Question #1 *Topic 1*

Which two BGP features will result in successful route exchanges between eBGP neighbors sharing the same AS number? (Choose two.)

A. advertise-best-external

B. bestpath as-path ignore

C. client-to-client reflection

D. as-override

E. allow-as-in

**Correct Answer:** *DE*

*Community vote distribution*

DE (100%)

**Heorhiiyatskovskyi** 1 year, 4 months ago

**Selected Answer: DE**

D and E are correct

upvoted 1 times

**XalaGyan** 2 years, 5 months ago

**Selected Answer: DE**

Provided answer is correct

upvoted 1 times

Question #2 *Topic 1*

A customer with an IPv4 only network topology wants to enable IPv6 connectivity while preserving the IPv4 topology services. The customer plans to migrate IPv4 services to the IPv6 topology, then decommission the IPv4 topology. Which topology supports these requirements?

A. dual stack

B. 6VPE

C. 6to4

D. NAT64

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Heorhiiyatskovskyi** 1 year, 4 months ago

**Selected Answer: A**

Who Needs Dual Stack Support?
• Companies that need or want to deploy IPv6 on their
internal network infrastructure

https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/IPV6at_a_glance_c45-625859.pdf

upvoted 1 times

**XalaGyan** 2 years, 5 months ago

**Selected Answer: A**

Provided answer is correct

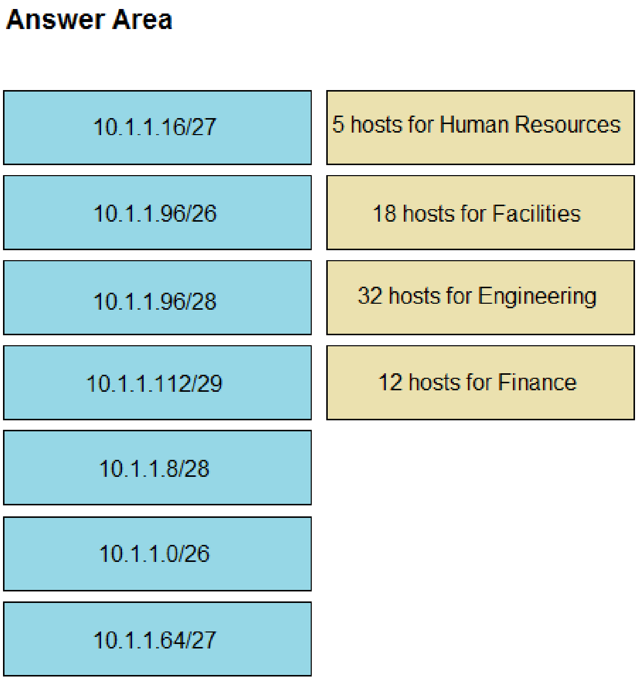
upvoted 2 times

Question #3 *Topic 1*

DRAG DROP -

An engineer is designing an addressing plan for a small business using a single /24 network. Each department must have its own subnet. Drag and drop the subnets from the left onto the requirements of the department they fulfill on the right. Not all options are used.

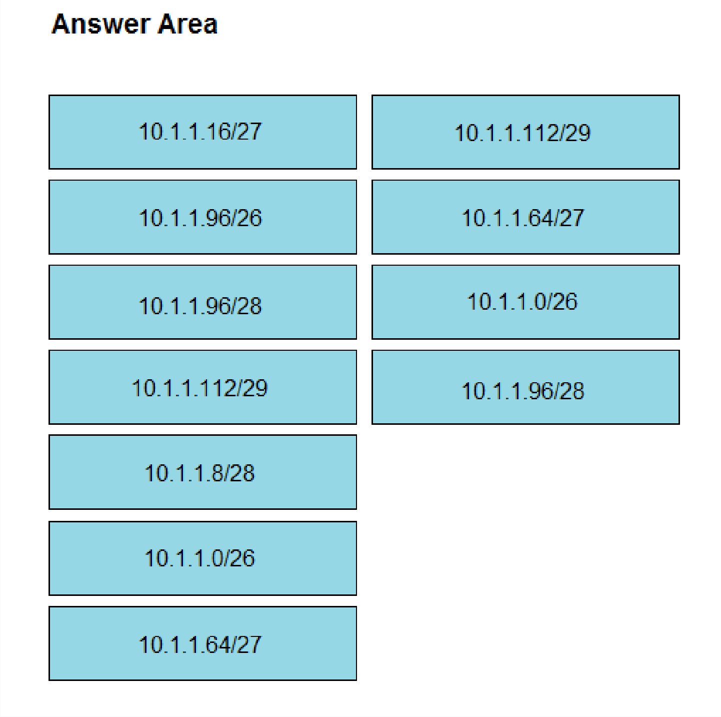
Select and Place:



**Answer Area**

| | |
|---|---|
| 10.1.1.16/27 | 5 hosts for Human Resources |
| 10.1.1.96/26 | 18 hosts for Facilities |
| 10.1.1.96/28 | 32 hosts for Engineering |
| 10.1.1.112/29 | 12 hosts for Finance |
| 10.1.1.8/28 | |
| 10.1.1.0/26 | |
| 10.1.1.64/27 | |

**Correct Answer:**



**Answer Area**

| | |
|---|---|
| 10.1.1.16/27 | 10.1.1.112/29 |
| 10.1.1.96/26 | 10.1.1.64/27 |
| 10.1.1.96/28 | 10.1.1.0/26 |
| 10.1.1.112/29 | 10.1.1.96/28 |
| 10.1.1.8/28 | |
| 10.1.1.0/26 | |
| 10.1.1.64/27 | |

**teems5uk** 1 year, 6 months ago

USABLE ADDRESSES

/24 = 253

/25 = 126

/26 = 62

/27 = 30

/28 = 14

/29 = 6

/30 = 2

upvoted 1 times

**Mebeelen** 2 years, 1 month ago

I used another /27 network. Why use this ones? What are the major issue which I don´t see?

upvoted 1 times

**LSLS55** 1 year, 11 months ago

You should start subnetting bigger to smaller subnets. Using the other possible /27 you end up with overlapping subnets.

upvoted 1 times

**SergeBesse** 2 years, 11 months ago

good answer

upvoted 1 times

Question #4 *Topic 1*

A company is running BGP on a single router, which has two connections to the same ISP. Which BGP feature ensures traffic is load balanced across the two links to the ISP?

A. Multihop

B. Multipath Load Sharing

C. Next-Hop Address Tracking

D. AS-Path Prepending

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**XalaGyan** 1 year, 5 months ago

**Selected Answer: B**

Provided answer is correct

upvoted 2 times

Question #5 *Topic 1*

Company A recently acquired another company. Users of the newly acquired company must be able to access a server that exists on Company A's network, both companies use overlapping IP address ranges. Which action conserves IP address space and provides access to the server?

A. Use a single IP address to create overload NAT

B. Use a single IP address to create a static NAT entry

C. Build one-to-one NAT translation for every user that needs access

D. Re-IP overlapping address space in the acquired company

**Correct Answer:** *A*

*Community vote distribution*

A (67%) B (33%)

⊟ **iLikeHamburgers** Highly Voted 👍 3 years, 5 months ago

A is not correct. You wouldn't create a NAT to convert every single user from the newly acquired company into one IP address in the other existing company. You would create a static NAT for traffic destined to the server at the network boundary between the 2 companies. Traffic destined to the server from the newly acquired company would be NAT'd to the server IP in Company A.

upvoted 5 times

⊟ **Patrick1234** 2 years, 11 months ago

But you wouldn't know if the server sends traffic back towards the right hosts since the source ip's are not translated... I think it's A, because you need to make sure the source ip's are being translated as well. You are only able to do this with option A.

upvoted 3 times

⊟ **NoHombre** Most Recent 🕒 6 months ago

Selected Answer: A

A is correct

upvoted 1 times

⊟ **ciscofan** 6 months, 2 weeks ago

Selected Answer: A

A is correct. First off there is tricky question about to conserve IP address space. NAT overload will map multiple hosts to single IP. Static NAT will map only one IP.

Generally in many resources there is NAT definition like this:
Static NAT - one-to-one
Dynamic NAT - many-to-many
PAT(Overload) - many-to-one

So from my point of view B and C is almost the same. They just confuse you with wording. "Use single IP to create static NAT entry" and "Built one-to-one NAT"(what is also static NAT).
In B you use only single IP so then only one host would be translated.
In C you does not conserve IP addresses as you would have to map all inside host to translated IP pool(outside).

Here some reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/621/fdm/fptd-fdm-config-guide-621/fptd-fdm-nat.html#ID-2090-0000001d

upvoted 1 times

⊟ **Abdhakeem** 9 months, 3 weeks ago

Selected Answer: A

option B do not manage the IP Addresses as it is a static (one-to-one) mapping.

upvoted 1 times

⊟ **wolfone** 1 year ago

Selected Answer: A

If A company client use net A (10.0.0.0/24)
if B company client use net A (10.0.0.0/24)
if server is on net S (172.16.0.0/24)

Client form B must masquerade their source to avoid backward traffic (backward of traffic originated from company B client that reached the servers) goes to Company A.
so A is OK.
upvoted 1 times

**andrewChan** 1 year, 5 months ago

**Selected Answer: A**

this is a tricky question, many users require to access a server
so from source side (clients) point of view, it could be overloading NAT, configuration is simple; or 1 to 1 static NAT for all users also possible.

from destination side (server), it may require a static NAT (simple), or a port forwarding NAT in a overloading NAT setup.

And according to the question, "Which action conserves IP address space and provides access to the server?"
I beleive asking which NAT solution allows client to access to the server so A is correct.
or in another way to understand, overloading NAT is able to use in both side, so A is most possible correct one.
For B, it only corrects in server side, but on client side, need many static NAT entries
upvoted 2 times

**salmarin** 2 years ago

**Selected Answer: B**

one to one for the server
upvoted 1 times

**Clauster** 2 years, 9 months ago

**Selected Answer: A**

Here's why:
B. Use a single IP address to create a static NAT entry: It's not specific enough, create a Single IP Static NAT Entry of what ? it doesn't specify anything or say it's for the server and it needs to be very clear.
C. Build one-to-one NAT translation for every user that needs access: This is not feasible, you are not going to create a Static NAT for every host so this is wrong.
D. Re-IP overlapping address space in the acquired company: When you acquire a company with overlapping networks you want to try to avoid re-IP the entire network initially. The question also states you want to keep the same IP Subnet space which means you want to keep things as it is so a redo of IP Subnets is not an option.

Leaves us with the only correct answer which is A. It can also be found on the OCG Book on page 15
upvoted 3 times

**Nickplayany** 2 years, 10 months ago

Why not D. Re-IP overlapping address space in the acquired company ?
upvoted 2 times

> **nicolamazzoletti** 2 years, 5 months ago
>
> Because it is a requirement to conserve subnets
> upvoted 1 times

**GustavoF** 2 years, 10 months ago

**Selected Answer: A**

A is correct.
upvoted 1 times

**Reinier_veen** 3 years, 4 months ago

I think the big question here is what adresses reside on both global and local site. Is it the address of the server (answer B) or the clients (answer A).
upvoted 2 times

**Eards** 3 years, 4 months ago

**Selected Answer: B**

B seems better option
upvoted 3 times

⊟ **NayTwister** 3 years, 5 months ago

Answer is B.

upvoted 3 times

⊟ **XalaGyan** 3 years, 11 months ago

**Selected Answer: A**

Provided answer is correct

upvoted 2 times

Question #6 *Topic 1*

Which design consideration should be observed when EIGRP is configured on Data Center switches?

A. Perform manual summarization on all Layer 3 interfaces to minimize the size of the routing table.

B. Prevent unnecessary EIGRP neighborships from forming across switch virtual interfaces.

C. Lower EIGRP hello and hold timers to their minimum settings to ensure rapid route reconvergence.

D. Configure multiple EIGRP autonomous systems to segment Data Center services and applications.

**Correct Answer:** *B*

*Community vote distribution*

A (50%) B (50%)

⊟ **Benzzyy** Highly Voted 5 years, 1 month ago

Answer is B

upvoted 11 times

⊟ **CCNPWILL** 4 years, 8 months ago

I agree with B. Besides, A is not specific to the data center. its best practice, in general, to summarize at particular points in the EIGRP hierarchical design. Not all L3 interfaces.

upvoted 3 times

⊟ **Mardouk** Highly Voted 4 years, 8 months ago

Answer is A

reference : ENSLD 300-420 Cert Guide - Chapter 3 "Routing Protocol Characteristics, EIGRP, and IS-IS" - EIGRP in the Data Center

upvoted 11 times

⊟ **chmacnp** Most Recent 5 months ago

Selected Answer: A

A - the keyword 'all' layer 3 interfaces is misleading, but the OCG does give weight to summarising specifically at the datacenter. B is correct, but passive-interfaces are generally used on access facing interfaces more so.

upvoted 1 times

⊟ **NoHombre** 6 months ago

Selected Answer: A

When EIGRP is used in the data center (DC), several design considerations
are important. Because DCs will have many different services, networks, and
applications, you should design for summarizing data center subnets, just as
you would do in wide-area networking.

upvoted 1 times

⊟ **aki3aki3** 6 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 1 times

⊟ **khazbimoas** 9 months, 2 weeks ago

Selected Answer: A

Answer A is correct

upvoted 1 times

⊟ **Seb82** 1 year, 5 months ago

Selected Answer: B

While summarization is important for scalability, it's not specific to EIGRP on data center switches and might not be necessary on "all" Layer 3 interfaces

upvoted 3 times

⊟ **MasiEB** 2 years, 8 months ago

Answer is A 100%
EIGRP in the Data Center
When EIGRP is used in the data center (DC), several design considerations are important.
Because DCs will have many different services, networks, and applications, you should
design for summarizing data center subnets, just as you would do in wide-area networking.
Furthermore, it is a good idea to advertise a default route into the DC from the aggregation
layer. This way, you do not have to advertise all global network routes into the DC.

upvoted 2 times

**Clauster** 2 years, 9 months ago

Selected Answer: A

A is 100% correct.
Chapter 3 Page 114
"EIGRP in the Data Center"
When EIGRP is used in the data center (DC), several design considerations are important. Because DCs will have my different services, networks and applications, you should design for summarizing data center subnets, just as you would do in WAN.

upvoted 5 times

**SpicyMochi** 2 years, 10 months ago

Selected Answer: B

Option B is the correct answer because EIGRP can form neighborships across switch virtual interfaces (SVIs) if the SVIs are configured with IP addresses. In a Data Center environment, where there are typically many SVIs, this can result in unnecessary EIGRP neighborships and potentially impact performance. To prevent this, it is recommended to configure EIGRP to only form neighborships on physical interfaces where necessary, rather than on all SVIs.

Option A, performing manual summarization on all Layer 3 interfaces to minimize the size of the routing table, may be useful in some cases, but it is not a specific design consideration for EIGRP on Data Center switches.

upvoted 4 times

**iLikeHamburgers** 3 years, 5 months ago

A is correct.
reference : ENSLD 300-420 Cert Guide
Chapter 3 "Routing Protocol Characteristics, EIGRP, and IS-IS"
EIGRP in the Data Center page 114
"Because DCs will have many different services, networks, and applications, you should design for summarizing data center subnets..."

upvoted 2 times

**SergeBesse** 3 years, 5 months ago

Selected Answer: A

reference : EIGRP in the Data Center Chapter 3
Because DCs will have many different services, networks, and applications, you should design for summarizing data center subnets, just as you would do in wide-area networking.

upvoted 3 times

**cwoolie** 3 years, 10 months ago

I researched this question I am strongly think answer is A. With answer B I do not think EIGRP will form neighbors on virtual interfaces because it is not possible. Forming neighbors has to be a physical connection not virtual.

upvoted 3 times

**Xavi07** 4 years, 8 months ago

Answer is A. Mardouk it´s right in chapter 3 - part EIGRP in the Data Center

upvoted 3 times

Question #7 Topic 1

Which design consideration must be made when using IPv6 overlay tunnels?

A. Overlay tunnels that connect isolated IPv6 networks are considered a final IPv6 network architecture.

B. Overlay tunnels should only be considered as a transition technique toward a permanent solution.

C. Overlay tunnels should be configured only between border devices and require only the IPv6 protocol stack.

D. Overlay tunneling encapsulates IPv4 packets in IPv6 packets for delivery across an IPv6 infrastructure.

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**kudasay** Highly Voted 4 years, 3 months ago

B is correct - he use of overlay tunnels should be considered as a transition technique toward a network that supports both the IPv4 and IPv6 protocol stacks or just the IPv6 protocol stack.

upvoted 10 times

**skjs** Highly Voted 4 years, 2 months ago

B is correct - Overlay tunnels can be configured between border devices or between a border device and a host; however, both tunnel endpoints must support the IPv4 and IPv6 protocol stacks.

upvoted 7 times

**akbntc** Most Recent 1 year, 6 months ago

Selected Answer: B

B is correcr.

upvoted 1 times

**MasiEB** 1 year, 8 months ago

B is the correct answer

Overlay tunnels reduce the maximum transmission unit (MTU) of an interface by 20 octets (assuming that the basic IPv4 packet header does not contain optional fields). A network that uses overlay tunnels is difficult to troubleshoot. Therefore, overlay tunnels that connect isolated IPv6 networks should not be considered a final IPv6 network architecture. The use of overlay tunnels should be considered as a transition technique toward a network that supports both the IPv4 and IPv6 protocol stacks or just the IPv6 protocol
stack.

upvoted 1 times

**Clauster** 1 year, 9 months ago

Selected Answer: B

A is incorrect

B is correct

C is incorrect: Page 69 OCG Book "IPv6 over Ipv4 Tunneling Strategy" Goes word by word but this answer is incorrect.

D This answer is also incorrect: Page 69 OCG Book "IPv6 over Ipv4 Tunneling Strategy" Goes word by word but this answer is incorrect.

upvoted 1 times

**SpicyMochi** 1 year, 10 months ago

Selected Answer: B

Option B is the correct answer because IPv6 overlay tunnels are typically used as a temporary solution to allow IPv6 connectivity across an IPv4 network. While overlay tunnels can provide IPv6 connectivity in the short term, they are not a long-term solution and can introduce additional complexity and overhead to the network. In general, it is recommended to migrate to a native IPv6 network architecture as soon as possible.

upvoted 1 times

**Heorhiiyatskovskyi** 1 year, 10 months ago

Selected Answer: B

b is correct

upvoted 1 times

**emre076** 2 years, 2 months ago

Selected Answer: B

b is correct

upvoted 1 times

**emre076** 2 years, 2 months ago

Selected Answer: B

b is correct

upvoted 1 times

**emre076** 2 years, 4 months ago

Selected Answer: B

b is correct

upvoted 2 times

**iLikeHamburgers** 2 years, 5 months ago

B is correct.

C is almost correct, however the part about "and require only the IPv6 protocol stack." is wrong. In the NSLD 300-420 Cert Guide - Chapter 2 "Internet Protocol Version 6 (IPv6) Design" - IPv6 over IPv4 Tunneling Strategy, page 69, it states "Overlay tunnels can be configured between border devices or between a border device and a host; however, both tunnel endpoints must support the IPv4 and IPv6 protocol stacks."

upvoted 1 times

**Hope66** 2 years, 10 months ago

B is correct, C is wrong. C state that "border devices and require only the IPv6 protocol stack"

while border devices and require IPV4 and IPv6 protocol stack.

upvoted 2 times

**cwoolie** 2 years, 11 months ago

Answer is B

upvoted 1 times

**cwoolie** 2 years, 11 months ago

Answer is B

upvoted 1 times

**roganjosh** 3 years ago

Selected Answer: B

B Is Correct

upvoted 1 times

**Xavi07** 3 years, 7 months ago

B is the correct

upvoted 2 times

**Mardouk** 3 years, 8 months ago

Answer is B

Reference : ENSLD 300-420 Cert Guide - Chapter 2 "Internet Protocol Version 6 (IPv6) Design" - IPv6 over IPv4 Tunneling Strategy

upvoted 4 times

Question #8 *Topic 1*

When a network is designed using IS-IS, which two circuit types are supported? (Choose two.)

A. nonbroadcast multiaccess

B. multiaccess

C. point-to-multipoint

D. nonbroadcast

E. point-to-point

**Correct Answer:** *BE*

**iLikeHamburgers** 1 year, 5 months ago

B, E are correct.
In the 300-420 Cert Guide - Chapter 3 "Routing Protocol Characteristics, EIGRP, and IS-IS" - "IS-IS Interface Types" on page 117 it states:
"IS-IS only has two network types (or interface types): point-to-point and broadcast."

upvoted 3 times

**Audie** 2 years ago

Band E are correct: "In Intermediate System-to-Intermediate System (IS-IS) Protocol, there are two types of networks: point-to-point and broadcast. Unlike Open Shortest Path First (OSPF) Protocol, IS-IS does not have other network types like non-broadcast and point-to-multipoint."

upvoted 2 times

Question #9 *Topic 1*

A network solution is being designed for a company that connects to multiple Internet service providers. Which Cisco proprietary BGP path attribute will influence outbound traffic flow?

A. Local Preference

B. MED

C. Weight

D. AS Path

E. Community

**Correct Answer:** *C*

**Benzzyy** Highly Voted 👍 3 years, 1 month ago

Weight is Cisco proprietary and is the first decision of all path attributes to influence outbound traffic on a singular router. Weight is non-transitive and will only influence routes as they leave that device.

upvoted 6 times

**iLikeHamburgers** Most Recent 🕒 1 year, 5 months ago

C is correct

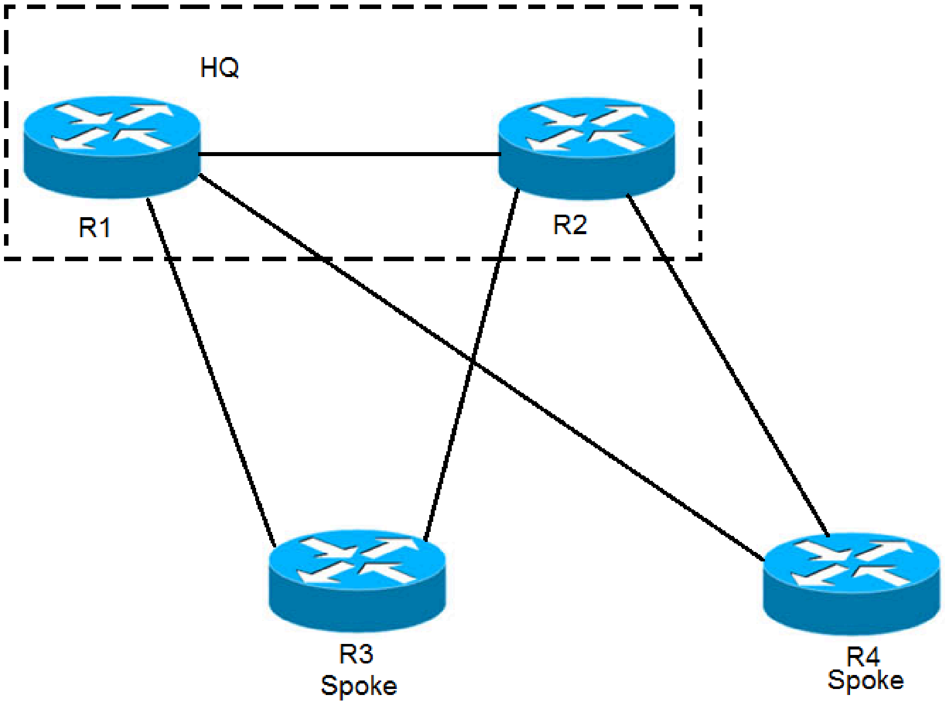
300-420 Cert Guide - Chapter 4 "OSPF, BGP, and Route Manipulation" - "Weight Attribute"

"Weight is assigned locally on a router to specify a preferred path if multiple paths exist out of a router for a destination. "

"Weight is specific to Cisco routers..."

upvoted 3 times

Question #10 *Topic 1*



Refer to the exhibit. EIGRP has been configured on all links. The spoke nodes have been configured as EIGRP stubs, and the WAN links to R3 have higher bandwidth and lower delay than the WAN links to R4. When a link failure occurs at the R1-R2 link, what happens to traffic on R1 that is destined for a subnet attached to R2?

A. R1 has no route to R2 and drops the traffic

B. R1 load-balances across the paths through R3 and R4 to reach R2

C. R1 forwards the traffic to R3, but R3 drops the traffic

D. R1 forwards the traffic to R3 in order to reach R2

**Correct Answer:** *A*

*Community vote distribution*

A (94%) 6%

⊟ **Mardouk** Highly Voted 4 years, 3 months ago

should be A. R1 has no route to R2 and drops the traffic

Stub router only advertise Connected and Summary - it will not re-advertise route

upvoted 16 times

⊟ **cerifyme85** 1 year, 11 months ago

it depends on the type of stub configured.. if they are cofigured as connected + summary, they will advertise connected route R2, but not subnets connected to it. So it will still forward traffic to R3 -> R2, but not to R2's subnet.. very confusing question.. could be A or D

upvoted 1 times

⊟ **Clauster** Most Recent 1 year, 8 months ago

Selected Answer: A

I've studied this topic in depth.

The correct answer is A

By default when you setup an EIGRP Router as a STUB it will advertise connected routers and summary routes only as a default behavior, however, it will NEVER advertise learned EIGRP routes learned from neighbors, in this case Hub 2 it's the destination.

The question answer will be found at the end of the question itself where it says What happens when R1 is trying to send a packet to a SUBNET attached to R2, this is not gonna happen because the Stub Router only advertise directly connected and summary routes to the Hub. By the way, R1 (Hub) won't even bother sending queries to R3 stub router either which also makes this answer correct. This answer can be found on the OCG Book Page 147 & 148, if you take time reading it you'll find it. This feature is cool but be careful and read it carefully.

upvoted 4 times

**LSLS55** 1 year, 5 months ago

Correct. And you mean page 147 and 148 of the OCG PDF file, but its page 111 and 112. Thanks for the info.

upvoted 1 times

**LSLS55** 1 year, 5 months ago

Like you said: "When the stub routing feature is enabled on the spoke router, the router only advertises specified routes to the hub router. The router does not advertise routes received from other EIGRP neighbors to the hub router. The only disadvantage is that the stub router cannot be used as a backup path between two hub sites." - p.111 OCG book

upvoted 1 times

**minon_bob** 1 year, 8 months ago

Selected Answer: A

Mocked up the scenario in the lab, A is correct.

upvoted 2 times

**CKL_SG** 1 year, 9 months ago

Selected Answer: A

The EIGRP stub routing feature can prevent this problem by preventing the remote device from advertising core routes back to the distribution devices. In the above example, routes learned by the remote device from distribution router 1 will not be advertised to distribution router 2. Therefore, distribution router 2 will not use the remote device as a transit for traffic destined to the network core

upvoted 2 times

**cerifyme85** 1 year, 10 months ago

Selected Answer: D

Just labbed this .. if on default - connected summary it installs the directly connected route on R1s table for R3. The only time it removes the next-hop R3 is you use the strcitest stub command which "receive-only" but the question does not say if one should use receive only on c+S

upvoted 1 times

**cerifyme85** 1 year, 10 months ago

Sorry guys "subnet connected to R2".. this will not work at all.

But the question options did not say .. Answer A says " R1 has no routes to R2" on stub C+ S it surely does. So A is still technically not correct and D is not either..Maybe this is a free question from cisco.. makes no sense

upvoted 1 times

**Papins** 2 years, 3 months ago

A is correct, but the question is how to reach R2. We already know that it will be drop base on the scenario presented that means the next step is to forward it to R3 to reach R2. ill go with D.

upvoted 2 times

**iLikeHamburgers** 2 years, 5 months ago

A is correct

300-420 Cert Guide - Chapter 3 "Routing Protocol Characteristics, EIGRP, and IS-IS" page 111

EIGRP Design > EIGRP Stub Routers

"When the stub routing feature is enabled on the spoke router, the router only advertises specified routes to the hub router. The router does not advertise routes received from other EIGRP neighbors to the hub router. The only disadvantage is that the stub router cannot be used as a backup path between two hub sites."

Being that the link between R1 and R2 has failed, the only routes that R1 will now know about are from R3. But remember, R3 will not advertise routes that it has learned from other routers (R2). So R1 will not know any routes from R2.

upvoted 3 times

**Bigmikemalta** 2 years, 11 months ago

Selected Answer: A

Stub routers cannot act as transit

upvoted 4 times

**Nonono** 3 years ago

Selected Answer: A

Stub mode does not transit

upvoted 2 times

**andre_b** 3 years, 1 month ago

I agree. A is correct. Stub routers can't be used as a backup path between two hub sites.

upvoted 1 times

⊟ **Alex147** 3 years, 1 month ago

**Selected Answer: A**

Spoke are configured in stub mode, the correct answer is A.

upvoted 3 times

⊟ **Hope66** 3 years, 1 month ago

A is correct. I've done a lab with GNS3 and it works confirming the answer A

upvoted 2 times

⊟ **cerifyme85** 1 year, 10 months ago

Just labbed this .. if on default - connected summary it installs the directly connected route on R1s table for R3.. did you run a traceroute? answer is D

upvoted 1 times

⊟ **Xavi07** 3 years, 8 months ago

Mardouk is right. EIGRP Stub Routers cannot be used as a backup path between two hub sites.

Chapter 3 - EIGRP Stub Routers

upvoted 1 times

⊟ **Benzzyy** 4 years, 1 month ago

A is correct. Once the link between R1 and R2 is lost, R2 will send out EIGRP queries ONLY to neighbors that do not advertise a STUB flag. R3 and R4 are both advertising the Stub flags, therefore R2 never queries R3 or R4 for a route to R1.

R2 looses the route to R1 - Answer is Def A

upvoted 2 times

⊟ **luisjuradoledesma** 4 years, 1 month ago

The correct answer is A

• The EIGRP stub routing feature will prevent the remote device from advertising core routes back to the distribution devices. Routes learned by the remote device from Distribution 1 will not be advertised to Distribution 2. Therefore, Distribution 2 will not use the remote device as a transit for traffic destined to the network core

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-mt/ire-15-mt-book/ire-eigrp-stub-rtg.html

upvoted 2 times

⊟ **jn4voip** 4 years, 2 months ago

I agree. Stub areas cannot be transit areas

upvoted 2 times

⊟ **escrotoman** 4 years, 3 months ago

Mardouk is right

upvoted 2 times

Question #11 *Topic 1*

A company is using OSPF between its HQ location and a branch office. HQ is assigned area 0 and the branch office is assigned area 1. The company purchases a second branch office, but due to circuit delays to HQ, it decides to connect the new branch office to the existing branch office as a temporary measure. The new branch office is assigned to area 2. Which OSPF configuration enables all three locations to exchange routes?

A. The existing branch office must be configured as a stub area

B. A virtual link must be configured between the new branch office and HQ

C. A sham link must be configured between the new branch office and HQ

D. The new branch office must be configured as a stub area

**Correct Answer:** *B*

**Benzzyy** Highly Voted 2 years, 1 month ago

Area 0 must connect to all other areas. When the network design goes against that practice we have to use virtual links to configure the connecting area as a transit area.

Answer is B

upvoted 8 times

**CCNPWILL** 1 year, 8 months ago

Agreed

upvoted 3 times

Question #12 *Topic 1*

Which method will filter routes between EIGRP neighbors within the same autonomous system?

A. distribute-list

B. policy-based routing

C. leak-map

D. route tagging

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**ghaith_gld** 1 year, 7 months ago

**Selected Answer: A**

correct

upvoted 1 times

**XalaGyan** 2 years, 5 months ago

**Selected Answer: A**

Provided answer is correct

upvoted 1 times

Question #13 *Topic 1*

What are two valid scaling techniques when an EIGRP network is designed that consists of more than 1000 routers? (Choose two.)

A. Use structured hierarchical topology with route summarization

B. Used sub-second timers

C. Use the distribute-list command to filter routes

D. Modify delay parameters on the links

E. Implement multiple EIGRP autonomous systems

**Correct Answer:** *AE*

*Community vote distribution*

AE (86%) 14%

**dougj** 4 months, 3 weeks ago

**Selected Answer: AB**

Using multiple AS systems is not recommended for large networks. A is correct and using sub second timers is also an option that will help, so answer is A and B

upvoted 1 times

**dougj** 4 months, 3 weeks ago

on reading further i also found using multiple AS systems can be justified in some cases and one of those is "Having an organization with an extremely large network " so answer is probably AE

upvoted 1 times

**Sancho502** 1 year, 6 months ago

**Selected Answer: AE**

OCG pg 111

upvoted 4 times

**rickyarchi** 2 years ago

**Selected Answer: AC**

Adding ASs to EIGRP does not improves scalability

upvoted 1 times

**akbntc** 2 years, 6 months ago

**Selected Answer: AE**

A and E are correct answers.

upvoted 1 times

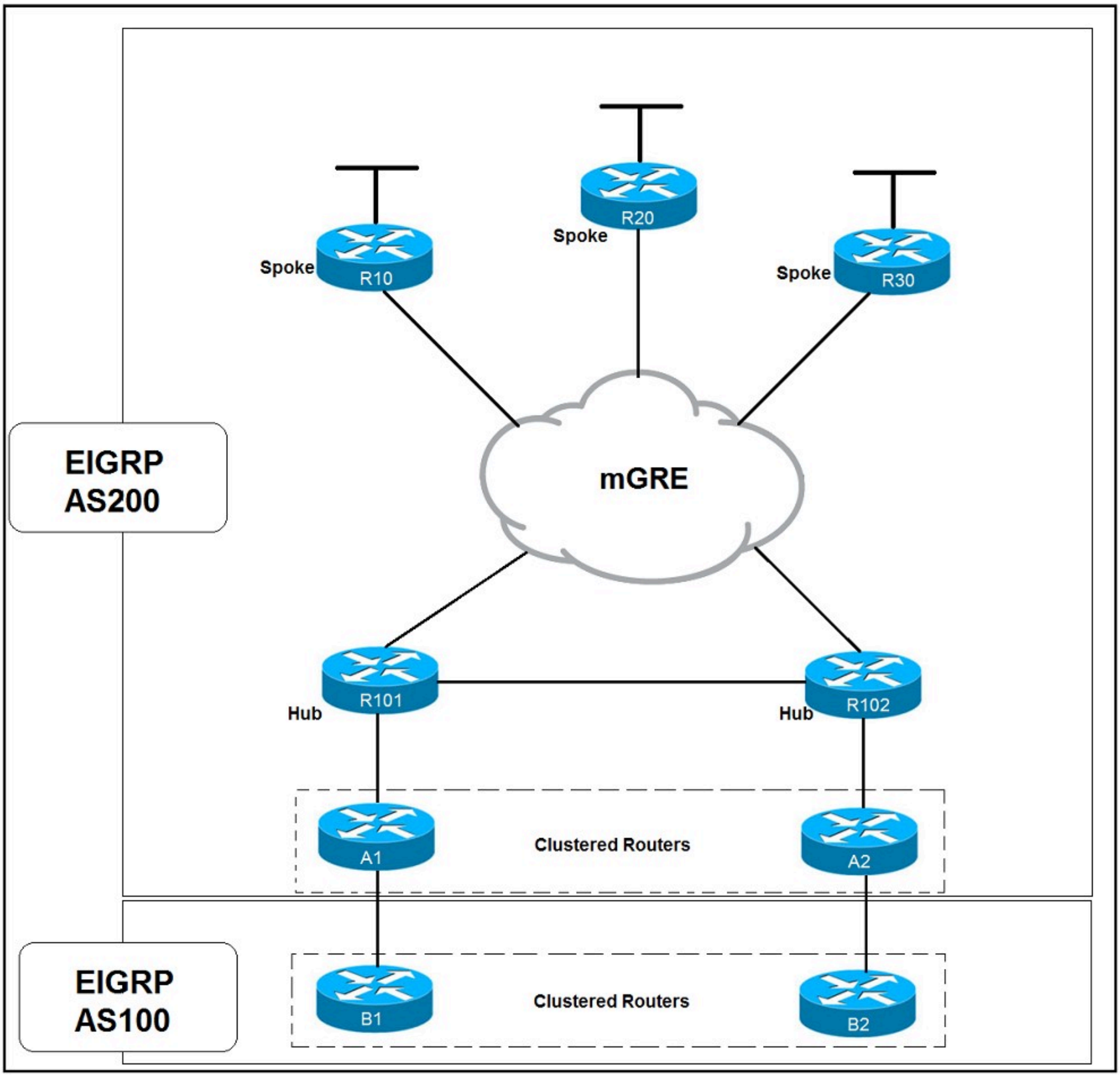
**XalaGyan** 3 years, 11 months ago

**Selected Answer: AE**

Provided answer is correct

upvoted 2 times

Question #14 Topic 1



Refer to the exhibit. Which solution decreases the EIGRP convergence time?

A. Enable subsecond timers

B. Increase the hold time value

C. Increase the dead timer value

D. Enable stub routing on the spokes

**Correct Answer:** *D*

*Community vote distribution*

A (100%)

aymeric Highly Voted 4 years ago

I disagree with Benzzyy.

I think response D is correct :

Query storms are eliminated, which saves bandwidth and CPU and allows the network to converge more quickly.

https://www.cisco.com/en/US/technologies/tk648/tk365/technologies_white_paper0900aecd8023df6f.html

upvoted 11 times

**Mardouk** Highly Voted 3 years, 8 months ago

Answer is D

Reference : ENSLD 300-420 Cert Guide - Chapter 3 "Routing Protocol Characteristics, EIGRP, and IS-IS" - EIGRP Stub

upvoted 6 times

**NoHombre** Most Recent 6 months ago

Selected Answer: D

D is correct

upvoted 1 times

**Niles_edu** 8 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

**lucky12321** 1 year ago

Selected Answer: A

I am thinking as here is asked for convergence time specifically that its answer A. Think about it, if we configure the spokes as stubs we might reduce the queries, take load off of the router and also increase stability but the convergence time would still be minimum 15 seconds (3xhello, 5sec default). So as resources and stability seems to be no problem here, I would go with reducing the timers.

upvoted 1 times

**atiWok** 1 year, 11 months ago

correct, quarries are not forwarded to stubs

upvoted 1 times

**cwoolie** 2 years, 11 months ago

D is correct

upvoted 1 times

**cwoolie** 2 years, 11 months ago

D Is correct...

upvoted 1 times

**XalaGyan** 2 years, 11 months ago

A. Enable subsecond timers => cool idea hold on to it and give it a value of 1 second for example

B. Increase the hold time value ==> the longer you hold the later you notice a downtime, bad idea

C. Increase the dead timer value ==> same as with B)

D. Enable stub routing on the spoke ==> not bad idea. Now assume you dont tweak anything, but the mere fact that STUBS are oneway advertisement roads saves on messages going back and forth no matter in what interval.

so imho i strongly believe D fits convergence time minimization purposes 100% while A) fits for some architectures and others not really so 99.9999% correct answer

Answer: D

upvoted 2 times

**Benzzyy** 4 years, 1 month ago

Answer is B.

Hold-Timer is the amount of time that passes till a route is deemed dead. If you increase the hold time, your delaying the amount of time it takes for that router to send out EIGRP queries to neighboring routers and determine if a new successor exists.

upvoted 1 times

**LSLS55** 1 year, 5 months ago

Your logic is correct, but what is asked is the opposite. By increasing the timers, you are increasing convergence time.

upvoted 1 times

Question #15 *Topic 1*

A router running ISIS is showing high CPU and bandwidth utilization. An engineer discovers that the router is configured as L1/L2 and has L1 and L2 neighbors.
Which step optimizes the design to address the issue?

A. Make this router a DIS for each of the interfaces

B. Disable the default behavior of advertising the default route on the L1/L2 router

C. Configure the router to be either L1 or L2

D. Configure each interface as either L1 or L2 circuit type

**Correct Answer:** *D*

*Community vote distribution*

D (86%) 14%

⊟ **MaryGalanP** Highly Voted 4 years, 4 months ago

You have an IS-IS router that is performing both L1 and L2 routing and has both L1 and L2 neighbors. How would you optimize the router's operation to conserve bandwidth and router resources?

Configure each interface as either L1 or L2 circuit type, depending on the type of adjacency needed out that interface. The command to do this is, at the interface configuration mode, isis circuit-type [level-1 | level-1-2 | level-2-only]. This prevents unnecessary hellos from being sent out interfaces, which uses bandwidth and router resources.

https://www.ciscopress.com/articles/article.asp?p=101756

upvoted 11 times

⊟ **Seb82** Most Recent 1 year, 4 months ago

Selected Answer: D

"the router is configured as L1/L2 and has L1 and L2 neighbors" - the router has to stay L1/L2 but the circuit-type can be set on each interface based on the type of neighbor (L1 or L2 router), and that will decrease the load. If we change the router type to either L1 or L2, some neighborship will be lost, depending on the option chosen.

upvoted 1 times

⊟ **Clauster** 2 years, 9 months ago

Selected Answer: D

I was finally able to find the answer
We all know that answers A and B make no sense.
C: This answer is incorrect, it states that the router is L1/L2 and it's got L1 Neighbor and an L2 Neighbor, If you set the router to L1 it will make an adjacency with L1 but not L2, L1 Routers will become adjacent with L1 and L1/L2s but not with L2s only:
https://www.cisco.com/c/en/us/support/docs/ip/integrated-intermediate-system-to-intermediate-system-is-is/200293-IS-IS-Adjacency-and-Area-Types.html

The Answer is D: You can configure an interface as L1 or L2, this will reduce the amount of Hellos it's sent therefor improves performance.

upvoted 2 times

⊟ **iLikeHamburgers** 3 years, 3 months ago

Selected Answer: D

I feel the answer is D.
Answer C would actually be the best answer, because running 2 databases would consume the most resources. However this is making the assumption that we have the option of changing this particular router to a Level 1, or Level 2. The question doesn't state that this is an option. If the question stated, "What is the best possible way to cut down on router resources.." and left it at that, I would be inclined to say C is the answer. However since it doesn't, and we have to work with that we have (A router running both L1/L2), answer D is the best choice given the circumstances. In a real world scenario, we would apply option D. If that didn't fix the issue we would resort to option C.

upvoted 2 times

⊟ **andrewChan** 3 years, 4 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios/iproute_isis/command/reference/irs_book/irs_is1.html

"You have an IS-IS router that is performing both L1 and L2 routing and has both L1 and L2 neighbors. How would you optimize the router's operation to conserve bandwidth and router resources?

