit the requirement.
Passive-interface prevents Hellos from being advertised on the link, which prevents OSPF from forming neighborships. This does not prevent OSPF from advertising routes if A) they fall within the network statement, and B) the link is configured to be part of the OSPF process ID
upvoted 3 times

teikitiz 5 months, 4 weeks ago

I was considering prefix-suppression for the "no extra ospf host routes are generated" (the link between routers has no hosts), but it doesn't seem to apply to this simple topology. My 1 cent.
upvoted 1 times

owenshinobi 8 months, 2 weeks ago

my config
R1
Router ospf 1
Passive interface default
Interface loopback 0
Ip ospf 1 area 0
Ip ospf 1 area 0 network-type point-to-point
no passive interface
Interface Ether0/0
ip ospf 1 area 0
ip ospf 1 area 0 network-type point-to-point
no passive interface
R2
Router ospf 1
passive interface default
interface loopback 0
ip ospf 1 area 0
ip ospf 1 aera 0 network-type point-to-point
interface Ether0/0
ip ospf 1 area 0
ip ospf 1 area 0 network-type point-to-point
please verify
upvoted 2 times

owenshinobi 8 months, 2 weeks ago

editanswer:
R1
Router ospf 1
Passive interface default
no passive interface loopback 0

no passive interface Ether0/0
Interface loopback 0
Ip ospf 1 area 0
Ip ospf 1 area 0 network-type point-to-point
Interface Ether0/0
ip ospf 1 area 0
ip ospf 1 area 0 network-type point-to-point
Copy running-config startup-config
R2
Router ospf 1
passive interface default
no passive interface loopback 0
no passive interface Ether0/0
interface loopback 0
ip ospf 1 area 0
ip ospf 1 aera 0 network-type point-to-point
interface Ether0/0
ip ospf 1 area 0
ip ospf 1 area 0 network-type point-to-point
copy running-config startup-config

upvoted 1 times

gibblock 9 months ago

My understanding of this question is as following

1. under "router ospf" a non network statement
#router ospf 1
#redistribute connected subnets

2. a single command - must be the network point-to-point under interface configuration
#ip ospf network point-to-point
#ip ospf 1 area 0

R1#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
2.2.2.2 0 FULL/ - 00:00:37 192.168.0.2 GigabitEthernet0/0

R1#show ip ospf route
O E2 2.2.2.2 [110/20] via 192.168.0.2, 00:01:24, GigabitEthernet0/0

copy running-config startup-config

upvoted 1 times

HungarianDish 9 months ago

However, this might be a correct solution, I do not think that this is a typical case of redistributing routes into OSPF. With redistribution, the router becomes an ASBR which is unnecessary for this design. Also, type 5 LSA and type 4 LSA are then generated unnecessairily. With redistribution, the connected routes come in as external routes. It really think that in this task all routes should belong to the OSPF domain. We can achive this by enabling the protocol on the interface (ip ospf 1 are 0). Why would we want to complicate things?

upvoted 3 times

gibblock 9 months ago

After re-reading the task 1. for maybe the 10th time I think you are right.
It is not an actual must to use the "router ospf" command, but instead the alternative.
My bad.

upvoted 2 times

gibblock 9 months ago

It's not about complicating things, just following the requirements. It clearly states that the configuration should be set under "router ospf".
While I agree on the unnecessary ASBR role, it fulfills the task of distributing the networks without the network command.
Regarding the "ip ospf 1 area 0" you are not announcing the loopback networks.
I tried it on IOL and VIOS, but then again, maybe I misunderstood

upvoted 1 times

HungarianDish 9 months, 3 weeks ago

The loopbacks should have network type point-to-point, too.

upvoted 2 times

HungarianDish 9 months, 3 weeks ago

Sorry, I did not realize that the loopbacks are set as /32. In this case, the network type does not matter!
Task: "No extra OSPF host routes are generated" -> What is the goal of this task then?

upvoted 1 times

owenshinobi 8 months, 2 weeks ago

Task "No extra OSPF host routes are generated"
i config uder router ospf "Passive interface default"
and under interface using add command "no passive interface"

upvoted 1 times

[Removed] 6 months, 2 weeks ago

The passive interface default is to prevent the generation of hellos that are used to form ospf neighborships. This does not mean that routes aren't advertised. Routes are advertised if a) they fall within the network statement under router configuration mode, or b) if the interface is configured with the interface command ip opsf <id> area <area> command. So I do not think this is necessary

upvoted 1 times

JackDRipper 9 months, 2 weeks ago

Maybe it's just /32 in the diagram? I wonder what the loopback ip address config looks like. Only way for that 2nd sub-task to work with the loopback is if the loopback has a mask less than /32.

upvoted 1 times

HungarianDish 9 months, 3 weeks ago

For no DR/BDR and no host route apply:
"ip ospf network point-to-point" under interface config.

upvoted 1 times

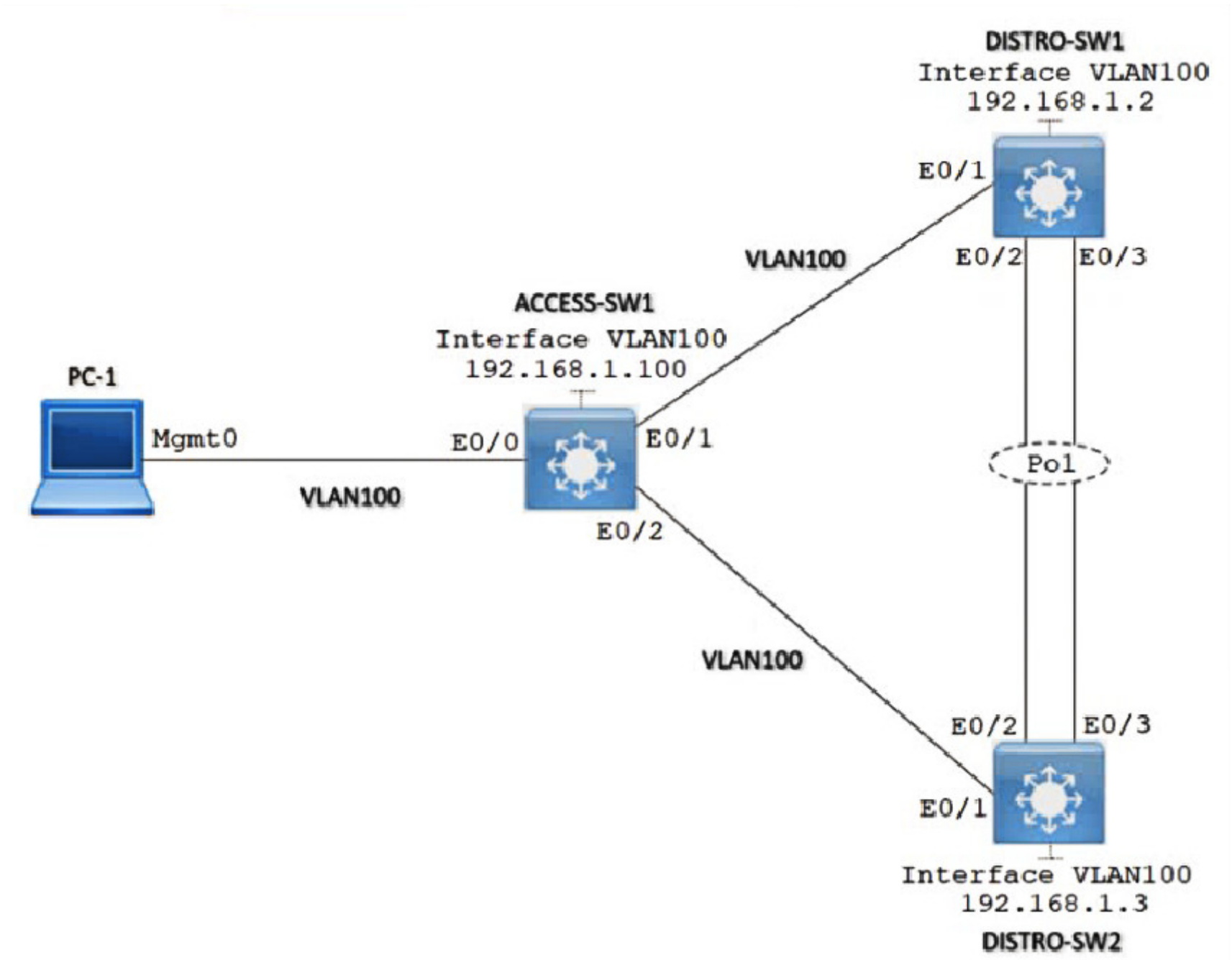
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

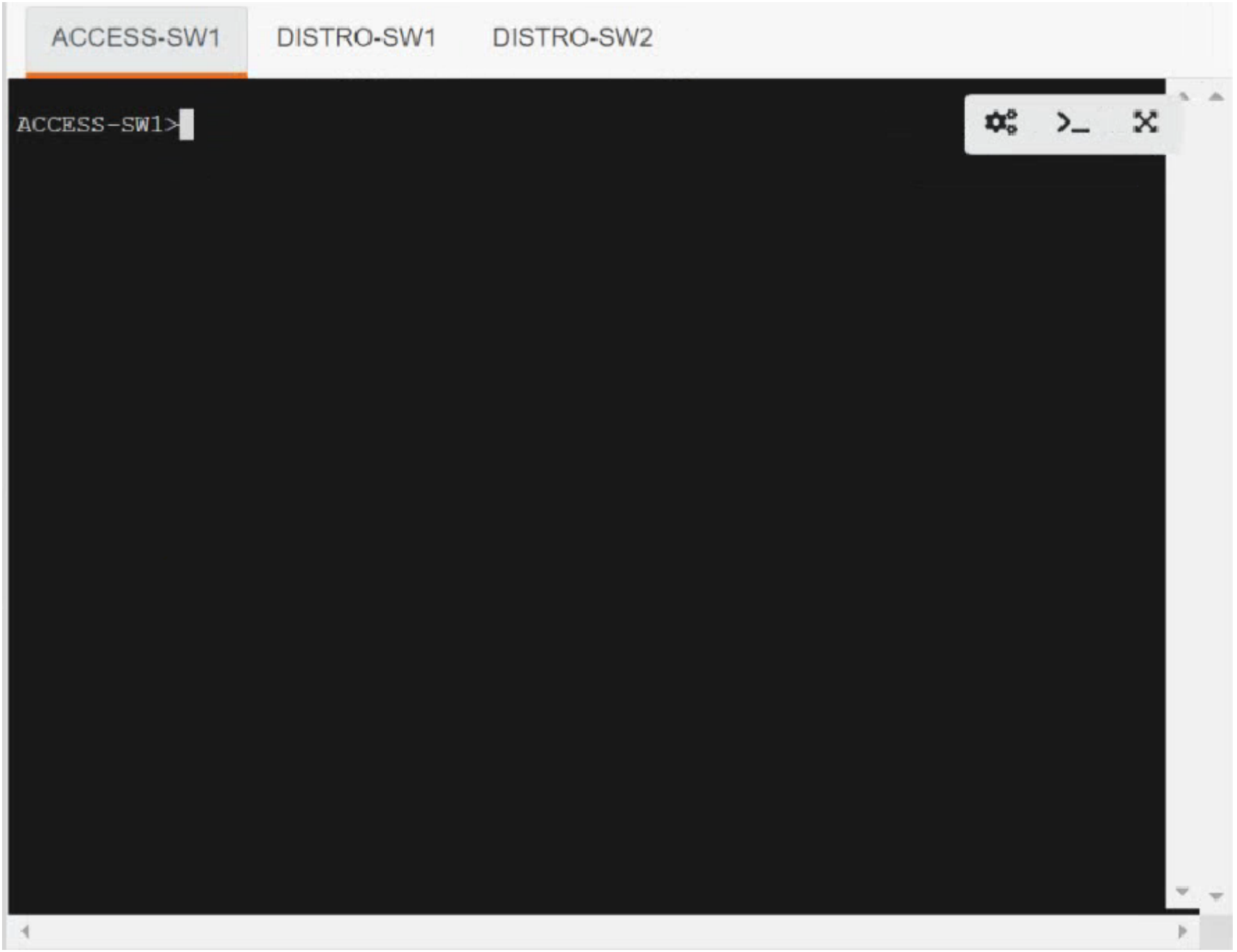
Topology
-

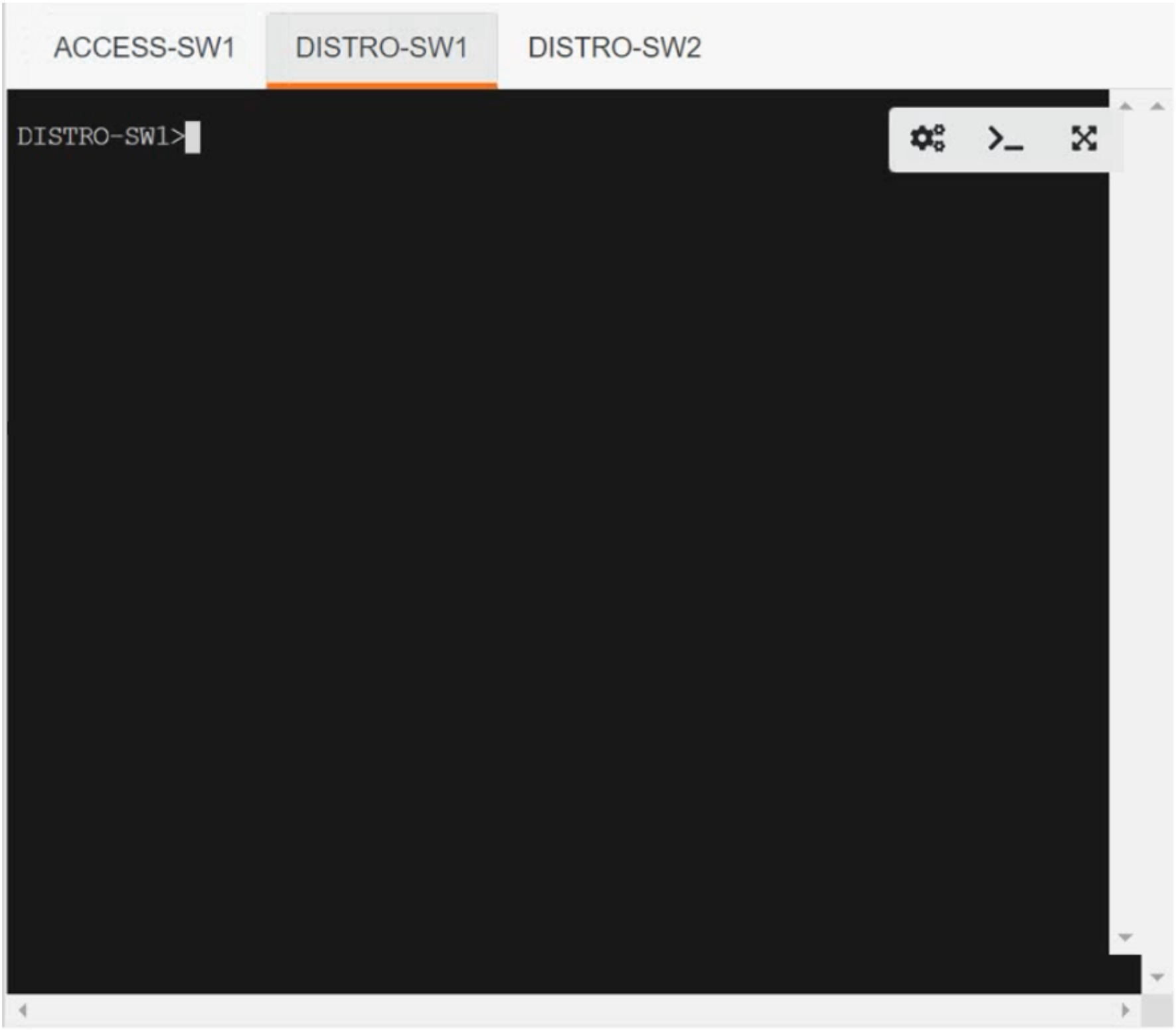


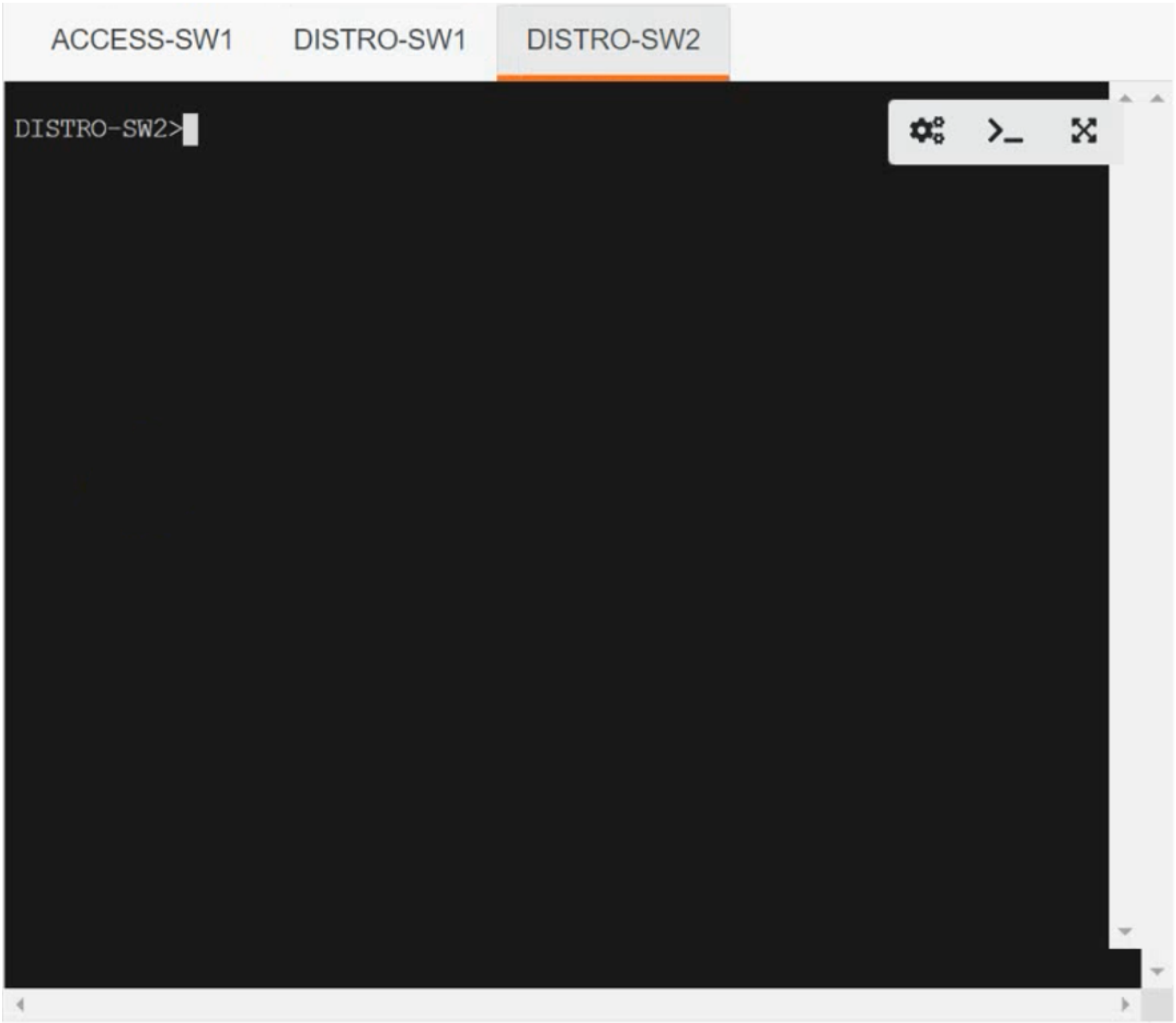
Tasks
-

Implement VRRP between DISTRO-SW1 and DISTRO-SW2 on VLAN100 for hosts connected to ACCESS-SW1 to achieve these goals:

1. Configure group number 200 using the virtual IP address of 192.168.1.200/24.
2. Configure DISTRO-SW1 as the active router using a priority value of 200 and DISTRO-SW2 as the standby router.
3. DISTRO-SW1 and DISTRO-SW2 should exchange VRRP hello packets every 20 seconds.




ACCESS-SW1
DISTRO-SW1
DISTRO-SW2
DISTRO-SW1>



Correct Answer:

DISTRO-SW1
Config t
Interface vlan 100
Ip address 192.168.1.2
255.255.255.0
Vrrp 200 ip 192.168.1.200
Vrrp 200 priority 200
Vrrp 200 advertise 20
Wr mem

DISTRO-SW2
Config t
Interface vlan 100
Ip address 192.168.1.3 255.255.255.0
Vrrp 200 ip 192.168.1.200
Vrrp 200 advertise 20
Wr mem

eojedad Highly Voted 9 months, 3 weeks ago

here my config

dist-01
int vl100
ip addr 192.168.1.2 255.255.255.0
vrrp 200 ip 192.168.1.200
vrrp 200 priority 200
vrrp 200 timers advertise 20
vrrp 200 timers learn
copy run start

Question #747 *Topic 1*

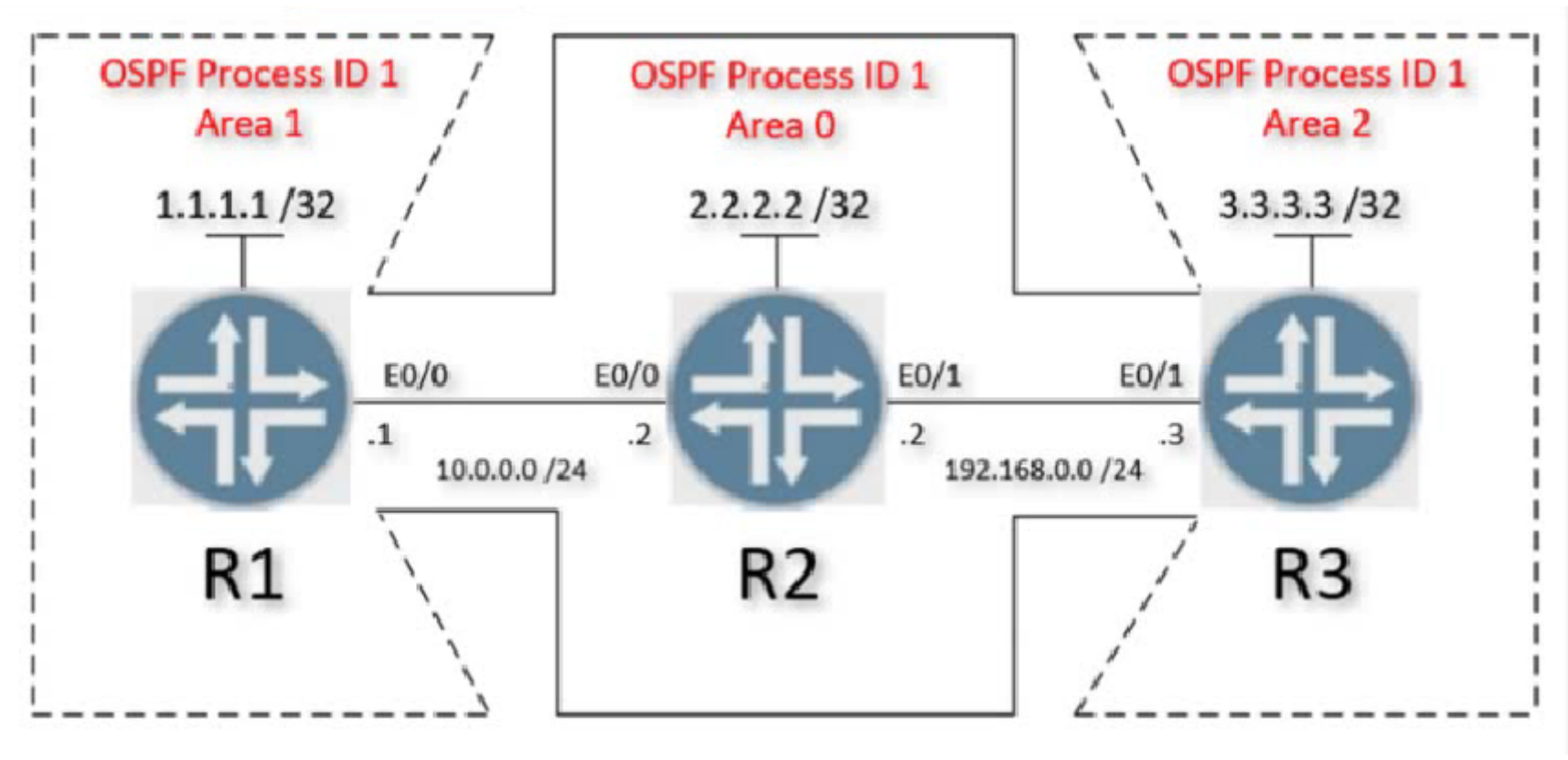
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

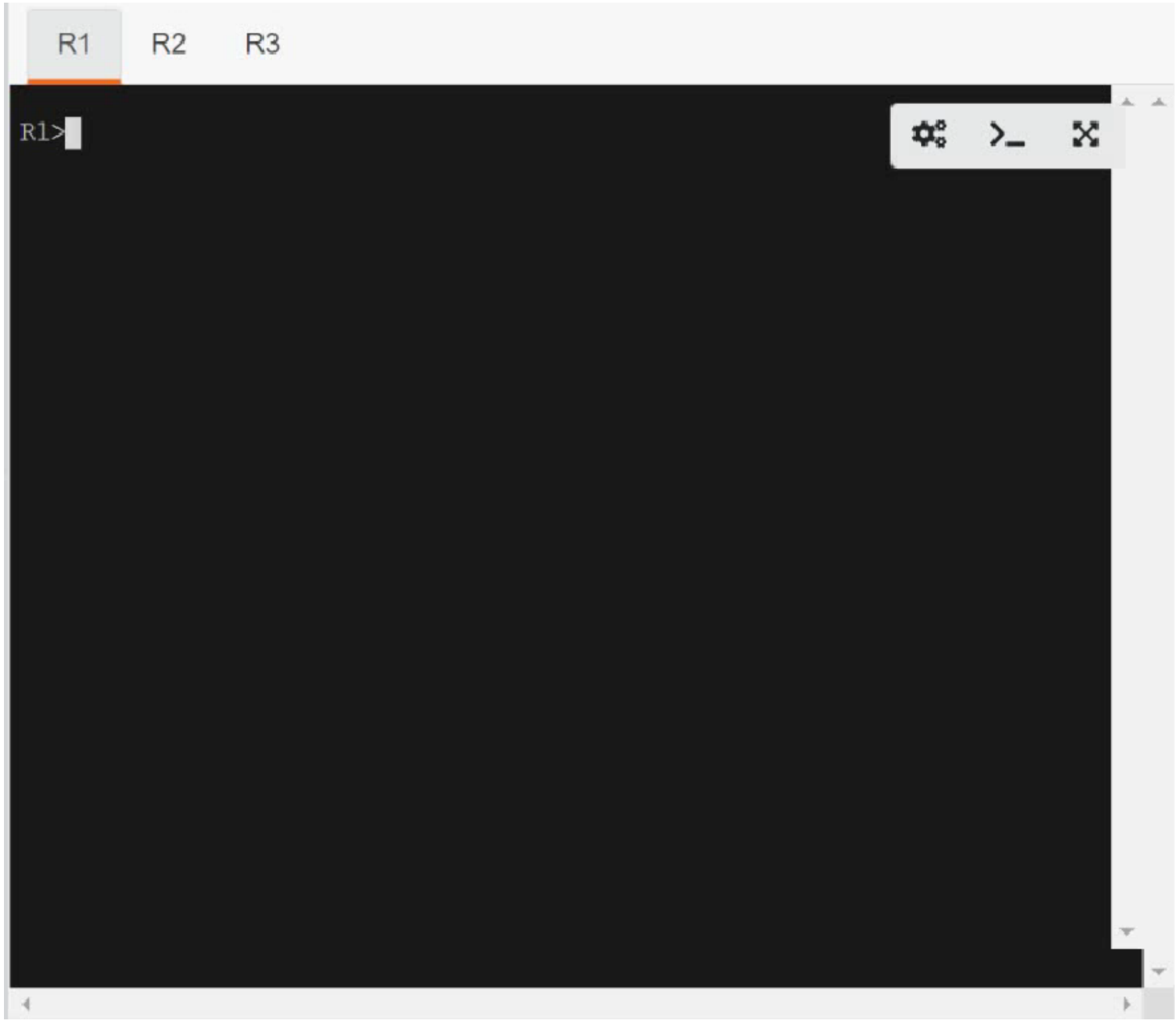
Topology
-

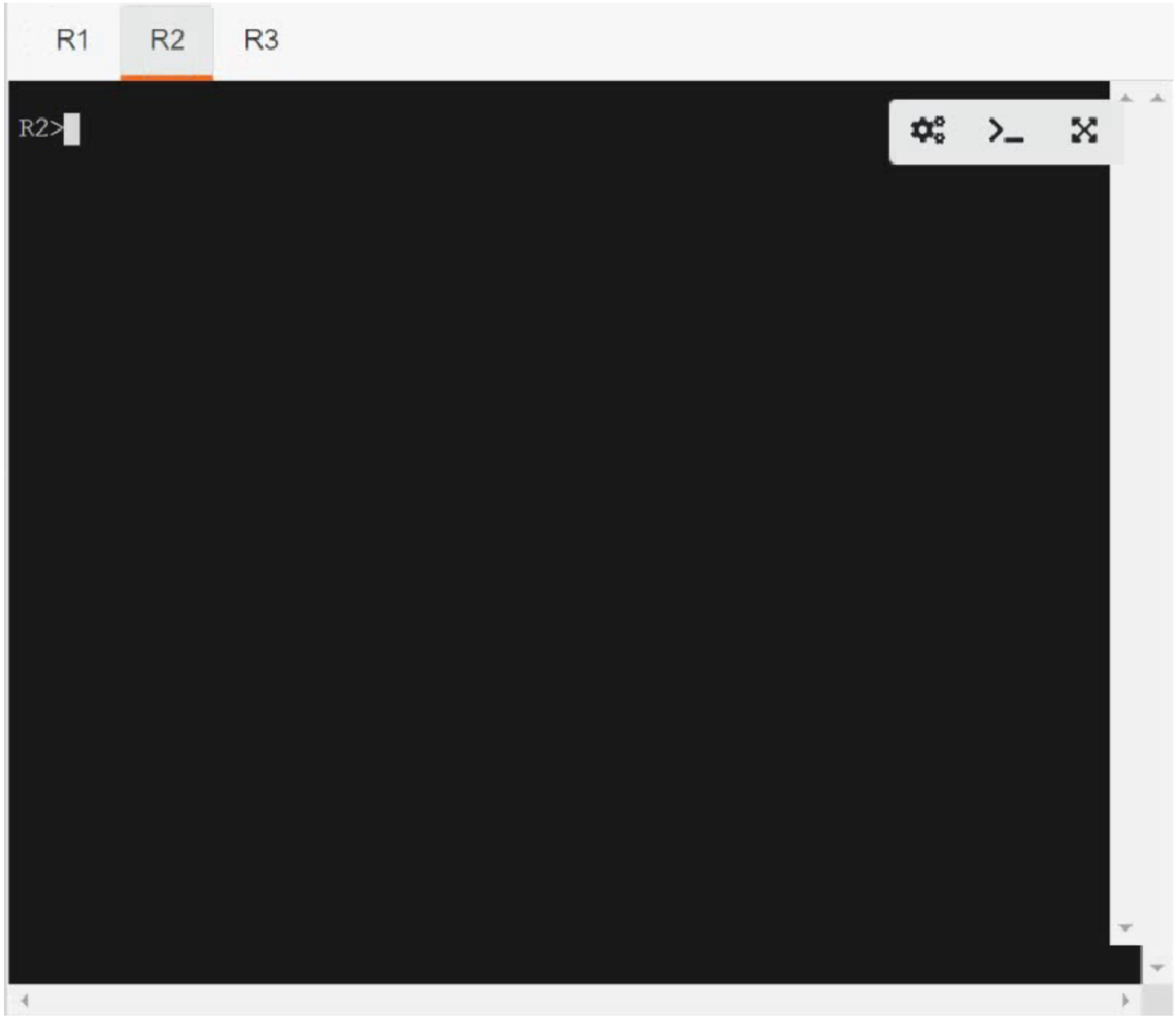


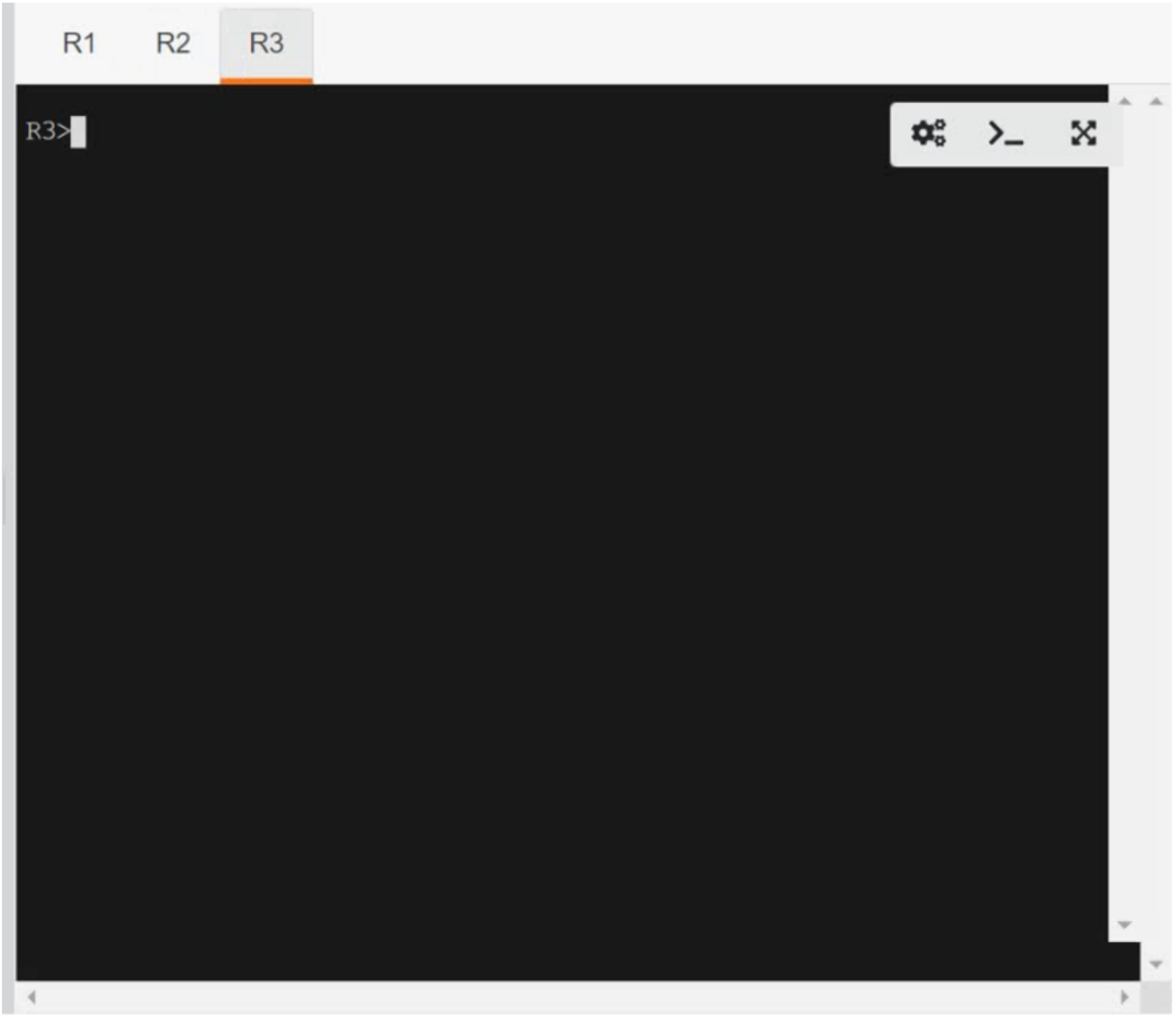
Tasks
-

Configure OSPF on all three routers according to the topology diagram to achieve these goals:

1. Enable OSPF on all interfaces using the network statement and match the network mask of each interface.
2. Ensure that all networks are advertised between the routers.
3. Ensure that all routers use OSPF process ID 1 and that the Lo0 interface is used for the router ID.
4. Configure OSPF MD5 authentication on every physical interface running OSPF using key 1 and the password ccnp321.


R1
R2
R3
R1>


R1
R2
R3
R2>


R1
R2
R3
R3>

Correct Answer:

R1
Router ospf 1
Network 10.0.0.0 0.0.0.255 area 1
Network 1.1.1.1 0.0.0.0 area 1
Router-id 1.1.1.1
area 1 authentication message-digest

Interface E0/0
ip ospf message-digest-key 1 md5 ccnp321

R2
Router ospf 1
Network 10.0.0.0 0.0.0.255 area 1
Network 192.168.0.0 0.0.0.255 area 2
Network 2.2.2.2 0.0.0.0 area 0
Router-id 2.2.2.2
area 1 authentication message-digest
area 2 authentication message-digest

Interface E0/0
ip ospf message-digest-key 1 ccnp321

Interface E0/1
ip ospf message-digest-key 1 ccnp321

R3
Router ospf 1
Network 192.168.0.0 0.0.0.255 area 2
Network 3.3.3.3 0.0.0.0 area 2
Router-id 3.3.3.3
area 2 authentication message-digest

Interface E0/1
ip ospf message-digest-key 1 ccnp321

asiansensation Highly Voted 9 months, 2 weeks ago

R1
interface Loopback0
ip address 1.1.1.1 255.255.255.255

interface Ethernet0/0
ip address 10.0.0.1 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 ccnp321

router ospf 1
router-id 1.1.1.1
network 1.1.1.1 0.0.0.0 area 1
network 10.0.0.0 0.0.0.255 area 0

R2
interface Loopback0
ip address 2.2.2.2 255.255.255.255

interface Ethernet0/0
ip address 10.0.0.2 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 ccnp321

interface Ethernet0/1
ip address 192.168.0.2 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 ccnp321

router ospf 1

router-id 2.2.2.2
network 2.2.2.2 0.0.0.0 area 0
network 10.0.0.0 0.0.0.255 area 0
network 192.168.0.0 0.0.0.255 area 0

R3
interface Loopback0
ip address 3.3.3.3 255.255.255.255

interface Ethernet0/1
ip address 192.168.0.3 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 ccnp321

router ospf 1
router-id 3.3.3.3
network 3.3.3.3 0.0.0.0 area 3
network 192.168.0.0 0.0.0.255 area 0

upvoted 13 times

tempaccount00001 6 months, 1 week ago

I would agree with this!

usually interfaces are configured already, if not then verify with "show ip interface brief". if the interfaces aren't configured, they are most likely also shut down, so make sure you dont get caught on the "no shut". verify with "show ip ospf neighbor".

This would be my config BTW, almost exactly like yours:

R1:
router ospf 1
id 1.1.1.1
network 1.1.1.1 0.0.0.0
network 10.0.0.0 0.0.0.255
int e0/0
ip ospf authentication message-digest
ip ospf message-digest-key 1 MD5 ccnp321

R2:
router ospf 1
id 2.2.2.2
network 2.2.2.2 0.0.0.0
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.0.255
int e0/0
ip ospf authentication message-digest
ip ospf message-digest-key 1 MD5 ccnp321
int e0/1
ip ospf authentication message-digest
ip ospf message-digest-key 1 MD5 ccnp321

R3:
router ospf 1
id 3.3.3.3
network 3.3.3.3 0.0.0.0
network 192.168.0.0 0.0.0.255
int e0/1
ip ospf authentication message-digest
ip ospf message-digest-key 1 MD5 ccnp321

upvoted 1 times

Cryptoking112211 6 months, 1 week ago

Router 3 is in Area 2 - not area 3 .....

R3
interface Loopback0
ip address 3.3.3.3 255.255.255.255

interface Ethernet0/1
ip address 192.168.0.3 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 ccnp321

router ospf 1
router-id 3.3.3.3
network 3.3.3.3 0.0.0.0 area 2
network 192.168.0.0 0.0.0.255 area 0

upvoted 1 times

sledgey121 Most Recent 2 weeks, 1 day ago

Area 0 is within the solid lines, area 1 and 2 are within the dashed lines. The whole of R2 is area0 and only the R1/R2 loopbacks are the different areas. Only configure the auth on the interfaces.

upvoted 1 times

[Removed] 6 months ago

I would configure the authentication on the interfaces instead of the router ospf process

upvoted 1 times

danman32 6 months ago

Makes you wonder if exam expects you to statically set the router ID to "ensure" the desired router ID, or let auto determination of router ID which would use the L0 interface as ID.
Could be the test grades on whether the RID matches the L0 IP, regardless of your method.

I agree with others, all physical segments are within area 0 based on the dashed lines.

But probably the biggest scoring is the wildcard masks used for the network statements, and that you configured a working MD5 authentication.

upvoted 1 times

VincentY 8 months, 1 week ago

Two mistakes here.
1. The area configurations are wrong. Notice the types of the line in the exhibit.
2.The

upvoted 4 times

VincentY 8 months, 1 week ago

2. The “authentication on every physical interface” indicates the authentication command should all be on the physical interfaces.

upvoted 4 times

Symirnian 9 months, 2 weeks ago

R1# router ospf 1
#router-id 1.1.1.1
#network 1.1.1.1 0.0.0.0 area 1
#network 10.0.0.0 0.0.0.255 area 0
#exit
#interface e0/0
#ip ospf message-digest-key 1 md5 ccnp321
#ip ospf authentication message-digest
#do write

R2#router ospf 1
#network 2.2.2.2 0.0.0.0 area 0
#network 10.0.0.0 0.0.0.255 area 0
#network 192.168.0.0 0.0.0.255 area 0
#interface range e0/0-1
#ip ospf message-digest-key 1 md5 ccnp321
#ip ospf authentication message-digest
#do write

upvoted 2 times

HungarianDish 9 months, 3 weeks ago

authentication:
task: "Configure OSPF MD5 authentication on every physical interface running OSPF"
-> I assume that they requested a configuration per interface, and NOT per area:

interface e0/0
ip ospf message-digest-key 1 md5 ccnp321
ip ospf authentication message-digest

https://networklessons.com/ospf/how-to-configure-ospf-md5-authentication

You can enable "authentication message-digest" under the ospf process for an entire area. or You can enable it under the interface.

upvoted 3 times

HungarianDish 9 months, 3 weeks ago

router-ID:
- we do not need to specify the router-id explicitly, because the ip of loopback0 was elected as the router-id automatically

OSPF uses the following criteria to select the router ID:

Manual configuration of the router ID.
Highest IP address on a loopback interface.
Highest IP address on a non-loopback interface.

https://networklessons.com/ospf/ospf-router-id

upvoted 2 times

HungarianDish 9 months, 3 weeks ago

I tested the two possible configs in CML. It works both way.
1) R1 and R3 can also have their physical interface in "area 0" -> so, R1 and R3 become ABR for non-backbone areas
2) however, it is enough to place only the loopback of R2 in "area 0", and all the rest can be in non-backbone areas -> R2 becomes ABR

It depends on the desired design.

Some sources:
https://notes.networklessons.com/ospf-backbone-area-0

All non-backbone areas must have an ABR that is also connected to Area 0.
...
Area 0 must exist on at least one interface of an ABR router.

https://lpmazariegos.com/2016/02/02/interconnecting-ospf-areas/

Backbone Router – Routers where at least one OSPF interface must belong to area 0 (backbone area).
upvoted 1 times

Symirnian 9 months, 3 weeks ago
I think answer is wrong! 3 routers should have "area 0" command. All interfaces of R2 should be in area 0 and the counter interface on R1 and R3 must be in area 0 too. What is your opinion?
upvoted 2 times

Badger_27 9 months, 3 weeks ago
I think you are right.
upvoted 1 times

HungarianDish 9 months, 3 weeks ago
The area configuration of the provided solution is correct. However, I am not sure that the router-ID and the authentication are configured as specified in the task.
upvoted 1 times

Nickplayany 9 months, 3 weeks ago
Hey! I think you are wrong. Read more about it and check the exact same scenario here:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html

Search for
Example: Complex Internal Router with ABR and ASBR
upvoted 1 times

Symirnian 9 months, 2 weeks ago
On the design area0 is continued line and ABR is R1 and R3.
area 2 and area 1 are dashed lines on R1 and R3 other sides.
upvoted 3 times

Question #748 *Topic 1*

By default, which virtual MAC address does HSRP group 30 use?

A. 05:0c:5e:ac:07:30

B. 00:00:0c:07:ac:1e

C. 00:43:19:74:89:1e

D. 00:05:0c:07:ac:30

Correct Answer: *B*

Community vote distribution

B (75%) D (25%)

mgiuseppe86 3 months, 4 weeks ago

30 = 00011110 = 0001|1110 = 1|14 = 1E

upvoted 1 times

HarwinderSekhon 6 months, 1 week ago

Selected Answer: B

Hex
00:00:0c:07:ac:1e

upvoted 1 times

Based_Engineer 6 months, 1 week ago

Selected Answer: B

It's in HEX, not decimal.

upvoted 1 times

[Removed] 6 months, 2 weeks ago

Selected Answer: B

Sorry @Backward_CEE, but you are wrong.
Group number in HSRP has to be converted to HEX to be plugged into the virtual mac address
30decimal = 0x1e
A quick to resolve this is by dividing 30 by 16 = 1, and leaves a remainder of 14, 14 in Hex is e, therefore 1e

upvoted 1 times

Backward_CEE 7 months, 3 weeks ago

Selected Answer: D

HSRPv1 0000.0c07.acXX (XX = group number)

upvoted 1 times

Burik 7 months ago

It's B. decimal 30 = hexadecimal 1e.

upvoted 2 times

Question #749 *Topic 1*

Which NTP mode must be activated when using a Cisco router as an NTP authoritative server?

A. primary

B. peer

C. broadcast client

D. server

Correct Answer: *B*

Community vote distribution

D (83%) B (17%)

connorm 3 months, 3 weeks ago

Selected Answer: D

When using a Cisco router as an NTP (Network Time Protocol) authoritative server, you typically want to configure it in NTP Server mode. In NTP terminology, this is referred to as the "NTP Server" mode.

In this mode, the Cisco router will provide time synchronization information to other devices in your network, acting as a time source for them. Other devices can then synchronize their clocks with the Cisco router's clock. To configure a Cisco router as an NTP server, you would use commands like:

shell:
ntp server <server-ip-address>

upvoted 2 times

msstanick 6 months, 4 weeks ago

Selected Answer: D

That is just fantastic... The Q is about the mode, not a command. So, server is the mode while you need to use master command to enable it hence the answer is D.

upvoted 3 times

jrquissak 4 months, 2 weeks ago

Totally Agree!!
Cisco just wants to confuse us with words, we need to pay attention to the question.

upvoted 1 times

commandlineclown 7 months ago

Selected Answer: B

ntp server is the command that points it to a server. NTP master or NTP peer is for creating authoritative NTP server.

upvoted 1 times

JackDRipper 9 months ago

I think these types of questions are planted in there just to mess with test takers.

"Master" is when you want a Cisco router to act as an authoritative NTP server.
"Server <ip-address-of-authoritative-server>" is when you want a Cisco router to act as an NTP client and sync from an authoritative NTP server.

upvoted 3 times

Burik 7 months ago

Wrong dump if you ask me.

upvoted 1 times

JackDRipper 9 months ago

System as an Authoritative NTP Server:
Use the ntp master command in global configuration mode if you want the system to be an authoritative NTP server, even if the system is not synchronized to an outside time source.

https://www.cisco.com/c/dam/en/us/td/docs/ios-xml/ios/bsm/configuration/xe-3se/3650/bsm-xe-3se-3650-book.html#:~:text=ntp%20server%20command.-,System%20as%20an%20Authoritative%20NTP%20Server,to%20an%20outside%20time%20source.&text=Use%20the%20ntp%20master%20command%20with%20caution.

upvoted 1 times

MJane 9 months ago

agree. and if we don't have master as an option, i would say peer?

upvoted 1 times

Dataset 9 months, 3 weeks ago

Selected Answer: D

Is D for me..
Regards

upvoted 1 times

RocketS17 9 months, 3 weeks ago

Selected Answer: D

Server mode.

upvoted 2 times

Symirnian 9 months, 3 weeks ago

Selected Answer: D

Server mode

upvoted 2 times

Badger_27 10 months ago

Selected Answer: B

Server mode

upvoted 1 times

Question #750 *Topic 1*

Refer to the exhibit.

```
Router A
Interface GigabitEthernet 1/0
ip address 192.168.0.1 255.255.255.0
vrrp priority 120

Router B
Interface GigabitEthernet 1/0
ip address 192.168.0.200 255.255.255.0
vrrp priority 100

Router C
Interface GigabitEthernet 1/0
ip address 192.168.0.3 255.255.255.0
vrrp priority 130

Router D
Interface GigabitEthernet 1/0
ip address 192.168.0.4 255.255.255.0
vrrp priority 90
```

Which router is elected as the VRRP primary virtual router?

A. Router A

B. Router B

C. Router C

D. Router D

Correct Answer: *C*

dragonwise Highly Voted 9 months, 1 week ago

Sometimes you spend more time in such simple questions wondering about what trick are they playing 😂

upvoted 15 times

jrquissak 4 months, 2 weeks ago

Totally agree =]
This is a Cisco exam :)

upvoted 1 times

HarwinderSekhon 6 months, 2 weeks ago

Agree lol

upvoted 1 times

Burik Most Recent 7 months ago

None of the answers are correct, as there is no "vrrp priority" command. It should be "vrrp <group ID> priority". Wrong dump, remove this question.

upvoted 3 times

mgiuseppe86 3 months, 4 weeks ago

actually, 'vrrp priority' will default to group 0.

upvoted 1 times

mgiuseppe86 3 months, 4 weeks ago

Nope, im wrong. you can do that with standby(HSRP)
oh well

upvoted 1 times

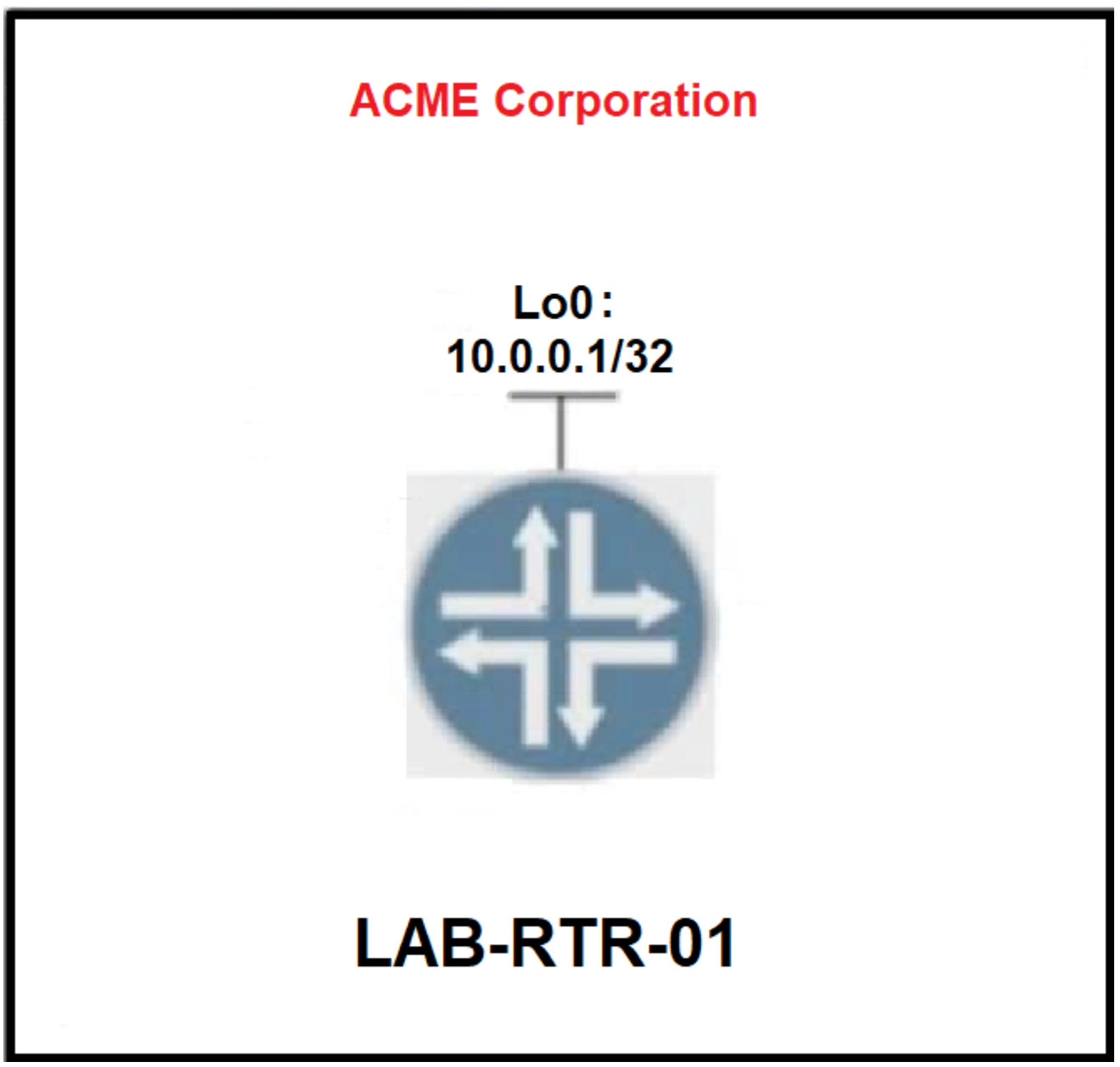
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

Topology
-



Tasks
-

Configure an EEM applet on LAB-RTR-01 that will automatically re-enable interface Loopback0 if it is administratively shut down.

Correct Answer:

```
event manager applet LOOP0
event syslog pattern "Interface Loopback0.* down" period 1
action 1.0 syslog msg "Interface Loopback0 DOWN"
action 2.0 cli command "enable"
action 2.1 cli command "config t"
action 2.2 cli command "interface loopback 0"
action 2.3 cli command "no shutdown"
action 3.0 syslog msg "Interface Loopback0 UP"
```

Vlad_Is_Love_ua Highly Voted 10 months ago

event manager applet int_loopback_Shutdown
event syslog pattern "Interface Loopback0, changed state to administratively down"
action 1.0 cli command "enable"
action 1.5 cli command "config t"
action 2.0 cli command "interface loopback0"
action 2.5 cli command "no shutdown"
action 3.0 cli command "end"

upvoted 20 times

tempaccount00001 Highly Voted 6 months, 1 week ago

This would be my take:

event manager applet NOSHUT_LOOPBACK0
event syslog pattern "Interface Loopback0, changed state to administratively down"
action 1.0 command "enable"

action 2.0 command "conf t"
action 3.0 command "interface loopback0"
action 4.0 command "no shutdown"
action 5.0 command "end"

also do not stress too much about learning the syntax of "Interface Loopback0, changed state to administratively down" just chuck in a "term mon" and shut it, and then look at what the message is.

In case term mon does not work, you can do:
conf t
logging on
logging console
int loopback 0
shut
end
sho log

this will essentially enable logging and then write it into the logs for you to view. copy and paste the text you want to match and happy days

upvoted 12 times

SHONA1 3 months, 3 weeks ago

@Tempaccount000001
You are a legent son, I had few probs with that one in the exam. tried the actual command and shut the interface down to see if would bring it up, but it was not having it after the 3rd try it worked. Thanks man, passed today the question still asked.

upvoted 3 times

[Removed] Most Recent 6 months, 1 week ago

The answer is wrong. The syslog pattern needs to be specific to "administratively down". Vlad_Is_Love_ua is correct.

upvoted 3 times

Papins 7 months, 3 weeks ago

make it simple you can find to the below as reference
https://www.youtube.com/watch?v=32VZDHCrU-4

upvoted 1 times

Papins 7 months, 3 weeks ago

event manager applet int_loopback_Shutdown
event syslog pattern "Interface Loopback0, changed state to administratively down"
action 1.0 cli command "enable"
action 1.1 cli command "config t"
action 1.2 cli command "interface loopback0"
action 1.3 cli command "no shutdown"

upvoted 3 times

HungarianDish 9 months, 3 weeks ago

Apply "exit" when the eem applet config is ready.