Configure each interface as either L1 or L2 circuit type, depending on the type of adjacency needed out that interface. The command to do this is, at the interface configuration mode, isis circuit-type [level-1 | level-1-2 | level-2-only]. This prevents unnecessary hellos from being sent out interfaces, which uses bandwidth and router resources."

upvoted 2 times

⊟ **dranzer6** 3 years, 4 months ago

Selected Answer: C

You configure the router as Level 1, Level 2 or Level 1/2. Not the interface.

upvoted 1 times

⊟ **cwoolie** 3 years, 11 months ago

D is correct

upvoted 1 times

⊟ **cyclops1** 4 years, 4 months ago

To solve the acknowledgment problem and to reduce the size of the link-state database, we use a special mechanism. When IS-IS routers become neighbors, they also do an election to decide who becomes the DIS (Designated IS).

upvoted 1 times

⊟ **ImAlwaysRight** 4 years, 4 months ago

One of the few questions for this exam which I can't find the answer. Neither of the answers make sense for me.

upvoted 1 times

Question #16 *Topic 1*

Which two routing protocols allow for unequal cost load balancing? (Choose two.)

A. EIGRP

B. IS-IS

C. BGP

D. OSPF

E. RIPng

**Correct Answer:** *AC*

*Community vote distribution*

AC (67%) AD (33%)

**Askhat** 1 year, 2 months ago

**Selected Answer: AC**

A,C is correct

upvoted 2 times

**Papins** 1 year, 4 months ago

unequal-cost load balancing on Cisco routers are IGRP, EIGRP and BGP.

upvoted 2 times

**Buffering** 1 year, 5 months ago

**Selected Answer: AD**

OSPF supports UCMP - https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/710x/routing/configuration/guide/b-routing-cg-asr9000-710x/implementing-ospf.html#concept_1C8B0FDD4C01402794D3972072C0F6CB

upvoted 1 times

**Lungful** 2 years ago

Is Unequal Cost Multipath (UCMP) different than unequal cost load balancing? Is there a chance IS-IS could be one of the answers?

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-17/segrt-xe-17-book/m_isis_ucmp.pdf

upvoted 4 times

**cwoolie** 3 years, 5 months ago

A,C is correct

upvoted 1 times

Question #17 *Topic 1*

Which two steps can be taken to improve convergence in an OSPF network? (Choose two.)

A. Use Bidirectional Forwarding Detection

B. Merge all the areas into one backbone area

C. Tune OSPF parameters

D. Make all non-backbone areas stub areas

E. Span the same IP network across multiple areas.

**Correct Answer:** *AC*

*Community vote distribution*

AC (75%) CD (25%)

**aai5548** Highly Voted 4 years, 1 month ago

A and c.

upvoted 13 times

**Mardouk** Highly Voted 4 years, 3 months ago

not d. - should be a.use BFD

upvoted 9 times

**VasiliyF** Most Recent 2 months, 1 week ago

Selected Answer: AD

thinking about it, A and D could be correct answers

upvoted 1 times

**dougj** 4 months, 3 weeks ago

Selected Answer: AD

thinking about it, A and D could be correct answers too as A,C and D are all used to reduce convergence

upvoted 1 times

**dougj** 4 months, 3 weeks ago

Selected Answer: CD

Tune OSPF timers and use STUB areas is the recommended method

upvoted 1 times

**Clauster** 1 year, 7 months ago

Selected Answer: AC

A and C are the most effective way to improve convergence on an OSPF Network.

upvoted 2 times

**after_eight** 1 year, 9 months ago

Selected Answer: CD

A seems wrong since it improves convergence time only if the physical layer is not able to detect the failure. Suppose you have direct fibers in your network, you do not need BFD.

Tuning OSPF for fast convergence is necessary, because the default timers are very conservative, thus C is correct

Changing the non backbone areas type to stub will decrease the number of routes inside the areas, therefore decrease convergence time and D is correct.

upvoted 3 times

**iLikeHamburgers** 2 years, 5 months ago

Selected Answer: AC

A, C

First let's define convergence: Network convergence is the time that is needed for the network to respond to events.

One of the significant factors in routing convergence is the detection of link or node failure (events). This is where BFD comes in to play.

OSPF Timers

"The default OSPF LSA propagation timers are quite conservative. Lowering the values of the timers that control OSPF LSA generation can significantly improve OSPF convergence times"

https://www.ciscopress.com/articles/article.asp?p=1763921&seqNum=6

upvoted 1 times

**brzl** 2 years, 10 months ago

**Selected Answer: AC**

There are only 2 sub-topic for fast convergence: ospf timers and BFD. see following article at the end:

https://www.ciscopress.com/articles/article.asp?p=1763921&seqNum=6

upvoted 1 times

**cwoolie** 2 years, 11 months ago

A and C

upvoted 2 times

**cwoolie** 2 years, 11 months ago

A and C

upvoted 2 times

**Nonono** 3 years ago

**Selected Answer: AC**

A and C

upvoted 3 times

**Xavi07** 3 years, 7 months ago

Yes, A and C

upvoted 1 times

**luisjuradoledesma** 4 years, 1 month ago

Yes, I believe this answer should be A&C

upvoted 1 times

Question #18 *Topic 1*

Which OSPF area blocks LSA Type 3, 4 and 5, but allows a default summary route?

A. normal

B. stub

C. NSSA

D. totally stubby

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**vangio** 1 year, 7 months ago

CORRECT IS D

upvoted 1 times

**atiWok** 1 year, 11 months ago

**Selected Answer: D**

correct

upvoted 1 times

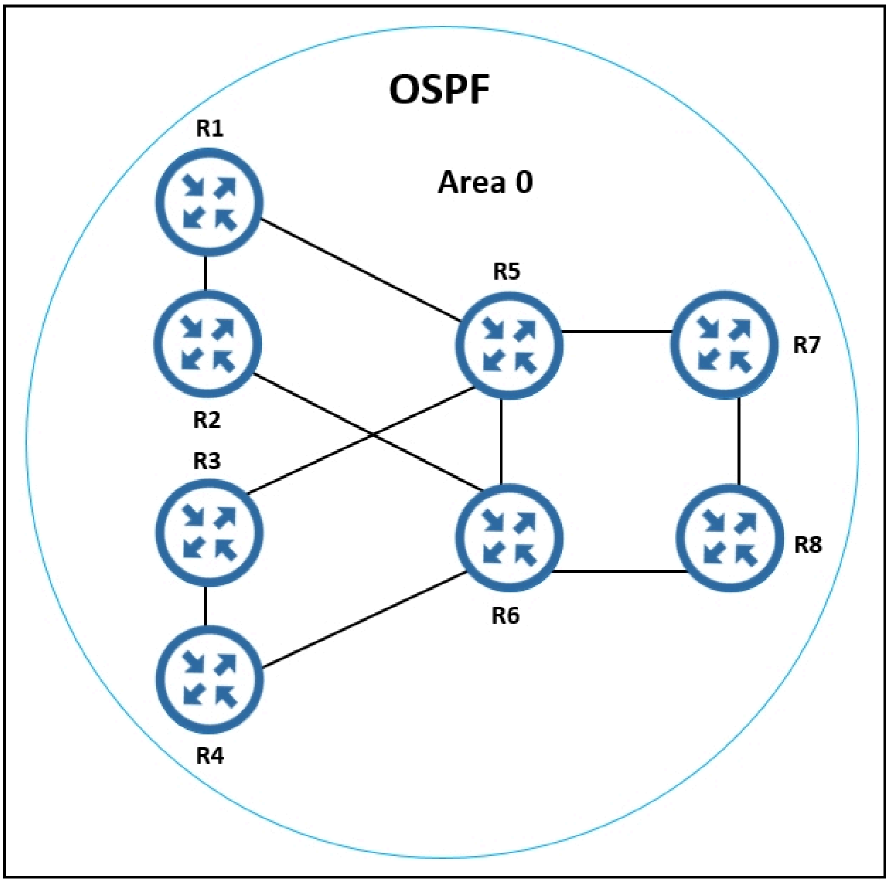
**XalaGyan** 2 years, 11 months ago

**Selected Answer: D**

Provided answer is correct

upvoted 1 times

Question #19 *Topic 1*



Refer to the exhibit. All routers currently reside in OSPF area 0. The network manager recently used R1 and R2 as aggregation routers for remote branch locations and R3 and R4 as aggregation routers for remote office locations. The network has since been suffering from outages, which are causing frequent SPF runs. To enhance stability and introduce areas to the OSPF network with the minimal number of ABRs possible, which two solutions should the network manager recommend? (Choose two.)

A. a new OSPF area for R1 and R2 connections, with R1 and R2 as ABRs

B. a new OSPF area for R3 and R4 connections, with R5 and R6 as ABRs

C. a new OSPF area for R3 and R4 connections, with R3 and R4 as ABRs

D. a new OSPF area for R1, R2, R3, and R4 connections, with R1, R2, R3, and R4 as ABRs

E. a new OSPF area for R1 and R2 connections, with R5 and R6 as ABRs

**Correct Answer:** *BE*

*Community vote distribution*

BE (100%)

**cwoolie** 1 year, 5 months ago

B,E is correct

upvoted 1 times

**XalaGyan** 1 year, 5 months ago

Selected Answer: BE

Provided answer is correct

upvoted 1 times

**kkks009** 1 year, 6 months ago

I think it is because we need to keep number of routers in backbone as small as possible.

upvoted 3 times

**cryptonite** 1 year, 6 months ago

Why not A and C?

upvoted 1 times

⊟ **bogd** 1 year, 6 months ago

The requirements state "minimum number of ABRs"

upvoted 2 times

Question #20 *Topic 1*

An engineer must design a solution to provide backup connectivity between two sites. The engineer plans to use an Internet connection, but company policy requires the connection to be encrypted. Additionally, there are several applications that utilize multicast to deliver video streams between the sites. Which technology should the design include?

A. GRE over IPsec

B. IPsec direct encapsulation

C. GETVPN

D. DMVPN

**Correct Answer:** *A*

*Community vote distribution*

A (83%) D (17%)

**Beehurls** 1 year, 1 month ago

**Selected Answer: A**

I would say GETVPN is the ideal choice because of the multicast video, but the only thing holding me back is that this is a backup connection. So the cost and complexity may be too high for something rarely used. GRE over IPSEC has more overhead, but will be simple to setup and manage.

upvoted 1 times

**uzu13** 1 year, 8 months ago

**Selected Answer: A**

DMVPN is useful when where are many remote sites. For site to site connection, GETVPN is the reasonable solution.

upvoted 1 times

**python_tamer** 1 year, 9 months ago

**Selected Answer: A**

A - GRE over IPsec. There is no need for GETVPN or DMVPN as there are only 2 sites and question does not say there will be more. Keep it simple.

upvoted 3 times

**cwoolie** 1 year, 11 months ago

Answer is A. GRE over IPSEC is encrypted..

upvoted 2 times

**cwoolie** 1 year, 11 months ago

Answer A

upvoted 2 times

**XalaGyan** 1 year, 11 months ago

**Selected Answer: D**

According to this website i recommend DMVPN

https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/IntegNet_Feb17_915_Lynn.pdf

Dynamic Multipoint VPN (DMVPN)
Major F eatures
 Configuration reduction and no-touch deployment
 I P unicast, I P multicast and dynamic routing protocol s
 Spokes with dynamical l y assigned addresses

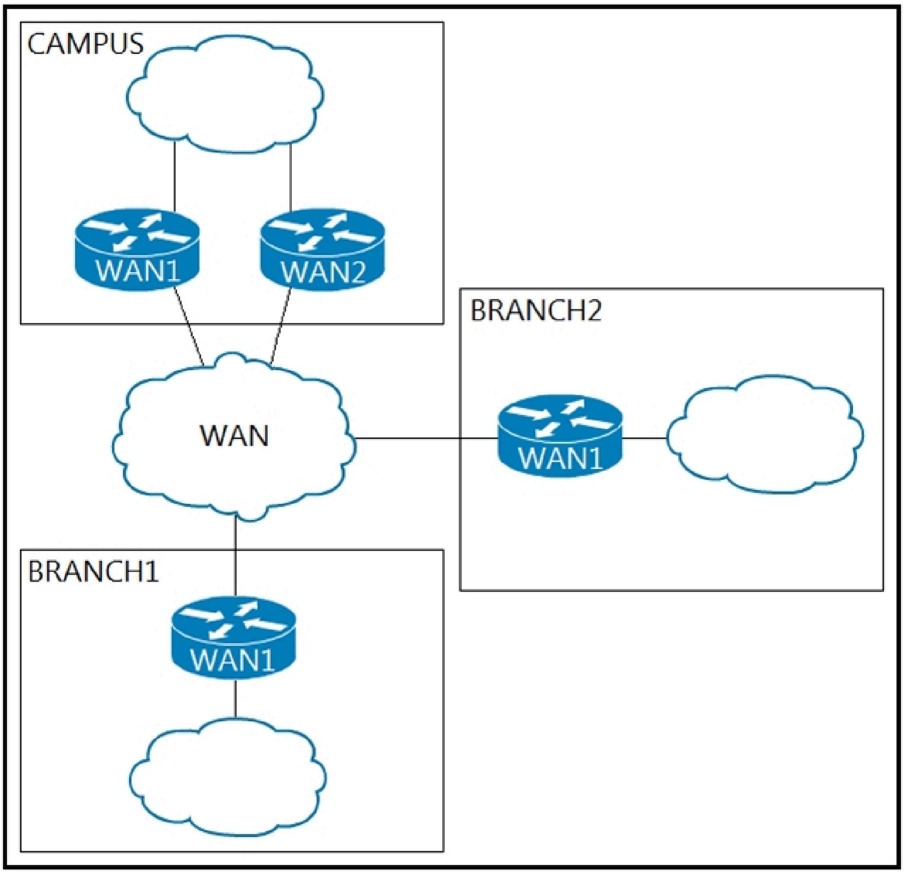
upvoted 1 times

**python_tamer** 1 year, 9 months ago

No need to DMVPN. Question states a single VPN between just 2 sites.

upvoted 3 times

Question #21 *Topic 1*



Refer to the exhibit. An architect must design an IP addressing scheme for a multisite network connected via a WAN transit. The campus site must accommodate

12,000 devices, and the branch sites must accommodate 1,000 devices. Which address scheme optimizes network device resources, contains convergence events to the different blocks of the network, and ensures the network's future growth?

A. ג€¢ Campus: 10.0.0.0/18 ג€¢ Branch1: 10.0.192.0/21 ג€¢ Branch2: 10.0.200.0/21

B. ג€¢ Campus: 10.0.0.0/16 ג€¢ Branch1: 10.255.0.0/20 ג€¢ Branch2: 10.255.16.0/20

C. ג€¢ Campus: 10.0.0.0/10 ג€¢ Branch1: 10.64.0.0/10 ג€¢ Branch2: 10.128.0.0/10

D. ג€¢ Campus: 10.0.0.0/20 ג€¢ Branch1: 10.0.64.0/21 ג€¢ Branch2: 10.0.128.0/21

**Correct Answer:** *A*

**mgiuseppe86** 1 year, 5 months ago

/18 = 16384 address

/21 = 2048 addresses

a /20 (1021 usable IPs) would have worked for the Branch Networks but that wasnt available in the answers.

upvoted 1 times

**akbntc** 1 year, 7 months ago

A is correct.

upvoted 1 times

**Noproblem22** 2 years, 1 month ago

A is correct

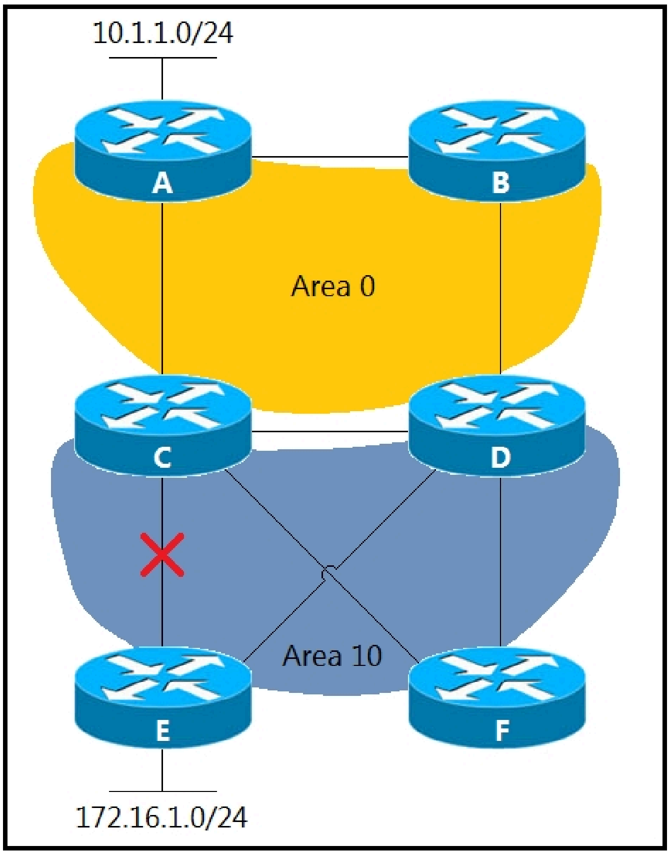
upvoted 1 times

**XalaGyan** 2 years, 11 months ago

Provided answer is correct

upvoted 1 times

Question #22 Topic 1



Refer to the exhibit. Area 10 is a regular OSPF area, and networks 10.1.1.0/24 and 172.16.1.0/24 are internal. Which design provides optimal routing between both networks when the link between routers C and E fails?

A. Move the link between routers C and D to area 10.

B. Create an OSPF virtual link between routers E and F.

C. Create a tunnel between routers E and F in area 10.

D. Make area 10 a not-so-stubby area.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**cerifyme85** 1 year, 10 months ago

Selected Answer: A

Honestly, it is a very stupid question.. none of the other options make sense but A anyway

upvoted 1 times

**python_tamer** 2 years, 9 months ago

Selected Answer: A

Answer is A because links A<>B and C<>D are not OSPF neighbours at all so without implementing option A, there is no route if link C<>E fails because D has no route.

upvoted 2 times

**Hope66** 2 years, 10 months ago

I see that the link between C and D is not in ospf area and nor the link between A and B.

So one possible solution is answer A

upvoted 2 times

**mgiuseppe86** 1 year, 5 months ago

I guess I never considered the blobs of colours meaning anything. But now i should pay attention to that. I didnt realize C and D werent in an OSPF area because the yellow or blue blobs dont reflect that

upvoted 2 times

⊟ **XalaGyan** 2 years, 11 months ago

can anyone please explain what the point is? i dont quite get the problem here in this question.

upvoted 1 times

⊟ **python_tamer** 2 years, 9 months ago

I think it's because links A<>B and C<>D are not OSPF neighbours at all so without implementing option A, there is no route if link C<>E fails.

upvoted 2 times

⊟ **funkeymonkey** 2 years, 7 months ago

Because of the SPF algorithm. OSPF calculates intra-area routes before inter-area routes. If the link between C and D was in area 0, C would calculate C-F-D-E as the shortest route, which isn't true. If the link between C and D is in area 10, C will calculate C-D-E as the shortest route.

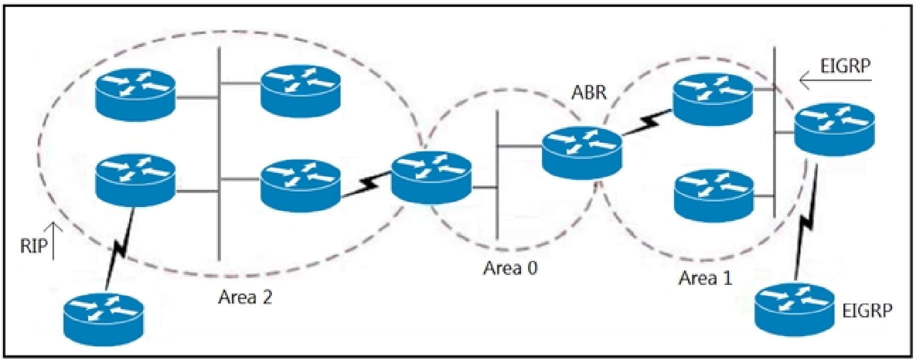
upvoted 5 times

⊟ **cerifyme85** 1 year, 10 months ago

This does not make any sense

upvoted 1 times

Question #23 Topic 1



Refer to the exhibit. An engineer is designing an OSPF network for a client. Requirements dictate that the routers in Area 1 should receive all routes belonging to the network, including EIGRP, except the ones that originated in the RIP domain. Which action should the engineer take?

A. Make area 1 a NSSA.

B. Make area 1 a stub.

C. Make area 1 a standard OSPF area.

D. Make the area 1 routers part of area 0.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

⊟ **Eddy1608** Highly Voted 3 years, 3 months ago

Area 1 is attached to EIGRP, so , It could not be a stub area. NSSA could be an external route and I think that the best option es A.

upvoted 11 times

⊟ **andre_b** Highly Voted 3 years, 1 month ago

I believe A is correct. Area 1 should be an NSSA because of the ASBR advertising EIGRP routes.

upvoted 7 times

⊟ **akbntc** Most Recent 1 year, 6 months ago

Selected Answer: A

Correct answer is A.

upvoted 1 times

⊟ **oaban** 2 years, 9 months ago

Selected Answer: A

A is correct

upvoted 1 times

⊟ **cwoolie** 2 years, 11 months ago

Answer is A

upvoted 1 times

⊟ **cwoolie** 2 years, 11 months ago

Answer is A

upvoted 1 times

⊟ **k22a** 2 years, 12 months ago

Selected Answer: A

there is an ASBR in area 1 , so it should be NSSA

upvoted 1 times

⊟ **roganjosh** 3 years ago

Selected Answer: A

A is the answer

upvoted 2 times

## Question #24 *Topic 1*

An engineer is tasked with designing a dual BGP peering solution with a service provider. The design must meet these conditions:
* The routers will not learn any prefix with a subnet mask greater than /24.
* The routers will determine the routes to include in the routing table based on the length of the mask alone.
* The routers will make this selection regardless of the service provider configuration.
Which solution should the engineer include in the design?

A. Use a route map and access list to block the desired networks, and apply the route map to BGP neighbors inbound.

B. Use a route map and prefix list to block the desired networks, and apply the route map to BGP neighbors outbound.

C. Use an IP prefix list to block the desired networks and apply the IP prefix list to BGP neighbors outbound.

D. Use an IP prefix list to block the desired networks and apply the IP prefix list to BGP neighbors inbound.

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**SpicyMochi** 1 year, 4 months ago

**Selected Answer: D**

D. Use an IP prefix list to block the desired networks and apply the IP prefix list to BGP neighbors inbound.

To meet the design conditions, the engineer should create an IP prefix list that blocks prefixes with a subnet mask greater than /24, and apply the IP prefix list to BGP neighbors inbound. This will filter out undesired networks and ensure that the routers will only learn prefixes with a subnet mask of /24 or less. This selection will be made based on the length of the mask alone, and it will be independent of the service provider's configuration.

upvoted 1 times

**XalaGyan** 2 years, 5 months ago

**Selected Answer: D**

Provided Answer is correct

* The routers will determine the routes to include in the routing table based on the length of the mask alone. ==> prefix list == length of mask alone , otherwise route-map is always more versatile

upvoted 2 times

Question #25 *Topic 1*

An engineer is designing an EIGRP network for a small branch office site where there is only one Layer 3 router. The engineer wants the router to advertise the local LAN network to remote EIGRP neighbors without sending any unnecessary multicast messages on the local LAN. Which action should the engineer take?

A. Use a static default route for this site instead of EIGRP

B. Advertise the local LAN using the network command and the passive-interface feature

C. Redistribute the local LAN network using the redistribute connected command

D. Advertise the local LAN subnet as a stub network

**Correct Answer:** *B*

*Community vote distribution*

B (69%) D (31%)

**teems5uk** 1 year, 6 months ago

**Selected Answer: B**

Passive Interface: When an interface is configured as a passive interface in EIGRP, it stops sending and receiving EIGRP hello packets. This means that the router will not form EIGRP neighbor relationships on that interface.
Effect on Routing Updates: The effect of the passive interface command in EIGRP is that it suppresses both outgoing and incoming routing updates. This is because EIGRP forms neighbor relationships by exchanging hello packets, and these relationships are required for the exchange of routing updates.

Use Cases: The passive interface feature is typically used in scenarios where you want to prevent EIGRP from sending or receiving updates on an interface, but still want the network connected to that interface to be advertised to other EIGRP neighbors.

upvoted 3 times

**leadac** 1 year, 9 months ago

**Selected Answer: B**

Making it a stub network (Option D) will not disable Hellos being sent through any interface. Instead, option B is suggesting to use Network command + passive interface command (Notice it does not say passive-interface default) so, in this case, the engineer should use his/her own criteria to determine on which interface to apply this command to. That is my justification to say that option B is correct.

upvoted 3 times

**mgiuseppe86** 1 year, 11 months ago

I am choosing B. The answer is in the question. Advertise the local LAN: via network command, however, without sending unnecessary multicast messages. so we make it passive.

upvoted 1 times

**Clauster** 2 years, 1 month ago

**Selected Answer: B**

The answer for this one is 100% B.
When you configure an interface as Passive EIGRP will not form a neighbor adjacency with any other routers on the interface, there for it will not send Multicast Messages on Passive Interfaces, in this case we want to configure our Passive Interface on the Local LAN.

upvoted 2 times

**CKL_SG** 2 years, 3 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

**SpicyMochi** 2 years, 4 months ago

**Selected Answer: B**

B. Advertise the local LAN using the network command and the passive-interface feature

The engineer should use the network command to advertise the local LAN network in EIGRP and then apply the passive-interface feature to the LAN interface. By doing this, the router will advertise the local LAN network to remote EIGRP neighbors, but it will not send any unnecessary EIGRP multicast messages on the local LAN. The passive-interface feature prevents EIGRP from sending updates or forming adjacencies on the specified interface, which is useful in this scenario since there is only one Layer 3 router at the site.

upvoted 1 times

**emre076** 2 years, 8 months ago

**Selected Answer: B**

b is correct. if you make it a stub then it wont advertise the local lan to the remote neighbor, which is a requirement. the router has as atleast 2 interfaces. one that connects to the remote neighbor and one for the local lan. passive interface can be configured per interface. so you make the local lan interface a passive interface done!

upvoted 1 times

**Furiel** 2 years, 9 months ago

I think the confusion on this question is that the passive interface would be to the LAN and not to the remote router otherwise they cant form an adjacency, question states they dont want to send unnecessary multicast traffic to the LAN (not remote router). Answer is B

upvoted 1 times

**andrewChan** 2 years, 10 months ago

B is correct. imagine there is 2 interfaces on the router, one connect to the WAN and the other connect to the LAN, in the router EIGRP, both interface must advertise by netowrk command, and the mulitcast of hello message started at this point. As the question state only 1 router on the network, there is no peer on LAN and passive-interface will stop the multicast for peering.
and of cause, stub will eliminate query (send as multicast) from hub site via WAN, while the question is asking about LAN, so B is correct.

upvoted 1 times

**python_tamer** 3 years, 2 months ago

**Selected Answer: B**

Sorry, forget my last comment, the correct answer is definitely B as the requirement is simply to advertise the network but NOT send MC traffic on the local LAN. For this you have to make it a passive interface. There are no requirements stated to make it a stub.

upvoted 1 times

**python_tamer** 3 years, 3 months ago

**Selected Answer: D**

Agree with D

upvoted 2 times

**TMe392** 3 years, 5 months ago

D is right as passive-interface block incoming and outgoing eigrp route updates

upvoted 2 times

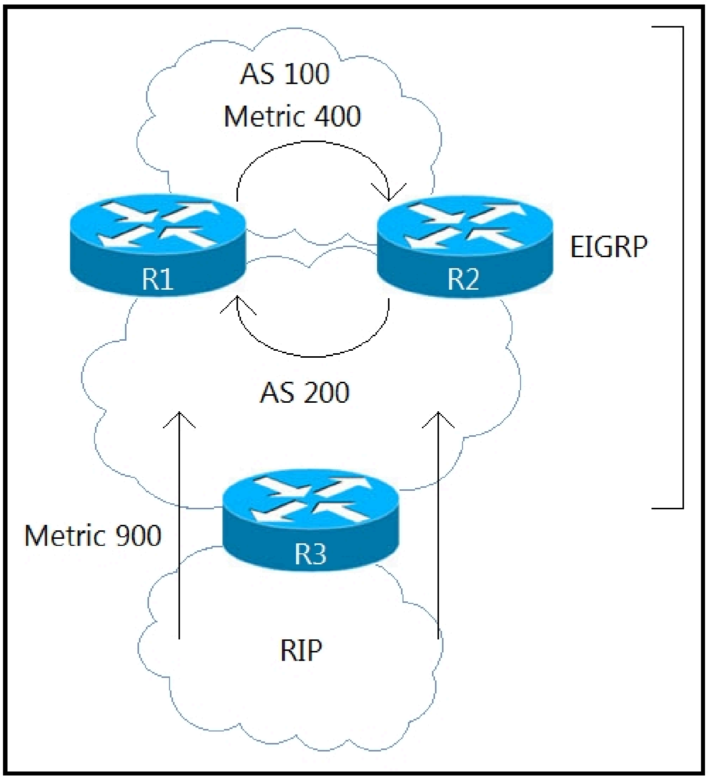
**XalaGyan** 3 years, 5 months ago

**Selected Answer: B**

Provided answer is correct

upvoted 1 times

Question #26 Topic 1



Refer to the exhibit. An architect must design a solution to connect the network behind R3 with the EIGRP network. Which mechanism should be included to avoid routing loops?

A. down bit

B. split-horizon

C. route tags

D. summarization

**Correct Answer:** *C*

*Community vote distribution*

C (81%) B (19%)

⊟ **certstudent2016** Highly Voted 👍 3 years, 4 months ago

Selected Answer: C

https://www.ciscopress.com/articles/article.asp?p=1763921&seqNum=5

upvoted 10 times

⊟ **XalaGyan** 2 years, 7 months ago

many thanks certstudent2016

upvoted 1 times

⊟ **XalaGyan** 2 years, 7 months ago

Outbound route tags can be used to filter redistribution and support EIGRP scaling with multiple EIGRP autonomous systems, as shown in Figure 3-10.

Figure 3-10

Figure 3-10 Filtering EIGRP Redistribution with Route Tags

External routes can be configured to carry administrative tags. When the external route is redistributed into autonomous system 100 at router A or B, it can be tagged. This tag can then be used to filter the redistribution of the route back into autonomous system 200. This filtering blocks the formation of the loop, because router A will no longer receive the redistributed routes from router B through autonomous system 200.

In the configuration snippets, when routers A and B redistribute autonomous system 200 routes into autonomous system 100, they tag the routes with tag 100. Any routes tagged with tag 100 can then be prevented from being redistributed back into autonomous system 200. This successfully prevents a routing loop from forming.

upvoted 2 times

**Lungful** 2 years ago

The exhibit is the same as figures 3-9 and 3-10. C is correct.

upvoted 1 times

**teems5uk** Most Recent 1 year, 6 months ago

Selected Answer: C

https://www.ciscopress.com/articles/article.asp?p=1763921&seqNum=5#:~:text=Filtering%20EIGRP%20Redistribution,loop%20from%20forming.

upvoted 1 times

**Noproblem22** 2 years, 8 months ago

C is the best answer

upvoted 1 times

**oaban** 3 years, 3 months ago

Selected Answer: C

I think C is correct

upvoted 2 times

**cwoolie** 3 years, 5 months ago

Route Tags is correct Answer

upvoted 3 times

**BolleOtter** 3 years, 8 months ago

Selected Answer: B

Used by distance vector. Routes learned from a neighbour are not sent back to that neighbour

upvoted 1 times

**h40017** 3 years, 7 months ago

Within a routing protocol, your statement is correct. However, redistribution is in play here, the given answer is correct.

upvoted 6 times

Question #27 *Topic 1*

An architect is creating a migration strategy for a large organization in which the choice made by the application between IPv6 and IPv4 is based on the DNS request. Which migration strategy does the architect choose?

A. AFT for public web presence

B. host-initiated tunnels

C. dual-stack

D. site-to-site IPv6 over IPv4 tunnels

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**XalaGyan** 1 year, 7 months ago

**Selected Answer: C**

The transition is driven by DNS. If a dual-stacked device queries the name of a destination and DNS gives it an IPv4 address (a DNS A Record), it sends IPv4 packets. If DNS responds with an IPv6 address (a DNS AAAA Record), it sends IPv6 packets.

upvoted 2 times

**XalaGyan** 1 year, 7 months ago

https://www.juniper.net/documentation/us/en/software/junos/is-is/topics/concept/ipv6-dual-stack-understanding.html

The transition is driven by DNS. If a dual-stacked device queries the name of a destination and DNS gives it an IPv4 address (a DNS A Record), it sends IPv4 packets. If DNS responds with an IPv6 address (a DNS AAAA Record), it sends IPv6 packets.

upvoted 1 times

Question #28 *Topic 1*

An engineer is creating a design to enable IPv6 to run on an existing IPv4 IS-IS network. The IPv4 and IPv6 topologies will match exactly, and the engineer plans to use the same IS-IS router levels for each protocol per interface. Which IS-IS design is required?

A. multi topology without enabling transition feature

B. multi topology with transition feature enabled

C. single topology without enabling transition feature

D. single topology with transition feature enabled

**Correct Answer:** *C*

*Community vote distribution*

C (78%) 13% 9%

**Gabi512** Highly Voted 3 years, 9 months ago

Selected Answer: C

I would say C as both IPV4 and IPV6 are sharing the exact same topology. No need of multipology nor transition mode:
https://www.ws.afnog.org/afnog2011/are/ipv6-presentations/4-isis-for-ipv6.pdf

upvoted 12 times

**dougj** Most Recent 4 months, 3 weeks ago

Selected Answer: A

In OCG on page 121 it states "IS-IS provides support for IPv4 and IPv6 as separate topologies" therefore multi topology setting is required without transition

upvoted 1 times

**dougj** 4 months, 3 weeks ago

Further reading says that single topology with Dual Stack will also work, so it can still be either single or multi topology for this question

upvoted 1 times

**neiker45** 1 year, 8 months ago

Selected Answer: C

https://datatracker.ietf.org/meeting/105/agenda/v6ops-drafts.pdf
Single Topology: 4.1 Third Paragraph
Transition: 4.2.1 First Paragraph

upvoted 1 times

**LSLS55** 1 year, 10 months ago

Selected Answer: B

According to OCG, page 120: "IS-IS support IPv6 as a separate protocol(...)" and page 121 "IS-IS provides support for IPv4 and IPv6 as separate topologies" -> this means it needs two separate topologies for different address families = MULTITOPOLOGY.

upvoted 1 times

**12504a3** 6 months, 3 weeks ago

No, it is C. On the same page of OCG you are mentioning, same paragraph, it is stated at the end :
"It is important to know that if IPv4 and IPv6 are sharing the same topologies with the same router levels, there is no need for multi-topology or transition features."

upvoted 1 times

**draxon** 2 years ago

Selected Answer: B

https://rayka-co.com/lesson/isis-ipv6-multi-topology/

upvoted 1 times

**Clauster** 2 years, 1 month ago

Selected Answer: D

The answer is 100% D

upvoted 1 times

**Clauster** 2 years, 1 month ago

Sorry folks the answer is indeed C

upvoted 1 times

**SpicyMochi** 2 years, 4 months ago

Selected Answer: C

C. single topology without enabling transition feature

In a single topology design, both IPv4 and IPv6 addresses can be carried within the same IS-IS domain without creating separate topologies. IS-IS, being a Layer 2 protocol, can natively support both IPv4 and IPv6. By utilizing a single topology design without any transition feature, the engineer can enable IPv6 on the existing IPv4 IS-IS network with the same router levels for each protocol per interface, while still maintaining a single, integrated topology.

upvoted 2 times

**andrewChan** 2 years, 10 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/xe-3s/irs-xe-3s-book/ip6-route-isis-xe.html#GUID-04990BCF-8228-459E-AFAA-9FAF1E2136E9

single topology with no adjacency-check, so D is correct

For single-topology IS-IS IPv6, routers must be configured to run the same set of address families. IS-IS performs consistency checks on hello packets and will reject hello packets that do not have the same set of configured address families. For example, a router running IS-IS for both IPv4 and IPv6 will not form an adjacency with a router running IS-IS for IPv4 or IPv6 only. In order to allow adjacency to be formed in mismatched address-families network, the adjacency-check command in IPv6 address family configuration mode must be disabled.

Enter the no adjacency-check command only when you are running IPv4 IS-IS on all your routers and you want to add IPv6 IS-IS to your network but you need to maintain all your adjacencies during the transition.

upvoted 1 times

**iLikeHamburgers** 2 years, 11 months ago

The key thing here is that it states there is a currently deployed IPV4 network. Once you configure IPv6 on an interface that is currently running IPv4, you break the requirement that states "all interfaces on which IS-IS is configured must support the identical set of network address families." There is also a requirement that states "all routers in the IS-IS area (for Level 1 routing) or domain (for Level 2 routing) must support the identical set of network layer address families." I don't have the ability to lab this at the moment, however I would be curious to see if you had a network running single topology IPv4 only, and then started configuring IPv6 on the interfaces, would it break anything. I would question whether C is correct or not. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/xe-3s/irs-xe-3s-book/ip6-route-mult-isis-xe.html#GUID-EA369F57-430A-4F30-B467-4529140CB0B6

upvoted 2 times

> **andrewChan** 2 years, 10 months ago
>
> yes it would break adjanency when address familty is different during transition, according to cisco doc:
> For single-topology IS-IS IPv6, routers must be configured to run the same set of address families. IS-IS performs consistency checks on hello packets and will reject hello packets that do not have the same set of configured address families. For example, a router running IS-IS for both IPv4 and IPv6 will not form an adjacency with a router running IS-IS for IPv4 or IPv6 only. In order to allow adjacency to be formed in mismatched address-families network, the adjacency-check command in IPv6 address family configuration mode must be disabled.
>
> https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/xe-3s/irs-xe-3s-book/ip6-route-isis-xe.html#GUID-04990BCF-8228-459E-AFAA-9FAF1E2136E9
>
> upvoted 1 times

**python_tamer** 3 years, 3 months ago

Selected Answer: C

I agree with C.

upvoted 1 times

**oaban** 3 years, 3 months ago

Selected Answer: C

I thinks C. Topologies match exact, no need multitopology.

upvoted 2 times

**certstudent2016** 3 years, 4 months ago

Selected Answer: B

https://www.ws.afnog.org/afnog2011/are/ipv6-presentations/4-isis-for-ipv6.pdf

toward the ends its given answer - B is correct

https://datatracker.ietf.org/doc/rfc5120/

upvoted 1 times

⊟ **XalaGyan** 2 years, 7 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/15-mt/irs-15-mt-book/ipv__routing__is-is_multitopology_support_for_ipv_.pdf

Transition from Single-Topology to Multitopology Support for IPv6

All routers in the area or domain must use the same type of IPv6 support, either single-topology or multitopology. A router operating in multitopology mode will not recognize the ability of the single-topology mode router to support IPv6 traffic, which will lead to holes in the IPv6 topology. To transition from single-topology support to the more flexible multitopology support, a multitopology transition mode is provided.

upvoted 1 times

⊟ **XalaGyan** 2 years, 7 months ago

The multitopology transition mode allows a network operating in single-topology IS-IS IPv6 support mode to continue to work while upgrading routers to include multitopology IS-IS IPv6 support. While in transition mode, both types of TLVs (single-topology and multitopology) are sent in LSPs for all configured IPv6 addresses, but the router continues to operate in single-topology mode (that is, the topological restrictions of the single-topology mode are still in effect). After all routers in the area or domain have been upgraded to support multitopology IPv6 and are operating in transition mode, transition mode can be removed from the configuration. Once all routersin the area or domain are operating in multitopology IPv6 mode, the topological restrictions of single-topology mode are no longer in effect.

upvoted 1 times

⊟ **XalaGyan** 2 years, 7 months ago

Again i agree with you certstudent2016.

At some point in the configuration we have to introduce IPv6 to an already running and converged IPv4 IS-IS single topology. Single topology mandates the use of a single address family. ==> this brings adjacencies down

Solution is to go MULTITOPOLOGY as MT dont bother about Address Families. Then you have to have transition feature enabled due to the EXACT SAME TOPOLOGY part of the question.

later when you have multitopology and ipv4 and ipv6 then you disable transition feature.

upvoted 2 times

Question #29 Topic 1

An engineer must connect a new remote site to an existing OSPF network. The new site consists of two low-end routers, one for WAN, and one for LAN. There is no demand for traffic to pass through this area. Which area type does the engineer choose to provide minimal router resource utilization, while still allowing for full connectivity to the rest of the network?

A. not so stubby

B. totally not so stubby

C. totally stubby area

D. stubby area

**Correct Answer:** *C*

*Community vote distribution*

C (75%) D (25%)

⊟ **eduardooramos** Highly Voted 👍 3 years, 7 months ago

I this correct answer is C.

upvoted 6 times

⊟ **LSLS55** Most Recent ⏲ 1 year, 9 months ago

Selected Answer: C

Btw, there are STUB areas, STUBBY areas do not exist (if it does, I cannot find it on Cisco documentation).

upvoted 2 times

⊟ **bubd** 2 years ago

Ans: D

A stubby area in OSPF is used to reduce router resource utilization and limit the size of the routing table while still allowing for full connectivity to the rest of the OSPF network. This choice is appropriate when you have no demand for traffic to pass through the area, as it blocks the type 5 external LSAs, thereby reducing the routing information and resources required in that specific area.

upvoted 1 times

⊟ **Clauster** 2 years ago

Selected Answer: D

The provided answer is correct the answer is D.

- Stub Area will be able to talk to the rest of the network (This is a requirement) where as the TSA can't.
- The WAN router IS NOT an ASBR, it is simply an ABR connected to the rest of the OSPF Network, it would of been an ASBR if EIGRP or a different routing protocol was running here.
- Stub area also uses low resources, o tho TSA uses less but unfortunately it does not mee the (needs to reach the rest of the network requirement) where as Stubby Area does.

upvoted 1 times

⊟ **drinu89** 2 years, 5 months ago

Selected Answer: D

D is Correct

upvoted 1 times

⊟ **ghaith_gld** 2 years, 7 months ago

Selected Answer: C

we need ASBR for WAN, and stub area does not have ASBR

upvoted 1 times

⊟ **Noproblem22** 2 years, 8 months ago

C is better answer than D.

A stub area is an area in which advertisements of external routes are not allowed, reducing the size of the database. A totally stubby area (TSA) is a stub area in which summary link-state advertisement (type 3 LSAs) are not sent. A default summary LSA, with a prefix of 0.0.

upvoted 3 times

⊟ **kos9** 2 years, 8 months ago

Selected Answer: C

C correct

upvoted 1 times

**andrewChan** 2 years, 10 months ago

Selected Answer: C

totally stubby area inject 1 default route into the area, it should able to connect rest of the network with minimal resource used

upvoted 2 times

**iLikeHamburgers** 2 years, 11 months ago

Selected Answer: C

“There is no demand for traffic to pass through this area.” So we know from this that an NSSA or a totally not so stubby area is needed. NSSA’s or totally NSSA’s are only needed if routes are being injected into the OSPF domain. So A and B are not correct.
C and D are both similar in that they both do not inject Type 5 LSA, which would keep router utilization down. However, if we desire to cut down on as many LSA’s as possible, which would then cut down on the router utilization due to the OSPF routers not having to run the SPF calculation, then answer C is MOST correct. A totally stubby area restricts not only type 5, but also type 4 and type 3 LSA’s. Since the requirement states “provide minimal resource utilization” answer C “totally stubby area” is correct.

upvoted 4 times

**python_tamer** 3 years, 3 months ago

Selected Answer: C

I think C - Totally Stubby Area is correct. Just a default into this new area is fine.

upvoted 2 times

**cwoolie** 3 years, 4 months ago

Why not A?

upvoted 1 times

**TMe392** 3 years, 5 months ago

I think C as LSA type1 + type2 + Defaut required to minimise Router resources utilization -> total stub area

upvoted 2 times

**cwoolie** 3 years, 5 months ago

Sorry. Answer should be C as Stub area blocks external traffic

upvoted 2 times

**cwoolie** 3 years, 5 months ago

D is answer

upvoted 1 times

**roganjosh** 3 years, 6 months ago

Selected Answer: D

Answer is right D, 2 routers, means Layer 3 LSA's need to get in so the area knows how to reach routes on the LAN/ other Areas.

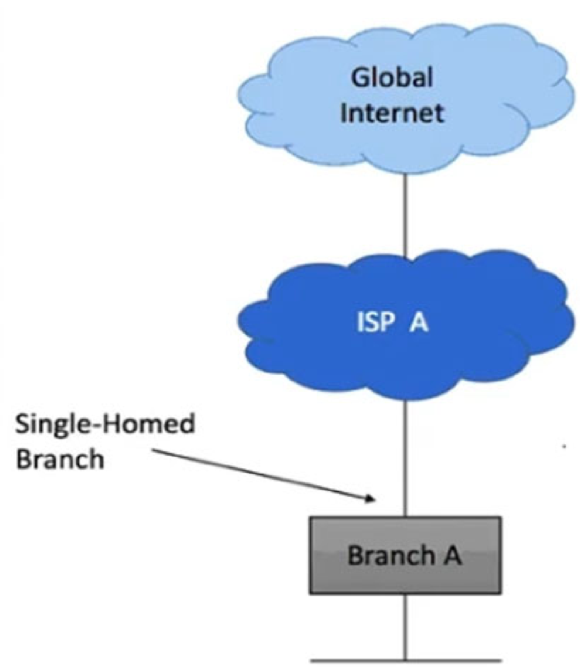
upvoted 2 times

**configt** 3 years, 6 months ago

A totally stubby area is an area that is not able to accept LSA type 3 or 5 which contain routes from outside the OSPF domain and is not able to accept routes from outside the area; traffic is only able to exit the area via a default route (which is injected via the ABR).Jan 18, 2012

upvoted 2 times

Question #30 *Topic 1*



Refer to the exhibit. An architect is designing a BGP solution to connect a remote branch to a service provider. There are several prefixes within the branch that the company does not want to be advertised to the Internet. Which solution should the architect use to accomplish this?

A. Attach the No-Export community with the prefixes to exclude.

B. Use the BGP No-Advertise community for the prefixes to exclude.

C. Set the BGP Internet community for all prefixes.

D. Implement the NOPEER community.

**Correct Answer:** *A*

*Community vote distribution*

A (62%) B (38%)

**Clauster** Highly Voted 2 years, 1 month ago

**Selected Answer: A**

Guys i am sorry, the answer is actually A. Thank god i had to double check my work.
Here i will put it easy for you to understand and you can backup what i am saying by looking at Cisco documentation
No-Adverstise: It restricts a BGP Router to not advertise prefixes to iBGP AND eBGP
No-Export: It restricts a BGP Router to not advertise prefixes to eBGP ONLY, iBGP prefixes WILL BE ADVERTISED. This is the less restrictive option.
Well since this is an Internet Service Provider we can very easly assume this is a Public Network where eBGP lives, so we can use the no-export here instead of the no-advertise, even though both would work they are testing your knowledge.

upvoted 5 times

**iLikeHamburgers** Highly Voted 2 years, 11 months ago

**Selected Answer: A**

Both A and B will get the job done, as they both will keep Branch A prefixes from being advertised to the internet, however there is a fundamental difference in what happens after the prefix is advertised to ISP A. If the No-Export community is used, then the prefixes will only be advertised to other BGP speakers with the same AS as ISP A. Which means the prefix will not be advertised to the internet but will be advertised within ISP A's network which would be ideal.
If the No-Advertise community is used, then only the BGP router that is peered with Branch A will have the routes. And while it won't advertise these prefixes to the internet, it also won't advertise them to any other routers with the same AS as it (ISP A). This would keep all other routers inside of ISP A from learning the routes, which is not ideal from a failover perspective.

upvoted 5 times

**InYoPie** Most Recent 1 year, 6 months ago

Answer A makes more sense in this case.

The question clearly states that this is a remote branch site. So I would assume the ISP A in this case is some kind of WAN link and we would want the ISP A to propagate the internal routes within our Branch A location so that our HQ can send traffic out (destined for the restricted Branch A prefixes) and be routed through the ISP A network to reach the Branch location.

Answer B does make sense if it the picture did not show ISP A, but rather a direct connection to Global Internet with an ISP A router sitting in the Internet cloud.

upvoted 1 times

⊟ **Clauster** 2 years, 1 month ago

Selected Answer: B

The No-Export and No-Advertise communities in BGP are both used to control the advertisement of routes to external BGP (eBGP) peers. However, there are some key differences between the two communities.

The No-Export community prevents a router from advertising a route to eBGP peers outside of a specific autonomous system (AS). This can be useful for preventing routes from being leaked to other ASes.

The No-Advertise community prevents a router from advertising a route to any eBGP peers. This can be useful for preventing routes from being advertised to the public internet.

upvoted 4 times

⊟ **GustavoF** 2 years, 4 months ago

Selected Answer: B

B makes more sense to me to not send it to Internet.
There`s a risk of ISP A backbone being huge, it`s going to propagate to all other routers inside the same AS if we use No-Export community, others customers from ISP A connected to Internet are going to use the ISP A backbone to reach out the Customer networks.
Using No-Adversite, makes more sense and avoid that because it will be installed on the ISP router and won`t be advertised to anyone.

upvoted 1 times

⊟ **SergeBesse** 2 years, 11 months ago

Selected Answer: A

A - this answer is good.
When a No-Advertise community is attached to a route, the BGP speaker won't advertise the route to any internal or external BGP peers.
When a No-Export community is attached to a route, the router won't advertise the route to external peers--only to internal peers.
reference: https://www.catchpoint.com/network-admin-guide/bgp-communities

upvoted 1 times

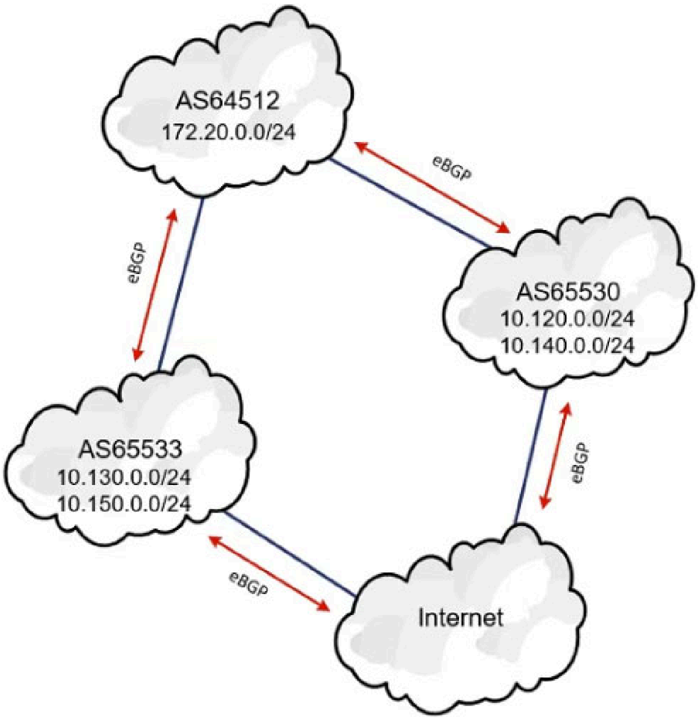
⊟ **funkeymonkey** 3 years, 1 month ago

Selected Answer: B

no advertise community makes more sense

upvoted 1 times

## Question #31 *Topic 1*



Refer to the exhibit. AS65533 and AS65530 are announcing a partial Internet routing table as well as their IP subnets. An architect must create a design that ensures AS64512 does not become a transit AS. Which filtering solution must the architect choose?

A. no-advertise

B. next-hop

C. no-export

D. maximum-prefix

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**andrewChan** Highly Voted 2 years, 4 months ago

Selected Answer: C

4 methods how you can prevent becoming a transit AS:

1 Filter-list with AS PATH access-list.

2 No-Export Community.

3 Prefix-list Filtering

4 Distribute-list Filtering

upvoted 5 times

**Clauster** Most Recent 1 year, 7 months ago

Selected Answer: C

Again, the no-export is used for eBGP ONLY

the no-advertised is used on both iBGP and eBGP.

When the question strictly refers to or assumes to be eBGP only please only use no-export.

In this question this is obviously eBGPs

upvoted 3 times

**XalaGyan** 2 years, 11 months ago

Selected Answer: C

Provided answer is correct

upvoted 2 times

⊟ **XalaGyan** 2 years, 11 months ago

Provided answer is correct

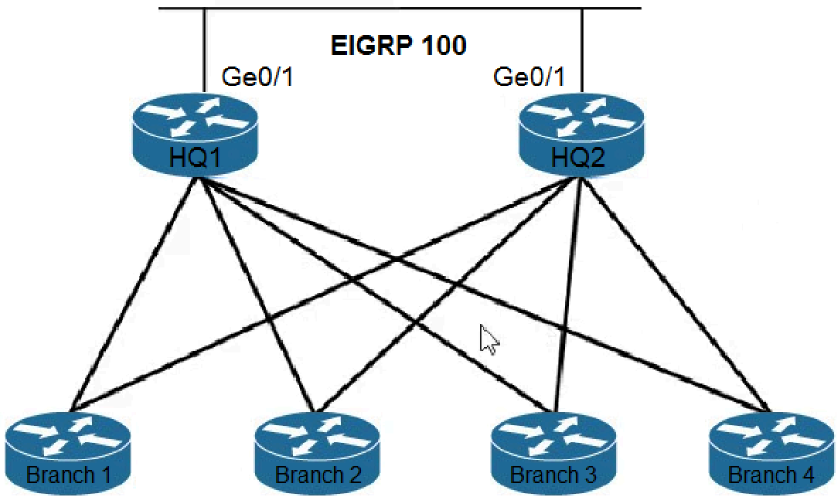
upvoted 1 times

⊟ **cwoolie** 2 years, 11 months ago

I found answer to be "D"

upvoted 2 times

Question #32 *Topic 1*



Refer to the exhibit. An architect must create a stable and scalable EIGRP solution for a customer. The design must:

➾ conserve bandwidth, memory, and CPU processing

➾ prevent suboptimal routing

avoid any unnecessary queries

▪

Which two solutions must the architect select? (Choose two.)

A. route summarization

B. prefix lists

C. distribute lists

D. stub routing

E. static redistribution

**Correct Answer:** *AD*

*Community vote distribution*

AD (88%) 13%

**Eddy1608** Highly Voted 2 years, 10 months ago

I think is A and D:

The EIGRP stub routing feature provides four advantages when implemented in hub-and-spoke networks;

*It prevents sub-optimal routing from occurring within hub-and-spoke EIGRP networks
*It prevents stub routers with low-speed links from being used as transit routers
*It eliminates EIGRP Query storms, allowing the EIGRP network to convergence faster
*It reduces the required amount of configuration commands on the stub routers

upvoted 23 times

**andrewChan** 1 year, 10 months ago

agree. when link between HQ1 & HQ2 down, without stub on branch routers, HQ routers will pick either link as backup, the traffic loading may cause congestion and unstable to the branch routers. And suppose the HQs should have resilience link in reality.

upvoted 3 times

**CKL_SG** Most Recent 1 year, 3 months ago

**Selected Answer: AD**

Sub-optimal routing is eliminated because the stub spoke routers will only process traffic for which it has explicitly advertised availability

upvoted 1 times

**Hope66** 2 years, 2 months ago

It seems that A and D or A and C are both valid. I read from Cisco Press :
"What really stops a query is general scaling methods using summarization, distribution lists, and stubs."
https://www.ciscopress.com/articles/article.asp?p=1763921&seqNum=5

upvoted 1 times

**python_tamer** 2 years, 3 months ago

Selected Answer: AD

I think AD.
I don't think you would want your branches becoming transits if the link between HQ1 <> HQ2 failed. We don't know the link speeds. Could be slow. Hopefully there are other backup links between the HQs that are not shown.
The issue with using dist lists rather than stub areas is that dist lists will not "avoid any unnecessary queries" which is one of the design requirements.

upvoted 2 times

**certstudent2016** 2 years, 4 months ago

Selected Answer: AC

https://www.ciscopress.com/articles/article.asp?p=1763921&seqNum=5

upvoted 1 times

**mazinhoo** 2 years, 5 months ago

i think its A and C, the issue with D is " The only disadvantage is that the stub router cannot be used as a backup path between two hub sites" in this question we have two hub sites

upvoted 2 times

**XalaGyan** 2 years, 5 months ago

I agree with you because the question states stable
Refer to the exhibit. An architect must create a stable and scalable EIGRP solution for a customer.

for me if the stubby architecture is applied and the ethernet link between HQ 1 and 2 breaks, there wont be fallback routes and i therefore dont see it as stable.

while with distribution lists eventhough it sux to manage but can get the needed resource optimization done while allowing for fallback routes. that is at least more stable

upvoted 1 times

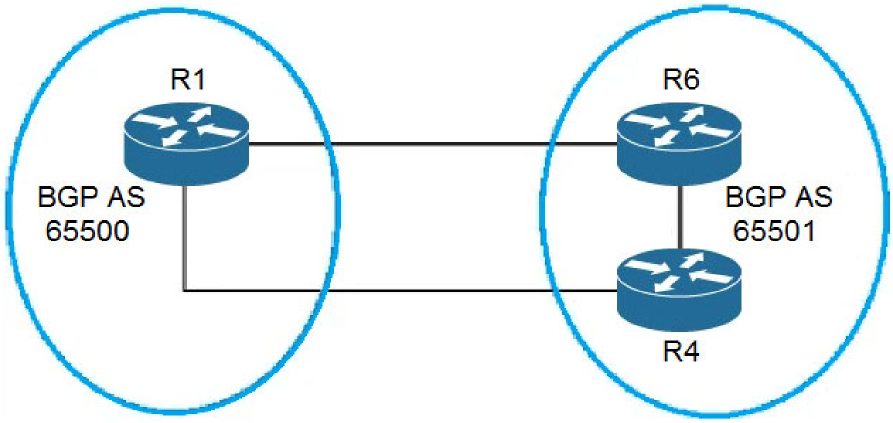
**roganjosh** 2 years, 6 months ago

Selected Answer: AD

A & D Are correct

upvoted 1 times

Question #33 *Topic 1*



Refer to the exhibit. An architect must design a solution to connect the two ASs. To optimize bandwidth, the design will implement load sharing between router R6 and router R1. Which solution should the design include?

A. Use update-source to specify the Loopback interface.

B. Use next-hop-self attributes only for routes that are learned from eBGP peers.

C. Configure the eBGP TTL to support eBGP multihop.

D. Use maximum-paths to install multiple paths in the routing table.

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**SpicyMochi** 1 year, 4 months ago

**Selected Answer: D**

D. Use maximum-paths to install multiple paths in the routing table: This configuration allows multiple paths to be installed in the routing table for the same destination prefix, enabling load sharing between R1 and R6. By using the maximum-paths command, traffic can be load balanced between the two routers, optimizing bandwidth utilization.

upvoted 1 times

**konyuz** 1 year, 6 months ago

C is the correct answare. R6 wants two bgp sessio to R1, one of direct other is not. Therefore second session is not able to succes becouse of BGP ttl=1. You have to setting ebgp-multihop .
https://networklessons.com/bgp/ebgp-multihop

upvoted 1 times

**vallzo** 1 year ago

It is only 1 eBGP hop for both paths

upvoted 1 times

**XalaGyan** 2 years, 5 months ago

**Selected Answer: D**

Provided answer is correct

upvoted 1 times

Question #34 *Topic 1*

A customer's environment includes hosts that support IPv6-only. Several of these hosts must communicate with a public web server that has only IPv4 domain name resolution. Which solution should the customer use in this environment?

A. utilize NAT64 to translate the addresses

B. implement NAT44 at the edge of the customer network

C. use 6to4 and a tunnel to translate the addresses

D. implement 6PE to resolve hostname resolution

**Correct Answer:** *A*

**eva27** 1 year, 7 months ago

NAT64 is a mechanism for IPv4-to-IPv6 transition and IPv4-IPv6 coexistence. Together with DNS64, the primary purpose of NAT64 is to allow an IPv6-only client to initiate communications to an IPv4-only server.NAT64 can also be used for IPv4-only clients initiating communications with IPv6-only servers using static or manual bindings

upvoted 3 times

Question #35 *Topic 1*

A company is planning to open two new branches and allocate the 2a01:c30:16:7009::3800/118 IPv6 network for the region. Each branch should have the capacity to accommodate a maximum of 200 hosts. Which two networks should the company use? (Choose two.)

A. 2a01:0c30:0016:7009::3a00/120

B. 2a01:0c30:0016:7009::3b00/121

C. 2a01:0c30:0016:7009::3a80/121

D. 2a01:0c30:0016:7009::3c00/120

E. 2a01:0c30:0016:7009::3b00/120

**Correct Answer:** *AE*

**Sickcnt** Highly Voted 2 years, 4 months ago

Answers A, E are correct:

Network range for 2a01:c30:16:7009::3800/118
2a01:0c30:0016:7009:0000:0000:0000:3800-
2a01:0c30:0016:7009:0000:0000:0000:3bff

Network Range for 2a01:0c30:0016:7009::3a00/120
2a01:0c30:0016:7009:0000:0000:0000:3a00-
2a01:0c30:0016:7009:0000:0000:0000:3aff

Network range for 2a01:0c30:0016:7009::3b00/120
2a01:0c30:0016:7009:0000:0000:0000:3b00-
2a01:0c30:0016:7009:0000:0000:0000:3bff

(As you see it ends with 2a01:0c30:0016:7009:0000:0000:0000:3bff
So that means 2a01:0c30:0016:7009:0000:0000:0000:3c00/120 is out of the picture)

upvoted 7 times

**XalaGyan** 2 years, 1 month ago

very well explained

upvoted 1 times

**Mebeelen** Most Recent 1 year, 7 months ago

And why not ::3c00/120 ? Is the same, isn´t it?

upvoted 2 times

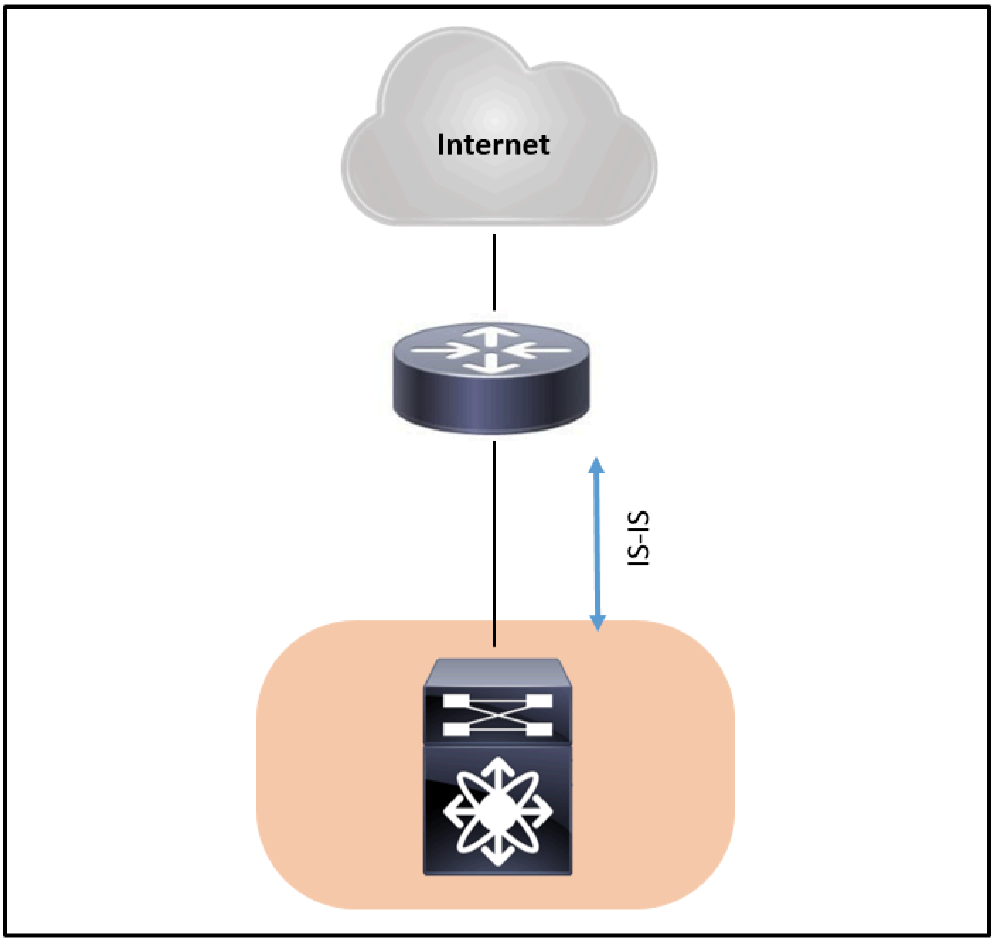
**mgiuseppe86** 1 year, 5 months ago

it falls out of scope of ::3800/118 as it is 3800-3bff

upvoted 2 times

Question #36 *Topic 1*

Refer to the exhibit.



A network engineer must improve the current IS-IS environment. The Catalyst switch is equipped with dual supervisors. Each time a stateful switchover occurs, the network experiences unnecessary route recomputation. Which solution addresses this issue if the upstream router does not understand graceful restart messaging?

A. Enable IS-IS remote LFA FRR on both devices.

B. Enable NSR on the switch.

C. Enable NSF on the switch.

D. Configure ISIS aggressive timers on both devices.

**Correct Answer:** *B*

*Community vote distribution*

B (81%) C (19%)

⊟ **SergeBesse** Highly Voted 3 years, 5 months ago

Selected Answer: B

the correct answer is B (NSR)

NSF is also known as gracefull restart. And the router does not understand GR.

upvoted 8 times

⊟ **ef869f0** Most Recent 9 months, 1 week ago

Selected Answer: B

-------------------------------NSR --------------------------------------------------------

--attempts to maintain neighbor adjacencies during an RP failover.

--does not require cooperation from neighbors (unlike GR), so the neighbors are not aware that an RP failover is happening.

--In addition to checkpointing the FIB, routing protocol state information is also checkpointed to standby RP.

answer is B (since the upstream device does not understand GR)

upvoted 1 times

**Seb82** 1 year, 6 months ago

**Selected Answer: C**

Non-Stop Routing (NSR) is a Cisco proprietary feature similar to NSF, but it requires support on both the switch and the upstream router. The question states that the upstream router doesn't understand graceful restart messaging, so NSR won't work.

upvoted 2 times

**vallzo** 1 year, 5 months ago

Its the opposite. NSF uses the GR mechanism, not NSR.

upvoted 3 times

**mgiuseppe86** 2 years, 5 months ago

Everyone is voting B, but all the answers are are explaining C.

The very last mssage of the question says the upstream router doesnt understand graceful restart. So we must use NSR instead

upvoted 1 times

**LSLS55** 2 years, 4 months ago

It's B. Check my comment regarding this with information from OCG page 168.

upvoted 2 times

**akbntc** 2 years, 5 months ago

**Selected Answer: C**

Repeating again... it's C. NSR helps for a graceful restart (GR). But our scenario is SSO (Stateful Switchover), where NSF is used.

upvoted 1 times

**akbntc** 2 years, 6 months ago

**Selected Answer: C**

Correct answer is C.

After a supervisor engine switchover, NSF's primary goal is to keep forwarding IP traffic. To reduce the amount of time a network is inaccessible to its users after a switchover, NSF collaborates with SSO. SSO is always used by Cisco NSF, which offers redundancy for Layer 3 communications.

upvoted 1 times

**Elburnio** 2 years, 7 months ago

NSR is correct IMO for this reason - NSR is for control plane and NSF is for data plane. wherever you need forwarding you should choose NSF and wherever you need Routing convergence , you should choose NSR.

upvoted 1 times

**ccnproute1** 2 years, 11 months ago

So which one is the correct answer. For me it feels more to be NSR, as the neighbor router does not understand GR. And gr are exchanged through routing protocol IS-IS. So with NSR the neighbor will not understand that there was a switchover

upvoted 1 times

**XalaGyan** 3 years, 1 month ago

**Selected Answer: B**

i stick also with B

NSR is an internal (vendor-specific) mechanism to extend the awareness of routing to the standby routing plane so that in case of failover, the newly active routing plane can take charge of the already established sessions.

https://www.ciscopress.com/articles/article.asp?p=1395746&seqNum=2

upvoted 1 times

**XalaGyan** 3 years, 1 month ago

sorry i meant to choose Option C. NSR is vendor specific and might not be supported everywhere.

upvoted 1 times

**Mohali98** 3 years, 3 months ago

**Selected Answer: B**

Graceful Restart (GR) (also known as Non Stop Forwarding (NSF)) and Non Stop Routing (NSR) are two different mechanisms to prevent routing protocol re-convergence during a processor switchover.

When Graceful Restart (NSF) is used, peer networking devices are informed, via protocol extensions prior to the event (so peers should also be NSF (GR) capable). The peer routers are aware of a failure and so will give the switching over router a "grace" period to re-establish the neighbor relationship, while continuing to forward to the routes from that peer.
When NSR is used, peer networking devices have no knowledge of any event on the switching over router. All information needed to continue the routing protocol peering state is transferred to the standby processor so it can "pick up" immediately upon a switchover. NSR is desirable in cases where the routing protocol peer doesn't support the RFCs necessary to support Graceful Restart.

Following this logic, the answer is B (NSR)

upvoted 4 times

**Reinier_veen** 3 years, 4 months ago

Selected Answer: B

https://community.cisco.com/t5/xr-os-and-platforms/nsr-nsf-and-graceful-restart/td-p/2212355

upvoted 1 times

**Sickcnt** 3 years, 4 months ago

Actually,

NSF does not exchange any GR messages with it's peer ( so NSF is the correct answer)

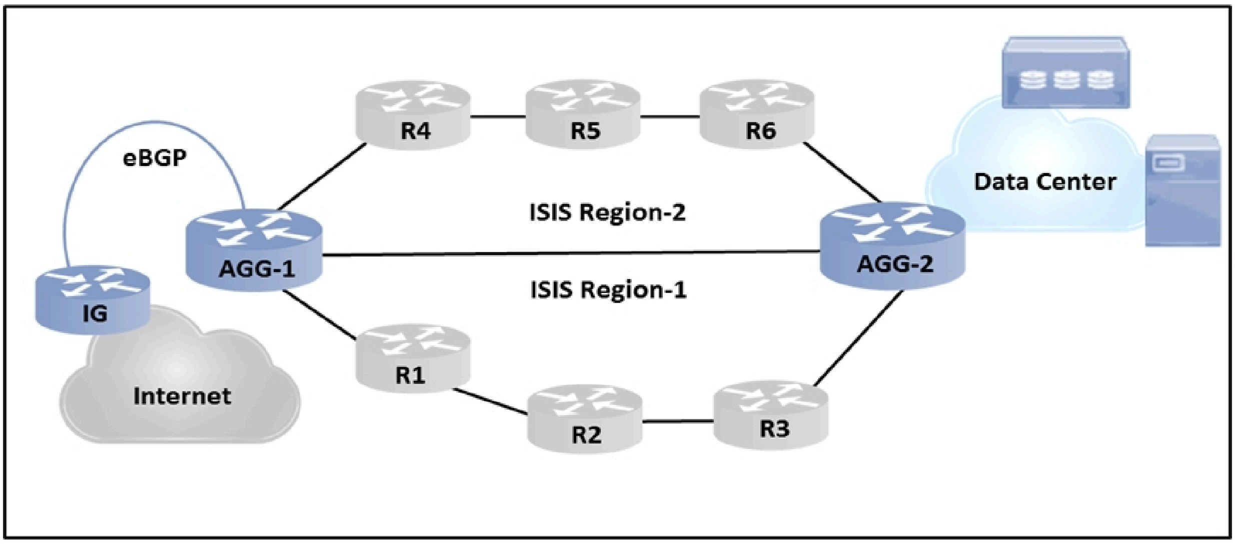
And NSR is indeed exchanging GR messages with the peer ( So its the incorrect answer)

Source:
https://forum.huawei.com/enterprise/en/difference-between-nsr-nsf-and-gr/thread/601106-861

upvoted 3 times

Question #37 *Topic 1*

Refer to the exhibit.



An architect must design an IGP solution for an enterprise customer. The design must support:

➾ Physical link flaps should have minimal impact.

➾ Access routers should converge quickly after a link failure.

Which two ISIS solutions should the architect include in the design? (Choose two.)

A. Use BGP to IS-IS redistribution to advertise all Internet routes in the Level 1 area.

B. Advertise the IS-IS interface and loopback IP address toward the Internet and data center.

C. Reduce SPF and PRC intervals to improve convergence time.

D. Configure all access and aggregate routers to establish Level 1 / Level 2 adjacencies across the network.

E. Configure access routers to establish a Level 1 adjacency and aggregate routers to establish a Level 1 / Level 2 adjacency.

**Correct Answer:** *CE*

*Community vote distribution*

CE (100%)

**Sickcnt** Highly Voted 2 years, 4 months ago

Selected Answer: CE

C and E is the correct answer

upvoted 5 times

**akbntc** Most Recent 1 year, 6 months ago

Selected Answer: CE

C and E are correct.

upvoted 1 times

**XalaGyan** 2 years, 1 month ago

Selected Answer: CE

correct answers are C and E

upvoted 1 times

**Sickcnt** 2 years, 4 months ago

C and E seems to be the correct Answers:

Answer C should be responsible for timer optimalization

Answer E should be the proper design in an "IS-IS Hybrid topology design"
(L1/L2 routers maintain a separate lin-state database for L1 routes and L2 routes > This increases their CPU > So Access routes should never be both

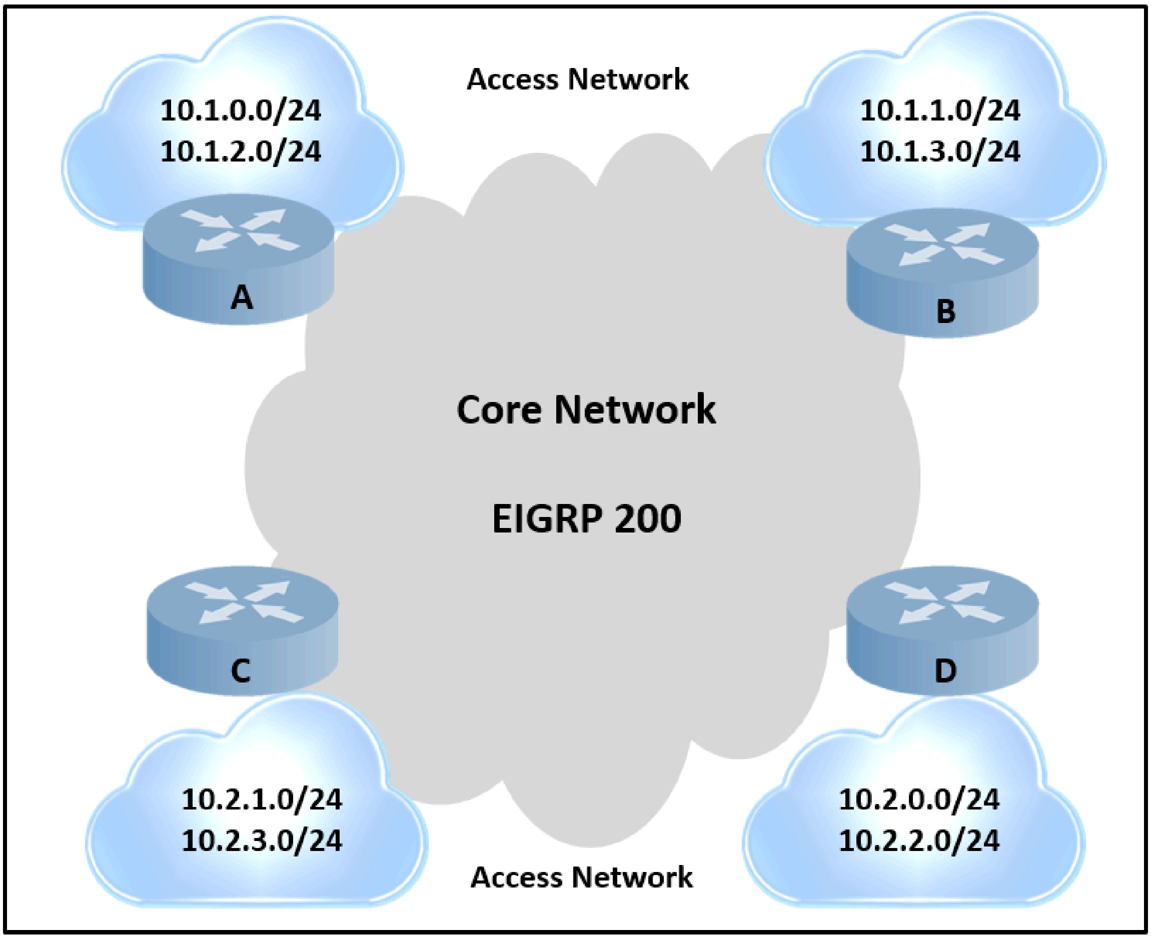
L1/L2 devices, only pure L1 devices)

(Source ENSLD 300-420 official cert book page: 119)

upvoted 4 times

Question #38 Topic 1

Refer to the exhibit.



An engineer is designing a routing solution for a customer. The design must ensure that a failure of network 10.1.0.0/24, 10.1.2.0/24, 10.2.1.0/24, or 10.2.3.0/24 does not impact the core. It also requires fast convergence time during any link failover in the core or access networks.

Which solution must the engineer select?

A. Add aggregation layer between core and access networks.

B. Enable graceful restart on routers A and C.

C. Enable FRR for the connected networks of routers A and C.

D. Enable summarization on routers A and C.

**Correct Answer:** *C*

*Community vote distribution*

C (56%) A (22%) D (22%)

**dougj** 4 months, 3 weeks ago

Selected Answer: A

I think the answer could be A here, although C looks very good until you read the question again. It says ...."It also requires fast convergence time during any link failover in the core or access networks". So the answer must also impact the Band D routers to. Answer A is the only answer that impacts the core and access layers.

upvoted 1 times

**1a17c3b** 6 months, 3 weeks ago

Selected Answer: C

Design Requirements

Failure of specific networks (10.1.0.0/24, etc.) must not impact the core

- This implies route isolation: the core shouldn't be burdened by instability from access networks.

Fast convergence during link failover

- This demands rapid rerouting, ideally sub-second, to maintain service continuity.

Best Solution:
C. Enable FRR for the connected networks of routers A and C
This meets the fast convergence requirement. However, D (summarization) is also valuable for route stability, especially to prevent access network flaps from impacting the core.

upvoted 1 times

**1a17c3b** 6 months, 3 weeks ago

**Selected Answer: C**

The best solution is C. Enable FRR for the connected networks of routers A and C
This meets the fast convergence requirement. However, D (summarization) is also valuable for route stability, especially to prevent access network flaps from impacting the core.

upvoted 1 times

**Guff89** 8 months ago

**Selected Answer: A**

Emily23 has a point. A summary route would include R2 as well.
Within EIGRP the summary route AD is 5 so i would not go with D

upvoted 1 times

**khazbimoas** 9 months, 1 week ago

**Selected Answer: D**

Correct is D. If 10.1.0.0/24, 10.1.2.0/24, 10.2.1.0/24, or 10.2.3.0/24 goes down, only the more-specific is withdrawn inside the access router. The /22 summary remains unchanged, so no query or route recomputation is triggered in the core EIGRP domain.

C is wrong because FRR on connected networks – speeds data-plane failover on a single router only; it does not prevent EIGRP query storms or LSDB growth across the core.

upvoted 1 times

**wolfone** 1 year ago

**Selected Answer: D**

The best solution is to enable summarization on routers A and C. This way, individual /24 subnet failures (10.1.x.x and 10.2.x.x) do not cause routing changes in the core (which only sees the summarized routes), thereby reducing convergence times and limiting the impact of failures on the core.

Fast Reroute (FRR) in EIGRP can provide sub-second convergence for link or node failures if there is an alternate path.
However, FRR does not hide route withdrawals from the core if the subnet itself fails (and there is no redundant path to that subnet).

upvoted 3 times

**wolfone** 1 year ago

**Selected Answer: D**

Correct Answer: D

upvoted 2 times

**26d13e9** 1 year, 4 months ago

**Selected Answer: A**

A......The FRR thing .....in order for it to be valid, it should not be only on routers A and C. On top of that, it still has impact (even though less but still has). Question says no impact.
option A however, completely hide the impact from the core. Plus its mentioned everywhere in the cisco material.

upvoted 1 times

**Clauster** 2 years, 1 month ago

**Selected Answer: C**

The answers are B & C
GraceFul Restart a feature in EIGRP that allows a router to gracefully restart without disrupting network traffic. When a router is configured for graceful restart, it will send a notification to its neighbors before it restarts. This allows the neighbors to prepare for the restart by building alternate routes to the networks that the router is advertising, it won't impact the core this way.

For Fast Convergence: (FRR) is a feature in EIGRP that allows a router to quickly reroute traffic around a failed link. FRR uses a technique called Feasible Successors to pre-calculate backup routes that can be used in the event of a link failure.

upvoted 3 times

**Emily23** 2 years, 2 months ago

It is A.
C?!... it is EIGRP. It uses DUAL.
D? Pls review CCNA subnetting and summarizing before posting.
upvoted 3 times

⊟ **Kacein** 1 year, 4 months ago

EIGRP Loop-Free Alternate (LFA) Fast Reroute (FRR) is a feature that allows EIGRP to switch to a backup path in less than 50 ms. Fast reroute means we switch to another next hop, Loop-free alternate is an alternative path in the network that is loop free.