"Before modifying an EEM applet, you need to be aware that the existing applet is not replaced until you exit applet configuration mode."

https://www.ciscopress.com/articles/article.asp?p=3100057&seqNum=4

upvoted 8 times

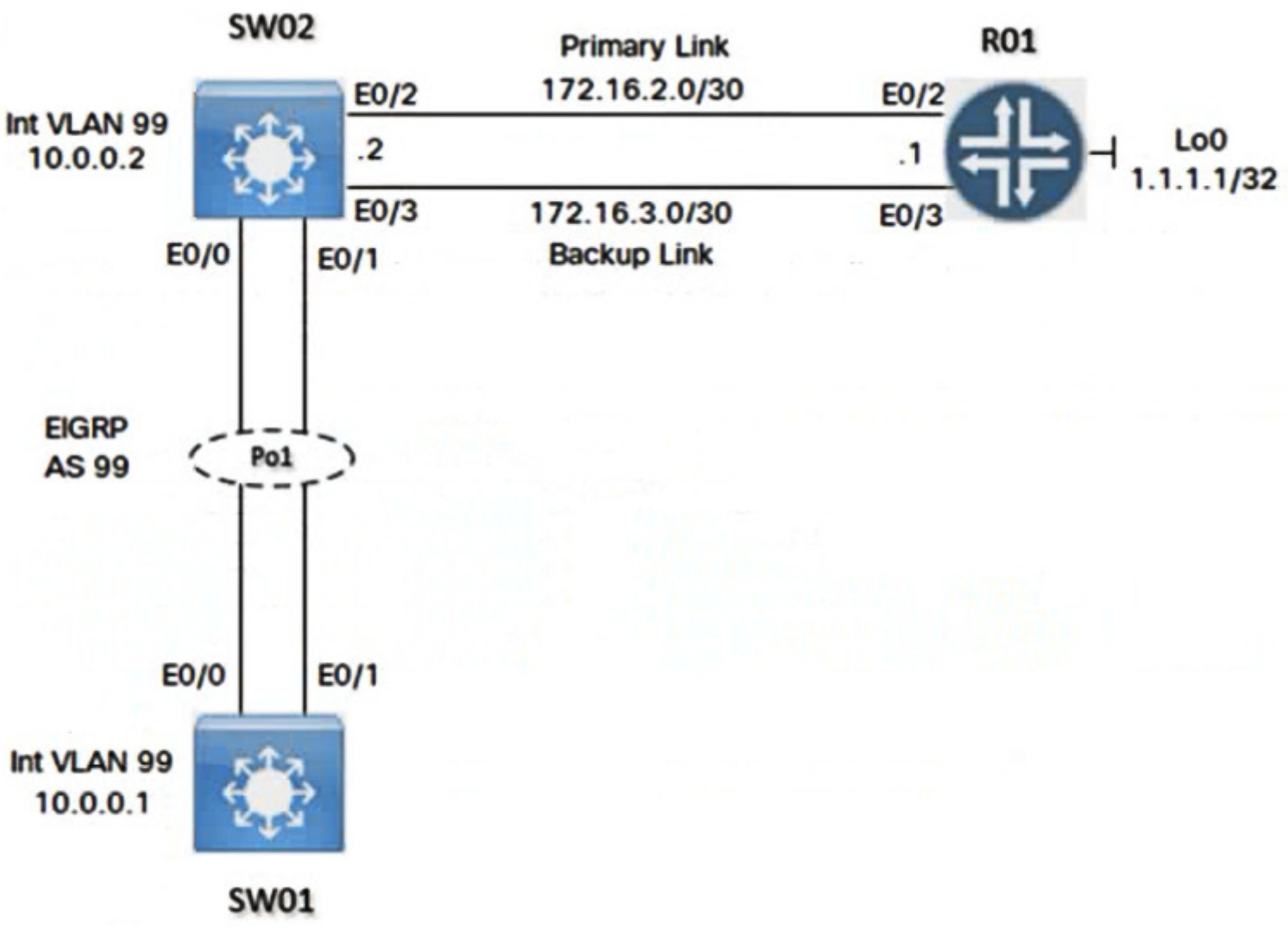
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

Topology
-

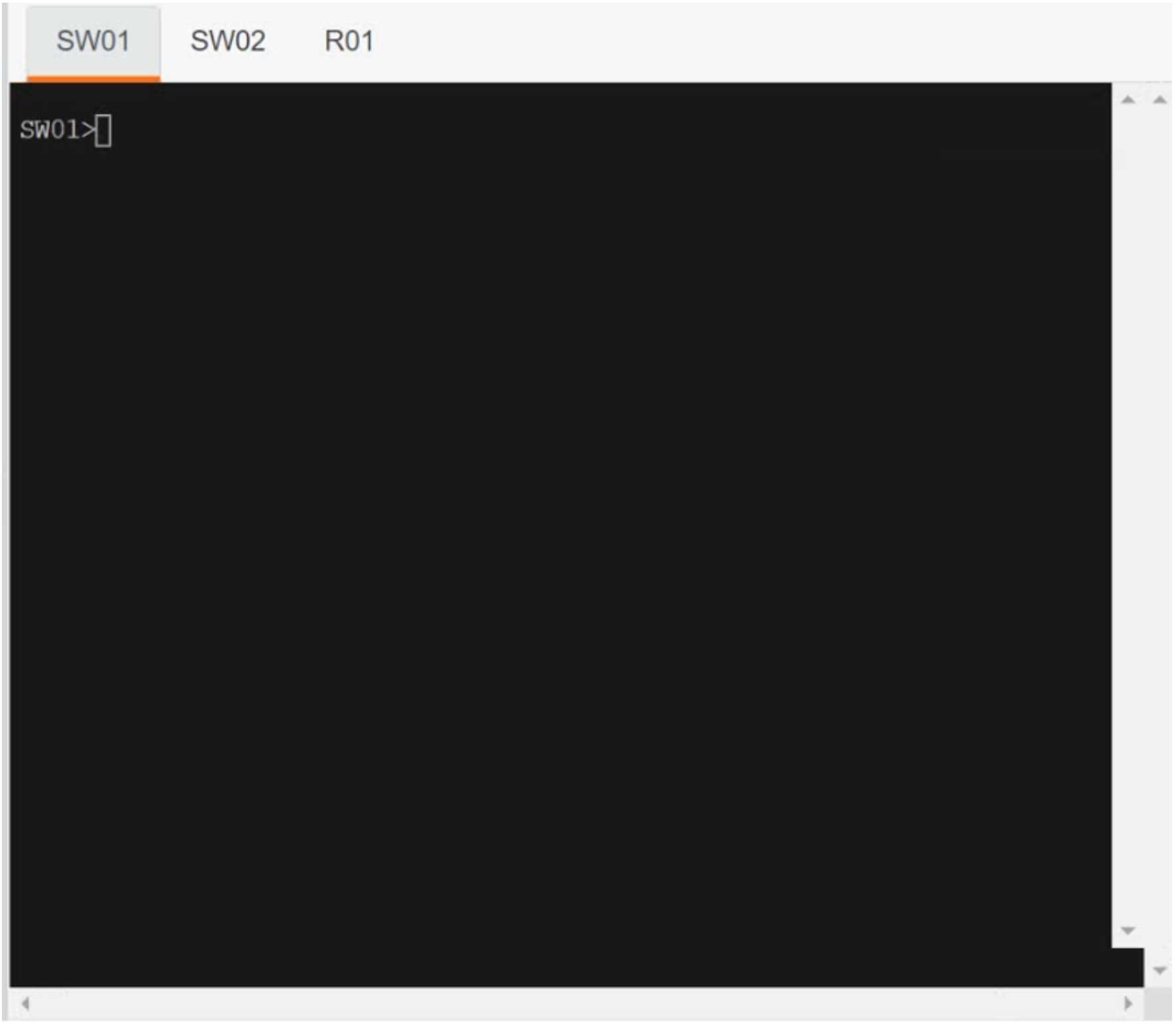


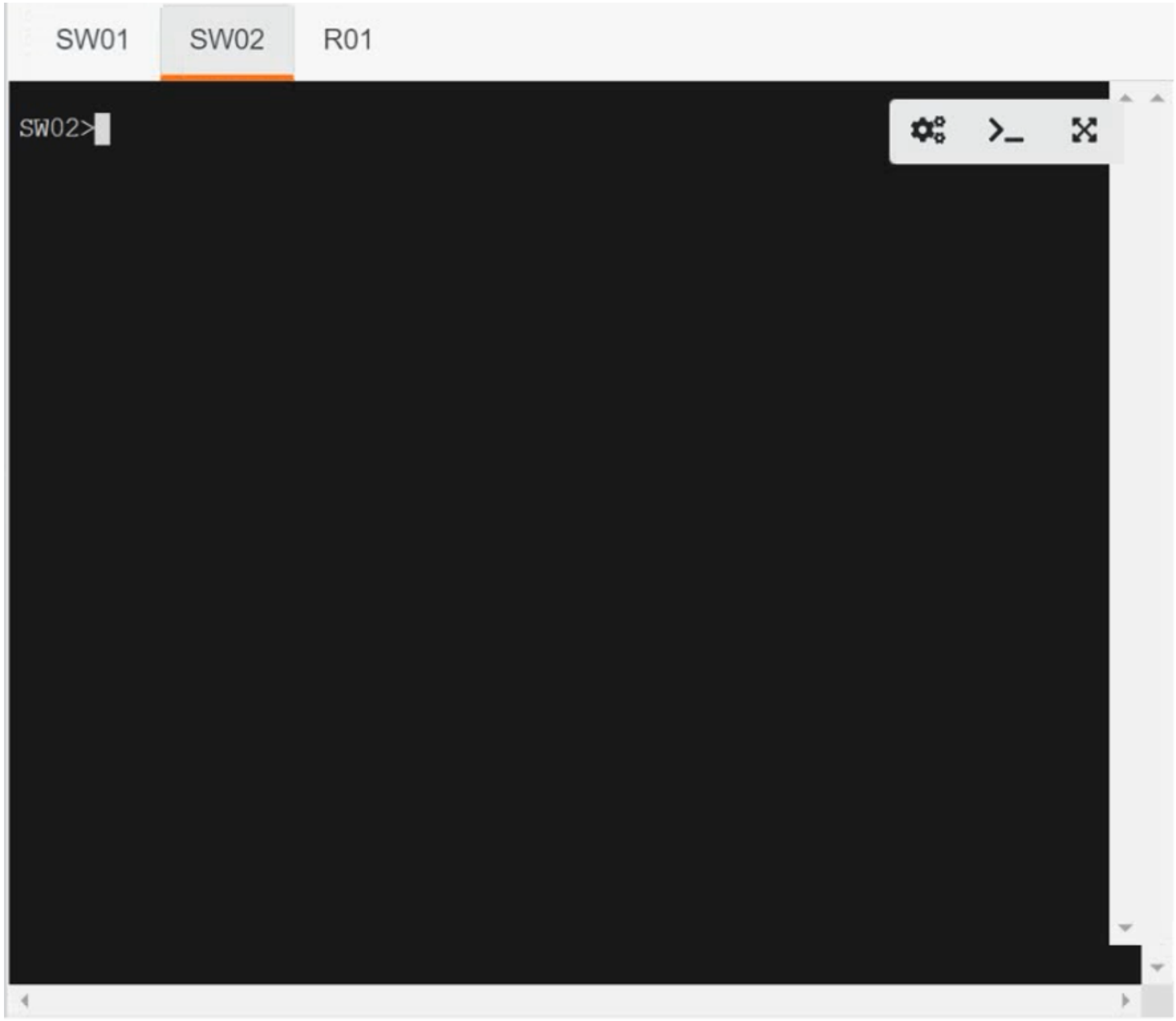
Tasks
-

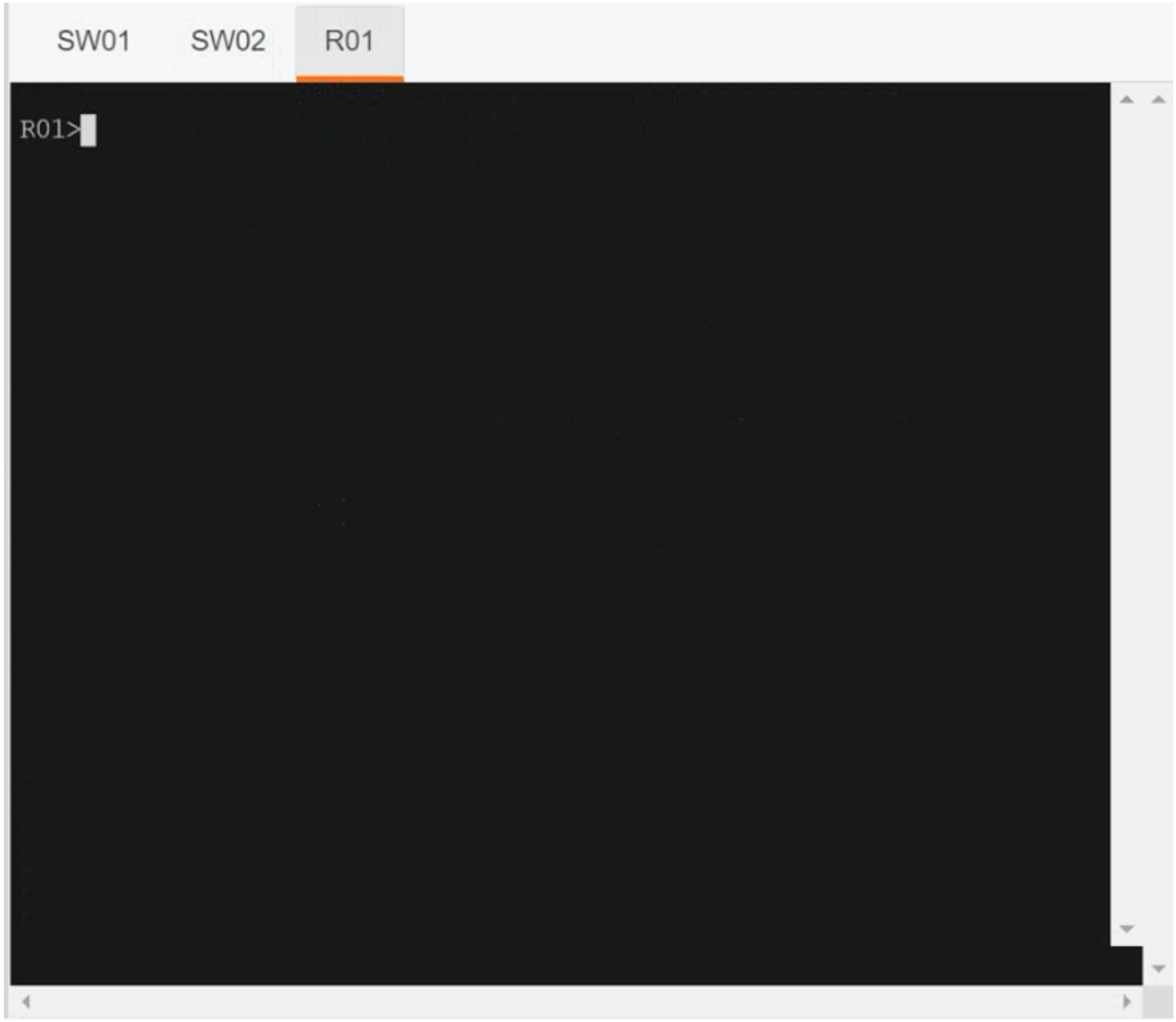
Configure the devices according to the topology to achieve these goals:

1. Configure a SPAN session on SW01 using these parameters:
• Session Number: 20

• Source Interface: VLAN 99
• Traffic Direction: Transmitted Traffic
• Destination Interface: Ethernet 0/1
2. Configure the NetFlow Top Talkers feature for outbound traffic on interface E0/2 of R01 with these parameters:
• Number of Top Talkers: 50
• Sort Type: Packets
• Cache Timeout: 30 seconds
3. Configure an IP SLA operation on SW02 and start the ICMP probe with these parameters:
• Entry Number: 10
• Target IP: 1.1.1.1
• Source IP: 172.16.2.2
• Frequency: 5 seconds
• Threshold: 250 milliseconds
• Timeout: 3000 milliseconds
• Lifetime: Forever




SW01
SW02
R01
SW02>


SW01
SW02
R01
R01>

Correct Answer:

SW1

```
Config t
Monitor session 20
Source interface vlan 99 tx
Destination interface ethernet 0/1
Wr mem
```

R01

```
Config t
Interface E0/2
ip flow egress
ip flow-top-talkers
top 50
sort-by packets
wr mem
```

SW02

```
Config t
Ip sla 10
 Icmp-echo 1.1.1.1 source-ip 172.16.2.2
 Frequency 5
 Threshold 250
 Timeout 3000
 Life forever
Wr mem
```

Nickplayany Highly Voted 9 months, 4 weeks ago

At the second part 2. Configure the NetFlow Top Talkers feature for outbound traffic on interface E0/2 of R01 with these parameters:
• Number of Top Talkers: 50
• Sort Type: Packets
• Cache Timeout: 30 seconds

There is something missing - the last part of cache timeout.

Correct output as below:

R01
config t
interface et0/2
ip flow egress
ip flow-top-talkers
top 50
sort-by packets
cache-timeout 30000 <- that is missing
wr mem

upvoted 15 times

FerroForce Highly Voted 8 months, 2 weeks ago

SW01
conf t
monitor session 20
source vlan 99 tx
destination interface ethernet 0/1
!
write memory

R01
config t
interface et0/2
ip flow egress
ip flow-top-talkers
top 50
sort-by packets
cache-timeout 30000

!
wr mem

SW02
ip sla 10
icmp-echo 1.1.1.1 source-ip 172.16.2.2
threshold 250
timeout 3000
frequency 5
!
ip sla schedule 10 life forever start-time now
!
wr mem

upvoted 9 times

123robinsong Most Recent 6 months, 1 week ago

This commands are not supported on the interface , but only on the global config mode:
ip flow egress
ip flow-top-talkers
top 50
sort-by packets
cache-timeout 30000

upvoted 3 times

tempaccount00001 6 months, 1 week ago

almost correct!

interface eth 0/1
ip flow egress
exit
ip flow-top-talkers
top 50
sort-by packets
timeout 30000

upvoted 2 times

Papins 5 months, 3 weeks ago

almost correct but the interface is eth0/2
int e0/2
ip flow egress
exit
ip flow-top-talkers
top 50
sort-by packets
timeout 30000

upvoted 2 times

rogi2023 6 months ago

I agree with 123robinsong and I am not sure if exiting the intf eth0/1 with the cmd ip flow egress will bind it with the rest of cmds in global config..Maybe Yes. see the
http://www.bscottrandall.com/9.7.3.html
R1(config)# ip flow-top-talkers
R1(config-flow-top-talkers)#?
Netflow top talker configuration commands:
cache-timeout Configure cache timeout
default Set a command to its defaults
exit Exit from top talkers configuration mode
match Configure match criteria
no Negate a command or set its defaults
sort-by Configure top talker sort criteria
top Configure number of top talkers
=======there is a match cmd =========
So I would go with this:
ip flow-top-talkers
top 50
sort-by packets
cache-timeout 30000
match output-interface Ethernet0/2

is this the same as tempaccount..sugests?

upvoted 1 times

DavideDL 8 months, 3 weeks ago

For the first section (SPAN) , I think this is the correct configuration:

monitor session 20 source vlan 99 tx (You can choose between a phisical interface or a vlan NOT an interface vlan)
monitor session 20 destination interface ethernet 0/1
write memory

or (It depends on the OS you are using):

monitor session 20
source vlan 99 tx
destination interface ethernet 0/1
write memory

upvoted 7 times

Klimy 1 month, 2 weeks ago

So we mirror the traffic of the VLAN to Ethernet0/1 which is part of a Port channel and on the other side connected to a switchport. Khhmm. Realistic :-)

upvoted 1 times

JackDRipper 8 months, 3 weeks ago

When it says "Configure the devices according to the topology to achieve these goals", does it include setting up things like routing, etherchannel and whatnot? Or is the topology already built, complete and operational, and we only need to do specifically what is being asked under Tasks?

upvoted 1 times

gibblock 8 months, 3 weeks ago

Topology is already configured. Apply only the configuration you are asked for.

upvoted 3 times

gibblock 9 months ago

Correct configuration should be
ip sla 10
icmp-echo 1.1.1.1 source-ip 172.16.2.2
threshold 250
timeout 3000
frequency 5
ip sla schedule 10 life forever start-time now

Keep in mind that "ip sla schedule 10 ..." is a separate command that activates the SLA.
Furthermore do not forget to append "start-time" otherwise the scheduler does not start.

upvoted 3 times

gibblock 9 months ago

and of course

copy running startup

upvoted 2 times

HungarianDish 9 months, 1 week ago

I encountered a problem when performing the first task, SPAN in my lab in CML. Under "monitor session 20 source... or source interface...", I do not have the option for "interface vlan...".
The solution suggests to use "interface vlan 99" as the source. However, only the commands "source vlan..." or "source interface GigabitEthernet... or Port-channel..." are given in the IOS that I am using. I read about this topic, and "interface vlan..." does not seem to be offered as the source in the SPAN configuration generally.

SW01(config)#monitor session 20 source ?
interface SPAN source interface
remote SPAN source Remote
vlan SPAN source VLAN

SW01(config)#monitor session 20 source interface ?
GigabitEthernet GigabitEthernet IEEE 802.3z
Port-channel Ethernet Channel of interfaces

Did someone successfully test the solution?

upvoted 2 times

HungarianDish 9 months, 1 week ago

This is what I can set in my lab:

SW01(config)#monitor session 20 source vlan 99 tx

upvoted 2 times

gibblock 9 months ago

I tried it on a 3750 and 3850 and the "interface vlan" option was missing. You can only choose between interface or vlan.Not 100% sure if it's a limitation by the emulators I am using (including my hardware as well) or it should be that way.
I guess the latter one.

upvoted 1 times

jorgeoscar90 9 months, 1 week ago

ip sla 10
icmp-echo 1.1.1.1 source-ip 172.16.2.2
threshold 250
timeout 3000
frequency 5
ip sla schedule 10 life forever

upvoted 1 times

An engineer applies this EEM applet to a router:

```
event manager applet Test
  event timer watchdog time 600
  action 1.0 cli command "enable"
  action 2.0 cli command "term exec prompt timestamp"
  action 3.0 cli command "term length 0"
  action 4.0 cli command "show ip arp | in 0005.4319.7489"
  action 5.0 regexp ".*(ARPA).*" $_cli_result
  action 6.0 if $_regexp_result eq 1
  action 7.0 syslog msg $_cli_result
  action 8.0 end
```

What does the applet accomplish?

A. It generates a syslog message every 600 seconds on the status of the specified MAC address.

B. It compares syslog output to the MAC address table every 600 seconds and generates an event when no match is found.

C. It compares syslog output to the MAC address table every 600 seconds and generates an event when there is a match.

D. It checks the MAC address table every 600 seconds to see if the specified address has been learned.

Correct Answer: *D*

Community vote distribution

D (62%) A (33%) 5%

mgiuseppe86 3 months, 4 weeks ago

It's A

Read Engish.

It generates a syslog message.

None of the other answers say that. and action 7 generates a syslog message.

I tested this in my lab.

D does NOT check a mac address table, it checks the arp table.

upvoted 3 times

Chuckzero 4 months, 1 week ago

The correct answers are A and D.

This question should have a (choose two) options answer. They must have forgotten to say, "choose two".

The EEM script does A and D.

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: D

A. It DOESN'T generate a syslog message every 600 seconds - if only MAC exists
B. it DOESN'T It compare syslog output- it compares cli output
C. It DOESN'T compare syslog output - it compares cli output
D. It DOESN'T check the MAC address table - it checks ARP

upvoted 1 times

artemiwwe 5 months, 2 weeks ago

Poorly described ansers :(None is correct. It does not *generete every 600 seconds*, it *checks every 600 seconds* if the MAC address is present in ARP table, and *IF* it is present, generates syslog.
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-16/216091-best-practices-and-useful-scripts-for-ee.html
Useful EEM Scripts -> Track Specific MAC Address for MAC Address Learn

upvoted 1 times

Dv123456 5 months, 2 weeks ago

THe most probable answer is A:
B and C-> Seems there si no such a syslog output to compare with.
D - > The check is made in the arp table, not in the mac address-table

upvoted 1 times

rogue_user 6 months ago

D is wrong since it checks ARP table

upvoted 1 times

danman32 6 months ago

Answer A seems plausible but it says a syslog message is generated every 600 seconds, reporting the status (exists or not) of the MAC address. But that's not what the script is doing. A syslog message is generated ONLY if the MAC address is found.'

I agree with those pointing out that answers B-D are addressing the MAC table, which isn't quite right. It is the ARP table that is checked. But that's Cisco for you. Best fit if you overlook table terminology is answer D.

upvoted 1 times

danman32 6 months ago

Plus answers B and C assume the script is checking syslog messages. It doesn't CHECK syslog messages, it GENERATES a syslog message IF. And the IF check is done every 600 seconds.

upvoted 1 times

CKL_SG 6 months, 2 weeks ago

Selected Answer: D

Tested in GNS3
syslog message is generated only if the specific MAC address is found, it's not generated every 600 seconds. If the MAC isn't found, no syslog message is generated.

upvoted 2 times

TroyMcLure 6 months, 2 weeks ago

Selected Answer: D

This one is tricky. Please, pay attention to the wordings.
With the command “show ip arp | in 0005.4278.9866”, the “ARPR” text is only found if this MAC address has been learned in the router.
Answer A is not correct as the syslog message is only generated if the specific MAC address is found (not every 600 seconds).

upvoted 4 times

Entivo 6 months, 3 weeks ago

Selected Answer: D

Burik is correct, the answer is D.

upvoted 1 times

Burik 6 months, 4 weeks ago

Selected Answer: D

It's D. The ARP table is checked every 600 seconds, but the syslog message is generated only if the specific MAC address is found, it's not generated every 600 seconds. If the MAC isn't found, no syslog message is generated.

if $_regexp_result eq 1 <-- if the MAC is found...
syslog msg $_cli_result <-- ...then generate a syslog entry, otherwise do nothing

upvoted 3 times

Splashisthegreatestmovie 7 months ago

Answers A and D are splitting hairs to me

upvoted 1 times

Burik 6 months, 4 weeks ago

They are not. This question wants to check our knowledge of the use of the IF statement in EEM applets. Answer A is wrong because Action 7.0 will run only *IF* Action 6.0 returns 1. The answer is D.

upvoted 1 times

JackDRipper 9 months, 1 week ago

Selected Answer: A

B and C are obviously wrong.
D seems correct at first glance, but the EEM is reading the ARP table, not the MAC address table
A is the only valid answer.

upvoted 2 times

Burik 6 months, 4 weeks ago

So what? The show ip arp command shows MAC addresses as well. It's D.

upvoted 2 times

HungarianDish 9 months, 1 week ago

Selected Answer: A

The question is based on this:
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-16/216091-best-practices-and-useful-scripts-for-ee.html

"Useful EEM Scripts

Track Specific MAC Address for MAC Address Learn
...
If the MAC is seen, the script takes these actions:
outputs a syslog message"

syslog msg $_cli_result => display syslog message if MAC is found, so answer A) as others concluded in earlier posts.
upvoted 1 times

Burik 6 months, 4 weeks ago

No. Action 6.0 makes it so that action 7.0 runs only if the MAC is found, so the syslog entry is generated only if the MAC address is found. It's D.
upvoted 1 times

DavideDL 9 months, 2 weeks ago

Selected Answer: D

I'm not an applet expert but for what I can understand the script generate a syslog message every 600s ONLY if the MAC Address: 0005.4319.7489 is in the ARP table.
For this reason I would exclude A.

B and C are wrong because It doesn't compare a syslog output.

D It isn't completely correct but seems OK to me... It checks the *ARP table...

My €0.02
upvoted 2 times

Burik 6 months, 4 weeks ago

Which contains MAC addresses as well.
upvoted 1 times

Nickplayany 9 months, 3 weeks ago

Selected Answer: A

It´s A!!

I have been checking that and the applet checks the status of the specified MAC in the ARP table every 600 seconds and generates a syslog message when the address is found
upvoted 2 times

Burik 6 months, 4 weeks ago

So it's D. The ARP table is checked every 600 seconds, but the syslog message is generated only if the specific MAC address is found (not every 600 seconds). If the MAC isn't found, no syslog message is generated.
upvoted 2 times

Bluntedcase 6 months, 4 weeks ago

I agree. For me D makes sense
upvoted 1 times

Nickplayany 9 months, 3 weeks ago

Selected Answer: C

It could be C but if someone is more expert please check that.

It is checking the ARP

action 5.0 regexp "ARPA" "$_cli_result" -> That compares the results of the previous CLI command "$_cli_result" with the string ARPA

if $_regexp_result eq 1 That means -> when it is successful

syslog msg $_cli_result That means -> Sends the ARPA status message which got from the CLI command, to the syslog, or to the screen if you are consoled in
upvoted 1 times

Nickplayany 9 months, 3 weeks ago

It´s A!!

I have been checking that and the applet checks the status of the specified MAC in the ARP table every 600 seconds and generates a syslog message when the address is found

As I can see C says event which is the mistake and the tricky part
upvoted 1 times

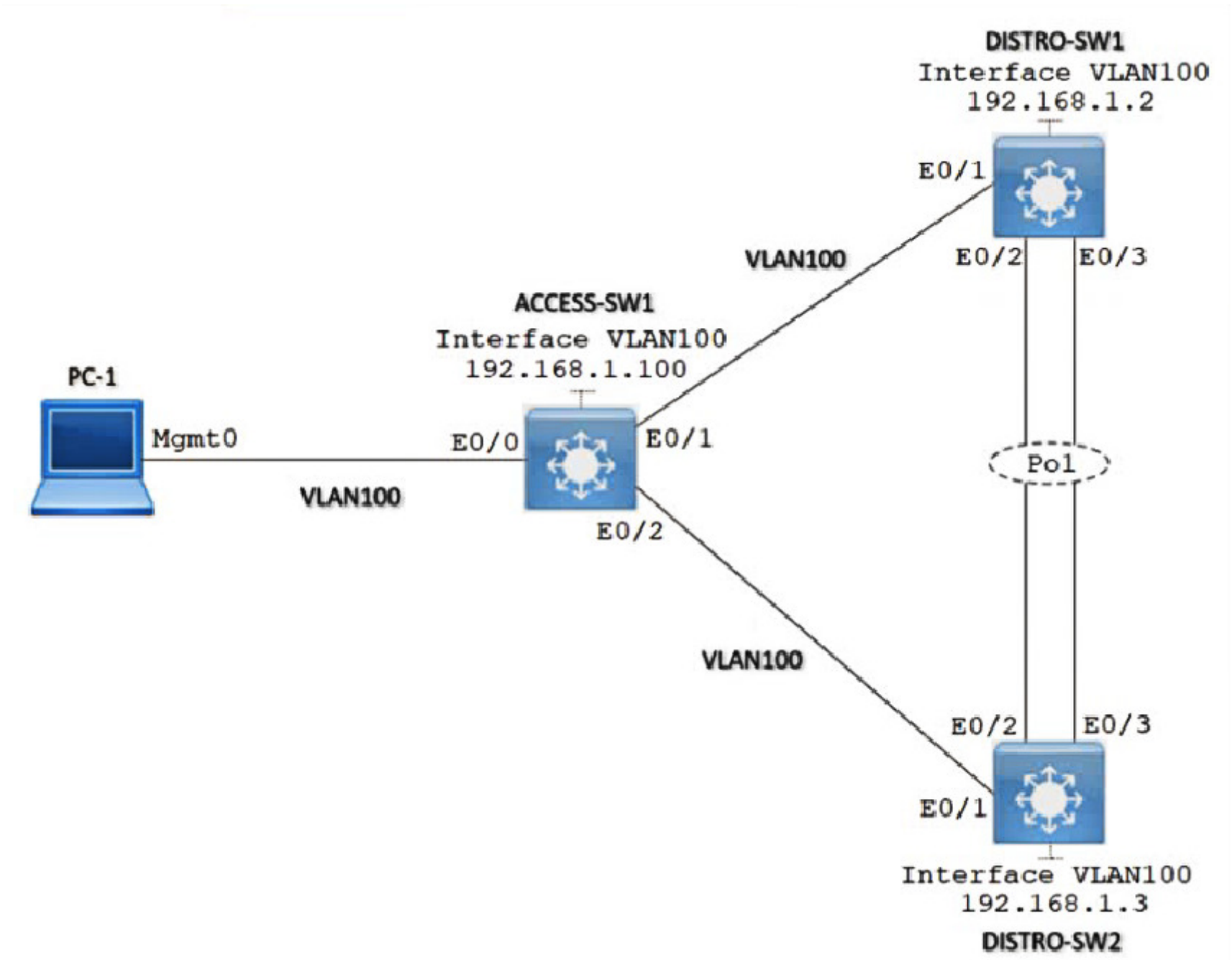
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

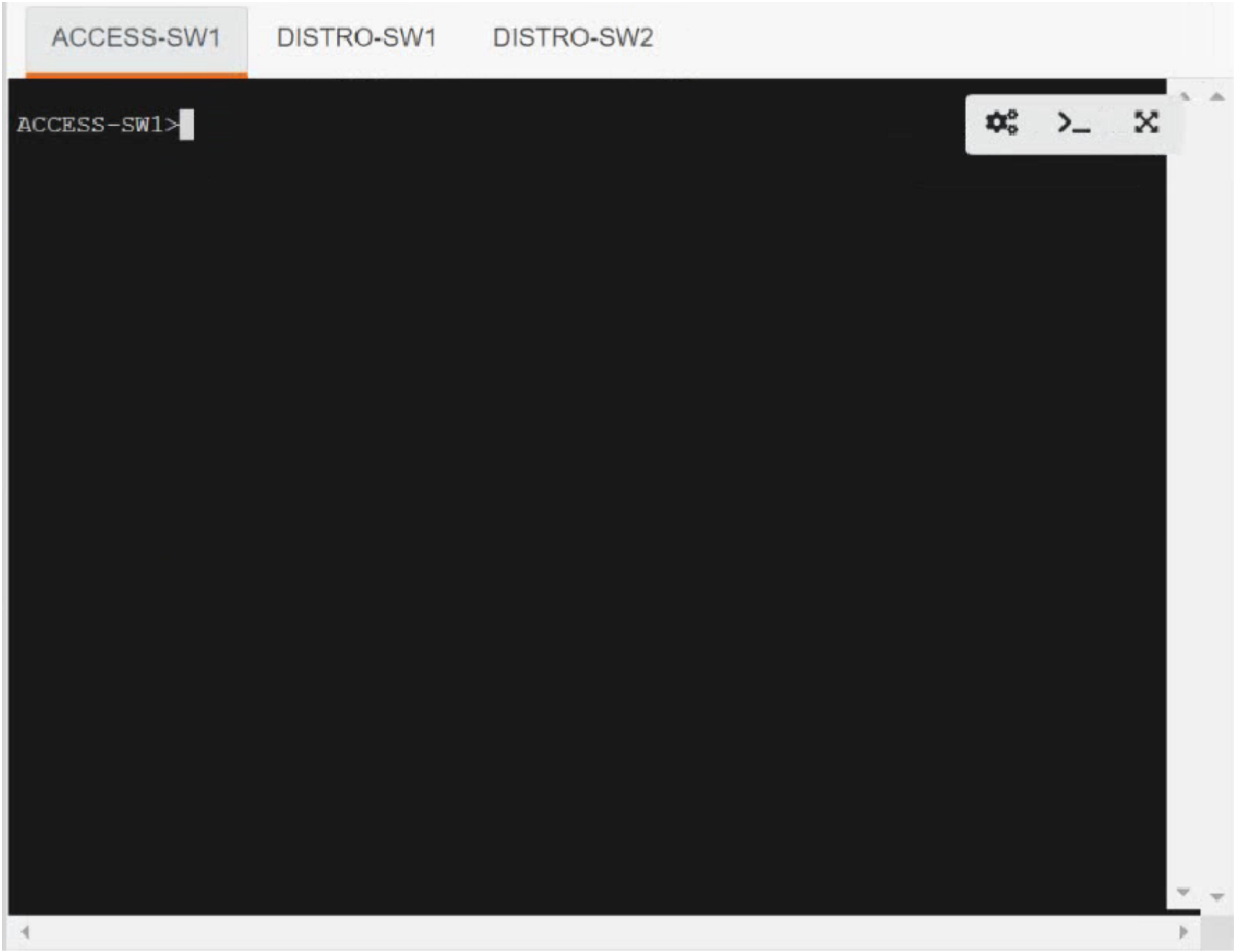
Topology
-

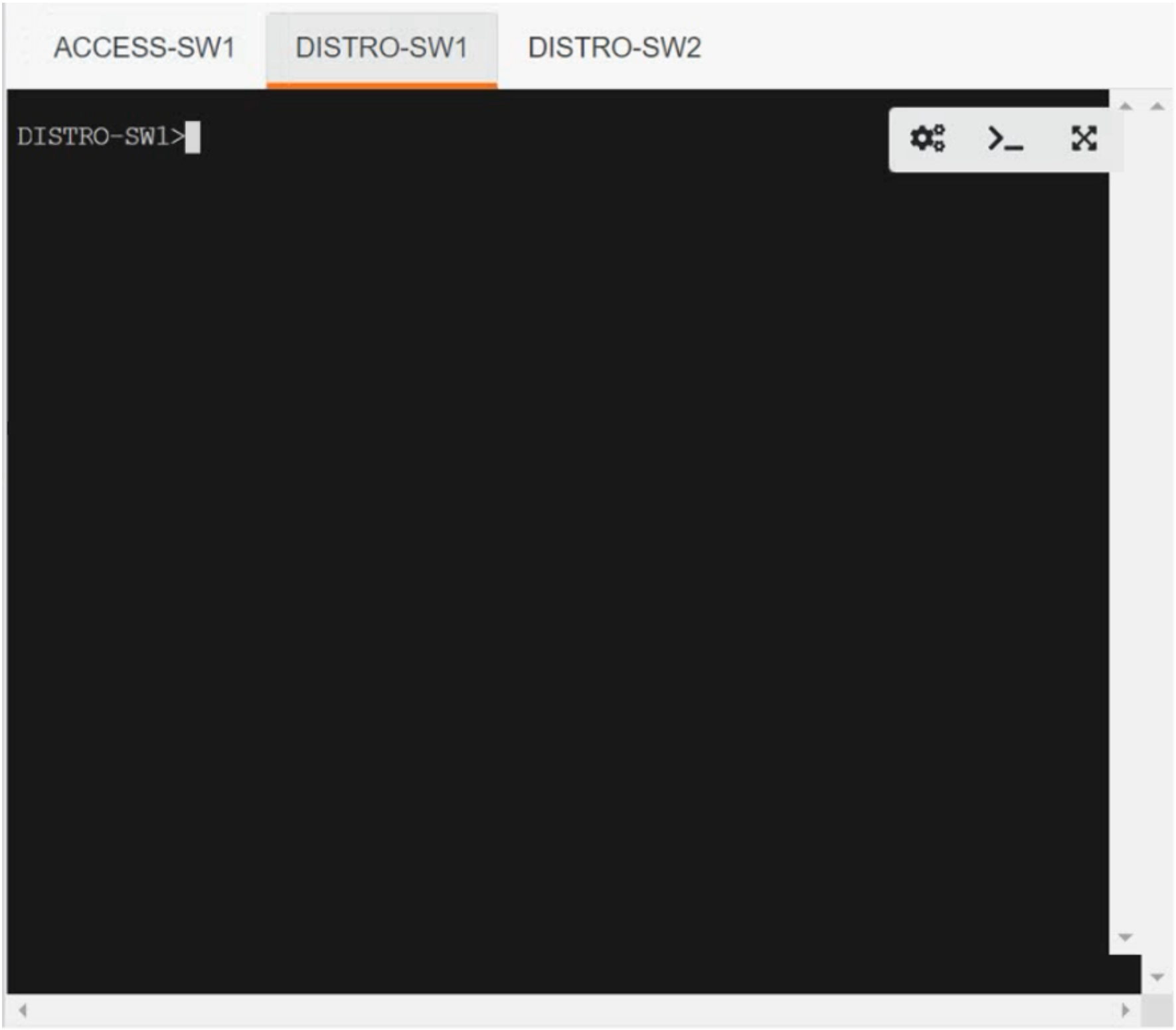


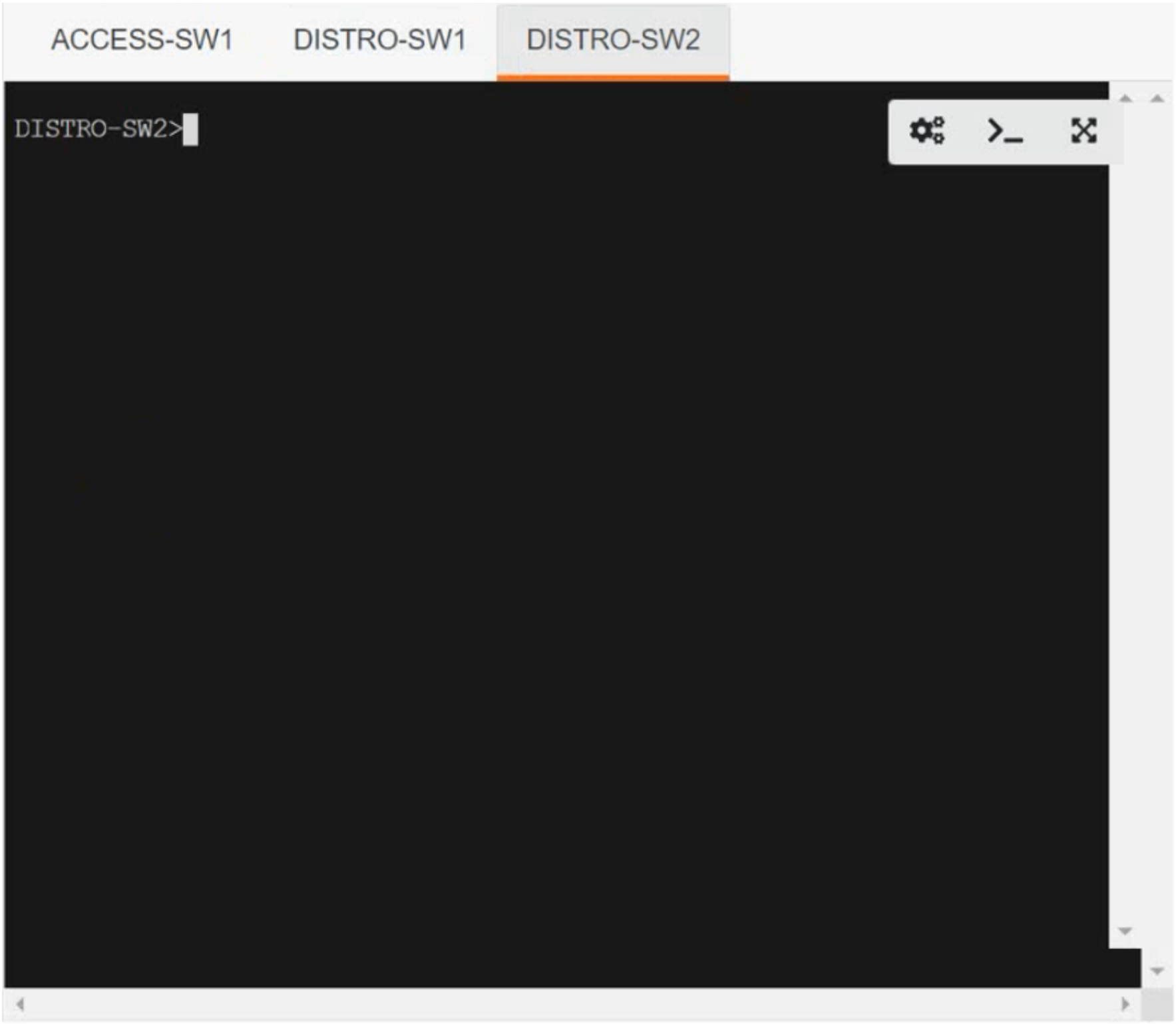
Tasks
-

Implement GLBP between DISTRO-SW1 and DISTRO-SW2 on VLAN100 for hosts connected to ACCESS-SW1 to achieve these goals:

1. Configure group 30 using the virtual IP address of 192.168.1.254.
2. Configure DISTRO-SW1 as the AVG using a priority value of 130.
3. If DISTRO-SW1 suffers a failure and recovers, ensure that it automatically resumes the AVG role after waiting for a minimum of 35 seconds.




ACCESS-SW1
DISTRO-SW1
DISTRO-SW2
DISTRO-SW1>



Correct Answer:

DISTRO-SW1

```
int vlan 100
glbp 30 ip 192.168.1.254
glbp 30  priority 130
glbp 30  timers 5 35
glbp 30  preempt
copy run start
```

DISTRO-SW2

```
int vlan 100
glbp 30  ip 192.168.1.254
glbp 30  timers 5 35
glbp 30  preempt
copy run start
```

olaniyijt Highly Voted 8 months, 3 weeks ago

Primary Switch:
interface Vlan100
ip address 192.168.1.2 255.255.255.0
glbp 30 ip 192.168.1.254
glbp 30 priority 130
glbp 30 preempt delay minimum 35
end

Secondary Switch:
interface Vlan100
ip address 192.168.1.3 255.255.255.0

glbp 30 ip 192.168.1.254

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/Configuring-GLBP.html
upvoted 17 times

larsis Highly Voted 9 months ago
Tbh I wouldn't touch the counters. I think they want us to configure preempt delay instead:
Primary SW:
glbp 30 ip 192.168.1.254
glbp 30 priority 130
glbp 30 preempt delay minimum 35

Secondary SW:
glbp 30 ip 192.168.1.254
upvoted 7 times

MJane 9 months ago
i actually would put the preempt command with the delay on the second too, just in case the second boots up first and takes the active role
upvoted 1 times

JackDRipper 8 months, 3 weeks ago
The way I understand it is, SW1 has a higher priority + preempt so as soon as it is up, it will count 35 seconds then take over the Active role from SW2.
upvoted 3 times

HungarianDish 9 months ago
You are right! Thank you!
upvoted 1 times

sledgey121 Most Recent 6 days, 2 hours ago
Just passed but had 3 labs that are not detailed on this site. All good though and should be well within the capabilities of CCNA/CCNP network engineers.
upvoted 1 times

danman32 6 months ago
I agree, hold timer manipulation is not the means of delaying preempt.
The hold time is when an AVG will determine a failure has occurred.
If the question was asked to delay action on failure, then managing the timers would be appropriate, though in real world probably not ideal.
But criteria is about the primary delaying taking back AVG role.

Question #755 *Topic 1*

/ AVG)

Which authorization framework gives third-party applications limited access to HTTP services?

A. IPsec

B. GRE

C. Basic Auth

D. OAuth 2.0

Correct Answer: *D*

HungarianDish 9 months ago
Seems to be correct.

https://auth0.com/docs/authenticate/protocols/oauth
"The OAuth 2.0 authorization framework is a protocol that allows a user to grant a third-party web site or application access to the user's protected resources, without necessarily revealing their long-term credentials or even their identity."

https://auth0.com/intro-to-iam/what-is-oauth-2
"...is a standard designed to allow a website or application to access resources hosted by other web apps on behalf of a user."
upvoted 3 times

Active is local, weighting 100
Forwarder 2
State is Listen
MAC address is 0007.b400.1e02 (learnt)
Owner ID is 5254.001a.8064
Time to live: 14400.000 sec (maximum 14400 sec)

Question #756 *Topic 1*

How does Cisco Express Forwarding switching differ from process switching on Cisco devices?

A. Cisco Express Forwarding switching saves memory by storing adjacency tables in dedicated memory on the line cards, and process switching stores all tables in the main memory.

B. Cisco Express Forwarding switching uses adjacency tables built by the CDP protocol, and process switching uses the routing table.

C. Cisco Express Forwarding switching uses dedicated hardware processors, and process switching uses the main processor.

D. Cisco Express Forwarding switching uses a proprietary protocol based on IS-IS for MAC address lookup, and process switching uses the MAC address table.

Correct Answer: *A*

Community vote distribution

C (75%) A (25%)

connorm 3 months, 3 weeks ago

Cisco Express Forwarding (CEF) is a switching technology used in Cisco devices to improve packet forwarding efficiency. It is a Layer 3 IP switching technology that uses dedicated hardware processors (such as ASICs - Application-Specific Integrated Circuits) to make forwarding decisions based on information in the Forwarding Information Base (FIB) and Adjacency Table. CEF offloads packet switching from the main CPU, which allows for faster and more efficient packet forwarding.

In contrast, process switching involves the main processor (CPU) of the router or switch making forwarding decisions for each packet. This method is less efficient and can result in higher CPU utilization, especially in high-traffic environments. Process switching doesn't rely on dedicated hardware processors for forwarding decisions.

Option C accurately describes the difference between Cisco Express Forwarding and process switching, as CEF uses dedicated hardware processors, while process switching relies on the main CPU. The other options do not accurately describe the key differences between the two switching methods.

upvoted 1 times

pc_evans 4 months ago

Distributed CEF (dCEF) mode - When dCEF is enabled, line cards maintain identical copies of the FIB and adjacency tables. The line cards can perform the express forwarding by themselves, and this relieves the main processor - Gigabit Route Processor (GRP) - of involvement in the switching operation. This is the only switching method available on the Cisco 12000 Series Router.

https://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: C

dedicated hardware processor means packet processing ASIC

upvoted 1 times

ALOVEVIKS 7 months, 3 weeks ago

Selected Answer: C

I think C

upvoted 1 times

Chiaretta 8 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

Nickplayany 8 months, 2 weeks ago

Selected Answer: C

I would go with C

upvoted 1 times

JackDRipper 8 months, 4 weeks ago

Selected Answer: A

CEF uses CAM to store the FIB and the Adjacency Table. Process switching uses the RIB, which is stored in RAM.
C to me is incorrect because CEF utilizes an ASIC, not a dedicated processor.

upvoted 2 times

HungarianDish 9 months ago

Selected Answer: C

C) Correct

https://www.networkfashion.net/l3-forwarding-techniques-process-switching-fast-switching-cef/
"When the forwarding engine is decoupled from the RP and located in the line cards, then the forwarding decision is made there and is not passed to the route processor. "

However "dedicated hardware processors" is not the appropriate terminology, this answer fits best.
There are different terms for this technology, like Superviser Engine, forwarding engine, L3 engine, Network Processing Unit...

upvoted 2 times

HungarianDish 9 months ago

A) Wrong -> An advantage of CEF is the lower CPU usage and not the lower memory usage
https://community.cisco.com/t5/routing/enabling-cef-question/td-p/2041858

https://networkengineering.stackexchange.com/questions/48699/cisco-catalyst-switching-with-supervisor-and-line-cards

dCEF:
"When distributed Cisco Express Forwarding is enabled, line cards maintain an identical copy of the FIB and adjacency tables.
The line cards perform express forwarding between port adapters, thus relieving the RP of involvement in the switching operation. "

Same here:
https://study-ccnp.com/cisco-express-forwarding-cef-overview/

B) Worng -> Adjacency table contains information mainly learned from from ARP table.
https://www.networkfashion.net/l3-forwarding-techniques-process-switching-fast-switching-cef/

D) It is not worth mentioning.

upvoted 2 times

Question #757 *Topic 1*

```
1   def main():
2       vlans_list = [10, 20, 30]
3       add_vlans(vlans_list)
4       print(vlans_list)
5   def add_vlans(vlans):
6       for i in range(len(vlans)):
7           vlans[i]+=100
8
9   if __name__ == '__main__':
10      main()
```

Refer to the exhibit. What is the result of running this code?

A. A list of lists is created.

B. A list of new VLANs is created.

C. An error is displayed.

D. A dictionary is created.

Correct Answer: *B*

Community vote distribution

B (83%) C (17%)

HarwinderSekhon 6 months, 1 week ago

Tested

vlans_list = [10, 20, 30]

def add_vlans(vlans):
for i in range(len(vlans)):
vlans[i]+=100

add_vlans(vlans_list)

print(vlans_list)
[110, 120, 130]

upvoted 1 times

MJane 9 months ago

Selected Answer: B

tried it online. the thing is that the vars are referenced and not sent by value.
def main():
vlans_list = [10, 20, 30]
add_vlans(vlans_list)
print(vlans_list)
def add_vlans(vlans):
for i in range(len(vlans)):
vlans[i]+=100

if _name_ == '_main_':
main()

upvoted 1 times

DavideDL 9 months ago

Selected Answer: B

vlans_list is a python list contaning the numbers: 10 , 20 and 30 (as integers)

The function "add_vlans" scan the list and 100 to every item.
The result should be:
[110, 120, 130]

So in my opinion the answer should be:
[B] - A list of new VLANs is created.

upvoted 3 times

JackDRipper 9 months ago

Selected Answer: B

```
def main():
vlans_list = [10,20,30]
add_vlans(vlans_list)
print(vlans_list)
def add_vlans(vlans):
for i in range(len(vlans)):
vlans[i]+=100

if __name__=='__main__':
main()
```

==========OUTPUT==========

[110, 120, 130]

upvoted 1 times

HungarianDish 9 months ago

Selected Answer: C

Run in Visual Studio. In this for it always throws an error.

"NameError: name '_name_' is not defined"

Could someone double check this please?

upvoted 1 times

MJane 9 months ago

you are missing an _. there should be 2x_

upvoted 2 times

```
Cat9300(config)# monitor session 1 type erspan-source
Cat9300(config-mon-erspan-src)# source interface Gi1/0/3
Cat9300(config-mon-erspan-src)# destination
Cat9300(config-mon-erspan-src-dst)# erspan-id 1
Cat9300(config-mon-erspan-src-dst)# ip address 198.51.100.123
Cat9300(config-mon-erspan-src-dst)# origin ip address 10.4.255.100
Cat9300(config-mon-erspan-src-dst)# do ping 198.51.100.123 source 10.4.255.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.123, timeout is 2 seconds:
Packet sent with a source address of 10.4.255.100
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Refer to the exhibit. The administrator configures an ERSPAN session, but no packets are received on the destination host. Which action is required to complete the configuration?

A. Ensure that the ERSPAN destination addresses are not reachable through the Mgmt-vrf VRF.

B. Ensure that the ERSPAN destination is reachable from the switch.

C. Configure the ERSPAN destination VLAN as an RSPAN VLAN.

D. Enable the ERSPAN session.

Correct Answer: *D*

Community vote distribution

D (100%)

HungarianDish Highly Voted 9 months ago

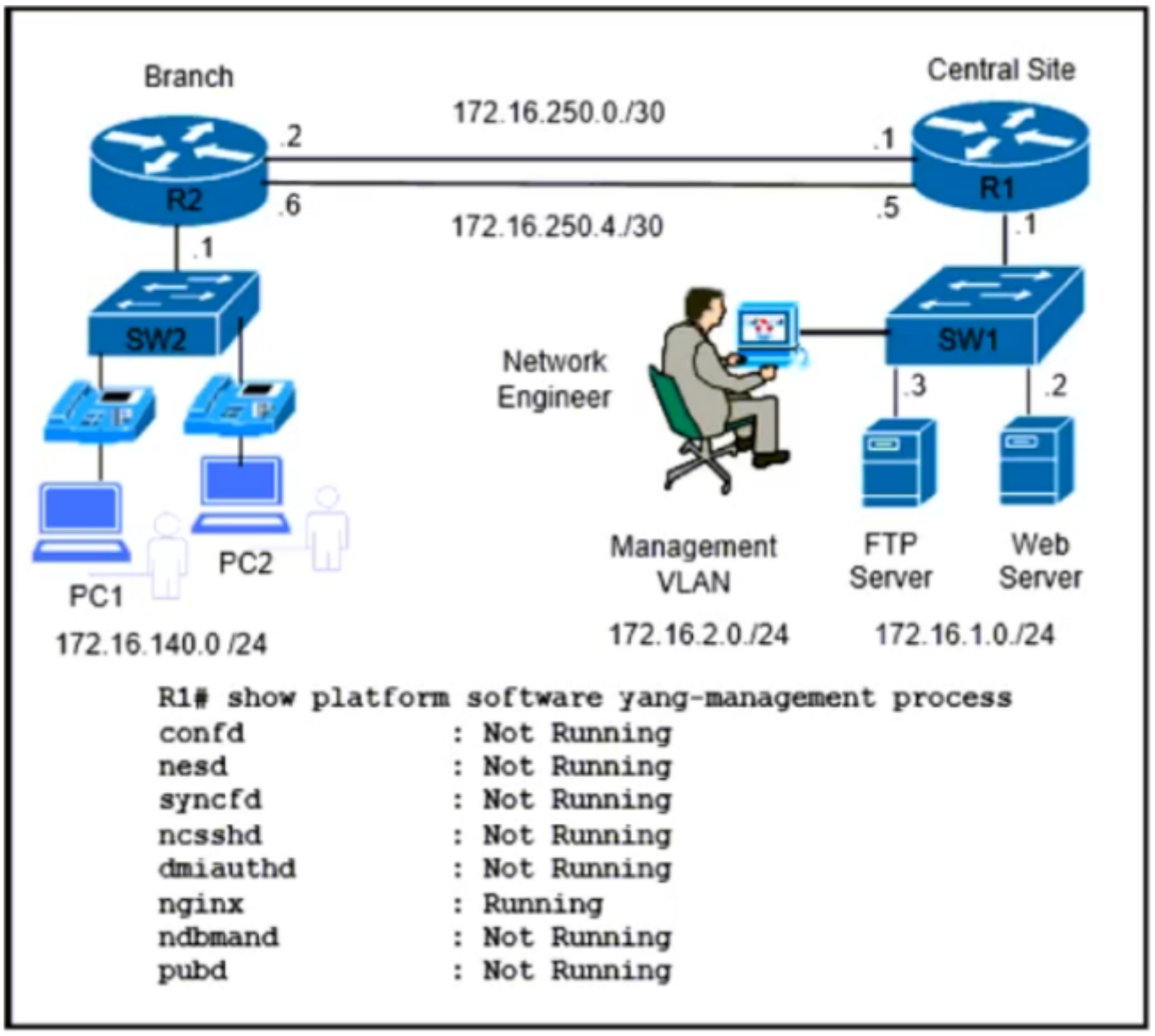
Selected Answer: D

"Finally, enable the session using the 'no shutdown' command to guarantee it is active."

https://study-ccnp.com/erspan-encapsulated-remote-span-explained/

upvoted 12 times

Question #759 *Topic 1*



Refer to the exhibit. Which command is required on router R1 to start receiving RESTCONF requests?

A. R1(config)# ip http accounting commands 12 default

B. R1(config)# ip http server

C. R1(config)# restconf

D. R1(config)# ip http access-class 12

Correct Answer: *C*

Community vote distribution

C (100%)

HungarianDish Highly Voted 9 months ago

Selected Answer: C

The example is taken exactly from this document:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/167/b_167_programmability_cg/restconf_programmable_interface.pdf

Section "Verifying RESTCONF Configuration"

"The nginx process gets restrated and DMI process are started, when the restconf command is configured
...
After AAA and the RESTCONF interface is configured, and nginx process and relevant DMI processes are running; the device is ready to receive RESTCONF requests."

upvoted 5 times

Asombrosso Most Recent 4 months, 1 week ago

Selected Answer: C

Device(config)# restconf
//Enables the RESTCONF interface on your
network device.

upvoted 1 times

Question #760 *Topic 1*

What is a command-line tool for consuming REST APIs?

A. Python requests

B. Postman

C. cURL

D. Firefox

Correct Answer: *C*

Community vote distribution

C (91%) 9%

Asombrosso 4 months, 1 week ago

Selected Answer: C

cURL is CLI-only

upvoted 2 times

MJane 9 months ago

Selected Answer: C

curl is a command-line tool for transferring data, and it supports about 22 protocols, including HTTP. This combination makes it a very good ad-hoc tool for testing our REST services.

upvoted 3 times

JackDRipper 9 months ago

Selected Answer: C

Postman comes in both GUI and CLI versions, making this question vague. However, cURL is CLI-only, so I'll have to go with C.

upvoted 4 times

DavideDL 9 months ago

Selected Answer: C

I think C is correct:
https://blog.hubspot.com/website/curl-command

(cURL, pronounced “curl”) is a command line tool that enables data exchange between a device and a server through a terminal.

I don't think Postman is a command line software....

upvoted 1 times

larsis 9 months ago

Selected Answer: B

Isn't it Postman for REST?

upvoted 1 times

JackDRipper 9 months ago

cURL is CLI-only while Postman comes in both GUI and CLI. I get what you mean, though. The way these questions are written, the world makes no sense no more.

upvoted 1 times

Question #761 *Topic 1*

An engineer receives a report that an application exhibits poor performance. On the switch where the server is connected, this syslog message is visible: SW_MATM-4-MACFLAP_NOTIF: Host 0054.3962.7651 in vlan 14 is flapping between port Gi1/0/1 and port Gi1/0/2.

What is causing the problem?

A. undesirable load-balancing configuration on the switch

B. invalid port channel configuration on the switch

C. wrong SFP+ and cable connected between the server and the switch

D. failed NIC on the server

Correct Answer: *A*

Community vote distribution

B (73%) D (27%)

Asombrosso 4 months, 1 week ago

Selected Answer: B

On IOS-based switches, if the physical member ports of an EtherChannel do not successfully negotiate the bundling through LACP, they will continue operating as individual ports. That can lead to MAC flap scenarios indeed.

upvoted 1 times

rogue_user 6 months ago

Selected Answer: D

You can't bring LACP with switch up when ports are not in PO. When you have server NICs TEAMed/BONDed, they run active/standby and switch only learns MAC on Active side. If Active NIC bounces, MAC will bounce as well.

upvoted 1 times

Burik 6 months, 4 weeks ago

Selected Answer: B

It's B. This is a scenario where you have two interfaces bonded together on the server, but there is no valid port channel configuration on the switch. This way the server will send always the same MAC on both interfaces, which will appear twice on the switch on both its G1/0/1 and G1/0/2 ports, rather than only once on its port-channel interface.

A is wrong, actually misleading, as if anything you'd have to change load balancing on the server as a rough workaround, not on the switch.

C is wrong as the interface[s] would be down, therefore no MAC flapping would occur.

D is wrong as the interface[s] would be down as well.

upvoted 3 times

danman32 6 months, 3 weeks ago

I was going to choose A, since the load balancing configuration for port-channel on the switch would dictate which port was used for the MAC.
But you made a good point that the flapping is based on ingress learned MAC which would be controlled by the server.
I believe too that if 2 interfaces were bundled into port-channel, then the switch would not consider the MAC appearing on two member interfaces as flapping.

upvoted 1 times

wanta 7 months, 3 weeks ago

Selected Answer: D

A. undesirable load-balancing configuration on the switch - Probably NOT
B. invalid port channel configuration on the switch - Possibly, although nothing to suggest a Po is actually configured.
C. wrong SFP+ and cable connected between the server and the switch - Probably NOT
D. failed NIC on the server - This is the most likely, with the server set up for active/backup NICs, and the primary fails.

The logs don't suggest that the event keeps on happening, so it's a one time event where the primary server NIC dies and fails over.

upvoted 2 times

MJane 9 months ago

Selected Answer: B

I also vote for B cause it states that the server is connected to the switch and those are the links with the problem. But it can also be A or D :)

upvoted 2 times

JackDRipper 9 months ago

I'm leaning towards B...
https://support.hpe.com/hpesc/public/docDisplay?docId=c02936677

Can anyone confirm if misconfiguring the "port-channel load-balance xxx" can result in MAC flapping? If so, then the answer could be A, especially since it's obviously a LAG/bonded/teaming connection to a server/host.

upvoted 1 times

rogue_user 6 months ago

mac stays on PO regardless of the load balancing method, that affects only hashing

upvoted 1 times

DavideDL 9 months ago

Selected Answer: B

I'm a bit doubtful on this question....
To me sounds good B because if the EtherChannel has not been established (for some misconfiguration), and the switch still treats the ports as individual ports while the other end is already using them as a bundle We have MAC flapping...

https://learningnetwork.cisco.com/s/question/0D53i00000Kt7h8CAB/mac-address-flapping-on-port-channel

upvoted 2 times

DRAG DROP

-

Drag and drop the snippets onto the blanks within the code to construct a script that brings up the failover Ethernet port if the primary port goes down and also shuts down the failover port when the primary returns to service. Not all options are used.

Answer Area

```
event manager applet SRV-1-Up
 event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9, changed state to [          ]"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "Interface GigabitEthernet3/0/10"
 action 4.0 cli command "no shutdown"
action 5.0 cli command "end"
event manager applet SRV-1-Down
 event syslog pattern "Line protocol on Interface [          ], changed state to up"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "Interface GigabitEthernet3/0/10"
 action 4.0 cli command "[          ]"
action 5.0 cli command "end"
```

Shutdown | Up | GigabitEthernet3/0/10

No shutdown | Down | GigabitEthernet4/0/9

Correct Answer:

Answer Area

```
event manager applet SRV-1-Up
 event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9, changed state to [Down]"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "Interface GigabitEthernet3/0/10"
 action 4.0 cli command "no shutdown"
action 5.0 cli command "end"
event manager applet SRV-1-Down
 event syslog pattern "Line protocol on Interface [GigabitEthernet4/0/9], changed state to up"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "Interface GigabitEthernet3/0/10"
 action 4.0 cli command "[Shutdown]"
action 5.0 cli command "end"
```

Shutdown | Up | GigabitEthernet3/0/10

No shutdown | Down | GigabitEthernet4/0/9

JackDRipper Highly Voted 9 months ago

- Down
- GigabitEthernet4/0/9
- Shutdown

upvoted 9 times

tempaccount00001 Most Recent 6 months, 1 week ago

yup, makes perfect sense, answer is correct
Down
gig4/0/9
shut

upvoted 3 times

```
R2#show ip ospf neighbor

R2#show ip ospf interface fastEthernet 1/1
FastEthernet1/1 is up, line protocol is up
  Internet Address 192.168.0.5/30, Area 0
  Process ID 1, Router ID 10.0.0.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.0.0.5, Interface address 192.168.0.5
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R2#ping 192.168.0.6 df-bit size 1500

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 192.168.0.6, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/16 ms
```

```
R3#show ip ospf neighbor

R3#show ip ospf interface fastEthernet 1/1
FastEthernet1/1 is up, line protocol is up
  Internet Address 192.168.0.6/29, Area 0
  Process ID 1, Router ID 10.0.0.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.0.0.3, Interface address 192.168.0.6
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R3#ping 192.168.0.5 df-bit size 1500

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 192.168.0.5, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/20 ms
```

Refer to the exhibit. Why does the OSPF neighborship fail between the two interfaces?

A. The MTU is not the same.

B. The OSPF timers are different.

C. There is a mismatch in the OSPF interface network type.

D. The IP subnet mask is not the same.

Correct Answer: *D*

Community vote distribution

D (100%)

Jack2002 9 months ago

Selected Answer: D

Answer D is correct

upvoted 1 times

JackDRipper 9 months ago

Selected Answer: D

R2: /30 vs R3: /29

upvoted 3 times

Question #764 *Topic 1*

Which technology enables a redundant supervisor engine to take over when the primary supervisor engine fails?

A. SSO

B. FHRP

C. graceful restart

D. NSF

Correct Answer: *A*

Community vote distribution

A (100%)

tsamoko 4 months ago

Selected Answer: A

ok is A .
https://community.cisco.com/t5/switching/difference-between-nsf-and-sso/td-p/2262550#:~:text=NSF%20Operation,following%20a%20supervisor%20engine%20switchover.

upvoted 1 times

JackDRipper 9 months ago

Selected Answer: A

SSO is the base technology that has this capability at L-2. NSF sits on top of SSO to extend the same capability to L-3.

upvoted 2 times

Question #765 *Topic 1*

A customer requires their wireless data traffic to egress at the switch port of the access point. Which access point mode supports this?

A. FlexConnect

B. Sniffer

C. Bridge

D. Monitor

Correct Answer: *A*

Community vote distribution

A (100%)

JackDRipper Highly Voted 9 months ago

Selected Answer: A

https://study-ccnp.com/cisco-wireless-access-point-ap-modes-explained/
"FlexConnect Mode
FlexConnect AP mode enables switching traffic between an SSID and a VLAN locally if the CAPWAP to the WLC is down, even when the AP is at a remote site. It can also be configured to egress at the access point's LAN port."

upvoted 6 times

Question #766 *Topic 1*

What is a capability of the Cisco DNA Center southbound API?

A. It adds support for managing non-Cisco devices from Cisco DNA Center.

B. It connects to ITSM services such as ServiceNow.

C. It sends webhooks from Cisco DNA Center when alerts are triggered.

D. It allows administrators to make API calls to Cisco DNA Center.

Correct Answer: *A*

Community vote distribution

A (100%)

JackDRipper Highly Voted 8 months, 3 weeks ago

Selected Answer: A

Answer A is correct.
Southbound—Multivendor Support APIs/SDK:
The Cisco DNA Center Multivendor SDK allows partners to add support for managing non-Cisco devices directly from Cisco DNA Center.
https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitive-advantage

upvoted 5 times

Tadese Most Recent 2 weeks, 5 days ago

Selected Answer: A

Southbound—Multivendor Support APIs/SDK
The Cisco DNA Center Multivendor SDK allows partners to add support for managing non-Cisco devices directly from Cisco DNA Center. This tool provides the ability to build "device packs" customized for the level of automation and reporting that each new device allows. Once built, this capability permits basic device visibility, monitoring and Command Runner compatibility, and enables a non-Cisco device to be identified properly in inventory.

upvoted 1 times

CCNPWILL 3 months, 2 weeks ago

Correct. Answer is A.

upvoted 1 times

feynmanr 4 months, 3 weeks ago

Selected Answer: A

Voting A
I think the other answers refer to Northbound APIs

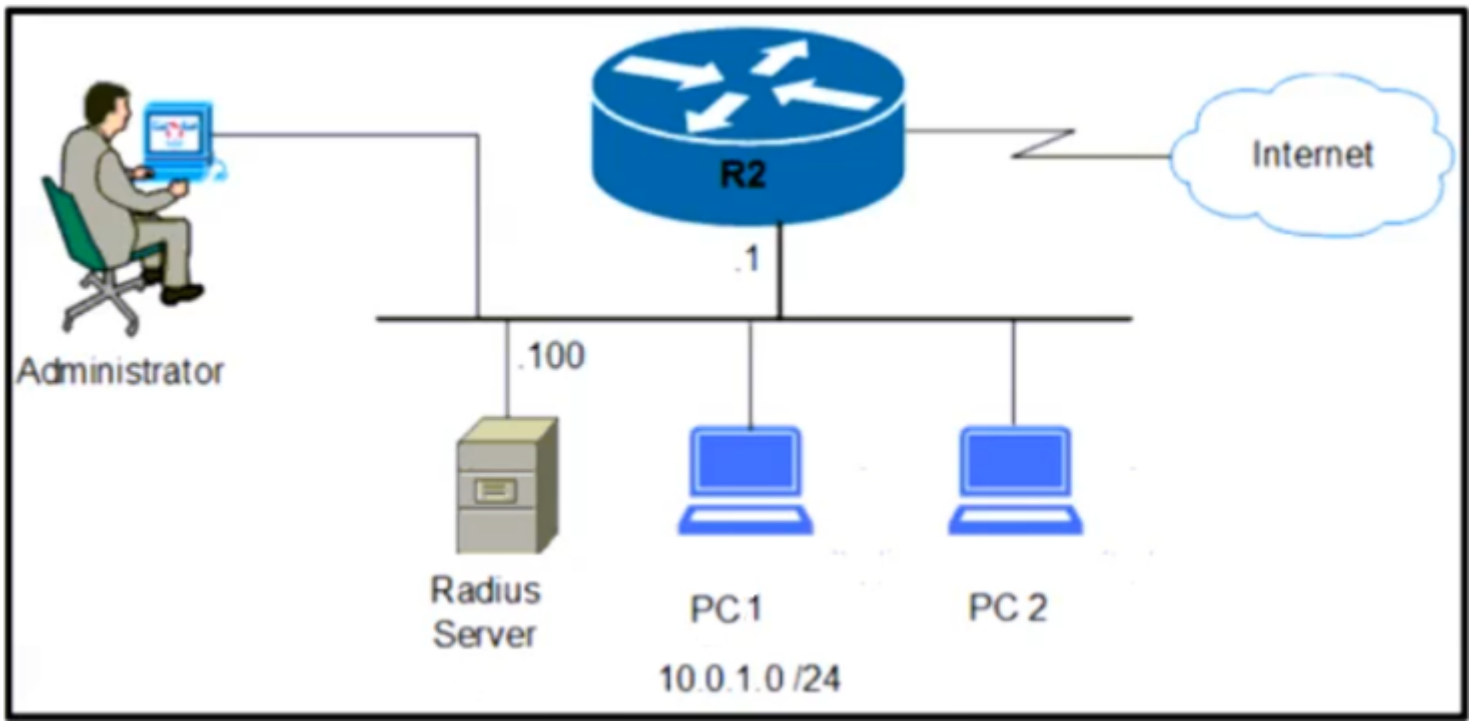
upvoted 1 times

Din04 1 month, 1 week ago

I think B is westbound API

upvoted 1 times

Question #767 *Topic 1*



Refer to the exhibit. Which command set enables router R2 to be configured via NETCONF?

A. R1(config)# netconf -
R1(config)# ip http secure-server

B. R1(config) # username Netconf privilege 15 password example_password

R1(config)# netconf-yang -
R1(config)# netconf-yang feature candidate-datastore

C. R1(config)# snmp-server manager -
R1(config)# snmp-server community ENCOR rw

D. R1(config)# snmp-server manager -
R1(config)# snmp-server community ENCOR ro

Correct Answer: *B*

Community vote distribution

B (64%) A (36%)

Asombrosso 4 months, 1 week ago

Selected Answer: B

netconf-yang

upvoted 1 times

PureInertiaCopy 4 months, 3 weeks ago

No one going to mention that face that the answers are giving a configuration response for "R1" which doesn't even exist in the exhibit??

upvoted 3 times

adamzet33 2 months ago

It happened to me once that i restarted wrong core switch during maintenance works, almost no one noticed :) Only one of my senior asked me smth aka ~did something just blinked or it was my computer..?

upvoted 1 times

Nickplayany 8 months, 3 weeks ago

Selected Answer: B

B like 100%

upvoted 2 times

JackDRipper 9 months ago

Selected Answer: B

A is missing the privilege 15 AAA credentials
B is correct

upvoted 2 times

MJane 9 months ago

Selected Answer: B

https://developer.cisco.com/docs/ios-xe/#!enabling-netconf-on-ios-xe/authentication

upvoted 2 times

Rman0059 9 months ago

Selected Answer: A

Also voting A

upvoted 1 times

DavideDL 9 months ago

Selected Answer: A

I would say A base on this link:
https://developer.cisco.com/docs/ios-xe/#!enabling-restconf-on-ios-xe/httphttps

RESTCONF runs over HTTPS. The following commands must be enabled to support
ip http secure-server

The CLI command to enable RESTCONF is displayed below:
restconf

upvoted 3 times

DavideDL 8 months, 3 weeks ago

I'm sorry I read RESTCONF instead of NETCONF....
I think B is the correct answer

upvoted 2 times

larsis 9 months ago

Is this really correct?

upvoted 1 times

Question #768 *Topic 1*

In the Cisco DNA Center Image Repository, what is a golden image?

A. The latest software image that is available for a specific device type.

B. The Cisco recommended software image for a specific device type.

C. A software image that is compatible with multiple device types.

D. A software image that meets the compliance requirements of the organization.

Correct Answer: *B*

Community vote distribution

D (100%)

DavideDL Highly Voted 9 months ago

Selected Answer: D

I don't think It is an image recommended by Cisco....

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/user_guide/b_cisco_dna_center_ug_2_1_2/b_cisco_dna_center_ug_2_1_1_chapter_0100.html#concept_qj4_fzx_f1b

Cisco DNA Center allows you to designate software images and SMUs as golden. A golden software image or SMU is a validated image that meets the compliance requirements for the particular device type.

So I would say It is something that meet the requirements of an Organization for a specific type of device.

My €0,02

upvoted 6 times

Haidary Most Recent 2 months, 3 weeks ago

D is correct

upvoted 1 times

CCNPWILL 3 months, 2 weeks ago

If you go to download an SDWAN software image.. you will see a gold star. That means its recommended by Cisco. But apparently, this golden image terminology means something different in DNAC.. Im going with Cisco recommended.

upvoted 2 times

connorm 3 months, 3 weeks ago

Selected Answer: D

We use DNA at work - you can manually edit an image to become the Gold Image.

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: D

particular deviceDesignating a software image or SMU as golden saves you time by eliminating the need to make repetitive configuration changes and ensures consistency across your devices. You can designate an image and a corresponding SMU as golden to create a standardized image. type.

upvoted 1 times

Ray_Dell 5 months, 1 week ago

B is closest to the "recommended" image

upvoted 1 times

MerlinTheWizard 6 months, 1 week ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/user_guide/b_cisco_dna_center_ug_2_1_2/b_cisco_dna_center_ug_2_1_1_chapter_0100.html#concept_qj4_fzx_f1b

A golden software image or SMU is a validated image that meets the compliance requirements for the particular device type

upvoted 2 times

foreignbishop 7 months, 3 weeks ago

From OnDemandLearning Course:

Golden Image
A golden image is a tag that indicates to the system that an image is optimal for running on a particular device family, type, or role, or at an enterprise site.

None of these answers are in fact identical to the training. It IS an image for a specific device type and it is an organizations image. It's a "tag" to a base image.

upvoted 2 times

enivoJkraM 8 months ago

Provided answer seems to be correct according to Cisco site.
B: The Cisco recommended software image for a specific device type.

In the Cisco DNA Center Image Repository, a golden image is a validated software image or SMU that meets the compliance requirements specific to the device type. Cisco DNA Center displays the Cisco-recommended software images according to device type, and by designating a recommended image as golden, administrators can centralize and simplify software management across the network. Therefore, selecting the Cisco recommended software image for a specific device type as a golden image ensures compliance and allows for standardized software deployment.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-3/user_guide/b_cisco_dna_center_ug_2_3_3/b_cisco_dna_center_ug_2_3_3_chapter_0100.html#task_a1z_zzp_1cb

upvoted 1 times

MJane 9 months ago

Selected Answer: D

Cisco DNA Center allows you to designate software images and SMUs as golden. A golden software image or SMU is a validated image that meets the compliance requirements for the particular device type.

upvoted 3 times

Nickplayany 8 months, 3 weeks ago

So it´s B not D :)

upvoted 1 times

Question #769 *Topic 1*

What are two benefits of implementing a traditional WAN instead of an SD-WAN solution? (Choose two.)

A. lower control plane abstraction

B. faster fault detection

C. simplified troubleshooting

D. comprehensive configuration standardization

E. lower data plane overhead

Correct Answer: *CD*

Community vote distribution

AE (91%) 9%

nNasty Highly Voted 9 months ago

Selected Answer: AE

The provided answers are for the benefits of SD-WAN compared to traditional WAN

upvoted 5 times

Asombrosso Most Recent 4 months, 1 week ago

Selected Answer: AE

AE IMHO

upvoted 1 times

mohican1 5 months, 3 weeks ago

Selected Answer: BC

Traditional WAN solutions often have simpler network architectures and fewer components compared to SD-WAN. This can result in faster fault detection as there are fewer potential points of failure and network issues can be more easily identified.
Simplified troubleshooting: With a traditional WAN, the network topology and configuration are typically more straightforward and standardized. This can simplify troubleshooting processes as network administrators can have a clearer understanding of the network design and can more easily identify and resolve issues.

SD-WAN offers benefits such as lower control plane abstraction, comprehensive configuration standardization, and lower data plane overhead.

upvoted 1 times

tempaccount00001 6 months, 1 week ago

Selected Answer: AE

By a mile! AE

upvoted 1 times

HarwinderSekhon 6 months, 2 weeks ago

A traditional WAN might have lower control plane abstraction and lower data plane overhead than an SD-WAN solution.

Traditional WANs typically have a simpler architecture where the control plane (which is responsible for routing decisions) and the data plane (which carries the user data) are not separated. This results in lower control plane abstraction.

Also, since traditional WANs are not overlay networks like SD-WANs, they generally incur less data plane overhead. Overlay networks add extra information (headers) to the original packets, which results in increased overhead and potentially less efficient use of the available bandwidth.

It's important to note that while these may be perceived as benefits in certain cases, the trade-offs include less flexibility, more complex configuration and management, and lack of some features like centralized control, easy scalability, and advanced traffic management that are typically found in SD-WAN solutions.

By Chat GPT.

upvoted 1 times

HarwinderSekhon 6 months, 2 weeks ago

Selected Answer: AE

A and E seems valid

upvoted 1 times

Chiaretta 8 months, 2 weeks ago

Selected Answer: AE

I agree

upvoted 2 times

olaniyijt 8 months, 3 weeks ago

I'd choose A & E

upvoted 3 times

Question #770 *Topic 1*

Which technology uses network traffic telemetry, contextual information, and file reputation to provide insight into cyber threats?

A. security services

B. security intelligence

C. segmentation

D. threat defense

Correct Answer: *B*

Community vote distribution

D (78%) B (22%)

kmb192006 Highly Voted 8 months, 3 weeks ago

Selected Answer: D

I'm going for D

OCG clearly stated Threat Defense "provides this visibility through network telemetry, file reputation, and contextual information ..." (P. 709)

upvoted 8 times

post20 Most Recent 1 week, 4 days ago

correct answer is D. Here the link: https://study-ccnp.com/network-security-design-cisco-safe/#:~:text=Threat%20Defense%20%E2%80%93%20provides%20cyber%20threat,respond%20appropriately%20to%20cyber%20threats.

upvoted 1 times

peugeotdude 1 month, 1 week ago

D - As per the Cisco Press Cert Guide ..

Threat defense: It is important to have visibility into the most dangerous cyber threats. Threat defense provides this visibility through network traffic telemetry, file reputation, and contextual information (such as device types, locations, users, identities, roles, privileges levels, login status, posture status, and so on). It enables assessment of the nature and the potential risk of suspicious activity so that the correct next steps for cyber threats can be taken.

upvoted 1 times

Haidary 2 months, 3 weeks ago

D is correct

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: B

security intelligence - is a technology
threat defense - is a solution

upvoted 1 times

Asombrosso 4 months, 1 week ago

my fault! its a D. threat defense

upvoted 1 times

eww_cybr 6 months ago

Selected Answer: D

Threat Defense – provides cyber threat visibility through network traffic telemetry, file reputation, and contextual data. It assesses the nature and possible risk of suspicious activities to respond appropriately to cyber threats.

https://study-ccnp.com/network-security-design-cisco-safe

upvoted 1 times

DavideDL 8 months, 3 weeks ago

Selected Answer: D

https://media.zones.com/images/pdf/cisco-cyber-threat-defense-solution.pdf

This document outlines the specifications for the three main functional components of the Cisco Cyber Threat Defense Solution:
- Generating network-wide security telemetry
- Aggregating, normalizing, and analyzing NetFlow telemetry data to detect threats and suspicious behavior
- Providing contextual information to determine the intent and severity of the threat

upvoted 3 times

MJane 8 months, 4 weeks ago

Selected Answer: B

can also be B; from the same document: The Lancope StealthWatch system, available through Cisco, is a purpose-built, high-performance network visibility and security intelligence solution.

upvoted 3 times

MJane 8 months, 4 weeks ago

Selected Answer: D

The initial version of the Cisco Cyber Threat Defense solution was introduced in 2013, with a Cisco Validated Design (CVD) to bring together NetFlow telemetry from the Cisco network infrastructure, the Cisco Identity Services Engine (ISE) for user and device identity, and the StealthWatch System through a partnership with Lancope, Inc. to provide network behavior analysis and threat detection in the interior of the network.

upvoted 2 times

Question #771 *Topic 1*

Which IEEE standard provides the capability to permit or deny network connectivity based on the user or device identity?

A. 802.1d

B. 802.1w

C. 802.1q

D. 802.1x

Correct Answer: *D*

Community vote distribution

D (100%)

due 4 months, 2 weeks ago

Selected Answer: D

A. 802.1d: Original Spanning Tree Protocol for loop prevention.

B. 802.1w: Rapid Spanning Tree Protocol for faster convergence.

C. 802.1q: VLAN tagging standard for network segmentation.

D. 802.1x: Port-based network access control based on identity.

upvoted 2 times

andyforreg 5 months, 1 week ago

Selected Answer: D

Seems to be ok

upvoted 2 times

Refer to the exhibit.

```
hostname CPE
!
ip dhcp excluded-address 192.168.10.0 192.168.10.10
!
ip dhcp pool LAN
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.0.2.254
!
interface Loopback0
 ip address 192.168.255.1 255.255.255.255
!
interface GigabitEthernet0/1
 description => LAN <=
 ip address 192.168.10.1 255.255.255.0
!
--
CPE# debug ip dhcp server packet
DHCP server packet debugging is on.
CPE#
*Sep 11 11:00:12.520: DHCPD: inconsistent relay information.
*Sep 11 11:00:12.520: DHCPD: relay information option exists, but giaddr is zero.
CPE#
```

The CPE router acts as a DHCP server for the locally attached LAN. After DHCP snooping is enabled on the switch where the DHCP clients are connected, clients are unable to obtain their configuration from the DHCP server. What is the cause of this issue?

A. The IP address of the DHCP server is in the excluded DHCP range.

B. The configuration of Gi0/1 is missing the ip helper-address 192.168.255.1 command.

C. The DHCP server drops DHCP packets carrying Option 82 and an empty relay agent IP address.

D. The excluded DHCP range contains the subnet address of the entire LAN network.

Correct Answer: *C*

Community vote distribution

C (100%)

due 4 months, 2 weeks ago

Selected Answer: C

Focus on log
DHCPD: relay information option exists, but giaddr is zero
giaddr (Gateway IP Address) is a field within DHCP packets used in DHCP relay scenarios. It contains the IP address of the relay agent (gateway) that forwards the DHCP request from a client to the DHCP server. This helps the DHCP server assign appropriate IP addresses and configuration to clients on different subnets.

Add giaddr on the interface that perform DHCP.
" ip dhcp relay information trusted giaddr_IP " command, you indicate that the relay agent IP address should be included in DHCP packets as they are forwarded to the DHCP server.

upvoted 1 times

PureInertiaCopy 4 months, 3 weeks ago

Can someone please explain?

upvoted 1 times

feynmanr 4 months, 3 weeks ago

https://ine.com/blog/2009-07-22-understanding-dhcp-option-82

This link explains it much better than I can, because I still am not sure how this works. Hope this helps.

upvoted 1 times

andyforreg 5 months, 1 week ago

Selected Answer: C

Seems to be ok
A,B,D - incorrect

upvoted 1 times

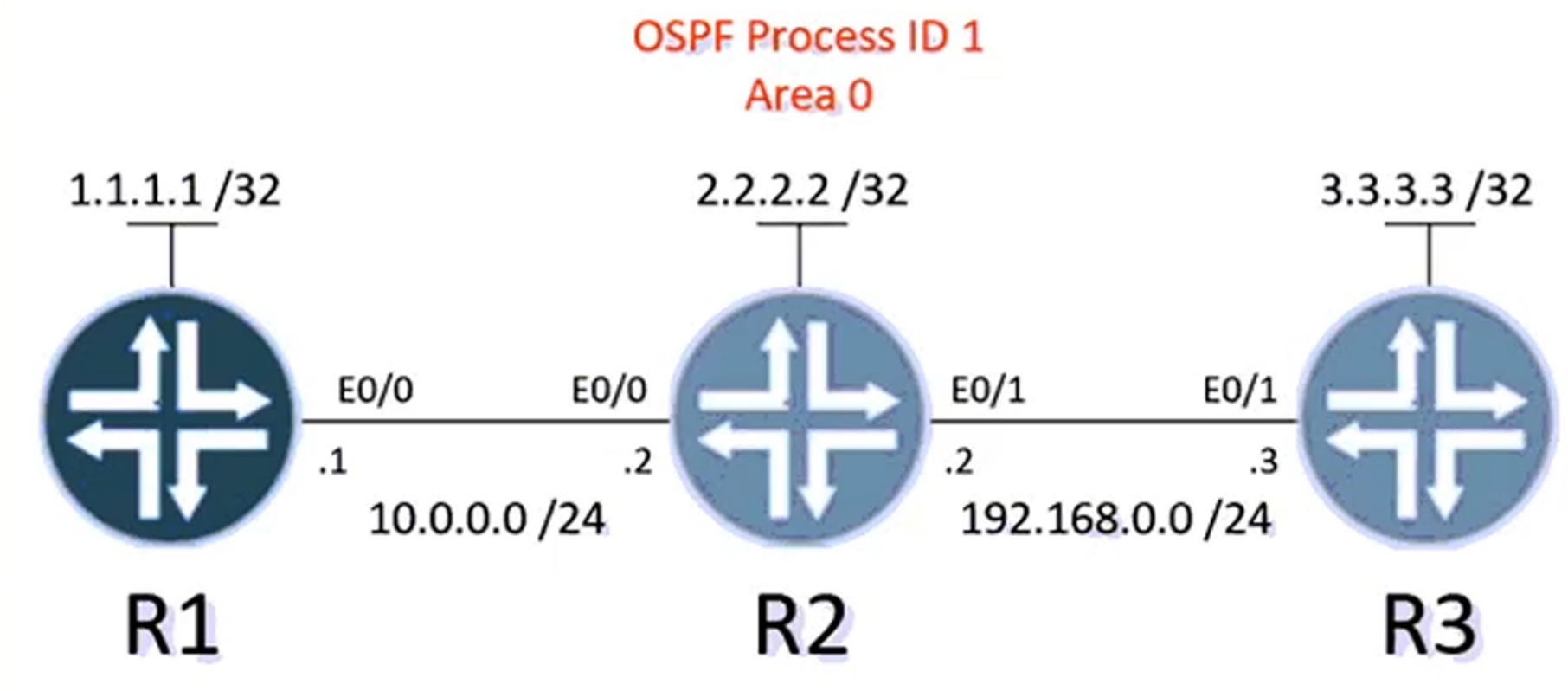
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question
• When Next is clicked, the lab closes and cannot be reopened.

Topology
-



Tasks
-

Configure OSPF on all three routers according to the topology to achieve these goals:

1. Configure OSPF without using the “network” statement under the “router ospf” configuration section.
2. Ensure that all networks are advertised between the routers.
3. Configure a single command under each Ethernet interface to prevent OSPF neighbors from participating in a DR/BDR election and ensure

that no extra host routes are generated.

#R1

interface e0/0

ip ospf 1 area 0

ip ospf network point-to-point

interface lo0

ip ospf 1 area 0

ip ospf network point-to-point

copy running-config startup-config

#R2

interface e0/0

ip ospf 1 area 0

ip ospf network point-to-point

Correct Answer:

interface e0/1

ip ospf 1 area 0

ip ospf network point-to-point

interface lo0

ip ospf 1 area 0

ip ospf network point-to-point

#R3

interface e0/1

ip ospf 1 area 0

ip ospf network point-to-point

interface lo0

ip ospf 1 area 0

ip ospf network point-to-point

copy running-config startup-config

darcone23 4 months ago

also for the part where no extra routes shouldn't be generated:
on every router under ospf process:
passive-interface default
no passive-interface loopback0
no passive-interface e0/0
no passive-interface e0/1 -> on R2 only

also, no need for point-to-point network type under loopback interfaces considering /32 subnet.. cant go more than that :)

upvoted 2 times

mgiuseppe86 3 months, 4 weeks ago

Negative.. I think you are wrong.

Step 3 asks for a single command, that is network-type point-to-point

passive-interface default and then having to do 'no passive-interface" is 2 commands and more.

Again, Step 3 asks for a SINGLE COMMAND to accomplish TWO tasks.

upvoted 1 times

Alondrix 2 months, 1 week ago

Passive interface applied to e0/0 and e0/1 would break the neighbor adjacency and stop ospf routing. It could be used on Lo0, but that isn't what is needed. To prevent the BR/BDR election it would be on the interface, "ip ospfy network-type point-to-point".

upvoted 2 times

NavidO 4 months, 1 week ago

R1

Interface loopback0
Ip address 1.1.1.1 255.255.255.255
Ip ospf 1 area 0

Interface e0/0
Ip address 10.0.0.1 255.255.255.0
Ip ospf 1 area 0
Ip ospf network-type point-to-point

R2

Interface e0/0
Ip address 10.0.0.2 255.255.255.0
Ip ospf 1 area 0
Ip ospf network-type point-to-point

Interface e0/1
Ip address 192.168.0.2 255.255.255.0
Ip ospf 1 area 0
Ip ospf network-type point-to-point

R3

Interface e0/1
Ip address 192.168.0.3 255.255.255.0
Ip ospf 1 area 0
Ip ospf network-type point-to-point

upvoted 2 times

NavidO 4 months, 1 week ago

R2
Interface loopback0
Ip address 2.2.2.2 255.255.255.255
Ip ospf 1 area 0
R3
Interface loopback0
Ip address 3.3.3.3 255.255.255.255
Ip ospf 1 area 0

upvoted 2 times

eddgg 4 months, 1 week ago

If we create a loopback and give classful or classless addresses, then by default the route to that loop back is advertised as the most specific route: /32 prefix and it will ignore any configured prefix.

Eg:
interface Loopback0
ip address 2.2.2.2 255.255.255.0
Here, the loopback network address is 2.2.2.0/24. By default OSPF will advertise this route to loopback0 as 2.2.2.2/32 (most specific route to that loopback).

To override this we have to change the network type to point-to-point. After this OSPF will advertise the address to loopback as 2.2.2.0/24.

interface Loopback0
ip address 2.2.2.2 255.255.255.0
ip ospf network point-to-point

upvoted 1 times

NewLife77 4 months, 1 week ago

Out of curiosity, why would we want to change it to 2.2.2.0/24? Why not keep it as 2.2.2.2/32? The question is showing its already configured as 2.2.2.2/32. Your example here is showing it as 2.2.2.2/24. Please clarify.

upvoted 1 times

NewLife77 4 months, 4 weeks ago

I don't believe the lo0 need ip ospf network point-to-point. It works correctly without it. If someone else believes the loopbacks need it, please let us know.

Only the interfaces between the routers need the ip ospf network point-to-point command.

upvoted 3 times

Question #774 *Topic 1*

Which solution simplifies management of secure access to network resources?

A. RFC 3580-based solution to enable authenticated access leveraging RADIUS and AV pairs

B. 802.1AE to secure communication in the network domain

C. ISE to automate network access control leveraging RADIUS AV pairs

D. TrustSec to logically group internal user environments and assign policies

Correct Answer: *C*

Community vote distribution

D (83%) C (17%)

jhonmeikel 5 months ago

Selected Answer: D

The answer is D

upvoted 1 times

hamish88 5 months, 1 week ago

Selected Answer: D

The answer is D. From 31 days before CCNP, page 524:
Cisco TrustSec simplifies the provisioning and management of secure access to network services and applications.

upvoted 3 times

alex711 5 months, 1 week ago

Selected Answer: C

C is correct. according to following link.

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_introduction.html#:~:text=Cisco%20Identity%20Services%20Engine%20(ISE,network%20device%20administration%20for%20enterprises.

upvoted 1 times

Lungful 5 months ago

this link doesn't mention RADIUS AV pairs anywhere though.

upvoted 1 times

andyforreg 5 months, 1 week ago

Selected Answer: D

I think - D...

upvoted 1 times

Question #775 *Topic 1*

What is a characteristic of a Type 2 hypervisor?

A. It is completely independent of the operating system.

B. It is installed on an operating system and supports other operating systems.

C. It eliminates the need for an underlying operating system.

D. Its main task is to manage hardware resources between different operating systems.

Correct Answer: *B*

Community vote distribution

B (100%)

Colmenarez 5 months, 1 week ago

Selected Answer: B

Option B

upvoted 1 times

alex711 5 months, 1 week ago

Selected Answer: B

Yes B is correct

upvoted 1 times

andyforreg 5 months, 1 week ago

Selected Answer: B

Seems to be ok

upvoted 2 times

Question #776 *Topic 1*

What is the recommended minimum SNR for data applications on wireless networks?

A. 20

B. 25

C. 15

D. 10

Correct Answer: *A*

Community vote distribution

A (100%)

shefo1 2 months, 2 weeks ago

20 for data application
25 for voice application
upvoted 2 times

bob7 3 months, 1 week ago

option A is correct
upvoted 1 times

Colmenarez 5 months, 1 week ago

Selected Answer: A

Option A. Option B is for voice
upvoted 3 times

alex711 5 months, 1 week ago

Selected Answer: A

A is correct
upvoted 1 times

andyforreg 5 months, 1 week ago

Selected Answer: A

Seems to be ok
https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength#:~:text=Generally%2C%20a%20signal%20with%20an,networks%20that%20use%20voice%20applications.
upvoted 2 times

Question #777 *Topic 1*

What does the Cisco DNA Center Authentication API provide?

A. list of VLAN names

B. client health status

C. access token to make calls to Cisco DNA Center

D. list of global issues that are logged in Cisco DNA Center

Correct Answer: *C*

Community vote distribution

C (100%)

Colmenarez 5 months, 1 week ago

Selected Answer: C

Option C

upvoted 1 times

alex711 5 months, 1 week ago

Selected Answer: C

C is Ok.

https://developer.cisco.com/learning/modules/dna-dne-platforms-api/intro-dnac-api/authentication/

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/DEVNET-2087.pdf

upvoted 1 times

eddgg 5 months, 1 week ago

Selected Answer: C

The Cisco DNA Center Authentication API provides an access token that allows external applications and services to make authorized API calls to Cisco DNA Center. This access token acts as a secure authentication mechanism, ensuring that only authorized clients can interact with the Cisco DNA Center APIs.

upvoted 1 times

andyforreg 5 months, 1 week ago

Selected Answer: C

Seems to be ok

upvoted 2 times

Question #778 *Topic 1*

What does the destination MAC on the outer MAC header identify in a VXLAN packet?

A. the leaf switch

B. the next hop

C. the remote switch

D. the remote spine

Correct Answer: *B*

Community vote distribution

B (75%) A (25%)

blitzstorm 4 months, 1 week ago

Selected Answer: B

B seems correct

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: A

Outer MAC Header: The outer MAC header includes the source and destination MAC addresses of the VTEPs (tunnel endpoints) involved in the VXLAN communication. The destination MAC address in the outer MAC header points to the VTEP that should receive the VXLAN packet.

upvoted 1 times

Asombrosso 4 months, 1 week ago

my fault, its a B. the next hop

upvoted 1 times

due 4 months, 2 weeks ago

Selected Answer: B

Question ask for outer MAC header.
The outer MAC header is the Ethernet header added to encapsulated packets for transport across the underlay network. It guides the packet within the physical network.
The inner MAC header is from the original packet and guides the packet's delivery within the overlay network.
destination MAC address in the outer MAC header could indeed represent the next hop device, which is the device responsible for forwarding the packet to its final destination. This is commonly seen in standard Ethernet forwarding.
destination MAC address in the inner MAC header should be the leaf switch.

upvoted 1 times

andyforreg 5 months, 1 week ago

Selected Answer: B

Seems to be OK

upvoted 1 times

alex711 5 months, 1 week ago

Yes I agree

upvoted 1 times

Question #779 *Topic 1*

What does the statement print(format(0.8, '.0%')) display?

A. 8.8%

B. .08%

C. 8%

D. 80%

Correct Answer: *D*

Community vote distribution

D (100%)

due 4 months, 2 weeks ago

Selected Answer: D

The statement print(format(0.8, '.2%')) will display the value 0.8 as a percentage with a precision of 2 decimal places, resulting in the output '80.00%'.

upvoted 4 times

Colmenarez 5 months, 1 week ago

Selected Answer: D

Option D, 80%

upvoted 3 times

alex711 5 months, 1 week ago

Selected Answer: D

Provided answer is correct

upvoted 2 times

Question #780 *Topic 1*

An engineer must implement a configuration to allow a network administrator to connect to the console port of a router and authenticate over the network. Which command set should the engineer use?

A. aaa new-model
aaa authentication login console local

B. aaa new-model
aaa authentication login console group radius

C. aaa new-model
aaa authentication login default enable

D. aaa new-model
aaa authentication enable default

Correct Answer: *B*

Community vote distribution

B (100%)

shefo1 2 months ago

A. is wrong because not use external server
c. is wrong because use the (default) keyword
d. is wrong because use the (default) keyword and not use the external server

connect to the console port => mean just console , default keyword is wrong because is mean all methods (vty,aux,cons).

authenticate over the network => mean use external server (tacacs+ , radius).

upvoted 1 times

Colmenarez 5 months, 1 week ago

there is not such command #aaa authen login console or I missing something?

upvoted 1 times

alex711 5 months, 1 week ago

Selected Answer: B

B seems to be Correct according to the follwoing link.

https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

upvoted 2 times

andyforreg 5 months, 1 week ago

Selected Answer: B

network means Radius, TACACS+
So correct answer should be:

aaa new-model
aaa authentication login default group radius

or

aaa new-model
aaa authentication login console group radius
line con 0
aaa authentication login console

upvoted 4 times

Question #781 *Topic 1*

When a DNS host record is configured for a new Cisco AireOS WLC, which hostname must be added to allow APs to successfully discover the WLC?

A. CONTROLLER-CAPWAP-CISCO

B. CISCO-CONTROLLER-CAPWAP

C. CAPWAP-CISCO-CONTROLLER

D. CISCO-CAPWAP-CONTROLLER

Correct Answer: *D*

Community vote distribution

D (100%)

blitzstorm 3 months, 4 weeks ago

That is exactly question that can make you failed the exam. Fuck you cisco with your shit question

upvoted 2 times

alex711 5 months, 1 week ago

Selected Answer: D

D is correct.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/5700/software/release/3e/consolidated/configuration-guide/b_multi_3e_5700_cg/b_multi_3e_5700_cg_chapter_01001011.html#:~:text=CAPWAP%2C%20which%20is%20based%20on,Cisco%20products%20that%20use%20CAPWAP

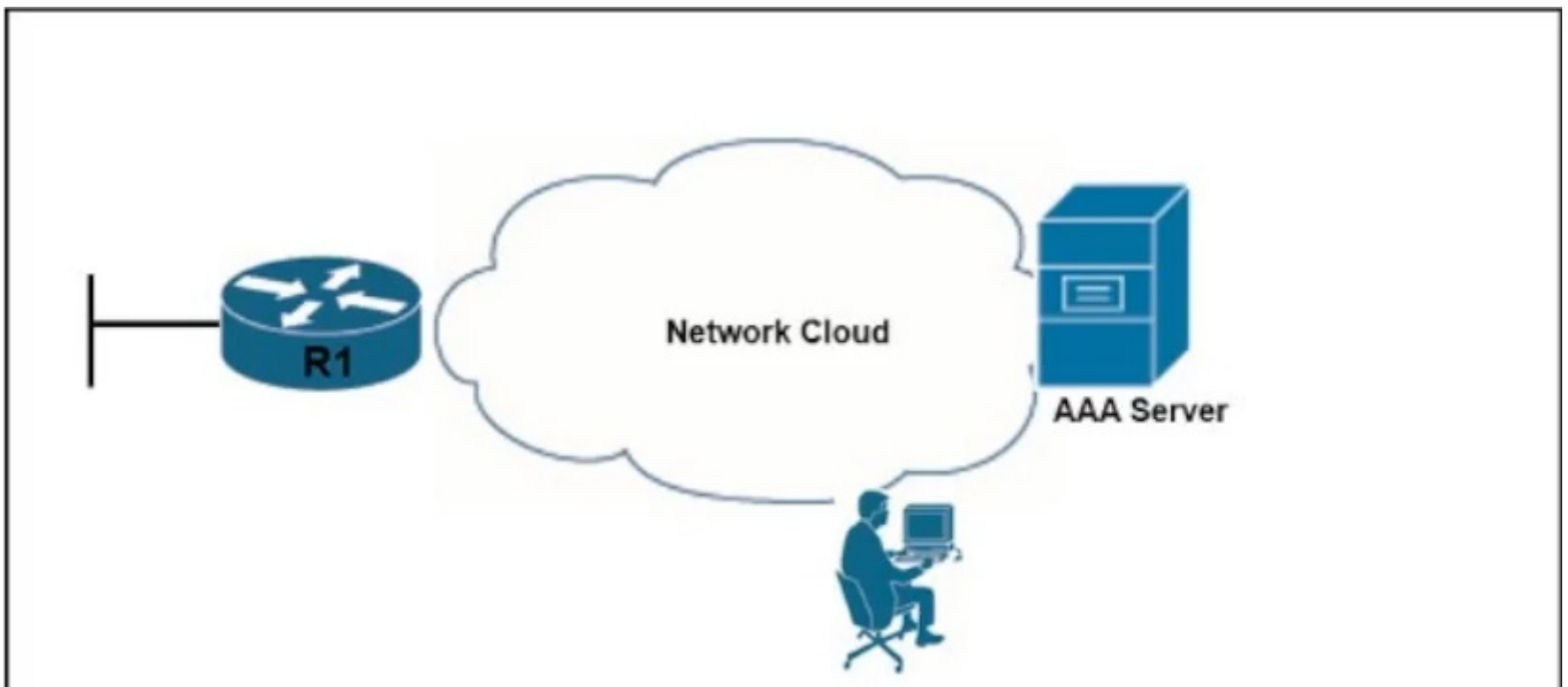
upvoted 3 times

andyforreg 5 months, 1 week ago

Selected Answer: D

Seem to be OK

upvoted 2 times




```
Router1$ ssh -s admin@192.168.20.3 -p 830 netconf
admin@192.168.20.3's password: cisco123

<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
<capability>urn:ietf:params:netconf:base:1.1</capability>
<capability>urn:ietf:params:netconf:capability:writable-
running:1.0</capability>
<capability>urn:ietf:params:netconf:capability:xpath:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.1</capability>
<capability>urn:ietf:params:netconf:capability:rollback-on-
error:1.0</capability
--snip--
</capabilities>
<session-id>2870</session-id></ hello>]]>]]>

Use < ^C > to exit
```

Refer to the exhibit. An engineer tries to log in to router R1. Which configuration enables a successful login?

A. R1#username admin privilege 15 -
aaa authorization exec default local

B. R1#username admin privilege 15 -
aaa authorization exec default local
netconf-yang

C. R1#netconf-yang -
username admin privilege 15 secret cisco123
aaa new-model
aaa authorization exec default local

D. R1#aaa new-model -
aaa authorization exec default local
enable aaa admin privilege 15

Correct Answer: *C*

Community vote distribution

C (100%)

CCNPWILL 3 months, 2 weeks ago

Selected Answer: C

C is correct.

upvoted 1 times

alex711 5 months, 1 week ago

Selected Answer: C

C is correct.

upvoted 1 times

andyforreg 5 months, 1 week ago

Selected Answer: C

Seems to be OK

upvoted 1 times

Which statement must be used to export the contents of the devices object in JSON format?

```
from json import dumps, loads

Devices=[
{
   'name' : 'SwitchA',
   'ip' : '10.10.10.1',
   'model' : 'WS-2960',
   'serial' : 'S5016350ADX',
   'user' : 'CiscoAdmin',
   'pass' : 'd451991709c0'
}]
```

A. json.repr(Devices)

B. json.loads(Devices)

C. json.print(Devices)

D. json.dumps(Devices)

Correct Answer: *D*

Community vote distribution

D (83%) B (17%)

Asombrosso 4 months, 1 week ago

Selected Answer: D

json.loads(jsonString) — json string to python object
json.dumps(pythonObject) — python object to json string
json.load(fileHandler) — json file to python object — python object from file
json.dump(jsonString or pythonObject, fileHandler) — json string or python object to json file

upvoted 2 times

due 4 months, 2 weeks ago

Selected Answer: D

json.loads(Devices): Restore a JSON string (like Devices) to Python objects.
json.dumps(Devices): Convert Python objects (like Devices) to a JSON-formatted.
json.repr and json.print not a valid Python JSON-related function.
Keyword , export JSON format = json.dumps.

upvoted 1 times

ihateciscoreally 4 months, 2 weeks ago

Selected Answer: B

in my opinion it should be B. you have JSON string format and you want to export it. json.loads() is only viable option.

upvoted 1 times

CCNPWILL 3 months, 2 weeks ago

you hate cisco so you are trying to sabotage everyone else? The answer is D. a simple google search would have told you.

upvoted 2 times

alex711 5 months, 1 week ago

Selected Answer: D

D is Ok.

upvoted 2 times

Question #784 *Topic 1*

Why does the vBond orchestrator have a public IP?

A. to allow for global reachability from all WAN Edges in the Cisco SD-WAN and to facilitate NAT traversal

B. to provide access to Cisco Smart Licensing servers for license enablement

C. to enable vBond to learn the public IP of WAN Edge devices that are behind NAT gateways or in private address space

D. to facilitate downloading and distribution of operational and security patches

Correct Answer: *A*

Community vote distribution

A (100%)

CCNPWILL 3 months, 2 weeks ago

Answer is A. Correct.

upvoted 1 times

Lungful 5 months ago

Selected Answer: A

A is correct.
Two more links to add to Alex's:
https://learningnetwork.cisco.com/s/question/0D56e0000Bzp2B4CQI/vbond-public-ip-address
https://community.cisco.com/t5/sd-wan-and-cloud-networking/vmanage-vbond-and-vsmart-behind-nat/td-p/3776576

upvoted 2 times

alex711 5 months, 1 week ago

Selected Answer: A

A is correct.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html#:~:text=Cisco%20vBond%20Orchestrator%20is%20a,network%20can%20connect%20to%20it.

upvoted 3 times

Question #785 *Topic 1*

Why would a small or mid-size business choose a cloud solution over an on-premises solution?

A. Cloud provides greater ability for customization than on-premises.

B. Cloud provides more control over the implementation process than on-premises.

C. Cloud provides lower upfront cost than on-premises.

D. Cloud provides higher data security than on-premises.

Correct Answer: *C*

Community vote distribution

C (100%)

Hamo1 4 months, 2 weeks ago

c is correct

upvoted 1 times

andyforreg 5 months, 1 week ago

Selected Answer: C

Seems to be OK

upvoted 2 times

Question #786 *Topic 1*

Which two new security capabilities are introduced by using a next-generation firewall at the Internet edge? (Choose two.)

A. stateful packet inspection

B. integrated intrusion prevention

C. NAT

D. VPN

E. application-level inspection

Correct Answer: *BE*

Community vote distribution

BE (100%)

CCNPWILL 3 months, 2 weeks ago

Correct

upvoted 1 times

Manvek 5 months ago

Selected Answer: BE

B and E seems correct in accordance with Cisco.

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html#~ngfw-firewall

upvoted 4 times

andyforreg 5 months, 1 week ago

Selected Answer: BE

B,E defenetly

upvoted 2 times

alex711 5 months, 1 week ago

I agree

upvoted 1 times

```
ip access-list extended 101
 10 deny   ip any any
!
event manager applet Block_Users
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "interface GigabitEthernet1"
 action 4.0 cli command "ip access-group 101 in"
 action 5.0 cli command "ip access-group 101 out"
```

Refer to the exhibit. An engineer builds an EEM script to apply an access list. Which statement must be added to complete the script?

A. action 6.0 cli command "ip access-list extended 101"

B. action 3.1 cli command "ip access-list extended 101"

C. event none

D. action 2.1 cli command "ip access-list extended 101"

Correct Answer: *C*

Community vote distribution

C (100%)

Manvek 5 months ago

Selected Answer: C

C is correct. The applet is missing the trigger event configuration. In this case there is no trigger event, so none must be selected. The access list is already configured, the applet only needs to apply it.

event manager applet Block_Users
event none
action 1.0 cli command "enable"
action 2.0 cli command "configure terminal"
action 3.0 cli command "interface GigabitEthernet1"
action 4.0 cli command "ip access-group 101 in"
action 5.0 cli command "ip access-group 101 out"
action 7.0 cli command "end"

upvoted 4 times

andyforreg 5 months, 1 week ago

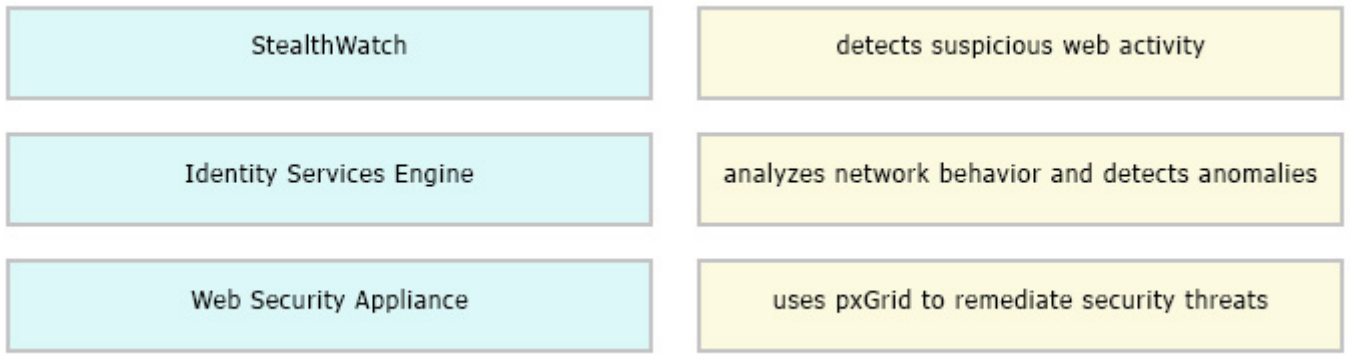
Selected Answer: C

Seems to be OK

upvoted 1 times

DRAG DROP
-

Drag and drop the solutions that comprise Cisco Cyber Threat Defense from the left onto the objectives they accomplish on the right.



Correct Answer:

Identity Services Engine	StealthWatch
Web Security Appliance	Identity Services Engine

Lungful 5 months ago

Answers look to be correct.
https://developer.cisco.com/docs/pxgrid/#!ise-as-a-provider

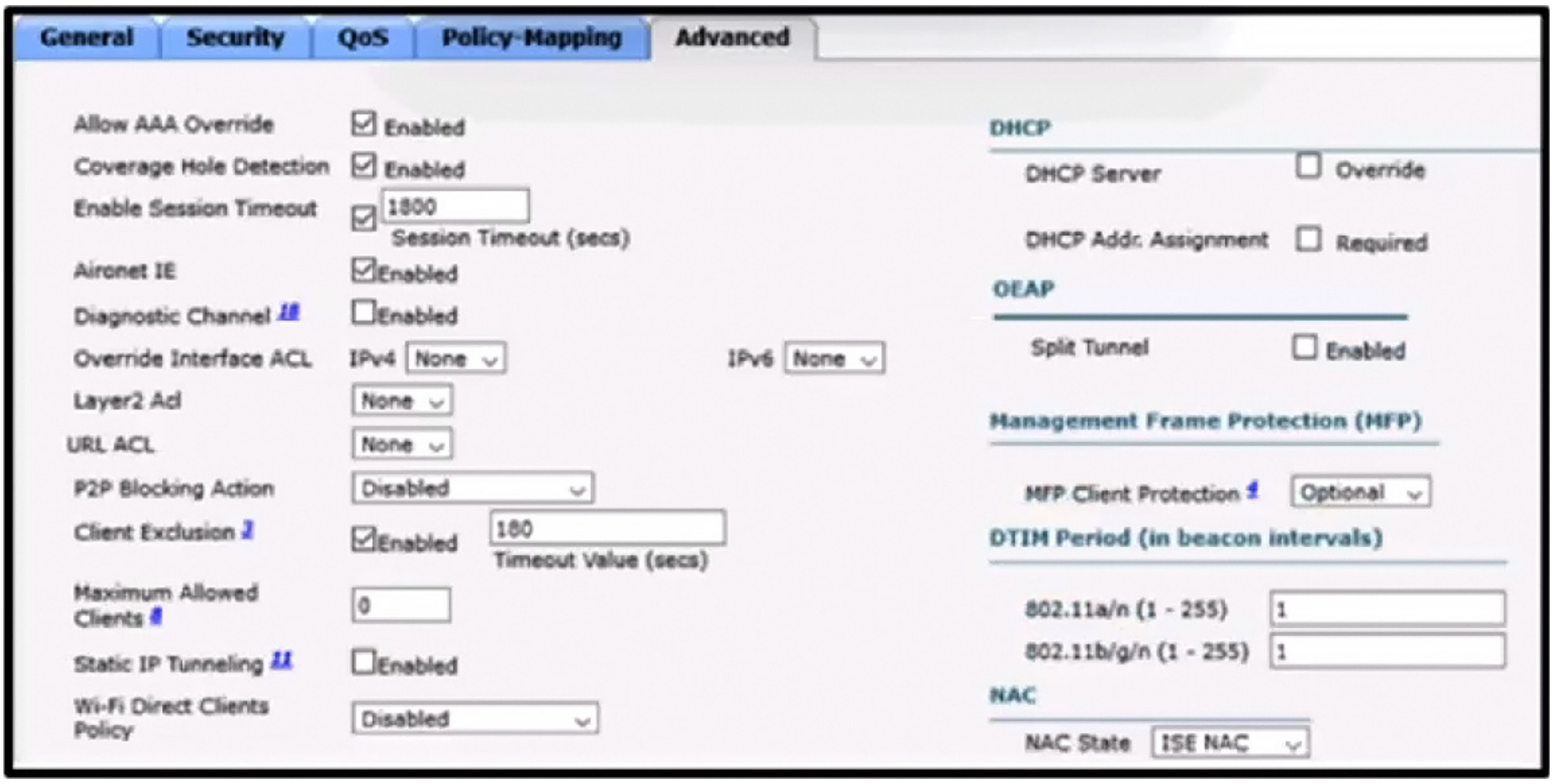
upvoted 1 times

Manvek 5 months ago

Answers are correct.

upvoted 3 times

Question #789 *Topic 1*



Refer to the exhibit. An engineer is troubleshooting an issue with client devices triggering excessive power changes on APs in the 2.4 GHz band. Which action resolves this issue?

A. Disable Aironet IE.

B. Set the 802.11b/g/n DTIM interval to 0.

C. Enable MFP Client Protection.

D. Disable Coverage Hole Detection.

Correct Answer: *D*

Community vote distribution

D (100%)

Manvek 5 months ago

Selected Answer: D

Provided answer is correct.

"The device discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the device mitigates the coverage hole by increasing the transmit power level for that specific access point"

https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/16-12/config-guide/ewc_cg_16_12/coverage_hole_detection.pdf

upvoted 2 times

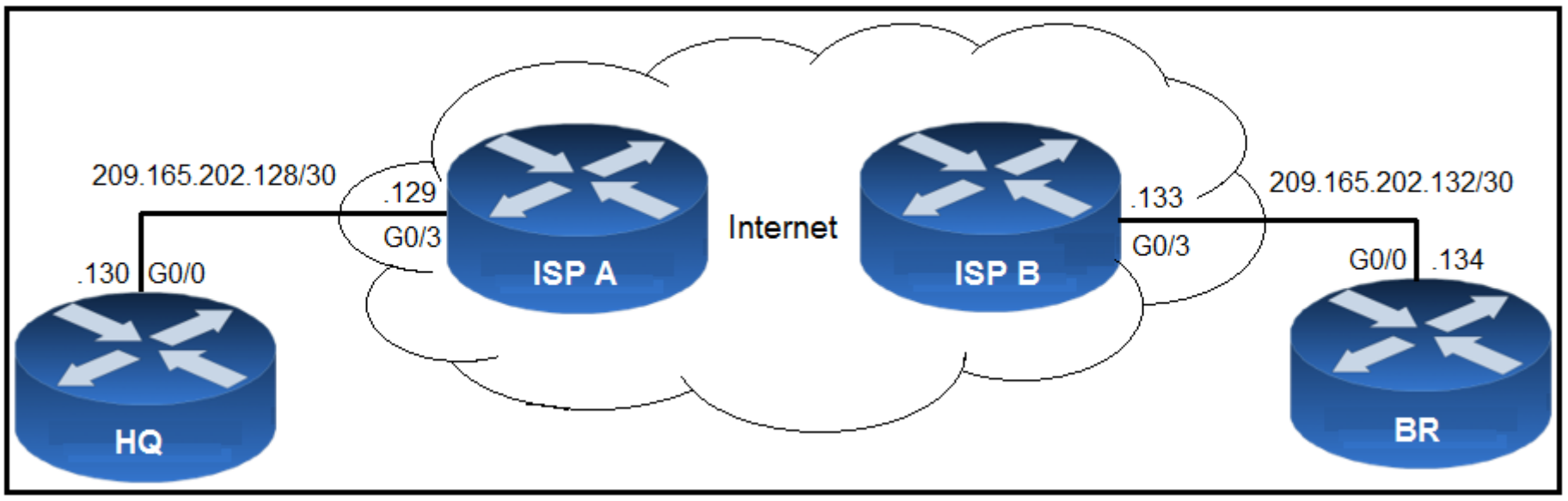
alex711 5 months, 1 week ago

Selected Answer: D

the given answer seems correct.

upvoted 1 times

Question #790 *Topic 1*



Refer to the exhibit. What is the effect of these commands on the BR and HQ tunnel interfaces?