Now you might be thinking that this sounds familiar. After all, EIGRP has feasible successors. Those are loop-free alternate paths that EIGRP has calculated. If the successor fails, EIGRP can use a feasible successor right away.

This is true, but there's one big "gotcha". EIGRP feasible successors are not installed in the routing table right away. Only the successor route is installed. When the successor fails, EIGRP installs the feasible successor, and this takes time. Fast reroute installs both the successor route and the feasible successor route in the routing table which makes convergence even faster.
upvoted 2 times

⊟ **SpicyMochi** 2 years, 4 months ago

**Selected Answer: C**

C. Enable FRR for the connected networks of routers A and C is the solution that the engineer should select.

FRR (Fast Reroute) is a mechanism that provides fast convergence times during any link or node failure. It works by precomputing alternate backup paths that can be used in case of a failure, eliminating the need for the router to go through a time-consuming SPF calculation. In this scenario, enabling FRR on the connected networks of routers A and C ensures that any failure of network 10.1.0.0/24, 10.1.2.0/24, 10.2.1.0/24, or 10.2.3.0/24 will not impact the core, and fast convergence time will be achieved during any link failover in the core or access networks.
upvoted 2 times

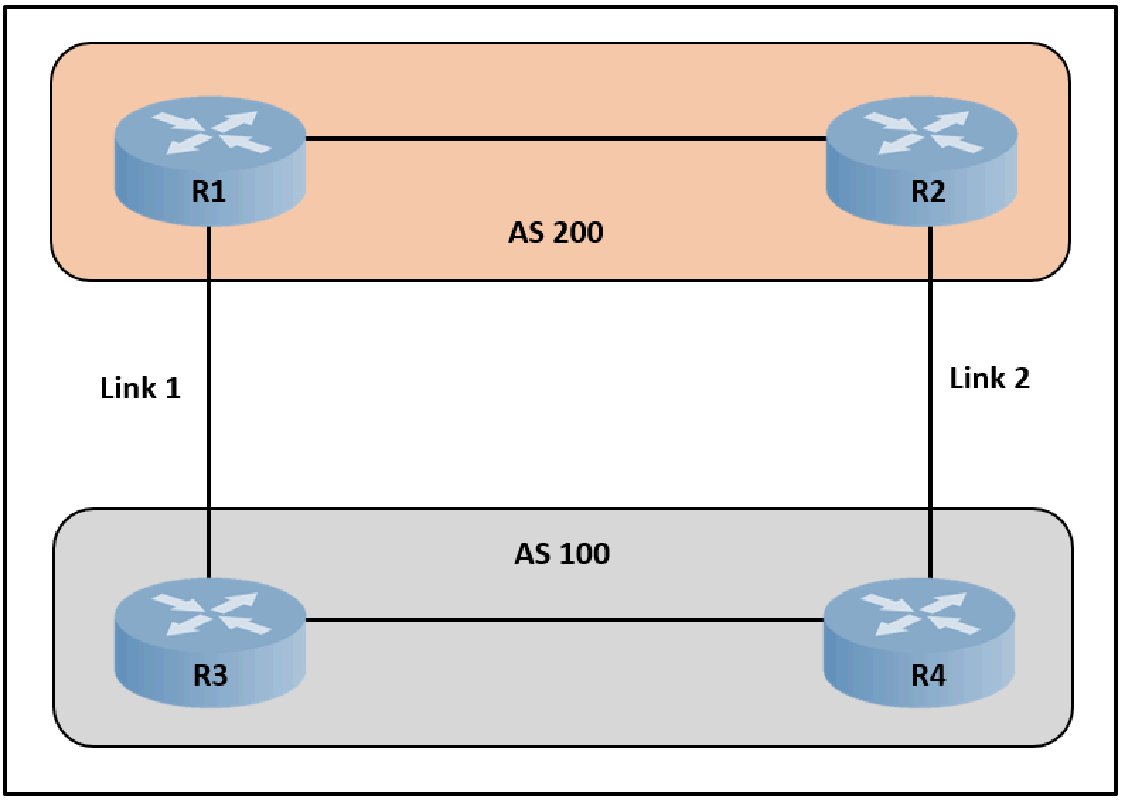
⊟ **cerifyme85** 2 years, 5 months ago

**Selected Answer: A**

I think the answer should be A and D
upvoted 1 times

Question #39 *Topic 1*

Refer to the exhibit.



A network engineer is designing a network for AS100. The design should ensure that all traffic enters AS100 via link 1 unless there is a network failure. In the event of a failure, link 2 should function as the path for incoming traffic. Which solution should the design include?

A. Modify the next-hop attribute on R3.

B. Use AS-Path prepending on R3.

C. Modify the next-hop attribute on R4.

D. Use AS-Path prepending on R4.

**Correct Answer:** *D*

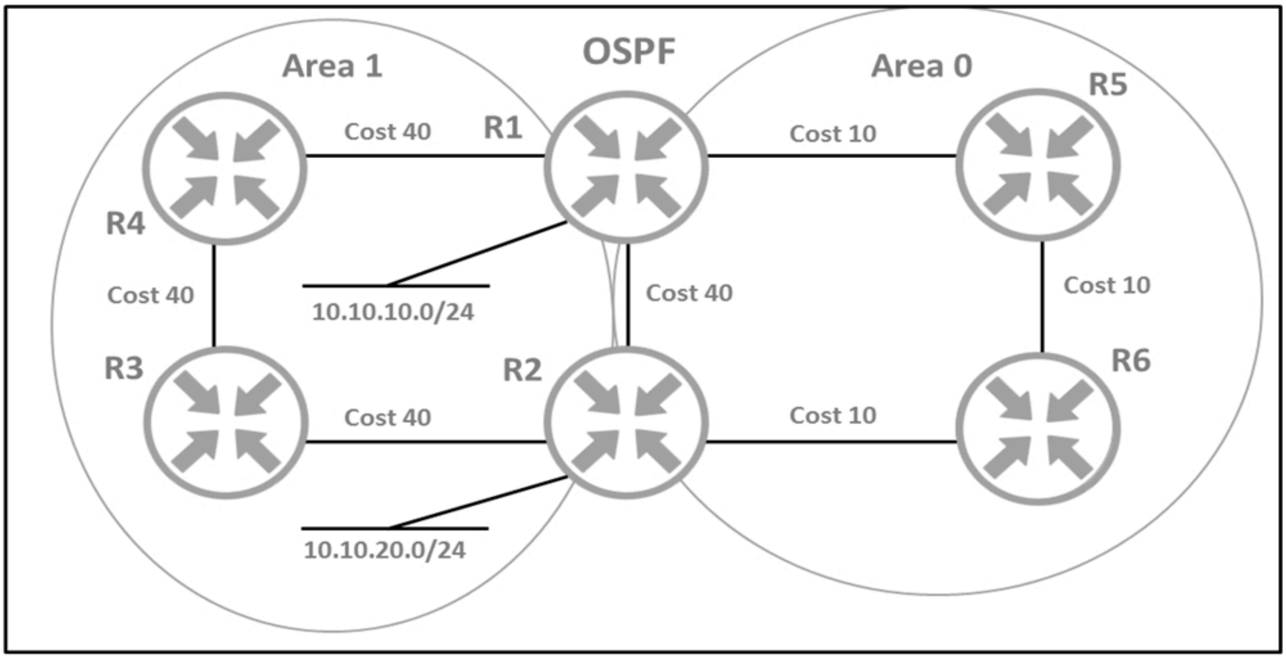
**Sickcnt** 1 year, 4 months ago

Answer D is 100% right

upvoted 2 times

Question #40 *Topic 1*

Refer to the exhibit.



An architect must design a solution that uses the direct link between R1 and R2 for traffic from 10.10.10.0/24 toward network 10.10.20.0/24. Which solution should the architect include in the design?

A. Configure the OSPF cost of the link to a value lower than 30.

B. Lower the Administrative Distance for OSPF area 0.

C. Place the link into area 2 and install a new link between R1 and R2 in area 0.

D. Configure the link to provide multiarea adjacency.

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**teems5uk** 1 year, 6 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/118879-configure-ospf-00.html#:~:text=Area%20Adjacency%20Configuration-,As%20previously%20mentioned%20%2C%20Multi%2DArea%20ADJ%20can%20be%20used%20to%20fo The%20OSPF%20ADJ

upvoted 1 times

**cooliday** 2 years, 1 month ago

Selected Answer: D

yep - I replicated this in a lab and can confirm - the correct answer is D

upvoted 2 times

**cerifyme85** 2 years, 5 months ago

weird question, but only logical answer seems to be D. I would have thought the cost would have an impact, but point-point link is an area 0 at cost 40, which is higher than the other cost in area 0.

upvoted 1 times

**Tiamat** 2 years, 9 months ago

Selected Answer: D

D is the right answer

upvoted 1 times

**andrewChan** 2 years, 10 months ago

Selected Answer: D

OSPF first look at the prefered path list as below and secondly compare path metric:

Intra-Area (O)

Inter-Area (O IA)

External Type 1 (E1)

NSSA Type 1 (N1)

External Type 2 (E2)

NSSA Type 2 (N2)

so most apporiate answer is to configure R1-R2 link as multiarea adjacency.

under the interface configuration mode:

ip ospf network point-to-point

ip ospf multi-area 1

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/118879-configure-ospf-00.html

upvoted 1 times

⊟ **Eards** 2 years, 10 months ago

Am I missing something it is routing in area 0 and you need to avoid using R5 and R6 and go direct in same area. A: Lower the cost of link between the R1-R2, to be less than R1-R5-R6-R2

upvoted 1 times

⊟ **Eards** 2 years, 10 months ago

missed networks are in area 1 - D could be correct https://ipwithease.com/ospf-multi-area-adjacency-example-scenario/

upvoted 1 times

⊟ **leo_591** 2 years, 11 months ago

la respuesta es D

upvoted 2 times

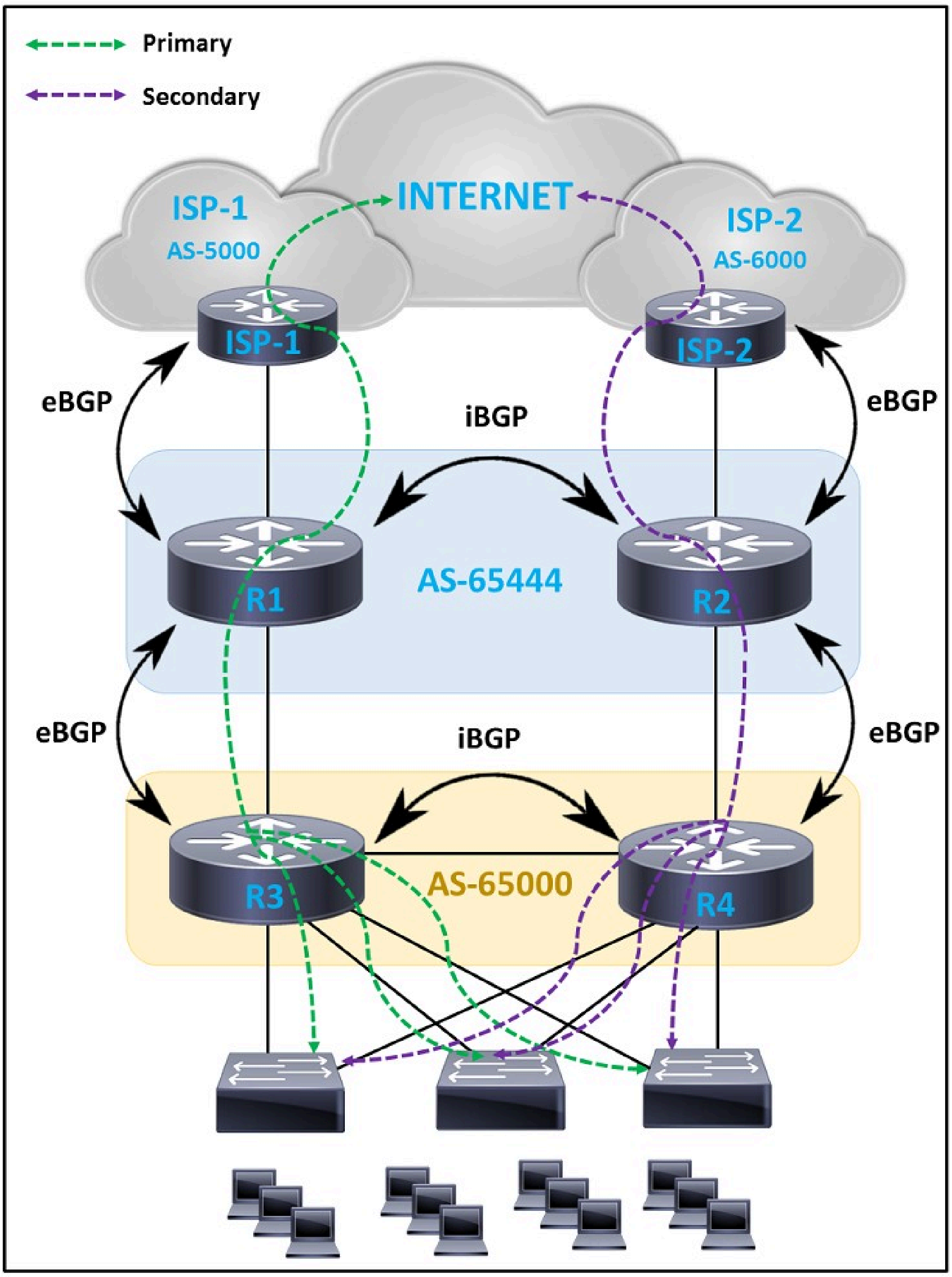
⊟ **SlyNZ99** 2 years, 11 months ago

Selected Answer: D

default path selection preference for OSPF is Intra-Area first before even looking and Inter-Area routes. After alot of reading multi-area adjancy is the only real logical answer

upvoted 4 times

Refer to the exhibit.



An engineer must design a WAN solution so that ISP-1 is always preferred over ISP-2. The path via ISP-2 is considered as a backup and must be used only when the path to ISP-1 is down. Which solution must the engineer choose?

A. R1: - Routes advertised to ISP-1: 0x AS-path prepend - Routes received from ISP-1: HIGH local-preference - Routes advertised to R2: no action - Routes received from R2: community NO-EXPORT R2: - Routes advertised to ISP-2:5x AS-path prepend - Routes received from ISP-2: LOW local-preference - Routes advertised to R1: community NO-ADVERTISE - Routes received from R1: no action

B. R1: - Routes advertised to ISP-1: 0x AS-path prepend - Routes received from ISP-1: HIGH local-preference - Routes advertised to R2: community NO-EXPORT - Routes received from R2: no action R2: - Routes advertised to ISP-2: 5x AS-path prepend - Routes received from ISP-2: LOW local-preference - Routes advertised to R1: no action - Routes received from R1: no action

C. R1: - Routes advertised to ISP-1: 0x AS-path prepend - Routes received from ISP-1: LOW local-preference - Routes advertised to R2: community NO-ADVERTISE - Routes received from R2: no action R2: - Routes advertised to ISP-2: 5x AS-path prepend - Routes received from ISP-2: HIGH local-preference - Routes advertised to R1: no action - Routes received from R1: community NO-ADVERTISE

D. R1: - Routes advertised to ISP-1: 5x AS-path prepend - Routes received from ISP-1: LOW local-preference - Routes advertised to R2: community NO-ADVERTISE - Routes received from R2: no action R2: - Routes advertised to ISP-2: 0x AS-path prepend - Routes received from

ISP-2: HIGH local-preference - Routes advertised to R1: community NO-EXPORT - Routes received from R1: no action

**Correct Answer:** *B*

*Community vote distribution*

A (50%) B (50%)

**johnu329** Highly Voted 2 years, 11 months ago

B is correct.

- Routes advertised to ISP-1 do NOT need to have AS-path prepend
- Routes advertised to ISP-2 need to have AS-path prepend
- Routes received from ISP-1 need to have HIGH local-preference
- Routes received from ISP-2 need to have LOW local-preference

---> This already rules out C and D

- NO-ADVERTISE to internal routers is wrong (R1 and R2 should each know both paths)

--> This rules out A.

upvoted 10 times

**jahax** 1 year, 8 months ago

I am not sure, about your last sentence. Its not that R2 with NO-ADVERTISE will not send its network to R1, it will but R1 will not redistribute them anywhere else (e/iBGP), as we sends this community from R2. Based on the drawing, and having limited konwledge of rest of the config, it can rule out that R1 is still able to reach Internet via R2, and inform about this R3 which will preffer it as its eBGP and still act as gateway. I will vote for A.

upvoted 1 times

**jahax** 1 year, 8 months ago

Ok and now I just found that A/B differ also in direction in quesiton...

A: R2 out>R1 (mark as NO-ADV), while R2> in R1 (mark as NO-EX)

B: R1 our>R2 (mark as NO-EX)

upvoted 1 times

**LearnMachine** Most Recent 6 months, 3 weeks ago

Selected Answer: B

Simple explanation here, from my point of view.

B:

* FROM R1 *

NO AS-path prepend to ISP1

Routes Received from ISP1 - give it high local-preference so the traffic out is via ISP1

Routes Sent to R2 - set community NO-EXPORT so you are not a transit network

Routes received from R2 - no action as you will not receive any routes from R2 because BGP advertise only the best route, and the best route from R2 will be R1 as per higher local preference

* FROM R2 *

set 5x AS-path prepend to ISP2 - so the return traffic is from ISP1

Routes Received from ISP2 - give it low local-preference so the traffic out is via R1>ISP1

Routes Sent to R1 - No action as BGP send only the best route and the best route is R1 (Because local preference set to high on R1), no risk of transit network as you will NOT advertise what you learned from ISP2

Routes received from R1 - no action as that will be your select best routes.

upvoted 1 times

**Beehurls** 1 year, 1 month ago

Selected Answer: B

I do not need to address C and D, because it is easy to see ISP1 needs no AS-path prepend and higher local preference and ISP2 needs the opposite to favor ISP1.

The confusion is with A and B, which differ for the path from/to AS-5000. So for A, it is telling R1 not to advertise anything from R2 and R2 is telling R1 the same. The diagram is showing that the primary path should go through R3 to R1, but R2 still can advertise R1's ISP to R4 and then R4 can go through R2-R1-ISP1.

With answer B, R1 is telling R2 not to pass on any advertisements it gives it to anyone outside of the AS. So, now R3 and R4 will only know the path to ISP1 through R1 and will also still get the ISP2 path through R2.

upvoted 2 times

**samael666** 1 year, 3 months ago

**Selected Answer: A**

from Enterprise LAN point, if I advertised to R2 prefixes with community no export and R1 is down, what happens is that, INTERNET doesn't known my LAN so there is no conectivity, instead If advertised to R1 as no-advertise community doesn't happen anything in AS 65444, the election will be in INTERNET, and here will select the short AS-PATH atribute.

upvoted 1 times

**Beehurls** 1 year, 1 month ago

R1:

- Routes advertised to ISP-1: 0x AS-path prepend
- Routes received from ISP-1: HIGH local-preference
- Routes advertised to R2: community NO-EXPORT
- Routes received from R2: no action

R2:

- Routes advertised to ISP-2: 5x AS-path prepend
- Routes received from ISP-2: LOW local-preference
- Routes advertised to R1: no action
- Routes received from R1: no action

Answers should look like this. R2 will still receive the LAN routes from R4.

upvoted 1 times

**26d13e9** 1 year, 4 months ago

i dont know.......B is correct on all except the NO-EXPORT to R2. In case of ISP1 failure, how will internal routes be advertised to ISP2 if routes advertised to R2 have NO-EXPORT ?? internet will not be able to have customer routes. Am I missing something ?

upvoted 1 times

**26d13e9** 1 year, 4 months ago

Hmmm I guess we dont internal advertised to ISP......but in this case dont we need to do the same for R1 ?

upvoted 1 times

**Sickcnt** 2 years, 10 months ago

In answer B:

"Routes advertised to R2: community NO-EXPORT"

This seems very weird, because if we give out this community that would mean that Route 2 wouldn't advertise the routes towards ISP2 (AS-6000) even if the route towards R1 and ISP1 failed...

So ALL the answers seem to be incorrect (but I guess answer B makes the most sense)

Please correct me if I'm wrong tho

upvoted 1 times

**cerifyme85** 2 years, 4 months ago

Doesn't advertise learned routes to ebgp, but can stilff form ebgp peers with another AS. I guess we use the no-export to avoid R2 becoming a transit AS

upvoted 1 times

**cerifyme85** 2 years, 4 months ago

it also uses the no-export to advertise to ISP's ibgp

upvoted 1 times

Question #42 *Topic 1*

Which feature must be incorporated into the campus LAN design to enable Wake on LAN?

A. dynamic ARP Inspection Snooping on layer 2 devices

B. directed broadcasts on layer 3 devices

C. proxy ARP on layer 3 devices

D. DHCP Snooping on layer 2 devices

**Correct Answer:** *B*

*Community vote distribution*

B (86%) 14%

**htchapme** 1 year, 7 months ago

Answer is B.

configure ip directed-broadcast.

upvoted 2 times

**iLikeHamburgers** 1 year, 11 months ago

**Selected Answer: B**

"the routers must be configured to allow directed broadcasts"

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/91672-catl3-wol-vlans.html

upvoted 1 times

**certstudent2016** 2 years, 4 months ago

**Selected Answer: B**

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/91672-catl3-wol-vlans.html

upvoted 1 times

**cwoolie** 2 years, 4 months ago

Answer is B. WOL requires directed broadcasts

upvoted 1 times

**roganjosh** 2 years, 6 months ago

**Selected Answer: B**

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/91672-catl3-wol-vlans.html

Answer is B

upvoted 4 times

**jpml91** 2 years, 6 months ago

From CCNP Enterprise Design ENSLD 300-420 Official Cert Guide

" If you send WoL packets from remote networks, the routers must be configured to allow directed broadcasts."

Answer is B

upvoted 3 times

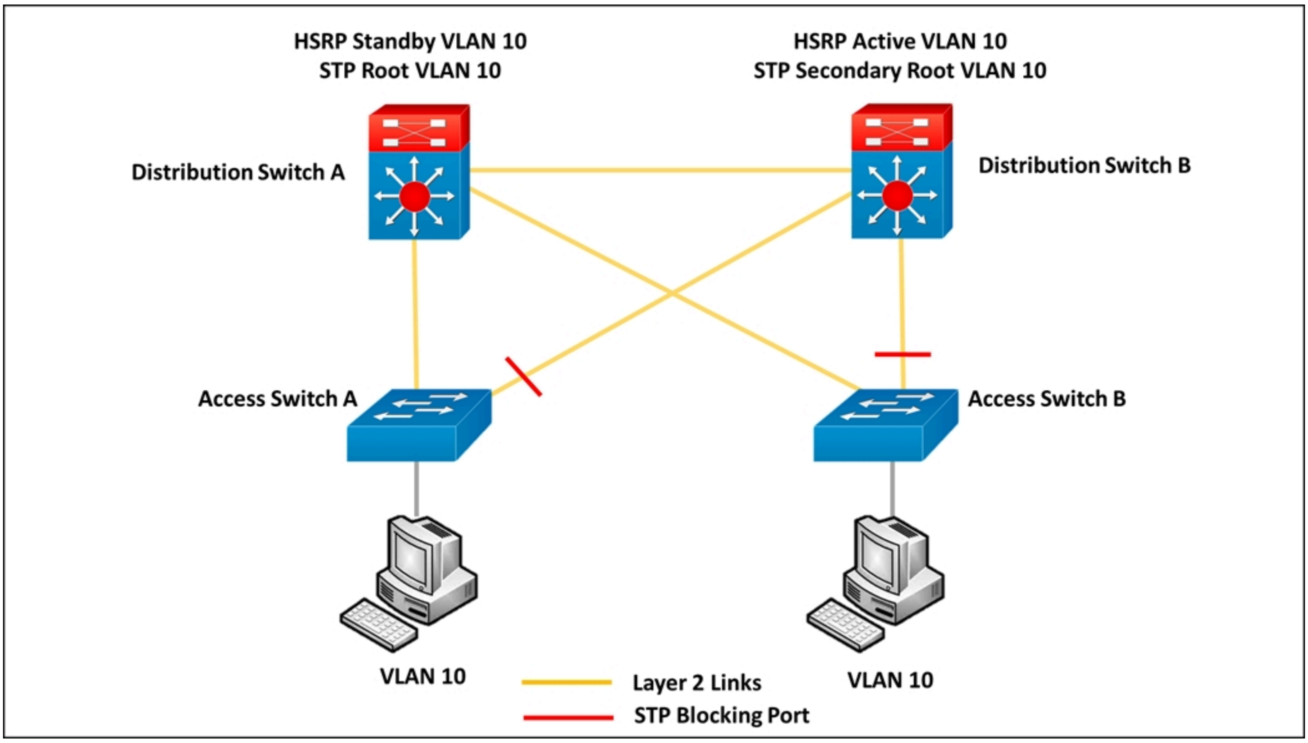
**configt** 2 years, 6 months ago

**Selected Answer: D**

WAKE ON LAN IS A LAYER 2 YOU WOULD NEED DHCP HELPER

upvoted 1 times

Question #43 *Topic 1*



Refer to the exhibit. An engineer must optimize the traffic flow of the network. Which change provides a more efficient design between the access layer and the distribution layer?

A. Add a link between access switch A and access switch B

B. Reconfigure the distribution switch A to become the HSRP Active

C. Change the link between distribution switch A and distribution switch B to be a routed link

D. Create an EtherChannel link between distribution switch A and distribution switch B

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**XalaGyan** 1 year, 7 months ago

Selected Answer: B

Reconfigrue Distribution-SW-A to be HSRP Active

upvoted 1 times

**leo_591** 1 year, 11 months ago

Es la resouesta correcta

upvoted 1 times

Question #44 *Topic 1*

Which first hop redundancy protocol ensures that load balancing occurs over multiple routers using a single virtual IP address and multiple virtual MAC addresses?

A. GLBP

B. IRDP

C. VRRP

D. HSRP

**Correct Answer:** *A*

**Reinier_veen** 1 year, 4 months ago

keyword is "multiple" here? (more than 2)

upvoted 1 times

**cwoolie** 1 year, 10 months ago

A is correct. GLBP is first hop

upvoted 1 times

Question #45 *Topic 1*

A company with multiple service providers wants to speed up BGP convergence time in the event a failure occurs with their primary link. Which approach achieves this goal and does not impact router CPU utilization?

A. Utilize BFD and tune the multiplier to 50

B. Lower the BGP hello interval

C. Decrease the BGP keepalive timer

D. Utilize BFD and keep the default BGP timers

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**goku2020** Highly Voted 👍 4 years, 3 months ago

Correct is D

upvoted 22 times

**jn4voip** Highly Voted 👍 4 years, 2 months ago

Decreasing the BGP timer would increase the hellos, thereby increasing CPU use

upvoted 10 times

**minon_bob** Most Recent 🕒 1 year, 8 months ago

**Selected Answer: D**

Internet is not a stable network, setting the holdtimer too low will be bad to router CPU as the route will keep on withdrawing and adding.

upvoted 1 times

**Eards** 2 years, 4 months ago

**Selected Answer: D**

Voting D - Agree with the rest

upvoted 4 times

**cwoolie** 2 years, 11 months ago

Answer is. D

upvoted 1 times

**cwoolie** 2 years, 11 months ago

I have D as answer..Please correct

upvoted 1 times

**mazinhoo** 2 years, 11 months ago

correct is D, "because some parts of BFD cab be distributed to the data plane , it can be less CPU-intensive than the reduced protocol timers , which exist wholly at the control plane"

upvoted 1 times

**roganjosh** 3 years ago

**Selected Answer: D**

Answer is D, Leaving a Vote

upvoted 3 times

**rgigs** 3 years, 2 months ago

Correct is D

upvoted 1 times

**John_Aung** 3 years, 5 months ago

I would like to know what is the correct answer? please ?

upvoted 1 times

**Xavi07** 3 years, 7 months ago

the answer is D

upvoted 1 times

⊟ **luisjuradoledesma** 4 years, 1 month ago

I think the answer should be D - the issue is to speed up BGP convergence time in the event a FAILURE occurs and keep the CPU utilisation low - then BFD is the solution

upvoted 5 times

⊟ **poetmj** 4 years, 1 month ago

I think the Answer is D. BFD can be configured with subsecond convergence

upvoted 5 times

## Question #46 *Topic 1*

An engineer is designing an enterprise campus network. The LAN infrastructure consists of switches from multiple vendors, and Spanning Tree must be used as a
Layer 2 loop prevention mechanism. All configured VLANs must be grouped in two STP instances. Which standards-based Spanning Tree technology supports this design solution?

A. MSTP

B. RSTP

C. Rapid PVST

D. STP

**Correct Answer:** *A*

**cwoolie** 1 year, 4 months ago

A.MSTP is correct

upvoted 3 times

Question #47 *Topic 1*

A network engineer must segregate three interconnected campus networks using IS-IS routing. A two-layer hierarchy must be used to support large routing domains and to avoid more specific routes from each campus network being advertised to other campus network routers automatically. Which two actions does the engineer take to accomplish this segregation? (Choose two.)

A. Designate two IS-IS routers as BDR routers at the edge of each campus, and configure one BDR for all Level 1 routers and one BDR for all Level 2 routers.

B. Designate two IS-IS routers from each campus to act as Level 1/Level 2 backbone routers at the edge of each campus network.

C. Assign the same IS-IS NET value for each campus, and configure internal campus routers with Level 1/Level 2 routing.

D. Utilize different MTU values for each campus network segment. Level 2 backbone routers must utilize a larger MTU size of 9216.

E. Assign a unique IS-IS NET value for each campus, and configure internal campus routers with Level 1 routing.

**Correct Answer:** *BE*

**neiker45** 1 year, 3 months ago

A. Remember that level 2 is necessary for inter-area communication so both should be level 1/2. Wrong.

B. The routers having two levels allows them to communicate intra and inter area, passing packets as necessary. Correct

C. The NET value is unique and cannot be the same. Plus, having internal routers handling level 1/2 is not efficient as they use 2 different tables. The level 2 won't be used. Wrong.

D. MTU in this situation has nothing to do with the prompt. Wrong

E. Internal routers use level 1 and unique NET IDs. Correct

upvoted 1 times

**akbntc** 1 year, 6 months ago

B & E are correct.

upvoted 1 times

Question #48 *Topic 1*

Which consideration must be taken into account when using the DHCP relay feature in a Cisco SD-Access Architecture?

A. DHCP-relay must be enabled on fabric edge nodes to provide the correct mapping of DHCP scope to the local anycast gateway.

B. A DHCP server must be enabled on the border nodes to allow subnets to span multiple fabric edges.

C. DHCP servers must support Cisco SD-Access extensions to correctly assign IPs to endpoints in an SD-Access fabric with anycast gateway.

D. DHCP Option-82 must be enabled to map the circuit IP option to the access fabric node where the DHCP discover originated.

**Correct Answer:** *D*

*Community vote distribution*

D (75%) A (25%)

**iSDA69** 4 months, 3 weeks ago

Selected Answer: C

I'm adding a different POV after asking Google AI that I hope could help the reasoning:

A: "This statement is factually true, but it is not the most critical consideration for the overall architecture to function".
Anyway, to be precise, the DHCP relay function does not provide "the correct mapping of DHCP scope to the local anycast gateway".

B: is totally wrong.

C: It says the right answer is C because "the most important consideration is that the DHCP server understand the SD-ACCESS extensions to lease the ip address correctly...as it would not be able to differentiate between DHCP requests originating from different edge nodes...". The DHCP extensions in general are a real thing.

D: "This statement is also factually true, and it is a crucial component of the DHCP relay process in SD-Access. However, the statement is slightly misleading by referring to a "circuit IP option"".
This "circuit IP option" actually does not exists, and the option-82 does not contain the info of the user who sent the DHCP discover.

upvoted 1 times

**J2J2J2J** 1 year, 8 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/sda_dhcp/b_cisco_sda_dhcp.html

upvoted 2 times

**minon_bob** 1 year, 8 months ago

Selected Answer: D

The ip Anycast is the problem with DHCP and SDA. So the ip relay information option has to be set, it is by DNAC automagically, for DHCP to work in the fabric.

https://community.cisco.com/t5/networking-knowledge-base/dhcp-in-the-fabric/ta-p/3918003

upvoted 2 times

**iLikeHamburgers** 2 years, 2 months ago

Selected Answer: D

Answer A is partially correct, because there is a need to have a the DHCP Discover packet relayed to the DHCP server, however the mapping of the client to the correct DHCP scope is not done with the anycast gateway, it is done within the DHCP Option82 sub options.This is needed because every edge device in the fabric has the same anycast gateway. There would be no way for the DHCP server to get the request back to the originating requestor with out the sub options from Option 82, specifically the source RLOC. Look under “Fabric DHCP Packet Flow” in the link below
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

upvoted 1 times

**Eards** 2 years, 4 months ago

Selected Answer: D

Answer D

upvoted 1 times

⊟ **Kevinbob** 2 years, 4 months ago

ANSWER D https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/sda_dhcp/b_cisco_sda_dhcp.html

upvoted 2 times

⊟ **simcos** 2 years, 6 months ago

**Selected Answer: D**

Regarding answer A, yes the feature is enabled on the edge nodes, but the rest of the sentence doesn't make sense.
The option 82 is used to map the DHCP request to the Edge device where it was originated (via RLOC).
https://community.cisco.com/t5/networking-knowledge-base/dhcp-in-the-fabric/ta-p/3918003#toc-hId--1229221529

upvoted 1 times

⊟ **Kamran202034** 2 years, 7 months ago

**Selected Answer: A**

There is not such a thing as "access fabric node" in SD-Access and unless there is typo, there is not such a thing as "circuit IP"; It is circuit ID! so if answer wording in the exam is as exactly as mentioned here I will go with A

upvoted 2 times

⊟ **Hope66** 2 years, 9 months ago

The answer could be A: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/sda_dhcp/b_cisco_sda_dhcp.html
Paragraf : Host DHCP Onboarding Process

upvoted 2 times

⊟ **cwoolie** 2 years, 11 months ago

Answer is D

upvoted 1 times

⊟ **cwoolie** 2 years, 11 months ago

Answer is D

upvoted 1 times

⊟ **cwoolie** 2 years, 11 months ago

I have answer as D

upvoted 1 times

⊟ **roganjosh** 3 years ago

**Selected Answer: D**

Answer is D, adding for a vote

upvoted 4 times

⊟ **Xavi07** 3 years, 7 months ago

I think A is the correct.

upvoted 3 times

⊟ **kakito** 3 years, 10 months ago

I think "A" is corret, Is true that OPTION 82 is used, however its a feature that is and should be automatically added by the FENs. Therefore the Relay-agent has to be the FEN Fabric Edge Node.

upvoted 3 times

Question #49 *Topic 1*

Which function are fabric intermediate nodes responsible for in an SD-Access Architecture?

A. mapping EIDs to RLOCs

B. encapsulating user traffic in a VXLAN header including the SGT

C. registering new endpoints in the HTDB

D. transporting IP packets between edge nodes and border nodes

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**bccabrera** 1 year, 3 months ago

**Selected Answer: D**

The intermediate node can be an intermediate router or extended switch that only provides underlay services in the Software Defined Access fabric.

upvoted 1 times

**certstudent2016** 2 years, 4 months ago

**Selected Answer: D**

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

upvoted 1 times

**Audie** 2 years, 6 months ago

D is Corect: Intermediate nodes are part of the Layer 3 network used for interconnections among the devices operating in a fabric role such as the interconnections between border nodes and edge nodes. These interconnections are created in the Global Routing Table on the devices and is also known as the underlay network.

upvoted 4 times

Question #50 *Topic 1*

How do endpoints inside an SD-Access network reach resources outside the fabric?

A. a VRF fusion router is used to map resources in one VN to another VN

B. Fabric borders use VRFs to map VNs to VRFs

C. SD-Access transit links are used to transport encapsulated traffic from one fabric to another

D. A fabric edge is used to de-encapsulate VXLAN traffic to normal IP traffic then transported over the outside network

**Correct Answer:** *B*

*Community vote distribution*

B (58%) D (33%) 8%

**aai5548** Highly Voted 4 years, 1 month ago

I think it's B.

Not A; VN to another VN is not external to the fabric, so this is not what we need here.
Could be B; your VN will be mapped to a VRF, and so providing access to networks outside the SDA.
Not C; fabric to fabric; nope.
Not D; fabric edge is device connecting clients, not providing external access (that's a border node's job).

upvoted 16 times

**Ranx01** Highly Voted 4 years, 1 month ago

I think the answer is B - "Fabric border routers handle the ingress & egress traffic for the SD-Access fabric, they are responsible for translating the policy, VRF & SGT information between the SD-Access fabric and the external networks." Boson ExSim-Max for Cisco 350-401 ENCOR. Reference Cisco SD-Access Solutions Design Guide (CVD): SD-Access Solutions Components.

upvoted 13 times

**i_krezz** Most Recent 1 month, 3 weeks ago

Selected Answer: B

VRF route leaking is not mandatory for traffic to leave the fabric so B is the correct answer. D is by far the most wrong anwser since edge nodes encapsulate, they do not de-encapsulate the traffic when it leaves the fabric

upvoted 1 times

**night_wolf_in** 2 months, 3 weeks ago

Selected Answer: B

Fabric Border needs to be used. not edge.

upvoted 1 times

**1a17c3b** 6 months, 3 weeks ago

Selected Answer: B

Key Concepts
Fabric Edge Nodes: Connect endpoints to the fabric
Fabric Border Nodes: Connect the fabric to external networks
Virtual Networks (VNs): Logical segmentation within the fabric
VRFs (Virtual Routing and Forwarding): Used to isolate routing tables per VN
VXLAN: Used inside the fabric for encapsulation

Correct Answer
B. Fabric borders use VRFs to map VNs to VRFs
This is how SD-Access connects internal VNs to external networks
Each VN inside the fabric is mapped to a corresponding VRF on the border node
This allows policy enforcement and segmentation to be preserved outside the fabric

Incorrect Answer
D. A fabric edge is used to de-encapsulate VXLAN traffic to normal IP traffic then transported over the outside network

VXLAN de-encapsulation is done by border nodes, not edge nodes

Edge nodes are for endpoint access, not external routing

upvoted 1 times

⊟ **1a17c3b** 6 months, 3 weeks ago

Selected Answer: D

I used the help of copilot to help me find the correct answer to this question and it advised D.

upvoted 2 times

⊟ **khazbimoas** 9 months, 1 week ago

Selected Answer: D

D is correct.

upvoted 2 times

⊟ **PSETGS** 1 year, 7 months ago

Selected Answer: B

Fabric borders use VRFs to map VNs to VRFs: This method uses VRFs to map VNs to VRFs at the fabric border. The fabric border is the edge of the fabric where it connects to other networks or services. The VRFs are used to separate the traffic between different VNs, and they are used to route the traffic between the fabric and the outside networks.

upvoted 1 times

⊟ **Clauster** 1 year, 7 months ago

Selected Answer: D

This question is not even fair, All of the answers are actually correct, these are methods that Endpoints use to get to the Outside Resources. However, Answer D has to be the best answer as the Edge Node is the first Node the Endpoints reach so that traffic leaves the Fabric. Crazy question and i doubt we will get this one on the exam because of how uncertain the question is.

upvoted 3 times

⊟ **minon_bob** 1 year, 8 months ago

Selected Answer: A

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.

upvoted 2 times

⊟ **DOSKIM** 1 year, 11 months ago

it is definelty D

upvoted 1 times

⊟ **teddyberry** 2 years ago

Selected Answer: D

Obviously Border node is an exit to external networks, but in the answer D, they are saying about "fabric edge" (they do not say "Edge node"), so if they mean that Border node is a "fabric edge", which is true, the rest of the sentence is also true, that's why D might is correct. That's tricky answer, so I am not sure.

upvoted 3 times

⊟ **iLikeHamburgers** 2 years, 5 months ago

Selected Answer: B

Answer A is not correct as the Fusion Routers have no concept of a VN. Only the Fabric Borders and Fabric Edges use VN's.

ENSLD 300-420 CCNP Enterprise Design Official Cert Guide

Chapter 10: SD-Access Design page 334

"The border design for the SD-Access fabric involves connectivity to the outside or external networks."

As aai5548 already mentioned, the question states "access to the outside", B is the only that facilitates this.

upvoted 1 times

⊟ **zlimvos** 2 years, 9 months ago

Selected Answer: B

Whatever it is doing, it is the border node doing it, so I will go for B 'border router'

upvoted 1 times

⊟ **cwoolie** 2 years, 10 months ago

Im going with B. I don't like how A answer is worded. VRF Fusion Router?

upvoted 1 times

⊟ **cwoolie** 2 years, 11 months ago

Answer is B

upvoted 1 times

⊟ **mazinhoo** 2 years, 11 months ago

i think its B ,

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

upvoted 2 times

Question #51 *Topic 1*

When vEdge router redundancy is designed, which FHRP is supported?