```
BR(config)#interface tunnel1
BR(config-if)#keepalive 5 3

HQ(config)#interface tunnel1
HQ(config-if)#keepalive 5 3
```

A. The keepalives are sent every 3 seconds and 5 retries.

B. The tunnel line protocol goes down when the keepalive counter reaches 5.

C. The keepalives are sent every 5 seconds and 3 retries.

D. The tunnel line protocol goes down when the keepalive counter reaches 6.

Correct Answer: *C*

Community vote distribution

C (100%)

eearmani 2 weeks, 2 days ago

Selected Answer: C

send keep alive every 5 seconds and 3 retries

upvoted 1 times

tivi92 4 months, 1 week ago

C correct, 100%.

upvoted 1 times

blitzstorm 4 months, 2 weeks ago

Selected Answer: C

Answser C is valid, tested in GNS3.
Switch(config-if)#keepalive ?
<0-32767> Keepalive period (default 10 seconds)
<cr>

Switch(config-if)#keepalive 5 ?
<1-255> Keepalive retries (default 3 times)
<cr>

upvoted 3 times

Question #791 *Topic 1*

Which protocol is used to encrypt control plane traffic between SD-WAN controllers and SD-WAN endpoints?

A. DTLS

B. IPsec

C. PGP

D. HTTPS

Correct Answer: *A*

Community vote distribution

A (100%)

eearmani 2 weeks, 2 days ago

Selected Answer: A

he Cisco Catalyst SD-WAN control plane has been designed with network and device security in mind. The foundation of the control plane is one of two security protocols derived from Secure Sockets Layer (SSL)—the Datagram Transport Layer Security (DTLS) protocol and the Transport Layer Security (TLS) protoco

upvoted 1 times

blitzstorm 4 months, 2 weeks ago

Selected Answer: A

Given answer is correct.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/security-overview.html

upvoted 3 times

Question #792 *Topic 1*

What is one difference between SaltStack and Ansible?

A. SaltStack uses the Ansible agent on the box, whereas Ansible uses a Telnet server on the box.

B. SaltStack uses an API proxy agent to program Cisco boxes in agent mode, whereas Ansible uses a Telnet connection.

C. SaltStack uses SSH to interact with Cisco devices, whereas Ansible uses an event bus.

D. SaltStack is constructed with minion, whereas Ansible is constructed with YAML.

Correct Answer: *D*

tivi92 4 months, 1 week ago

D correct, 100%

upvoted 2 times

remen78 4 months, 2 weeks ago

given answer is correct

upvoted 2 times

Question #793 *Topic 1*

A customer has a pair of Cisco 5520 WLCs set up in an SSO cluster to manage all APs. Guest traffic is anchored to a Cisco 3504 WLC located in a DMZ. Which action is needed to ensure that the EoIP tunnel remains in an UP state in the event of failover on the SSO cluster?

A. Use the same mobility domain on all WLCs.

B. Enable default gateway reachability check.

C. Configure back-to-back connectivity on the RP ports.

D. Use the mobility MAC when the mobility peer is configured.

Correct Answer: *D*

Community vote distribution

D (100%)

blitzstorm 3 months, 4 weeks ago

Selected Answer: D

Answer D :
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-5/High_Availability_DG.html

upvoted 2 times

Horsefeathers 2 weeks, 2 days ago

Mobility MAC
Unique MAC address shared between peers in HA setup. This mac address should be used to form a mobility pair between HA setup and another WLCs in HA setup or with independent controllers.

upvoted 1 times

Question #794 *Topic 1*

Which configuration filters out DOT1X messages in the format shown below from being sent toward Syslog server 10.15.20.33?

Nov 20 13:47:32/553 %DOT1X-5-FAIL:Authentication failed for client (e04f.438e.de4f) on interface Gi1/0/1 AudtiSessionID 0A0B50A5000004543910739E

A. logging discriminator DOT1X facility drops DOT1X
logging host 10.15.20.33 discriminator DOT1X

B. logging discriminator DOT1X msg-body drops DOTX
logging host 10.15.20.33 discriminator DOTX

C. logging discriminator DOT1X mnemonics includes DOTX
logging host 10.15.20.33 discriminator DOT1X

D. logging discriminator DOT1X mnemonics includes DOT1X
logging host 10.15.20.33 discriminator DOTX

Correct Answer: *B*

Community vote distribution

A (100%)

Tadese 2 weeks, 4 days ago

Selected Answer: A

Logging discriminator discr-name [[facility] [mnemonics] [msg-body] { drops string | includes string }] [severity { drops sev-num | includes sev-num }] [rate-limit msglimit]

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: A

filters out facility=DOT1X messages and drops them

upvoted 3 times

eddgg 4 months, 1 week ago

Selected Answer: A

it should be A

upvoted 1 times

tivi92 4 months, 1 week ago

I think that the correct answer should be A).
logging discriminator DOT1X facility drops DOT1X
logging host 10.15.20.33 discriminator DOT1X

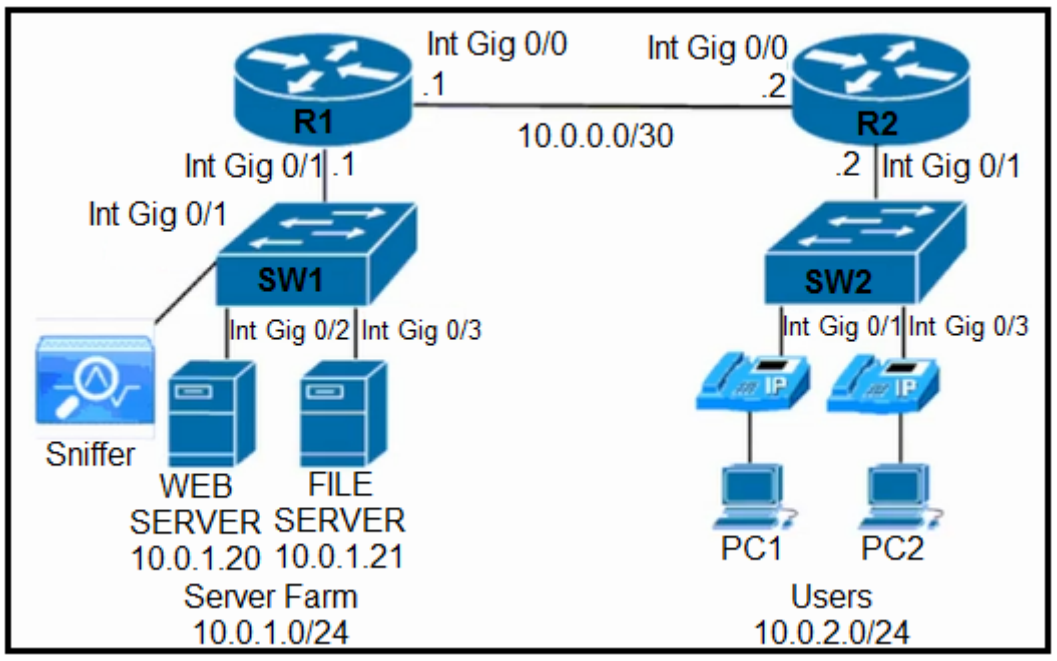
upvoted 1 times

blitzstorm 4 months, 2 weeks ago

Selected Answer: A

Given answer is wrong. The message body doesn't contain "DOT1X". However the logging facility is "DOT1X" so A seems good.
https://youtu.be/Lbb7vlQoGt0?feature=shared&t=154

upvoted 2 times



Refer to the exhibit. A network engineer is troubleshooting an issue with the file server based on reports of slow file transmissions. Which two commands or command sets are required to switch SW1 to analyze the traffic from the file server with a packet analyzer? (Choose two.)

A. SW1#show monitor

B. SW1(config)#monitor session 1 source interface gigabitethernet0/3
SW1(config)#monitor session 1 destination interface gigabitethernet0/1 encapsulation replicate

C. SW1#show ip route

D. SW1#show vlan

E. SW1(config)#monitor session 1 source interface gigabitethernet0/1
SW1(config)#monitor session 1 destination interface gigabitethernet0/3 encapsulation replicate

Correct Answer: *AB*

Community vote distribution

AB (100%)

blitzstorm 4 months ago

Selected Answer: AB

Given answer is correct.

upvoted 4 times

Question #796 *Topic 1*

What are two benefits of implementing a Cisco SD-WAN architecture? (Choose two.)

A. It enforces a single, scalable, hub-and-spoke topology.

B. It simplifies endpoint provisioning through standalone router management.

C. It allows configuration of application-aware policies with real time enforcement.

D. It improves endpoint protection by integrating embedded and cloud security features.

E. It provides resilient and effective traffic flow using MPLS.

Correct Answer: *CD*

Community vote distribution

CD (100%)

Toob93 4 months ago

Selected Answer: CD

C and D are correct.

upvoted 3 times

Question #797 *Topic 1*

Which two functions is an edge node responsible for? (Choose two.)

A. authenticates endpoints

B. provides the default entry point for fabric traffic

C. provides multiple entry and exit points for fabric traffic

D. provides the default exit point for fabric traffic

E. provides a host database that maps endpoint IDs to a current location

Correct Answer: *AC*

Community vote distribution

AC (71%) AB (29%)

cwauch 6 days, 17 hours ago

Selected Answer: AC

A. is definitely correct but C is explained below.
A fabric edge performs the encap and decap of host traffic to and from its connected endpoints. CCNP ENCOR Cert guide - p.623

upvoted 1 times

djedeen 3 months, 3 weeks ago

Selected Answer: AB

Edge Node provides first-hop services for Users / Devices connected to a Fabric
[A] • Responsible for Identifying and Authenticating Endpoints (e.g. Static, 802.1X, Active Directory)
[B] • Performs encapsulation / de-encapsulation of data traffic to and from all connected Endpoints
https://www.cisco.com/c/dam/m/hr_hr/training-events/2019/cisco-connect/pdf/VH-Cisco-SD-Access-Connecting.pdf

upvoted 1 times

tsamoko 4 months, 1 week ago

Selected Answer: AC

A 100% is correct , per book .
C is also seems right . Edge node is an xTR that provides, provides onboarding and mobility services for wired users and devices (including fabric-enabled WLCs and APs) connected to the fabric.

upvoted 4 times

Horsefeathers 2 weeks, 2 days ago

I prefer C over B because of this:
VXLAN encapsulation/de-encapsulation
Packets and frames received from endpoint... are encapsulated in fabric VXLAN and forwarded across the overlay.
When fabric encapsulated traffic is received for the endpoint... it is de-encapsulated and sent to that endpoint.

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

upvoted 1 times

Asombrosso 4 months, 1 week ago

Selected Answer: AB

A. fabric edge first identifies and authenticates wired endpoints (through 802.1x), in order to place them in a host pool (SVI and VRF instance) and scalable group (SGT assignment). It then registers the specific EID host address (that is, MAC, /32 IPv4, or /128 IPv6) with the control plane node.
B. It's next-hop VTEP for hosts
!=C. The control plane (host database) maps all EID locations to the current fabric edge or border node.

upvoted 1 times

Yizhou 4 months, 2 weeks ago

Answer is wrong. Should be C and E

upvoted 1 times

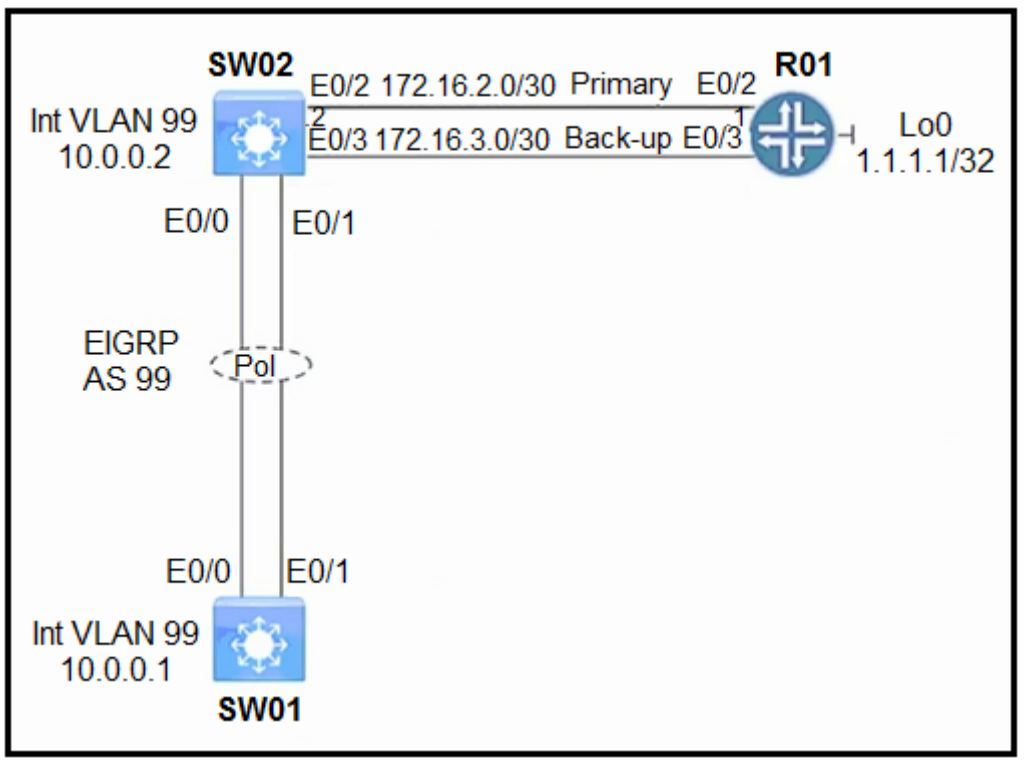
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

Topology
-



Tasks
-

Configure logging on SW01 and NetFlow on R01 to achieve these goals:

1. Enable archive logging on SW01 to track each time a change is made to the configuration and the user who made the change.
2. The NetFlow Top Talkers feature has been preconfigured on R01. Enable the feature for all inbound traffic on interface E0/2 of R01.

R01
-

```
R01>
R01>en
R01#config t
Enter configuration commands, one per line, End with CNTL/Z
R01(config)#inter
R01(config)#interface eh
R01(config)#interface eth
R01(config)#interface ethernet 0/2
R01(config-if)#ip ro
R01(config-if)#ip route-c
R01(config-if)#ip route-cache fl
R01(config-if)#ip route-cache flow
R01(config-if)#exit
R01(config)#exit
R01#sh
R01#show
*Jul 10 19:52:41.513: %SYS-5-CONFIG_I: Configured from console by console
R01#show ip ca
R01#show ip cache fl
R01#show ip cache flow
```

```
IP packet size distribution (0 total packets):
1-32 64   96   128  160  192  224  256  288  320  352
480
.000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
.000

512  544  576  1024 1536 2040 2560 3072 3504 4096 4608
.000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
     0 active, 4096 inactive, 0 added
     0 ager polls, 0 flow alloc failures
     Active flows timeout in 30 minutes
     Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
     0 active, 1024 inactive, 0 added, 0 added to flow
     0 alloc failures, 0 force free
     1 chunk, 1 chunk added
     last clearing of statistics never
Protocol  Total     Flows     Packet Bytes   Packets Active(Sec) Idle(Sec
--------       Flows     /Sec /Flow     /Pkt /Sec /Flow          /Flow

SrcIf     SrcIPaddress   DstIf     DstIPaddress   Pr SrcP DstP
  Pkts
R01#
```

```
R01#
R01#sh ip flo
R01#sh ip flow to
R01#sh ip flow top-talkers
% Cache is empty
R01#c
R01#
R01#
R01#
R01#sh ip flow top-talkers
% Cache is empty
R01#
R01#
R01#
R01#
R01#copy ru
R01#copy running-config st
R01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
[OK]
R01#
R01#
```

SW01

-

```
SW01>
SW01>
SW01>en
SW01#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW01(config)#
SW01(config)#arc
SW01(config)#archive
SW01(config-archive)#log
SW01(config-archive)#log con
SW01(config-archive)#log config
SW01(config-archive-log-cfg)# log
SW01(config-archive-log-cfg)# logging en
SW01(config-archive-log-cfg)# logging enable
SW01(config-archive-log-cfg)#exit
SW01(config-archive)#exit
SW01(config)#
SW01(config)#exit
SW01#
*Jul 10 19:53:32.388: %SYS-5-CONFIG_I: Configured from console by console
SW01#copy ru
SW01#copy running-config st
SW01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
Compressed configuration from 1226 bytes to 803 bytes[OK]
SW01#
SW01#
```

Correct Answer:

Task 1.
SW01(config)#archive
SW01(config-archive)# log config
SW01(config-archive-log-config)# logging enable

Task 2.
R01(config)#interface Ethernet 0/2
R01(config-if)#ip route-cache flow

Verification:

R1#show ip cache flow
R1#sh ip flow top-talkers
Save the configuration
SW01,R01#copy running-config startup-con

eearmani 2 weeks, 2 days ago

ip route-cache flow (works only under L3 interface IP native interface)

upvoted 1 times

JJBIG 3 months, 3 weeks ago

I try on IOS version 15.9
ip route-cache flow = ip flow ingress only on the interface
ip flow egress = outbound
ip flow ingress= inbound
So we should use command "ip flow egress" on router for monitor outbound traffic

upvoted 1 times

JJBIG 3 months, 3 weeks ago

Sorry the question ask: "all inbound traffic on interface E0/2 of R01"
"ip route-cache flow" and "ip flow ingress" has the same functions

upvoted 1 times

blitzstorm 4 months ago

For 1st part I'd go with (starting in global config mode):
archive
log config
logging enable

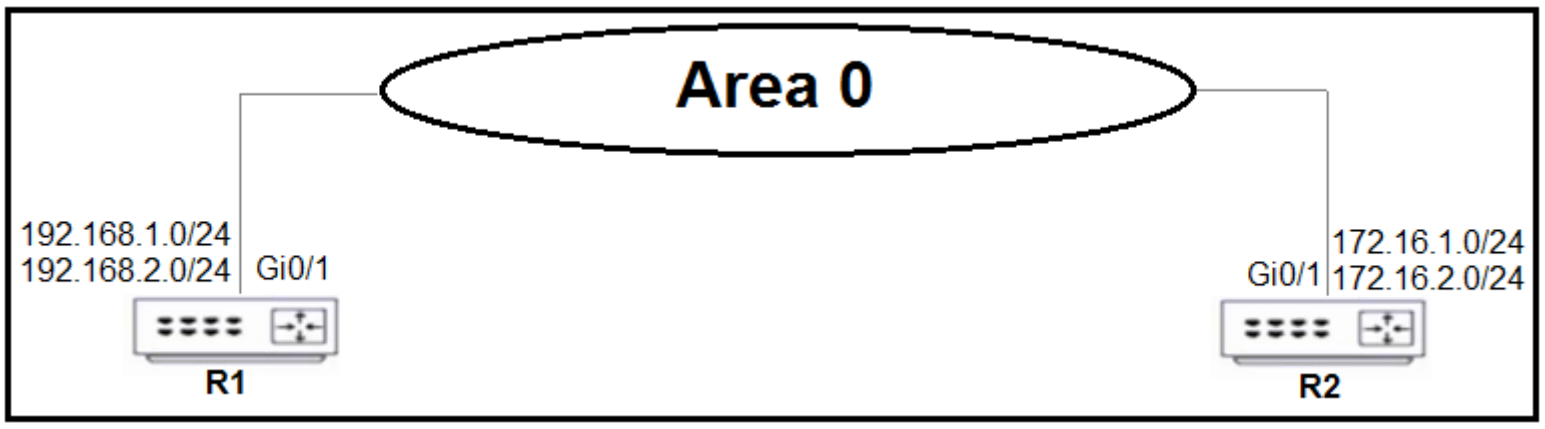
For 2nd part I'd go with(starting in interface config mode):
ip flow ingress

upvoted 2 times

eddgg 4 months ago

The "ip route-cache flow" can be used only under the main interface, while the "ip flow ingress" was an enhancement to be used under subinterfaces.

upvoted 1 times



Refer to the exhibit. Which two configurations enable R1 and R2 to advertise routes into OSPF? (Choose two.)

A. R2 -
router ospf 0
network 172.16.1.0 0.0.0.255 area 0
network 172.16.2.0 0.0.0.255 area 0

B. R1 -
router ospf 0
network 192.168.1.0 255.255.255.0 area 0
network 192.168.2.0 255.255.255.0 area 0

C. R2 -
router ospf 0
network 172.16.1.0 255.255.255.0 area 0
network 172.16.2.0 255.255.255.0 area 0

D. R1 -
router ospf 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0

E. R2 -
router ospf 0
network 172.16.1.0 0.0.0.255 area 0
network 172.16.2.0 255.255.255.0 area 0

Correct Answer: *AD*

Community vote distribution

AD (100%)

kaupz 2 months, 1 week ago

Selected Answer: AD

A & D are correct

upvoted 1 times

blitzstorm 4 months ago

Selected Answer: AD

Simple, in answers B,C & E, a network mask is used instead of a wildcard mask.
A & D are remaining.

upvoted 1 times

Question #800 *Topic 1*

Which Python library is used to work with YANG data models via NETCONF?

A. ncclient

B. requests

C. cURL

D. Postman

Correct Answer: *A*

Community vote distribution

A (100%)

blitzstorm Highly Voted 4 months, 2 weeks ago

Selected Answer: A

Given answer is correct.

Python files usually start with "from ncclient import manager"

upvoted 5 times

eearmani Most Recent 2 weeks, 2 days ago

Selected Answer: A

ncclient is python library that facilitate NETCONF

upvoted 1 times

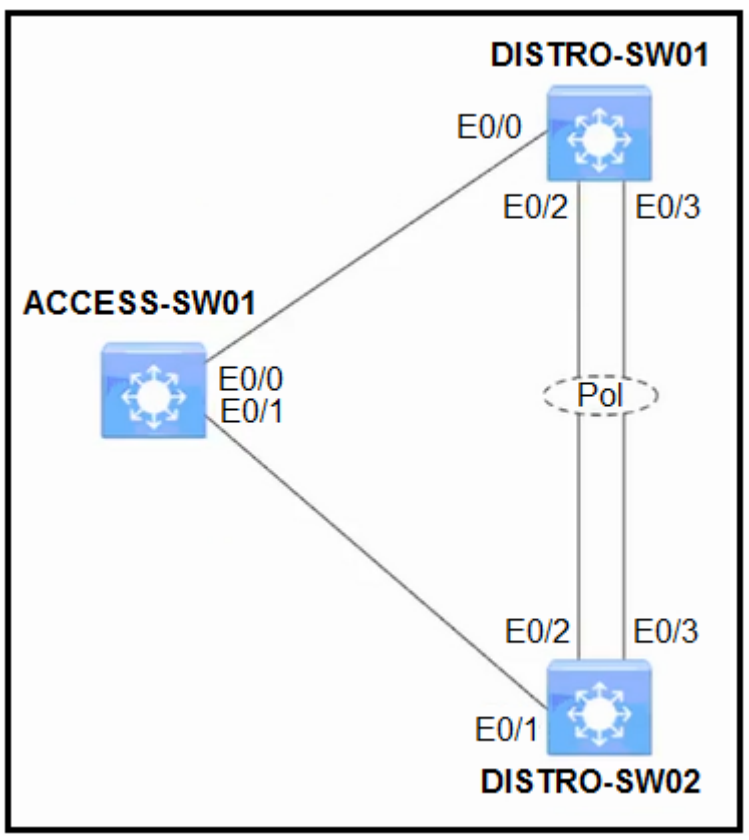
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

Topology
-



Tasks
-

The operations team started configuring network devices for a new site.
Complete the configurations to achieve these goals:
1. Ensure that port channel Po1 between DISTRO-SW01 and DISTRO-SW02 is operational using the LACP protocol. Configuration changes for this task must be made on DISTRO-SW01.
2. Ensure that traffic on VLAN 10 is carried as untagged traffic between DISTRO-SW01 and DISTRO-SW02.
3. Complete the Rapid-PVST+ configuration on DISTRO-SW2 by ensuring it it the secondary root switch for all VLANs in the range of 1 to 1005.

DISTRO-SW01
-

```
DISTRO-SW01>
DISTRO-SW01>
DISTRO-SW01>en
DISTRO-SW01#config t
Enter configuration commands, one per line. End with CNTL/Z.
DISTRO-SW01(config)# in
DISTRO-SW01(config)# interface e0/0
DISTRO-SW01(config-if)#no cha
DISTRO-SW01(config-if)#no channel-g
DISTRO-SW01(config-if)#no channel-group 1
DISTRO-SW01(config-if)#no channel-group 1 mo
DISTRO-SW01(config-if)#no channel-group 1 mode pas
DISTRO-SW01(config-if)#no channel-group 1 mode passive
DISTRO-SW01(config-if)#
* Jul 10 20:07:53.469: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0,
changed state to up
DISTRO-SW01(config-if)#
DISTRO-SW01(config-if)#exit
DISTRO-SW01(config)#
DISTRO-SW01(config)# in
DISTRO-SW01(config)# interface ran
DISTRO-SW01(config) # interface range e
DISTRO-SW01(config)# interface range ethernet 0/2-3
DISTRO-SW01(config-if-range)#ch
DISTRO-SW01(config-if-range)#channel-gr
DISTRO-SW01(config-if-range)#channel-group 1
DISTRO-SW01(config-if-range)#channel-group 1 mo
DISTRO-SW01(config-if-range)#channel-group 1 mode ac
DISTRO-SW01(config-if-range)#channel-group 1 mode active
DISTRO-SW01(config-if-range)#
* Jul 10 20:08:25.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2,
changed state to up
* Jul 10 20:08:25.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3,
changed state to up
DISTRO-SW01(config-if-range)#exit
DISTRO-SW01(config)#
* Jul 10 20:08:31.447: %LINK-3-UPDOWN: Interface Port-channel, changed state to up
* Jul 10 20:08:32.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3,
changed state to up
DISTRO-SW01(config)#
DISTRO-SW01(config)#exit
DISTRO-SW01#
* Jul 10 20:08:39.212: %SYS-5-CONFIG_I: Configured from console by console
DISTRO-SW01#sh eth
DISTRO-SW01#sh etherc
DISTRO-SW01#sh etherchannel s
DISTRO-SW01#sh etherchannel summary
```

```
DISTRO-SW01#sh etherchannel s
DISTRO-SW01#sh etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregate

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

      A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group     Port-channel   Protocol  Ports
---------+------------------+-------------------+----------
1    Pol(SU)        LACP      Et0/2(P)  Et0/3(P)
```

```
DISTRO-SW01#
DISTRO-SW01# config t
Enter configuration commands, one per line, End with CNTL/Z.
DISTRO-SW01(config)#inte
DISTRO-SW01(config)#interface po
DISTRO-SW01(config)#interface port-
DISTRO-SW01(config)#interface port-channel 1
DISTRO-SW01(config-if)#sw
DISTRO-SW01(config-if)#switchport tr
DISTRO-SW01(config-if)#switchport trunk na
DISTRO-SW01(config-if)#switchport trunk native vl
DISTRO-SW01(config-if)#switchport trunk native vlan 10
DISTRO-SW01(config-if)#
* Jul 10 20:09:27.352: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/3 (10), with DISTRO-SW02 Ethernet0/3 (1).
DISTRO-SW01(config-if)#
* Jul 10 20:09:27.857: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent
peer vlan id 1 on Port-channel1 VLAN10.
* Jul 10 20:09:27.857: %SPANTREE-2-BLOCK_PVID_PEER: Blocking Port-channel1 on
VLAN0001. Inconsistent peer vlan.
* Jul 10 20:09:27.857: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking Port-channel1 on
VLAN0010. Inconsistent local vlan.
DISTRO-SW01(config-if)#
```

```
* Jul 10 20:09:27.857: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan
id 1 on Port-channel1 VLAN10.
* Jul 10 20:09:27.857: %SPANTREE-2-BLOCK_PVID_PEER: Blocking Port-channel1 on VLAN0001.
Inconsistent peer vlan.
* Jul 10 20:09:27.857: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking Port-channel1 on VLAN0010.
Inconsistent local vlan.
DISTRO-SW01(config-if)#
* Jul 10 20:09:30.710: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/2 (10), with DISTRO-SW02 Ethernet0/2 (1).
DISTRO-SW01(config-if)#
* Jul 10 20:10:03.864: %SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking Port-channel on
VLAN0001. Port consistently restored
* Jul 10 20:10:03.864: %SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking Port-channel on
VLAN0010. Port consistently restored
DISTRO-SW01(config-if)#
DISTRO-SW01(config-if)#exit
DISTRO-SW01(config)#
DISTRO-SW01(config)#exit
DISTRO-SW01#co
DISTRO-SW01#co
* Jul 10 20:10:35.644: %SYS-5-CONFIG_I: Configured from console by console
DISTRO-SW01#copy ru
DISTRO-SW01#copy running-config st
DISTRO-SW01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
Compressed configuration from 1447 bytes to 886 bytes[OK]
DISTRO-SW01#
DISTRO-SW01#
```

DISTRO-SW02

-

```
DISTRO-SW02>
* Jul 10 20:08:25.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2,
changed state to up
* Jul 10 20:08:25.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3,
changed state to up
DISTRO-SW02>
* Jul 10 20:08:31.447: %LINK-3-UPDOWN: Interface Port-channel, changed state to up
* Jul 10 20:08:32.448: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel,
changed state to up
DISTRO-SW02>
* Jul 10 20:09:27.848: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer
vlan id 10 on Port-channel1 VLAN1.
* Jul 10 20:09:27.848: %SPANTREE-2-BLOCK_PVID_PEER: Blocking Port-channel1 on VLAN0010.
Inconsistent peer vlan.
* Jul 10 20:09:27.857: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking Port-channel1 on VLAN0001.
Inconsistent local vlan.
DISTRO-SW02>
* Jul 10 20:09:31.330: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/3 (1), with DISTRO-SW01 Ethernet 0/3 (10).
```

```
DISTRO-SW02>en
DISTRO-SW02#config t
Enter configuration commands, one per line, End with CNTL/Z.
DISTRO-SW02(config)#
DISTRO-SW02(config)#inter
DISTRO-SW02(config)#interface por
DISTRO-SW02(config)#interface port-ch
DISTRO-SW02(config)#interface port-channel 1
DISTRO-SW02(config)#interface port-channel 1
DISTRO-SW02(config-if)#sw
DISTRO-SW02(config-if)#switchport tr
DISTRO-SW02(config-if)#switchport trunk na
DISTRO-SW02(config-if)#switchport trunk native vl
DISTRO-SW02(config-if)#switchport trunk native vlan 10
DISTRO-SW02(config-if)#exit
DISTRO-SW02(config)#
DISTRO-SW02(config)#sp
DISTRO-SW02(config)#spanning-tree vl
DISTRO-SW02(config)#spanning-tree vlan 1-
* Jul 10 20:10:04.934: %SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking
Port-channel1 on VLAN0010. Port consistently restored.
* Jul 10 20:10:04.934: %SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking
Port-channel1 on VLAN0001. Port consistently restored.
DISTRO-SW02(config)#spanning-tree vlan 1-1005 ro
DISTRO-SW02(config)#spanning-tree vlan 1-1005 root se
DISTRO-SW02(config)#spanning-tree vlan 1-1005 root secondary
DISTRO-SW02(config)#exit
```

```
DISTRO-SW02 con0 is now available



Press RETURN to get started
DISTRO-SW02>
DISTRO-SW02>
DISTRO-SW02>en
DISTRO-SW02#copy ru
DISTRO-SW02#copy running config st
DISTRO-SW02#copy running config startup-config
Destination filename [startup-config]?
Building configuration…
Compressed configuration from 1449 bytes to 889 bytes[OK]
DISTRO-SW02#
DISTRO-SW02#
DISTRO-SW02#
```

Correct Answer:

Task 1. Ensure that port channel Po1 between DISTRO-SW01 and DISTRO-SW02 is operational using the LACP protocol.
Configuration changes
for this task must be made on DISTRO-SW01.
The port towards to ACCESS-SW1 was part of port channel 1 which was used towards to DISTRO-SW02, so remove the port channel config pointing to the ACCESS-SW1 first.

DISTRO-SW01(config)#int e0/0
DISTRO-SW01(config-if)#no channel-group 1
Set the LACP mode active on this switch:
DISTRO-SW01(config-if)#int range e0/2 – 3
DISTRO-SW01(config-if)#channel-group 1 mode active

Verification:
We can verify if the Port-channel was formed with the "show etherchannel summary" command
DISTRO-SW01# show etherchannel summary
-- output omitted --
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+------------ +-----------+---
1 Po1(SU) LACP Et0/2(P) Et0/3(P)
If we see the "Po1(SU)" means our configuration worked correctly.

Task 2. Ensure that traffic on VLAN 10 is carried as untagged traffic between DISTRO-SW01 and DISTRO-SW02.

DISTRO-SW01,DISTRO-SW02(config)#interface port-channel 1
DISTRO-SW01,DISTRO-SW02(config-if)#switchport trunk native vlan 10

Task 3. Complete the Rapid-PVST+ configuration on DISTRO-SW2 by ensuring it is the secondary root switch for all VLANs in the range of 1 to 1005.

DISTRO-SW02(config)#spanning-tree vlan 1-1005 root secondary
Save the configuration
DSW1,DSW2(config)#copy running-config startup-config

mgiuseppe86 Highly Voted 4 months, 1 week ago

Distro-SW01
#int po1
#switchport mode trunk
#switchport trunk native vlan 10

#int e0/2
#channel-group 1 mode active
#int e0/3
#channel-group 1 mode active

Distro-SW02
#int po1
#switchport mode trunk
#switchport trunk native vlan 10

#spanning-tree mode rapid-pvst
#spanning-tree vlan 1-1005 root secondary

upvoted 5 times

eddgg Most Recent 4 months, 2 weeks ago

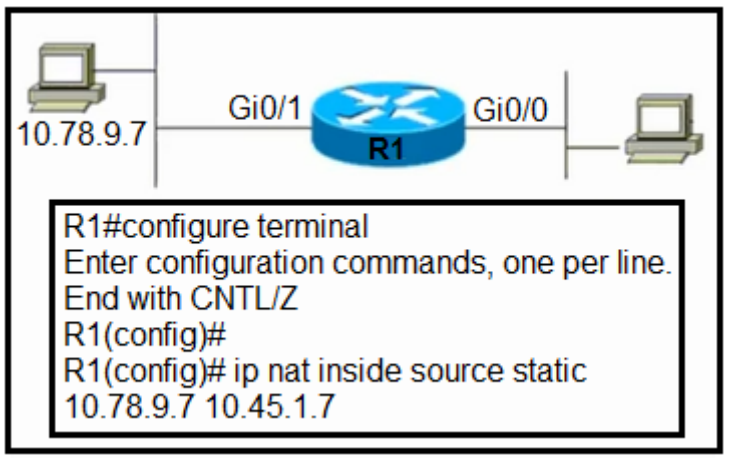
sw01

int e0/0
no channel-group 1
int range e0/2-3
channel-group 1 mode active

sw1
interface port-channel 1
switchport trunk native vlan 10

sw2
interface port-channel 1
switchport trunk native vlan 10
interface port-channel 1
spanning-tree vlan 1-1005 root secondary

upvoted 2 times



Refer to the exhibit. A network architect has partially configured static NAT. Which commands should be added to complete the configuration?

A. R1(config)# interface GigabitEthernet 0/0

R1(config)# ip pat inside -
R1(config)# interface GigabitEthernet 0/1

R1(config)# ip pat outside -

B. R1(config)# interface GigabitEthernet 0/0

R1(config)# ip pat outside -
R1(config)# interface GigabitEthernet 0/1

R1(config)# ip pat inside -

C. R1(config)# interface GigabitEthernet 0/0

R1(config-if)# ip nat inside -
R1(config)# interface GigabitEthernet 0/1

R1(config-if)# ip nat outside -

D. R1(config)# interface GigabitEthernet 0/0

R1(config-if)# ip nat outside -
R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip nat inside

Correct Answer: *D*

Community vote distribution

D (100%)

NewLife77 4 months, 2 weeks ago

Selected Answer: D

D is correct. There is no such thing as 'ip pat inside/outside'.

upvoted 4 times

tsamoko 4 months, 3 weeks ago

Selected Answer: D

Configure the inside static NAT by using the command "ip nat inside source static inside-local-ip inside-global-ip." . First is inside local ip = 10.78.9.7 (ge0/1)

upvoted 1 times

Asombrosso 4 months, 3 weeks ago

Selected Answer: D

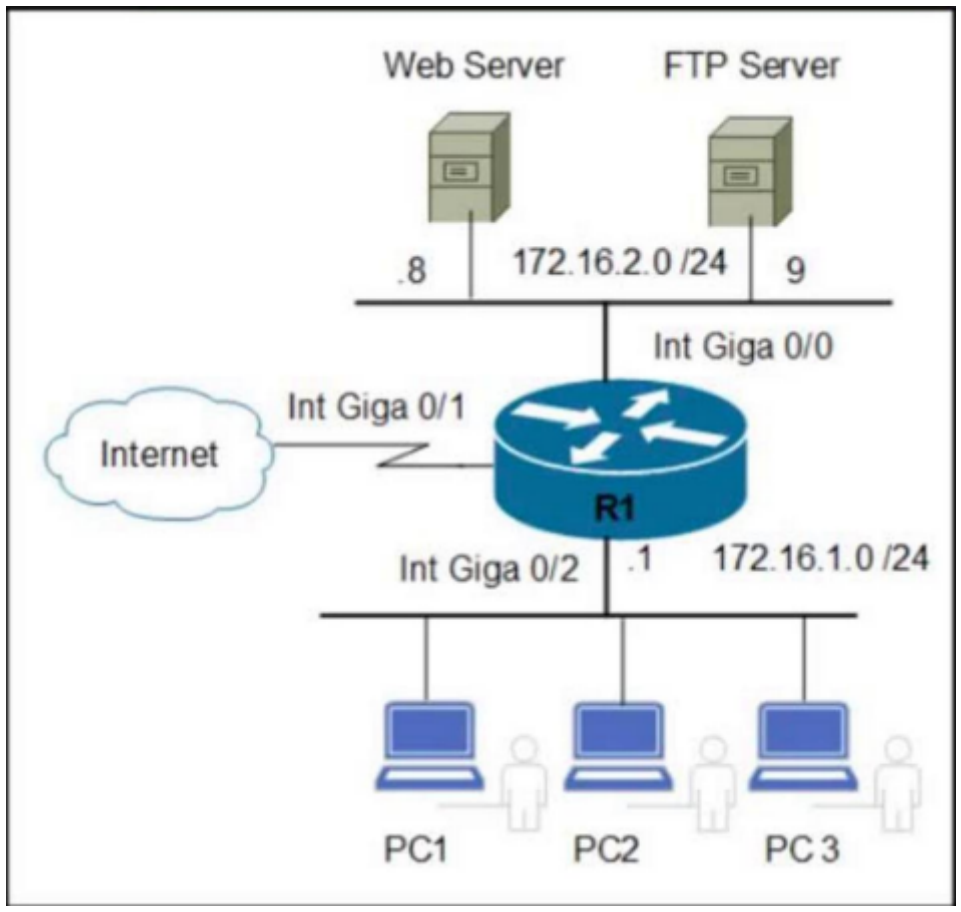
there's no "ip pat inside" command :)

upvoted 2 times

Mbonz 4 months, 3 weeks ago

A is the answer
Gi0/0 is translating the inside local addresses on Gi0/1 into the outside global pool of addresses D is not correct

upvoted 1 times



Refer to the exhibit. An engineer must allow the FTP traffic from users on 172.16.1.0 /24 to 172.16.2.0 /24 and block all other traffic. Which configuration must be applied?

A. R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255

R1 (config)#interface giga 0/2 -
R1 (config-if)#ip access-group 120 in

B. R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 20
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21

R1(config)#interface giga 0/2 -
R1 (config-if)#ip access-group 120 in

C. R1 (config)# access-list 120 deny any any
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21

R1 (config)#interface giga 0/0 -
R1(config-if)#ip access-group 120 out

D. R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)# access-list 120 permit udp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255

R1 (config)#interface giga 0/2 -
R1(config-if)#ip access-group 120 out

Correct Answer: *B*

Community vote distribution

B (100%)

djedeen 1 month, 3 weeks ago

Selected Answer: B

Has to be B, ftp 'active mode' uses port 21 for control and 20 for data, both are TCP. ftp in passive mode will use a random port instead of 20 for data, typical is 1024 to 65535.

upvoted 3 times

Question #804 *Topic 1*

High bandwidth utilization is occurring on interface Gig0/1 of a router. An engineer must identify the flows that are consuming the most bandwidth. Cisco DNA Center is used as a flow exporter and is configured with the IP address 192.168.23.1 and UDP port 23000. Which configuration must be applied to set NetFlow data export and capture on the router?

A.
```
R1(config)# ip flow-export
R1(config)# ip flow-export destination 192.168.23.1 23000
R1(config)# interface Gig0/1
R1(config-if)# ip flow monitor
```

B.
```
R1(config)# ip flow-export
R1(config)# ip flow-export destination 192.168.23.1
R1(config)# interface Gig0/1
R1(config-if)# collect counter bytes
R1(config-if)# collect counter packets
```

C.
```
R1(config)# ip flow-export version 9
R1(config)# ip flow-export destination 192.168.23.1 23000
R1(config)# interface Gig0/1
R1(config-if)# ip flow ingress
R1(config-if)# ip flow egress
```

D.
```
R1(config)# ip flow-export version 9
R1(config)# ip flow-export destination 192.168.23.1 23000
R1(config)# interface Gig0/1
R1(config-if)# ip flow-top-talkers
```

Correct Answer: *A*

Community vote distribution

C (100%)

f490efc 5 days, 21 hours ago

Selected Answer: C

DNA center would be "collector" rather then "exporter"

upvoted 1 times

eearmani 4 weeks, 1 day ago

Selected Answer: C

C is correct as it is traditional Netflow configuration
under the interface it accept configuration for ingress and egress traffic

upvoted 1 times

Fanny1493 2 months ago

C correct
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf

upvoted 2 times

kaupz 2 months, 3 weeks ago

Selected Answer: C

D, because
R1(config)#ip flow-export
% Incomplete command.
---this rules out A and B
and D should be ruled out, because top-talkers need to be first enabled before assigned to an interface: https://tech-wiki.net/index.php/Cisco_Legacy_Neflow_-_%22Top_Talkers%22_Commands

C should be correct answer

upvoted 4 times

DRAG DROP

-

Drag and drop the code snippets from the bottom onto the blanks in the code to construct a request that configures policy-based routing.

```
{
  "route-map": {
    "name": "auto",
    "ios-route-map:route-map-without-order-seq": {
      "ios-route-map:seq_no": "100",
      "ios-route-map:operation": "          ",
      "ios-route-map:          ": {
        "ios-route-map:ip": {
          "ios-route-map:          ":{"ios-route-map:address": "\"\"\" + isp2iprmt + \"\"\""}
        }
      },
      "ios-route-map:match": {
        "ios-route-map:ip": {
          "ios-route-map:          ":{"ios-route-map:access-list": "auto"}
        }
      }
    }
  }
}
```

address | permit | next-hop | set

Correct Answer:

```
{
  "route-map": {
    "name": "auto",
    "ios-route-map:route-map-without-order-seq": {
      "ios-route-map:seq_no": "100",
      "ios-route-map:operation": "permit",
      "ios-route-map:set": {
        "ios-route-map:ip": {
          "ios-route-map:next-hop":{"ios-route-map:address": "\"\"\" + isp2iprmt + \"\"\""}
        }
      },
      "ios-route-map:match": {
        "ios-route-map:ip": {
          "ios-route-map:address":{"ios-route-map:access-list": "auto"}
        }
      }
    }
  }
}
```

Question #806 *Topic 1*

Which DNS record type is required to allow APs to discover a WLC by using DNS on IPv4?

A. NS

B. A

C. SOA

D. MX

Correct Answer: *B*

Community vote distribution

B (100%)

djedeen 1 month, 3 weeks ago

Selected Answer: B

B: For AP discovery of WLC via DNS you need an 'A-record' for cisco-lwapp-controller with the Mgmt IP of the WLC (not AP Mgr interface).

upvoted 2 times

Evreni 2 months, 3 weeks ago

Selected Answer: B

B. is correct DNS A
The "A" record maps a hostname to an IPv4 address.

upvoted 3 times

benvz 1 month, 3 weeks ago

no a its "b"

upvoted 1 times

Question #807 *Topic 1*

What is modularity in network design?

A. ability to bundle several functions into a single layer of the network

B. ability to create self-contained, repeatable sections of the network

C. ability to self-heal the network to prevent service outages

D. ability to scale and accommodate future needs of the network

Correct Answer: *B*

Community vote distribution

D (88%) 13%

kaupz Highly Voted 2 months, 3 weeks ago

Selected Answer: D

D,

You can design a campus network in a logical manner, using a modular approach. In this approach, each layer of the hierarchical network model can be broken into basic functional units. These units, or modules, then can be sized appropriately and connected, while allowing for future scalability and expansion.

https://www.ccexpert.us/root-bridge/modular-network-design.html

upvoted 5 times

kivi_bg Most Recent 1 day, 2 hours ago

Answer B
The advantage of the modular approach is largely due to the isolation that it can provide.
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html#wp708877

upvoted 1 times

teems5uk 2 days, 20 hours ago

Selected Answer: B

B. Ability to create self-contained, repeatable sections of the network

The ability to create self-contained, repeatable sections or modules within the network. This approach allows for easier management, troubleshooting, and scalability. Each module can operate independently, and changes or updates in one module should not impact others. Modularity is a key principle in designing networks that are flexible, scalable, and easier to maintain.

upvoted 1 times

Luiggi 1 week, 1 day ago

Selected Answer: D

for me, is D

upvoted 1 times

Fanny1493 2 months ago

Selected Answer: D

i think D correct

upvoted 1 times

```
*Apr 6 13:35:07.826: AAA/BIND(00000055): Bind i/f
*Apr 6 13:35:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Apr 6 13:35:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*Apr 6 13:35:07.826: TPLUS(00000055) login timer started 1020 sec timeout
*Apr 6 13:35:07.826: TPLUS: processing authentication start request id 85
*Apr 6 13:35:07.826: TPLUS: Authentication start packet created for 85()
*Apr 6 13:35:07.826: TPLUS: Using server 10.106.60.182
*Apr 6 13:35:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: Would block while reading
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*Apr 6 13:35:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*Apr 6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr 6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

Refer to the exhibit. An engineer configured TACACS+ to authenticate remote users, but the configuration is not working as expected. Which configuration must be applied to enable access?

A. R1 (config)# ip tacacs source-interface Gig 0/0

B. R1 (config)# tacacs server prod -
R1(config-server-tacacs)# port 1020

C. R1 (config)# aaa authorization exec default group tacacs+ local

D. R1 (config)# tacacs server prod -
R1(config-server-tacacs)# key cisco123

Correct Answer: *D*

Community vote distribution

D (100%)

teems5uk 2 days, 20 hours ago

Selected Answer: D

D.

bash
Copy code
R1(config)# tacacs server prod
R1(config-server-tacacs)# key cisco123
This configuration sets up the TACACS+ server named "prod" with the key "cisco123". Ensure that the key configured on the router matches the key configured on the TACACS+ server. Also, make sure that the TACACS+ server is reachable and correctly configured to handle authentication requests from the router.

upvoted 1 times

Horsefeathers 4 weeks, 1 day ago

Selected Answer: D

This is a sample debug output from the Router, when the TACACS server is configured with a wrong pre shared key:
...
*Apr 6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr 6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).

https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/200467-Troubleshoot-TACACS-Authentication-Issue.html

upvoted 2 times

raajj354 4 weeks, 1 day ago

Please explain. I cannot understand.

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: D

Correct

upvoted 1 times

Question #809 *Topic 1*

A customer has two Cisco WLCs that manage separate APs throughout a building. Each WLC advertises the same SSID but terminates on different interfaces. Users report that they drop their connections and change IP addresses when roaming. Which action resolves this issue?

A. Configure high availability.

B. Enable fast roaming.

C. Configure mobility groups.

D. Enable client load balancing

Correct Answer: *C*

Community vote distribution

C (100%)

kaupz 2 months, 3 weeks ago

Selected Answer: C

Mobility or roaming services enables a WLAN client to retain its association !!!seamlessly!!! while moving from one Access Point to another. Cisco WLAN controllers (WLC) can be organized into wireless mobility groups to support intercontroller roaming.
C - should be
https://study-ccnp.com/what-is-a-wireless-mobility-group/

upvoted 3 times

benvz 1 month, 3 weeks ago

stop confuse people the exam cost 300$

upvoted 1 times

Question #810 *Topic 1*

What is one difference between the RIB and the FIB?

A. The RIB keeps all routing information received from peers, and the FIB keeps the minimum information necessary to make a forwarding decision.

B. The RIB works at the data plane, and the FIB works at the control plane.

C. The FIB contains routing prefixes, and the RIB contains the Layer 2 and Layer 3 information necessary to make a forwarding decision.

D. The RIB is known as the CEF table, and the FIB is known as the routing table.

Correct Answer: *A*

Community vote distribution

A (100%)

kaupz 2 months, 3 weeks ago

Selected Answer: A

Correct

upvoted 3 times

Question #811 *Topic 1*

What is a characteristic of an AP operating in FlexConnect mode?

A. All traffic traverses the WLC to ensure policy enforcement on client traffic.

B. Forwarding for locally switched traffic continues when the AP loses connectivity to the WLC.

C. APs connect in a mesh topology and elect a root AP

D. FlexConnect enables an AP to connect to multiple WLCs.

Correct Answer: *D*

Community vote distribution

B (100%)

teems5uk 2 days, 20 hours ago

Selected Answer: B

B. Forwarding for locally switched traffic continues when the AP loses connectivity to the WLC.

In FlexConnect mode, the access point (AP) is capable of locally switching user traffic and forwarding it directly to the destination without the need to tunnel the traffic back to the wireless LAN controller (WLC). This allows for efficient utilization of network resources and helps to reduce latency. If the AP loses connectivity to the WLC, it can still forward locally switched traffic, providing continuity for user data forwarding even in case of a temporary disconnection from the controller.

upvoted 1 times

Jakubu1 1 month, 1 week ago

Hello Moderators, it would be kind if you could offer the Cisco documentation where the answer you chose exists. Sincerely, A learner.

upvoted 3 times

Wazerface 2 months ago

Selected Answer: B

B for sure

upvoted 1 times

Fanny1493 2 months ago

Selected Answer: B

Correct is B

upvoted 1 times

yassirbouchdak 2 months, 3 weeks ago

Selected Answer: B

Forwarding continues when the AP loses connectivity to the WLC

upvoted 3 times

kaupz 2 months, 3 weeks ago

Selected Answer: B

B should be correct

upvoted 3 times

What is the benefit of using TCAM for IP forwarding decisions versus using the CAM table?

A. TCAM finds results based on binary, and CAM uses the longest match to find results

B. TCAM processes lookups in a hardware CPU. and CAM relies on binary masks to find results.

C. TCAM finds results based on masks, and CAM finds results basing on exact match.

D. TCAM uses low cost hardware memory to store addresses, and CAM uses expensive hardware memory.

Correct Answer: *C*

Community vote distribution

C (70%) B (30%)

teems5uk 2 days, 20 hours ago

Selected Answer: C

The benefit of using TCAM (Ternary Content Addressable Memory) for IP forwarding decisions is that TCAM allows for matching based on masks. TCAM can perform ternary (three-state) matching, which means it can match on exact values as well as wildcard masks. This capability is particularly useful for routing lookups where variable-length prefixes (subnets) are involved. TCAM is efficient for performing lookups based on both exact matches and prefix matches, making it well-suited for forwarding decisions in routers where variable-length subnet masks are common.

On the other hand, CAM (Content Addressable Memory), typically used in traditional MAC address tables, performs exact matching and doesn't support wildcard masks for variable-length matches like TCAM does.

upvoted 1 times

post20 3 weeks, 4 days ago

Correct answer C. Check this link: https://learningnetwork.cisco.com/s/article/tcam-demystified#:~:text=TCAM%20entries%20are%20organized%20by,fast%20operation%20of%20the%20TCAM.

upvoted 1 times

Tadese 4 weeks ago

Selected Answer: C

CAM can only search on exact matches of binary strings.

TCAM, for its part, searches the memory to match the key, like CAM, and can also use a mask to indicate "don't care" or wildcard bits. This results in three possible states: 0, 1 and X, a wildcard. Using mask bits allows for much more flexibility in searching

upvoted 3 times

Horsefeathers 4 weeks, 1 day ago

Selected Answer: C

CAM
-exact matches
-ones and zeros (binary)
-layer 2
TCAM
-VMR (Value, Mask and Result)
-layer 3

https://community.cisco.com/t5/networking-knowledge-base/cam-content-addressable-memory-vs-tcam-ternary-content/ta-p/3107938

upvoted 3 times

Fanny1493 2 months ago

https://community.cisco.com/t5/documentos-routing-y-switching/uso-de-memoria-tcam-y-cam-en-los-routers-y-switchs/ta-p/4536017

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: B

B should be correct

The problem with CAM is that it can only do exact matches on ones and zeros (binary CAMs)

https://community.cisco.com/t5/networking-knowledge-base/cam-content-addressable-memory-vs-tcam-ternary-content/ta-p/3107938

By implementing router prefix lookup in TCAM, we are moving process of Forwarding Information Base lookup from software to hardware.

https://howdoesinternetwork.com/2015/tcam-memory

upvoted 3 times

Question #813 *Topic 1*

```
R1#
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2
OSPF-1 HELLO Gi0/0: No more immediate hello for nbr 10.2.2.2, which has been sent on this intf 2 times
OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 10.0.0.1
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2
OSPF-1 HELLO Gi0/0: No more immediate hello for nbr 10.2.2.2, which has been sent on this intf 2 times
OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 10.0.0.1
OSPF-1 ADJ   Gi0/0: Rcv DBD from 10.2.2.2 seq 0xE09 opt 0x52 flag 0x7 len 32  mtu 1400 state INIT
OSPF-1 ADJ   Gi0/0: 2 Way Communication to 10.2.2.2, state 2WAY
OSPF-1 ADJ   Gi0/0: Neighbor change event
OSPF-1 ADJ   Gi0/0: Nbr 10.2.2.2: Prepare dbase exchange
OSPF-1 ADJ   Gi0/0: Send DBD to 10.2.2.2 seq 0x1C01 opt 0x52 flag 0x7 len 32
OSPF-1 ADJ   Gi0/0: NBR Negotiation Done. We are the SLAVE
OSPF-1 ADJ   Gi0/0: Nbr 10.2.2.2: Summary list built, size 5
OSPF-1 ADJ   Gi0/0: Send DBD to 10.2.2.2 seq 0xE09 opt 0x52 flag 0x2 len 132
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2
OSPF-1 ADJ   Gi0/0: Rcv DBD from 10.2.2.2 seq 0xE09 opt 0x52 flag 0x7 len 32  mtu 1400 state EXCHANGE
OSPF-1 ADJ   Gi0/0: Nbr 10.2.2.2 has smaller interface MTU
OSPF-1 ADJ   Gi0/0: Send DBD to 10.2.2.2 seq 0xE09 opt 0x52 flag 0x2 len 132
OSPF-1 HELLO Gi0/0: Rcv hello from 10.2.2.2 area 0 10.0.0.2
OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 10.0.0.1
```

Refer to the exhibit. Two indirectly connected routers fail to form an OSPF neighborship. What is the cause of the issue?

A. failing hello packets between the two routers

B. DR/BDR selection dispute

C. MTU mismatch

D. OSPF network type mismatch

Correct Answer: *C*

Community vote distribution

C (100%)

Evreni 2 months, 3 weeks ago

Selected Answer: C

C is correct
neighbor 10.2.2.2 has smaller interface MTU

upvoted 3 times

Question #814 *Topic 1*

Which feature is provided by Cisco Mobility Services Engine in a Cisco Wireless Unified Network architecture?

A. It adds client packet capturing.

B. It enables NetFlow data collection.

C. It adds client tracking and location API.

D. It identifies authentication problems.

Correct Answer: *C*

Community vote distribution

C (100%)

teems5uk 2 days, 20 hours ago

Selected Answer: C

C. It adds client tracking and location API.

Cisco Mobility Services Engine (MSE) in a Cisco Wireless Unified Network architecture provides features related to location-based services. It adds client tracking and offers a location API (Application Programming Interface) that allows applications to access information about the location of wireless clients within the network. This capability enables the development of location-aware applications and services. MSE can provide information about the real-time location of wireless clients, facilitating applications such as asset tracking, location-based services, and more.

upvoted 1 times

shefo1 1 month, 3 weeks ago

from OCG p.553

Cisco APs and WLCs can integrate with management
platforms like Cisco Prime Infrastructure or DNA Center, along with location servers like
Cisco Mobility Services Engine (MSE), Cisco Connected Mobile Experiences (CMX), or
Cisco DNA Spaces to gather location information in real time and present that information
in a relevant way.

upvoted 3 times

kaupz 2 months, 3 weeks ago

Selected Answer: C

should be C, but not so sure about API part

This solution allows a customer to track any Wi-Fi device, including clients, active RFID tags, and rogue clients and access points (APs).
https://mrncciew.com/2013/04/05/mobility-service-engine-mse/

upvoted 2 times

Question #815 *Topic 1*

Which unit of measure is used to measure wireless RF SNR?

A. dBi

B. dB

C. dBm

D. mW

Correct Answer: *C*

Community vote distribution

B (100%)

eearmani 1 month ago

SNR in dB

upvoted 2 times

Din04 1 month, 3 weeks ago

Selected Answer: B

SNR is in dB

upvoted 2 times

Fanny1493 2 months ago

Selected Answer: B

dB its to SNR
https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength

upvoted 3 times

Calinserban 2 months, 1 week ago

bBm is for RSSI power that can be measured in W.
dB is the difference between RSSI leves.
Answer is B

upvoted 3 times

Just_little_me 2 months, 1 week ago

Selected Answer: B

i think it also B
https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength

upvoted 1 times

zahardb57 2 months, 1 week ago

From that link it says dB answer needs to be B.

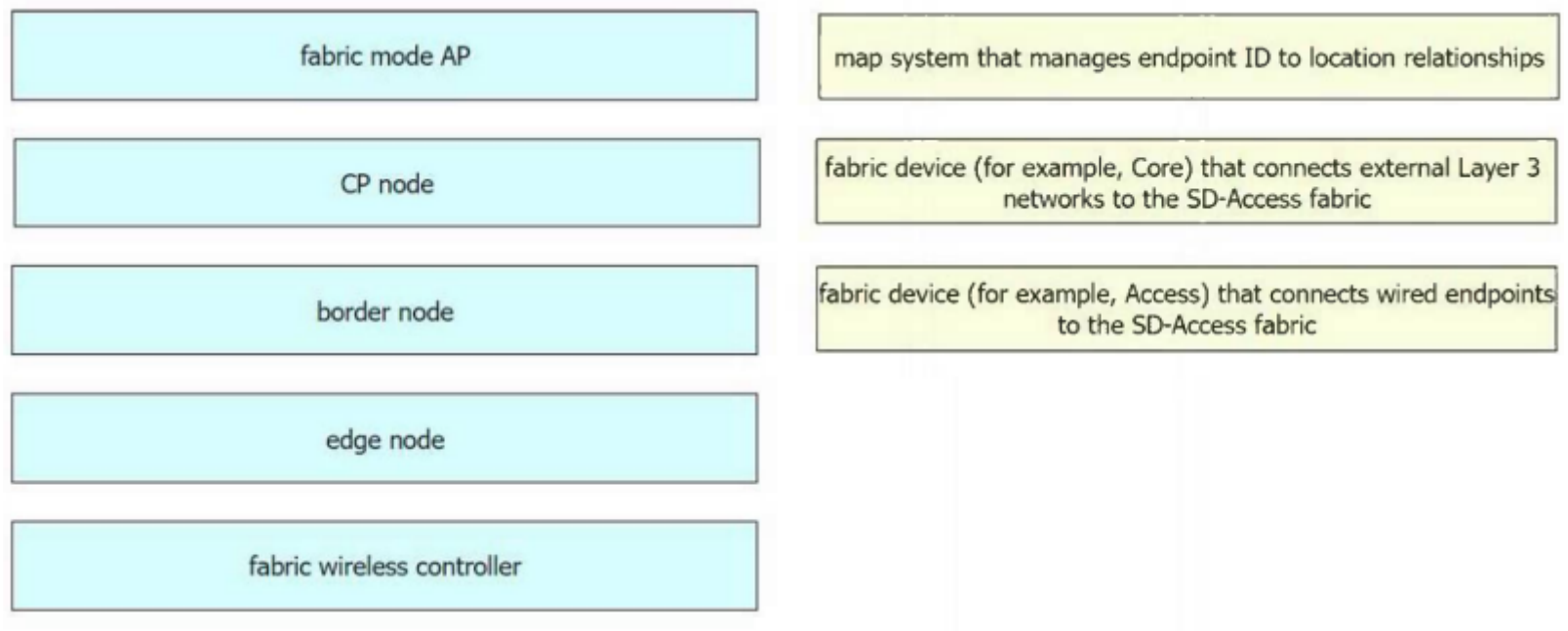
Evreni 2 months, 3 weeks ago

C looks correct
https://www.sonicwall.com/support/knowledge-base/rf-basic-background-signal-strength-and-snr/170505562736646/#:~:text=SNR%20(Signal%20to%20Noise%20Radio,to%20be%20considered%20during%20deployment.

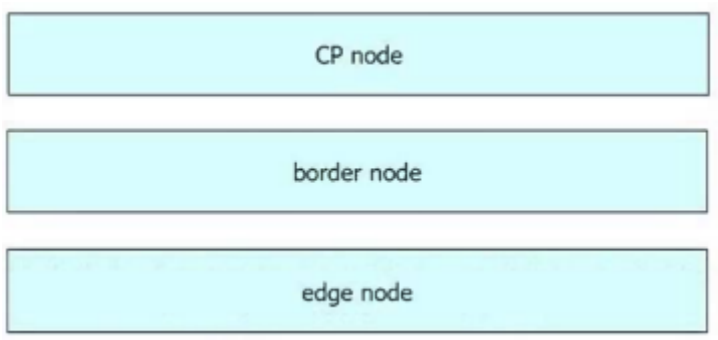
upvoted 2 times

DRAG DROP
-

Drag and drop the components of the Cisco SD-Access fabric architecture from the left onto the correct descriptions on the right. Not all options are used.



Correct Answer:



b7c04a1 1 month, 2 weeks ago

Guys whats is CP node?

upvoted 1 times

b7c04a1 1 month ago

Forget this, i found https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf

upvoted 2 times

kaupz 2 months, 3 weeks ago

CP
border node
edge node
seems logical

upvoted 3 times

Question #817 *Topic 1*

In a campus network design, what are two benefits of using BFD for failure detection? (Choose two.)

A. BFD speeds up routing convergence time.

B. BFD is an efficient way to reduce memory and CPU usage.

C. BFD provides fault tolerance by enabling multiple routers to appear as a single virtual router.

D. BFD provides path failure detection in less than a second.

E. BFD enables network peers to continue forwarding packets in the event of a restart.

Correct Answer: *AD*

Community vote distribution

AD (100%)

Fanny1493 2 months ago

Selected Answer: AD

correct answer

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: AD

provided answer is correct

upvoted 2 times

Question #818 *Topic 1*

```
router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
router#

12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05:     ICMP type=0, code=0
12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05:     ICMP type=0, code=0
12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05:     ICMP type=0, code=0
```

Refer to the exhibit. A network engineer issues the debug command while troubleshooting a network issue. What does the output confirm?

A. ACL 100 is tracking ICMP traffic from 10.1.1.1 destined for 1.1.1.1.

B. ACL100 is tracking all traffic from 10.1.1.1 destined for 1.1.1.1.

C. ACL100 is tracking ICMP traffic from Serial1/0 destined for Serial3/0.

D. ACL100 is tracking ICMP traffic from 1.1.1.1 destined for 10.1.1.1.

Correct Answer: *D*

Community vote distribution

D (100%)

NikosTsironis 1 month, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

Evreni 2 months, 3 weeks ago

Selected Answer: D

Correct

upvoted 2 times

kaupz 2 months, 3 weeks ago

A. ACL 100 is tracking ICMP traffic from 10.1.1.1 destined for 1.1.1.1. -- source is 1.1.1.1 --wrong
B. ACL100 is tracking all traffic from 10.1.1.1 destined for 1.1.1.1.-- source is 1.1.1.1 --wrong
C. ACL100 is tracking ICMP traffic from Serial1/0 destined for Serial3/0. -- tracks ips that just happen to be in these interfaces, ACL is configured with ips --wrong
D. ACL100 is tracking ICMP traffic from 1.1.1.1 destined for 10.1.1.1. -- seems to be correct

upvoted 3 times

```
line vty 0 4
 exec-timeout 120 0
 login local
line vty 5 15
 exec-timeout 30 0
 login local
```

Refer to the exhibit. An engineer must update the existing configuration to achieve these results:

• Only administrators from the 192.168.1.0/24 subnet can access the vty lines.
• Access to the vty lines using clear-text protocols is prohibited.

Which command set should be applied?

A.
```
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 15
access-class 1 in
transport input none
```

B.
```
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 15
access-class 1 in
transport input telnet ssh
```

C.
```
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 15
access-class 1 in
transport input ssh
```

D.
```
access-list 1 permit 192.168.1.0 255.255.255.0
line vty 0 15
access-class 1 in
transport input telnet rlogin
```

Correct Answer: *C*

Community vote distribution

C (100%)

NikosTsironis 1 month, 1 week ago

Selected Answer: C

C is correct - wildcard mask and ssh

upvoted 1 times

Evreni 2 months, 3 weeks ago

Selected Answer: C

C: looks correct
clear-text protocols is prohibited.
Transport input SSH

upvoted 4 times

Question #820 *Topic 1*

Which version of NetFlow does Cisco Threat Defense utilize to obtain visibility into the network?

A. NBAR2

B. IPFIX

C. 8

D. flexible

Correct Answer: *D*

Community vote distribution

D (100%)

kldoyle97 1 week, 5 days ago

"The latest iteration of Cisco-developed NetFlow is Flexible NetFlow. Flexible NetFlow extends NetFlow version 9 capabilities to help customer determine how to optimize resource usage, plan network capacity, and identify the optimal application layer for quality of service (QoS)."
https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

upvoted 1 times

Just_little_me 2 months, 1 week ago

check if you want to read more
https://community.cisco.com/t5/security-knowledge-base/configuring-nsel-netflow-on-cisco-firepower-threat-defense-ftd/ta-p/3646300

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: D

flexible

upvoted 2 times

Question #821 *Topic 1*

```
1  def main():
2      vlans = {'vlan10':'192.168.1.0',
3           'vlan20':'192.168.2.0',
4           'vlan30':'192.168.3.0' }
5      vlans_key(vlans)
6
7  def vlans_key(vlans):
8      for key in vlans.keys():
9          print(str(key) +' '+ str(vlans[key]))
10
11 if __name__ == '__main__':
12     main()
```

Refer to the exhibit. What is printed to the console when this script is run?

A. a key-value pair in tuple type

B. an error

C. a key-value pair in list type

D. a key-value pair in string type

Correct Answer: *D*

Community vote distribution

D (100%)

Horsefeathers 4 weeks, 1 day ago

Selected Answer: D

Here is the output of the Python program:

```
vlan10 192.168.1.0
vlan20 192.168.2.0
vlan30 192.168.3.0
```

A string representation of key-value pairs with a space separating the key and value.

upvoted 2 times

Question #822 *Topic 1*

What is a difference between Chef and other automation tools?

A. Chef is an agentless tool that uses playbooks, and Ansible is an agent-based tool that uses cookbooks.

B. Chef is an agentless tool that uses a primary/minion architecture, and SaltStack is an agent-based tool that uses a primary/secondary architecture

C. Chef is an agent-based tool that uses cookbooks, and Ansible is an agentless tool that uses playbooks.

D. Chef uses Domain Specific Language, and Puppet uses Ruby.

Correct Answer: *C*

Community vote distribution

C (100%)

janbaz 1 month ago

Selected Answer: C

Given answer is correct

upvoted 1 times

NikosTsironis 1 month, 1 week ago

Selected Answer: C

https://learningnetwork.cisco.com/s/question/0D56e0000CwDQqvCQG/what-is-chef

Chef uses different terminology to Puppet. Instead of modules and manifests, Chef has cookbooks and recipes.

A kitchen is an environment where recipes and cookbooks are tested before deployment.

upvoted 1 times

Evreni 2 months, 3 weeks ago

Selected Answer: C

C: is correct

Chef is agent based tool that uses cookbooks

upvoted 3 times

Question #823 *Topic 1*

An engineer must configure a new WLAN that supports 802.11r and requires users to enter a passphrase. What must be configured to support this requirement?

A. 802.1X and Fast Transition

B. FT PSK and Fast Transition

C. 802.1X and SUITEB-1X

D. FT PSK and SUITEB-1X

Correct Answer: *D*

Community vote distribution

B (100%)

kaupz Highly Voted 2 months, 3 weeks ago

Selected Answer: B

802.11r is FT -- so It is A or B
But A requires users to authenticate not only with password, but with username also, and PSK indicates PreSharedKey.
B should be the correct answer
https://blogs.cisco.com/networking/what-is-802-11r-why-is-this-important

upvoted 5 times

janbaz Most Recent 1 month ago

Selected Answer: B

Fast Transition (FT), often referred to as 802.11r, allows wireless clients to seamlessly switch between access points (APs) within the same WLAN without any noticeable interruption in connectivity. This significantly improves the user experience, especially for mobile users or applications sensitive to network disruptions.

upvoted 2 times

Jakubu1 1 month, 1 week ago

Hello Moderators, it would be kind if you could offer the Cisco documentation where the answer you chose exists. Sincerely, A learner.

upvoted 2 times

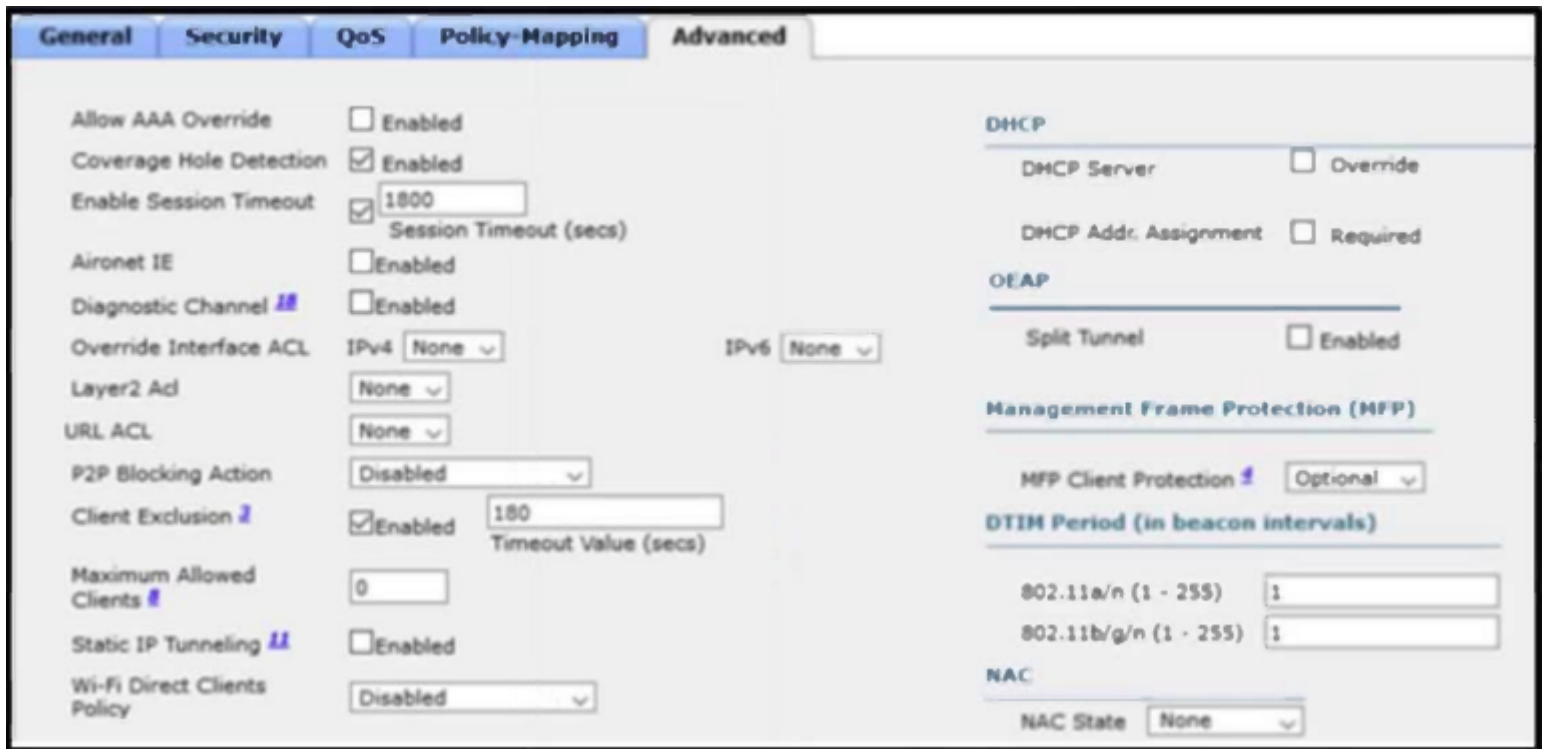
Fanny1493 2 months ago

Selected Answer: B

Correct answer is B

upvoted 2 times

Question #824 *Topic 1*



Refer to the exhibit. An engineer is troubleshooting an mDNS issue in an environment where Cisco ISE is used to dynamically assign mDNS roles to users. The engineer has confirmed that ISE is sending the correct values, but name resolution is not functioning as expected. Which WLC configuration change resolves the issue?

A. Enable AAA Override.

B. Enable Aironet IE.

C. Set MFP client protection to Required.

D. Change NAC state to ISE NAC.

Correct Answer: *A*

Community vote distribution

A (100%)

cwauch 3 weeks ago

Selected Answer: A

The answer is enable AAA Overide.
On the controller, enable the Allow AAA Override configuration parameter using the GUI or CLI. Enabling this parameter allows the controller to accept the attributes returned by the RADIUS server. The controller then applies these attributes to its clients.

upvoted 1 times

Jakubu1 1 month, 1 week ago

Hello Moderators, it would be kind if you could offer the Cisco documentation where the answer you chose exists. Sincerely, A learner.

upvoted 2 times

Toob93 1 month ago

There is no cisco documentation. They use ChatGPT lol

upvoted 1 times

Horsefeathers 4 weeks, 1 day ago

Speaking of ChatGPT:
Given the scenario where Cisco ISE is used to dynamically assign mDNS roles to users, and the issue is with name resolution not functioning as expected despite ISE sending correct values, the most relevant configuration option to consider on the Cisco Wireless LAN Controller (WLC) is likely to be: Changing NAC State to ISE NAC.

By changing the NAC state to ISE NAC, you are ensuring a more comprehensive integration with Cisco ISE, which could potentially resolve issues related to dynamic role assignments and permissions influencing name resolution.

I'm going with D.

upvoted 1 times

Horsefeathers 3 weeks, 5 days ago

Disregard this I think it's most likely Enable AAA Override now, one of the earlier questions about ISE functioning correctly with WLC required enabling it too.

upvoted 1 times

Question #825 *Topic 1*

What is one role of the VTEP in a VXLAN environment?

A. to maintain VLAN configuration consistency

B. to forward packets to non-LISP sites

C. to provide EID-to-RLOC mapping

D. to encapsulate the tunnel

Correct Answer: *D*

Community vote distribution

D (100%)

teems5uk 2 days, 19 hours ago

Selected Answer: D

virtual tunnel endpoint (VTEP) An entity that originates or terminates a VXLAN tunnel. It maps Layer 2 and Layer 3 packets to the VNI to be used in the overlay network.

upvoted 1 times

Just_little_me 2 months, 1 week ago

Selected Answer: D

VTEP = VXLAN Tunnel Endpoint = what switch to tunnel traffic to, for delivery to that IP / MAC (computer).
https://netcraftsmen.com/sd-access-flows-registration-and-same-fabric-forwarding/

upvoted 1 times

kaupz 2 months, 3 weeks ago

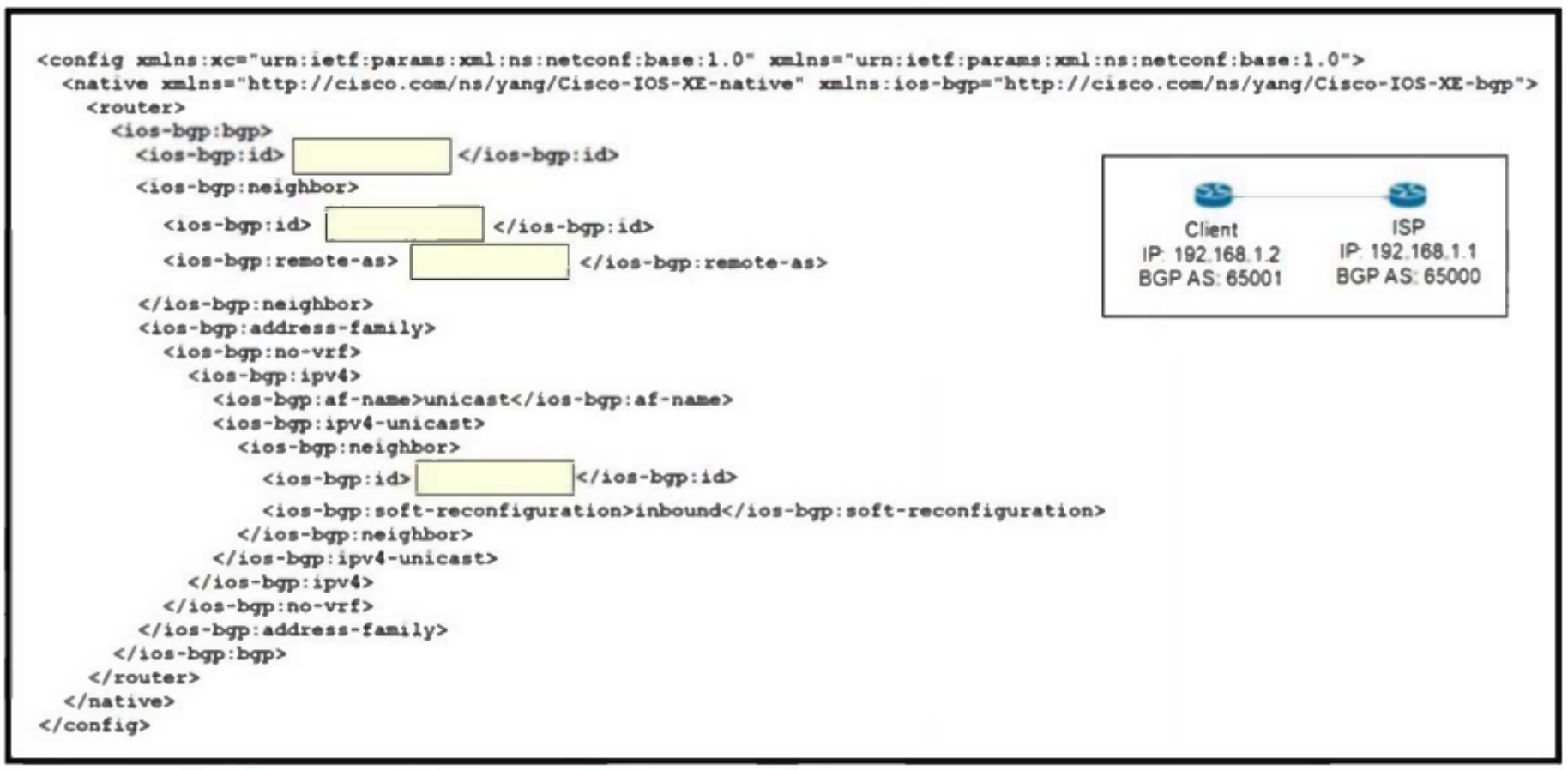
vtep encapsulates/decapsulates VXLANs

upvoted 2 times

DRAG DROP

-

Drag and drop the snippets onto the blanks within the code to construct a script that configures BGP according to the topology. Not all options are used, and some options may be used twice.



192.168.1.1 | 192.168.1.2 | 65000 | 65001

Correct Answer:

IgorLVG 1 week, 5 days ago

the router id is an IP address.

ref: https://iosxr-lab-ciscolive.github.io/LTRSPG-2414-cleur2019/wkinstructions/2019-02-01-step-5-playing-iosxr-Yang-Models/
should be
192.168.1.2
192.168.1.1
65000
192.168.1.2

upvoted 1 times

Din04 1 month, 2 weeks ago

Where did you guys get the hint that we're configuring from the client router?

upvoted 3 times

Horsefeathers 4 weeks, 1 day ago

The exam is Enterprise Core so we are the Enterprise/Client not the Service Provider. And the answer is correct.

upvoted 2 times

Din04 3 weeks, 6 days ago

Okay this makes sense.

upvoted 1 times

adamzet33 3 weeks, 6 days ago

That is really a piece of creative logic.. after so many questions proving otherwise:)

upvoted 1 times

Storcaks 1 month, 3 weeks ago

Given answer is correct.
65001
182.168.1.1
65000
192.168.1.1
https://www.noction.com/blog/bgp-yang-next-generation

upvoted 2 times

adamzet33 2 months, 1 week ago

In my opinion:
192.168.1.2
192.168.1.1
65000
192.168.1.2

upvoted 2 times

studying_1 2 months, 1 week ago

No, answer is correct ... on client router
router bgp 65001
neighbor 192.168.1.1 remote-as 65000
address family ipv4 ... neighbor 192.168.1.1

upvoted 1 times

kaupz 2 months, 3 weeks ago

correct

upvoted 1 times

Question #827 *Topic 1*

How is CAPWAP data traffic encapsulated when running an Over the Top WLAN in a Cisco SD-Access wireless environment?

A. LISP

B. VXLAN

C. GRE

D. IPsec

Correct Answer: *B*

Community vote distribution

B (100%)

kaupz 2 months, 3 weeks ago

Selected Answer: B

B
page 98 Figure 29 is about OTT network design

https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf

upvoted 4 times

```
PYTHON CODE:
import requests
import json

url='http://switch.foo.com/ins'
switchuser='username'
switchpassword='password'

myheaders={'content-type':'application/json'}
payload={
  "ins_api": {
    "version": "1.0",
    "type": "cli_conf",
    "chunk": "0",
    "sid": "1",
    "input": "configure terminal ;interface e1/32 ;shutdown",
    "output_format": "json"
  }
}
response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword)).json()
```

Refer to the exhibit. What does the Python code accomplish?

A. It configures interface e1/32 to be in an admin down state

B. It generates a status code of 403 because the type is incorrect.

C. It configures interface e1/32 to be in an err-disable state.

D. It returns data in JSON-RPC format.

Correct Answer: *A*

```
CPE# show iox-service
IOx service (CAF)          : Not Running
IOx service (HA)           : Not Supported
IOx service (IOxman)       : Not Running
Libvirtd                   : Running

CPE# show platform software yang-management process
confd            : Running
nesd             : Running
syncfd           : Running
ncsshd           : Not Running
dmiauthd         : Running
nginx            : Not Running
ndbmand          : Running
pubd             : Running
```

Refer to the exhibit. Which action must be performed to allow RESTCONF access to the device?

A. Enable the NETCONF service.

B. Enable the SSH service.

C. Enable the IOX service.

D. Enable the HTTPS service.

Correct Answer: *D*

Community vote distribution

D (100%)

kaupz 2 months, 3 weeks ago

Selected Answer: D

RESTCONF runs over HTTPS. The following commands must be enabled to support RESTCONF over port 443:

ip http secure-server

https://developer.cisco.com/docs/ios-xe/#!enabling-restconf-on-ios-xe/authentication

Hence D

upvoted 3 times

Which JSON script is properly formatted?

A.
```
"student":[
      {
          "grade":"9",
          "ID":"7460059362",
          "type":"on-line",
       }]
```

B.
```
{
   "plants":
      [
          "name":"Fern",
          "color":"green",
          "type":"indoor",
       ]
}
```

C.
```
{
  "class": [
   {
   "title":"Cooking 101",
    "type":"elective",
    "session":"fall"
   }
  ]
 }
```

D.
```
[
  "class": {
   [
    "title":"History",
    "grade":"5",
    "location":"Site 2"
   }
  ]
]
```

Correct Answer: *C*

Community vote distribution

C (100%)

kaupz Highly Voted 2 months, 3 weeks ago

Selected Answer: C

A & B end with ,
D brackets openings/locations/closings are all messed up
Only option left is C

upvoted 6 times

Question #831 *Topic 1*

Which technology is used as the basis for the Cisco SD-Access data plane?

A. LISP

B. 802.1Q

C. VXLAN

D. IPsec

Correct Answer: *C*

Community vote distribution

C (100%)

kaupz 2 months, 3 weeks ago

Selected Answer: C

VXLAN is correct

upvoted 3 times

Question #832 *Topic 1*

How is OAuth framework used in REST API?

A. as a framework to hash the security information in the REST URL

B. by providing the external application a token that authorizes access to the account

C. as a framework to hide the security information in the REST URL

D. by providing the user credentials to the external application

Correct Answer: *B*

Community vote distribution

B (100%)

Horsefeathers 4 weeks, 1 day ago

Selected Answer: B

The threat defense REST API uses Oauth 2.0 for authenticating calls from API clients. OAuth is an access token-based method, and the threat defense uses JSON web tokens for the schema.

https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-api/guide/ftd-rest-api/auth-ftd-rest-api.pdf

upvoted 2 times

Question #833 *Topic 1*

What is a characteristic of Cisco DNA southbound APIs?

A. implements monitoring by using the SOAP protocol

B. enables orchestration and automation of network devices based on intent

C. utilizes REST API

D. simplifies management of network devices

Correct Answer: *D*

Community vote distribution

B (70%) D (30%)

kldoyle97 1 day, 17 hours ago

Selected Answer: D

North Bound APIs are intent based.
Southbound APIs are made for device management. (Vendor neutral/agnostic)

upvoted 1 times

teems5uk 2 days, 19 hours ago

Selected Answer: B

Considering this from the OCG page 820:
"Southbound API
If a network operator makes a change to a switch's configuration in the management software of the controller, those changes are then pushed down to the individual devices by using a Southbound API. These devices can be routers, switches, or even wireless access points. APIs interact with the components of a network through the use of a programmatic interface."
Both B and D make sense, but I'll go with the option B.

upvoted 1 times

kiyaye1 3 weeks, 1 day ago

Selected Answer: D

This has to be D, B inclines to NB APIs

upvoted 2 times

raajj354 4 weeks ago

D is more apt. It's to manage NW devices. As simple as that.

upvoted 2 times

Tadese 1 month ago

Select Answer D
B is not correct because Northbound—Intent APIs
Intent APIs enable developers to access Cisco DNA Center Automation and Assurance workflows. Through this access, you can simplify the process of creating workflows that consolidate multiple network actions.

upvoted 3 times

peugeotdude 1 month, 1 week ago

Selected Answer: B

B makes sense to me

upvoted 2 times

Just_little_me 2 months, 1 week ago

Southbound is primarily aimed at non-Cisco "thirdparty" devices!

Northbound: Discovery and management of the network over REST API
Southbound: SDK integration into the DNA Center via device packs to support multivendor environment
Eastbound: Event / Notification Handler
Westbound: Integration of reporting, analysis, service management

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: B

southbound api-s are used for communicating network devices - thinking B here

upvoted 4 times

Question #834 *Topic 1*

Where is the wireless LAN controller located in a mobility express deployment?

A. The wireless LAN controller exists in a server that is dedicated for this purpose.

B. The wireless LAN controller is embedded into the access point.

C. The wireless LAN controller exists in the cloud.

D. There is no wireless LAN controller in the network.

Correct Answer: *B*

Community vote distribution

B (90%) 10%

kaupz Highly Voted 2 months, 3 weeks ago

Selected Answer: B

In a Cisco Mobility Express network, Access Point (AP) running the wireless controller function is designated as the primary AP - Answer B, since WLC lives in AP.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-2/b_Mobility_Express_Deployment_guide/b_Mobility_Express_Deployment_guide_chapter_01.html

upvoted 6 times

Evreni 2 months, 3 weeks ago

yes, you are right, its B
i missunderstood question

upvoted 2 times

teems5uk Most Recent 2 days, 19 hours ago

Selected Answer: B

B. The wireless LAN controller is embedded into the access point.

In a Cisco Mobility Express deployment, the wireless LAN controller functionality is embedded directly into one of the access points, which is designated as the "master" access point. This allows the network to function without the need for a separate physical wireless LAN controller device. The master access point manages and coordinates the activities of other access points in the network, providing centralized control for WLAN configuration, security, and management functions.

upvoted 1 times

Fanny1493 2 months ago

Selected Answer: B

Correct anwer is B

upvoted 2 times

Evreni 2 months, 3 weeks ago

Selected Answer: A

i think the correct answer is A: because WLC should be on a server

upvoted 1 times

Question #835 *Topic 1*

```
Router# show running-config
! lines omitted for brevity
enable secret 5 $dfefw525ffd$@$R@D2d2d2f
username cisco password 0 cisco
aaa new-model
radius-server host 10.11.11.11 auth-port 1812 acct-port 1646
radius-server host 10.11.11.12 auth-port 1645 acct-port 1646
radius-server key cisco123
```

Refer to the exhibit. A network engineer must permit administrators to automatically authenticate if there is no response from either of the AAA servers. Which configuration achieves these results?

A. aaa authentication enable default group radius local

B. aaa authentication login default group radius

C. aaa authentication login default group tacacs+ line

D. aaa authentication login default group radius none

Correct Answer: *D*

Community vote distribution

D (100%)

kaupz 2 months, 3 weeks ago

Selected Answer: D

authenticates automatically a.k.a. no authentication

upvoted 2 times

TheGorn 2 months ago

And it's the only logical one that is of the type "login".

upvoted 1 times

Question #836 *Topic 1*

Which hypervisor requires a host OS to run and is not allowed to directly access the hosts hardware and resources?

A. native

B. bare metal

C. type 1

D. type 2

Correct Answer: *D*

Community vote distribution

D (100%)

Evreni Highly Voted 2 months, 3 weeks ago

Selected Answer: D

The correct answer is D:

upvoted 6 times

```
<?xml version="1.0"?>
<nc:rpc message-id="101" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
    <nc:get>
        <nc:filter type="subtree">
            <native xmlns="http://cisco.com/ns/yang/ned/ios">
             <interface>
              <GigabitEthernet>
               <name>1</name>
                 <ip></ip>
              </GigabitEthernet>
             </interface>
            </native>
        </nc:filter>
    </nc:get>
</nc:rpc>
]]>]]>
```

Refer to the exhibit. The NETCONF object is sent to a Cisco IOS XE switch. What is the purpose of the object?

A. Discover the IP address of interface GigabitEthernet1

B. Remove the IP address from interface GigabitEthernet1

C. Set the description of interface GigabitEthernet1 to "1"

D. View the configuration of all GigabitEthernet interfaces

Correct Answer: *A*

Community vote distribution

A (100%)

kaupz Highly Voted 2 months, 3 weeks ago

Selected Answer: A

Correct

upvoted 5 times

Question #838 *Topic 1*

Which protocol does Cisco SD-WAN use to protect control plane communication?

A. STUN

B. OMP

C. IPsec

D. DTLS

Correct Answer: *D*

Community vote distribution

D (100%)

kaupz Highly Voted 2 months, 3 weeks ago

Selected Answer: D

correct

upvoted 5 times

nobodyknows11 Most Recent 2 weeks, 5 days ago

Selected Answer: D

correct

upvoted 1 times

Question #839 *Topic 1*

Which security option protects credentials from sniffer attacks in a basicAPI authentication?

A. next-generation firewall

B. TLS or SSL for communication

C. VPN connection between client and server

D. AAA services to authenticate the API

Correct Answer: *B*

Community vote distribution

B (100%)

NikosTsironis 1 month, 1 week ago

Selected Answer: B

Correct, it cant be anything from the rese

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: B

correct

upvoted 3 times

Question #840 *Topic 1*

Which mechanism can be used to enforce network access authentication against an AAA server if the endpoint does not support the 802.1X supplicant functionality?

A. WebAuth

B. MACsec

C. private VLANs

D. port security

Correct Answer: *A*

Community vote distribution

A (80%) D (20%)

teems5uk 2 days, 18 hours ago

Selected Answer: A

Correct!

upvoted 1 times

b7c04a1 1 month, 2 weeks ago

Selected Answer: D

"Use the web-based authentication feature, known as web authentication proxy, to authenticate end users on host systems that do not run the IEEE 802.1x supplicant."
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-2/configuration_guide/sec/b_172_sec_9600_cg/configuring_web_based_authentication.html

upvoted 1 times

b7c04a1 1 month, 2 weeks ago

Sorry, Answer is A

upvoted 3 times

kaupz 2 months, 3 weeks ago

Selected Answer: A

correct

upvoted 3 times

Question #841 *Topic 1*

An engineer must configure router R1 to validate user logins via RADIUS and fall back to the local user database if the RADIUS server is not available. Which configuration must be applied?

A. aaa authentication exec default radius local

B. aaa authentication exec default radius

C. aaa authorization exec default radius local

D. aaa authorization exec default radius

Correct Answer: *A*

Community vote distribution

A (63%) C (38%)

sledgey121 3 weeks, 6 days ago

Selected Answer: C

Answer C as answer A doesn't exist. Its a poorly worded question but you must choose what actually exists.

upvoted 2 times

raajj354 4 weeks ago

Answer should be C.

upvoted 1 times

Horsefeathers 4 weeks ago

Selected Answer: A

The commands are wrong. They should have been:
a) aaa authentication login default group radius local
b) aaa authentication login default group radius
c) aaa authorization exec default group radius local
d) aaa authorization exec default group radius

We can eliminate B & D because without "local" keyword, if the AAA server does not reply to the authentication/authorization request, the authentication/authorization fails.

The reason I selected A is:
"Authentication allows administrators to identify who can connect to a router by including the user's username and password."
"Authorization comes into play after authentication. Authorization allows administrators to control the level of access users have after they successfully gain access to the router."

Validate user logins - authentication.

https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

https://www.ciscopress.com/articles/article.asp?p=422947&seqNum=2

upvoted 2 times

Horsefeathers 3 weeks, 5 days ago

If the question remains the same but the answers look like this:
a) aaa authentication exec default group radius local
b) aaa authentication exec default group radius
c) aaa authorization exec default group radius local
d) aaa authorization exec default group radius,
then I'd go with C.

upvoted 1 times

NikosTsironis 1 month, 1 week ago

Selected Answer: C

The correct is C but its missing the " default ". It should be :
C. aaa authorization exec default group radius local Most Voted

https://www.examtopics.com/discussions/cisco/view/102230-exam-350-401-topic-1-question-726-discussion/

upvoted 1 times

NikosTsironis 1 month, 1 week ago

sorry i wanted to write " group "

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: A

correct

upvoted 3 times

kaupz 2 months, 3 weeks ago

sorry, C is closest correct answer
since no such command as "aaa authentication exec default radius local"- so instead of authentication, the authorization is the closest hit, although as I understand then they want to validate user logins(a.k.a check user and password), not set the permissions and rights.
dumb question

upvoted 3 times

Wazerface 1 month, 4 weeks ago

I agree

upvoted 1 times

Question #842 *Topic 1*

What does the Cisco WLC Layer 3 roaming feature allow clients to do?

A. maintain their IP address when roaming to an AP or controller with a different client VLAN assignment

B. maintain their connection between APs even when the AP management VLANs are different

C. maintain their connection even if the client IP address changes when roaming

D. roam seamlessly between controllers even when the controller management VLANs are different

Correct Answer: *A*

Community vote distribution

A (67%) D (33%)

Horsefeathers 4 weeks ago

Selected Answer: A

Layer 3 roaming occurs when the wireless LAN interfaces of the controllers are on different IP subnets.
The roam remains transparent to the wireless client, and the client maintains its original IP address.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/overview.html

upvoted 1 times

riktammenaars 1 month, 2 weeks ago

Selected Answer: A

When a client initiates an L3 intercontroller roam, the two controllers involved can compare the VLAN numbers that are assigned to their respective WLAN interfaces
If the two VLAN IDs differ, the controllers arrange a Layer 3 roam (also known as a local-to-foreign roam) that will allow the client to keep using its IP address.

D: wrong -> talks about management VLAN of the controller

upvoted 3 times

Fanny1493 2 months ago

Correct A

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: D

L3 roaming enables client to preserve its ip when roaming to an AP that is connected to another WLC
https://study-ccnp.com/wlan-intercontroller-layer-2-layer-3-roaming/

upvoted 2 times

Alondrix 2 months, 3 weeks ago

I think you mean A based on your response.

upvoted 2 times

Question #843 *Topic 1*

Which JSON script is properly formatted?

A.
```
["animals": {
            "type": horse,
            "breed":"Palamino,
            "color":tan
          }
 ]
```

B.
```
[ "Vendor":
        {
            "type":wholesale,
            "location":on-line,
            "contact":646-168-2143
         }
]
```

C.
```
[
    "subject":
 {
   "title":"Language"
   "ID":"841963"
   "location":"Main Campus"
 }
]
```

D.
```
{
  "plants": [
  {
   "type":"annual",
    "color":"yellow",
    "season":"summer"
  }
 ]
}
```

Correct Answer: *A*

Community vote distribution

D (100%)

Fanny1493 Highly Voted 2 months ago

Selected Answer: D

correct its D

upvoted 6 times

kaupz Highly Voted 2 months, 3 weeks ago

Selected Answer: D

Thinking D here

upvoted 5 times

Alondrix 2 months, 3 weeks ago

Agree, the script needs to be enclosed within { }. Answer D is the only option where this is true.

upvoted 1 times

Horsefeathers 4 weeks ago

Additionally option C is missing commas in the list and A & B are missing quotes for values.

upvoted 1 times

Question #844 *Topic 1*

What is the function of Cisco DNA Center in a Cisco SD-Access deployment?

A. It is responsible for the design, management, deployment, provisioning, and assurance of the fabric network devices

B. It is responsible for routing decisions inside the fabric

C. It provides integration and automation for all nonfabric nodes and their fabric counterparts

D. It possesses information about all endpoints, nodes, and external networks related to the fabric

Correct Answer: *A*

Community vote distribution

A (100%)

Fanny1493 2 months ago

Selected Answer: A

Correct A

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: A

correct

upvoted 2 times

Question #845 *Topic 1*

How do the MAC address table and TCAM differ?

A. TCAM is populated from the ARP file, and the MAC address table is populated from the switch configuration file

B. TCAM stores Layer 2 forwarding information, and the MAC address table stores QoS information

C. TCAM lookups can match only 1s and 0s, and MAC address lookups can match 1s, 0s and a third "care/don't care" state

D. TCAM is a type of memory and the MAC address table is a logical structure

Correct Answer: *D*

Community vote distribution

D (88%) 13%

teems5uk 2 days ago

Selected Answer: D

D. TCAM is a type of memory, and the MAC address table is a logical structure.

upvoted 1 times

b7c04a1 1 month, 1 week ago

Selected Answer: D

https://www.geeksforgeeks.org/difference-between-tcam-and-cam/

upvoted 3 times

Fanny1493 2 months ago

Selected Answer: A

I thik that correct answer is A

upvoted 1 times

TheGorn 1 month, 3 weeks ago

Mac address-table is populated as traffic ingresses into the port from hosts. Not sure the 2nd part of the answer in A is quite right. It seems to suggest that the only way to populate it would be with a static entry.

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: D

since A,B,C are wrong, then D is left

upvoted 3 times

Question #846 *Topic 1*

Which technology provides an overlay fabric to connect remote locations utilizing commodity data paths and improves network performance, boosts security, and reduces costs?

A. InfiniBand

B. VTEP

C. SD-WAN

D. VXLAN

Correct Answer: *C*

Community vote distribution

C (100%)

kaupz 2 months, 3 weeks ago

Selected Answer: C

correct

upvoted 4 times

Question #847 *Topic 1*

Which two actions are recommended as security best practices to protect REST API? (Choose two.)

A. Enable dual authentication of the session

B. Use a password hash

C. Use SSL for encryption

D. Use TACACS+ authentication

E. Enable out-of-band authentication

Correct Answer: *AC*

Community vote distribution

BC (100%)

kaupz Highly Voted 2 months, 3 weeks ago

Selected Answer: BC

B and C
2.2. Always Use HTTPS - a.k.a SSL
2.3. Use Password Hash
https://restfulapi.net/security-essentials/

upvoted 6 times

TheGorn 1 month ago

Agreed. And considering the overwhelming majority of API calls in automation are "machine to machine", how exactly would the 2FA even work...

upvoted 1 times

peugeotdude Most Recent 1 month, 3 weeks ago

Not sure what "Dual Authentication" means?

upvoted 1 times

b7c04a1 1 month, 2 weeks ago

i think is two-factor authentication

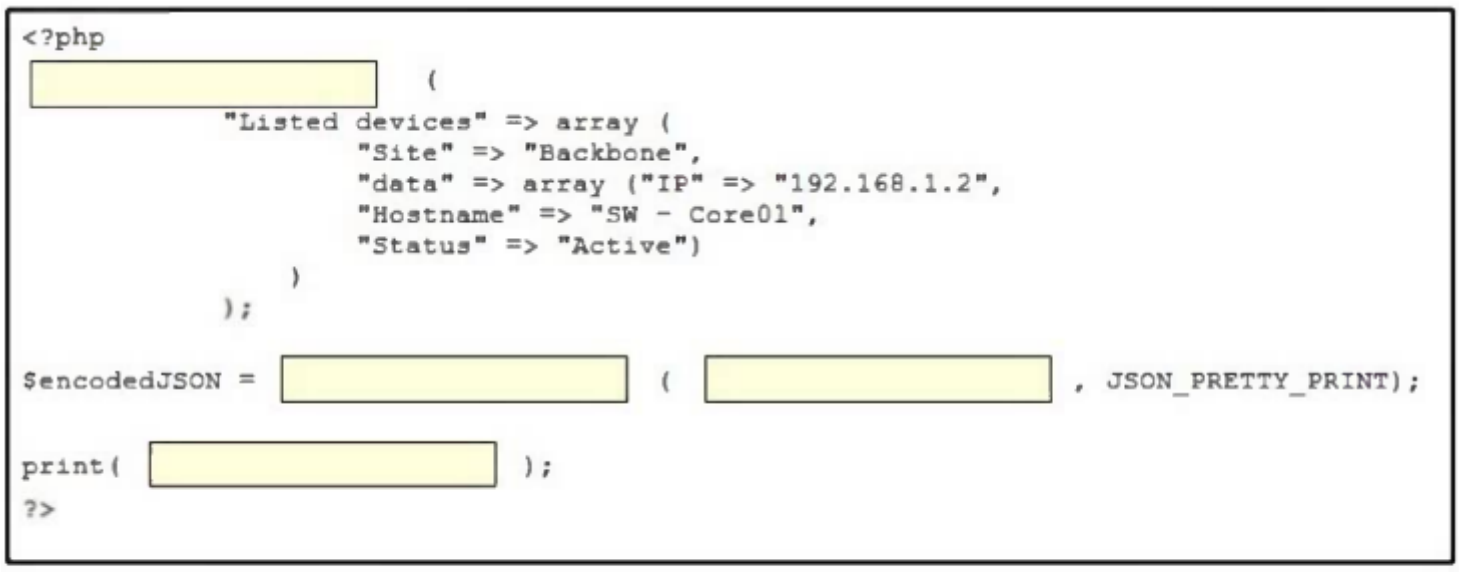
upvoted 2 times

Question #848 *Topic 1*

DRAG DROP

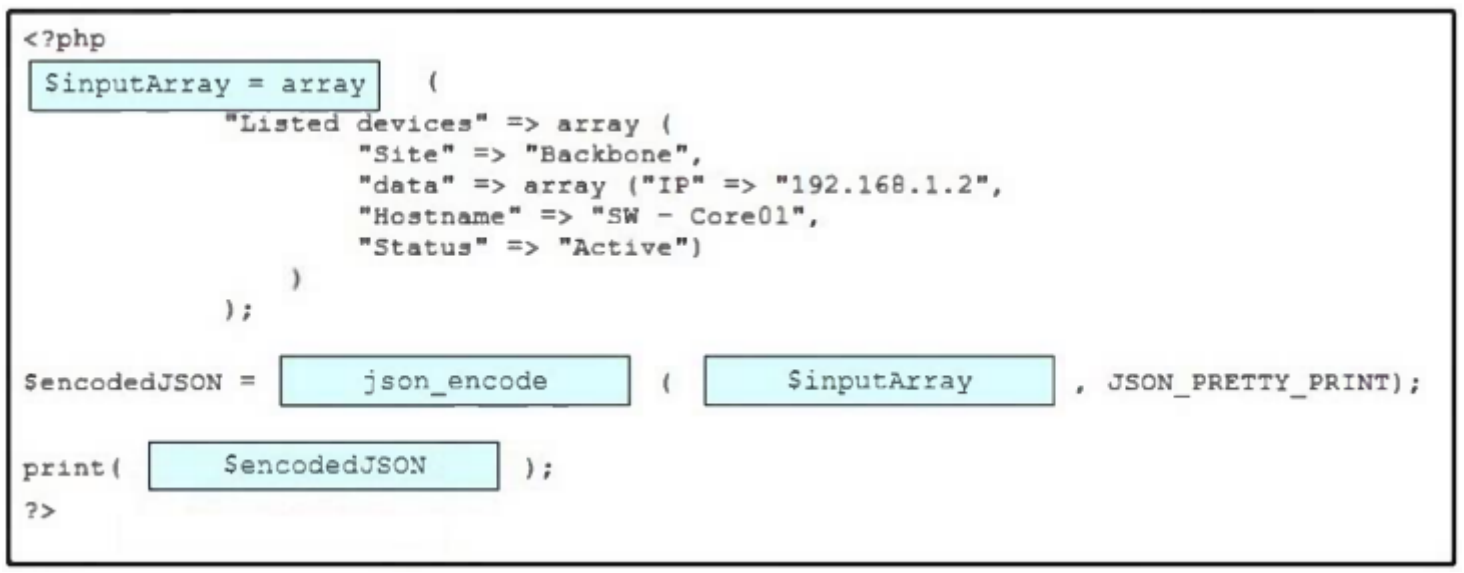
-

Drag and drop the code snippets from the bottom onto the blanks in the PHP script to convert a PHP array into JSON format. Not all options are used.



$encodedJSON | $inputArray = array | json_decode | $inputArray | json_encode

Correct Answer:



shefo1 1 month, 3 weeks ago

correct answer from google bard

```
<?php

$inputArray = array(
"Listed devices" => array(
"Site" => "Backbone",
"data" => array(
"IP" => "192.168.1.2",
"Hostname" => "SW Core01",
"Status" => "Active"
)
)
);

$encodedJSON = json_encode($inputArray, JSON_PRETTY_PRINT);

print($encodedJSON);

?>
```

upvoted 2 times

studying_1 2 months, 1 week ago

Answer is correct.
// first configure array
$InputArray = array(.....);
// json_encode function... the format is json_encode(name of the array)
$encodedJSON = json_encode($InputArray, JSON_PRETTY_PRINT);

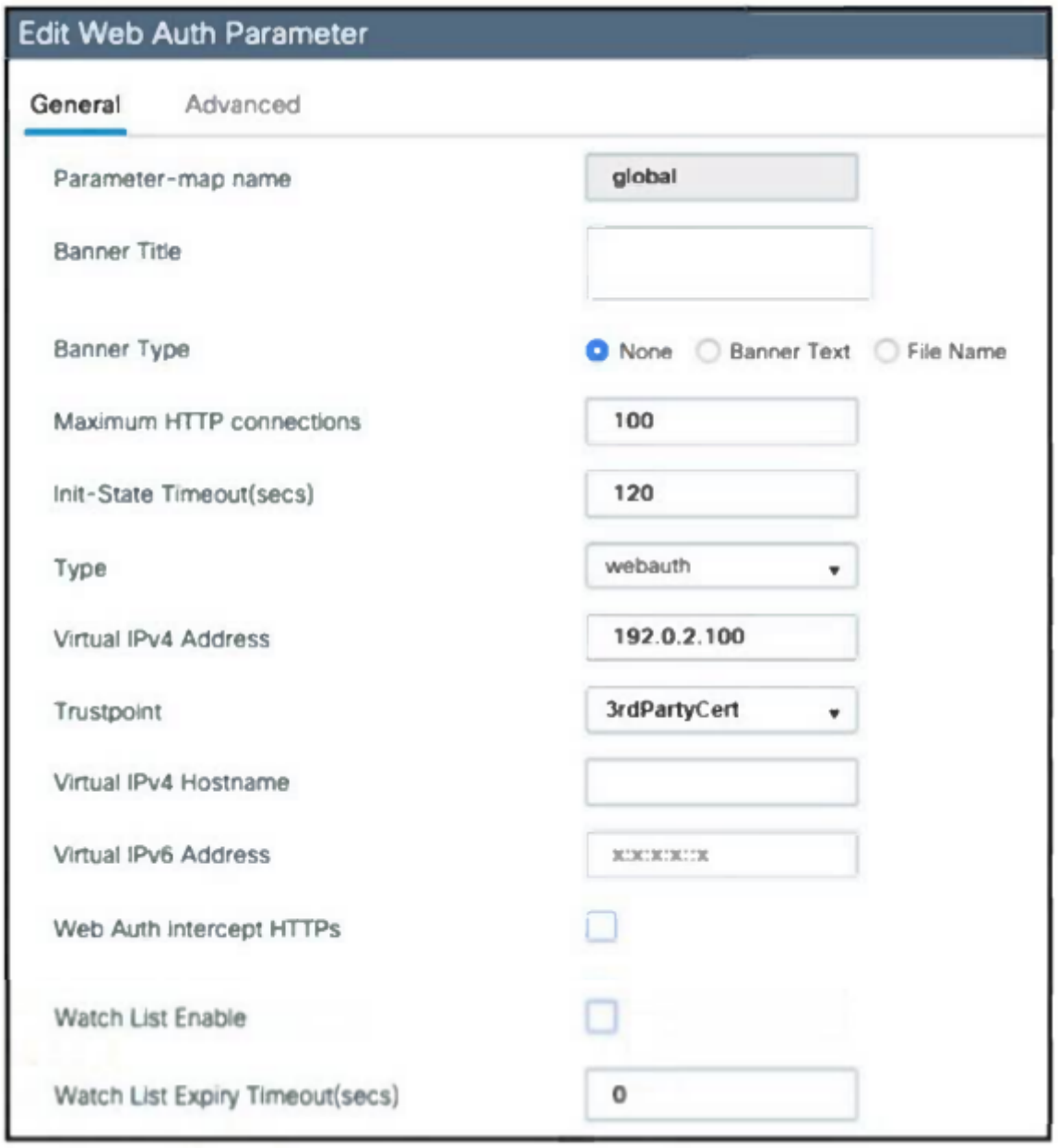
//Finally print
Print ($encodedJSON)
upvoted 2 times

mmt1mmt1 2 months, 1 week ago
Could someone confirm if this is correct?
upvoted 1 times

studying_1 2 months, 1 week ago
Yes, answer is correct
upvoted 2 times

Alondrix 2 months, 3 weeks ago
My networking skills are incredibly enhanced with the research required to answer this question!
upvoted 3 times

Question #849 *Topic 1*



Refer to the exhibit. An engineer is configuring WebAuth on a Cisco Catalyst 9800 Series WLC. The engineer has purchased a third-party certificate using the FQDN of the WLC as the CN and intends to use it on the WebAuth splash page. What must be configured so that the clients do not receive a certificate error?

A. Virtual IPv4 Hostname must match the CN of the certificate

B. Virtual IPv4 Address must be set to a routable address

C. Web Auth Intercept HTTPs must be enabled

D. Trustpoint must be set to the management certificate of the WLC

Correct Answer: *A*

kaupz 2 months, 3 weeks ago

if FQDN and SSL CN and/or SAN mismatch, then you'll receive certificate warning in browser.

upvoted 2 times

kaupz 2 months, 3 weeks ago

A should be correct

upvoted 3 times

```
hostname router
ip domain-name cisco.com

line vty 0 15
session-timeout 30
exec-timeout 120 0
login local
```

Refer to the exhibit. Which configuration must be added to enable remote access only using SSHv1 or SSHv2 to this router?

A.
```
R1(config)# ip ssh version 2
R1(config)# line vty 0 15
R1(config-line)# transport input ssh
R1(config-line)# transport output ssh
```

B.
```
R1(config)# crypto key generate rsa modulus 2048
R1(config)# line vty 0 15
R1(config-line)# transport input ssh
```

C.
```
R1(config)# line vty 0 15
R1(config-line)# transport input ssh
R1(config-line)# transport output ssh
```

D.
```
R1(config)# crypto key generate rsa modulus 2048
R1(config)# ip ssh version 2
R1(config)# line vty 0 15
R1(config-line)# transport input all
```

Correct Answer: *C*

Community vote distribution

B (100%)

Just_little_me Highly Voted 2 months, 1 week ago

Selected Answer: B

for vty only input is needed. and you need a crypto key for ssh

upvoted 6 times

teems5uk Most Recent 2 days ago

B.
RSA key must be generated

upvoted 1 times

Jakubu1 1 month, 1 week ago

Please indicate why the answer is C with evidence, team. It would be helpful. I as well see the answer as B, but am willing to be educated on why I am wrong.

upvoted 1 times

Fanny1493 2 months ago

Selected Answer: B

correct B

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: B

only input ssh is needed

upvoted 3 times

```
args_dict = {'1st_item':'645298791871446',
             '2nd_item_that_must_display':'jlugyydt'}

for key,value in args_dict.items():
    txt='{:#<15} : {:#<10}'.format(key,str(value))
    print(txt)
```

Refer to the exhibit. What is the output of this code?

A. 1st_item#######: 645298791871446
2nd_item_that_must_display: jlugyydt##

B. 1st_item#######: 6452987918
2nd_item_that_m: jlugyydt##

C. 1st_item#######: 8791871446
at_must_display: jlugyydt

D. 645298791871446
##jlugyydt

Correct Answer: *B*

Community vote distribution

A (100%)

Jakubu1 1 month, 1 week ago

Did anyone take the exam and have this question? What was the answer? While Python's books may have one answer, Cisco's exam's decision for the correct answer is what decides the correct answer for Cisco unfortunately, so would love to now.

upvoted 1 times

reheheeeehe 1 month, 2 weeks ago

Selected Answer: A

https://www.online-python.com/

```
args_dict = {
'1st_item':'645298791871446',
'2nd_item_that_must_display':'jlugyydt'
}

for key,value in args_dict.items():
txt = '{:#<15} : {:#<10}'.format(key,str(value))
print(txt)
```

Output:

```
1st_item####### : 645298791871446
2nd_item_that_must_display : jlugyydt##
```

upvoted 1 times

Alondrix 2 months, 3 weeks ago

Answer is A.
{:#<15} - This is adding # to the returned string to fill 15 characters. It does nothing if the string is greater than 15 characters.
{:#<10} - This is adding # to the returned string to fill 10 characters. It does nothing if the string is greater than 10 characters.

upvoted 4 times

Will_91 2 months, 3 weeks ago

Selected Answer: A

Tested its A

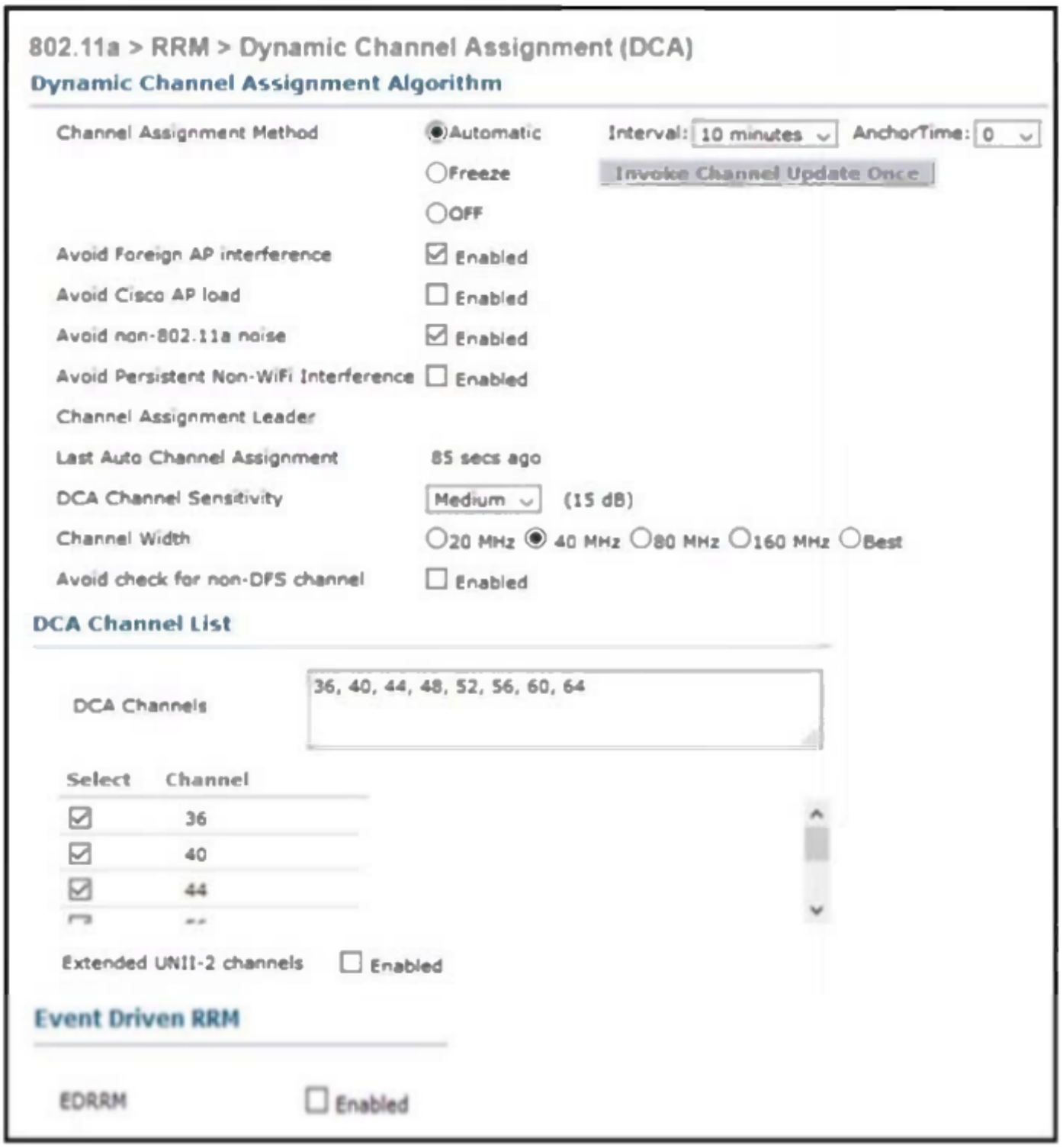
upvoted 1 times

BoyuanLIU 2 months, 3 weeks ago

Selected Answer: A

in "B" - The value '6452987918' is truncated to 10 characters, which does not happen in Python's string formatting; the entire string should be displayed even if it exceeds the specified width.

upvoted 1 times



Refer to the exhibit. An engineer is troubleshooting an issue with non-Wi-Fi interference on the 5-GHz band. The engineer has enabled Cisco CleanAir and set the appropriate traps, but the AP does not change the channel when it detects significant interference. Which action will resolve the issue?

A. Enable the Avoid Persistent Non-WiFi interference option

B. Change the DCA Sensitivity option to High

C. Enable the Event Driven Radio Resource Management option

D. Disable the Avoid Foreign AP Interference option

Correct Answer: *C*

Community vote distribution

C (71%) B (29%)

teems5uk 2 days ago

Selected Answer: C

Given answer is correct.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg/cisco-cleanair.html#:~:text=the%20connected%20devices.-,EDRRM%20and%20AQR%20Update%20Mode,by%20default%2C%20you%20must%20first%20enable%20CleanAir%20and%20then%20enable%20EDRRM.,-Prerequisites%20for%20CleanAir

upvoted 1 times

Tadese 1 month ago

Selected Answer: C

Answer C

upvoted 1 times

Fanny1493 2 months ago

Selected Answer: C

Answer C

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg/cisco-cleanair.html

upvoted 2 times

studying_1 2 months, 1 week ago

Selected Answer: C

I guess the answer is correct
Event Driven RRM (ED-RRM) is a feature that allows an AP in distress to bypass normal RRM intervals and immediately change channels.

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: B

DCA sensitivity to high

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/dca.html

upvoted 2 times

Alondrix 2 months, 3 weeks ago

Your link to the White Paper indicates the channel can be changed with DCA to to high, medium, or low.
I think the correct answer is as stated, RRM per the same link.
ED-RRM is not directly related to RRM, but will cause channel changes if invoked.

upvoted 1 times

```
pl1= [
"""
<get-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <source>
  <running/>
 </source>
 <filter>
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
   <ip>
    <access-list>
     <extended xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-acl">
      <name>flp</name>
     </extended>
    </access-list>
   </ip>
  </native>
 </filter>
</get-config>
"""
]
with manager.connect(host=10.1.1.1, port=830, username=cisco, password=cisco, timeout=90, hostkey_verify=False) as m:
  for rpc in pl1:
    r1= m.dispatch(et.fromstring(rpc))
    d1= xmltodict.parse(r1.xml)['rpc-reply']['data']['native']['ip']['access-list']['extended']['access-list-seq-rule']
```

Refer to the exhibit. What is achieved by the XML code?

A. It displays the access list sequence numbers from the output of the show ip access-list extended flp command on the terminal screen

B. It displays the output of the show ip access-list extended flp command on the terminal screen

C. It reads the access list sequence numbers from the output of the show ip access-list extended flp command into a dictionary list

D. It reads the output of the show ip access-list extended flp command into a dictionary list

Correct Answer: *D*

Community vote distribution

A (100%)

yanickjames320 1 week, 2 days ago

Selected Answer: A

WhatsApp +1(409)223 7790 PASS CISCO EXAMS(CCNA,CCNP)pay us after confirmation of passed results

1. COMPTIA (network+ security+)

2: GMAT,GRE exams

3: IAPP Certifications
(CIPP/E CIPM, CIPT)

4: ISACA certifications (CISA,CISM/ CRISC)

5: GIAC CERTIFICATION

6: PMI (PMP/CAPM/ACP/PBA ,RMP)

7: IMA (CMA certification)

8: CIA,IFRS, CERTIFICATIONS

9: ACCA,CFA,ICAEW certifications

10:CWNA certification

12. APICS CERTIFICATIONS, CSCP, CPIM, CLTD

Book for online proctor exam and we'll remotely take the exam for you. Pay us after confirmation of PASSED results

https://ittca.org/

WhatsApp +1(409)223 7790

upvoted 1 times

kldoyle97 1 week, 2 days ago

A and B cannot be correct because the python code is not using the print function/ display information.
based on the code, I believe the answer is C because the last line is reference Sequence numbers ["access-list-seq-rule"]

upvoted 2 times

Question #854 *Topic 1*

An engineer measures the Wi-Fi coverage at a customer site The RSSI values are recorded as follows:

• Location A: -72 dBm
• Location B: -75 dBm
• Location C -65 dBm
• Location D -80 dBm

Which two statements does the engineer use to explain these values to the customer? (Choose two.)