A. HSRP

B. OMP

C. GLBP

D. VRRP

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

⊟ **guerreroa25** 10 months ago

**Selected Answer: D**

The correct answer is D. VRRP (Virtual Router Redundancy Protocol).

upvoted 1 times

⊟ **SpicyMochi** 1 year, 4 months ago

**Selected Answer: D**

The correct answer is D. VRRP (Virtual Router Redundancy Protocol).

vEdge router redundancy is designed to provide high availability and failover capabilities in a network. VRRP is the supported First Hop Redundancy Protocol (FHRP) for vEdge routers because it is an open standard protocol (defined in RFC 5798) that allows for router redundancy in IP networks.

upvoted 1 times

⊟ **iLikeHamburgers** 1 year, 11 months ago

**Selected Answer: D**

CCNP Enterprise Design Official Cert Guide
ENSLD 300-420
Chapter 11: SD-WAN Design page 357
“It can be accomplished by using VRRP from the switches infrastructure or Layer 3 routing from a Layer 3 switch or router.”

upvoted 2 times

Question #52 Topic 1

What is the purpose of an edge node in an SD-Access network fabric?

A. Edge nodes identify and authenticate endpoints and register endpoint information with control plane nodes.

B. Edge nodes track endpoint IDs to location mappings, along with IPv4, IPv6, or MAC addresses.

C. Edge nodes are the gateway between the fabric domain and network outside of the fabric.

D. Edge nodes resolve lookup requests from edge and border nodes to locate destination endpoint IDs.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Emily23** 1 year, 8 months ago

(A)

A fabric edge node provides onboarding and mobility services for wired users and devices (including fabric-enabled WLCs and APs) connected to the fabric. It is a LISP tunnel router (xTR) that also provides the anycast gateway, endpoint authentication, and assignment to overlay host pools (static or DHCP), as well as group-based policy enforcement (for traffic to fabric endpoints).

ENCOR cert guide, chapter 22

upvoted 2 times

**Sickcnt** 2 years, 4 months ago

**Selected Answer: A**

Edge Node:

"As soon as Endpoints gets connected to edge node, it gets added to Local tracking database often called as EID table of edge node. Now Edge node send the LISP MAP register message to inform control plane node about the endpoint so that control plane registers that EID in its HTDB."

Source:

https://www.dclessons.com/sd-access-solution-components

upvoted 4 times

Question #53 *Topic 1*

Which component of Cisco SD-Access integrates with Cisco DNA Center to perform policy segmentation and enforcement through the use of security group access control lists and security group tags?

A. Cisco Application Policy Infrastructure Controller Enterprise Module

B. Cisco Network Data Platform

C. Cisco Identity Services Engine

D. Cisco TrustSec

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**SpicyMochi** 1 year, 4 months ago

**Selected Answer: C**

The correct answer is C. Cisco Identity Services Engine (ISE).

Cisco ISE integrates with Cisco DNA Center to perform policy segmentation and enforcement in an SD-Access network. It uses security group access control lists (SGACLs) and security group tags (SGTs) to enforce policies based on user and device profiles. ISE enables the creation and management of these security policies, ensuring that proper access is granted based on user and device identity.

upvoted 2 times

**cerifyme85** 1 year, 4 months ago

**Selected Answer: C**

SGT ==> DNAC + ISE

While SGTs are administered by Cisco ISE through the tightly integrated REST APIs, Cisco DNA Center is used as the pane of glass to manage and create SGTs and define their policies.

upvoted 2 times

**cerifyme85** 1 year, 4 months ago

SGT ==> DNAC + ISE

While SGTs are administered by Cisco ISE through the tightly integrated REST APIs, Cisco DNA Center is used as the pane of glass to manage and create SGTs and define their policies.

TrustSec--> Just a term

Cisco TrustSec is an umbrella term for security improvements to Cisco network devices based on the capability to strongly identify users, hosts and network devices within a network. TrustSec provides topology independent and scalable access controls by uniquely classifying data traffic for a particular role. TrustSec ensures data confidentiality and integrity by establishing trust among authenticated peers and encrypting links with those peers.

The key component of Cisco TrustSec is the Cisco Identity Services Engine. It is typical for the Cisco ISE to provision switches with TrustSec Identities and Security Group ACLs (SGACLs), though these may be configured manually.

upvoted 1 times

**DOSKIM** 1 year, 5 months ago

IT IS TRUSTSEC

upvoted 1 times

**iLikeHamburgers** 1 year, 8 months ago

**Selected Answer: C**

also if you look at the OCG, pg330, it says "Cisco ISE is a critical component of SD-Access for policy enforcement..."

upvoted 2 times

**iLikeHamburgers** 1 year, 11 months ago

**Selected Answer: C**

Answer is C

"The key component of Cisco TrustSec is the Cisco Identity Services Engine."

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/trustsec.pdf

upvoted 2 times

**SergeBesse** 1 year, 11 months ago

**Selected Answer: C**

C is the correct answer. Cisco ISE is a sd-access component. Cisco trustsec is a feature

upvoted 2 times

**Kamran202034** 2 years, 1 month ago

**Selected Answer: C**

C is correct.

Policy management with identity services is enabled in an SD-Access network using ISE integrated with Cisco DNA Center for dynamic mapping of users and devices to scalable groups.

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

upvoted 2 times

**python_tamer** 2 years, 2 months ago

I'm torn between C and D.

Trustsec is the name of the feature.

But it's ISE that actually pushes SGTs and SGACLs to the NADs.

DNAC is a single pane of glass to manage it.

So I think the answer is more likely to be C because ISE has to be integrated with DNAC for Trustsec to work in SDA.

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

upvoted 1 times

**Xavi07** 3 years, 1 month ago

Yes, it-s trustsec

upvoted 3 times

**luisjuradoledesma** 3 years, 7 months ago

Effectively, it's Cisco TrustSec - ISE is for identity context, authentication, posture validation, etc

Cisco TrustSec - Security provided by Cisco TrustSec ® infrastructure (Security Group Tags [SGT], SGACLs) and Cisco segmentation capabilities (Cisco Locator/ID Separation Protocol [LISP], VXLAN, and Virtual Routing and Forwarding [VRF]).

Identity context for users and devices, including authentication, posture validation, and device profiling, provided by the Cisco ISE.

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-09-sda-faq-cte-en.html

upvoted 4 times

**CCNPWILL** 3 years, 2 months ago

Correct. Answer is D.

upvoted 2 times

Question #54 *Topic 1*

Which design element should an engineer consider when multicast is included in a Cisco SD-Access architecture?

A. PIM SSM must run in the underlay.

B. Multicast clients reside in the underlay, and the multicast source is outside the fabric or in the overlay.

C. Rendezvous points must be used in a PIM SSM deployment.

D. Multicast traffic is transported in the overlay and the EID space for wired and wireless clients.

**Correct Answer:** *D*

Reference:

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKEWN-2020.pdf

Slide 113

*Community vote distribution*

D (40%) A (40%) C (20%)

**goku2020** Highly Voted 4 years, 9 months ago

Client mulicast or receiver resides inside overlay. Both for source.

D is correct.

See page # 87 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 12 times

**iLikeHamburgers** 2 years, 8 months ago

its on page 105

"Multicast traffic is transported in the overlay, in the EID space, for both wired and wireless clients."

upvoted 1 times

**luisjuradoledesma** Highly Voted 4 years, 7 months ago

D is correct - please, refer to: Multicast traffic is transported in the overlay, in the EID space, for both wired and wireless clients

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKEWN-2020.pdf

upvoted 7 times

**chivastaba** 1 year, 9 months ago

Link was updated. Refer to page 133 of 138

https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2020/pdf/BRKEWN-2020.pdf

upvoted 2 times

**LearnMachine** Most Recent 6 months, 2 weeks ago

Selected Answer: D

Is not A because the wording users is MUST.

We could use native multicast with PIM-SSM but we could also use the overlay.

So PIM-SSM is not a must.

upvoted 1 times

**TheGorn** 1 year, 8 months ago

Selected Answer: A

A follows the CBT Nuggets explanation

upvoted 1 times

**XalaGyan** 2 years, 7 months ago

Selected Answer: A

i will go with PIM SSM in the underlay as first things to do.

https://community.cisco.com/t5/networking-knowledge-base/cisco-sd-access-multicast/ta-p/4068110

upvoted 1 times

**iLikeHamburgers** 2 years, 11 months ago

**Selected Answer: C**

Answer is C.

CCNP Enterprise Design Official Cert Guide

ENSLD 300-420 Ch 10 : SD-Access Design page 340

"Both PIM Source-Specific Multicast(SSM) and PIM-Sparse Mode are supported with SD-Access. When using IP multicast in the overlay, the use of a RP is required."

upvoted 1 times

**A_Wolf** 3 years, 2 months ago

**Selected Answer: D**

Provided explanation is clear - D

upvoted 1 times

**Xavi07** 4 years, 1 month ago

Luis Jurado is right. D is correct

ulticast traffic is transported in the overlay, in the EID space, for both wired and wireless clients

page 113 of his link

upvoted 1 times

**poetmj** 4 years, 7 months ago

Am assuming we are talking about the overlay in which case i think it is C. "Multicast sources can be supported both inside and outside the SD-Access fabric. With PIM implementations, a rendezvous point (RP) is used on the border for all multicast clients in the overlay. The multicast protocol configurations can be done within Cisco DNA Center.Both PIM Source-Specific Multicast (SSM) and PIM–Sparse Mode are supported with SD-Access. When using IP multicast in the overlay, the use of a RP is required. Multicast Source Discovery Protocol (MSDP) can be used for RP redundancy, if desired"

upvoted 1 times

Question #55 *Topic 1*

What is the role of a control-plane node in a Cisco SD-Access architecture?

A. fabric device that connects wired endpoints to the SD-Access fabric

B. map system that manages endpoint to device relationships

C. fabric device that connects APs and wireless endpoints to the SD-Access fabric

D. map system that manages External Layer 3 networks

**Correct Answer:** *B*

Reference:

https://netaavi.com/my-blog-1/f/overview-of-sda-fabric-solution

*Community vote distribution*

B (100%)

**DOSKIM** 1 year, 5 months ago

correct

upvoted 1 times

**iLikeHamburgers** 1 year, 11 months ago

**Selected Answer: B**

CCNP Enterprise Design Official Cert Guide

ENSLD 300-420 Ch 10 : SD-Acces Design page 333

"The database for identifying endpoints is the responsibility of the fabric control plane nodes in the SD-Access fabric. "

upvoted 1 times

## Question #56 *Topic 1*

How is end-to-end microsegmentation enforced in a Cisco SD-Access architecture?

A. VLANs are used to segment traffic at Layer 2.

B. 5-tuples and ACLs are used to permit or deny traffic.

C. SGTs and SGTACLs are used to control access to various resources.

D. VRFs are used to segment traffic at Layer 3.

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**DOSKIM** 1 year, 5 months ago

correct

upvoted 1 times

**iLikeHamburgers** 1 year, 11 months ago

**Selected Answer: C**

CCNP Enterprise Design Official Cert Guide

ENSLD 300-420 Ch10 : SD-Access Design page 334

"Segmentation adds to unified policy by enabling VRF instance/VN (macro) and SGT (micro) segmentation to be deployed in the SD-Access fabric."

upvoted 1 times

Question #57 *Topic 1*

Which two border nodes are available in the Cisco SD-Access architecture? (Choose two.)

A. extended border

B. edge border

C. internal border

D. anywhere border

E. intermediate border

**Correct Answer:** *CD*

*Community vote distribution*

CD (100%)

**RexChen** Highly Voted 3 years, 6 months ago

so CD is right , A is extended

upvoted 9 times

**ExodiaNecross59** Highly Voted 4 years, 2 months ago

There are 3 types of border nodes in SD-Access:

External. Default exit from fabric with no specific routes injection

Internal. Gateway only for a set of networks, such as shared services prefixes

Anywhere. Combination of external and internal functionality

upvoted 9 times

**aydot** Most Recent 1 year, 7 months ago

Selected Answer: CD

There are 3 types of border nodes in SD-Access:

External. Default exit from fabric with no specific routes injection

Internal. Gateway only for a set of networks, such as shared services prefixes

Anywhere. Combination of external and internal functionality

upvoted 1 times

**DOSKIM** 1 year, 11 months ago

CD right

upvoted 1 times

**Reinier_veen** 2 years, 4 months ago

Selected Answer: CD

External

Internal

Anywhere

upvoted 3 times

**zlimvos** 2 years, 9 months ago

C and D

A is 'extended' not 'external'

upvoted 1 times

**certstudent2016** 2 years, 10 months ago

Selected Answer: CD

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

Unless A option is changed to External

upvoted 1 times

**brzl** 2 years, 10 months ago

Selected Answer: CD

SD-Access knows only Internal, External and Anywhere roles for border nodes.

upvoted 1 times

⊟ **cwoolie** 2 years, 11 months ago

C,D is answer

upvoted 1 times

⊟ **cwoolie** 2 years, 11 months ago

C,D is answer

upvoted 1 times

⊟ **roganjosh** 3 years ago

**Selected Answer: CD**

CD is correct

upvoted 2 times

Question #58 *Topic 1*

Which control-plane protocol is used to map an endpoint to a location in a Cisco SD-Access network?

A. FabricPath

B. IS-IS

C. LISP

D. MP-BGP

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**bccabrera** 1 year, 3 months ago

**Selected Answer: C**

The SD-Access fabric control plane is based on the Locator/ID Separation Protocol (LISP). LISP eliminates router processing for every IP destination address and route by moving the remote destination information to the LISP Map Server (MS), a centralized mapping database, and a control plane node in SD-Access. The LISP MS allows the routers to manage their local routes and query the map system to locate destination Endpoint Identifiers (EIDs).

It provides SD-Access benefits such as smaller routing tables, dynamic host mobility for wireless and wired network endpoints, and built-in network segmentation via VRF instances. Cisco SD-Access also includes distributed Anycast Gateway, VN Extranet, and Fabric Wireless.

upvoted 1 times

Question #59 *Topic 1*

Which feature is required for graceful restart to recover from a processor failure?

A. Cisco Express Forwarding

B. Virtual Switch System

C. Stateful Switchover

D. Bidirectional Forwarding Detection

**Correct Answer:** *C*

*Community vote distribution*

C (91%) 9%

⊟ **goku2020** Highly Voted 👍 4 years, 3 months ago

C => stateful switchover

upvoted 7 times

⊟ **SpicyMochi** Most Recent 🕒 1 year, 10 months ago

Selected Answer: C

The correct answer is C. Stateful Switchover (SSO).

Stateful Switchover (SSO) is a feature that allows graceful restart to recover from a processor failure in a network device. SSO enables a device to maintain its forwarding capability while recovering from a processor failure, minimizing the impact on network traffic. This is accomplished by synchronizing the control plane information between the active and standby processors in the device. In the event of a processor failure, the standby processor takes over the control plane functions without causing any disruption to the forwarding plane.

upvoted 2 times

⊟ **DOSKIM** 1 year, 11 months ago

Cc is correct

upvoted 1 times

⊟ **iLikeHamburgers** 2 years, 2 months ago

Selected Answer: C

This is a tricky question.
In the OCG pg 168 it states "Graceful Restart (GR), also known as Non-Stop Forwarding..."
So Graceful Restart and Non-Stop Forwarding are one in the same.
Now looking at the this site
https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftbgpnsf.html
it states "SSO is a prerequisite of NSF". So going by what the OCG said above, and after reading the link above, what we can conclude is SSO is a prerequisite of Graceful Restart.

upvoted 2 times

⊟ **mgiuseppe86** 1 year, 5 months ago

You need to learn how to read. Answer A is Cisco Express Forwarding, not NON-STOP Forwarding. Two completely different things. CEF is a layer 2 switching mechanism. NSF is a protocol in junction with SSO

upvoted 1 times

⊟ **python_tamer** 2 years, 9 months ago

Selected Answer: C

I say C.
CEF is required for uninterrupted traffic flow, yes, but....
SSO is required for GR to work at all and this is what is asked in the question.

upvoted 2 times

⊟ **cwoolie** 2 years, 11 months ago

C is answer

upvoted 1 times

**Audie** 3 years ago

"Cisco NSF is supported by the BGP, EIGRP, OSPF, and IS-IS protocols for routing and by Cisco Express Forwarding (CEF) for forwarding"

upvoted 1 times

**MaestroGJE** 3 years, 2 months ago

A is correct... (although it migh seem strange...)
I found this:
In Cisco networking devices, packet forwarding is provided by
Cisco Express Forwarding.
Cisco Express Forwarding maintains the FIB
and uses the FIB information that was
current at the time of the switchover to

continue forwarding packets during a switchover.

The ability to continue packet forwarding
------------------------------------------------------------------ eliminates downtime during the switchover.----- i find it here:
https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd801dc5e2.html

upvoted 2 times

**Waiemzh** 3 years, 2 months ago

Selected Answer: C

C is 100% correct

upvoted 3 times

**rgigs** 3 years, 2 months ago

C is correct

upvoted 1 times

**BW1001** 3 years, 4 months ago

C !
The Stateful Switchover (SSO) feature works with Nonstop Forwarding (NSF) in Cisco software to minimize the amount of time a network is unavailable to its users following a switchover. The primary objective of SSO is to improve the availability of networks constructed with Cisco routers.

upvoted 1 times

**Xavi07** 3 years, 8 months ago

Is A:
Cisco Express Forwarding for NSF
A key element of NSF is packet forwarding. The OSPF protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once OSPF has converged, CEF updates the Forwarding Information Base (FIB) table and removes stale route entries. CEF then updates the line cards with the new FIB information. CEF maintains the FIB and uses the FIB information that was current at the time of a switchover to continue forwarding packets during the switchover. This feature reduces traffic interruption during the switchover.

upvoted 2 times

**CCNPWILL** 3 years, 8 months ago

Easy. C SSO

upvoted 2 times

**aai5548** 4 years, 1 month ago

I think it is A.
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. In Cisco networking devices, packet forwarding is provided by Cisco Express Forwarding. Cisco Express Forwarding maintains the FIB and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. The ability to continue packet forwarding eliminates downtime during the switchover.

Each protocol depends on Cisco Express Forwarding to continue forwarding packets during switchover, while the routing protocols rebuild the Routing Information Base (RIB).

https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd801dc5e2.html

upvoted 2 times

**CCNPWILL** 3 years, 8 months ago

Totally off base. CEF is for hardware based forwarding. nothing to do with this tech.
upvoted 1 times

⊟ **mgiuseppe86** 1 year, 5 months ago

Bro learn how to read. A is CEF, not NSF. Just because you see the word "Fowarding" doesnt mean its NSF.
upvoted 1 times

⊟ **ExodiaNecross59** 4 years, 2 months ago

I don't know.. It's probably "A" belong this : https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/high-availability/solution_overview_c22-487228.html

GR and NSR, when coupled with SSO provide the foundation for fast recovery from a processor failure and allow the use of ISSU to perform software upgrades with little downtime. SSO is necessary to handle other non routing protocol related items needed for the router to operate following a switchover. These include syncing the complete router configuration, Cisco Express Forwarding (CEF) forwarding entries and other needed information to the standby processor.
upvoted 2 times

⊟ **kudasay** 4 years, 3 months ago

C is correct! - GR is the only feature that interacts with peer network devices, all other
features (SSO/NSF/NSR) are internal to the router and therefore don't
require standards.
Source: https://archive.nanog.org/meetings/nanog42/presentations/Weissner_SSO.pdf
upvoted 4 times

Question #60 *Topic 1*

An architect is designing a network that will utilize the spanning tree protocol to ensure a loop-free topology. The network will support an engineering environment where it is necessary for end-users to connect their own network switches for testing purposes. Which feature should the architect include in the design to ensure the spanning-tree topology is not affected by these rogue switches?

A. BPDU Skew Detection

B. BPDU guard

C. loop guard

D. root guard

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**certstudent2016** Highly Voted 👍 2 years, 4 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html

As I mentioned earlier dont trust posts from cwoolie

upvoted 7 times

**wolfone** Most Recent ⏱ 1 year ago

Selected Answer: D

The better solution, in my opinion, would be "bpdu filter", but it's not in the list!

upvoted 1 times

**DOSKIM** 1 year, 5 months ago

D is the way to go with

upvoted 1 times

**Mohali98** 1 year, 9 months ago

Selected Answer: D

D is the right answer ... root guard is the required feature

upvoted 2 times

**Hope66** 2 years, 4 months ago

Rogue switch could become the new root switch. This can influence the spanning-tree topology

I think that the answer is D (root guard)

upvoted 2 times

**cwoolie** 2 years, 4 months ago

This should be loop guard not root guard.

upvoted 2 times

**zlimvos** 2 years, 2 months ago

No. bpgu guard: don't allow any switch to connect on your STP. root guard: allow switch to connect but with lower priority.

upvoted 1 times

**johnu329** 1 year, 11 months ago

If you were to use bpdu guard, it would no longer be possible "for end-users to connect their own network switches for testing purposes". Their switches may send BPDU's and therefore the port would not become operation.

So, in this case you would choose: root guard

That way, they will be able to connect their switches, yet no topology change will occur.

upvoted 3 times

Question #61 *Topic 1*

An engineer is designing a Layer 3 campus network running EIGRP between the core, aggregation, and access layers. The access layer switches will be connected to the aggregation layer using Layer 3 copper connections. The engineer wants to improve the convergence time for access layer switch failures.
Which technique must the design include?

A. enabling BFD for EIGRP on the access layer uplinks

B. reducing the EIGRP Hello / Hold timer values

C. EIGRP summarization from core to aggregation layer

D. EIGRP summarization from access to aggregation layer

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**NoHombre** 5 months, 2 weeks ago

**Selected Answer: D**

It's D:
When an access switch fails (power down or link down) on direct L3 copper uplinks, the physical link drops and the EIGRP neighborship on the aggregation switch tears down immediately. Failure detection isn't the bottleneck; the bigger factor in EIGRP convergence is bounding the query domain when many connected routes behind the access switch disappear at once.

upvoted 1 times

**12504a3** 6 months ago

**Selected Answer: B**

I disagree, answer should be B :
- Yes BFD can help to reduce convergence time, but option A told us to enable it only in access layer, not in aggregation layer as well. BFS must be enabled in both ends.
- Cisco documentation "recommends in the Layer 3 campus design that the EIGRP hello and dead timers be reduced to 1 and 3 seconds, respectively" ... "Reducing the EIGRP hello and hold timers from defaults of 5 and 15 seconds provides for a faster routing convergence in the rare event that L1/2 remote fault detection fails"

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/routed-ex.html#pgfId-1027653

upvoted 1 times

**SpicyMochi** 1 year, 4 months ago

**Selected Answer: A**

The correct answer is A. enabling BFD for EIGRP on the access layer uplinks.

Bidirectional Forwarding Detection (BFD) is a protocol used to quickly detect failures in the forwarding path between two adjacent devices. By enabling BFD for EIGRP on the access layer uplinks, the engineer can significantly improve the convergence time for access layer switch failures. BFD works independently of the routing protocol and can provide faster failure detection than relying on routing protocol timers alone.

upvoted 2 times

Question #62 *Topic 1*

An existing network solution is using BFD in echo mode. Several network devices are experiencing high CPU utilization, which an engineer has determined is related to the BFD feature. Which solution should the engineer leverage to reduce the CPU load?

A. Implement slow timers between peers with low CPU resources.

B. Implement BFD asynchronous mode between peers with low CPU resources.

C. Enable BFD multi-hop on the devices with low CPU resources.

D. Utilize carrier delay on all routers in the network.

**Correct Answer:** *A*

*Community vote distribution*

A (80%) B (20%)

**1a17c3b** 6 months, 3 weeks ago

**Selected Answer: B**

Key Concepts: BFD Modes
Echo Mode:
- One device sends echo packets; the peer loops them back.
- High CPU usage because it requires packet processing in software.
- Not ideal for devices with limited CPU resources.
Asynchronous Mode:
- Both devices send control packets at regular intervals.
- Lower CPU impact, especially when hardware-assisted.
- Preferred in most modern deployments.

Option Analysis
A. Implement slow timers between peers with low CPU resources
Reducing timer frequency can help, but it increases failure detection time
Doesn't address the root cause: echo mode's CPU intensity
🚫 Not optimal

B. Implement BFD asynchronous mode between peers with low CPU resources
Asynchronous mode is less CPU-intensive and often hardware-accelerated
Ideal for reducing CPU load while maintaining fast failure detection
✅ Best solution

upvoted 2 times

**kolp** 1 year, 1 month ago

**Selected Answer: B**

The BFD feature that uses less CPU usage is BFD asynchronous mode.

upvoted 3 times

**244afa3** 1 year, 8 months ago

This question of kind of tricky.
BFD has echo mode and echo disable mode (aynchronous mode).
echo mode waits for bfd packets from opposite router and the session goes down.
On the other hand, the session goes down without bfd packet from the opposite router on echo disable mode.
But i am not sure if changing from echo mode to asynchronous mode lowers cpu usage.
so i guess i will go with the answer A

upvoted 1 times

**Clauster** 2 years, 7 months ago

The BFD feature that uses less CPU usage is BFD asynchronous mode. In asynchronous mode, BFD sessions are initiated independently by each router in a BFD adjacency. This means that each router sends BFD packets periodically, regardless of whether or not it has received any BFD packets from its neighbor.

In contrast, BFD synchronous mode requires both routers in a BFD adjacency to agree on the interval at which BFD packets are sent. This means that both routers must be synchronized, which can require more CPU resources.

Additionally, BFD asynchronous mode does not require BFD packets to be acknowledged. This means that BFD packets can be sent and received more quickly, which can also reduce CPU usage.
upvoted 1 times

**Clauster** 2 years, 6 months ago
Sorry Folks, Answer is going to be A

https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fs_bfd.html#wp1221586
upvoted 2 times

**bccabrera** 2 years, 9 months ago
A y B son las dos válidas. Pero con A aumentas el tiempo de convergencia y con B estás cambiando el modo de funcionamiento del BFD. No te especifica qué es lo que puedes cambiar. Pues a saber.
upvoted 1 times

**SpicyMochi** 2 years, 10 months ago
Selected Answer: B
The correct answer is B. Implement BFD asynchronous mode between peers with low CPU resources.

Bidirectional Forwarding Detection (BFD) has two modes of operation: echo mode and asynchronous mode. In echo mode, BFD packets are sent back and forth between peers, and the forwarding plane handles the processing, which can lead to high CPU utilization.

In asynchronous mode, BFD control packets are sent periodically between peers, and the control plane handles the processing. Asynchronous mode is less CPU-intensive compared to echo mode. Thus, implementing BFD asynchronous mode between peers with low CPU resources can help reduce the CPU load on these network devices.
upvoted 4 times

**Emily23** 2 years, 8 months ago
When echo mode, the BFD packet loops back through the interface of the peer without processing. What you are saying is not logic.

If you invoke control plane, than it's deffinetly using CPU.
upvoted 3 times

**Sickcnt** 3 years, 4 months ago
Selected Answer: A
"...Finally, “BFD can use the slow timer to slow down the asycnhronous session when the echo function is enabled and reduce the number of BFD control packets that are sent between two BFD neighbors.”

That is, BFD echo can go fast without interrupting the CPU, and since that will detect an outage, you don’t need BFD control packets running as often, since the control packets aren’t being used for the rapid detection function. That in turn lightens the CPU load and allows more use of BFD. Clever!"

Source:
https://netcraftsmen.com/clarifying-bfd-and-bfd-echo/
upvoted 4 times

**zlimvos** 3 years, 9 months ago
Selected Answer: A
SLow timers is correct. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/interfaces/configuration/guide/if_cli/if_bfd.html
Unde BFD echo function " BFD can use the slow timer to slow down the asycnhronous session when the echo function is enabled and reduce the number of BFD control packets that are sent between two BFD neighbors. "
upvoted 4 times

Question #63 Topic 1

How is a sub-second failure of a transport link detected in a Cisco SD-WAN network?

A. Hellos are sent between the WAN Edge routers and the vSmart controller.

B. BFD runs on the IPsec tunnels between WAN Edge routers.

C. BGP is used between WAN Edge routers and the vSmart controller.

D. Link state change messages are sent between vSmart controllers.

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**XalaGyan** 1 year, 5 months ago

**Selected Answer: B**

Provided answer is correct

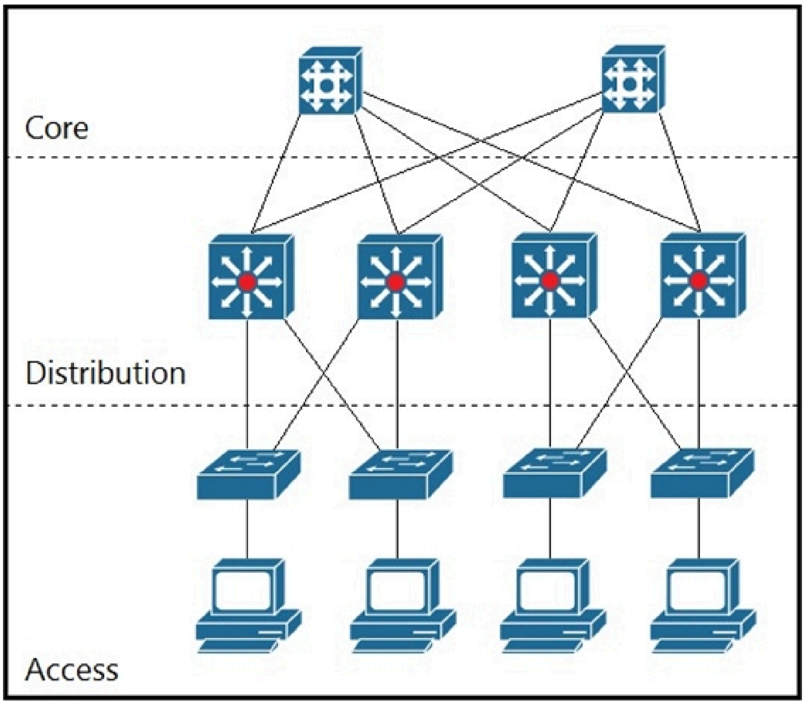
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/m-network.html

BFD Protocol
The Role of BFD in Cisco SD-WAN Solution
The BFD protocol detects links failures between routers. It measures data loss and latency on the data tunnel to determine the status of the devices at either end of the connection.

For data plane resiliency, the Cisco SD-WAN software implements the BFD protocol, which runs automatically on the secure IPsec and GRE connections between routers. These connections are used for the data plane, and for data traffic, and are independent of the DTLS tunnels used by the control plane.

upvoted 3 times

## Question #64 Topic 1



Refer to the exhibit. Which two solutions maximize the use of the links between the core and distribution layers? (Choose two.)

A. use multiple equal-cost links

B. use an IGP

C. use HSRP

D. use RPVSTP+

E. use multiple unequal-cost links

**Correct Answer:** *AB*

*Community vote distribution*

AB (100%)

XalaGyan Highly Voted 2 years, 11 months ago

Selected Answer: AB

Refer to the exhibit. Which two solutions maximize the use of the links between the core and distribution layers? (Choose two.)

A. use multiple equal-cost links ==> looks good

B. use an IGP ==> is mandatory to do equal/non-equal load balancing

C. use HSRP ==> not bad but that is First Hop Failure and belongs between Access and Distribution layer

D. use RPVSTP+ ==> layer 2 technology, has nothing to do between those layers

E. use multiple unequal-cost links ==> nice but to make that decision more details of the links are needed and since they are not given, A is the better choice

Answer: AB

upvoted 6 times

cerifyme85 1 year, 11 months ago

unequal only supported for eigrp anyway, question did not specify.. other IGPs will use equal cost

upvoted 1 times

bubd Most Recent 1 year, 6 months ago

Options B (use an IGP), C (use HSRP), and D (use RPVSTP+) are not directly related to maximizing link utilization between the core and distribution layers.

upvoted 1 times

Question #65 *Topic 1*

A customer's current Layer 2 infrastructure is running Spanning Tree 802.1d, and all configuration changes are manually implemented on each switch. An architect must redesign the Layer 2 domain to achieve these goals:
* reduce the impact of topology changes
* reduce the time spent on network administration
* reduce manual configuration errors
Which two solutions should the architect include in the new design? (Choose two.)

A. Implement Rapid PVST+ instead of STP.

B. Implement MST instead of STP.

C. Use VTP to propagate VLAN information and to prune unused VLANs.

D. Configure broadcast and multicast storm control on all switches.

E. Configure dynamic trunking protocol to propagate VLAN information.

**Correct Answer:** *AC*

*Community vote distribution*

AC (60%) | BC (30%) | 10%

**jddalo** Highly Voted 3 years, 9 months ago

I think its A & C

upvoted 11 times

**26d13e9** Most Recent 1 year, 4 months ago

B can not work with C. The basic idea of MSTP is to have all vlans configured on all interfaces. If this is the case, then you can not have something like VTP disturbing that system via going around and pruning vlans. If we are choosing C, then the other one may be A.

upvoted 1 times

**LSLS55** 1 year, 11 months ago

Lets not forget this is a Cisco exam and unless stated that another vendor is used or a specific protocol is not compatible, go with Cisco proprietary protocols. I would say it's A and C.

upvoted 2 times

**Clauster** 2 years ago

Selected Answer: AC

Realistically speaking A and C are the best answers.
MSTP requires you to configure each switch manually causing more administrative overhead. It's also fishy that the answer said "MST" instead of MSTP so that's another reason i am choosing A instead of B.

upvoted 3 times

**Clauster** 2 years, 1 month ago

Selected Answer: BC

Answers are B & C please hear me out so you don't get this wrong on the exam.
- We need a Protocol that is best suited to reduce admin overhead (RSTP and MSTP are both suited)
- We need a protocol that helps us reduce VLAN configuration, this is without a doubt VTP.
- We need a protocol that reduces MANUAL CONFIGURATION, unfortunately RSTP does not meet this requirement because you have to configure everything manually on every switch in the network therefor leaving MSTP as the our only and final winner. Hope this helps you guys.

upvoted 1 times

**Clauster** 2 years, 1 month ago

Selected Answer: BC

The correct answers are B & C
Rapid PVST+ requires too much manual configuration on it's ports, one of the requirements is to reduce Administrator Overhead, you reduce Admin Overhead with MST, MSTP is the entire reason you can run it on Data Centers because of how many VLANs can be ran.
VTP Allows VLAN to flow through out the Network again reducing Administrator Overhead.
MSTP is also fast to converge. I hope this clears up your doubts.

upvoted 1 times

**SpicyMochi** 2 years, 4 months ago

Selected Answer: AC

A. Implement Rapid PVST+ instead of STP.
C. Use VTP to propagate VLAN information and to prune unused VLANs.

To achieve the stated goals of reducing the impact of topology changes, reducing the time spent on network administration, and reducing manual configuration errors, the architect should implement the following solutions:

A. Implement Rapid PVST+ (Per VLAN Spanning Tree Plus) instead of STP (Spanning Tree Protocol). Rapid PVST+ is based on the IEEE 802.1w standard (Rapid Spanning Tree Protocol) and converges faster than the traditional 802.1d STP. This will help to reduce the impact of topology changes.

C. Use VTP (VLAN Trunking Protocol) to propagate VLAN information and to prune unused VLANs. VTP is a Cisco proprietary protocol that simplifies VLAN administration across multiple switches by automatically distributing VLAN configuration information. This reduces the time spent on network administration and the potential for manual configuration errors.

upvoted 2 times

**DOSKIM** 2 years, 5 months ago

environement may include non cisco switch so in this case i will go wtih MST and VTP as PVST+ is cisco proprietary.
MST is standard.

upvoted 1 times

**Noproblem22** 2 years, 7 months ago

AC is the best answer. CD will not reduce the impact of topology change.

upvoted 1 times

**andrewChan** 2 years, 10 months ago

Selected Answer: AC

B- implement MST require certain downtime if network contrains lots of switches
D- not related to any requirement
E- DTP is not propagate VLAN info, instead how the trunk link form
so rest A, C
A - RPVST and PVST (STP) can coexist
C- setup VTP server (although answer does not mention but requrire when purning) and purning unused VLAN.....
on the other hand, the biggest errors is removing VLAN(s) on the VTP server accidentally and propergate to whole switch network. So most of real implementation are using VTP mode transparent instead

upvoted 3 times

**zlimvos** 3 years, 2 months ago

Selected Answer: AC

Also think A and C

upvoted 1 times

**python_tamer** 3 years, 3 months ago

Selected Answer: AC

For MST to work properly, the config has to be correctly configured on every switch in the L2 domain. I think this goes against the requirement for "reduce manual configuration errors", so I'm going with A and C.

upvoted 2 times

**cwoolie** 3 years, 5 months ago

A C is answer

upvoted 2 times

**XalaGyan** 3 years, 5 months ago

Selected Answer: BC

A customer's current Layer 2 infrastructure is running Spanning Tree 802.1d, and all configuration changes are manually implemented on each switch.
An architect must redesign the Layer 2 domain to achieve these goals:
* reduce the impact of topology changes ==> MST

* reduce the time spent on network administration ==> VTP (with MST vtp3)

* reduce manual configuration errors ==> VTP Pruning ???

Which two solutions should the architect include in the new design? (Choose two.)

I strongly believe MST and VTP ( B and C) should be appropriate here.

Please comment

upvoted 4 times

**cerifyme85** 2 years, 5 months ago

VTP server mode not recommeded

upvoted 1 times

**roganjosh** 3 years, 6 months ago

**Selected Answer: AC**

It's A and C

upvoted 2 times

**MangoBingsu** 3 years, 9 months ago

I believe its A &C as well

upvoted 4 times

Question #66 *Topic 1*

Which component is part of the Cisco SD-Access overlay architecture?

A. border node

B. spine node

C. leaf node

D. Cisco DNA Center

**Correct Answer:** *A*

*Community vote distribution*

A (88%) 13%

**wolfone** 1 year ago

**Selected Answer: A**

Cisco DNA Center is a management and automation platform. Although it is part of the overlay, the term "overlay" usually refers to the network devices that operate in the logical plane, not the management platform. Cisco DNA Center is more of an orchestration platform that acts as the "controller" of the SD-Access network.

upvoted 1 times

**kolp** 1 year, 1 month ago

**Selected Answer: D**

Why not D? DNA Center is neccessary component of SD Access Arch.

upvoted 1 times

**SpicyMochi** 1 year, 4 months ago

**Selected Answer: A**

A. border node

A border node is a component of the Cisco SD-Access overlay architecture. It serves as the gateway between the SD-Access fabric domain and the rest of the network, including external Layer 3 networks. Border nodes handle communication between the fabric domain and networks outside the fabric, making them essential for the overlay architecture.

upvoted 1 times

**Mohali98** 1 year, 9 months ago

**Selected Answer: A**

border node

upvoted 1 times

**zlimvos** 2 years, 2 months ago

**Selected Answer: A**

Border Node is part of the overlay. Check figure 5 on https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#OverlayNetwork

upvoted 2 times

**brzl** 2 years, 4 months ago

**Selected Answer: A**

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

Border Nodes are shown as members of the overlay network, thus answer A must be correct.

upvoted 1 times

**brzl** 2 years, 4 months ago

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

Border Nodes are shown as members of the overlay network, thus answer A must be correct.

upvoted 1 times

⊟ **cwoolie** 2 years, 4 months ago

A is correct after some research!!

upvoted 1 times

⊟ **cwoolie** 2 years, 5 months ago

D is correct..

upvoted 3 times

⊟ **roganjosh** 2 years, 6 months ago

**Selected Answer: A**

Answer is A

upvoted 1 times

⊟ **h40017** 2 years, 7 months ago

Answer is A, unless they are splitting hairs between "Border Node" and "Fabric Border Node"

upvoted 4 times

Question #67 *Topic 1*

How are wireless endpoints registered in the HTDB in a Cisco SD-Access architecture?

A. Border nodes first register endpoints and then update the HTDB.

B. Fabric WLCs update the HTDB as new clients connect to the wireless network.

C. Fabric APs update the HTDB with the clients' EID and RLOC.

D. Fabric edge nodes update the HTDB based on CAPPWAP messaging from the AP.

**Correct Answer:** *B*

Reference:

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

*Community vote distribution*

B (100%)

**henkpoa** 7 months, 3 weeks ago

**Selected Answer: B**

Check https://www.ciscolive.com/c/dam/r/ciscolive/global-event/docs/2022/pdf/BRKEWN-2308.pdf Page 16.

AP does connect to the edge nodes via VXLAN, while it talks to the WLC that handles the control plane.

upvoted 1 times

**khazbimoas** 9 months, 1 week ago

**Selected Answer: D**

correct answer is D.

keyword is "edge node". Endpoint connections (wired/wireless) are through edge nodes.

upvoted 1 times

**Beehurls** 1 year, 1 month ago

**Selected Answer: B**

Clients data traffic goes through VXLAN but the control traffic goes through CAPWAP tunnel to WLC.

upvoted 2 times

**Tjemz** 1 year, 6 months ago

B

Fabric WLC

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.

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

upvoted 3 times

Question #68 *Topic 1*

What is the purpose of a Cisco SD-Access underlay network?

A. to abstract IP-based connectivity from physical connectivity

B. to emulate LAN segments to transport Layer 2 frames over a Layer 3 network

C. to establish physical connectivity between switches and routers

D. to provide virtualization by encapsulating network traffic over IP tunnels

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**StandAlone** 1 year, 5 months ago

**Selected Answer: C**

Answer is correct.