A. The signal strength at location C is too weak to support web surfing

B. Location D has the strongest RF signal strength

C. The RF signal strength at location B is 50% weaker than location A

D. The RF signal strength at location C is 10 times stronger than location B

E. The signal strength at location B is 10 dB better than location C

Correct Answer: *CD*

Community vote distribution

CD (86%) 14%

Horsefeathers 4 weeks ago

Selected Answer: CD

The following matches options C & D perfectly:
"For every 3 dB decrease, the power is cut in half. Similarly, every 10 dB increase in level is 10 times the power, and every 10 dB decrease in level results in 1/10 the power. This is sometimes referred to as the “rule of 3s and 10s.”"

https://www.sciencedirect.com/topics/computer-science/signal-strength

upvoted 2 times

kaupz 1 month, 1 week ago

Selected Answer: CD

C and D(is the closest correct)
Because rule of 10 and 3s

upvoted 3 times

kaupz 1 month, 1 week ago

A)-65dBm is enough for web browsing) - wrong https://community.cisco.com/t5/wireless-mobility-knowledge-base/snr-rssi-eirp-and-free-space-path-loss/ta-p/3128478#:~:text=The%20closer%20this%20value%20to,on%20power%20levels%20and%20design.
"Typically voice networks require a -65dBm or better signal level while a data network needs -80dBm or better. Normal range in a network would be -45dBm to -87dBm depending on power levels and design"
B) the closer the value to + side, the better the signal - wrong

upvoted 1 times

kaupz 1 month, 1 week ago

C) -75dBm is 3dBm weaker than -72dBm, so this divides the coverage with 2 (50% less)
D) imagine 2squaremeters equals -80dBm, then if each time the RSSI gets better 3dBm then the the x squaremeters get multiplied with 2.
-80dBm = 2sqm
-77dBm = 4sqm
-74dBm = 8sqm
-71dBm = 16sqm
-68dBm = 32sqm
-65dBm = 64sqm
this means not only it is just 10 times stronger, but 32 times.
D) Yet again, the closer the value to + side, the better the signal, not the other way around - wrong

upvoted 1 times

kaupz 1 month, 1 week ago

oops - E) Yet again, the closer the value to + side, the better the signal, not the other way around - wrong

upvoted 1 times

Fanny1493 2 months ago

Selected Answer: CD

Correct answer C
for descarting wrong A,B,E, ... then other correct answer D

upvoted 1 times

JackDRipper 2 months, 2 weeks ago

Selected Answer: AC

C is 100% correct
A is subjective, but the all other choices are wrong, so A and C it is.

upvoted 1 times

adamzet33 2 months, 1 week ago

-65 should be enough for web browsing..

upvoted 1 times

Question #855 *Topic 1*

DRAG DROP
-

Drag and drop the code snippets from the bottom onto the blanks in the script to convert a Python object into a compact JSON object by removing space characters. Not all options are used.

```
import json

data = {
  "measurement": "cpmCPUTotal1minRev",
  "collectionInterval": "default",
  "tagCount": "0",
  "policy": None,
  "devices": [{"model": "Cisco 3500 Series WLC", "ipv4": "10.10.20.52"}]
}

obj = json.[          ]([          ],[          ])

print(obj)
```

`separators=(',', ':')` `"loads"` `data` `"dumps"`

Correct Answer:

```
obj = json.["loads"](data,separators=(',', ':'))

print(obj)
```

studying_1 Highly Voted 2 months, 1 week ago

I guess answer should be "dumps", data. separators
If you have a Python object, you can convert it into a JSON string by using the json.dumps() method.

upvoted 12 times

scarface35 Most Recent 4 weeks ago

given answer is wrong

import json
data = {
"measurement":"cpmCPUTotal1minRev",
"collectionInterval":"default",
"tagCount":"0",
"policy":None,
"devices": [{"model":"cisco 3500 Series WLC","ipv4":"10.10.10.45"}]
}

obj=json.dumps(data,separators=(',', ':'))

print(obj)

upvoted 2 times

Alondrix 2 months, 3 weeks ago

Given answer appears correct.

upvoted 1 times

Question #856 *Topic 1*

Where are operations related to software images located in the Cisco DNA Center GUI?

A. Services

B. Provisioning

C. Assurance

D. Design

Correct Answer: *B*

Community vote distribution

D (100%)

eearmani 1 month ago

In the Cisco DNA Center GUI, click the Menu icon () and choose Design > Image Repository.

upvoted 1 times

NikosTsironis 1 month ago

Selected Answer: D

D is the answer

upvoted 2 times

shefo1 2 months ago

Selected Answer: D

of course D is right , pls fix
from OCG , p.628

The following are some of the Cisco DNA [design] tools:
■ Network Hierarchy:
■ Network Settings:
■ Image Repository:
■ Network Profiles:

upvoted 3 times

Just_little_me 2 months, 1 week ago

Selected Answer: D

in Design you can choose the software images for your device. after that you go to Provision

In the Cisco DNA Center GUI, click the Menu icon () and choose Provision > Network Devices > Inventory.

Step 2

From the Focus drop-down list, choose Software Images. Select the device whose image you want to upgrade.

upvoted 1 times

kaupz 2 months, 3 weeks ago

Selected Answer: D

In the Cisco DNA Center GUI, click the Menu icon () and choose Design > Image Repository.
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0100.html

Correct is D

upvoted 2 times

Question #857 *Topic 1*

What is a difference between OSPF and EIGRP?

A. OSPF uses a default hello timer of 5 seconds. EIGRP uses a default hello timer of 10 seconds.

B. OSPF uses multicast addresses 224.0.0.5 and 224.0.0.6. EIGRP uses multicast address 224.0.0.10.

C. OSPF uses an administrative distance of 115. EIGRP uses an administrative distance of 160.

D. OSPF uses IP protocol number 88. EIGRP uses IP protocol number 89.

Correct Answer: *B*

Community vote distribution

B (100%)

kaupz 2 months, 3 weeks ago

Selected Answer: B

correct

upvoted 2 times

Question #858 *Topic 1*

Which type of antenna is designed to provide a 360-degree radiation pattern?

A. Yagi

B. patch

C. directional

D. omnidirectional

Correct Answer: *D*

Community vote distribution

D (100%)

Alondrix 2 months, 3 weeks ago

Selected Answer: D

D: Correct

upvoted 2 times

Evreni 2 months, 3 weeks ago

Selected Answer: D

D: is correct

upvoted 2 times

Question #859 *Topic 1*

Which two security mechanisms are used by Cisco Threat Defense to gain visibility into the most dangerous cyber threats? (Choose two.)

A. virtual private networks

B. file reputation

C. VLAN segmentation

D. Traffic Telemetry

E. dynamic enforce policy

Correct Answer: *BD*

Community vote distribution

BD (100%)

Horsefeathers 4 weeks ago

Selected Answer: BD

Question 770 answers this:
Which technology uses network traffic telemetry, contextual information, and file reputation to provide insight into cyber threats?
D. threat defense

upvoted 2 times

Question #860 *Topic 1*

Which action is a LISP ITR responsible for?

A. responding to map-request messages

B. forwarding user data traffic

C. finding EID-to-RLOC mappings

D. accepting registration requests from ETRs

Correct Answer: *C*

Community vote distribution

C (100%)

Storcaks 1 month, 2 weeks ago

Selected Answer: C

Given answer is correct.

LISP Ingress Tunnel Router (ITR)
An ITR is responsible for finding EID-to-RLOC mappings for all traffic destined for LISP-capable sites. When the ITR receives a packet destined for an EID, it first looks for the EID in its mapping cache. If the ITR finds a match, it encapsulates the packet inside a LISP header with one of its RLOCs as the IP source address

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/15-mt/irl-15-mt-book/irl-overview.pdf

upvoted 3 times

Question #861 *Topic 1*

An engineer modifies the existing ISE guest portal URL to use a static FQDN. Users immediately report that they receive certificate errors when they are redirected to the new page. Which two additional configuration steps are needed to implement the change? (Choose two.)

A. Add a new DNS record to resolve the FQDN to the PSN IP address

B. Create and sign a new CSR that contains the static FQDN entry

C. Manually configure the hosts file on each user device.

D. Disable HTTPS on the WLC under the Management menu

E. Add the FQDN entry under the WLC virtual interface

Correct Answer: *AB*

Community vote distribution

AE (60%) AB (40%)

teems5uk 1 day, 23 hours ago

Selected Answer: AB

Given answer is correct.

upvoted 1 times

shefo1 3 weeks ago

Selected Answer: AB

the below AI chatbots say that option A and B is right
- chatGPT , google BARD (google) , capilot (windows) , Aria (opera mini) , LEO (brave browser)

upvoted 1 times

nerostart 3 weeks, 5 days ago

Selected Answer: AE

I think correct answers should be A&E

upvoted 1 times

Tadese 1 month ago

Selected Answer: AE

AE think corect

upvoted 1 times

Toob93 1 month ago

Selected Answer: AE

I think correct answers should be A&E

upvoted 1 times

Question #862 *Topic 1*

Which JSON script is properly formatted?

A.
```
{
 "car": [
  {
   "type":"Ford",
   "color":"red",
   "year":"1998"
  }
 ]
}
```

B.
```
[
    "book":{
        "title":"Engineering",
        "grade":"11",
        "edition":"4".
            }
]
```

C.
```
"truck":[
        {
            "type":"Dodge",
            "color":"blue",
            "year":"2015"
        }
    ]
```

D.
```
{   "device":
    {[
        "type":"switch,
        "model":"Catalyst",
        "mac":"00:46:10:04:93:6c",
      ]
    }
}
```

Correct Answer: *C*

Community vote distribution

A (100%)

Exam12559 Highly Voted 2 months, 1 week ago

Selected Answer: A

A is correct as JSON syntax.

In C, [and { are reversed.

upvoted 9 times

Wazerface 1 month, 4 weeks ago

true that

upvoted 2 times

peugeotdude Most Recent 1 week, 4 days ago

Selected Answer: A

A looks to be correct

upvoted 1 times

Din04 3 weeks, 6 days ago

Selected Answer: A

Correct syntax is A

upvoted 1 times

Tadese 1 month ago

Selected Answer: A

A is correct answer

upvoted 1 times

janbaz 1 month ago

Selected Answer: A

Correct JSON syntax

upvoted 1 times

NikosTsironis 1 month ago

Selected Answer: A

A is the only correct answer

upvoted 2 times

Question #863 *Topic 1*

What is contained in the VXLAN header?

A. VXLAN network identifier

B. source and destination RLOC ID

C. endpoint ID

D. original Layer 2 VLAN ID

Correct Answer: *D*

Community vote distribution

A (100%)

teems5uk 1 day, 23 hours ago

Selected Answer: A

VXLAN network identifier (VNI) A 24-bit field in the VXLAN header that enables up to
16 million Layer 2 and/or Layer 3 VXLAN segments to coexist within the same infrastructure.

upvoted 1 times

maddyr 1 month, 2 weeks ago

Selected Answer: A

Should be VNI

upvoted 2 times

Din04 1 month, 3 weeks ago

Selected Answer: A

Answer A, please fix answers

upvoted 2 times

Jacobjob 1 month, 3 weeks ago

Correct answer is A

upvoted 2 times

Fanny1493 2 months ago

Selected Answer: A

Correct answer is A
VNI

upvoted 3 times

JackDRipper 2 months ago

Selected Answer: A

A is correct

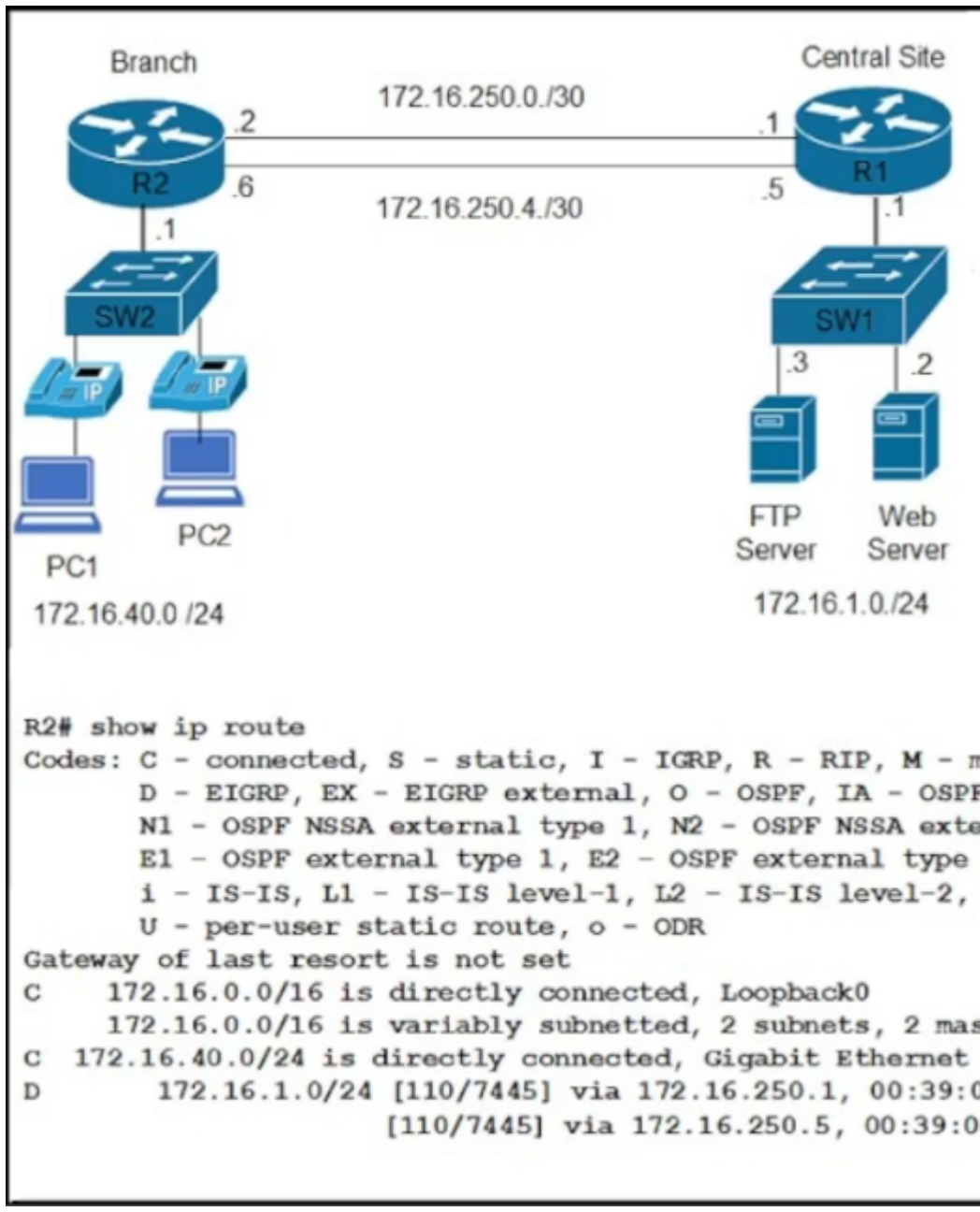
upvoted 2 times

Exam12559 2 months, 1 week ago

Selected Answer: A

VXLAN is typically used to extend L2 networks, but the original Layer 2 VLAN ID itself is not included in the VXLAN header.

upvoted 2 times




```
R2#traceroute 172.16.1.2

Type escape sequence to abort.

Tracing the route to 172.16.1.2

  1 172.16.250.1 2 msec

    172.16.250.5 5 msec

    172.16.250.1 2 msec

  2 172.16.250.1 2 msec

    172.16.250.5 5 msec

    172.16.250.1 2 msec
  3 172.16.1.2 6 msec 5 msec 5 msec
```

```
R2# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C    172.16.0.0/16 is directly connected, Loopback0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C  172.16.40.0/24 is directly connected, Gigabit Ethernet 0/1
D       172.16.1.0/24 [110/7445] via 172.16.250.1, 00:39:08, Gigabit Ethernet 0/0
                      [110/7445] via 172.16.250.5, 00:39:08, Gigabit Ethernet 0/4
```

Refer to the exhibit. Clients are reporting an issue with the voice traffic from the branch site to the central site. What is the cause of this issue?

A. There is a routing loop on the network

B. There is a high delay on the WAN links

C. Traffic is load-balancing over both links, causing packets to arrive out of order

D. The voice traffic is using the link with less available bandwidth

Correct Answer: *C*

Community vote distribution

C (63%) A (38%)

boyseven777 2 days, 4 hours ago

Selected Answer: C

no routing loop is identified in the traceroute

upvoted 1 times

adamzet33 3 weeks, 6 days ago

Selected Answer: C

Packets are reaching the destination.

upvoted 1 times

Horsefeathers 4 weeks ago

Selected Answer: C

With routing loop I would expect no traffic to reach the destination. Traceroute shows several repeated hops but the destination is eventually reached.
It also shows a delay of several ms which can be detrimental to voice traffic not so much to the other traffic.
Clients are complaining about voice traffic only, therefore I go with C.

upvoted 2 times

b7c04a1 1 month, 1 week ago

Selected Answer: C

The provider's answer seens correct. if you observe the routing table, R2 has two EIGRP routes to 172.16.1.0 and the packet came to Web Server. Another point, the question says that have problem only in traffic voice.
I'm going with C too.

upvoted 1 times

Exam12559 2 months, 1 week ago

Selected Answer: A

Looking at the Traceroute results, I see the same IP address repeated on each hop. This may be caused by repeated hops to the same IP address, causing packets to become stuck in a loop.

upvoted 3 times

TheGorn 1 month, 1 week ago

Typically though on a routing loop it continues on forever and it goes straight back and forth.
There are also duplicate replies and it did eventually reach it. IDK. Flip a coin I guess.

upvoted 2 times

Question #865 *Topic 1*

Which virtualization component creates VMs and performs hardware abstraction that allows multiple VMs to run at the same time?

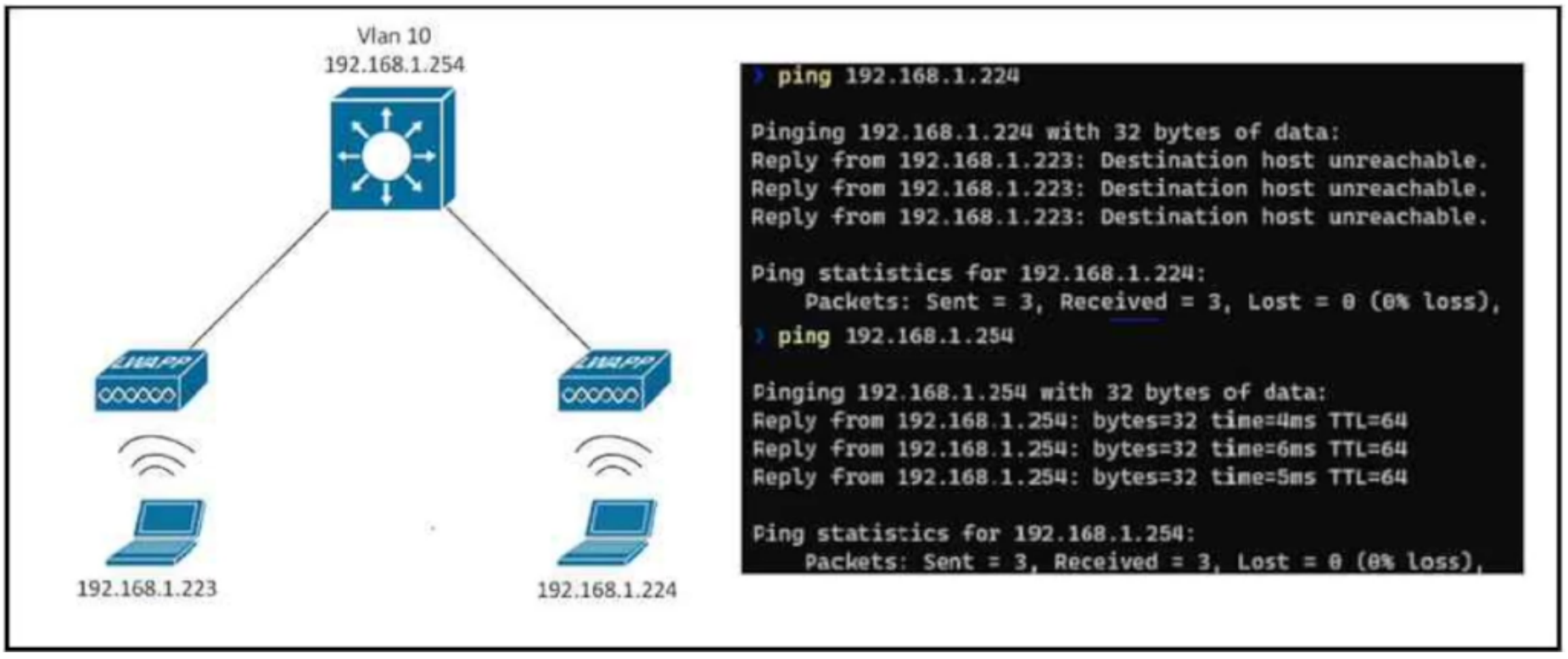
A. container

B. Docker

C. hypervisor

D. rkt

Correct Answer: *C*



Refer to the exhibit. An SSID is configured and both clients can reach their gateways on the Layer 3 switch, but they cannot communicate with each other. Which action resolves this issue?

A. Set the WMM Policy to Allowed

B. Set the P2P Blocking Action to Disabled

C. Set the WMM Policy to Required

D. Set the P2P Blocking Action to Forward-UpStream

Correct Answer: *B*

Community vote distribution

B (100%)

shefo1 1 month ago

Selected Answer: B

P2P Blocking is a security feature on some wireless controllers that can be used to prevent peer-to-peer communication between wireless clients. This feature is typically used to prevent unauthorized file sharing or other unwanted network traffic. In this case, it is likely that P2P Blocking is enabled and is preventing the two clients from communicating with each other.

Disabling P2P Blocking will allow the clients to communicate with each other on the Layer 2 network. This will allow them to ping each other and access any shared resources that are available on the network.

upvoted 2 times

NikosTsironis 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

Question #867 *Topic 1*

What is a characteristic of VXLAN?

A. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay

B. It has a 12-byte packet header

C. It uses TCP for transport,

D. It is a multi-tenant solution.

Correct Answer: *D*

Community vote distribution

sledgey121 3 weeks, 5 days ago

Selected Answer: D

It can't be A as it uses a L3 underlay, not a L2 underlay.

upvoted 1 times

Horsefeathers 4 weeks ago

Selected Answer: D

VXLAN offers the following benefits:
VLAN flexibility in multitenant segments - D
Higher scalability
Improved network utilization

https://www.ciscopress.com/articles/article.asp?p=2999385&seqNum=3

upvoted 1 times

benvz 1 month ago

Selected Answer: A

A. **It extends Layer 2 and Layer 3 overlay networks over a Layer 3 underlay.**

VXLAN is a network virtualization technology that enables the creation of Layer 2 and Layer 3 overlay networks on top of a Layer 3 (IP) underlay network. VXLAN is often used in virtualized and cloud environments to provide network segmentation and isolation. It allows for the extension of Layer 2 domains across Layer 3 networks.

The other options are not accurate:

B. VXLAN typically has a 50-byte packet header.

C. VXLAN uses UDP (User Datagram Protocol) for transport, not TCP.

D. VXLAN is often used in multi-tenant environments, but the term "multi-tenant solution" is a bit broad. VXLAN itself is a technology that facilitates network virtualization and segmentation, which can be used in multi-tenant scenarios.

upvoted 1 times

b7c04a1 1 month, 2 weeks ago

Shouldnt be A?

upvoted 1 times

TheGorn 1 month, 1 week ago

It extends L2 over L3.

upvoted 2 times

Question #868 *Topic 1*

Which network devices secure API platforms?

A. content switches

B. web application firewalls

C. next-generation intrusion detection systems

D. Layer 3 transit network devices

Correct Answer: *B*

kldoyle97 1 day, 17 hours ago

Provided answer is correct

upvoted 1 times

Question #869 *Topic 1*

What does Call Admission Control require the client to send in order to reserve the bandwidth?

A. SIP flow information

B. Wi-Fi multimedia

C. VoIP media session awareness

D. traffic specification

Correct Answer: *D*

Community vote distribution

D (100%)

Annielover007 4 weeks ago

Selected Answer: D

If your phone supports CAC (this is the case with a 7925), before any call (as you punch the numbers and press the green button), the phone is going to send to the AP and Add Traffic Tream (ADDTS) request. The request contains a Traffic Classification (TCLAS) field, that basically says that this is voice 2 ways. It also contains a field called traffic specification (TSPEC) that provides all the details you need for the call: average size of packets, volume of traffic on the way up (per second), on the way down, minimum data rate needed, etc. This is what allows the AP to determine if this call can be adminteed

upvoted 3 times

Question #870 *Topic 1*

Which capability does a distributed virtual switch have?

A. use floating static routes

B. provide configuration consistency across the hosts

C. run dynamic routing protocols

D. use advanced IPsec encryption algorithms

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #871 *Topic 1*

Which two methods are used to assign security group tags to the user in a Cisco TrustSec. architecture? (Choose two.)

A. web authentication

B. IEEE 802.1x

C. DHCP

D. modular QoS

E. policy routing

Correct Answer: *BC*

Community vote distribution

AB (100%)

Exam12559 Highly Voted 2 months, 1 week ago

Selected Answer: AB

A. Web authentication
Used when a user logs in using a web browser. When a user accesses the network using this method, web authentication authenticates the user and assigns a security group tag.
This is an effective authentication method when the client terminal does not have an 802.1X supplicant function.

B. IEEE 802.1x
A network access control protocol that provides authentication and authorization. It consists of three elements: an authentication server, an authenticator, and a supplicant. When a user connects to a network, they are authenticated using 802.1x and are granted permission to access the network. Through this authentication process, users are assigned the appropriate security group tag.

upvoted 5 times

teems5uk Most Recent 1 day, 22 hours ago

Selected Answer: AB

TrustSec uses SGT tags to perform ingress tagging and egress filtering to enforce access control policy. Cisco ISE assigns the SGT tags to users or devices that are successfully authenticated and authorized through 802.1x, MAB, or WebAuth. The SGT tag assignment is delivered to the authenticator as an authorization option (in the same way as a dACL). After the SGT tag is assigned, an access enforcement policy (allow or drop) based on the SGT tag can be applied at any egress point of the TrustSec network.

upvoted 1 times

NikosTsironis 1 month ago

Selected Answer: AB

AB is the correct, the rest make no sense for authentication

upvoted 3 times

shefo1 2 months ago

Selected Answer: AB

Admin please fix
from OCG p.735

Cisco ISE assigns the SGT tags to users or devices that are successfully authenticated and authorized through 802.1x, MAB, or WebAuth.

upvoted 3 times

Question #872 *Topic 1*

Which resource must the hypervisor make available to the virtual machines?

A. bandwidth

B. IP address

C. processor

D. secure access

Correct Answer: *C*

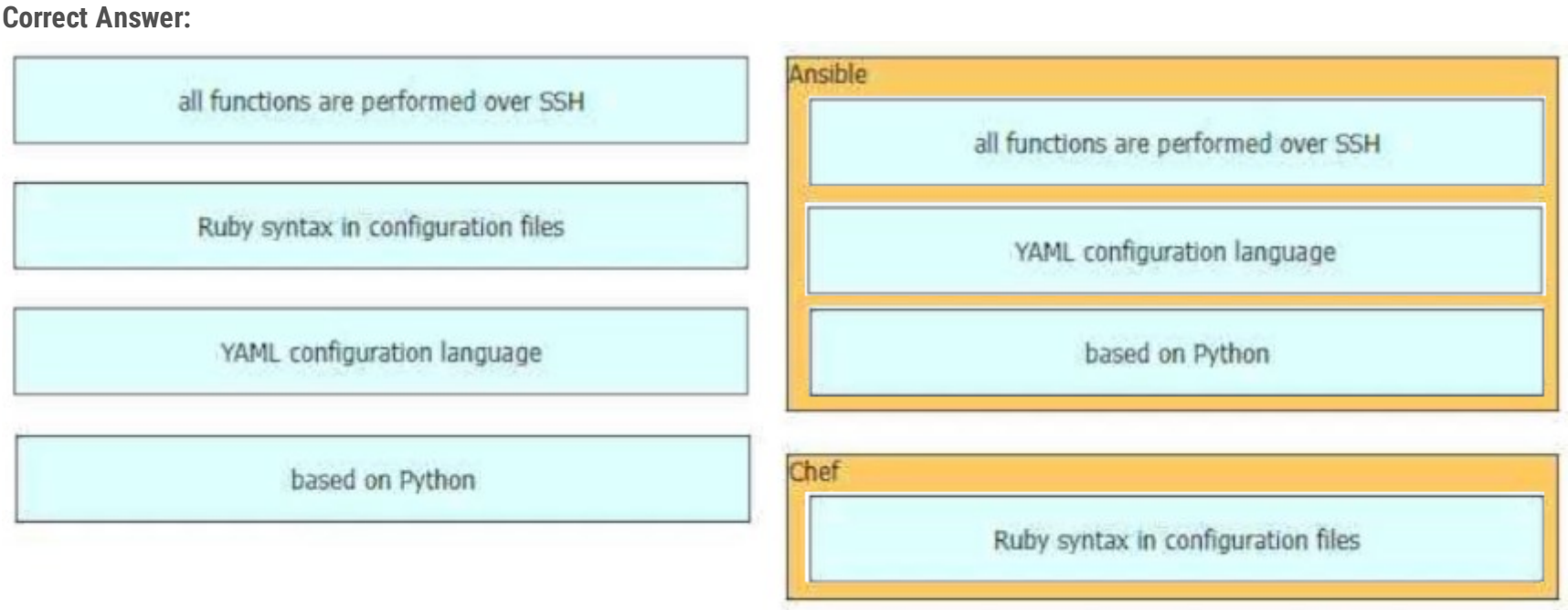
Question #873 *Topic 1*

DRAG DROP

-

Drag and drop the automation characteristics from the left onto the corresponding tools on the right.

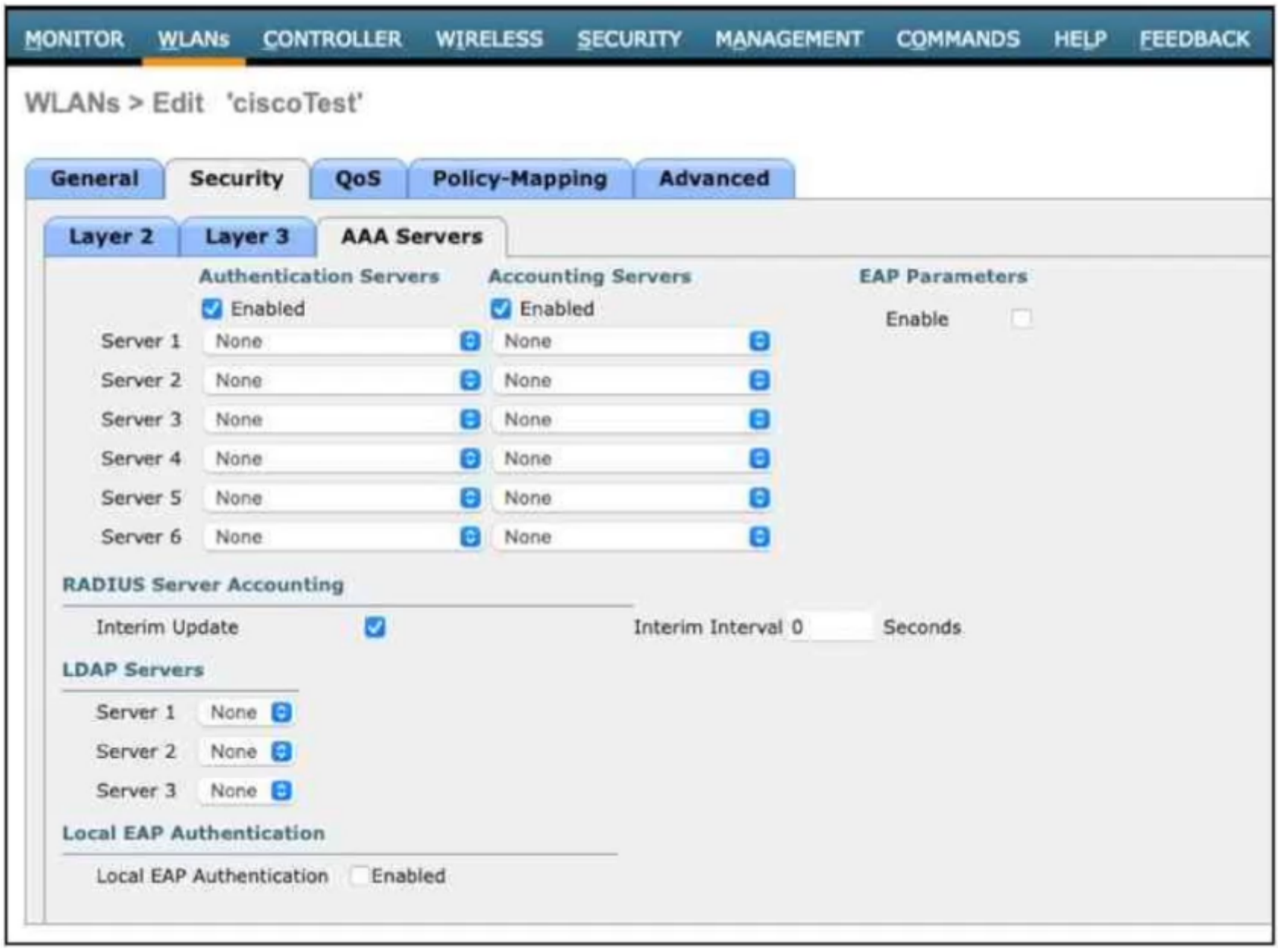
Correct Answer:



Calinserban 2 months, 1 week ago

Chef is based on Ruby

upvoted 3 times



Refer to the exhibit. An engineer must configure a Cisco WLC with WPA2 Enterprise mode and avoid global server lists. Which action is required?

A. Enable EAP parameters

B. Apply CISCO ISE default settings

C. Select a RADIUS authentication server

D. Disable the RADIUS server accounting interim update

Correct Answer: *C*

Community vote distribution

C (50%) A (50%)

noxy93 Highly Voted 1 month, 3 weeks ago

Answer C is correct
To configure a Cisco WLC with WPA2 Enterprise mode and avoid global server lists, the engineer must perform the following action:

1. Set up a RADIUS server for authentication and authorization.
2. Configure the WLC to use the RADIUS server for client authentication.
3. Enable WPA2 Enterprise mode on the WLC.
4. Disable the use of global server lists on the WLC.

upvoted 7 times

teems5uk Most Recent 1 day, 2 hours ago

Selected Answer: C

C. Select a RADIUS authentication server

upvoted 1 times

Fanny1493 2 months ago

Selected Answer: A

WPA2 Enterprise is 802.11x with EAP, i think that the correct answer is A

upvoted 1 times

Question #875 *Topic 1*

```
flow record v4Talkers
 match ipv4 source address
 match ipv4 destination address
 collect counter bytes long
!
flow record v6Talkers
 match ipv6 source address
 match ipv6 destination address
 collect counter bytes long
!
flow monitor v4Talkers
 record v4Talkers
!
flow monitor v6Talkers
 record v6Talkers
```

Refer to the exhibit. An administrator must collect basic statistics about the approximate amount of IPv4 and IPv6 flows entering Gi0/0 using NetFlow. However, the administrator is concerned that NetFlow processing during periods of high utilization on Gi0/0 will overwhelm the router CPU. Which configuration minimizes CPU impact and keeps the data flows across Gi0/0 intact?

A.
```
sampler R-1-1024
  mode random 1 out-of 1024
!
interface Gi0/0
  ip flow monitor v4Talkers sampler R-1-1024 input
  ipv6 flow monitor v6Talkers sampler R-1-1024 input
```

B.
```
policy-map Talkers
  class class-default
    police cir percent 50
      conform-action transmit
      exceed-action drop
!
interface Gi0/0
  service-policy input Talkers
  ip flow monitor v4Talkers
  ipv6 flow monitor v6Talkers
```

C.
```
interface Gi0/0
  load-interval 600
  ip flow monitor v4Talkers
  ipv6 flow monitor v6Talkers
```

D.
```
interface Gi0/0
  no ip route-cache
  ip flow monitor v4Talkers
  ipv6 flow monitor v6Talkers
```

Correct Answer: *A*

Community vote distribution

A (100%)

f490efc 5 days, 19 hours ago

Selected Answer: A

Sampler seems right

upvoted 1 times

Question #876 *Topic 1*

Which two mechanisms are used with OAuth 2.0 for enhanced validation? (Choose two.)

A. authorization

B. custom headers

C. request management

D. authentication

E. accounting

Correct Answer: *AD*

Community vote distribution

AD (100%)

teems5uk 1 day, 2 hours ago

Selected Answer: AD

A. Authorization (Correct): OAuth 2.0 is primarily used for authorization, allowing a third-party application to access resources on behalf of the resource owner after the resource owner grants permission. The authorization process is a fundamental part of OAuth 2.0.
D. Authentication (Correct): While OAuth 2.0 itself is not an authentication protocol, it is often used in conjunction with authentication mechanisms such as OpenID Connect. OpenID Connect is built on top of OAuth 2.0 and provides authentication capabilities. So, authentication is an important aspect when OAuth is used in certain contexts.

upvoted 1 times

ciscoccie20 2 weeks, 5 days ago

A & C I Believe
OAuth 2.0 is an authorization protocol and NOT an authentication protocol. As such, it is designed primarily as a means of granting access to a set of resources, for example, remote APIs or user data.

upvoted 1 times

Question #877 *Topic 1*

Which characteristic applies to the endpoint security aspect of the Cisco Threat Defense architecture?

A. detect and block ransomware in email attachments

B. outbound URL analysis and data transfer controls

C. user context analysis

D. blocking of fileless malware in real time

Correct Answer: *D*

Community vote distribution

D (60%) C (40%)

teems5uk 1 day, 2 hours ago

Selected Answer: D

Given answer is correct

upvoted 1 times

Horsefeathers 3 weeks, 5 days ago

Selected Answer: D

A. detect and block ransomware in email attachments - ESA
B. outbound URL analysis and data transfer controls - FirePOWER & FireSIGHT
C. user context analysis - NetFlow & StealthWatch
D. blocking of fileless malware in real time - AMP for Endpoints (one of the features of AMP - "The exploit prevention feature will defend endpoints from exploit-based, memory injection attacks." - where fileless malware is malicious code that works directly within a computer's memory.

https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf
https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html

upvoted 2 times

Fanny1493 2 months ago

Selected Answer: C

I think correct is C

https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

upvoted 2 times

Calinserban 2 months, 1 week ago

Cisco AMP for Endpoints provides file-matching analysis to identify suspicious files when they are transferred onto an endpoint. AMP can provide automated blocking of suspicious files as well as the ability to track the spread of a file throughout the network using a feature known as File Trajectory

upvoted 1 times

SIMULATION

-

Guidelines

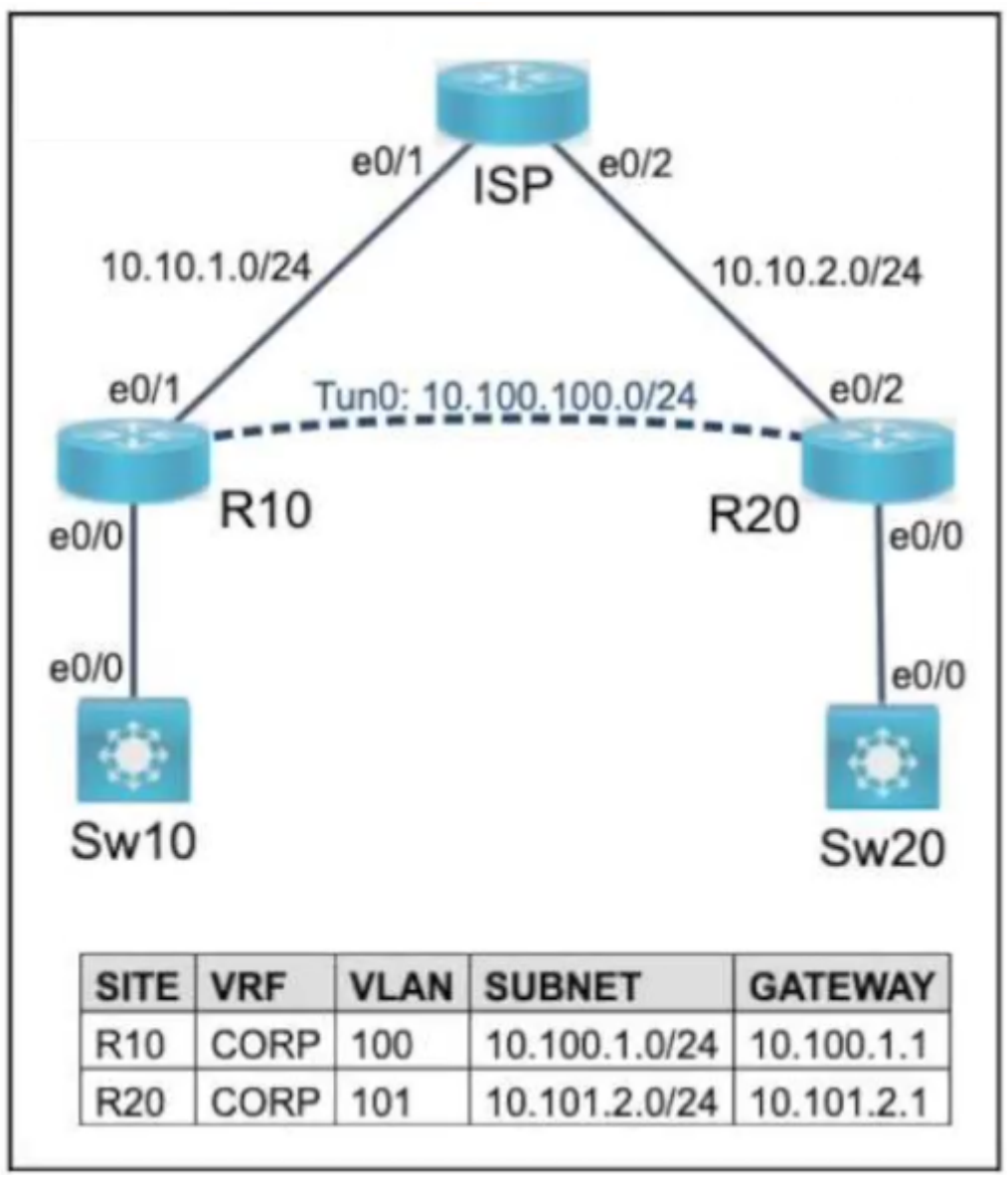
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

Topology

-



SITE	VRF	VLAN	SUBNET	GATEWAY
R10	CORP	100	10.100.1.0/24	10.100.1.1
R20	CORP	101	10.101.2.0/24	10.101.2.1

Tasks

-

The operations team started configuring network devices for a new site. R10 and R20 are preconfigured with the CORP VRF. R10 has network connectivity to R20. Complete the configurations to achieve these goals:

1. Extend the CORP VRF between R10 and R20 using Tunnel0.
2. Protect Tunnel0 using the preconfigured profile
3. Configure static routing on R10 and R20 so that users in VLANs100 and 101 that belong to the CORP VRF are able to communicate with each other. Tunnel0 should be the only interface used to route traffic for the CORP VRF

Correct Answer:

We need to find out the IP addresses of e0/1 of R10 and e0/2 of R20 first with the "show ip interface brief" command on these two routers. Supposethey are 10.10.1.10 and 10.10.2.20 respectively. We will use them in the "tunnel destination …" commands

R10

```
interface Tunnel 0
ip vrf forwarding CORP
tunnel source e0/1
tunnel destination 10.10.2.20
tunnel vrf TECH
```

R20

```
interface Tunnel 0
ip vrf forwarding CORP
tunnel source e0/2
tunnel destination 10.10.1.10
tunnel vrf TECH
```

We are not sure if "TECH" is another VRF configured on both routers. If yes then maybe this sim wants us to configure a "front-door VRF".On a tunnel interface you use the ip vrf forwarding command to place the tunnel interface in that particular routing table.The tunnel vrf command instructs the router to use the specified VRFs routing table for the tunnel source and destination IP addresses.

Static route:
R10:

```
ip route vrf TECH 10.100.1.0 255.255.255.0 tunnel0
```

R20:

```
ip route vrf TECH 10.101.2.0 255.255.255.0 tunnel0
```

Klimy Highly Voted 1 month, 1 week ago

This sim came up for me today without the ipsec. You just put it into vrf (ip vrf forwarding CORP) and set the 2 static routes in the CORP vrf.

R10

```
ip route vrf CORP 10.101.2.0 255.255.255.0 tunnel0
```

R20

```
ip route vrf CORP 10.100.1.0 255.255.255.0 tunnel0
```

And of course save config.

Just note that when you put it into vrf it loses the IP, so you need to set it again. (But you get a message, so you'll see…)

upvoted 6 times

sergiosolotrabajo Most Recent 2 weeks, 1 day ago

I've configured this on EVE-NG:

```
hostname R10
!
!
!
!
ip vrf CORP
description VRF-CORP
rd 12956:1
!
!
!
interface Loopback1
ip vrf forwarding CORP
```

```
ip address 10.10.10.10 255.255.255.255
no sh
!
interface Tunnel0
ip vrf forwarding CORP
ip address 10.100.100.2 255.255.255.0
tunnel source GigabitEthernet0/1
tunnel destination 10.10.2.2
tunnel vrf CORP
!
interface GigabitEthernet0/0
ip vrf forwarding CORP
ip address 10.100.1.1 255.255.255.0
no sh
!
!
interface GigabitEthernet0/1
ip vrf forwarding CORP
ip address 10.10.1.2 255.255.255.0
no sh
!
!
router ospf 1 vrf CORP
router-id 10.10.10.10
passive-interface default
no passive-interface GigabitEthernet0/1
network 10.10.10.10 0.0.0.0 area 0
network 10.10.1.2 0.0.0.0 area 0
network 10.100.1.0 0.0.0.255 area 0
exit
!
ip route vrf CORP 10.101.2.0 255.255.255.0 Tunnel 0
!
!
!
```

upvoted 1 times

sergiosolotrabajo 2 weeks, 1 day ago

```
hostname R20
!
!
!
!
ip vrf CORP
description VRF-CORP
rd 12956:1
!
!
!
interface Loopback1
ip vrf forwarding CORP
ip address 12.12.12.12 255.255.255.255
no sh
!
interface Tunnel0
ip vrf forwarding CORP
ip address 10.100.100.3 255.255.255.0
tunnel source GigabitEthernet0/2
tunnel destination 10.10.1.2
tunnel vrf CORP
!
interface GigabitEthernet0/0
ip vrf forwarding CORP
ip address 10.101.2.1 255.255.255.0
no sh
!
!
interface GigabitEthernet0/2
ip vrf forwarding CORP
ip address 10.10.2.2 255.255.255.0
no sh
!
!
router ospf 1 vrf CORP
router-id 12.12.12.12
passive-interface default
no passive-interface GigabitEthernet0/2
network 12.12.12.12 0.0.0.0 area 0
network 10.10.2.2 0.0.0.0 area 0
network 10.101.2.0 0.0.0.255 area 0
!
ip route vrf CORP 10.100.1.0 255.255.255.0 Tunnel0
!
```

!
!
upvoted 1 times

eearmani 2 weeks, 5 days ago

This one of the new labs
upvoted 1 times

post20 3 weeks, 1 day ago

Simulations need to be updated!... Took the test yesterday. Had 4 simulations. The only one I saw from all presents on "examtopic" was GRE tunnel, without the 3rd task. The other different simulations were OSPF (had to elect DR and BDR without using the command ip ospf network point-to-point), BGP, and the other one with issues on a trunk link between two switches + issues on an ether-channel on two other switches present in the same topology... failed the exam :(
upvoted 1 times

Exam12559 2 months ago

Although I do not know the pre-setting situation when questions are asked in the exam, I will assume that the following conditions are in place.

・"R10 and R20 are preconfigured with the CORP VRF. R10 has network connectivity to R20."
From the above, the underlays 10.10.1.0/24 and 10.10.2.0/24 may also be configured with CORP VRF.
・It is not necessarily necessary to create a new VRF. Use default routing process.

Therefore, I think the necessary settings are as follows.

[Task 1]
R10(config)# interface Tunnel 0
R10(config-if)# tunnel source e0/1
R10(config-if)# tunnel destination 10.10.2.20
R10(config-if)# tunnel vrf CORP
[Task 2]
R10(config-if)# tunnel protection ipsec EXAMPLE
[Task 3]
R10(config)# ip route 10.100.1.0 255.255.255.0 tunnel0
[others]
R10# copy run sta
upvoted 2 times

Exam12559 2 months ago

Correct the above.
In [Task 1], it is stated that the CORP VRF will be expanded, so I think the tunnel will be established on the CORP VRF.
The corrected version is as follows.

R10
[Task 1]
R10(config)# interface Tunnel 0
R10(config-if)# ip vrf forwarding CORP
R10(config-if)# ip add 10.100.100.10 255.255.255.0
R10(config-if)# tunnel source e0/1
R10(config-if)# tunnel destination 10.10.2.20

[Task 2]
R10(config-if)# tunnel protection ipsec EXAMPLE

[Task 3]
R10(config)# ip route vrf CORP 10.101.2.0 255.255.255.0 tunnel0

[others]
R10# copy run sta
upvoted 3 times

studying_1 1 month, 1 week ago

for task2, the word profile is missing,
the command is #tunnel protection ipsec profile (profile-name)
upvoted 3 times

Din04 1 month, 2 weeks ago

This is correct. When you apply the vrf on an interface, you always have to apply the IP address configuration again.

Not sure why the provided answers mentions TECH vrf.
upvoted 1 times

Question #879 *Topic 1*

```
#!/usr/bin/python3

import requests

requests.urllib3.disable_warnings()

AuthURL="https://dna-center/dna/system/api/v1/auth/token"
USER="admin"
PASSWORD="SomePassword"

Response = requests.post(AuthURL, auth=(USER, PASSWORD), verify=False)
if Response.status_code < 200 or Response.status_code > 299:
  print(f"Aborting; received status code {Response.status_code}")
  exit()

<...removed...>
```

```
admin@linux:~$ ./fetch.py
Aborting; received status code 401
```

Refer to the exhibit. An administrator writes a script to fetch the list of devices that are registered with Cisco DNA Center. Why does the execution abort?

A. The TLS certificate of DNA Center is invalid

B. The username or the password is incorrect

C. The “dna-center” hostname cannot be resolved to an IP address

D. The authentication URL is incorrect

Correct Answer: *B*

Community vote distribution

B (100%)

teems5uk 1 day, 1 hour ago

Selected Answer: B

B. The username or the password is incorrect.

This is because a status code of 401 usually indicates unauthorized access, which can happen if the provided username or password is incorrect.

upvoted 1 times

Question #880 *Topic 1*

When is GLBP preferred over HSRP?

A. When the gateway routers are a mix of Cisco and non-Cisco routers.

B. When encrypted hellos are required between gateways in a single group.

C. When the traffic load needs to be shared between multiple gateways using a single virtual IP.

D. When clients need the gateway MAC address to be the same between multiple gateways.

Correct Answer: *C*

Question #881 *Topic 1*

Which TLV value must be added to Option 43 when DHCP is used to ensure that APs join the WLC?

A. 0x77

B. AAA

C. 0xf1

D. 642

Correct Answer: *C*

Fanny1493 2 months ago

Correct C
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html
upvoted 1 times

Fanny1493 2 months ago

Correct C
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html
upvoted 1 times

Calinserban 2 months, 1 week ago

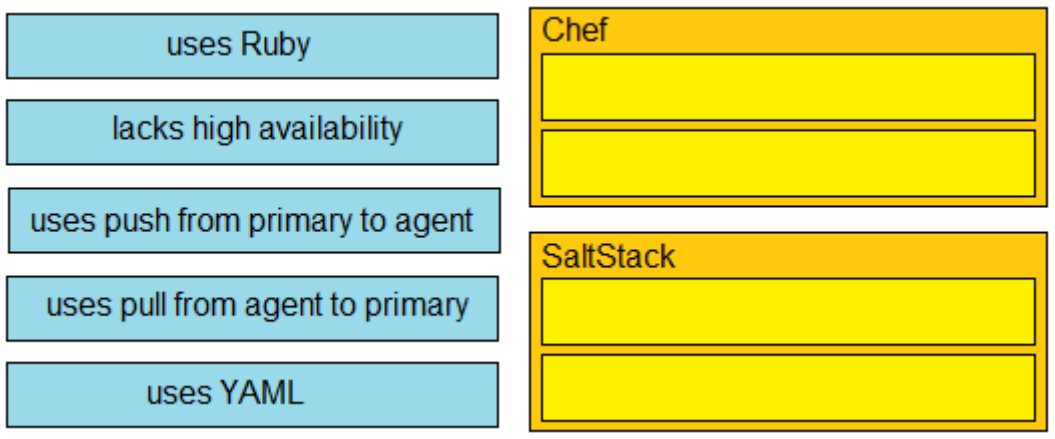
C
The following is the format of the TLV block:
• Type: 0xf1 (decimal 241)
• Length: Number of controller IP addresses * 4
• Value: List of WLC management interfaces
upvoted 1 times

Question #882 *Topic 1*

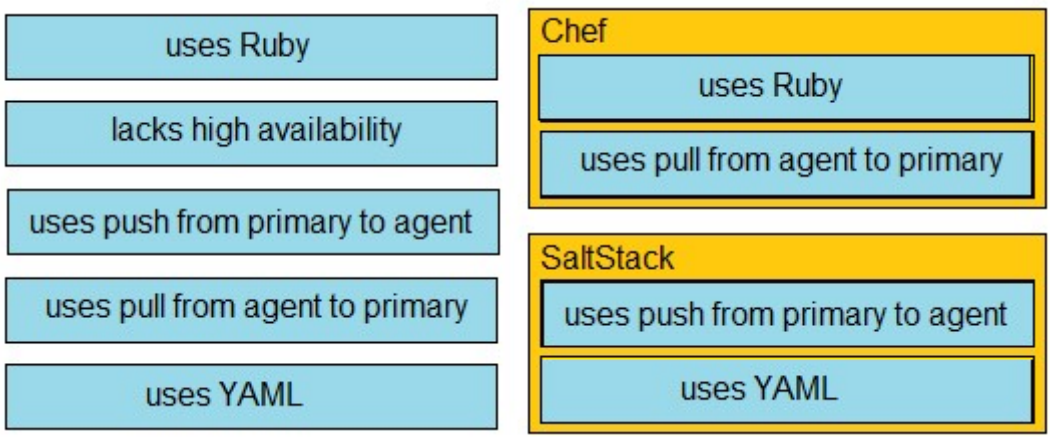
DRAG DROP

-

Drag and drop the automation characteristics from the left onto the appropriate tools on the right. Not all options are used.



Correct Answer:



Question #883 *Topic 1*

What is a characteristic of a virtual machine?

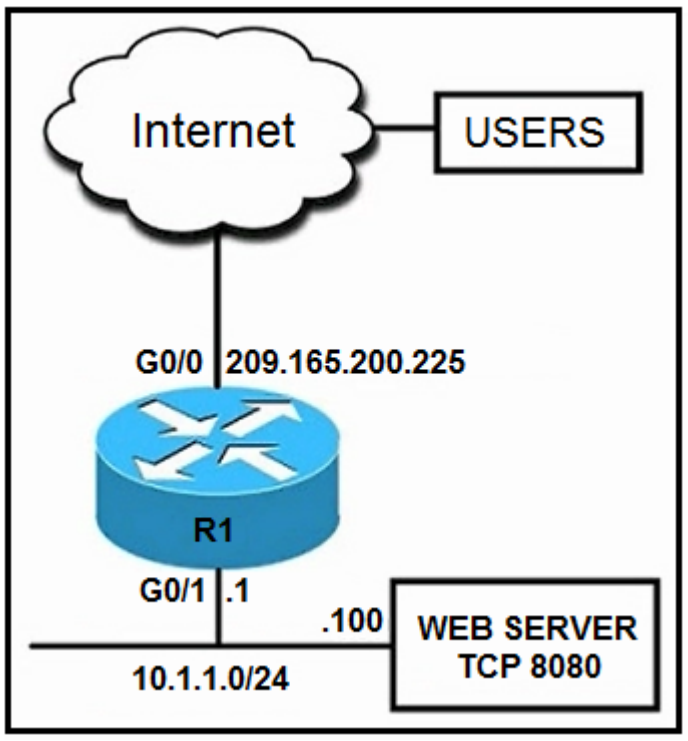
A. It is more resource efficient than a container.

B. It provides an environment completely isolated from the host OS.

C. It is more lightweight than a container.

D. It shares the host OS kernel, binaries, and libraries.

Correct Answer: *B*



Refer to the Exhibit. External users require HTTP connectivity to an internal company web server that is listening on TCP port 8080. Which command set accomplishes?

A. interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat outside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat inside

ip nat inside source static tcp 209.165.200.225 8080 10.1.1.100 8080

B. interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat outside

ip nat inside source static tcp 10.1.1.1 8080 209.165.200.225 80

C. interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat outside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat inside

ip nat inside source static tcp 10.1.1.1 8080 209.165.200.225 80

D. interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat outside

ip nat inside source static tcp 209.165.200.225 80 10.1.1.100 8080

Correct Answer: *C*

Community vote distribution

A (100%)

teems5uk 1 day, 1 hour ago

Selected Answer: A

interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat outside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat inside

ip nat inside source static tcp 209.165.200.225 8080 10.1.1.100 8080

The external interface (G0/0) is configured as an "outside" interface using ip nat outside.
The internal interface (G0/1) is configured as an "inside" interface using ip nat inside.
The static NAT translation is set up using ip nat inside source static tcp, which maps the external IP address and port to the internal IP address and port.
This configuration ensures that traffic entering the router from the internet on port 8080 is translated to the internal web server (10.1.1.100) on port 8080.

Options B, C, and D have incorrect configurations for achieving the specified goal.

upvoted 1 times

kldoyle97 1 week ago

Based on the wording of the question, the answer is either A or C since G0/1 is the inside address.
I believe the translated address should be 10.1.1.100 not "10.1.1.1" since we want to translate the servers address in choice C.
Choice A looks correct if we are trying to do Destination NAT, but it specifies "source".

Not sure what to go with :/

upvoted 1 times

Question #885 *Topic 1*

A network engineer must configure the VTY lines on a router to achieve these results:
• Remote access should be permitted only for secure protocols.
• Only a password should be required for device authentication.
• All idle EXEC sessions must be terminated in 60 minutes.

Which configuration should be applied?

A. line vty 0 15
password Cisco123
transport input ssh
exec-timeout 60

B. line vty 0 15
login
password Cisco123
transport input ssh
exec-timeout 60

C. line vty 0 15
password Cisco123
transport input telnet ssh
exec-timeout 60

D. line vty 0 15
password Cisco123
transport input all
session-timeout 60

Correct Answer: *B*

Community vote distribution

A (100%)

teems5uk 1 day, 1 hour ago

Selected Answer: A

Option A is the only correct answer here.

upvoted 1 times

f490efc 5 days, 3 hours ago

Selected Answer: A

Seems login command is enabled by default. Both A and B looks okay

upvoted 1 times

kldoyle97 1 week, 3 days ago

Its between A and B,
Leaning towards A since the question states that only a password is required.

B specifies "login" under vty configuration.
Doest that mean that it will prompt the user to enter a username and password? however there is no username configured

upvoted 1 times

Question #886 *Topic 1*

How does NETCONF YANG represent data structures?

A. as strict data structures defined by RFC 6020

B. in an XML tree format

C. in an HTML format

D. as modules within a tree

Correct Answer: *B*

Community vote distribution

B (100%)

teems5uk 1 day, 1 hour ago

Selected Answer: B

B. in an XML tree format

upvoted 1 times

Tadese 5 days, 20 hours ago

Selected Answer: B

NETCONF provides various operations to retrieve and edit configuration data from network devices. The Content Layer consists of configuration and state data which is XML-encoded. The schema of the configuration and state data is defined in a data modeling language called YANG.