Others mean overlay network

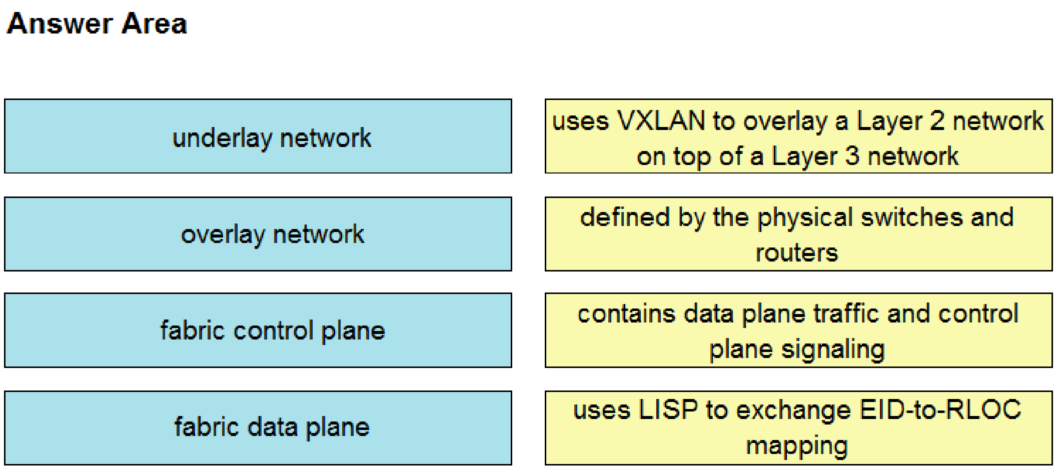
upvoted 2 times

Question #69 *Topic 1*

DRAG DROP -

Drag and drop the components in a Cisco SD-Access architecture from the left onto their descriptions on the right.

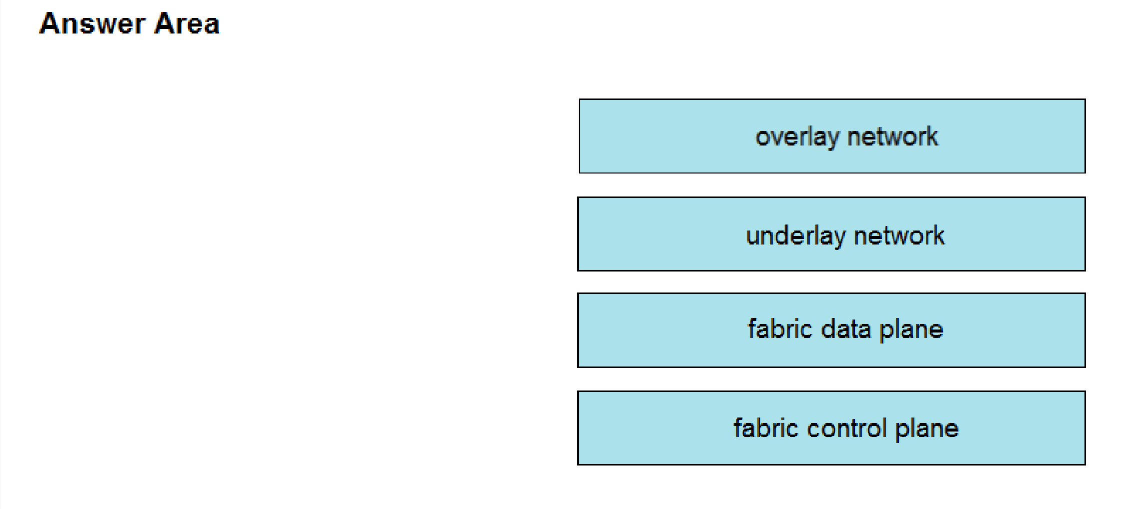
Select and Place:



**Answer Area**

| | |
|---|---|
| underlay network | uses VXLAN to overlay a Layer 2 network on top of a Layer 3 network |
| overlay network | defined by the physical switches and routers |
| fabric control plane | contains data plane traffic and control plane signaling |
| fabric data plane | uses LISP to exchange EID-to-RLOC mapping |

**Correct Answer:**



**Answer Area**

overlay network

underlay network

fabric data plane

fabric control plane

**bccabrera** Highly Voted 2 years, 3 months ago

Uses VXLAN - Data plane.

Defined by the physical switches and routers - Underlay.

Contains data plane traffic and control plane traffic - Overlay.

Uses LISP - Control plane.

upvoted 11 times

**salmarin** Most Recent 1 year, 7 months ago

use VXLAN is data plane

upvoted 1 times

**mgiuseppe86** 1 year, 11 months ago

Data Plane = VXLAN

Underlay = Physical equipment

Overlay = Virtual environment (Control/Data plan administration)

Fabric Control Plane = LISP

You learn this extensively in ENCOR...

upvoted 2 times

**oprince** 2 years, 2 months ago

Overlay and Data plane should be swapped.

"An overlay network is created on top of the underlay network through virtualization (virtual networks). The data plane traffic and control plane signaling are contained within each virtualized network,"

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

upvoted 2 times

**Hope66** 3 years ago

I'm agree too, Data Plane = VxLAN.

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/cvd-campus-fabric-design.pdf

upvoted 2 times

**Kamran202034** 3 years, 1 month ago

Agree, also Overlay includes data plane and control plain signaling traffic. Those two should be swapped.

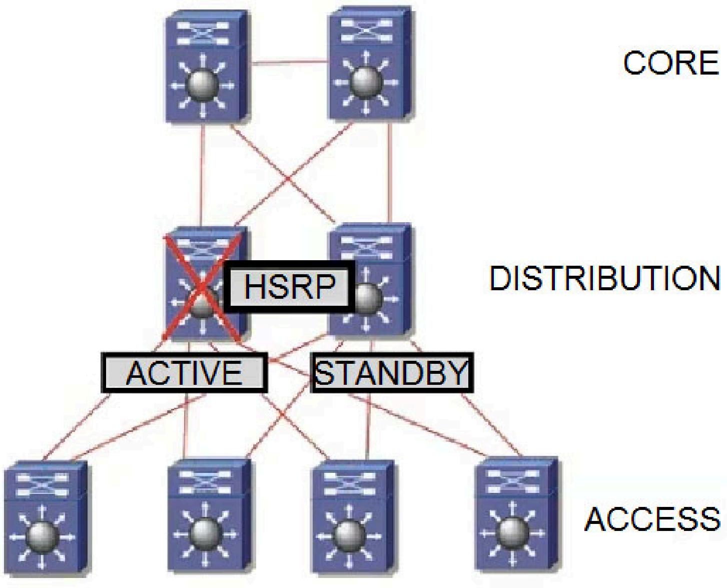
upvoted 1 times

**zlimvos** 3 years, 2 months ago

I think it is not correct. Data Plane = VxLAN

upvoted 4 times

Question #70 *Topic 1*



Refer to the exhibit. The distribution switches serve as the Layer 3 boundary. HSRP preemption is enabled. When the primary switch comes back after a failure, traffic is initially dropped. Which solution must be implemented to improve the design?

A. Increase the hello timers on both HSRP devices.

B. Use the preempt delay feature on the backup HSRP device.

C. Use the preempt delay feature on the primary HSRP device.

D. Configure a higher mac-refresh interval on both HSRP devices.

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**DOSKIM** 1 year, 11 months ago

B.should be on Backup router

upvoted 1 times

**DOSKIM** 1 year, 11 months ago

Sorry it is C.
we will delayed active router to become active again for specific amount of delay that we configured so that there could be IGP running on it it will form their adjacency before becoming active and run will properly before taking over everything.

upvoted 2 times

**Emily23** 1 year, 8 months ago

What you are saying makes no sense.
HSRP is used on L2 links, STP is involved. You use preempt delay in order to align with the STP topology.

IGP is L3 access.

upvoted 1 times

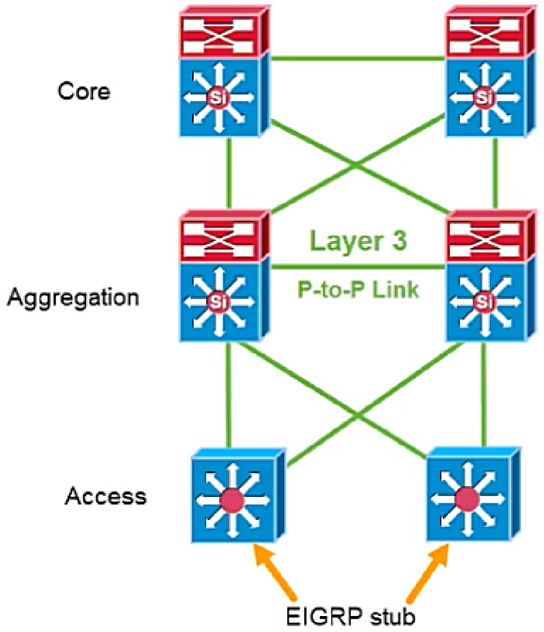
**funkeymonkey** 2 years, 7 months ago

Selected Answer: C

primary preempting prematurely

upvoted 1 times

Question #71 *Topic 1*



Refer to the exhibit. Where must an architect plan for route summarization for the topology?

A. from the core toward the aggregation and the access toward the aggregation

B. from the core toward the aggregation and the aggregation toward the core

C. from the aggregation toward the access and the access toward the aggregation

D. from the aggregation toward the core and the aggregation toward the access

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

⊟ **StandAlone** 1 year, 5 months ago

**Selected Answer: D**

I think answer is correct

'From the aggregation toward the core' seems right

upvoted 1 times

⊟ **bogd** 3 years, 6 months ago

Soo.... this question is basically "you have 3 layers: core, aggregation, access. At which layer would you AGGREGATE routes?" :)

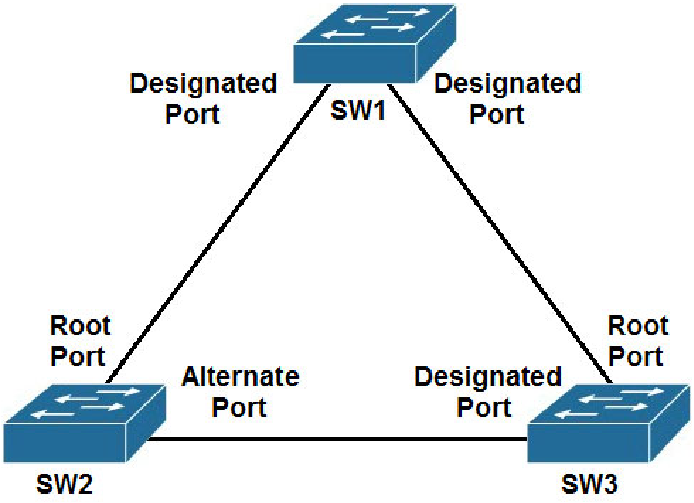
upvoted 2 times

⊟ **XalaGyan** 3 years, 5 months ago

at the firewall layer >D

upvoted 3 times

Question #72 *Topic 1*



Refer to the exhibit. The connection between SW2 and SW3 is fiber and occasionally experiences unidirectional link failure. An architect must optimize the network to reduce the change of Layer 2 forwarding loops when the link fails. Which solution should the architect include?

A. Utilize BPDU filter on SW3.

B. Utilize root guard on SW1.

C. Utilize BPDU guard on SW1.

D. Utilize loop guard on SW2.

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**StandAlone** 1 year, 5 months ago

Selected Answer: D

Reduce layer 2 forwarding loops -> loop guard

upvoted 1 times

**SpicyMochi** 2 years, 4 months ago

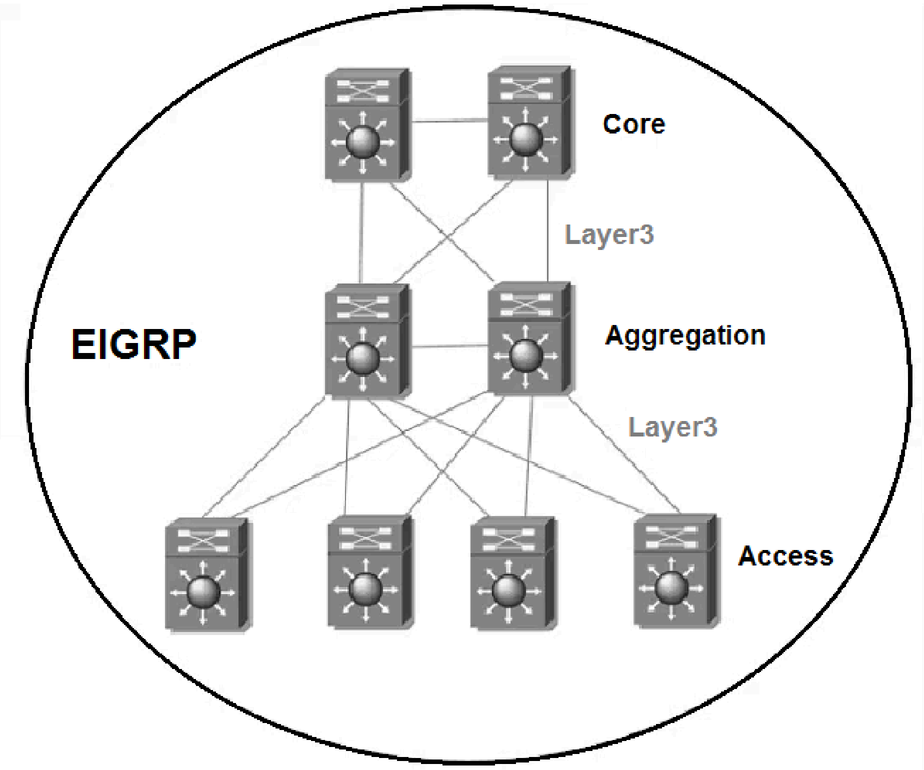
Selected Answer: D

The correct solution in this scenario is D. The architect should utilize loop guard on SW2.

Loop guard is a Layer 2 protocol that is designed to prevent forwarding loops caused by unidirectional links or other issues that can result in a break in the Layer 2 topology. When a port is designated as a root or alternate port, it is expected to receive BPDUs from the designated bridge, and it sends its own BPDUs out that port. If the port stops receiving BPDUs, it is considered a possible loop condition. Loop guard places the root port into a loop-inconsistent state to avoid forwarding loops, which prevents the forwarding of data frames until the issue is resolved.

upvoted 1 times

Question #73 Topic 1



Refer to the exhibit. The full EIGRP routing table is advertised throughout the network. Currently, users experience data loss when any one link in the network fails. An architect must optimize the network to reduce the impact when a link fails. Which solution should the architect include in the design?

A. Run BFD on the inter links between EIGRP neighbors.

B. Summarize the access layer networks from each access layer switch toward the aggregation layer.

C. Reduce the default EIGRP hello interval and hold time.

D. Summarize the access layer networks from the aggregation layer toward the core layer.

**Correct Answer:** *D*

*Community vote distribution*

D (60%) A (40%)

**SpicyMochi** Highly Voted 2 years, 10 months ago

Selected Answer: D

The correct solution for this scenario is D. The architect should summarize the access layer networks from the aggregation layer toward the core layer to optimize the network and reduce the impact when a link fails.

EIGRP is a distance-vector routing protocol that can support automatic summarization at network boundaries to reduce the size of the routing table and improve network performance. In this scenario, by summarizing the access layer networks from the aggregation layer toward the core layer, the full EIGRP routing table would be reduced in size and complexity, which would minimize the impact when a link fails.

upvoted 6 times

**1a17c3b** Most Recent 6 months, 3 weeks ago

Selected Answer: D

Key Details from the Question

EIGRP is used, and the full routing table is advertised across the network.

Users experience data loss when a link fails → implies slow convergence or routing instability.

Goal: Optimize the network design to reduce impact of link failures.

Option Analysis

A. Run BFD on the inter links between EIGRP neighbors
- BFD provides fast failure detection, which helps speed up convergence.
- However, it doesn't reduce routing table size or simplify reconvergence logic.
- Helpful, but not the most impactful solution in this scenario.
Good, but not best

D. Summarize the access layer networks from the aggregation layer toward the core layer
- Best practice in hierarchical design
- Reduces the number of routes advertised to the core
- Limits the scope of routing changes during link failures
- Improves stability and scalability
- Helps contain routing updates and minimize data loss
Correct Answer

upvoted 1 times

⊟ **guerreroa25** 9 months, 2 weeks ago

**Selected Answer: A**

A its the correct, by combining EIGRP with BFD, network administrators can achieve faster convergence and more reliable network connectivity. BFD enables faster detection of link failures, which triggers EIGRP to update its routing tables and choose a new best path. This reduces the amount of time it takes for the network to recover from a failure and ensures that the network is always using the most optimal path available.

upvoted 2 times

⊟ **5c725f5** 1 year, 5 months ago

**Selected Answer: A**

"currently, users experience data loss when any one link in the network fails"
Only BFD does this. Answer is A

upvoted 2 times

⊟ **Beehurls** 1 year, 1 month ago

Topology changes should not occur because of any one link. Summarization will help with that. BFD would just try to hide it.

upvoted 1 times

⊟ **iSDA69** 4 months, 3 weeks ago

There is already a feasible successor, and a partial update so there is not a network wide loss. The question says: "users experience...when any one link fails", the users of that failed link. Maybe is a little loss that is which is improved only by BFD.

upvoted 1 times

⊟ **Michellangelo** 2 years, 1 month ago

**Selected Answer: D**

I would go with answer D.
EIGRP Access Design Recommendations
When EIGRP is used as the routing protocol for a fully routed or routed access layer solution, with tuning it can achieve sub-200 ms convergence.

EIGRP to the distribution layer is similar to EIGRP in the branch, but it's optimized for fast convergence using these design rules:

Limit scope of queries to a single neighbor:

Summarize at the distribution layer to the core as is done in the traditional Layer 2 to Layer 3 border at the distribution layer. This confines impact of an individual access link failure to the distribution pair by stopping EIGRP queries from propagating beyond the core of the network. When the distribution layer summarizes toward the core, queries are limited to one hop from the distribution switches, which optimizes EIGRP convergence.
see: https://www.ciscopress.com/articles/article.asp?p=1315434&seqNum=3

upvoted 1 times

⊟ **ajinkya_gooner** 2 years, 1 month ago

should be D.
Its talking about optimization and not fast convergence.

upvoted 1 times

⊟ **mgiuseppe86** 2 years, 3 months ago

**Selected Answer: A**

The question states "when any one link in the network fails". Not just devices connected to the access network. Because of this I am going with A, BFD, sub-second convergence and path failure detection.

upvoted 2 times

⊟ **hir0_1010** 2 years, 3 months ago

**Selected Answer: D**

BFD is used to provide sub-sec link failure detection .. summerization is the correct answer. it summerizing the multiple smaller subnets to supernet ...any failure of those smaller subnets will not impact the others.

upvoted 4 times

⊟ **cooliday** 2 years, 7 months ago

**Selected Answer: A**

summarization doesn't really help here. BFD should be used. so answer A should be correct.

upvoted 3 times

⊟ **Marinheiro** 2 years, 7 months ago

An architect must optimize the network to reduce the impact when a link fails. Summarization has nothing to do with link failure. Latter A.

upvoted 1 times

⊟ **asd23355** 2 years, 9 months ago

**Selected Answer: A**

Bidirectional Forwarding Detection (BFD) protocol. BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols

upvoted 3 times

⊟ **DOSKIM** 2 years, 11 months ago

D is the correct answer

upvoted 4 times

Question #74 *Topic 1*

What is the purpose of a control plane node in a Cisco SD-Access network fabric?

A. to maintain the endpoint database and mapping between endpoints and edge nodes

B. to detect endpoints in the fabric and inform the host tracking database of EID-to-fabric-edge node bindings

C. to identify and authenticate endpoints within the network fabric

D. to act as the network gateway between the network fabric and outside networks

**Correct Answer:** *A*

*Community vote distribution*

A (79%) B (21%)

**John13121** Highly Voted 1 year, 8 months ago

Selected Answer: A

Definitely A

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

Answer B describes the Edge node purpose, not Control plane node!

upvoted 5 times

**J2J2J2J** Most Recent 1 year, 8 months ago

Selected Answer: B

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 1 times

**SpicyMochi** 1 year, 10 months ago

Selected Answer: B

The correct answer is B. The purpose of a control plane node in a Cisco SD-Access network fabric is to detect endpoints in the fabric and inform the host tracking database of EID-to-fabric-edge node bindings. The control plane nodes in the fabric keep track of the location of endpoints and communicate that information to the other nodes in the network to ensure that traffic is delivered to the correct destination. They are also responsible for forwarding policy information to the edge nodes to enforce access control and segmentation policies.

upvoted 2 times

> **SpicyMochi** 1 year, 10 months ago
>
> Actually rethinking this to be A as the correct answer.
>
> upvoted 2 times

**DOSKIM** 1 year, 11 months ago

A is the correct one

upvoted 1 times

**Tiamat** 2 years, 3 months ago

Selected Answer: A

The right answer is A

upvoted 3 times

**brzl** 2 years, 10 months ago

Answer A is correct.

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

Endpoint registration—Each edge node has a LISP control-plane session to all control plane nodes. After an endpoint is detected by the edge node, it is added to a local database called the EID-table. Once the host is added to this local database, the edge node also issues a LISP map-register message to inform the control plane node of the endpoint so the central HTDB is updated.

upvoted 4 times

⊟ **roganjosh** 3 years ago

**Selected Answer: A**

A is the answer

upvoted 4 times

⊟ **MangoBingsu** 3 years, 2 months ago

A is correct

upvoted 4 times

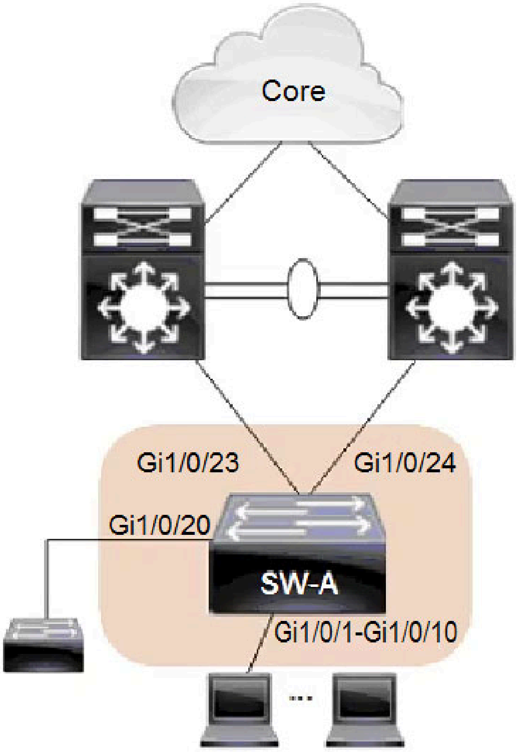
⊟ **veteranon2005** 3 years, 3 months ago

A is correct.

Each edge node has a LISP control-plane session to all control plane nodes. After an endpoint is detected by the edge node, it is added to a local database called the EID-table. Once the host is added to this local database, the edge node also issues a LISP map-register message to inform the control plane node of the endpoint so the central HTDB is updated.

upvoted 2 times

Question #75 *Topic 1*



Refer to the exhibit. An architect reviews the low-level design of a company's enterprise network and advises optimizing the STP convergence time. Which functionality must be applied to Gi1/0/1-10 to follow the architect's recommendation?

A. UplinkFast

B. root guard

C. BPDU guard

D. PortFast

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**python_tamer** Highly Voted 3 years, 3 months ago

Selected Answer: D

D is correct.

upvoted 5 times

**neiker45** Most Recent 1 year, 7 months ago

Portfast will skip STP states and go straight to forwarding.

upvoted 1 times

**LSLS55** 1 year, 11 months ago

Given answer is correct. Portfast is used in access ports allowing hosts to connect faster.

upvoted 1 times

**Hope66** 3 years, 4 months ago

I think that the answer is D.
Portfast is a spanning tree's functionality, once configured
It avoids the stp states (blocking, listening, learining, forwarding) every time any port among Gi1/0/1 Gi1/0/10 is connetcted again

upvoted 3 times

**alexanla** 3 years, 4 months ago

uplinkfast is for uplinks, what is shown are downlinks to end devices. Portfast.

upvoted 1 times

⊟ **cwoolie** 3 years, 4 months ago

A is the answer. UplinkFast is fast convergence.

upvoted 1 times

## Question #76 *Topic 1*

An engineer must design a large Layer 2 domain that contains hundreds of switches and VLANs. The engineer's primary goals are to:

✑ Efficiently utilize the bandwidth of all links

✑ Avoid Layer 2 loops

✑ Cause minimal impact on switch CPU and memory

Which technology should the engineer include in the design?

A. MST

B. Rapid PVST+

C. RSTP

D. PVST+

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**MangoBingsu** Highly Voted 👍 3 years, 2 months ago

Selected Answer: A

I believe it is MST. MST groups a large amount of VLANS into single instances which lower the amount of CPU and memory utilization.

https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html#mst

upvoted 11 times

**Clauster** Most Recent 🕒 1 year, 7 months ago

Oh Dang guys, MST is not a thing, they got us all with this, MST means nothing, MSTP is multiple Spanning Tree which would be the right answer but unfortunately is not listed so the next best Option is the Rapid one, i just realized this, dang Cisco is trying hard to make us fail the test. The Right answer is the given one.

upvoted 2 times

**mgiuseppe86** 1 year, 5 months ago

Bro you played yourself.

upvoted 2 times

**Lungful** 1 year, 6 months ago

This Cisco link uses "MST" everywhere. MST is fine. https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html

upvoted 2 times

**SpicyMochi** 1 year, 10 months ago

Selected Answer: A

MST (Multiple Spanning Tree) should be included in the design because it can efficiently utilize the bandwidth of all links while preventing Layer 2 loops, and it causes minimal impact on switch CPU and memory.

upvoted 1 times

**mgiuseppe86** 1 year, 5 months ago

You literally just copied and pasted the question and formulated a paragraph as if you retrieved it from somewhere.

upvoted 3 times

**andrewChan** 2 years, 4 months ago

configure mulitple MST groups may utilize all links, and reduce CPU usage. as each vlan on PVST+ /RPVST+ has it own SPT instance.

upvoted 1 times

**cwoolie** 2 years, 11 months ago

A is answer

upvoted 1 times

**laterst** 3 years ago

Selected Answer: A

Agree, MST builds a spanning tree topology per instance, while RPVST+ builds one topology per VLAN.
upvoted 1 times

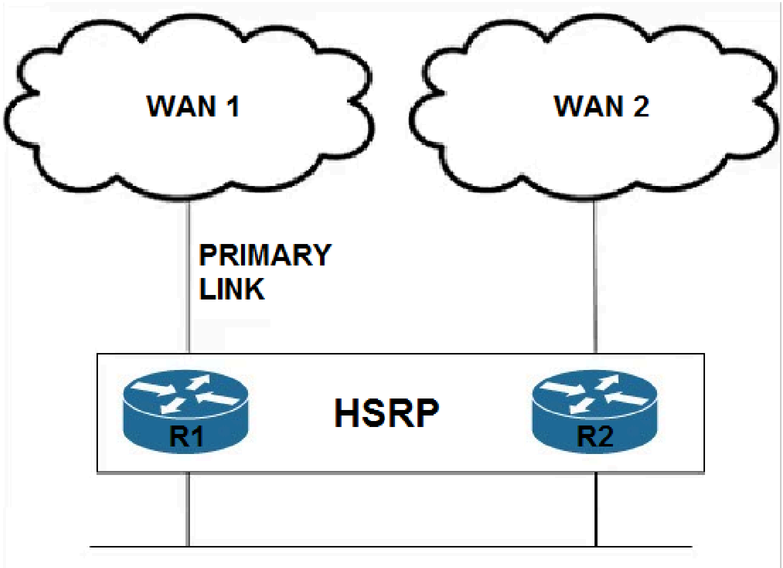
**MaestroGJE** 3 years, 2 months ago

Yes, I agree. MST is the right answer:

The CPU and memory requirements are less than for Rapid PVST+

https://www.ciscopress.com/articles/article.asp?p=2832407&seqNum=5
upvoted 4 times

Question #77 *Topic 1*



Refer to the exhibit. An engineer must design an automatic failover solution. The solution should allow HSRP to detect a WAN 1 failure and initiate an automatic failover, making router R2 the active HSRP router. Which two solutions should the engineer choose? (Choose two.)

A. implement IP SLA on router R1

B. implement PBR on router R1

C. implement Enhanced Object Tracking on router R1

D. use IP source routing

E. use a floating static route

**Correct Answer:** *AC*

*Community vote distribution*

AC (88%) 13%

**SpicyMochi** 1 year, 4 months ago

**Selected Answer: AC**

A. Implement IP SLA on router R1
C. Implement Enhanced Object Tracking on router R1

Explanation:

To achieve automatic failover with HSRP, you can use Enhanced Object Tracking (EOT) and IP SLA. EOT is a feature that enables tracking of a configurable object and can modify HSRP priority or state based on the status of the tracked object. IP SLA is a feature that generates and sends synthetic traffic to a specified destination and can trigger EOT based on the status of the tracked object. By configuring IP SLA on router R1 to track WAN 1 and then configuring EOT on R1 to decrement the HSRP priority or change the HSRP state, you can achieve automatic failover to router R2 in the event of a WAN 1 failure.

upvoted 3 times

**DOSKIM** 1 year, 5 months ago

AC are the correct answers

upvoted 1 times

**Reinier_veen** 1 year, 10 months ago

**Selected Answer: AC**

https://ipwithease.com/ip-sla-with-hsrp/

IP SLA to check availability ISP 1.
opject tracking the IP SLA vfor reducing preemtion

upvoted 4 times

Question #78 *Topic 1*

Which topology within a network underlay eliminates the need for first hop redundancy protocols while improving fault tolerance, increasing resiliency, and simplifying the network?

A. virtualized topology

B. routed access topology

C. Layer 2 topology

D. logical fabric topology

**Correct Answer:** *B*

*Community vote distribution*

B (92%) 8%

⊟ **akbntc** 1 year, 6 months ago

**Selected Answer: B**

Clue here is "underlay" network. Option-A and Option-C do not help with FHRP. Option-D is an "Overlay" technology. So, Option-B is the correct answer.

upvoted 2 times

⊟ **Clauster** 1 year, 7 months ago

**Selected Answer: B**

Option A (Virtualized Topology), Option C (Layer 2 Topology), and Option D (Logical Fabric Topology) do not inherently eliminate the need for first hop redundancy protocols or provide the same benefits as a routed access topology.

upvoted 1 times

⊟ **liksnetwork** 1 year, 7 months ago

**Selected Answer: D**

D is correct, routed access doesnot simplifying the network!

upvoted 1 times

⊟ **Patrick1234** 1 year, 11 months ago

Trick question. Routed access definitely does not simplify management. So i would go for D.

upvoted 2 times

⊟ **XalaGyan** 2 years, 1 month ago

**Selected Answer: B**

Layer 3 Routed Access is the correct answer.

upvoted 4 times

⊟ **Eards** 2 years, 4 months ago

**Selected Answer: B**

I agree with the above B

upvoted 2 times

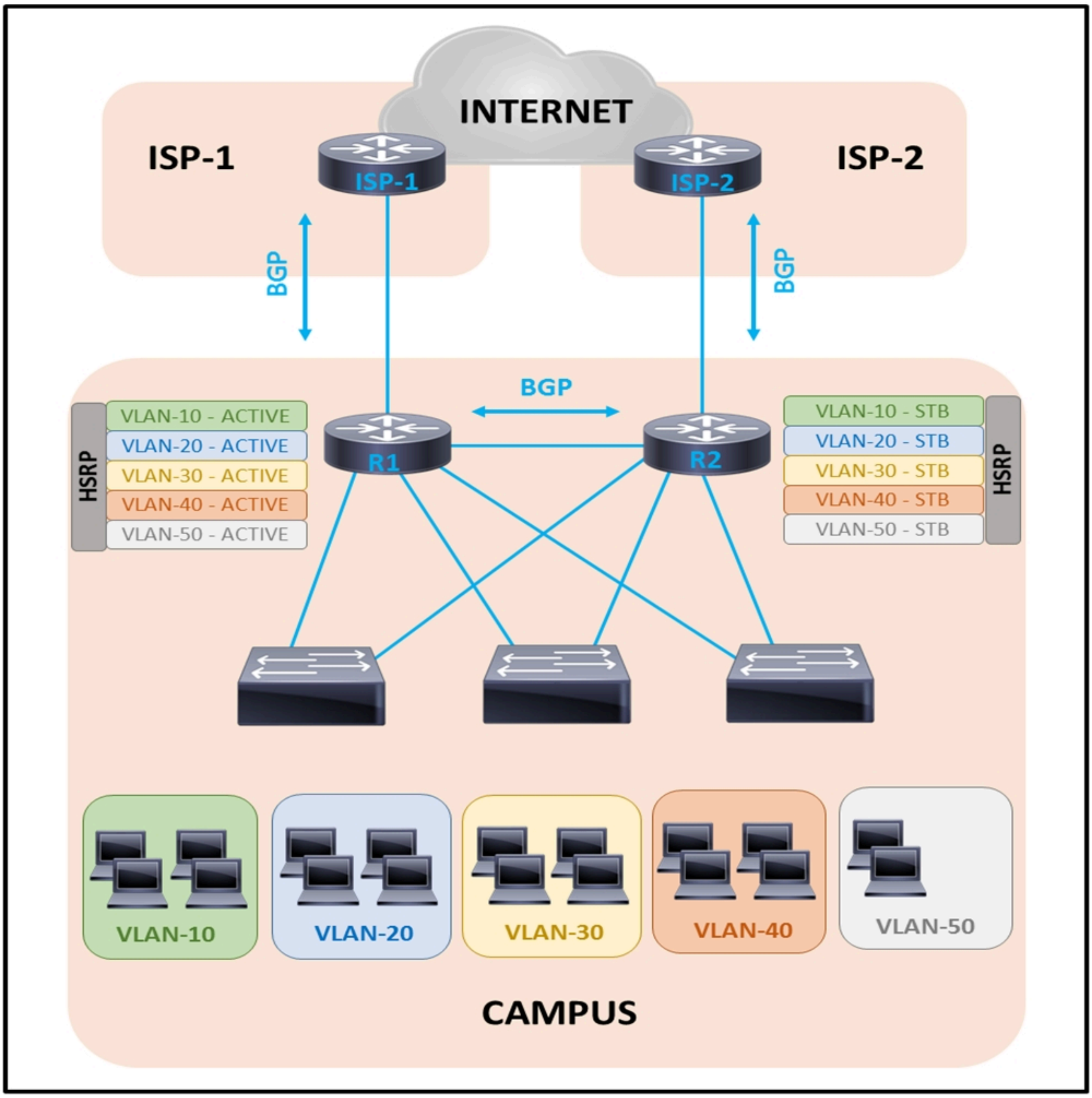
⊟ **NayTwister** 2 years, 5 months ago

I think B. Official Cert Guide by Bruno and Jordan, page 246. Layer 3 Access Layer: In this solution, the access layer switches act as default gateways and participate in routing, and there is no need for an FHRP.

upvoted 2 times

## Question #79 *Topic 1*

Refer to the exhibit.



A customer is running HSRP on the core routers. Over time the company has grown and requires more network capacity. In the current environment, some of the downstream interfaces are almost fully utilized, but others are not. Which solution improves the situation?

A. Make router R2 active for half of the VLANs.

B. Add more interfaces to R1 and R2.

C. Configure port channel toward downstream switches.

D. Enable RSTP on the downstream switches.

**Correct Answer:** *A*

*Community vote distribution*

A (67%) C (33%)

**khazbimoas** 9 months, 1 week ago

**Selected Answer: A**

Answer is A.

lets not complicate it. clearly all HSRP active on R1. This is "HSRP traffic asymmetry". soo balancing it would be the answer.
Answer C does improve resiliency for the L2 but not solve the HSRP traffic issue.

P.S.: Definitely need to configure STP (primary & secondary). But this is another part of the story.

upvoted 1 times

**Clauster** 1 year, 7 months ago

**Selected Answer: C**

So they try to confuse you with the first portion of the question, but the question is actually this one: "In the current environment, some of the downstream interfaces are almost fully utilized, but others are not. Which solution improves the situation?"
Well, if i got some Ethernet Links that are not being utilized and others are almost full idk about you but on my environment i am going to use PortChannels, not only is this going to alleviate some of those overutilized links but it will load balance across, it also answers this question which has nothing to do with HSRP in the first place.

upvoted 1 times

**Clauster** 1 year, 7 months ago

Actually, given the topology I only see one downlink to each Switch so i can't portchannel, answer has to be A.

upvoted 1 times

**mgiuseppe86** 1 year, 5 months ago

Great point... makes me reconsider my eyesight and my reading comprehension.

upvoted 4 times

**SpicyMochi** 1 year, 10 months ago

**Selected Answer: A**

A. Make router R2 active for half of the VLANs.

By making router R2 active for half of the VLANs, the customer can load balance the network traffic across the two core routers (R1 and R2) more efficiently. This will help to distribute the traffic more evenly between the routers, thus improving the overall network capacity utilization.

upvoted 2 times

**Sickcnt** 2 years, 4 months ago

**Selected Answer: A**

C could also be an option, but that would require "MultiChassis Etherchannel" and Also VSS for both the Layer 3 switches

Since thats not written anywhere I would go with Answer: A

upvoted 1 times

## Question #80 *Topic 1*

An architect must develop a campus network solution that includes:
✑ logically segmented and isolated networks
✑ ability to communicate between network segments when required
✑ support for overlapping IP addresses
✑ widely available technologies to avoid purchasing specialized equipment
Which solution must the architect select?

A. VSS with IGP

B. 802.1Q with HSRP

C. vPC with HSRP

D. VRF-Lite with OSPF

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**Sickcnt** 1 year, 4 months ago

**Selected Answer: D**

"support for overlapping IP addresses"

Because of this, VRF-Lite will 100% be needed

upvoted 3 times

Question #81 *Topic 1*

Which feature is used to optimize WAN bandwidth of IGMP network traffic among WAN Edge routers in the same VPN?

A. IGMPv2

B. multicast RP

C. multicast-replicator

D. multicast service routes

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

⊟ **Hope66** Highly Voted 👍 2 years, 11 months ago

I think C:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/bridging-routing-segmentation-qos/vedge/bridging-routing-segmentation-qos-book/multicast-overlay-routing.html

Replicators
For efficient use of WAN bandwidth, strategic vEdge routers can be deployed and configured as replicators throughout the overlay network.
Replicators mitigate the requirement for an ingress router to replicate a multicast stream once for each receiver.

upvoted 7 times

⊟ **Adaletherkesicin** Most Recent ⊙ 1 year, 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

⊟ **Clauster** 2 years, 1 month ago

They should of mentioned SD-WAN.

upvoted 2 times

⊟ **CKL_SG** 2 years, 3 months ago

Selected Answer: C

The Cisco SD-WAN design optimizes multicast packet distribution throughout the overlay network by eliminating packet replication on the ingress router, that is, on the router connected to a multicast source. Instead, the ingress router forwards multicast streams to a vEdge router that is designated to be a replicator, and it is this router that forwards streams to multicast receivers. This design saves bandwidth and computational resources on the ingress router.

upvoted 1 times

⊟ **SpicyMochi** 2 years, 4 months ago

Selected Answer: C

C. multicast-replicator

The multicast-replicator feature is used to optimize WAN bandwidth of IGMP network traffic among WAN Edge routers in the same VPN. By enabling multicast replication on the WAN Edge routers, multicast traffic is only forwarded to the required routers, thereby reducing unnecessary traffic and optimizing the WAN bandwidth utilization.

upvoted 1 times

⊟ **DOSKIM** 2 years, 5 months ago

It is C

upvoted 1 times

⊟ **Eards** 2 years, 10 months ago

Selected Answer: C

Agree with above C

upvoted 1 times

Question #82 *Topic 1*

Which consideration must be made when designing a Cisco SD-Access fabric underlay?

A. Subnets must be reduced to decrease latency.

B. Up to six control planes are supported.

C. The default MTU should be increased.

D. A unified policy must be used.

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**mgiuseppe86** 1 year, 5 months ago

**Selected Answer: C**

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

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.

upvoted 1 times

**John13121** 1 year, 8 months ago

**Selected Answer: C**

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

C is correct. Section SD-Access Considerations second bullet point is:

● Increase default MTU—The VXLAN header adds 50 bytes of encapsulation overhead. Enabling a campus and branch wide MTU of 9100 ensures that Ethernet jumbo frames can be transported without fragmentation inside the fabric.

upvoted 1 times

**ALOVEVIKS** 1 year, 9 months ago

**Selected Answer: C**

not should but have

upvoted 1 times

**DOSKIM** 1 year, 11 months ago

C is the right answer if it is for fabric overlay then D is the best answer

upvoted 2 times

**iLikeHamburgers** 2 years, 2 months ago

**Selected Answer: C**

Look under "Underlay Network Design". Its the second bullet point.

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

upvoted 2 times

**Furiel** 2 years, 3 months ago

Design consideration for underlay (not overlay), C should be the right answer

upvoted 1 times

**Reinier_veen** 2 years, 4 months ago

**Selected Answer: C**

I agree that a maximum of sic controlplane-NODES are supported. But six control planes?

I thing the right answer is C. Due to the extra VXLAN header the default MTU size must be increased.

9100 bytes is the default for SD-ACCESS i think.

upvoted 3 times

⊟ **Sickcnt** 2 years, 4 months ago

CCNP Enterprise Design ENSLD 300-420 page334 :

"SD-Access fabrics can support up to six control plane nodes in a wired deployment, and WLCs and can communicate with up to four control plane nodes."

upvoted 2 times

⊟ **Hope66** 2 years, 6 months ago

B is correct: CCNP Enterprise Design ENSLD 300-420 pag334

upvoted 1 times

Question #83 *Topic 1*

Which two functions does the control plane node provide in a Cisco SD-Access architecture? (Choose two.)