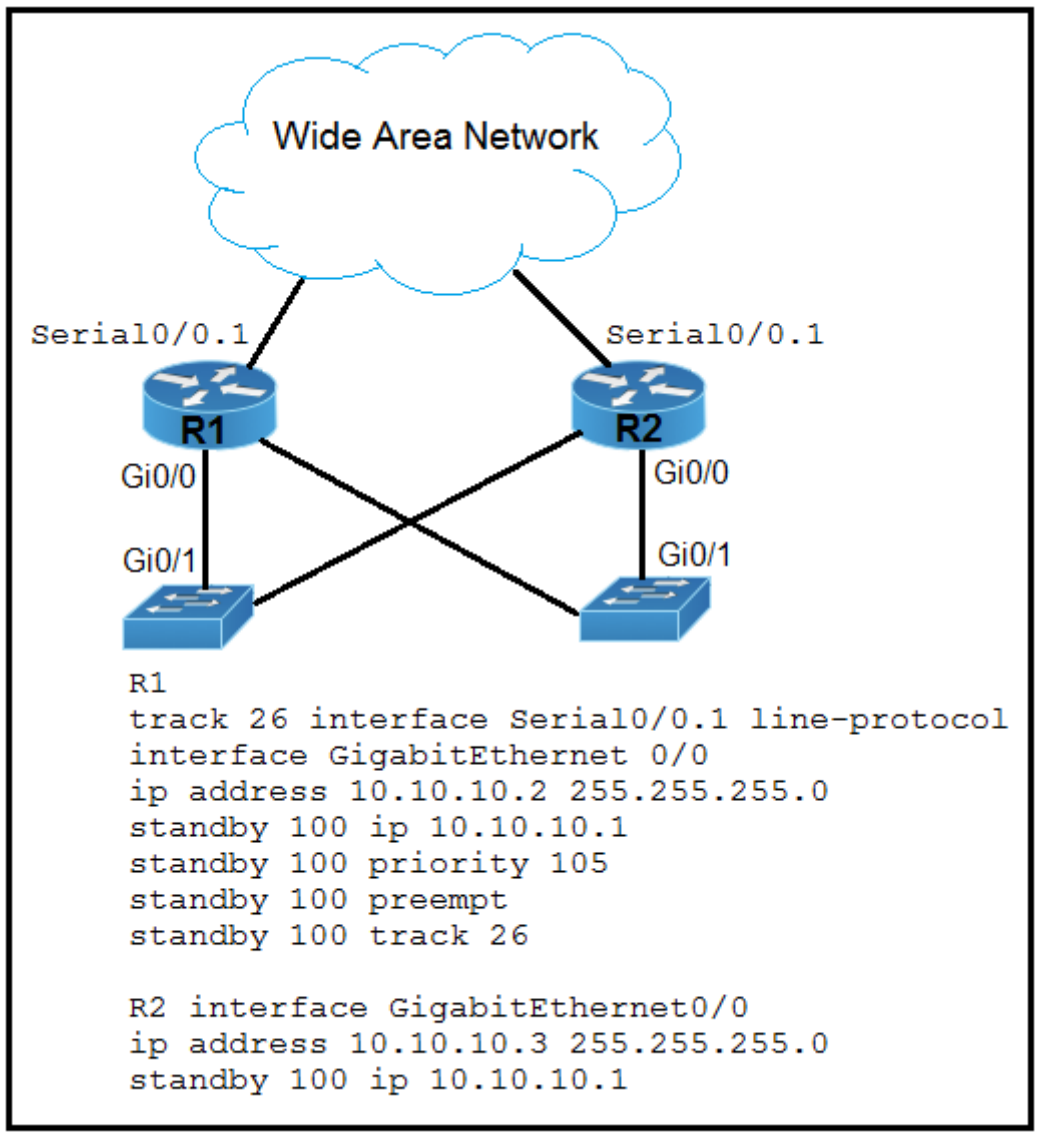
upvoted 1 times

kldoyle97 1 week, 3 days ago

B makes the most sense in a NETCONF context. YANG is leveraged by NETCONF to make RPCs (Remote Procedure Calls) in XML tree format.

options A & D generally describe what a YANG data model is, not relating to NETCONF.

upvoted 1 times



Refer to the exhibit. An engineer must modify the existing configuration so that R2 can take over as the primary router when serial interface 0/0.1 on R1 goes down. Which command must the engineer apply?

A. R2# standby 100 preempt

B. R2# standby 100 priority 100

C. R2# standby 100 track 26 decrement 10

D. R2# track 26 interface Serial0/0.1 line-protocol

Correct Answer: *A*

Community vote distribution

C (67%) A (33%)

teems5uk 1 day ago

Selected Answer: C

I'm going with the option C considering the Track 26 command already applied on R1 "standby 100 track 26".
The command instructs R2 to track the same interface (Serial0/0.1 with the number 26) as R1. When this tracked interface goes down on R1, both routers will adjust their HSRP priorities accordingly, facilitating a smooth failover to R2 if needed.

upvoted 1 times

f490efc 5 days, 3 hours ago

Selected Answer: A

Agree with A. Decrement 10 is default value so you dont need to specify. However, R2 won't takeover unless R1 does not go down completely.

upvoted 1 times

Tadese 5 days, 20 hours ago

Selected Answer: C

R2# standby 100 track 26 decrement 10

upvoted 1 times

Question #888 *Topic 1*

```
from ncclient import manager

netconf_host = manager.connect(host= 'ios-xe-example.com',
                               port=22.
                               username= 'cisco',
                               password= 'cisco',
                               hostkey_verify=False,
                               device_params={'name':'iosxe'})
print (netconf_host.get_config ('running'))
netconf_host.close_session()
```

Refer to the exhibit. An engineer deploys a script to retrieve the running configuration from a NETCONF-capable Cisco IOS XE device that is configured with default settings. The script fails. Which configuration must be applied to retrieve the configuration using NETCONF?

A. print (netconf_host.get_config('show running'))

B. port=830

C. device_params=('name':'los-xe'})

D. hostkey_verify=True,

Correct Answer: *B*

Community vote distribution

B (100%)

teems5uk 1 day ago

Selected Answer: B

B. port=830
NETCONF typically uses port 830 for communication.

upvoted 1 times

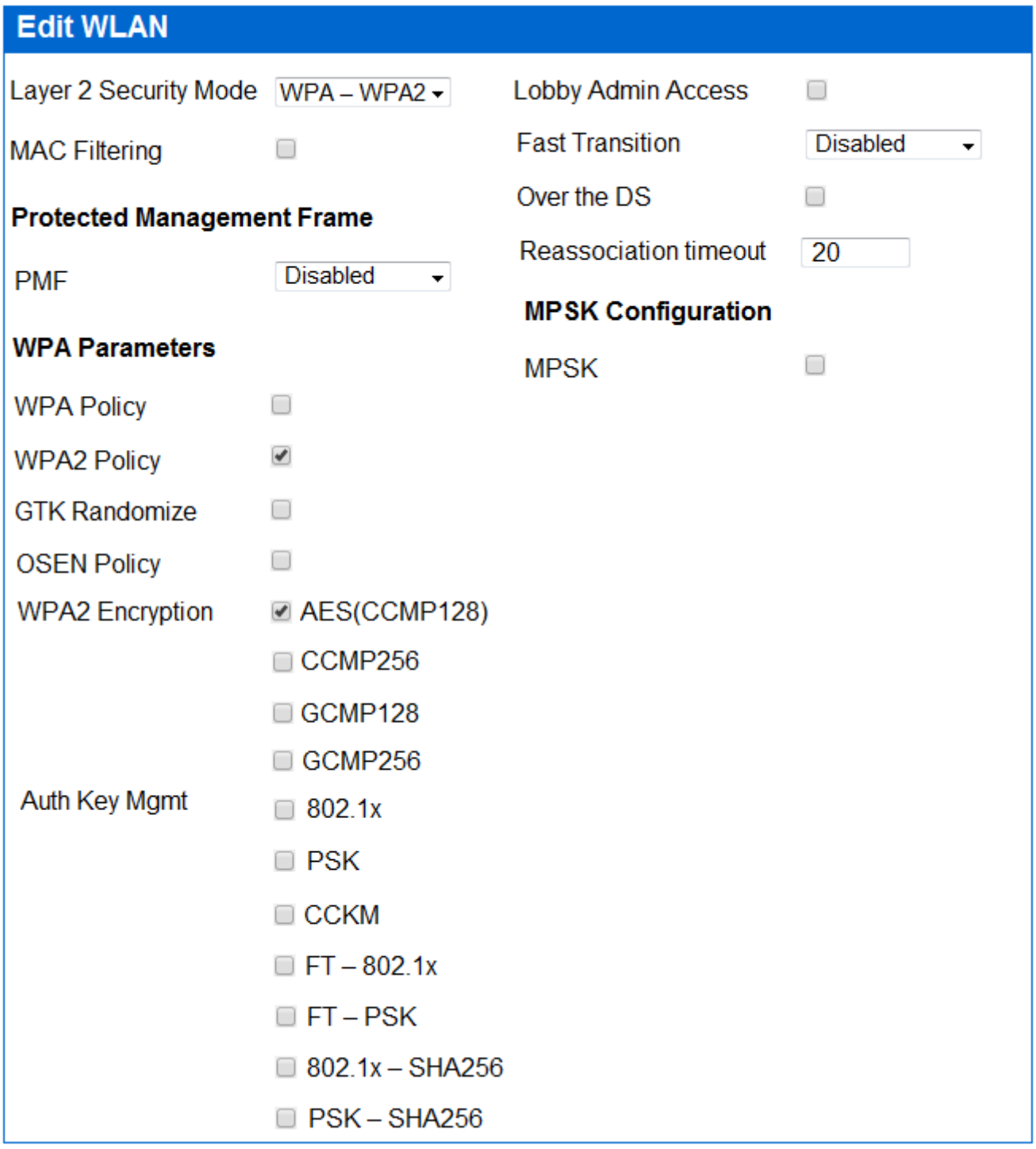
peugeotdude 1 week, 6 days ago

As per Cisco, Netconf uses SSH but defaults to port number 830

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1612/b_1612_programmability_cg/configuring_yang_datamodel.pdf

NETCONFuses a simple RemoteProcedure Call (RPC) based mechanism to facilitate communication between a client and a server. The client can be a script or application running as part of a network manager. The server istypically a network device (switch or router). It usesSecureShell (SSH) asthe transport layer across network devices. It uses SSH port number 830 as the default port. The port number is a configurable option.

upvoted 1 times



Refer to the exhibit. Which action must be taken to configure a WLAN for WPA2-AES with PSK and allow only 802.11r-capable clients to connect?

A. Enable Fast Transition and FT + PSK.

B. Enable Fast Transition and PSK.

C. Change Fast Transition to Adaptive Enabled and enable FT + PSK.

D. Enable PSK and FT + PSK

Correct Answer: *A*

Question #890 *Topic 1*

```
interface Ethernet0/0
 ipaddress 10.1.1.1 255.255.255.252
 ip natoutside
!
interface Ethernet0/0
 ipaddress 10.10.10.1 255.255.255.0
 ip natinside
!
ip nat inside source static 10.10.10.10 10.0.3.10
```

Refer to the exhibit. Which address type is 10.10.10.10 configured for?

A. outside global

B. inside global

C. outside local

D. inside local

Correct Answer: *D*

Question #891 *Topic 1*

```
Router (config) #ntp master
Router (config) #ntp source loopback 0
```

Refer to the exhibit. What is the result of the NTP configuration?

A. The router will use the address of loppback 0 to communicate with the NTP server.

B. The router will advertise but not listen to NTP broadcast packets.

C. The router will be used as an NTP authoritative server only if it synchronized with an outside source.

D. The router will be used as an NTP authoritative server, even if it is not synchronized with an outside source.

Correct Answer: *D*

Question #892 *Topic 1*

```
R2(config)#event manager applet script_1
R2(config-applet)#action 1 cli command “enable”
R2(config-applet)#action 2 cli command “config t”
R2(config-applet)#action 3 cli command “interface ge0/0”
R2(config-applet)#action 4 cli command “ip add 172.16.1.1 255.255.255.0”
R2(config-applet)#action 5 cli command “no sh”
R2(config-applet)#action 6 cli command “end”
R2(config-applet)#exit
```

Refer to the exhibit. An engineer must create a manually triggered EEM applet to enable the R2 router interface and assign an IP address to it. What is required to complete this configuration?

A. R2(config-apple)#action 4 cli command “ip add 172.16.1.1 0.0.0.255”

B. R2(config)# event manager session cli username

C. R2(config-applet)# event oir

D. R2(config-applet)# event none sync yes

Correct Answer: *D*

Question #893 *Topic 1*

What is stateful switchover?

A. cluster protocol used to facilitate switch failover

B. mechanism to take control from a failed RP while maintaining connectivity

C. mechanism used to prevent routing protocol loops during an RP switchover

D. First Hop Redundancy Protocol for host gateway connectivity

Correct Answer: *B*

Question #894 *Topic 1*

Which two features are available only in next-generation firewalls? (Choose two.)

A. application awareness

B. packet filtering

C. stateful inspection

D. deep packet inspection

E. virtual private network

Correct Answer: *AD*

```
R1#show policy-map control-plane
 Control Plane

 Service-policy input: CoPP
  Class-map: telnet_copp (match-all)
     33 packets, 1988 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: access-group 100
     Police:
          cir 8000 bps, bc 1500 bytes
       conformed 33 packets, 1998 bytes; actions:
          transmit
     exceeded 0 packets, 0 bytes; actions:
          drop
     conformed 0 bps, exceed 0 bps

Class-map: class-default (match-any)
     59 packets, 5516 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: any
R1#sh access-lists 100
Extended IP access list 100
     10 deny tcp host 10.0.0.5 any eq 22 (13 matches)
     20 permit tcp any any eq 22 (2 matches)
     30 deny tcp host 10.0.0.5 any eq telnet (18 matches)
     40 permit tcp any any eq telnet (31 matches)
R1#
```

Refer to the exhibit. Which result is achieved by the CoPP configuration?

A. Traffic that matches entry 10 of ACL 100 is always dropped.

B. Class-default is dropped.

C. Traffic that matches entry 10 of ACL 100 is always allowed with a limited CIR.

D. Traffic that matches entry 10 of ACL 100 is always allowed.

Correct Answer: *D*

Community vote distribution

A (100%)

teems5uk 23 hours, 45 minutes ago

Selected Answer: A

A. Traffic that matches entry 10 of ACL 100 is always dropped.

Correct. The access-list 100 denies traffic from host 10.0.0.5 to any destination on port 22. The CoPP configuration polices this traffic with a CIR and drops the packets exceeding the limit.

upvoted 1 times

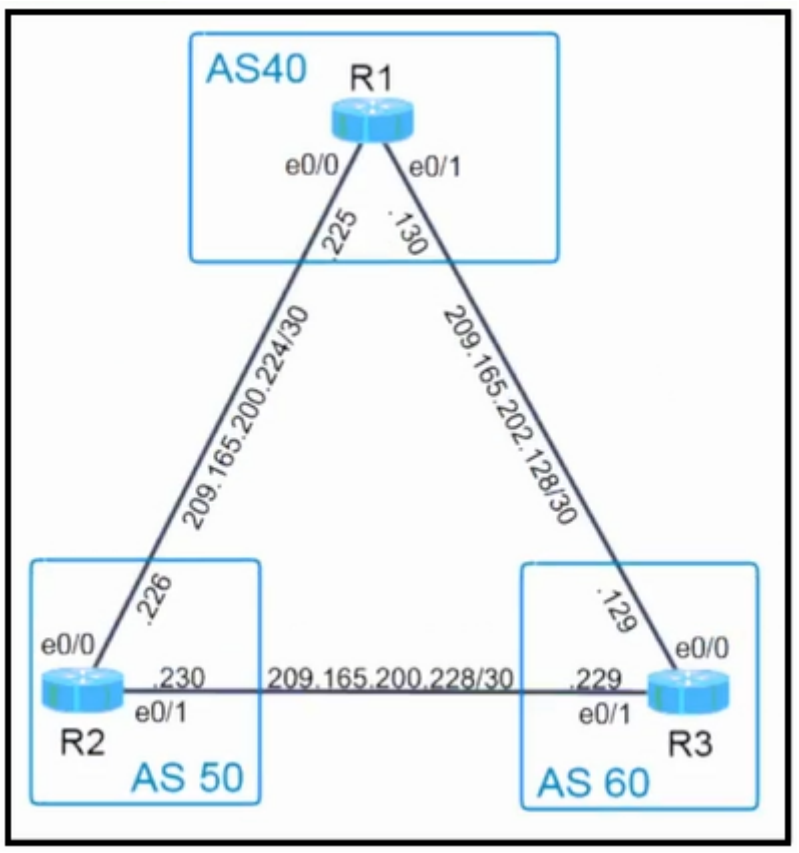
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

Topology
-



Tasks
-

Configure R2 according to the topology to achieve these results:
1. Configure eBGP using Loopback 0 for the router-id. Do not use the address-family command to accomplish this.
2. Advertise R2's Loopback 100 and Loopback 200 networks to AS40 and AS60.

R2
-

```
R2#sh run
Building configuration…

Current configuration : 1365 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
 mi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
  --More--
```

```
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.2.2.2 255.255.255.255
!
interface Loopback100
ip address 209.165.201.11 255.255.255.255
!
interface Loopback200
--More--
```

```
R1#sh run
Building configuration…

Current configuration : 1496 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
  --More--
```

R1

-

```
R1#sh run
Building configuration…

Current configuration : 1496 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
  --More--
```

```
no mmi pvc
mmi snmp-timeout 180

!
!
!
!
!
!
!
!
!
!
!
!
!
!
!

!
!
!
!
ip cef
no ipv6 cef
!
--More--
```

```
!
!
!
!
!
!
!
!
!

!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
--More--
```

```
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.255
!
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
 duplex auto
!
interface Ethernet0/1
 ip address 209.165.202.130 255.255.255.252
--More--
```

```
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.2.2.2 255.255.255.255
!
interface Loopback100
 ip address 209.165.201.11 255.255.255.255
!
interface Loopback200
 ip address 209.165.201.12 255.255.255.255

--More--
```

```
interface Loopback100
 ip address 209.165.201.11 255.255.255.255
!
interface Loopback200
 ip address 209.165.201.12 255.255.255.255
!
interface Ethernet0/0
 ip address 209.165.200.226 255.255.255.252
 duplex auto
!
interface Ethernet0/1
 ip address 209.165.200.230 255.255.255.252
 duplex auto
!
interface Ethernet0/2
 no ip address
 duplex auto
!
interface Ethernet0/3
 no ip address
 duplex auto
!
interface Ethernet1/0
 no ip address
 duplex auto
!
--More--
```

```
!
interface Ethernet1/1
 no ip address
 duplex auto
!
interface Ethernet1/2
 no ip address
 duplex auto
!
interface Ethernet1/3
 no ip address
 duplex auto
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 --More--
```

```
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input none
!
!
end

R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
```

```
R2#
R2#
R2#show ip int brief

% Invalid input detected at '^' marker.
 R2#
Interface      IP-Address          OK? Method Status
     Protocol
Ethernet0/0    209.165.200.226     YES  NVRAM up
     up
Ethernet0/1    209.165.200.230     YES  NVRAM up
     up
Ethernet0/2    unassigned          YES  NVRAM up
     up
Ethernet0/3    unassigned          YES  NVRAM up
     up
Ethernet1/0    unassigned          YES  NVRAM up
     up
Ethernet1/1    unassigned          YES  NVRAM up
     up
Ethernet1/2    unassigned          YES  NVRAM up
     up
Ethernet1/3    unassigned          YES  NVRAM up
     up
Loopback0      10.2.2.2            YES  NVRAM up
     up
Loopback100    209.165.201.11      YES  NVRAM up
     up
Loopback200    209.165.201.12      YES  NVRAM up
R2#
```

```
!
router bgp 40
 bgp router-id 10.10.10.1
 bgp log-neighbor-changes
 neighbor 209.165.200.226 remote-as 50
 neighbor 209.165.202.129 remote-as 60
!
address-family ipv4
 neighbor 209.165.200.226 activate
 neighbor 209.165.202.129 activate
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
--More--
```

R3

-

```
R3#sh config
Using 1496 out of 32768 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
--More--
```

```
!
!
!
!
!
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
--More--
```

```
!
!
!
interface Loopback0
 ip address 10.30.30.3 255.255.255.255
!
interface Ethernet0/0
 ip address 209.165.202.129 255.255.255.252
 duplex auto
!
interface Ethernet0/1
 ip address 209.165.202.229 255.255.255.252
 duplex auto
!
interface Ethernet0/2
 no ip address
 duplex auto
!
interface Ethernet0/3
 no ip address
 duplex auto
!
interface Ethernet1/0
 no ip address
 duplex auto
!
 -More--
```

```
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.30.30.3 255.255.255.255
!
interface Ethernet0/0
```

```
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input none
!
!
end

R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
```

Correct Answer:

```
R2#show ip bgp
 % BGP not active

R2#show ip bgp
 % BGP not active

R2#router bgp 50

% Invalid input detected at '^' marker.

R2#conf t
Enter configuration commands, one per line, End with CNTL/Z.
R2(config)#router bgp 50
R2(config-router)#bgp router-id 10.2
%Incomplete command.

R2(config-router)#bgp-router-id 10.2.2.2
R2(config-router)#neighbor 209.165.202.130 remote-as 40
R2(config-router)#neighbor 209.165.200.230 remote-as 60
%Cannot configure the local system as neighbor
R2(config-router)#neighbor 209.165.200.230 remote-as 60
```

```
R2(config-router)#neighbor 209.165.200.229 remote-as 60
R2(config-router)#route
```

```
*Oct 20 18:33:42.372: %BGP-5-ADJCHANGE: neighbor 209.165.200.229 Up
R2(config-router)#router bgp 50
R2(config-router)#network 209.165.201.11 mask 255.255.255.255
R2(config-router)#network 209.165.201.12 mask 255.255.255.255
R2(config-router)#exit
R2(config)#
```

Verification:

```
R1#
R1#
R1#
R1#
R1#
R1#show ip roturer bgp
Codes: L - local, C - connected, S - static, R - RIP, M - Mobile, B - BG
P
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, *- candidate default,U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

R1#
R1#show ip bgp summary
BGP router identifier 10.10.10.1, local AS number 40
BGP table version is 1, main routing table version 1

Neighbor        V    AS   MsgRcvd   MsgSent   TblVer    InQ  OutQ Up/Down   State/PfxRcd
209.165.200.226 4    50         0         0        1      0    0    never     Idle
209.165.202.129 4    60        78        77        1      0    0    01:08:50        0
```

```
R1#
R1#
R1#
R1#
R1#show ip bgp
R1#show ip bgp
R1#show ip bgp sum
BGP router identifier 10.10.10.1, local AS number 40
BGP table version is 2, main routing table version 2
1 network entries using 144 bytes of memory
1 path entries using 84 bytes of memory
1/1 BGP path/bestpath attribute entries using 160 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 412 total bytes of memory
BGP activity 1/0 prefexies, 1/0 paths, scan interval 60 secs

Neighbor        V    AS   MsgRcvd   MsgSent   TblVer    InQ  OutQ Up/Down   State/PfxRcd
209.165.200.226 4    50   0         0         1         0    0    never     Idle
209.165.202.129 4    60   86        85        2         0    0    01:16:10          1
```

```
Gateway of last resort is not set

     209.165.201.0/32 is subnetted, 2 subnets
B        209.165.201.11 [20/0] via 209.165.202.129, 00:01:15
B        209.165.201.12 [20/0] via 209.165.202.129, 00:00:44
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
[OK]
```

Question #897 *Topic 1*

An engineer must use flexible NetFlow on a group of switches. To prevent overloading of the flow connector, if the flow is idle for 20 seconds, the flow sample should be exported. Which command set should be applied?

A. flow record recordflow
exporter flowexport
record recordflow
cache timeout active 120
cache timeout inactive 20
cache type immediate

B. flow monitor monitorflow
exporter flowexport
record recordflow
cache timeout active 120
cache timeout inactive 20
cache type immediate

C. flow monitor monitorflow
exporter recordflow
cache timeout active 120
cache timeout inactive 20
cache type permanent

D. flow record recordflow
match ipv6 destination ip-address
match ipv6 source ip-address
match ipv6 protocol-type view
match interface input
match interface output
match transport destination-port
collect counter bytes long

Correct Answer: *B*

Community vote distribution

B (100%)

teems5uk 23 hours, 34 minutes ago

Selected Answer: B

Correct

upvoted 1 times

Question #898 *Topic 1*

When a branch location loses connectivity, which Cisco FlexConnect state rejects new users but allows existing users to function normally?

A. Authentication-Down/Switch-Local

B. Authentication-Down/Switching-Down

C. Authentication-Central/Switch-Local

D. Authentication-Local/Switch-Local

Correct Answer: *A*

Community vote distribution

A (100%)

Tadese 5 days, 19 hours ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/flexconnect.html#:~:text=authentication%20down%2C%20local%20switching%E2%80%94In,valid%20only%20in%20standalone%20mode.

upvoted 2 times

Question #899 *Topic 1*

```
client.connect(ip, port=22, username=usr, password=pswd)
stdin, stdout, stderr = client.exec_command('show ip bgp 192.168.101.0 bestpath\n')
print(stdout)
```

Refer to the exhibit. Which action does the Python script accomplish?

A. connects to the device using Telnet and exports the routing table information

B. connects to the device using SSH and exports the routing table information

C. displays the output of the show command in an unformatted way

D. displays the output of the show command in a formatted way

Correct Answer: *B*

teems5uk 23 hours, 21 minutes ago

This part ("exports the routing table information") of the option B makes it wrong in my opinion.

upvoted 1 times

ciscoccie20 6 days, 9 hours ago

should be D!

upvoted 1 times

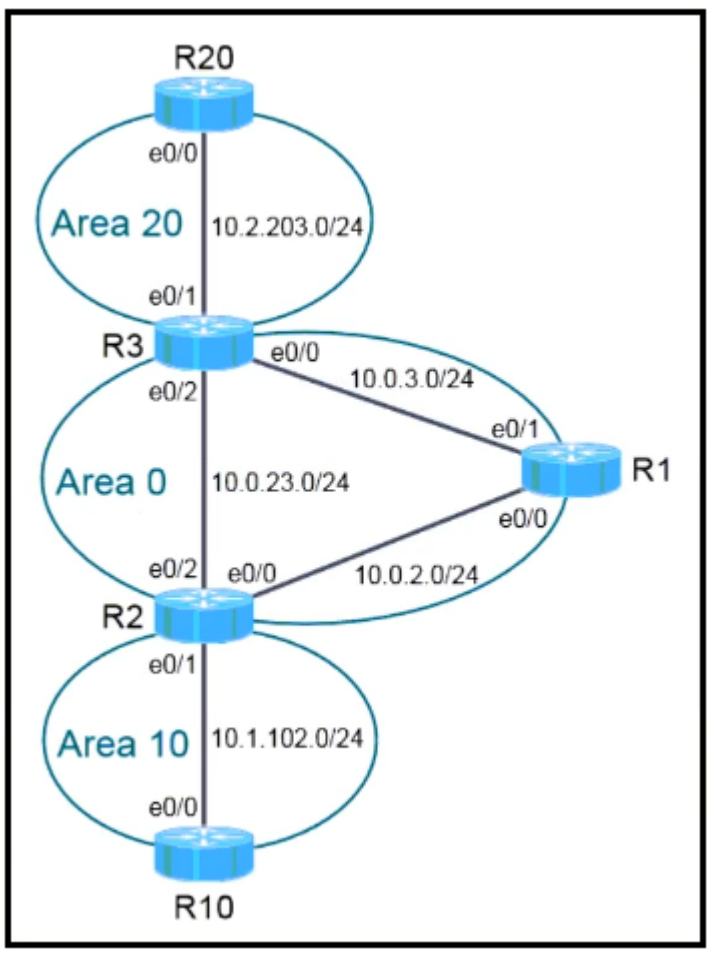
SIMULATION
-

Guidelines
-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.
• Refer to the Topology tab to access the device console(s) and perform the tasks.
• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
• All necessary preconfigurations have been applied.
• Do not change the enable password or hostname for any device.
• Save your configurations to NVRAM before moving to the next item.
• Click Next at the bottom of the screen to submit this lab and move to the next question.
• When Next is clicked, the lab closes and cannot be reopened.

Topology
-



Tasks
-

OSPF is partially configured. Complete the OSPF configurations to achieve these goals:

1. Configure R3 and R20 so they do not participate in a DR/BDR election process in Area 20.
2. Configure R10 so it is always the DR for Area 10. Do not change the router ID.

Correct Answer:

R3

Config t
int e0/1
ip ospf priority 0

R20

Config t
int e0/0
ip ospf priority 0

R10

Config t
int e0/0
ip ospf priority 255

Tadese 5 days, 19 hours ago

the provided correct without any doubt
Ip ospf 1 priority 0 ----No participation DR/BDR
Ip ospf 1 priority 255--

upvoted 1 times

post20 1 week, 2 days ago

I think what they are looking for is focusing on priorities. when you set the priority to 0 a Router won't be elected as DR or BDR. Also, priorities go from 0 to 255 being 255 the higher number. When you set the priority to 255 the Router will be always elected as the DR, unless there is another router using 255 as priority. In that situation, the tie-breaker would be the highest OSPF router ID.

upvoted 1 times

80085 1 week, 3 days ago

Shouldnt we configure an ospf point to point network for task 1? if we do that, then there is no DR/BDR so then there is no participation.

upvoted 4 times

incognitoborg 2 days, 20 hours ago

I'm also curious why point-to-point would be wrong, unless they don't care which method you use. Does anyone know?

upvoted 1 times

Question #901 *Topic 1*

An engineer must configure interface and sensor monitoring on a router. The NMS server is located in a trusted zone with IP address 10.15.2.19. Communication between the router and the NMS server must be encrypted and password-protected using the most secure algorithms. Access must be allowed only for the NMS server and with the minimum permission levels needed. Which configuration must the engineer apply?

A. ip access-list extended nms
permit 1 host 10.15.2.19 any

snmp-server view ro internet included

snmp-server view ro ifEntry included

snmp-server group nms v3 priv notify ro access nms
snmp-server user user1 nms v3 encrypted auth md5 Password1 pri 3des Password123

B. ip access-list standard nms
permit 10.15.2.19 0.0.0.0

snmp-server view ro iso included

snmp-server view ro ifEntry included

snmp-server group nms v3 priv read ro access nms
snmp-server user user1 nms v3 auth sha Password1 pri aes 256 Password123

C. ip access-list standard nms
permit 10.15.2.19 0.0.0.0

snmp-server view rw iso included

snmp-server view rw ifEntry included

snmp-server group nms v3 auth write rw access nms
snmp-server user user1 nms v3 auth des Password1 pri des Password123

D. ip access-list standard nms
permit 10.15.2.19 255.255.255.255

snmp-server view ro iso included

snmp-server view ro ifEntry included

snmp-server group nms v3 priv read ro access nms
snmp-server user user1 nms v3 auth 3des Password1 pri aes 192 Password123

Correct Answer: *B*

Question #902 *Topic 1*

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip address 10.0.0.3 255.255.255.0
Router(config-if)# standby 512 ip 10.0.0.1
```

Refer to the exhibit. An engineer attempts to configure standby group 512 on interface GigabitEthernet0/1, but the configuration is not accepted. Which command resolves this problem?

A. standby redirects

B. standby 512 priority 100

C. standby 512 preempt

D. standby version 2

Correct Answer: *D*

ciscoccie20 1 week, 5 days ago

Correct!
In HSRP version 1, group numbers are restricted to the range from 0 to 255. HSRP version 2 expands the group number range from 0 to 4095.

upvoted 2 times

Question #903 *Topic 1*

Which mechanism does OAuth use to strengthen REST API security when compared to BasicAuth?

A. Token

B. SSL

C. Authentication

D. TLS

Correct Answer: *A*

Question #904 *Topic 1*

What is the API keys option for REST API authentication?

A. a predetermined string that is passed from client to server

B. a one-time encrypted token

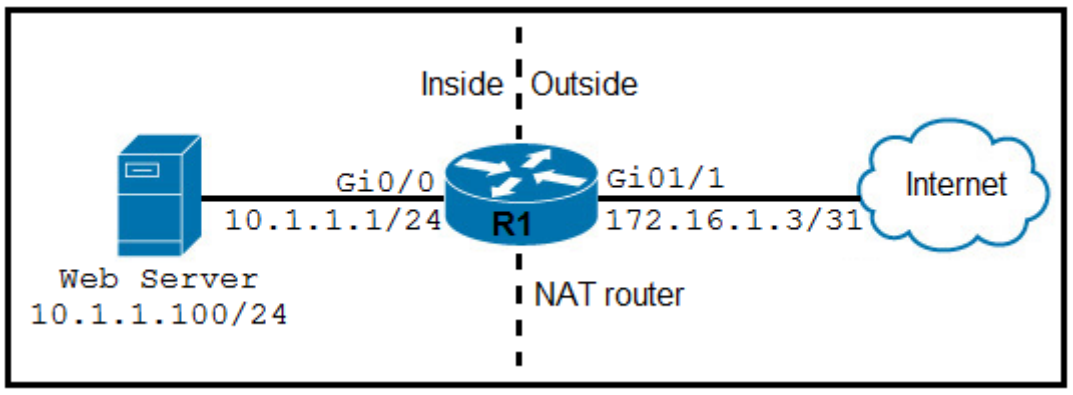
C. a credential that is transmitted unencrypted

D. a username that is stored in the local router database

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #905 *Topic 1*



Refer to the exhibit. The web server is configured to listen only to TCP port 8080 for all HTTP requests. Which command is required to allow Internet users to access the web server on HTTP port 80?

A. ip nat outside static tcp 10.1.1.100 8080 10.1.1.100 80

B. ip nat inside static tcp 10.1.1.100 80 10.1.1.100 8080

C. ip nat inside static tcp 10.1.1.100 8080 10.1.1.100 80

D. ip nat outside static tcp 10.1.1.100 80 10.1.1.100 8080

Correct Answer: *C*

Question #906 *Topic 1*

```
v= json.loads(requests.get("http://10.66.77.88:3000/version").text)[0]['ver']
c = json.loads(requests.get("http://10.66.77.88:3000/version").text)[1]['cnt']
bgp= []
for i in range (int(c)):
        bp.append(json.loads(requests.get("http://10.66.77.88:3000/badip").text)[i]['ip'])
```

Refer to the exhibit. What is achieved by this Python script?

A. It loads JSON data into an HTTP request.

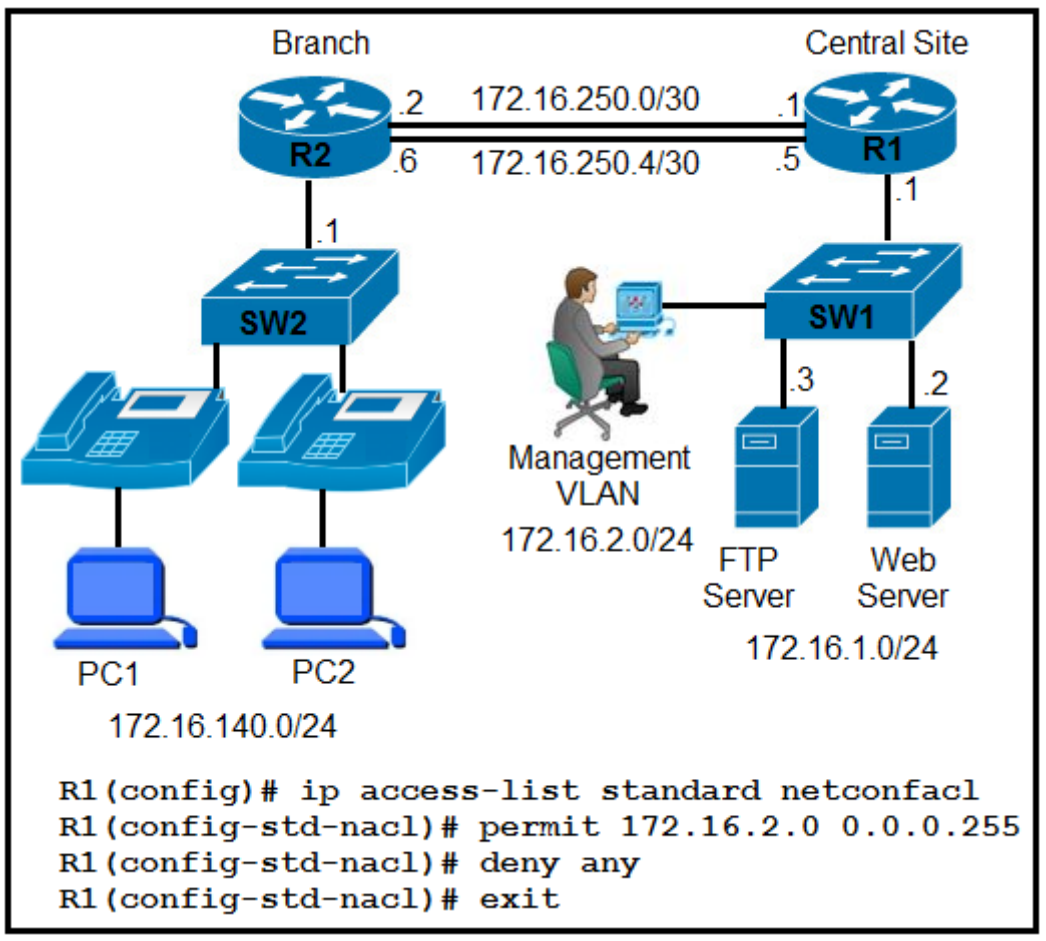
B. It converts JSON data to an HTML document.

C. It counts JSON data from a website.

D. It reads JSON data into a formatted list.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!



Refer to the exhibit. An engineer must configure router R1 to allow only NETCONF connections from the management VLAN. Which command completes this configuration?

A. R1(config-if)# ip access-group netconfacl in

B. R1(config)# netconf-yang ipv4 access-list name netconfacl

C. R1(config)#ip http secure-server
R1(config)# ip http accounting commands 12 default

D. R1(config-if)#ip access-group netconfacl out

Correct Answer: *A*

Community vote distribution

B (100%)

Tadese 5 days, 16 hours ago

Selected Answer: B

: Configuring an ACL for a NETCONF Session
Device# enable
Device# configure terminal
Device(config)# ip access-list standard acl1_permit
Device(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Device(config-std-nacl)# deny any
Device(config-std-nacl)# exit
Device(config)# netconf-yang ssh ipv4 access-list name acl1_permit
Device(config)# end

upvoted 1 times

peugeotdude 1 week, 4 days ago

Selected Answer: B

It's B see https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1612/b_1612_programmability_cg/netconf_and_restconf_service_level_acls.pdf

upvoted 4 times

Question #908 *Topic 1*

Which configuration saves the running configuration to the startup configuration and logs a “saving configuration automatically” message when a syslog message that contains “SYS-5-CONFIG_I” is received?

A.
```
event manager applet save_config
 event syslog pattern “SYS-5-CONFIG_I” period 1
 event track 1
 action 1.0 cli command “write mem”
 action 2.0 syslog msg “saving configuration automatically”
```

B.
```
event manager applet save_config
 action 1.0 string match “SYS-5-CONFIG_I” save_config
 action 2.0 cli command “write mem”
 action 3.0 syslog msg “saving configuration automatically”
```

C.
```
event manager applet save_config
 event syslog pattern “SYS-5-CONFIG_I” period 1
 action 1.0 cli command “end”
 action 2.0 cli command “write mem
 action 3.0 syslog msg “saving configuration automatically”
```

D.
```
event manager applet save_config
 event syslog pattern “SYS-5-CONFIG_I” period 1
 action 1.0 cli command “write mem”
 action 2.0 syslog msg “saving configuration automatically”
```

Correct Answer: *C*

bigyan_jhapaca4 1 week, 2 days ago

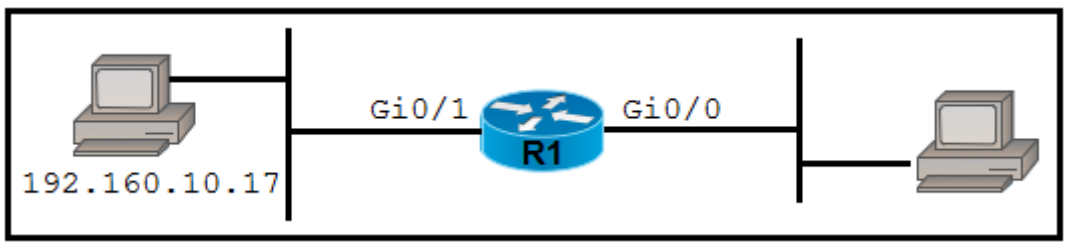
All options are wrong
Option C could be correct if action 1.0 has enable instead of end
action 1.0 cli command "enable"

upvoted 1 times

99a6054 6 days, 19 hours ago

I think C is right. Switch has to go to user exce mode for the 'wr mem' to work. 'end' will take to user exec mode directly from other modes.

upvoted 2 times



Refer to the exhibit. An engineer applies this configuration to R1: ip nat inside source static 192.168.10.17 192.168.27.42

Which command set should be added to complete the configuration?

A. R1(config)# interface GigabitEthernet 0/0

R1(config-if)# ip nat outside -

R1(config)# interface GigabitEthernet 0/1

R1(config-if)# ip nat inside -

B. R1(config)# interface GigabitEthernet 0/0

R1(config-if)# ip pat outside -

R1(config)# interface GigabitEthernet 0/1

R1(config-if)# ip pat inside -

C. R1(config)# interface GigabitEthernet 0/0

R1(config-if)# ip pat inside -

R1(config)# interface GigabitEthernet 0/1

R1(config-if)# ip pat outside -

D. R1(config)# interface GigabitEthernet 0/0

R1(config-if)# ip nat inside -

R1(config)# interface GigabitEthernet 0/1

R1(config-if)# ip nat outside

Correct Answer: *A*

Question #910 *Topic 1*

Which type of roaming event occurs when a client roams across multiple mobility groups?

A. Layer1

B. Layer7

C. Layer3

D. Layer2

Correct Answer: *D*

ciscoccie20 1 week, 5 days ago

Should be L3: C
When a client crosses a mobility group boundary while a roam, the client is fully authenticated, but the IP address is maintained, and EtherIP tunneling is initiated for Layer 3 roaming.

upvoted 3 times

Question #911 *Topic 1*

A Cisco administrstor deploys a new wireless network but CAPWAP APs cannot communicate with the wireless controller. IP connectivity in the network functions properly. Which action resolves the issue?

A. Open CAPWAP UDP port 12222 in the network firewall.

B. Open CAPWAP UDP ports 5246 and 5247 in the network firewall.

C. Enable the UDP Lite feature on the WLC.

D. Ensure that the controller is connected to a AAA server.

Correct Answer: *B*

Community vote distribution

B (100%)

shefo1 1 week ago

Selected Answer: B

UDP ports 5246 and 5247 are the designated ports for CAPWAP control and data traffic, respectively. If these ports are blocked by a firewall, the APs cannot establish a connection with the WLC.

upvoted 1 times

peugeotdude 1 week, 1 day ago

Selected Answer: B

Those are the correct port numbers

upvoted 1 times

Question #912 *Topic 1*

Which technique is used to protect end user devices and data from unknown file behavior?

A. crypto file ransomware protection using a file hash calculation

B. file retrospection using continuous scan and analyses

C. file sandboxing using a protected environment to analyze and simulate the behavior of unknown files

D. phishing file quarantine using an internal environment to store attached files

Correct Answer: *C*

Question #913 *Topic 1*

A client requests a wireless solution for remote branch offices to eliminate the need for a local controller at each branch. The branch users require local termination in a specifc VLAN for local internet breakout. Which solution must be deployed?

A. central switched

B. FlexConnect local switching

C. auto-anchor mobility

D. asymmetric tunneling

Correct Answer: *B*

Question #914 *Topic 1*

Which type of tunnel is required between two WLCs to enable intercontroller roaming?

A. CAPWAP

B. LWAPP

C. mobility

D. IPsec

Correct Answer: *A*

Question #915 *Topic 1*

```
no aaa new-model
username admin privilege 15 secret cisco 123
ip http secure-port 445
```

Refer to the exhibit. Which command must be applied to complete the configuration and enable RESTCONF?

A. ip http server

B. ip http client username restconf

C. ip http secure-port 443

D. ip http secure-server

Correct Answer: *D*

Question #916 *Topic 1*

Which device, in a LISP router architecture, receives LISP map requests and determines which ETR should handle the map request?

A. proxy ETR

B. routing locator

C. map resolver

D. map server

Correct Answer: *C*

Question #917 *Topic 1*

How does a WLC achieve stateful switchover for APs and clients?

A. The active WLC establishes a CAPWAP tunnel to the AP, and the standby WLC establishes a LWAPP tunnel to the AP.

B. The active WLC establishes a CAPWAP tunnel with the AP, and the standby WLC copies the AP database and the client database from the active WLC.

C. The active WLC establishes a CAPWAP tunnel with the AP and standby WLC to share the AP database information.

D. The active and standby WLCs establish separate CAPWAP tunnels to the AP.

Correct Answer: *C*

Community vote distribution

C (100%)

Tadese 16 hours, 20 minutes ago

Selected Answer: C

The new High Availability (HA) feature (that is, AP SSO) set within the Cisco Unified Wireless Network software release version 8.0 and above allows the access point (AP) to establish a CAPWAP tunnel with the Active WLC and share a mirror copy of the AP database with the Standby WLC. The APs do not go into the Discovery state when the Active WLC fails and the Standby WLC takes over the network as the Active WLC.

upvoted 1 times

kivi_bg 2 days, 21 hours ago

B
allows the access point (AP) to establish a CAPWAP tunnel with the Active WLC and share a mirror copy of the AP database with the Standby WLC
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/High_Availability_DG.html#pgfId-202764

upvoted 1 times

Question #918 *Topic 1*

```
R1
ntp source GigabitEthernet1/1
ntp master
ntp peer 192.168.1.1
interface GigabitEthernet 1/0
ip address 172.16.1.1 255.255.255.248
ntp broadcast
interface GigabitEthernet 1/1
ip address 172.31.100.1 255.255.255.0
```

Refer to the exhibit. What is the purpose of the configuration?

A. The router will function in NTP in client mode.

B. The router will use 172.16.1.1 as the source for NTP packets.

C. The router is allowed to receive NTP broadcast packets.

D. The router will function as an authoritative NTP server.

Correct Answer: *D*

Question #919 *Topic 1*

What is a consideration when designing a Cisco SD-Access underlay network?

A. It must support IPv4 and IPv6 underlay networks.

B. End user subnets and endpoints are part of the underlay network.

C. Static routing is a requirement.

D. The underlay switches provide endpoint physical connectivity for users.

Correct Answer: *D*

Question #920 *Topic 1*

Which JSON script is properly formatted?

A.
```
["Lodging": [
        {
                "type":hotel,
                "location":B01
                "contact":446-301-12847
 }
]
]
```

B.
```
{
 "truck":[
 {
  "type": "Ford",
  "color": "red",
  "year": "1998"
 }
]
}
```

C.
```
["car":{
        "type": "Ford"
        "color": "red",
        "year": "1998",
        }
]
```

D.
```
[
        "subject":{
                "title": "Art History"
                "listing": "elective"
                "session": "Spring"
         }
]
```

Correct Answer: *B*

Question #921 *Topic 1*

Which mechanism can be used to enforce network access authentication against an AAA server if the endpoint does not support the 802.1X supplicant functionality?

A. MAC Authentication Bypass

B. MACsec

C. private VLANs

D. port security

Correct Answer: *A*

Question #922 *Topic 1*

Which NTP concept is used to measure the distance from a device to its authoritative time source?

A. stratum

B. NTP peer

C. GPS

D. atomic clock

Correct Answer: *A*

Question #923 *Topic 1*

Which JSON script is properly formatted?

A.
```
["class": {
            "title": "Science"
            "Grade":"11",
            "location": "Room C",
        }
]
```

B.
```
[ "Lodging":
        {
            "type":B&B,
            "location":Oceanfront,
            "contact":946-509-6364
        }
]
```

C.
```
[
  "subject": {
   [
  "title":"Sewing"
   "listing":"elective"
   "session":"Summer"
  }
 ]
 ]
```

D.
```
{
  "frames": [
   {
    "type":"premium",
    "material":"wood",
    "shape":"square"
   }
 ]
}
```

Correct Answer: *D*

Question #924 *Topic 1*

In a Cisco SD-Access environment, which function is performed by the border node?

A. Connect users and devices to the fabric domain.

B. Group endpoints into IP pools.

C. Provide reachability information to fabric endpoints.

D. Provide connectivity to traditional Layer 3 networks.

Correct Answer: *D*

Question #925 *Topic 1*

What is a characteristic of the overlay network in the Cisco SD-Access architecture?

A. It provides multicast support to enable Layer 2 flooding capability in the underlay network.

B. It provides isolation among the virtual networks and independence from the physical network.

C. It uses a traditional routed access design to provide performance and high availability to the network.

D. It consists of a group of physical routers and switches that are used to maintain the network.

Correct Answer: *B*

Question #926 *Topic 1*

What gives priority on an egress interface, for database traffic that connected on an ingress interface, without changing the CoS value?

A. QoS group

B. policy map

C. CoS map

D. class map

Correct Answer: *B*

Question #927 *Topic 1*

In which way are EIGRP and OSPF similar?

A. Both protocols support autosummarization.

B. Both protocols use hello packets to discover neighbors.

C. Both protocols support unequal-cost load balancing.

D. Both protocols send updates using unicast addresses.

Correct Answer: *B*

Question #928 *Topic 1*

What is a difference between TCAM and the MAC address table?

A. The MAC address table supports partial matches. TCAM requires an exact match.

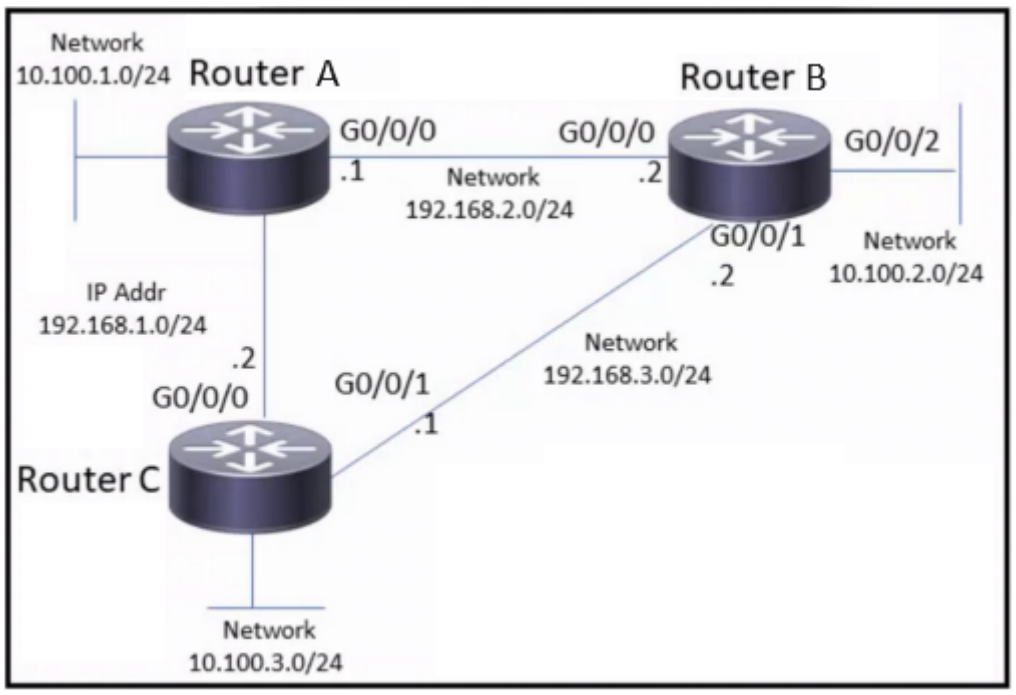
B. TCAM is used to make Layer 2 forwarding decisions. CAM is used to build routing tables.

C. The MAC address table is contained in CAM. ACL and QoS information is stored in TCAM.

D. Router prefix lookups happens in CAM. MAC address table lookups happen in TCAM.

Correct Answer: *C*

Question #929 *Topic 1*



Refer to the exhibit. A network engineer must block Telnet traffic from hosts in the range of 10.100.2.248 to 10.100.2.255 to the network 10.100.3.0 and permit everything else. Which configuration must the engineer apply?

A.
```
RouterB(config)# access-list 101 permit tcp 10.100.2.0 0.0.0.252 10.100.3.0 0.0.0.255
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

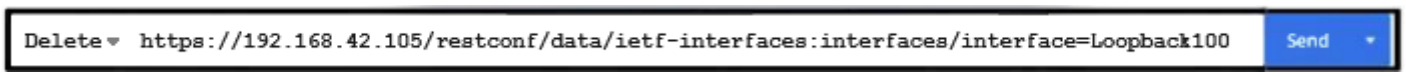
B.
```
RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 23
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

C.
```
RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 22
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

D.
```
RouterB(config)# access-list 101 deny icmp 10.100.2.0 0.0.0.248 10.100.2.0 0.0.0.248
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

Correct Answer: *B*

Question #930 *Topic 1*



Refer to the exhibit. What does the response "204 No Content" mean for the REST API request?

A. Interface loopback 100 is removed from the configuration.

B. Interface loopback 100 is not removed from the configuration.

C. Interface loopback 100 is not found in the configuration.

D. The DELETE method is not supported.

Correct Answer: *C*

Community vote distribution

A (100%)

ciscoccie20 Highly Voted 1 week, 3 days ago

A!
204 (200 http code generally) means successful
upvoted 5 times

Tadese Most Recent 4 days, 22 hours ago

Selected Answer: A

A 204 status code is used when the server successfully processes the request, but there is no content to return to the client. This is typically used for requests where the client wants to indicate that it has finished processing a request, such as a DELETE request
upvoted 1 times

peugeotdude 5 days, 15 hours ago

Selected Answer: A

I vote A
upvoted 1 times

Question #931 *Topic 1*

An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?

A. by organization

B. by hostname naming convention

C. by location

D. by role

Correct Answer: *C*

Question #932 *Topic 1*

What are two characteristics of vManage APIs? (Choose two.)

A. Northbound API is based on RESTCONF and JSON.

B. Southbound API is based on NETCONF and XML.

C. Southbound API is based on RESTCONF and JSON.

D. Southbound API is based on OMP and DTLS.

E. Northbound API is RESTful using JSON.

Correct Answer: *BE*

Question #933 *Topic 1*

Which API does Cisco DNA Center use to retrieve information about images?

A. SWIM

B. Img-Mgmt

C. PnP

D. Client Health

Correct Answer: *A*

Question #934 *Topic 1*

What is a characteristic of the Cisco DNA Center Template Editor feature?

A. It provides a high-level overview of the health of every network device.

B. It facilitates software upgrades to network devices from a central point.

C. It uses a predefined configuration through parameterized elements or variables.

D. It facilitates a vulnerability assessment of the network devices.

Correct Answer: *C*

Question #935 *Topic 1*

Which tunnel type allows clients to perform a seamless Layer 3 roam between a Cisco AireOS WLC and a Cisco IOS XE WLC?

A. CAPWAP

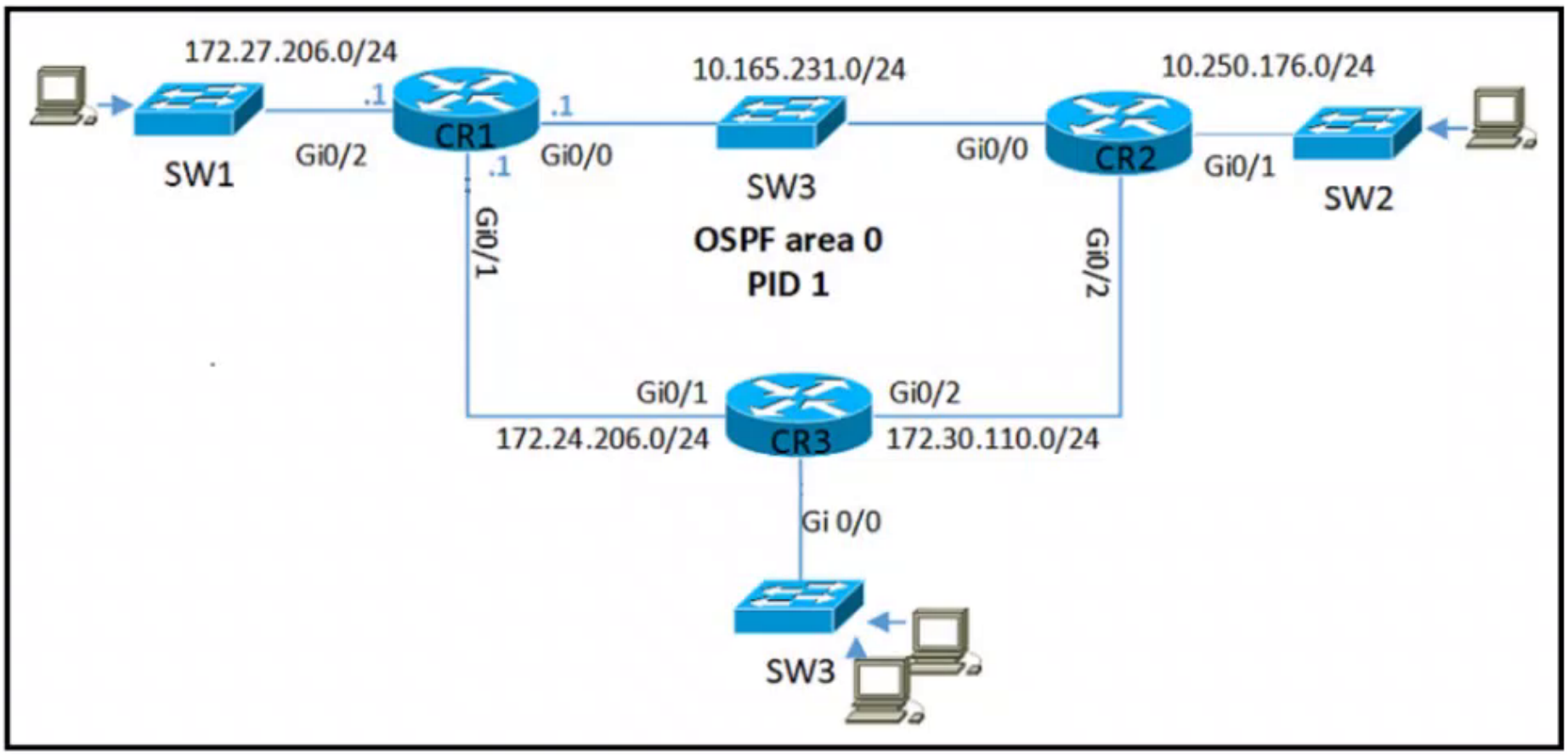
B. IPsec

C. VPN

D. Ethernet over IP

Correct Answer: *A*

Question #936 *Topic 1*



Refer to the exhibit. CR2 and CR3 are configured with OSPF. Which configuration, when applied to CR1, allows CR1 to exchange OSPF information with CR2 and CR3 but not with other network devices or on new interfaces that are added to CR1?

A.
```
router ospf 1
network 10.0.0.0 255.255.255.255  area 0
passive-interface GigabitEthernet0/2
```

B.
```
router ospf 1
network 10.165.231.0 0.0.0.255 area 0
network 172.27.206.0 0.0.0.255 area 0
network 172.24.206.0 0.0.0.255 area 0
passive-interface GigabitEthernet0/2
```

C.
```
interface Gi0/2
ip ospf 1 area 0
router ospf 1
passive-interface GigabitEthernet0/2
```

D.
```
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
network 172.16.0.0 0.15.255.255 area 0
passive-interface GigabitEthernet0/2
```

Correct Answer: *B*

Community vote distribution

B (67%) D (33%)

peugeotdude 4 days, 11 hours ago

Selected Answer: B

We want to advertise all 3 networks into OSPF but avoid forming OSPF adjacencies on that interface, so it is configured as passive-interface

upvoted 2 times

f490efc 4 days, 21 hours ago

Selected Answer: D

D makes most sense

upvoted 1 times

Calinserban 6 days, 5 hours ago

D should be

upvoted 1 times

Question #937 *Topic 1*

What is a characteristic of vManage?

A. It leverages the overlay management protocol to interface with WAN Edge devices.

B. It supports protocols such as OSPF to integrate with legacy network devices.

C. It requires a public IP address to allow WAN Edge devices to discover fabric components.

D. It uses NETCONF to configure vSmart devices to build the overlay network data plane.

Correct Answer: *D*

Question #938 *Topic 1*

```
event manager applet Config
 event cli pattern "configure terminal" [          ]
 action 1.0 cli command "enable"
```

Refer to the exhibit. An engineer constructs an EEM applet to prevent anyone from entering configuration mode on a switch. Which snippet is required to complete the EEM applet?

A. sync yes skip yes

B. sync no skip yes

C. sync no skip no

D. sync yes skip no

Correct Answer: *B*

```
Router(config)# clock timezone EST -5 0
Router(config)# clock summer-time EDT recurring
Router(config)#clock calendar-valid
Router(config)#ntp master
Router(config)#interface vlan 3
Router(config-if)#ntp broadcast
```

Refer to the exhibit. What are two results of the NTP configuration? (Choose two.)

A. It uses other systems as an authoritative time source.

B. It distributes the time via NTP broadcast and multicast packets.

C. It distributes the time via NTP broadcast packets.

D. It forms a peer association with another system.

E. It uses the hardware clock as an authoritative time source.

Correct Answer: *AC*

Community vote distribution

CE (100%)

shefo1 1 week ago

Selected Answer: CE

Explanation of why other options are incorrect:

A. It uses other systems as an authoritative time source: This is false because the ntp master command specifically makes the router the authoritative time source, not relying on external systems.
B. It distributes the time via NTP broadcast and multicast packets: This is partially correct, but the configuration only enables broadcast packets, not multicast.
D. It forms a peer association with another system: This is false because peer associations are formed between NTP servers that synchronize with each other, and this configuration sets the router as a master server that does not synchronize with others.

upvoted 2 times

peugeotdude 1 week, 3 days ago

Selected Answer: CE

I don't think the given answer is valid

upvoted 2 times

Question #940 *Topic 1*

DRAG DROP

-

Drag and drop the code snippets from the bottom onto blanks in the Python script so that the program changes the IP address and saves it as a new JSON file on the disk. Not all options are used.

Answer Area