A. LISP proxy ETR

B. host tracking database

C. policy mapping

D. map server

E. endpoint registration

**Correct Answer:** *BD*

*Community vote distribution*

BD (100%)

**J2J2J2J** 1 year, 8 months ago

**Selected Answer: BD**

The control plane node enables the following functions:

Host tracking database—The host tracking database (HTDB) is a central repository of EID-to-fabric-edge node bindings.

Map server—The LISP MS is used to populate the HTDB from registration messages from fabric edge devices.

Map resolver—The LISP MR is used to respond to map queries from fabric edge devices requesting RLOC mapping information for destination EIDs.

upvoted 2 times

**GustavoF** 1 year, 10 months ago

**Selected Answer: BD**

B & D are correct.

upvoted 1 times

**Hope66** 2 years, 6 months ago

B and D seems correct:

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKEWN-2020.pdf pag.33

upvoted 1 times

Question #84 *Topic 1*

A large chain of stores currently uses MPLS-based T1 lines to connect their stores to their data center. An architect must design a new solution to improve availability and reduce costs while keeping these considerations in mind:
✑ The company uses multicast to deliver training to the stores.
✑ The company uses dynamic routing protocols and has implemented QoS.
✑ To simplify deployments, tunnels should be created dynamically on the hub when additional stores open.
Which solution should be included in this design?

A. VPLS

B. GET VPN

C. DMVPN

D. IPsec

**Correct Answer:** *C*

*Community vote distribution*

C (67%) B (33%)

⊟ **ef869f0** 9 months, 2 weeks ago

**Selected Answer: C**

GET VPN is tunneless

upvoted 1 times

⊟ **Reinier_veen** 2 years, 4 months ago

**Selected Answer: C**

I go with C. (DMVPN)
This because of the question to go for a "NEW" solution (opposed to ther current MPLS solution). Reducing costs means to use the internet and hence no GETVPN. (due to the IP adressing restrictions).

upvoted 2 times

⊟ **Sickcnt** 2 years, 4 months ago

**Selected Answer: C**

"To simplify deployments, tunnels should be created dynamically on the hub when additional stores open."

This describes DMVPN

GETVPN brings up new tunnels via putting sites under groups and its handled via the "key server" not the HUB

I know it doesn't sound practical to do encryption via DMVPN in an MPLS environment (everyone in their right mind would do GETVPN) , but I have read a few scenarios when they did it and I know its possible.

upvoted 1 times

⊟ **zlimvos** 2 years, 8 months ago

If I completely ignore that the question is mentioning 'tunnels' while GETVPN is 'tunnel-less' , I will go with GETVPN since it is a bit cheaper and multicast works better. Also can't be coincidence that it is MPLS only network.

upvoted 1 times

⊟ **cwoolie** 2 years, 10 months ago

Agree C

upvoted 3 times

⊟ **cwoolie** 2 years, 11 months ago

MPLS is B

upvoted 1 times

⊟ **mazinhoo** 2 years, 11 months ago

i think its C , because of the third requirement :

✑ To simplify deployments, tunnels should be created dynamically on the hub when additional stores open.

upvoted 4 times

⊟ **bogd** 3 years ago

**Selected Answer: B**

MPLS connectivity, multicast requirement - both seem to point to GET VPN

upvoted 1 times

⊟ **cryptonite** 3 years ago

DMVPN can be run over MPLS, with all the benefits of QoS. Under the hood, DMVPN is GRE with IPSEC, and GRE will deliver multicast.

upvoted 1 times

⊟ **Emily23** 1 year, 8 months ago

With one mention: IPsec is not default, but can be configured.

upvoted 1 times

⊟ **laterst** 3 years ago

bear in mind, this should be a new solution, and one of the goals is to reduce costs. No more MPLS, internet VPN it is. DMVPN is pretty much the only option left.

upvoted 1 times

Question #85 *Topic 1*

A network engineer must connect two sites across a public network using a secure tunneling technology that supports multicast traffic. Which technology should be selected?

A. IPsec

B. GRE

C. PPTP

D. GRE over IPsec

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**Lungful** 1 year, 6 months ago

**Selected Answer: D**

D is correct: "GRE tunnels allow to tunnel unicast, multicast, and broadcast traffic between routers and are often used for routing protocols between different sites. The downside of GRE tunneling is that it is clear text and offers no protection. On Cisco IOS routers however we can use IPSEC to encrypt the entire GRE tunnel, this allows us to have a safe and secure site-to-site tunnel."

Reference: https://networklessons.com/cisco/ccie-routing-switching-written/encrypted-gre-tunnel-with-ipsec

upvoted 1 times

Question #86 *Topic 1*

A branch office has a primary L3VPN MPLS connection back to the main office and an IPSEC VPN tunnel that serves as backup. Which design ensures that data is sent over the backup connection only if the primary MPLS circuit is down?

A. Use EIGRP to establish a neighbor relationship with the main office via L3VPN MPLS and the IPSEC VPN tunnel.

B. Use BGP with the multipath feature enabled to force traffic via the primary path when available.

C. Use static routes tied to an IP SLA to prefer the primary path while a floating static route points to the backup connection.

D. Use OSPF with a passive-interface command on the backup connection.

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**python_tamer** Highly Voted 👍 2 years, 3 months ago

**Selected Answer: C**

C - Because it states the backup is an "IPSEC VPN tunnel" so we can't run a dynamic routing protocol over it which rules out A, B and D.

upvoted 6 times

**SpicyMochi** Most Recent 🕘 1 year, 4 months ago

**Selected Answer: C**

C. Use static routes tied to an IP SLA to prefer the primary path while a floating static route points to the backup connection.

Using static routes with IP SLA tracking allows you to prefer the primary L3VPN MPLS connection when it is available and automatically failover to the backup IPSEC VPN tunnel when the primary connection goes down. IP SLA tracking monitors the primary path's availability and adjusts the routing table accordingly. The floating static route, with a higher administrative distance, serves as a backup route that only becomes active when the primary route is unavailable. This design ensures that data is sent over the backup connection only if the primary MPLS circuit is down.

upvoted 1 times

**cwoolie** 2 years, 4 months ago

A or C would work I guess....

upvoted 1 times

**XalaGyan** 1 year, 7 months ago

EIGRP equal cost multi pathing by default across 2 links. if it was with passive-interface for listening to HQ only via MPLS that would work.

upvoted 1 times

**cwoolie** 2 years, 5 months ago

C is answer

upvoted 1 times

**TMe392** 2 years, 6 months ago

Floating static routes are static routes that are used to provide a backup path to a primary static or dynamic route, in the event of a link failure.

upvoted 1 times

**John_Aung** 2 years, 11 months ago

C is right answer?

upvoted 4 times

**virtux** 3 years, 1 month ago

Why not A? EIGRP support backup route (Feasible successor)

upvoted 1 times

**ImAlwaysRight** 2 years, 11 months ago

how to ensure that primary will have best cost? I will go with C

upvoted 1 times

**andit** 2 years, 7 months ago

EIGRP calculates Bandwith within its metric per default. So it should work fine.

upvoted 1 times

**brzl** 2 years, 4 months ago

EIGRP neighborship through the (non-VTI) tunnel is the problem. Answer C should be the right one.

upvoted 1 times

Question #87 *Topic 1*

Which solution allows overlay VNs to communicate with each other in an SD-WAN Architecture?

A. External fusion routers can be used to map VNs to VRFs and selectively route traffic between VRFs.

B. GRE tunneling can be configured between fabric edges to connect one VN to another.

C. SGTs can be used to permit traffic from one VN to another.

D. Route leaking can be used on the fabric border nodes to inject routes from one VN to another.

**Correct Answer:** *A*

*Community vote distribution*

A (58%) D (25%) B (17%)

**goku2020** Highly Voted 4 years, 9 months ago

A External fusion router.

upvoted 10 times

**BW1001** 3 years, 10 months ago

This question is about SD-WAN not SDA

upvoted 2 times

**cryptonite** 3 years, 6 months ago

All the answers seem to suggest SDA - Fusion, Border, Edge etc

upvoted 3 times

**Emily23** 2 years, 2 months ago

But the question is about SD-WAN.

I think you can go with the "I don't care what they ask, I will answer what is think" approach, but don't think is very efficient.

upvoted 1 times

**NoHombre** Most Recent 5 months, 3 weeks ago

Selected Answer: D

In Cisco SD-WAN, each overlay VN is implemented as a separate VPN/VRF on WAN Edge devices.
If two VNs must communicate, you selectively leak routes between those VPNs. This is done with policy-based route leaking (typically a centralized control policy on vSmart that matches routes from VPN X and "sets VPN" to Y), or with local inter-VRF route leaking on IOS-XE WAN Edges when both VRFs exist there.
This preserves segmentation while enabling only the intended prefixes to be reachable across VNs—exactly what "overlay VNs communicate with each other" requires.

upvoted 1 times

**Buffering** 1 year, 4 months ago

Selected Answer: D

The Vedge router configuration guide shows explicitly how to allow VPN to VPN communication - https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing-book/m-routing-leaking-for-service-sharing.html#Cisco_Concept.dita_037b791c-e340-491a-a74c-09c973301991

Its annoying they use VN instead of VPN to try and throw you off.

upvoted 1 times

**salmarin** 1 year, 7 months ago

Selected Answer: A

Clearly there is a typo in the question and it's SDA not SDWAN

upvoted 2 times

**akbntc** 1 year, 12 months ago

Selected Answer: A

Guys, read the questions carefully... it's about SD-WAN (not SD-Access).
Options B,C,D are for SD-Access components.
upvoted 1 times

**Clauster** 2 years ago

Selected Answer: D

THE ANSWER IS D
Fabric Routers are used in SD-Access not SD-WAN, This eliminates answer A.
Fabric Edges are also used in SD-Access so that eliminates that question as well.
The other answer makes no sense.
The answer is D: You can do Route leaking to talk between VN
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-routing-leaking-for-service-sharing.html

Lets' Gooo i was able to find it.
upvoted 1 times

**Clauster** 2 years ago

Selected Answer: D

CORRECT ANSWER IS D !!!!!!!

In an SD-WAN (Software-Defined Wide Area Network) architecture, route leaking is a common technique used to allow overlay Virtual Networks (VNs) to communicate with each other. Route leaking involves selectively sharing or injecting routes from one VN to another, thereby enabling traffic to flow between the isolated VNs.

Key points about route leaking in an SD-WAN architecture:

Fabric Border Nodes: Route leaking typically occurs at the border nodes of the SD-WAN fabric. These nodes are responsible for connecting the overlay VNs to external networks.

ALSO: FABRIC ROUTERS ARE USED ON SD-ACCESS NOT SD-WAN !! BE CAREFUL
upvoted 1 times

**Clauster** 2 years, 1 month ago

Selected Answer: A

The answer is absolutely A
upvoted 1 times

> **Clauster** 2 years ago
>
> This is not correct, moderator if you could please remove this comment i don't want users to get confused, the correct answer is D
> upvoted 1 times

**SpicyMochi** 2 years, 4 months ago

Selected Answer: A

My thoughts on this one:
GRE (Generic Routing Encapsulation) tunneling can also be used to enable communication between overlay VNs in some network designs. By configuring GRE tunnels between the fabric edge devices, traffic from one VN can be sent through the tunnel to another VN, enabling inter-VN communication.

However, option A, which involves using external fusion routers to map VNs to VRFs and selectively route traffic between VRFs, is a more common approach in SD-WAN architectures. It offers greater flexibility and control for policy-based routing, whereas GRE tunneling may require manual configuration and maintenance of tunnels, which can be more complex and less scalable in large deployments.

So, while both options A and B can be used to enable communication between overlay VNs, option A is more common and generally more suitable for SD-WAN architectures.
upvoted 1 times

**andrewChan** 2 years, 10 months ago

Selected Answer: A

according to ENSLD cert guide Page 335
any communication between endpoints in different VNs must go through a fusion router or firewall

and VNs belong to SD-Access. not SD-WAN

upvoted 2 times

⊟ **sonicwarrior** 3 years, 1 month ago

Hmm the question is wrong, that should mean SD-Access - VN virtual network, that is used within SD-Access not in SD-WAN

upvoted 1 times

⊟ **python_tamer** 3 years, 3 months ago

**Selected Answer: A**

All the answers relate to SDA rather than SD-WAN so I think the wording of the question is not right here. Therefore, the answer should be A.

upvoted 1 times

⊟ **cwoolie** 3 years, 5 months ago

Answer is B

upvoted 1 times

⊟ **roganjosh** 3 years, 6 months ago

**Selected Answer: B**

Leaning towards B guys, question say SD-WAN not SD-Access, Fusion routers are used in SD-Access.

upvoted 2 times

⊟ **Xavi07** 4 years, 1 month ago

to comunicate one VN to another VM is via internal tunel in the SD-WAN; so the correct is B.

upvoted 1 times

⊟ **Ranx01** 4 years, 7 months ago

The CCNP Enterprise Design ENSLD 300-420 Official Cert Guide mentions, "A Fusion router is used to allow endpoints in different VNs to communicate with each other", it also states "vEdge routers are responsible for establishing the network fabric and forwarding traffic; they bring up IPsec and GRE tunnels between sites...vEdge routers establish a control channel to vSmart controllers and IPsec tunnels to other vEdge devices to form the overlay network". If I understand correctly, I think "vEdge Routers" do the mapping of VN's to VRF's not "Fusion Routers". Fusion Routers acts as the next-hop to a VN. I'm swayed towards "B" as the correct answer.

upvoted 2 times

⊟ **luisjuradoledesma** 4 years, 7 months ago

I'm getting crazy with this one. Why every single supplier says GRE tunnels - it's by far more sensible A (External Fusion router) - I'm taking the test tomorrow - can anyone clarify please?

upvoted 2 times

⊟ **cwoolie** 3 years, 5 months ago

What is answer?

upvoted 1 times

Question #88 *Topic 1*

What are two benefits of designing an SD-WAN network fabric with direct Internet access implemented at every site? (Choose two.)

A. It decreases latency to applications hosted by public cloud service provider.

B. It decreases latency on Internet circuits.

C. It increases the speed of delivery of site deployments through zero-touch provisioning.

D. It increases the total available bandwidth on Internet circuits.

E. It alleviates network traffic on MPLS circuits.

**Correct Answer:** *AC*

*Community vote distribution*

AC (44%) AE (38%) AD (19%)

**night_wolf_in** 2 months, 3 weeks ago

**Selected Answer: AC**

No mention of MPLS circuits in the question.

upvoted 1 times

**adcym** 1 year, 1 month ago

**Selected Answer: AE**

A,E is answer.

upvoted 1 times

**mladjo89** 1 year, 3 months ago

According to the following link I would say A and E are correct answers:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy-2020aug.pdf

upvoted 1 times

**mladjo89** 1 year, 3 months ago

Answer is on the page 6.

upvoted 1 times

**Seb82** 1 year, 4 months ago

**Selected Answer: AC**

Nowhere in the question it is mentioned that the sites have also an MPLS circuit, so, having DIA at each site cannot alleviate traffic from some non-existent MPLS circuits, but it can be used to speed up the deployment via ZTP

upvoted 3 times

**Swiz005** 1 year, 5 months ago

**Selected Answer: AE**

I go with AE - These are advantages of SD-WAN

upvoted 2 times

**Swiz005** 1 year, 6 months ago

**Selected Answer: AC**

How is this not AC?

upvoted 2 times

**salmarin** 2 years, 1 month ago

**Selected Answer: AC**

the only two that make sense to me A and C.

upvoted 2 times

**akbntc** 2 years, 5 months ago

**Selected Answer: AC**

A & C. Option E is for deployment in MPLS circuits. The solution in asking for deploying SDWAN on DIA circuits.

upvoted 1 times

**foxiemulder** 2 years, 7 months ago

it's a A and C. The question doesn't even mention MPLS, so E doesn't make sense.

ZTP is a major benefit.

upvoted 2 times

**GustavoF** 2 years, 10 months ago

**Selected Answer: AE**

I go with A & E.

upvoted 2 times

**atiWok** 2 years, 11 months ago

**Selected Answer: AE**

Definetly AE

upvoted 3 times

**ccnproute1** 2 years, 11 months ago

I agree with A and E. From OCG states "With DIA, Internet-bound traffic or public cloud traffic from the branch is routed directly to the Internet, avoiding the latency involved in tunneling Internet-bound traffic to a central site." This corresponds to answer A. And then "Benefits of using DIA include reduced bandwidth consumption, latency, and costs

(thanks to offloading Internet traffic from the private WAN circuit)." Meaning that basically offloads internet traffic from the MPLS (private WAN) and routed directly to DIA. SD-WAN cannot increase by itself, only ISP can do that.

upvoted 4 times

> **akbntc** 2 years, 5 months ago
>
> A is correct, but why E? The solution is using DIA, not MPLS.
>
> upvoted 1 times

**Tjemz** 3 years ago

agree on A en D

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy-2020aug.pdf

upvoted 1 times

**XalaGyan** 3 years, 1 month ago

**Selected Answer: AD**

It is actually A and D. you have more resources available for cloud apps and in total you have more wan capacity for system to use

upvoted 3 times

**zlimvos** 3 years, 8 months ago

**Selected Answer: AE**

I agree with A and E by instinct alone. DIA is configured on the edge router way after you get access to it, i don't think ZTP is applicable.

upvoted 1 times

Question #89 *Topic 1*

Which routes does the overlay management protocol advertise in an SD-WAN overlay?

A. underlay, MPLS, and overlay

B. primary, backup, and load-balanced

C. prefix, TLOC, and service

D. Internet, MPLS, and backup

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**bccabrera** 1 year, 3 months ago

**Selected Answer: C**

vEdge routers advertise three types of routes via the Overlay Management Protocol (OMP) to the vSmart controllers:
OMP routes: 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.
TLOC routes advertise Transport Locators of the connected WAN transports, along with additional attributes such as public and private IP addresses, color, TLOC preference, site ID, weight, tags, and encryption keys.
Service routes advertise embedded network services such as firewalls and IPS that are connected to the vEdge local-site network.

https://www.networkacademy.io/ccie-enterprise/sdwan/omp-overview#:~:text=OMP%20routes%3A%20OMP%20Routes%2C%20also,service%20side%20of%20the%20vEdge.

upvoted 2 times

Question #90 *Topic 1*

What is one function of the vSmart controller in an SD-WAN deployment?

A. orchestrates vEdge and cEdge connectivity

B. responsible for the centralized control plane of the SD-WAN network

C. provides centralized network management and a GUI to monitor and operate the SD-WAN overlay

D. provides a data-plane at branch offices to pass traffic through the SD-WAN network

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**davedrangus** 1 year, 4 months ago

Selected Answer: B

Agree with B

upvoted 1 times

**Lungful** 2 years ago

Selected Answer: B

B is correct

A = vBond
B = vSmart
C = vManager
D = vEdge

upvoted 2 times

Question #91 *Topic 1*

In an SD-WAN architecture, which methods are used to bootstrap a vEdge router?

A. DHCP options or manual configuration

B. vManage or DNS records

C. ZTP or manual configuration

D. DNS records or DHCP options

**Correct Answer:** *C*

**luisjuradoledesma** 2 years, 1 month ago

My mistake - as we are talking about vEdge routers - the only 2x options are manual config or ZTP - refer to:
ZTP or manual configuration
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf

upvoted 2 times

**CCNPWILL** 1 year, 8 months ago

Correct. Best choice here is C.

upvoted 3 times

**luisjuradoledesma** 2 years, 1 month ago

I do think that the answer should be 'B' - vManage or DNS Records - manual, ZTP and bootstrap are different methods. Please, refer to:
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf

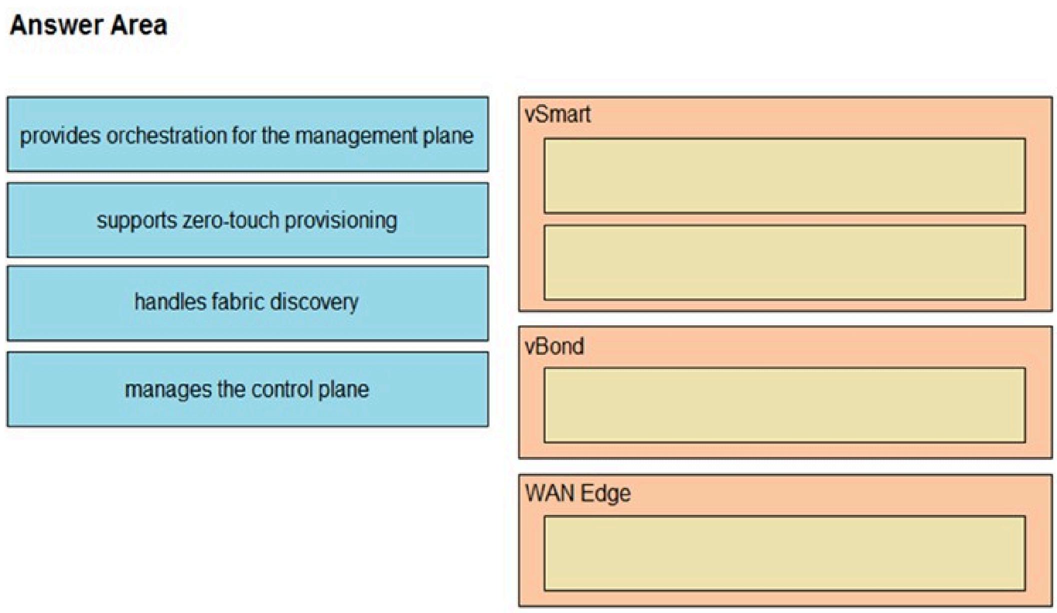
upvoted 1 times

Question #92 Topic 1

DRAG DROP -

Drag and drop the functions from the left onto the Cisco SD-WAN components that perform them on the right.

Select and Place:



Answer Area

provides orchestration for the management plane

supports zero-touch provisioning

handles fabric discovery

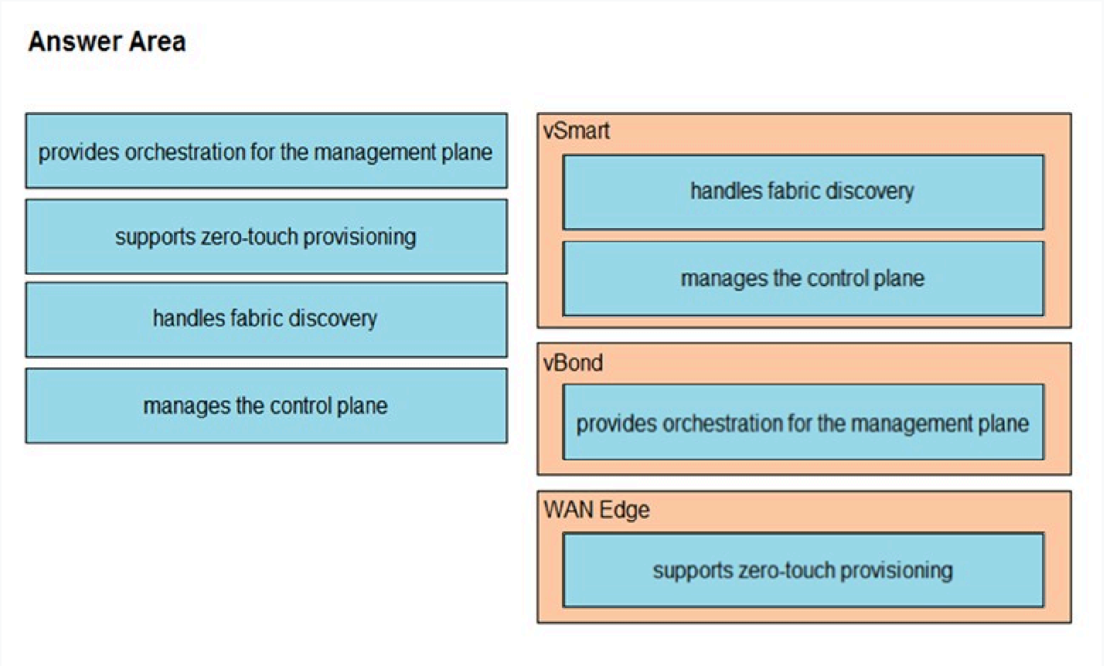
manages the control plane

vSmart

vBond

WAN Edge

**Correct Answer:**



Answer Area

provides orchestration for the management plane

supports zero-touch provisioning

handles fabric discovery

manages the control plane

vSmart

handles fabric discovery

manages the control plane

vBond

provides orchestration for the management plane

WAN Edge

supports zero-touch provisioning

**Lungful** 1 year, 6 months ago

The provided answer is correct.

upvoted 3 times

Question #93 *Topic 1*

Which two functions are provided by the Cisco SD-WAN orchestration plane? (Choose two.)

A. centralized provisioning

B. primary authentication point

C. NAT traversal facilitation

D. Zero Touch Provisioning

E. troubleshooting and monitoring

**Correct Answer:** *BC*

*Community vote distribution*

BC (60%) BD (40%)

**PicoOstrava** 1 year, 3 months ago

**Selected Answer: BC**

As per cisco u:The main characteristics of Cisco vBond orchestrator are:

Orchestrates connectivity

First point of authentication

Distributes list of vSmarts and vManage to all WAN Edge routers

Facilitates NAT traversal

Requires public IP address (could sit behind 1:1 NAT)

upvoted 3 times

**Pminiakhmetov** 1 year, 5 months ago

**Selected Answer: BD**

I think B and D are correct

upvoted 2 times

**muffedtrims** 1 year, 4 months ago

NAT traversal is part of the data plan. Correct answer is B & D

Orchestration plane provides authentication and ZTP

upvoted 1 times

**Pminiakhmetov** 1 year, 5 months ago

ChatGPT says that BC correct. Link https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html tell that correct answer is B and D.

NAT Traversal Facilitator correspond to Data Plane, not Orchestration Plane

upvoted 1 times

**GustavoF** 2 years, 10 months ago

**Selected Answer: BC**

B and C are correct.

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

upvoted 2 times

**CCNPWILL** 4 years, 8 months ago

Correct. B and C are responsibilities of the vBond which handles orchestration.

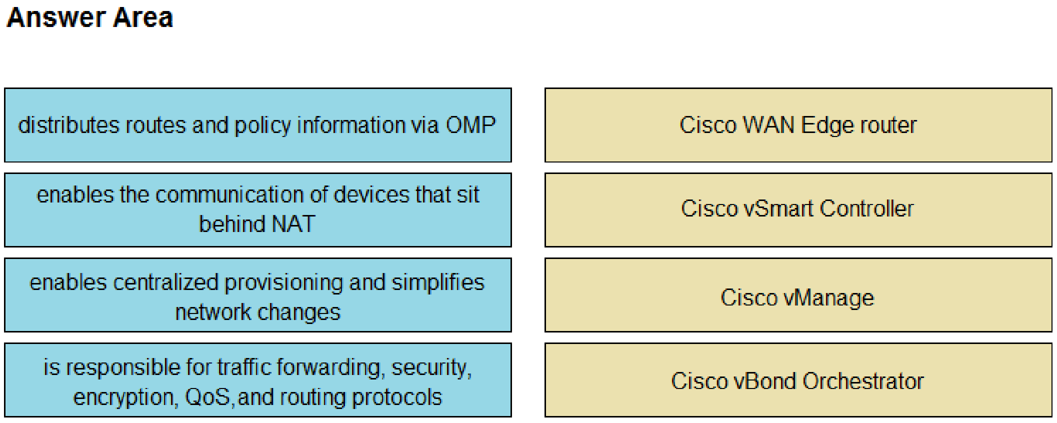
upvoted 3 times

Question #94 *Topic 1*

DRAG DROP -

Drag and drop the descriptions from the left onto the Cisco SD-WAN component they describe on the right.

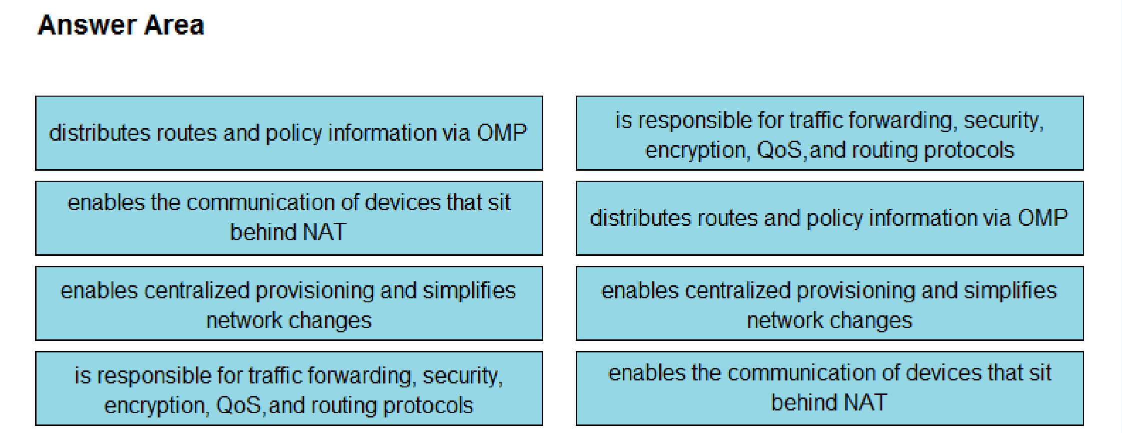
Select and Place:



**Answer Area**

| | |
|---|---|
| distributes routes and policy information via OMP | Cisco WAN Edge router |
| enables the communication of devices that sit behind NAT | Cisco vSmart Controller |
| enables centralized provisioning and simplifies network changes | Cisco vManage |
| is responsible for traffic forwarding, security, encryption, QoS, and routing protocols | Cisco vBond Orchestrator |

**Correct Answer:**



**Answer Area**

| | |
|---|---|
| distributes routes and policy information via OMP | is responsible for traffic forwarding, security, encryption, QoS, and routing protocols |
| enables the communication of devices that sit behind NAT | distributes routes and policy information via OMP |
| enables centralized provisioning and simplifies network changes | enables centralized provisioning and simplifies network changes |
| is responsible for traffic forwarding, security, encryption, QoS, and routing protocols | enables the communication of devices that sit behind NAT |

Reference:

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

**rted** 1 year, 8 months ago

Wan -> is responsible for traffic forwarding, security, encryption, QoS and routing protocols
vSmart -> distributes routes and policy information via OMP routes
vManage -> enables centralized provisioning and simplifies network changes
vBond -> enables the communication of devices that sit behind NAT

upvoted 1 times

**Clauster** 2 years, 7 months ago

distributes routes and policy information via OMP routes: Vsmart
enables the communication of devices that sit behind NAT: vBond
enables centralized provisioning and simplifies network changes: vManage
is responsible for traffic forwarding, security, encryption, QoS and routing protocols: Cisco WAN Edge Router

upvoted 3 times

Question #95 *Topic 1*

Which two techniques improve the application experience in a Cisco SD-WAN design? (Choose two.)

A. utilizing forward error correction

B. implementing a stateful application firewall

C. implementing AMP

D. utilizing quality of service

E. implementing Cisco Umbrella

**Correct Answer:** *AD*

Reference:

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf slide 33

*Community vote distribution*

AD (100%)

**salmarin** 1 year, 7 months ago

**Selected Answer: AD**

A and D improve the application experience.

upvoted 1 times

**SpicyMochi** 2 years, 4 months ago

**Selected Answer: AD**

A. utilizing forward error correction

D. utilizing quality of service

Two techniques that improve the application experience in a Cisco SD-WAN design are:

Utilizing forward error correction (FEC): FEC is a technique used to enhance the reliability and performance of data transmissions by proactively detecting and correcting errors in the transmission without requiring retransmission. In an SD-WAN environment, FEC helps maintain a better application experience by reducing the impact of packet loss and improving the overall quality of the connection.

Utilizing quality of service (QoS): QoS is a set of techniques used to manage and prioritize network traffic to ensure that critical applications receive the required bandwidth and performance levels. In an SD-WAN environment, QoS can be used to prioritize important applications over less critical ones, ensuring that the user experience remains consistent and optimal for essential applications even in situations with limited bandwidth or network congestion.

upvoted 1 times

Question #96 *Topic 1*

How is redundancy achieved among Cisco vBond Orchestrators in a Cisco SD-WAN deployment?

A. The IP addresses of all Orchestrators are mapped to a single DNS name.

B. The closest Orchestrator to each Cisco WAN Edge router is selected.

C. Cisco WAN Edge routers are configured with all Orchestrators using their IP addresses and priority.

D. A single Cisco Orchestrator is deployed in each network.

**Correct Answer:** *A*

Reference:

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf page 25

*Community vote distribution*

A (100%)

**bccabrera** 1 year, 3 months ago

**Selected Answer: A**

A highly available Cisco SD-WAN network has multiple vBond controllers working in an active/active manner, preferably deployed at different on-prem geographic locations or cloud regions. Then each SD-WAN device references the vBond orchestrator by a single FQDN name in its system configuration, as shown in the output below.

```
system
vbond vbond.xyz.com
!
```

At the DNS layer, the organization associates multiple IP addresses with the vBond's DNS name. Generally, when an SD-WAN device queries the DNS server, the server sends back the IP addresses of all vBond orchestrators. Then the device tries each IP in succession, with the first one determined by a hash function until it establishes a successful connection.

https://www.networkacademy.io/ccie-enterprise/sdwan/high-availability

upvoted 1 times

Question #97 *Topic 1*

Which design consideration must be made when dual WAN Edge routers are deployed at a branch site?

A. Use BGP AS-path prepending to influence egress traffic and use MED to influence ingress traffic from the branch.

B. HSRP priorities must match the OMP routing policy to prefer one WAN Edge over the other.

C. Traffic must be symmetrical as it egresses the WAN Edges and returns from remote sites for DPI to function properly.

D. Configure BFD between WAN Edge routers to detect sub-second link failures.

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**sk84** Highly Voted 4 years, 5 months ago

C) is the correct answer.
Traffic Symmetry for Application Visibility

For the localized application visibility features (DPI and NBAR2) to be able to classify most application traffic, it is important that the WAN Edge router sees network traffic in both directions. In dual-WAN Edge sites without any policy enabled, equal cost paths exist over each transport and to each WAN Edge router, and network traffic is hashed depending on fields in the IP header. Traffic is unlikely to always be forwarded to the same WAN Edge router in both the LAN-to-WAN direction and the WAN-to-LAN direction. To maintain symmetric traffic, it is recommended to set up routing so that traffic prefers one WAN Edge over another at dual-WAN Edge router sites.

upvoted 6 times

**salmarin** Most Recent 1 year, 7 months ago

Selected Answer: C

Traffic Symmetry for Application Visibility, C is correct

upvoted 1 times

**vangio** 2 years, 1 month ago

Correct C

upvoted 1 times

**SpicyMochi** 2 years, 4 months ago

Selected Answer: C

C. Traffic must be symmetrical as it egresses the WAN Edges and returns from remote sites for DPI to function properly.

When dual WAN Edge routers are deployed at a branch site, one of the design considerations is to ensure that traffic is symmetrical as it egresses the WAN Edges and returns from remote sites. This symmetry is crucial for proper functioning of Deep Packet Inspection (DPI) and other security features that require consistent traffic flows. Asymmetric traffic flows can lead to incorrect DPI results, ineffective security policies, and overall degraded network performance. To achieve symmetrical traffic flows, it's essential to carefully plan routing policies and load balancing mechanisms in the SD-WAN design.

upvoted 1 times

**Eards** 2 years, 10 months ago

Selected Answer: C

Answer C

upvoted 2 times

**simcos** 3 years ago

Selected Answer: C

See: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EE/IG-WAN/EE-WAN-IG/EE-WAN-IGch1.html

upvoted 2 times

**roganjosh** 3 years, 6 months ago

Selected Answer: C

Correct Answer is C

upvoted 3 times

⊟ **Surfside92** 3 years, 10 months ago

Answer A is incorrect. AS-path prepending influences ingress traffic - not egress traffic as stated in the answer A

upvoted 3 times

⊟ **CCNPWILL** 4 years, 2 months ago

Answer is A is correct as is.

upvoted 4 times

⊟ **ImAlwaysRight** 3 years, 12 months ago

Even when vSmart uses OMP for routing decisions and not BGP? I believe D is correct.

upvoted 3 times

⊟ **Emily23** 2 years, 2 months ago

You believe (or not) in God.
When it comes to technical documentation you either know it or not.

A is not correct because you use prepend to influence ingress traffic (not egress).

upvoted 1 times

⊟ **Clauster** 2 years, 1 month ago

Actually you can Prepend both ways Egress and Ingress, nice burn but you didn't finish it right.

upvoted 1 times

## Question #98 *Topic 1*

When IPsec VPNs are designed, what is a unique requirement if support for IP Multicast is required?

A. encapsulation of traffic with GRE or VTI

B. IPsec forwarding using transport mode

C. additional bandwidth for headend

D. IPsec forwarding using tunnel mode

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**rted** 1 year, 8 months ago

Dynamic routing protocols rely on using IP multicast or broadcast packets, but IPsec does not support encrypting multicast or broadcast packets. The current method for solving this problem is to use generic routing encapsulation (GRE) tunnels in combination with IPsec encryption.

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/41940-dmvpn.html

upvoted 1 times

**salmarin** 2 years, 1 month ago

**Selected Answer: A**

IPSec does not allow to transmit Multicast and Broadcast traffic via a IPSec VPN, so we should use GRE.

upvoted 1 times

**Lungful** 2 years, 6 months ago

**Selected Answer: A**

A is correct. IPsec does not natively support multicast traffic so encapsulation via GRE is commonly used.

upvoted 1 times

Question #99 *Topic 1*

Which control-plane technology allows the same subnet to exist across multiple network locations?

A. LISP

B. VXLAN

C. FabricPath

D. ISE mobility services

**Correct Answer:** *A*

*Community vote distribution*

A (89%) 11%

**lygris** Highly Voted 👍 4 years, 8 months ago

VXLAN is not a control plane technology, answer is A - LISP

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

upvoted 14 times

**Kacein** Most Recent 1 year, 4 months ago

Selected Answer: B

Just Like you, I thought that LISP was the answer. BUT LISP is not capable of extend a broadcast domain. VXLAN, on the other hand, can do this. AND LISP, is in fact, the control-plane but of the SD-Access, in the SDA environment, data plane is VXLAN, but generally speaking (that is, in "underlay") VXLAN is a control plane protocol, because routers and switches use the control plane to use VXLAN.

upvoted 1 times

**akbntc** 2 years ago

Selected Answer: A

It's A: LISP

upvoted 1 times

**Tiamat** 2 years, 9 months ago

Selected Answer: A

Answer is definitley A

upvoted 1 times

**andrewChan** 2 years, 10 months ago

Selected Answer: A

LISP for sure!

VXLAN is data plane

upvoted 2 times

**cwoolie** 3 years, 5 months ago

Answer is A

upvoted 1 times

**bogd** 3 years, 6 months ago

Selected Answer: A

LISP - control plane

upvoted 1 times

**Xavi07** 4 years, 1 month ago

Answer is LISP. I agree

upvoted 2 times

**luisjuradoledesma** 4 years, 7 months ago

I agree, it should be A - VXLAN is a data plane technology - LISP is control plane related.

upvoted 4 times

Question #100 *Topic 1*

An engineer is upgrading a company's main site to include a connection to a second ISP. The company will receive full Internet routing tables from both ISPs via
BGP. The engineer must ensure that the company does not become a transit autonomous system. Which solution should be included in this design?

A. Tag incoming routes from both ISPs with BGP community no-export.

B. Lower the MED for updates sent to the secondary ISP.

C. Use a route-map to prevent all prefixes from being advertised to either ISP.

D. Modify the local-preference for routes incoming from the primary ISP.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**ExodiaNecross59** Highly Voted 4 years, 8 months ago

As far as I know there are 4 methods how you can prevent becoming a transit AS:

Filter-list with AS PATH access-list.
No-Export Community.
Prefix-list Filtering
Distribute-list Filtering

https://networklessons.com/bgp/bgp-prevent-transit-as

upvoted 7 times

**TheGorn** Most Recent 1 year, 8 months ago

**Selected Answer: A**

no-export and no-advertise has been repeated endlessly in the course content.

upvoted 3 times

Question #101 *Topic 1*

An architect is working on a design to connect a company's main site to several small to medium-sized remote branches. The solution must include redundant
WAN links, but the customer has a limited budget and wants the ability to increase the link speed easily in the future. QoS will run on the branch routers, so there is no need for consistent end-to-end QoS. Which solution does the architect propose?

A. dual-homed WAN MPLS with single-edge router

B. dual-homed Internet with a single-edge router running a site-to-site VPN topology

C. dual-homed WAN MPLS and Internet links via dual-edge routers

D. dual-homed Internet with dual-edge routers running a hub-and-spoke VPN topology

**Correct Answer:** *B*

*Community vote distribution*

B (67%) D (33%)

**ALOVEVIKS** Highly Voted 2 years, 3 months ago

Selected Answer: B

The solution must include redundant WAN links - dual-homed Internet
but the customer has a limited budget - a single-edge router
and wants the ability to increase the link speed easily in the future. QoS will run on the branch routers, so there is no need for consistent end-to-end QoS. - site-to-site VPN topology

B. dual-homed Internet with a single-edge router running a site-to-site VPN topology

upvoted 5 times

**chaba7654321** Most Recent 11 months, 3 weeks ago

Selected Answer: D

going with D, as hub and spoke is more suitable

upvoted 1 times

**neiker45** 1 year, 7 months ago

Hub and spoke.