```
import json

with open("json ios xe.json", "r") as json file:
    json_file_content = json_file. [          ]

decoded_json = json. [          ] (json_file_content)

decoded_json['Cisco-IOS-XE-native:interface']['GigabitEthernet'][0]['ip']
            ['address']['primary']['address'] = \ "192.168.1.2"

encoded_json_compact = json. [          ] (decoded_json)
encoded_json indented = json.dumps(decoded json, indent = 4)

with open("json ios xe compact.json", "w") as json file:
    json_file. [          ] (encoded_json_compact)

with open("json ios xe indented.json", "w") as json file:
    json file.write(encoded json indented)
```

`write()` `loads()` `dumps()` `open()` `read()`

Correct Answer:

Answer Area

```
import json

with open("json ios xe.json", "r") as json file:
    json_file_content = json_file. [ read() ]

decoded_json = json. [ loads() ] (json_file_content)

decoded_json['Cisco-IOS-XE-native:interface']['GigabitEthernet'][0]['ip']
            ['address']['primary']['address'] = \ "192.168.1.2"

encoded_json_compact = json. [ dumps() ] (decoded_json)
encoded_json indented = json.dumps(decoded json, indent = 4)

with open("json ios xe compact.json", "w") as json file:
    json_file. [ write() ] (encoded_json_compact)

with open("json ios xe indented.json", "w") as json file:
    json file.write(encoded json indented)
```

`open()`

Question #941 *Topic 1*

What is the purpose of data modeling languages?

A. to describe a data schema convertible into any data encoding format

B. to provide a framework to describe data flow patterns in networks

C. to specify algorithms necessary to decode binary-encoded protocol data units

D. to translate encoded data for interoperability between different CPU architectures

Correct Answer: *A*

Question #942 *Topic 1*

Which characteristic applies to a traditional WAN solution but not to a Cisco SD-WAN solution?

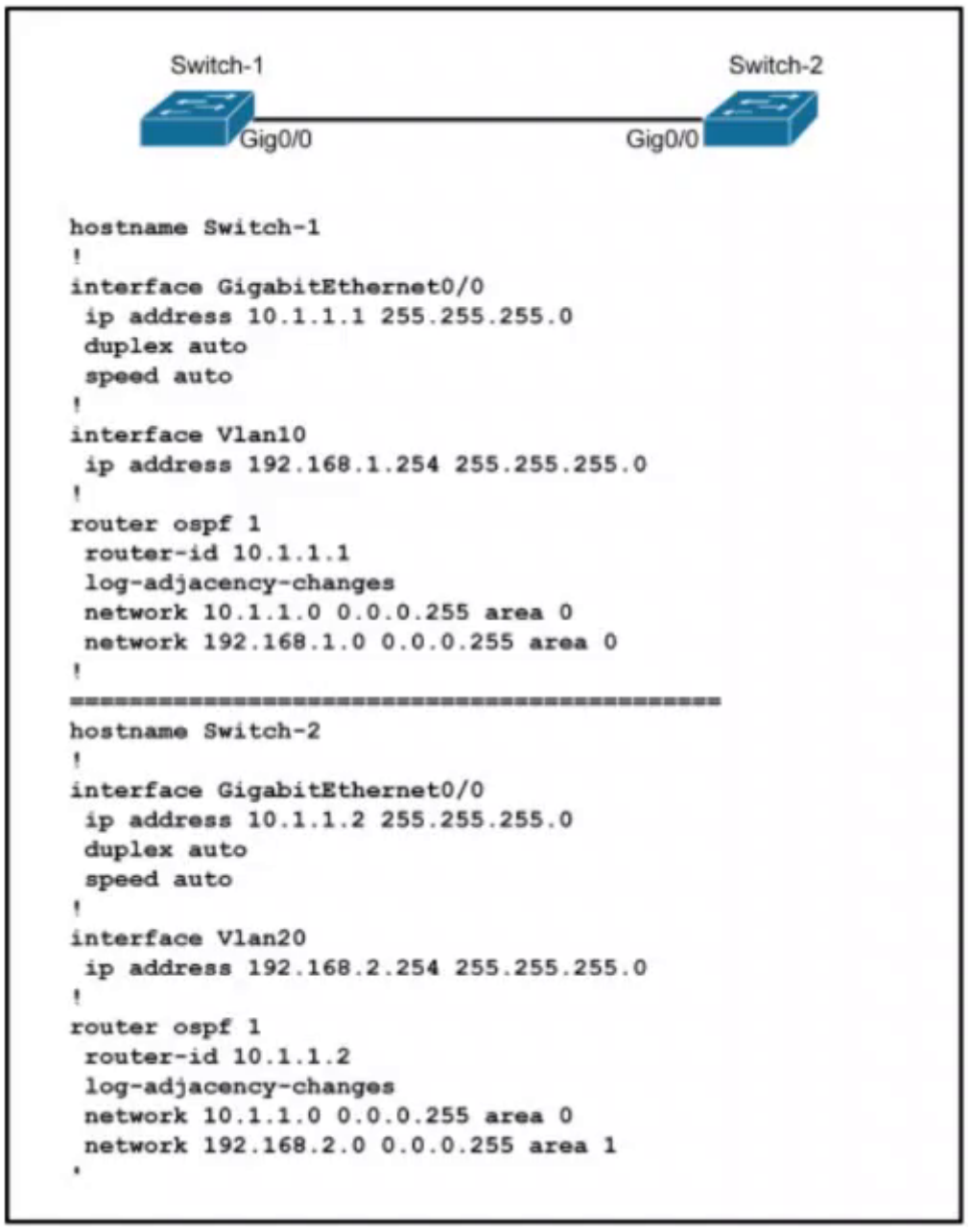
A. time consuming configuration and maintenance

B. centralized reachability, security, and application policies

C. low complexity and increased overall solution scale

D. operates over DTLS/TLS authenticated and secured tunnels

Correct Answer: *A*



Refer to the exhibit. An engineer must prevent VLAN 20 routes from appearing in the routing table of Switch-1. Which command set must be applied?

A. On Switch-1:
router ospf 1
distribute-list 1 out
access-list 1 deny 192.168.2.0 0.0.0.255

B. On Switch-2:
router ospf 1
distribute-list 1 in
access-list 1 deny 192.168.2.0 0.0.0.255

C. On Switch-2:
router ospf 1
distribute-list 1 out
access-list 1 permit 192.168.2.0 0.0.0.255

D. On Switch-1:
router ospf 1
distribute-list 1 in
access-list 1 deny 192.168.2.0 0.0.0.255

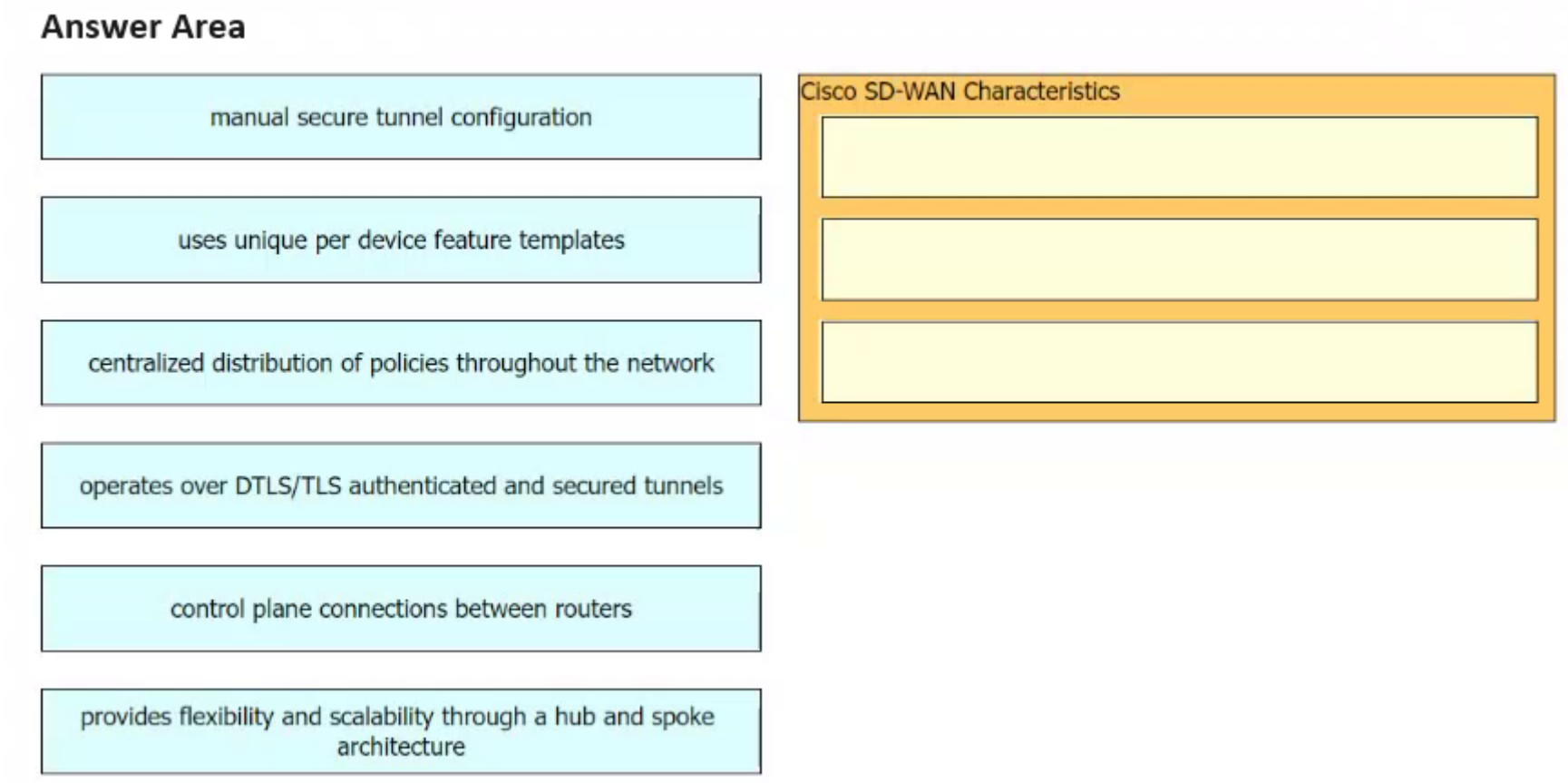
Correct Answer: *D*

Question #944 *Topic 1*

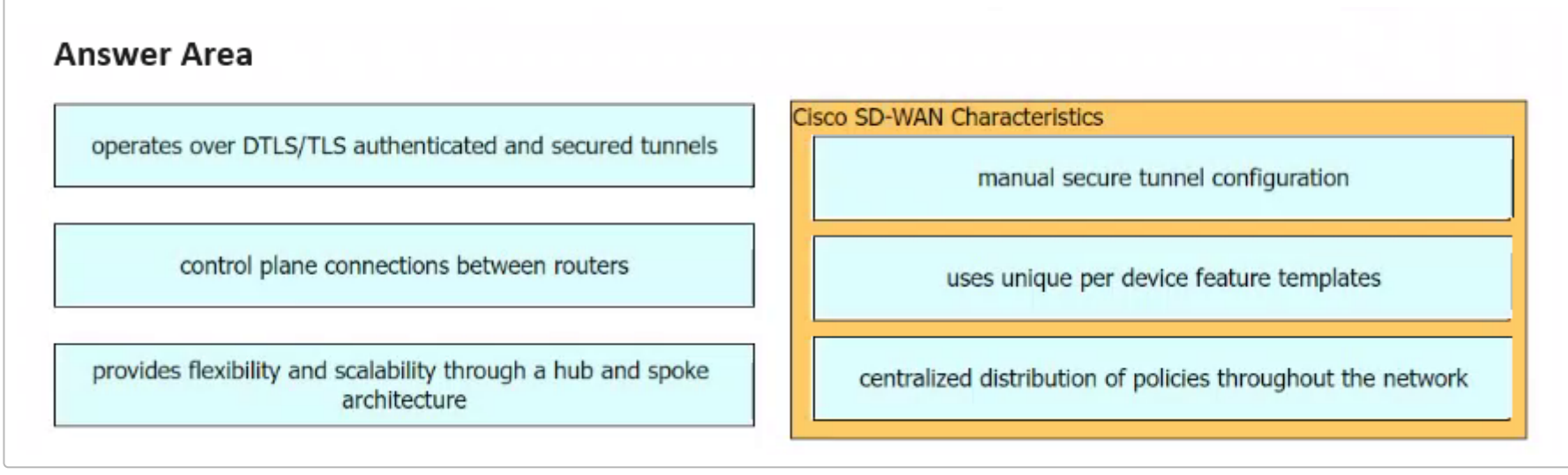
DRAG DROP

-

Drag and drop the characteristics of Cisco SD-WAN from the left onto the right. Not all options are used.



Correct Answer:



Question #945 *Topic 1*

Which policy feature is used with TrustSec to provide endpoint entitlement in an enterprise network?

A. security group tags

B. access control lists

C. virtual local area network

D. virtual routing and forwarding

Correct Answer: *A*

Question #946 *Topic 1*

```
%PM-4-ERR_DISABLE: channel-misconfig (STP) error detected on Po2, putting Et0/1 in err-disable state
FEC: pagp_switch_hotstandby: for agport Po2
FEC: pagp_switch_hotstandby: PAgP not enabled on agport Po2
FEC: pagp_switch_port_down: Et0/1 Inform no
FEC: pagp_switch_invoke_port_down: Et0/1
FEC: fec_unbundle: Et0/1
FEC: pagp_switch_change_vgc: gcchngreq == 0 for Et0/1
FEC: pagp_switch_change_vgc: Et0/1 gcchngreq = 0 gc = 0
FEC: pagp_switch_delete_port_from_agport_internal: delete_port_from_agport: for port Et0/1
FEC: delete port (Et0/1) from agport (Po2)
FEC: pagp_switch_delete_port_from_agport_list: afb->nports-- = 1 [Et0/1]
FEC: Un-Bndl msg NOT send to PM for port Et0/1 from Po2
FEC: pagp_switch_reset_load_index: reading load-index for port Po2
FEC: fec_set_agport_macaddr: Po2 Et0/1 (remove)
FEC: coerce_hwaddr_unix: get aabb.cc00.2020 for L2 Po2 from Et0/2
FEC: coerce_hwaddr_unix: set aabb.cc00.2020 for Po2, 1/1
```

Refer to the exhibit. After unsuccessfully configuring an EtherChannel link, an engineer enables debugging. Which action will resolve the issue?

A. Configure the EtherChannel members in desirable mode.

B. Set the EtherChannel to mode on.

C. Set the EtherChannel to mode active.

D. Configure the EtherChannel members in passive mode.

Correct Answer: *C*

Community vote distribution

A (100%)

shefo1 5 days, 18 hours ago

Selected Answer: A

im sure A is right because
if you look this log message , you see the PAgP , means the misconfigurations in PAgP configuration , in result you ignore the options that is talking about LAcP + static
B - on (static)
C - active (LAcP)
D - passive (LAcp)

upvoted 3 times

99a6054 6 days, 17 hours ago

A seems to be the right answer.

upvoted 1 times

Question #947 *Topic 1*

```
<interface>
   <Loopback>
     <name>100</name>
     <enabled>true</enabled>
   </Loopback>
 </interface>
```

Refer to the exhibit. What is achieved by this code?

A. It unshuts the loopback interface.

B. It displays the loopback interface.

C. It renames the loopback interface.

D. It deletes the loopback interface.

Correct Answer: *A*

Question #948 *Topic 1*

Which collection contains the resources to obtain a list of fabric nodes through the vManage API?

A. device inventory

B. administration

C. device management

D. monitoring

Correct Answer: *C*

Question #949 *Topic 1*

Which Cisco DNA Center Assurance feature verifies host reachability?

A. path trace

B. application experience

C. detail information

D. network time travel

Correct Answer: *A*

DRAG DROP

-

Drag and drop the code snippets from the bottom onto the blanks in the Python script to print the device model to the screen and write JSON data to a file. Not all options are used.

Answer Area

```
import json

data = {
  "measurement": "ifHCInOctets",
  "maxDataPoints": 30,
  "policy": "default",
  "params": None,
  "devices": [
    {"model": "Cisco Nexus 3550", "ipv4": '172.16.16.249'}
  ]
}
  ____ (data["devices"][0]["model"])
with ____ ("data.json", " ____ ") as file:
    json. ____ (data, file, indent=4)
```

dumps | print | dump | open | r | w

Correct Answer:

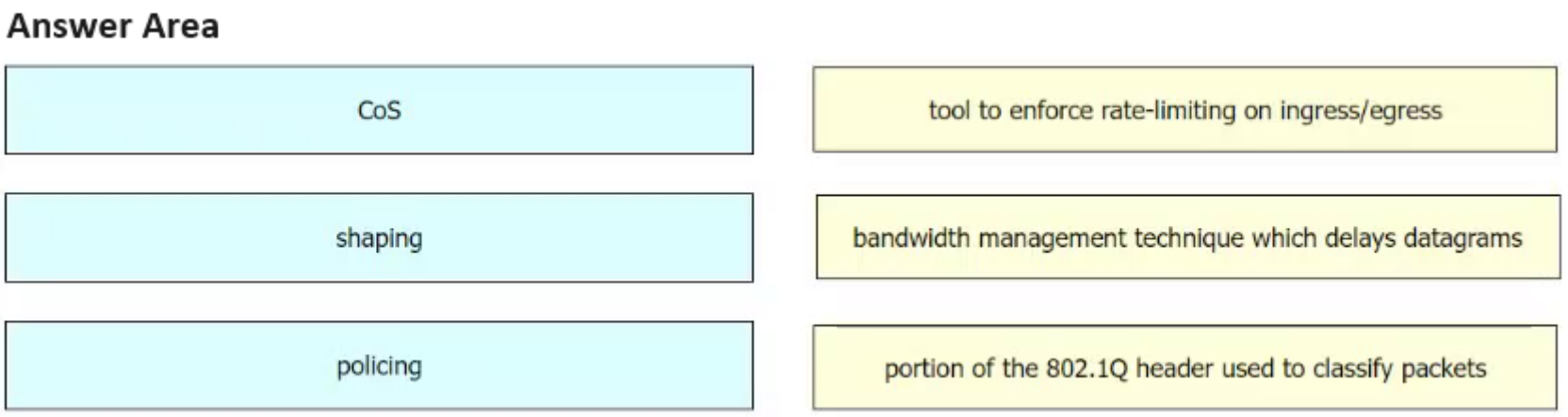
Answer Area

```
import json

data = {
  "measurement": "ifHCInOctets",
  "maxDataPoints": 30,
  "policy": "default",
  "params": None,
  "devices": [
    {"model": "Cisco Nexus 3550", "ipv4": '172.16.16.249'}
  ]
}
  print (data["devices"][0]["model"])
with open ("data.json", " w ") as file:
    json. dump (data, file, indent=4)
```

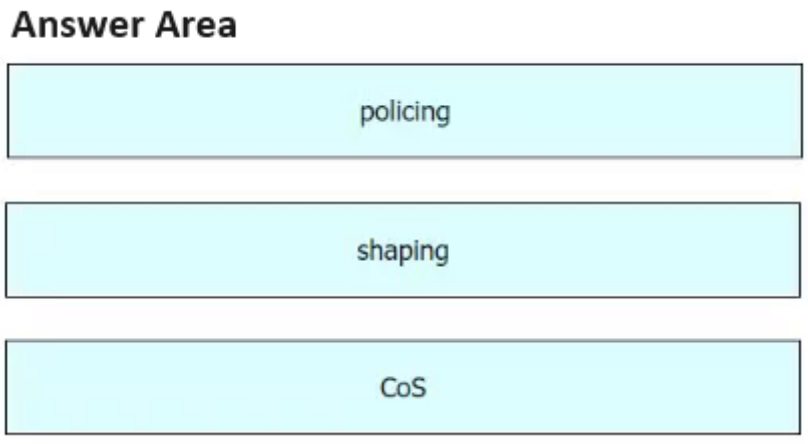
dumps | r

DRAG DROP
-

Drag and drop the QoS mechanisms from the left onto their descriptions on the right.



Correct Answer:



DRAG DROP
-

Drag and drop the code snippets from the bottom onto the blanks in the script to convert a Python object into a JSON string. Not all options are used.

Answer Area

```
import json

data = {
  "measurement": "cefcFRUPowerOperStatus",
  "maxDataPoints": 45,
  "alert":  "True",
  "errorDescription": None,
  "devices": [{"model": "Cisco 4331 ISR"}, {"model": "Cisco 3500 S"}]
}

obj = json. [          ](). [          ]( [          ])

print(obj)
```

JSONEncoder | data | decode | .encode | JSONDecoder

Correct Answer:

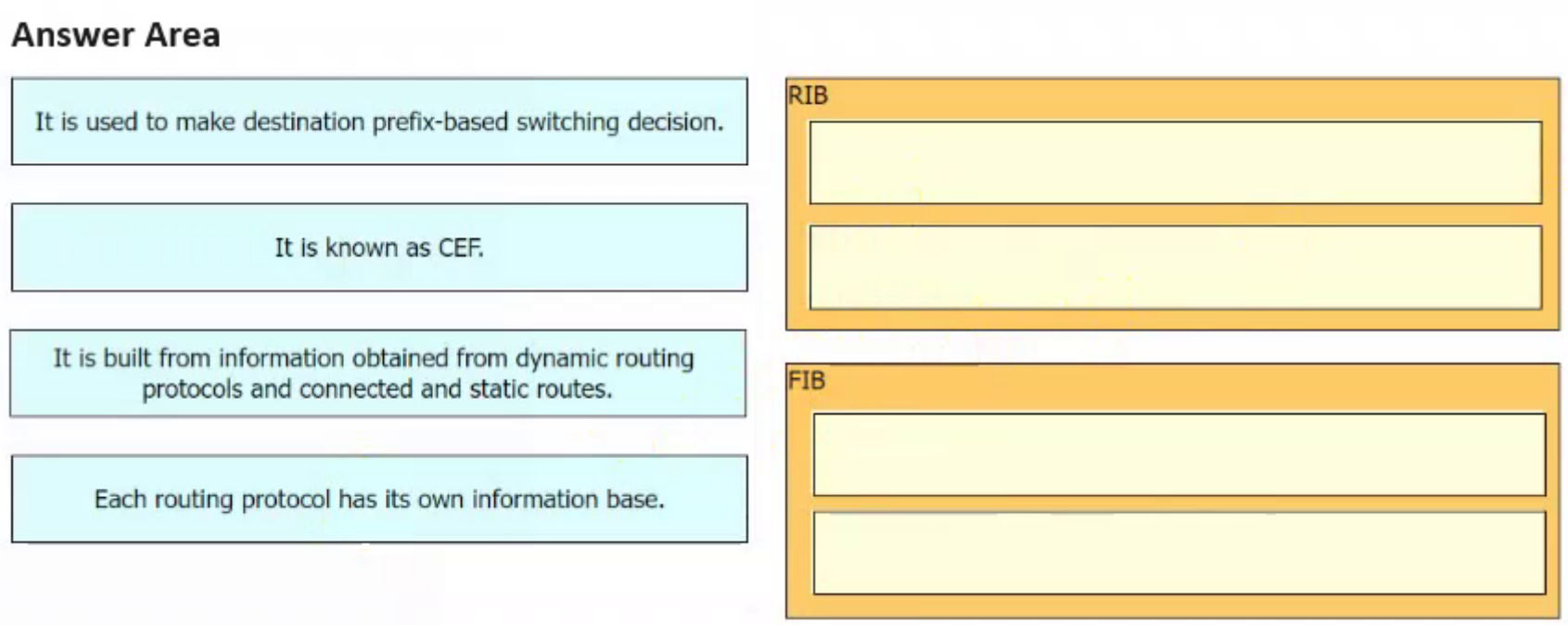
Answer Area

```
import json

data = {
  "measurement": "cefcFRUPowerOperStatus",
  "maxDataPoints": 45,
  "alert":  "True",
  "errorDescription": None,
  "devices": [{"model": "Cisco 4331 ISR"}, {"model": "Cisco 3500 S"}]
}

obj = json. JSONEncoder (). .encode ( data )

print(obj)
```

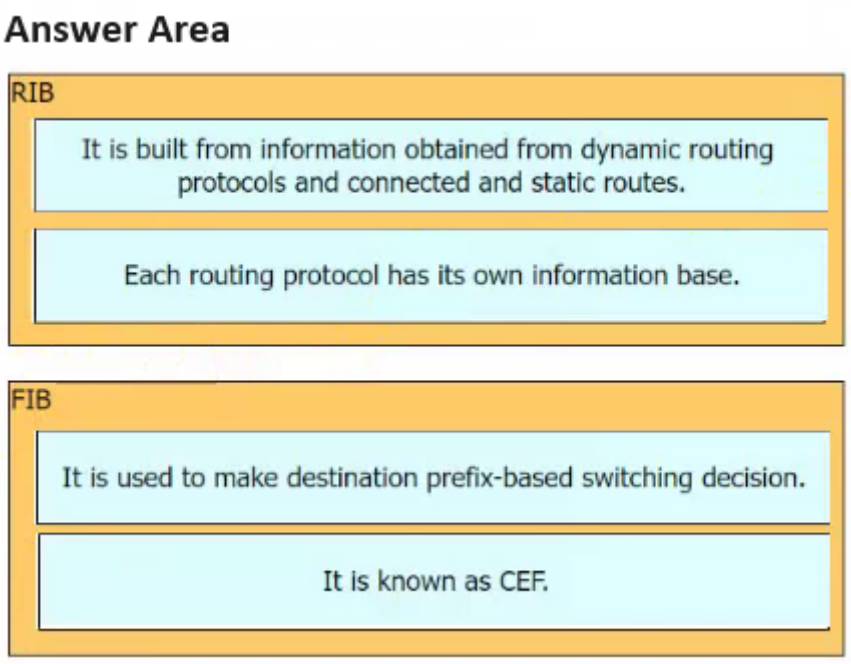
JSONDecoder | decode

DRAG DROP
-

Drag and drop the characteristics from the left onto the corresponding switching architectures on the right.



Correct Answer:



benvz 1 week, 1 day ago
the given answer is correct .
upvoted 2 times

Question #954 *Topic 1*

What is one characteristic of Cisco DNA Center and vManage northbound APIs?

A. They push configuration changes down to devices.

B. They exchange XML-formatted content.

C. They implement the RESTCONF protocol.

D. They implement the NETCONF protocol.

Correct Answer: *B*

Community vote distribution

C (100%)

Tadese 6 days, 19 hours ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-platform/2-3-7/user-guide/b-dnac-platform-ug-2-3-7/b-dnac-platform-ug-2-3-7-chapter-01.html#:~:text=Intent%20APIs%3A%20The%20Intent%20APIs,mechanisms%20that%20implement%20that%20outcome.

upvoted 1 times

benvz 1 week, 1 day ago

Selected Answer: C

WRONG .
One characteristic of Cisco DNA Center and vManage northbound APIs is that they implement the RESTCONF (RESTful Network Configuration Protocol) protocol. RESTCONF is a standard protocol that provides a programmatic interface for accessing and managing network devices. It is based on the principles of REST (Representational State Transfer) and uses HTTP methods (such as GET, POST, PUT, DELETE) to perform operations on network resources.

So, the correct answer is C. They implement the RESTCONF protocol.

upvoted 2 times

Question #955 *Topic 1*

Which feature is offered by the Cisco Advanced Malware Protection for Endpoints solution?

A. File Sandboxing

B. NetFlow

C. TrustSec

D. DNS Protection

Correct Answer: *A*

Calinserban 1 week ago

A
Sandbox analysis: If the file appears to be suspicious, the AMP solution might also execute it in a sandbox environment to observe its behavior in a controlled setting. This helps to identify any malicious activity that may not be immediately apparent.

https://www.aquasec.com/cloud-native-academy/cloud-attacks/advanced-malware-protection/#:~:text=Sandbox%20analysis%3A%20If%20the%20file,may%20not%20be%20immediately%20apparent.

upvoted 2 times

Which JSON script is properly formatted?

A.
```
["Rental": {
            "make": "Chevrolet"
            "model":"Corvette",
            "year": "2023",
        }
]
```

B.
```
[
    "Tables":{

  "use":"dining"
   "material":"glass"
   "shape":"round"
 }
]
]
```

C.
```
[ "Lodging":
        {
            "type":hostel,
            "location": Main Street,
            "phone":346-621-6616
         }
]
```

D.
```
{
  "drinks": [
  {
   "type":"soda",
    "size":"small",
   "cup":"to-go"
   }
  ]
}
```

Correct Answer: *D*

Question #957 *Topic 1*

How are control traffic, client authentication and data traffic handled in a mobility express environment?

A. Control traffic and client authentication is handled centrally by the controller. Data traffic is switched centrally by the controller.

B. Control traffic and client authentication is handled centrally by the controller. Data traffic is switched locally by the access points.

C. Control traffic and client authentication is handled locally by each access point. Data traffic is switched locally by the access points.

D. Control traffic and client authentication is handled locally by each access point. Data traffic is switched centrally by the controller.

Correct Answer: *B*

Community vote distribution

B (100%)

Tadese 4 days, 21 hours ago

Selected Answer: B

https://www.cisco.com/c/dam/en_us/partners/downloads/partner/WWChannels/technology/downloads/frequently-asked-questions.pdf

upvoted 1 times

Mekai2020 1 week ago

Selected Answer: B

Centrally controlled, locally switched

upvoted 2 times

Question #958 *Topic 1*

Which feature allows clients to perform Layer 2 roaming between wireless controllers?

A. mobility groups

B. N+1 high availability

C. RF grouping

D. SSO

Correct Answer: *A*

Question #959 *Topic 1*

What is a characteristic of Cisco DNA Northbound APIs?

A. They utilize multivendor support APIs.

B. They simplify the management of network infrastructure devices.

C. They utilize RESTCONF.

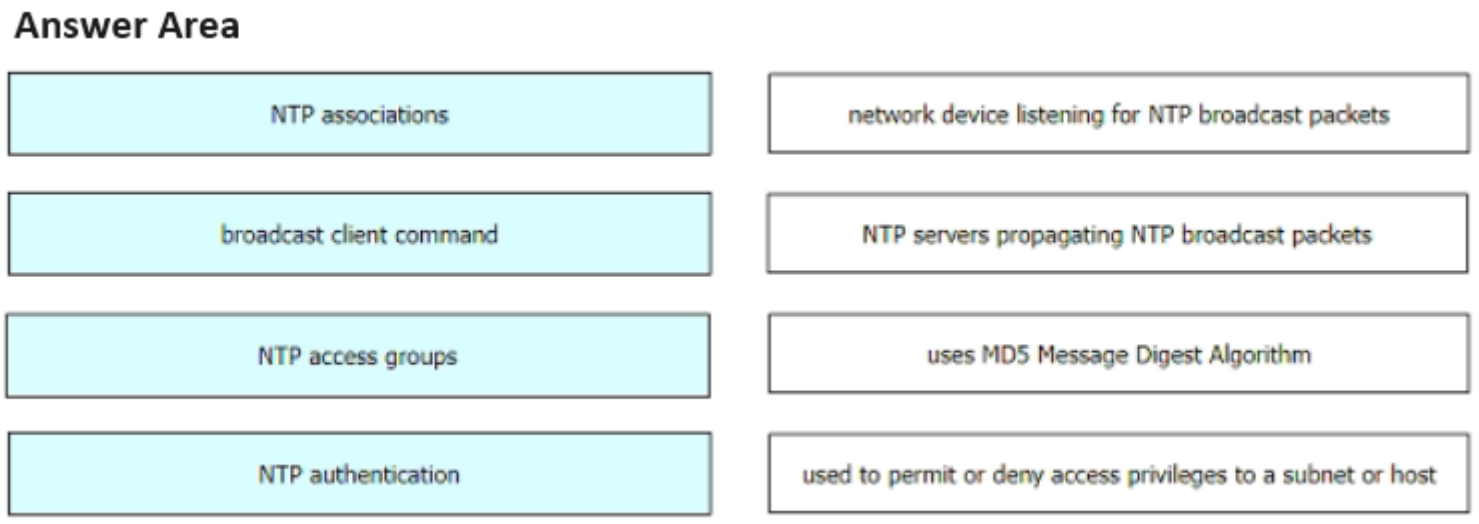
D. They enable automation of network infrastructure based on intent.

Correct Answer: *D*

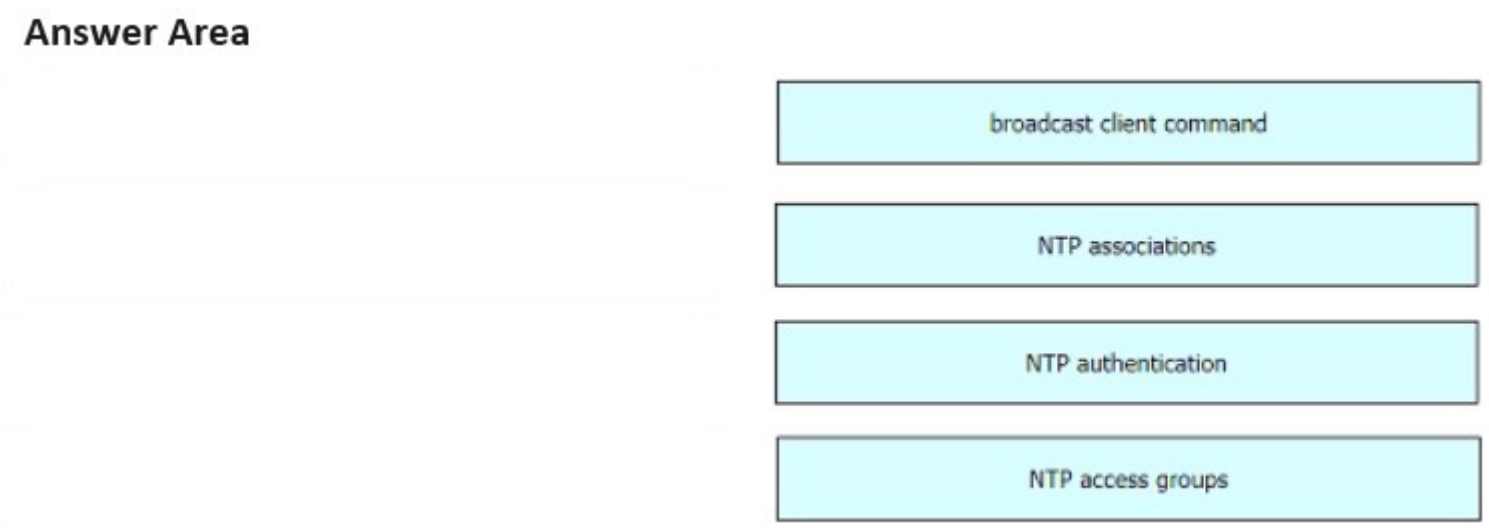
Question #960 *Topic 1*

DRAG DROP
-

Drag and drop the NTP elements from the left onto the correct descriptions on the right.



Correct Answer:



Mekai2020 4 days, 2 hours ago

associations = propagate broadcast
client = listen to broadcast
access = permit or deny access
authentication = MD5

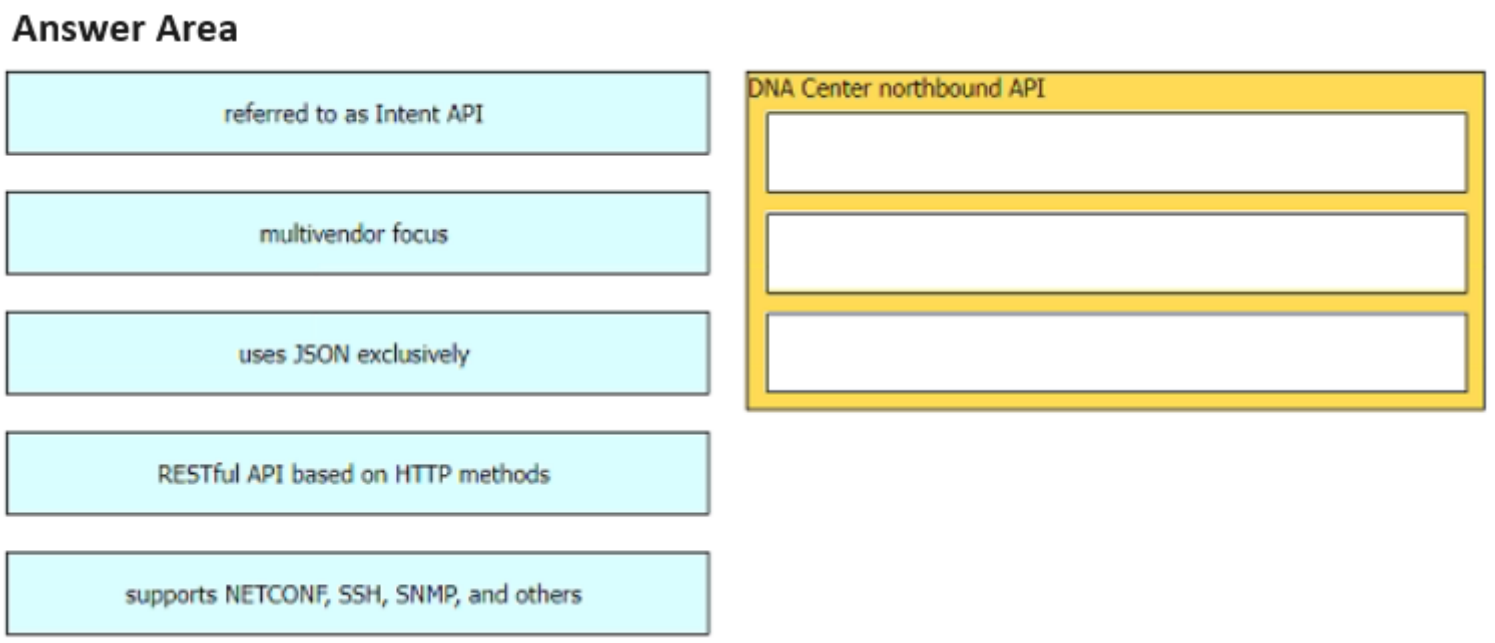
upvoted 1 times

Question #961 *Topic 1*

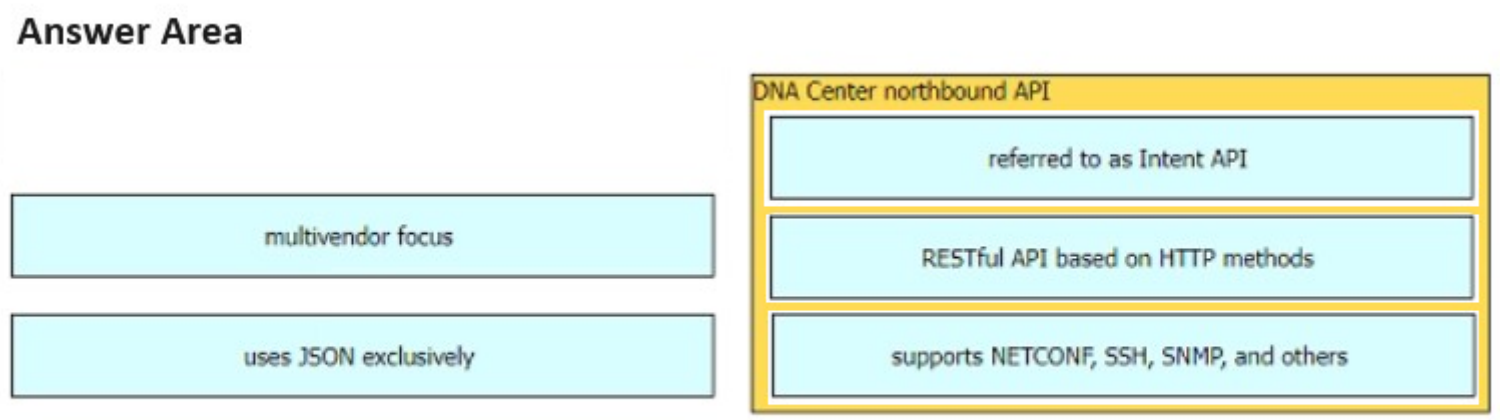
DRAG DROP

-

Drag and drop the Cisco DNA Center northbound API characteristics from the left to the right. Not all options are used.



Correct Answer:



Mekai2020 4 days, 2 hours ago

the answer is correct:

key X= "multivendor focus" and "json exclusive"

upvoted 1 times

Question #962 *Topic 1*


```
R1# debug vrrp error

00:15:30: %IP-4-DUPADDR: Duplicate address 10.18.0.2 on Ethernet1/0, sourced
by 0000.5e00.0101

June 12 8:41:54.447: VRRP: Grp 1 Advertisement Primary address 10.18.0.2

              different from ours 10.18.0.1

June 12 8:41:57.443: VRRP: Grp 1 Advertisement Primary address 10.18.0.2

        different from ours 10.18.0.1

June 12 8:42:00.443: VRRP: Grp 1 Advertisement Primary address 10.18.0.2

        different from ours 10.18.0.1
```

Refer to the exhibit. R1 and R2 are on the same VLAN. VRRP is configured between the two routers. What is the cause of the VRRP error?

A. R1 is configured with VIP 10.18.0.2 on VRRP group 1 and R2 is configured with VIP 10.18.0.1 on VRRP group 1.

B. R1 is configured with VIP 10.18.0.2 on VRRP group 1 and R2 is configured with VIP 10.18.0.2 on VRRP group 1.

C. R1 is configured with VIP 10.18.0.1 on VRRP group 1 and R2 is configured with VIP 10.18.0.2 on VRRP group 0.

D. R1 is configured with VIP 10.18.0.1 on VRRP group 1 and R2 is configured with VIP 10.18.0.2 on VRRP group 1.

Correct Answer: *D*

Community vote distribution

D (100%)

Mekai2020 4 days, 2 hours ago

Selected Answer: D

R1: "different from ours 10.18.0.1" on VRP group 1

upvoted 1 times

Question #963 *Topic 1*

An engineer is implementing a new SSID on a Cisco Catalyst 9800 Series WLC that must be broadcast on 6 GHz radios. Users will be required to use EAP-TLS to authenticate. Which wireless Layer 2 security method is required?

A. WPA2 Enterprise

B. WPA2 Personal

C. WPA3 Enterprise

D. WPA3 Personal

Correct Answer: *C*

Community vote distribution

C (100%)

Mekai2020 4 days, 2 hours ago

Selected Answer: C

When configuring a 6GHz SSID there are certain security requirements that must be met:

WPA3 L2 security with OWE, SAE or 802.1x-SHA256
Protected Management Frame Enabled;
Any other L2 security method is not allowed, that is, no mixed mode possible.

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220712-configure-and-verify-wi-fi-6e-wlan-layer.html

upvoted 1 times

Question #964 *Topic 1*

Which Cisco SD-WAN component authenticates the routers and the vSmart controllers?

A. vEdge

B. Manage NMS

C. Analytics

D. vBond orchestrator

Correct Answer: *D*

Community vote distribution

D (100%)

Mekai2020 4 days, 2 hours ago

Selected Answer: D

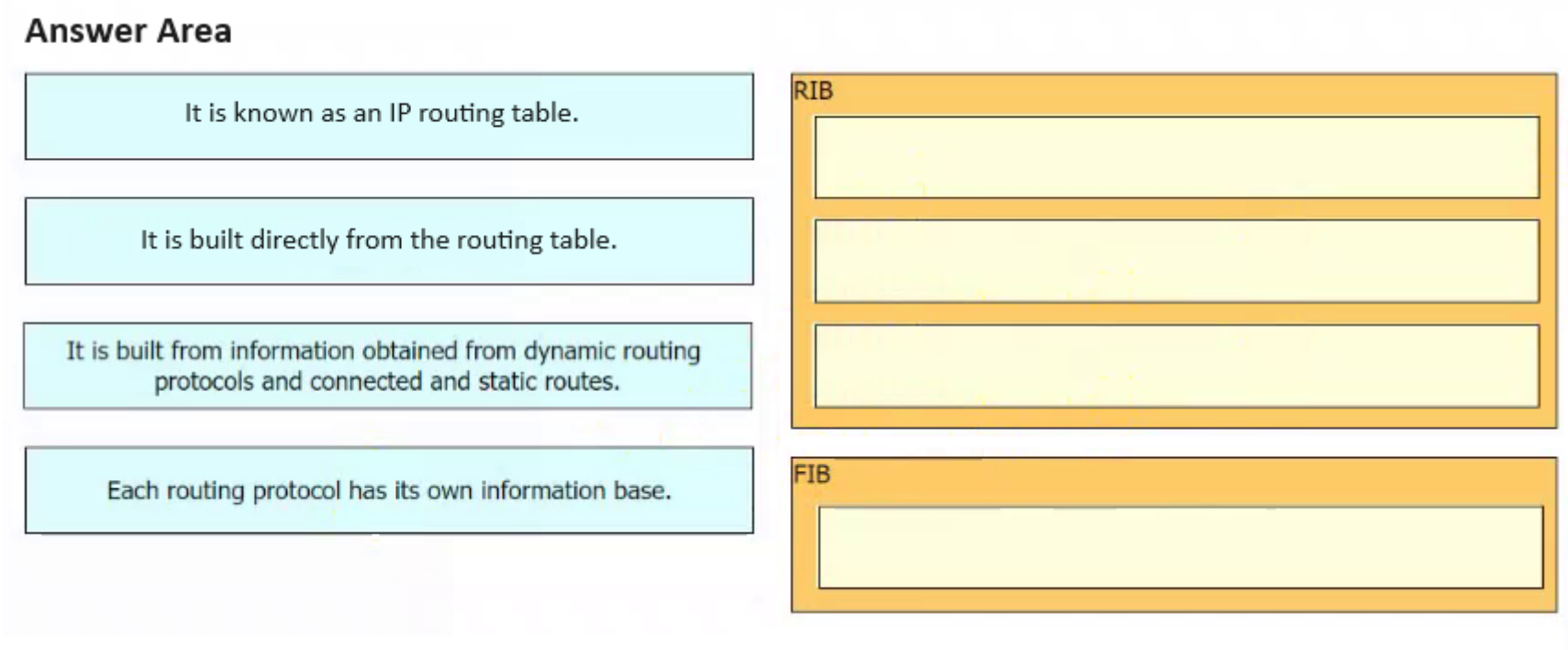
https://study-ccnp.com/cisco-sd-wan-architecture-overview/#:~:text=The%20vBond%20orchestrator%20is%20an,devices%20to%20connect%20to%20it.

upvoted 1 times

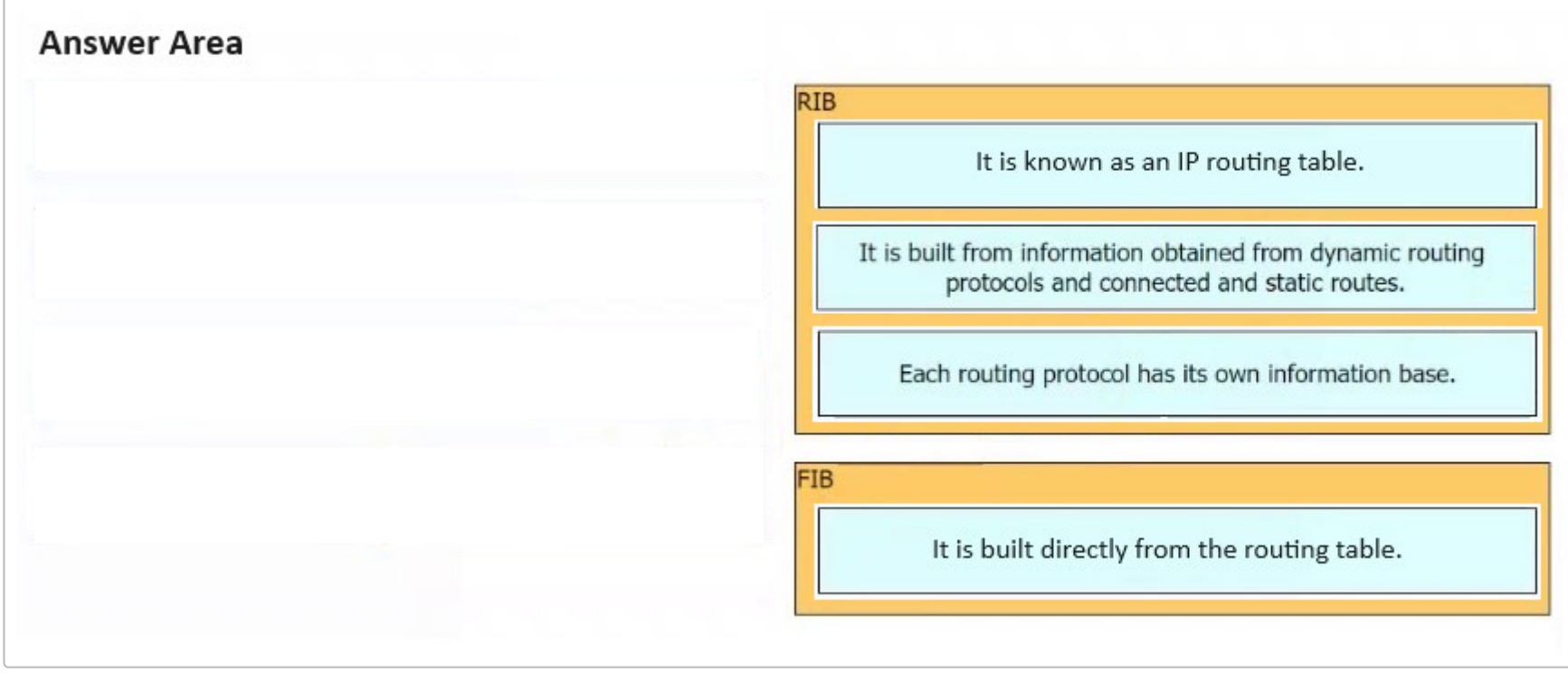
Question #965 *Topic 1*

DRAG DROP
-

Drag and drop the characteristics from the left onto the corresponding switching architectures on the right.



Correct Answer:



Mekai2020 4 days, 2 hours ago

the answer is correct. FIB is derived from RIB

https://learningnetwork.cisco.com/s/question/0D53i00000KssjfCAB/routing-rib-vs-fib

upvoted 1 times

Question #966 *Topic 1*

```
count = 8
while count > 4 :
       print(count)
       count -= 1
```

Refer to the exhibit. What is output by this code?

A. -1 -2 -3 -4

B. 8 7 6 5

C. 4 5 6 7

D. -4 -5 -6 -7

Correct Answer: *B*

Community vote distribution

B (100%)

Mekai2020 4 days, 2 hours ago

Selected Answer: B

while count > 4 : 8 = True
while count > 4 : 7 = True
while count > 4 : 6 = True
while count > 4 : 5 = True
while count > 4 : 4 = False!

upvoted 1 times

Question #967 *Topic 1*

What are two characteristics of a directional antenna? (Choose two.)

A. commonly used to cover large areas

B. low gain

C. provides the most focused and narrow beam-width

D. receive signals equally from all directions

E. high gain

Correct Answer: *CE*

Community vote distribution

CE (100%)

Mekai2020 4 days, 2 hours ago

Selected Answer: CE

directional = Focused + High Gain

https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/product_data_sheet09186a008008883b.html#Typesofantennas

upvoted 1 times

Question #968 *Topic 1*

DRAG DROP

-

Drag and drop the code snippets from the bottom onto the blanks in the script to convert a Python object into a JSON string. Not all options are used.

Answer Area

```
import [          ]

data = {
  "measurement": "freeMemory",
  "maxDataPoints": 30,
  "alert": True,
  "policy": "1.2.1",
  "devices": [{"model": "Cisco 2921 ISR", "ipv4": '10.10.10.1'}]
}
model = data["devices"][0]["model"]

json_string = [          ] (data)

print( [          ] )
```

model	json_string
json.loads	json.dumps
json	

Correct Answer:

Answer Area

```
import [ json ]

data = {
  "measurement": "freeMemory",
  "maxDataPoints": 30,
  "alert": True,
  "policy": "1.2.1",
  "devices": [{"model": "Cisco 2921 ISR", "ipv4": '10.10.10.1'}]
}
model = data["devices"][0]["model"]

json_string = [ json.loads ] (data)

print( [ json_string ] )
```

model
json.dumps

Mekai2020 4 days, 2 hours ago

json
json.dumps
json_string

https://www.w3schools.com/python/gloss_python_convert_into_JSON.asp

upvoted 1 times

Question #969 *Topic 1*

When does Cisco DNA Center make changes to a device?

A. when the device credentials are added

B. when the network device is assigned to the site and device controllability is turned on

C. when the network device is discovered and device controllability is turned on

D. when a NETCONF port has been configured

Correct Answer: *C*

Community vote distribution

B (100%)

Mekai2020 4 days, 2 hours ago

Selected Answer: B

When assigning devices to a site, if Device Controllability is enabled, a workflow is automatically triggered to push the device configuration from the site to the devices.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-2/user_guide/b_cisco_dna_center_ug_2_2_2/b_cisco_dna_center_ug_2_2_2_chapter_011.html

upvoted 2 times

Question #970 *Topic 1*

Which security actions must be implemented to prevent an API injection attack?

A. Log and monitor failed attempts.

B. Use password hash with biometric authentication.

C. Validate, filter, and sanitize all incoming data.

D. Use short-lived access tokens and authenticate the apps.

Correct Answer: *C*

Community vote distribution

C (100%)

Mekai2020 4 days, 3 hours ago

Selected Answer: C

"validate" https://www.computer.org/publications/tech-news/trends/api-injection-attacks-prevention

upvoted 1 times

```
Router#show running-config | section line vty
line vty 0 4
 login local
line vty 5 15
 login local
!
Router#show running-config | include username
username cisco secret 5 $1$cM67$v7NQK0g2BGit77x88U1/00
```

Refer to the exhibit. Which action automatically enables privilege exec mode when logging in via SSH?

A. Configure a password under the line configuration.

B. Configure the enable secret to be the same as the secret for user "Cisco".

C. Configure privilege level 15 under the line configuration.

D. Configure user "cisco" with privilege level 15.

Correct Answer: *D*

Community vote distribution

D (100%)

Mekai2020 4 days, 3 hours ago

Selected Answer: D

https://learningnetwork.cisco.com/s/question/0D53i00000KstA2CAJ/privilege-level-when-username-command-is-configured

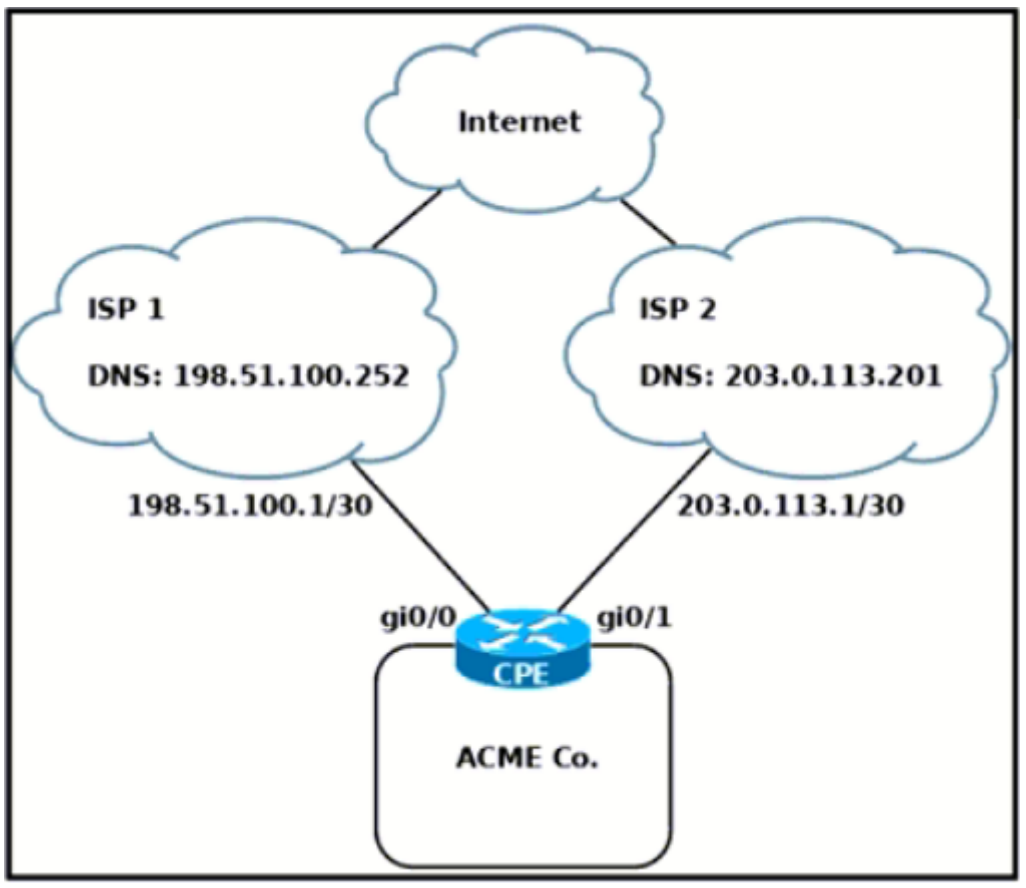
upvoted 1 times

Mekai2020 4 days, 3 hours ago

Selected Answer: D

https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels

upvoted 1 times



Refer to the exhibit. An engineer must verify the operational status of ISP 1 by testing the IP reachability of the ISP1 DNS server every 10 seconds. If the DNS server is not reachable from the CPE through the Gi0/0 interface, then the test should fail. Which two configuration sets must be used to accomplish this task? (Choose two.)

A. ip route 0.0.0.0 0.0.0.0 198.51.100.1
ip route 0.0.0.0 0.0.0.0 203.0.113.1

B. ip route 0.0.0.0 255.255.255.255 198.51.100.1
ip route 0.0.0.0 255.255.255.255 203.0.113.1

C. ip route 198.51.100.252 255.255.255.255 198.51.100.1

D. ip sla 1
icmp-echo 198.51.100.252
frequency 10
ip sla schedule 1 life forever start-time now

E. ip sla 1
dns www.cisco.com name-server 198.51.100.252
frequency 10
ip sla schedule 1 life forever start-time now

Correct Answer: *CD*

Community vote distribution

CD (100%)

Mekai2020 4 days, 3 hours ago

Selected Answer: CD

If the DNS server is not reachable from the CPE through the Gi0/0 interface, then the test should fail. Add static route to direct through Gi0/0 network.

C. ip route 198.51.100.252 255.255.255.255 198.51.100.1

verify the operational status of ISP 1 by testing the IP reachability of the ISP1 DNS server every 10 seconds.

D. ip sla 1
icmp-echo 198.51.100.252
frequency 10
ip sla schedule 1 life forever start-time now

upvoted 1 times

Question #973 *Topic 1*

```
Device# show flow monitor FLOW-CC
Flow Monitor FLOW-CC:
  Description:       User defined
  Flow Record:       CC
  Flow Exporter:     1
                     2
  Cache:
    Type:              normal (Platform cache)
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs
```

Refer to the exhibit. What can be determined from the output?

A. Flow record CC is configured with two separate exporters.

B. Flow record CC is configured with a single exporter.

C. Flow monitor FLOW-CC is configured with two separate flow records to a single exporter.

D. Flow monitor FLOW-CC is configured to two separate exporters.

Correct Answer: *D*

Community vote distribution

D (100%)

Mekai2020 4 days, 3 hours ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/xe-3se/fnf-xe-3e-book/fnf-export-ipv4.html

upvoted 1 times

```
from pythonping import ping
import paramiko
import sys

s= "%s %s" % (sys.argv[1],'')
s1=s.replace(' ','')
ip= s1
t= "%s %s" % (sys.argv[2],'')
r= ping(s1, count=7)
r1= r.success()
if r1 != True:
   exit()
client= paramiko.SSHClient()
client.load_system_host_keys()
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
client.connect(ip, port= 22, username= usr, password= pswd)
stdin, stdout, stderr = client.exec_command(t + '\n')
time.sleep(3)
print(t)
for u in stdout:
   print(u)
client.close()
```

Refer to the exhibit. Which action results from executing the Python script?

A. display the output of a command that is entered on that device

B. display the output of a command that is entered on that device in a single line

C. SSH to the IP address that is manually entered on that device

D. display the unformatted output of a command that is entered on that device

Correct Answer: *A*