The main site will be the hub and the branches the spokes. You could even use something like DMVPN to set up the links dynamically and while you're at it you are setting up the company for future expansion (more branches).

upvoted 1 times

**salmarin** 1 year, 7 months ago

Selected Answer: D

I would go with Hub and spoke rather than site to site, and what's the point of two WAN links with a single router ? despite the limited budget dual homed router make sense.

upvoted 1 times

**cerifyme85** 2 years, 5 months ago

Selected Answer: B

multiple branches does not mean u need multiple physical links or routers.. the WAN transport is internet with VPN tunnels.. answer is B

upvoted 3 times

**jzzmth** 2 years, 6 months ago

Selected Answer: B

I am definitely going with B here.
DIA is cheaper than MPLS
Single edge router is cheaper than dual edge routers

upvoted 4 times

**Noproblem22** 2 years, 7 months ago

I will go for D

upvoted 1 times

**iLikeHamburgers** 2 years, 8 months ago

**Selected Answer: B**

First of all, these answers suck.

An internet connection is usually cheaper than an MPLS

2 routers cost more to operate/own than 1

That being said C & D are out because both solution state "dual-edge" routers.

The cheapest solution between A & B is B because B is an internet link, and A is an MPLS link. Further more it mention that "there is no need for consistent end-to-end QoS.", well with MPLS we can ask/require for SLA's in our contract, with an internet connection we cannot. That leaves me with answer B.

upvoted 4 times

**andrewChan** 2 years, 10 months ago

**Selected Answer: B**

I would prefer B as following reason,

1. limited budget

2. does not mention about spoke to spoke connectivity in the requirement.

so D is not best in the suitation.

the VPN may configure as GRE IPSec or under VTI

upvoted 1 times

**zlimvos** 3 years, 2 months ago

**Selected Answer: D**

it's the 'hub and spoke' that we need rather than site2site vpn with multiple branches

upvoted 2 times

**bogd** 3 years, 6 months ago

**Selected Answer: D**

Multiple branches, redundant links.

upvoted 4 times

**cerifyme85** 2 years, 5 months ago

multiple branches does not mean u need multiple physical links or routers.. the WAN transport is internet with VPN tunnels.. answer is B

upvoted 2 times

**enterTheDevOps** 3 years, 7 months ago

Answer D:

Single Hub to multiple branches? I believe this should be D

upvoted 3 times

**cryptonite** 3 years, 6 months ago

The reason for B is the fact that the customer has limited budget.

upvoted 2 times

**rjamxy** 3 years, 5 months ago

That does make sense... They mention only redundant WAN links and limited budget... It might imply that they would be fine with only one router.

upvoted 2 times

**zlimvos** 3 years, 2 months ago

it's the 'hub and spoke' that we need rather than site2site vpn with multiple branches

upvoted 1 times

**cerifyme85** 2 years, 5 months ago

multiple branches does not mean u need multiple physical links or routers.. the WAN transport is internet with VPN tunnels.. answer is B

upvoted 1 times

Question #102 *Topic 1*

An engineer must design a solution to connect a customer to the Internet. The solution will include a Layer 3 circuit with a CIR of 50 Mbps from the service provider. The hand-off from the provider's switch to the customer's router is 1Gbps. Which solution should the engineer include to prevent potential issues with choppy voice traffic?

A. Reduce the bandwidth of the connection to the router.

B. Implement hierarchical QoS with a parent policing policy.

C. Implement hierarchical QoS with a parent shaping policy.

D. Add a bandwidth statement to the router interface.

**Correct Answer:** *C*

*Community vote distribution*

C (54%) B (46%)

**andrewChan** Highly Voted 👍 3 years, 4 months ago

**Selected Answer: B**

to correctly understand this question, firstly eliminate answer which are definitely no correct, A & D;
then look at answer B &C, hierarchical QoS, which is a method to put 2 policy-map nested together, the parent policy-map control the overall channel bandwidth granted, the child policy-map control actual bandwidth allocate to each type of service.

in the question, the service provicer grant CIR of 50Mbps which is allocated to parent policy-map and the voice traffic is allocated in child policy-map. As 50Mbps CIR is granted by ISP so (B) policing on parent policy is correct.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/xe-16/qos-plcshp-xe-16-book/qos-plcshp-hier-clr-plc.html

https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-2/qos/configuration/guide/qc42hqos.html

upvoted 8 times

**andrewChan** 3 years, 4 months ago

BTW, for Voice traffic is always assign to policing or priority queue in LLQ

Traffic Policing is recommended for Voice, Video and Rich media traffic where generally UDP based communication takes place, and delay for packets will cause poor in quality. On the other hand Traffic Shaping is recommended for TCP based applications which can bear delay in traffic but need high data transfer rate like SAP etc.

https://ipwithease.com/traffic-policing-vs-shaping/

upvoted 2 times

**andrewChan** 3 years, 4 months ago

sorry a bit misunderstand the feature.

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html#anc17

in this case the answer should be C, not related to the CIR but if parent policy-map use police, it will override priority of voice service in the child policy-map

upvoted 3 times

**jzzmth** Highly Voted 👍 3 years ago

**Selected Answer: C**

The answer is C.
Always SHAPE on egress towards a service provider in the parent policy, then use child policies to set priorities as you see fit (in this case VoiP).
Generally, shaping = egress (i.e. towards ISP), policing = ingress (this is how ISPs drop traffic that exceed the CIR you are paying them for).
Sources:
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html#anc17

upvoted 7 times

**stee_hello** 2 years, 12 months ago

Yep. Create a policy map with just the default class which contains the 50M CIR then a service-policy containing a priority queue for voice is how I'd do it.

upvoted 1 times

**12504a3** Most Recent 6 months, 1 week ago

Selected Answer: C

From OCG :
- Shaping : commonly used to smooth the traffic going out to the provider (useful to not exceed the contracted rate). Slows down the rate at which packets are sent out an interface (egress).
- Policing : Commonly used to give preferential treatment to critical apps (higher class) and reducing best-effort traffic (lower class). Sets the limit of traffic coming into an interface (ingress).

At first I wanted to put B as the answer, but the goal here is to not exceed CIR 50 Mbps and this is something we need to deal with because our egress interface is 1 Gbps. So I'm going with C.
B is one right answer, but not the best, since we are given the CIR and this is definitely related to Shaping. You are tested on this specific point on this question.

Even if, from my point of view, doing both Shaping and Policing should be the best answer.

upvoted 2 times

**5c725f5** 1 year, 5 months ago

Selected Answer: C

It's a sub line rate circuit. You need to shape that or it'll be messy. Shaping is a hard requirement, not policing. You'll attach a child policy with a strict priority queue. That queue technically is policed, but you need a shaper as the parent at the very minimum.

upvoted 2 times

**26d13e9** 1 year, 10 months ago

For this specific scenario, the only way to guarantee the ISP will not drop the voice traffic is to make sure not to exceed the CIR from the customer side. This can only be guaranteed by policing out. All comments about shaping is correct but for this particular question.....policing.

upvoted 1 times

**salmarin** 2 years, 1 month ago

Selected Answer: B

because it's voice.

upvoted 1 times

**Michellangelo** 2 years, 1 month ago

Selected Answer: C

Egress = Shaping , ingress Policing is the basic principle. To add, following this discussion, https://community.cisco.com/t5/routing/hierarchical-qos/td-p/456350 , I'm even more convinced the answer is C

upvoted 1 times

**salmarin** 2 years, 1 month ago

Selected Answer: C

we will use shaping not policing

upvoted 1 times

**LSLS55** 2 years, 5 months ago

I think that C is the correct answer. The engineer can configure Shaping on Egress interface towards ISP. ISP is Policing on Ingress interface, the engineer has no access nor can configure ISP devices. Anyone agrees?

upvoted 1 times

**beskar** 2 years, 6 months ago

Selected Answer: C

Pull up any hierarchal QOS example from Cisco on an ethernet interface an you will see it is the shape command for the parent policy.

upvoted 1 times

**Clauster** 2 years, 7 months ago

Selected Answer: C

Oh men after analyzing this question i just realized something, they want us to set this QoS on our Router, not the ISP router, and then it clicked, Shaping is using on Egress Interfaces and Policing is configured on Ingress Interfaces, in this case Shaping will be setup on our Router, but we can't do policing because we are not managing traffic into our network, we are managing packets out of our router (Egress) for the voice going out. This is Shaping. Makes sense

upvoted 2 times

**cerifyme85** 2 years, 11 months ago

**Selected Answer: C**

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/xe-16/qos-plcshp-xe-16-book/qos-plcshp-oview.html#:~:text=in%20the%20bucket.-,Traffic%20Policing,the%20traffic%20to%20the%20speed%20of%20the%20interface%20receiving%20the%20packet.,-Was%20this%20Document

upvoted 2 times

**Sickcnt** 3 years, 4 months ago

**Selected Answer: B**

B is correct.
Whats the difference between Policing and Shaping?

-If there is an exceeding burst of traffic Policing will cut off the exceeding traffic
-If there is an exceeding burst of traffic Shaping will put the traffic into a que and try to send out the packets once the congestion is gone.

It is silly to start Shaping (aka.: "Queuing") Voice traffic since it would be all over the place

Also for QoS we are usually doing "LLQ" to prioritize Voice traffic, but that would mean voice traffic could totally overtake the whole bandwitdh
> Thatswhy we put a "hard policing" at a certain bandwith on policing (not to take over the whole bandwitdth)

Configuration snippet for example:

https://networklessons.com/quality-of-service/policing-configuration-example

upvoted 2 times

**Audie** 4 years ago

C is correct. Never use Policing on Voice

upvoted 2 times

**XalaGyan** 3 years, 1 month ago

Always use police on voice. voice packets are small and contain 20ms of payload. human ears autofill those 20ms and are too slow to check if a packet or two are missing. never shape to no send packets delayed and out of order as the human ear will immediately notice the delay and the out of order of words or tones.

use a PQ , Fair Queue . put voice on PQ and prevent it from taking over the world by policing it down to how much BW you need to give for example 5% or fixed Mbps of total. that way everyone can live happily ever after

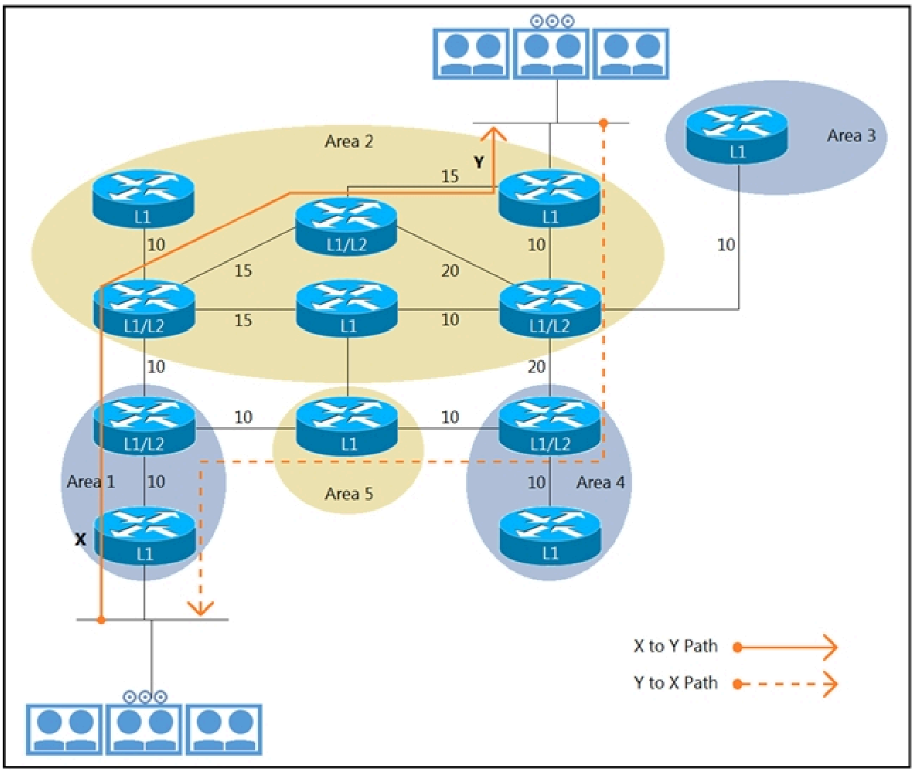
upvoted 1 times

**Emily23** 2 years, 8 months ago

Should I trust someone on the internet telling that payload is measured in ms ?... It is C

upvoted 1 times

Question #103 *Topic 1*



Refer to the exhibit. Customers report low video quality and delays when having point-to-point telepresence video calls between the two locations. An architect must optimize a design so that traffic follows the same path for egress and ingress traffic flows. Which technique optimizes the design?

A. Configure route leaking on the router in area 2.

B. Configure route leaking on the router in area 1.

C. Configure the high metric on the router in area 4.

D. Configure route filter on the router in area 4.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**andit** Highly Voted 3 years ago

The correct answer is A:
IS-IS Level1 Router allways take the route towards the closest L2 Router, when trying to reach a destination outside the AS. That is the reason why the return-traffic takes a different way here.
The problem occurs because Level1 and Level2 topologies are examied separatly by the respective routers. The solution is to hand down Level2 routing-information about the destination networks into Layer1 routing, so it can be included into path selection.
upvoted 9 times

**mgiuseppe86** 1 year, 5 months ago

After changing Area5 Router to L2, the Lab is accurate. X to Y flows one way, and Y to X flows another. I think it's a typo on the lab diagram.

There is just no possible way ingress would come back through A5 with the only router being an L1 router. its just not possible.
upvoted 2 times

**mgiuseppe86** Most Recent 1 year, 5 months ago

I dont quite understand this lab. I have created it and Area5 L1 router cannot form adjacencies with Area1 Area4 or Area2... A5 needs a L1L2 or L2 router. how is that path even working? There must be missing info on this lab. Some other routing protocol must be enabled for Area 5 to work.

Same can be said for Area 3 but that is not vital to the question, its just fluff.

upvoted 1 times

**CKL_SG** 1 year, 9 months ago

Selected Answer: A

IS-IS Route Leaking

IS-IS routers in a level 1 area only know the prefixes in their own area. If they want to reach something in another area, they have to use a default route to a level 1-2 router. If there are multiple level 1-2 routers, then IS-IS picks the closest level 1-2 router to exit the area. This sometimes causes sub-optimal routing.

We can deal with this by leaking prefixes from level 2 into level 1.

A level 1-2 router has access to the local area and also knows all prefixes because of its level 2 database. We can redistribute one or more prefixes from level 2 into the local area so that level 1 routers can select the most optimal path in the network.

upvoted 3 times

**emre076** 2 years, 2 months ago

Selected Answer: A

yep, A

upvoted 1 times

**zlimvos** 2 years, 8 months ago

Selected Answer: A

I also agree with route leaking in area2

upvoted 1 times

**python_tamer** 2 years, 9 months ago

Selected Answer: A

Yep, I think A is correct here.

upvoted 1 times

**rjamxy** 2 years, 11 months ago

Yeah it does seems that A can be the correct answer here

https://www.cisco.com/c/en/us/support/docs/ip/integrated-intermediate-system-to-intermediate-system-is-is/13796-route-leak.html

"Packets destined for an address that is outside of the L1 area are routed to the closest L1/L2 router to be forwarded on to the destination area. Routing to the closest L1/L2 router can lead to sub-optimal routing when the shortest path to the destination is through a different L1/L2 router. Route leaking helps reduce sub-optimal routing by providing a mechanism for leaking, or redistributing, L2 information into L1 areas. "

upvoted 1 times

**cwoolie** 2 years, 11 months ago

I research but can't find correct answer. Is it A or C???

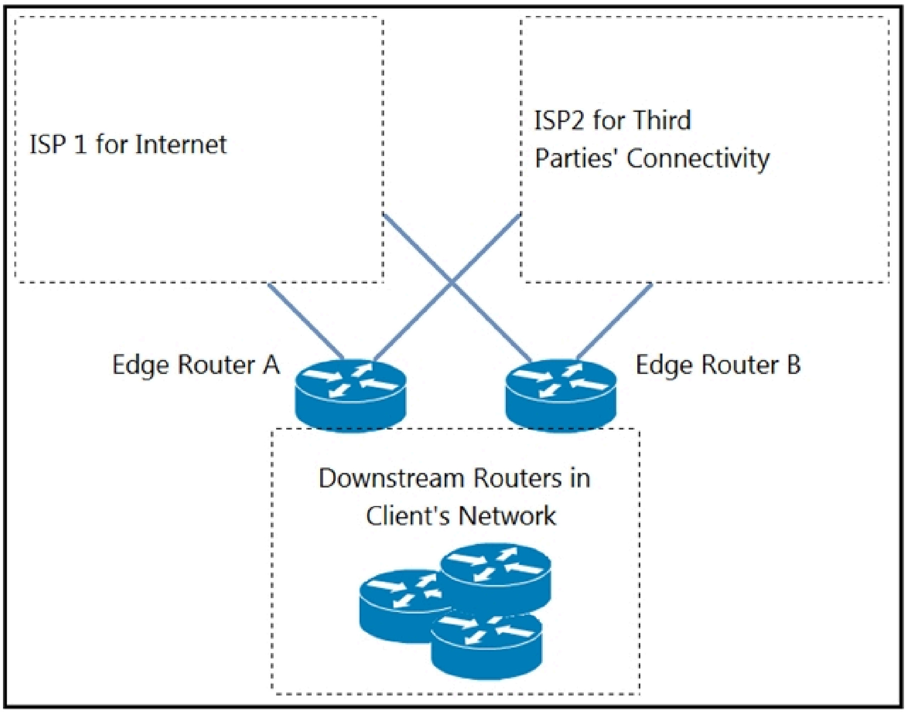
upvoted 1 times

**iSDA69** 4 months, 3 weeks ago

Cannot be C because the L1 router has the default route ONLY from the nearest L1/L2 router, that is the router below him (cost 10 vs cost 15 for the router on its side). If you change metric in area 4 does not change anything about this choice.

upvoted 1 times

Question #104 *Topic 1*


ISP 1 for Internet
ISP2 for Third Parties' Connectivity
Edge Router A
Edge Router B
Downstream Routers in Client's Network

Refer to the exhibit. An engineer is designing a BGP solution for a client that peers with ISP1 for full Internet connectivity and with ISP2 for direct exchange of routes for several third parties. Which action, when implemented on the edge routers, enables the client network to reach the Internet through ISP1?

A. Run an eBGP session within different VRFs for each ISP.

B. Advertise a default route for downstream routers within the client network.

C. Apply the AS-path prepend feature for ISP2.

D. Apply route filtering such that the client advertises only routes originated from its own AS.

**Correct Answer:** *B*

*Community vote distribution*

B (67%) D (33%)

**neiker45** 1 year, 7 months ago

You can provide your client's network access through a specific ISP by simply setting up a default route going through that ISP to the downstream routers.

upvoted 1 times

**salmarin** 1 year, 7 months ago

**Selected Answer: B**

advertise default route to downstream routers.

upvoted 2 times

**Nickplayany** 2 years, 3 months ago

**Selected Answer: B**

B is the answer

upvoted 1 times

**cerifyme85** 2 years, 4 months ago

Sorry guys B seems correct.. using neigh default-originate or network 0.0.0.0 at isp

upvoted 2 times

**cerifyme85** 2 years, 5 months ago

**Selected Answer: D**

I will go with either A or D.. with D as my preference

upvoted 1 times

⊟ **cerifyme85** 2 years, 5 months ago

hmmm not sure I agree with B.. how does it handle segregation of traffic to internet?

upvoted 1 times

⊟ **vins0** 2 years, 3 months ago

Default route for all internet traffic, for third party there will be more specific routes from ISP2. Anything else non-specific would take default route.

upvoted 2 times

Question #105 *Topic 1*

An engineer must propose a solution for a campus network that includes the capability to create multiple Layer 3 virtual networks. Each network must have its own addressing structure and routing table for data forwarding. The solution must be scalable to support hundreds of virtual networks and allow simple configuration and management with minimal administrative overhead. Which solution does the engineer recommend?

A. hop-by-hop EVN

B. multihop MPLS core

C. multihop IPsec tunneling

D. hop-by-hop VRF-Lite

**Correct Answer:** *B*

*Community vote distribution*

B (52%) D (33%) 14%

**cryptonite** Highly Voted 4 years ago

Selected Answer: B

I disagree on EVN because it has a limitation of 32 VNs. The questions says can scale to hundreds of Virtual Network

upvoted 7 times

**Clauster** Highly Voted 2 years, 6 months ago

I found the Cisco White Papers that talks about EVNs

- You are correct when you say we can only use 32VNs, but this is only limited to one IP Infrastructure. Since each Branch will have it's own IP Infrastructure then we can do 32VNs at each branch, so if you have 10 branches x 32VNs that puts you well over hundreds of VNs that can be supported with this feature.
- MPLS Core requires tons of Administrative Overhead.
- VRF Lite supports up to 8 VNs.
- Only Clear answer here is A, keep in mind they also mention Easy to configure, EVN is known for easy configuration.

upvoted 5 times

**Clauster** 2 years, 6 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/xe-3s/evn-xe-3s-book/evn-overview.html#GUID-3E71EB2C-7ACC-47AE-9173-FB31BA61C319

upvoted 1 times

**mgiuseppe86** 2 years, 5 months ago

As right as this may be, knowing Cisco, the question is really asking what routing protocol supports the most VNs. gun to my head i will say B, but A is probably more right given the scenario.

upvoted 1 times

**PicoOstrava** Most Recent 1 year, 3 months ago

Selected Answer: B

MPLS Core (B): MPLS is designed to scale and can handle the segmentation of hundreds of virtual networks much more effectively than VRF-Lite. MPLS allows for easier management of large-scale environments, especially when multiple virtual networks need to be created and routed independently. MPLS provides both scalability and flexibility, making it a good fit for large deployments with multiple virtual networks.

• VRF-Lite (D): While VRF-Lite can work in smaller networks, it doesn't scale well for hundreds of virtual networks. It can cause administrative overhead and performance degradation as the number of VRFs increases. It is more suited for smaller to medium-sized environments rather than large-scale deployments.

upvoted 1 times

**Adaletherkesicin** 2 years ago

Selected Answer: A

A is correct answer

upvoted 1 times

**Gilgamesh_SHA** 2 years ago

Selected Answer: A

MPLS Core is overkill for a campus network, and it can't separate address structures and routing tables by itself. MPLS VPN must be deployed for this purpose.

EVN supports 32 VNs per IP infrastructure/interface.

I go for A due to ease of management, scalability, and operational efficiency.

upvoted 2 times

⊟ **Clauster** 2 years, 7 months ago

**Selected Answer: B**

EVN: Supports up to 32 VN not hundreds like our requirements XX

VRF Lite: Is recommended for smaller amounts of VN requirements XX

IPsec Tunneling: Would be great but it requires Tons of Administrative Overhead because we would have to sit there and configure all of the VNs.

Multi Hop MPLS is the best answer, you can scale MPLS for hundreds if not thousands of Virtual Networks with very little overhead because your ISP does all the work. The requirements never stated we needed to save Money which we are kinda defaulted to in our IT Heads. Answer is C

upvoted 1 times

⊟ **CKL_SG** 2 years, 9 months ago

**Selected Answer: B**

VRF-lite support less than 8 vn

EVN only support up to 32 vn

MPLS Core support hundreds or thousand VN

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/Network_Virtualization/sccsolover.html#wp416666

upvoted 2 times

⊟ **SpicyMochi** 2 years, 10 months ago

**Selected Answer: D**

D. hop-by-hop VRF-Lite

To meet the requirement of creating multiple Layer 3 virtual networks, each with its own addressing structure and routing table for data forwarding, the recommended solution is hop-by-hop VRF-Lite. This solution provides logical separation of multiple routing domains over a single physical infrastructure, allowing for the creation of multiple virtual networks with unique routing tables and addressing structures. VRF-Lite is scalable, providing support for hundreds of virtual networks, and has simple configuration and management with minimal administrative overhead.

upvoted 1 times

⊟ **andrewChan** 3 years, 4 months ago

**Selected Answer: D**

Table 1 Network Virtualization Technique Comparison Chart has the answer

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/Network_Virtualization/sccsolover.html

upvoted 4 times

⊟ **python_tamer** 3 years, 9 months ago

**Selected Answer: D**

This question is super tricky. It cannot be A (EVN) because of the max 32 VN limit.

That leaves us with MPLS, IPsec tunnels or VRF-Lite.

MPLS is a maybe but not easy to configure.

IPsec tunnels is a no.

VRF-Lite is a maybe. Easier than MPLS but still plenty of admin overhead.

So I think the best option is VRF-Lite: D

upvoted 2 times

⊟ **cryptonite** 4 years ago

I disagree on EVN because it has a limitation of 32 VNs. The questions says can scale to hundreds of Virtual Network

upvoted 2 times

⊟ **ImAlwaysRight** 4 years, 5 months ago

They say EVN scales up to 32 VN's maximum... But I read also that EVN is more scalable than VRF-Lite, so I am prone to agree on EVN to be the answer, but still not sure as the question mentions hundreds.

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

upvoted 3 times

⊟ **Hope66** 4 years, 6 months ago

I think A:

Hop-by-hop easy virtual network (EVN) based: Hop-by-hop VRF-lite is manageable for networks with fewer numbers of virtual networks and fewer numbers of hops in a virtual network path. However, when the number of logical networks (virtual/tenants) increases, there will be a high degree of operational complexity to create and configure the interface or subinterface per VN. EVN provides the same benefits for guaranteeing traffic separation with more simplified operations. In other words, EVN builds on VRF-Lite concepts and capabilities and provides additional benefits, including the following:

- EVN offers better end-to-end VN scalability compared to the classic hop-by-hop 802.1Q-based solution.
- EVN offers simplified configuration and management.
- EVN offers the capability to provision shared services among different logical groups.

upvoted 2 times

Question #106 *Topic 1*

An engineer must design a VPN solution for a company that has multiple branches connecting to a main office. What are two advantages of using DMVPN instead of IPsec tunnels to accomplish this task? (Choose two.)

A. support for AES 256-bit encryption

B. greater scalability

C. support for anycast gateway

D. lower traffic overhead

E. dynamic spoke-to-spoke tunnels

**Correct Answer:** *BE*

*Community vote distribution*

BE (100%)

**XalaGyan** 1 year, 7 months ago

**Selected Answer: BE**

Given answer is correct

upvoted 1 times

**Noproblem22** 1 year, 7 months ago

Given response are correct

upvoted 1 times

Question #107 *Topic 1*

How is Internet access provided to a WAN Edge router that is connected to a MPLS transport link?

A. OMP advertises a default route from a WAN Edge router that is connected to the MPLS and Internet transport networks.

B. Internet access must be provided at the WAN Edge router through either a 4G/5G link or local Internet circuit.

C. An extranet must be provided in the MPLS transport network to allow private traffic to reach the public Internet.

D. TLOC extensions are used to route traffic to a WAN Edge router that is connected to the Internet transport network.

**Correct Answer:** *D*

*Community vote distribution*

D (58%) A (25%) B (17%)

**night_wolf_in** 2 months, 3 weeks ago

Selected Answer: A

TLOC used for vedge to build tunnels through secondary link on secondary vedge device.

upvoted 1 times

**NoHombre** 5 months, 3 weeks ago

Selected Answer: A

That dual-connected WAN Edge advertises a default route (0.0.0.0/0) into the SD-WAN overlay via OMP (Overlay Management Protocol).
Other WAN Edges that only have MPLS learn this default via OMP.
They then forward Internet-bound traffic across the MPLS transport to the dual-connected site, which exits locally to the Internet.

Why not D?
TLOC extensions extend transport interfaces between adjacent routers at a site. They don't provide Internet reachability across the SD-WAN fabric on their own; you still need the OMP-advertised default route.

upvoted 1 times

**rickyarchi** 1 year, 6 months ago

Selected Answer: A

T-LOC extension is for providing high availability when two EDGEs are connected to two different circuits. It allows to use the pair router as an underlay.

upvoted 2 times

**salmarin** 1 year, 7 months ago

Selected Answer: A

Traffic can route to internet via a central router that have internet via advertising a default route via OMP.

upvoted 3 times

**bubd** 2 years ago

Correct: B
When a WAN Edge router is connected to an MPLS transport link and you want to provide Internet access to it, the typical approach is:

B. Internet access must be provided at the WAN Edge router through either a 4G/5G link or a local Internet circuit.

In this scenario, the WAN Edge router is connected to the MPLS network for private traffic but needs a separate Internet connection to access the public Internet. This can be achieved through a 4G/5G cellular link or a dedicated local Internet circuit, allowing the router to route traffic to the public Internet while using the MPLS network for private traffic.

upvoted 1 times

**Clauster** 2 years, 1 month ago

Selected Answer: D

This question is a very good question, but the answer is TLOC Extensions, these guys explain it in such way here is amazing and it then clicks:
https://www.networkacademy.io/ccie-enterprise/sdwan/tloc-extension

upvoted 3 times

⊟ **cerifyme85** 2 years, 5 months ago

Selected Answer: B

Not sure I agree.. the question says a WAN edge router not 2.. and also "how is internet provided"? I am taking a stab for B

upvoted 2 times

⊟ **salmarin** 1 year, 7 months ago

exactly, one router not two , don't know how some people thing and answer.

upvoted 1 times

⊟ **Sickcnt** 2 years, 10 months ago

Selected Answer: D

"What is TLOC Extension?
TLOC extension is a feature that allows a WAN Edge router to communicate over the WAN transport connected to the adjacent WAN Edge router through a TLOC-extension interface"

Link:
https://www.networkacademy.io/ccie-enterprise/sdwan/tloc-extension

upvoted 4 times

⊟ **certstudent2016** 3 years, 4 months ago

D is correct!!
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKRST-2091.pdf

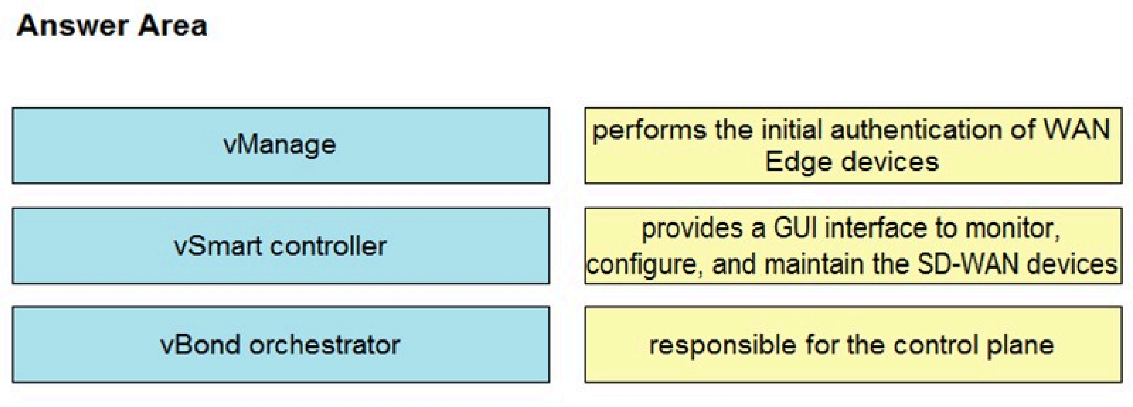
upvoted 2 times

Question #108 *Topic 1*

DRAG DROP -

Drag and drop the elements from the left onto the functions they perform in the Cisco SD-WAN architecture on the right.

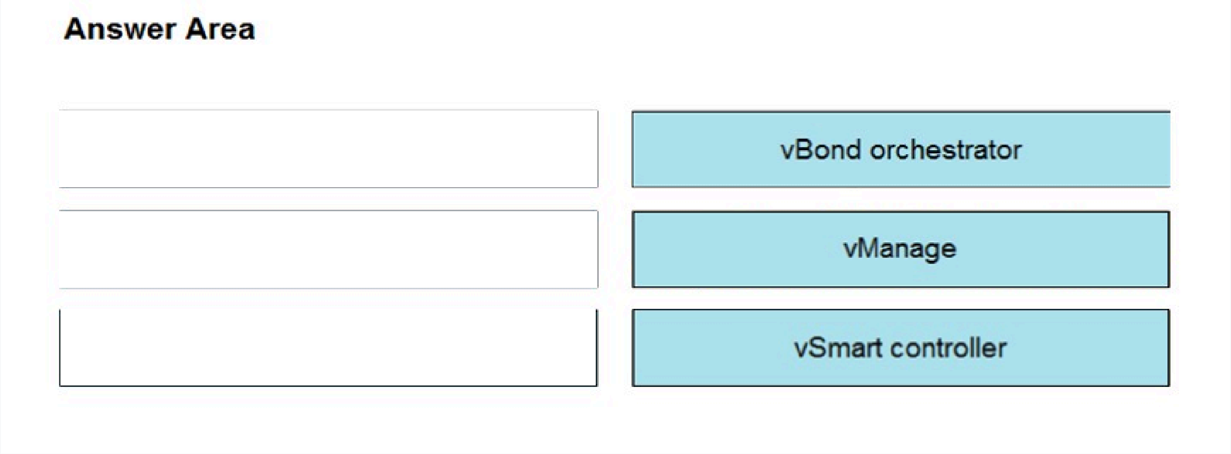
Select and Place:



**Answer Area**

| | |
|---|---|
| vManage | performs the initial authentication of WAN Edge devices |
| vSmart controller | provides a GUI interface to monitor, configure, and maintain the SD-WAN devices |
| vBond orchestrator | responsible for the control plane |

**Correct Answer:**



**Answer Area**

| | |
|---|---|
| | vBond orchestrator |
| | vManage |
| | vSmart controller |

**certstudent2016** 1 year, 4 months ago

Correct Answer!!

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html

upvoted 2 times

Question #109 *Topic 1*

Which method does Cisco SD-WAN use to avoid fragmentation issues?

A. PMTUD is used.

B. Access circuits are configured with 1600 byte MTU settings.

C. Jumbo frames are enabled.

D. Traffic is marked with the DF bit set.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**asd23355** 1 year, 2 months ago

**Selected Answer: A**

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 source to its destination.

upvoted 1 times

**certstudent2016** 2 years, 4 months ago

A is correct!

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

**ARTU_IT** 2 years, 7 months ago

**Selected Answer: A**

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf page 42

upvoted 1 times

**XalaGyan** 1 year, 7 months ago

Path MTU Discovery

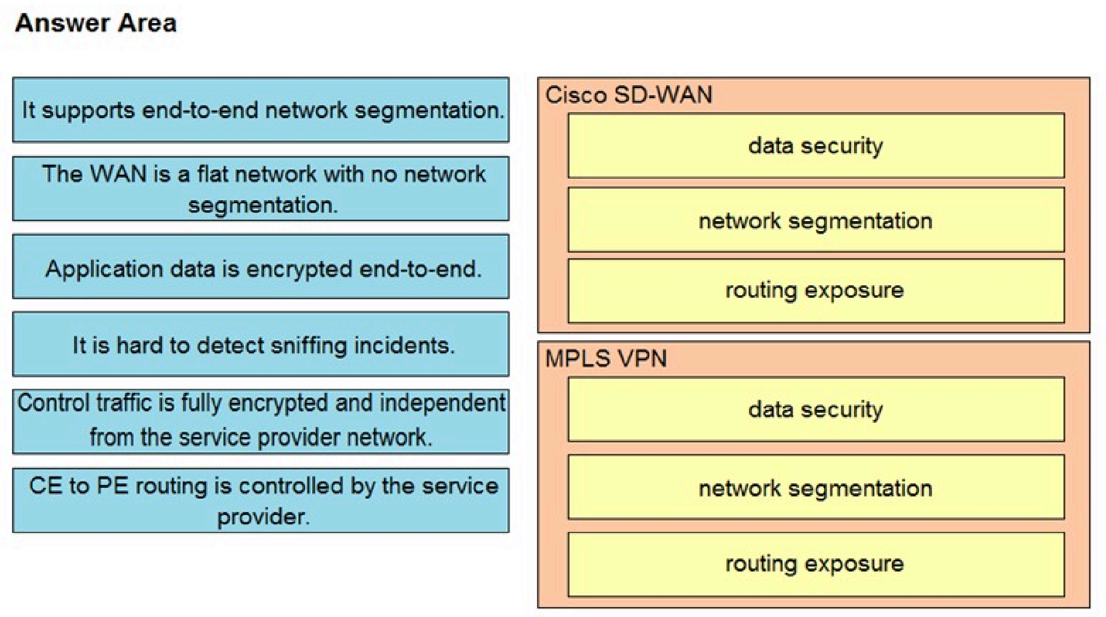
upvoted 1 times

Question #110 Topic 1

DRAG DROP -

Drag and drop the descriptions from the left onto the corresponding WAN connectivity types and categories on the right.

Select and Place:



Answer Area

It supports end-to-end network segmentation.

The WAN is a flat network with no network segmentation.

Application data is encrypted end-to-end.

It is hard to detect sniffing incidents.

Control traffic is fully encrypted and independent from the service provider network.

CE to PE routing is controlled by the service provider.

Cisco SD-WAN

data security

network segmentation

routing exposure

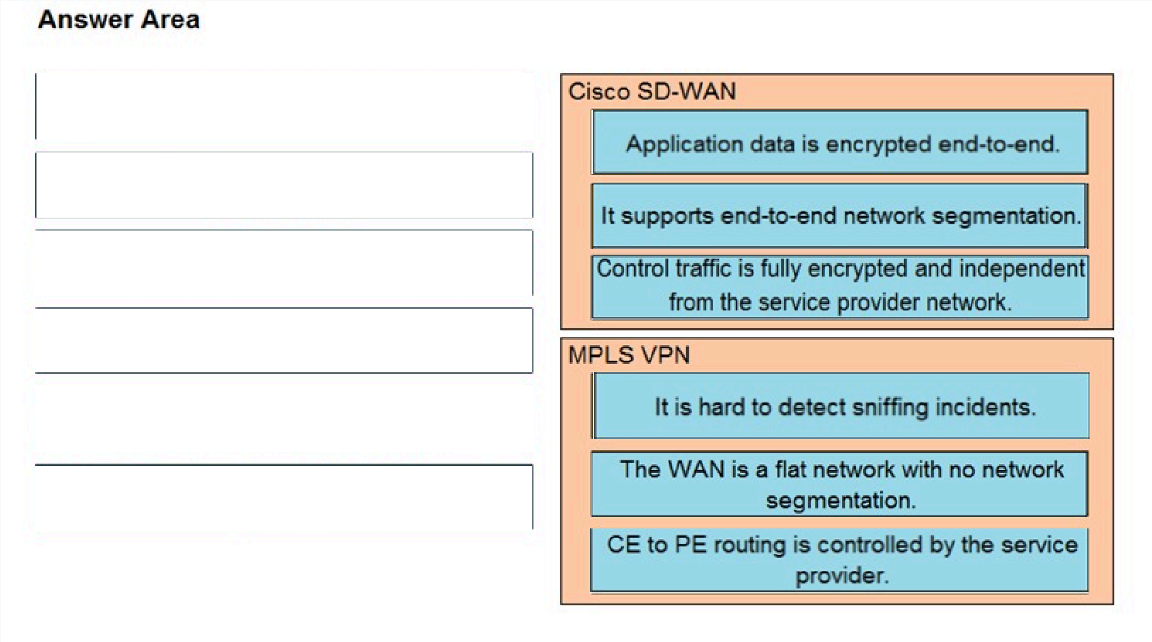
MPLS VPN

data security

network segmentation

routing exposure

**Correct Answer:**



Answer Area

Cisco SD-WAN

Application data is encrypted end-to-end.

It supports end-to-end network segmentation.

Control traffic is fully encrypted and independent from the service provider network.

MPLS VPN

It is hard to detect sniffing incidents.

The WAN is a flat network with no network segmentation.

CE to PE routing is controlled by the service provider.

⊟ **Lungful** 1 year, 6 months ago

I also agree that the answer is correct.

upvoted 1 times

⊟ **certstudent2016** 2 years, 10 months ago

Answer is Correct!!

https://www.teneo.net/blog/how-secure-is-the-sd-wan-vs-mpls-vpn-service/

upvoted 2 times

Question #111 *Topic 1*

A global organization with several branches hired a network architect to design an overlay VPN solution. The branches communicate with each other frequently.

The customer expects to add more branches in the future. To meet the customer's security requirements, the architect plans to provide traffic protection using dynamic IPsec tunnels. Which solution should the architect choose?

A. DMVPN

B. EasyVPN

C. L2TP

D. GETVPN

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**salmarin** 1 year, 7 months ago

**Selected Answer: A**

DMVPN for dynamic tunnels

upvoted 1 times

**asd23355** 2 years, 2 months ago

**Selected Answer: A**

DMVPN : can be thought of as an evolution of the standard IPsec tunnel with some added redundancy benefits. While IPsec VPN tunnels are hardcoded and essentially "nailed up" between two locations, DMVPN builds tunnels between locations as needed.

upvoted 1 times

**bccabrera** 2 years, 3 months ago

**Selected Answer: A**

https://www.routexp.com/2017/08/quick-comparison-ipsec-vs-dmvpn-vs.html

upvoted 1 times

**Noproblem22** 2 years, 7 months ago

A is the right answer

upvoted 1 times

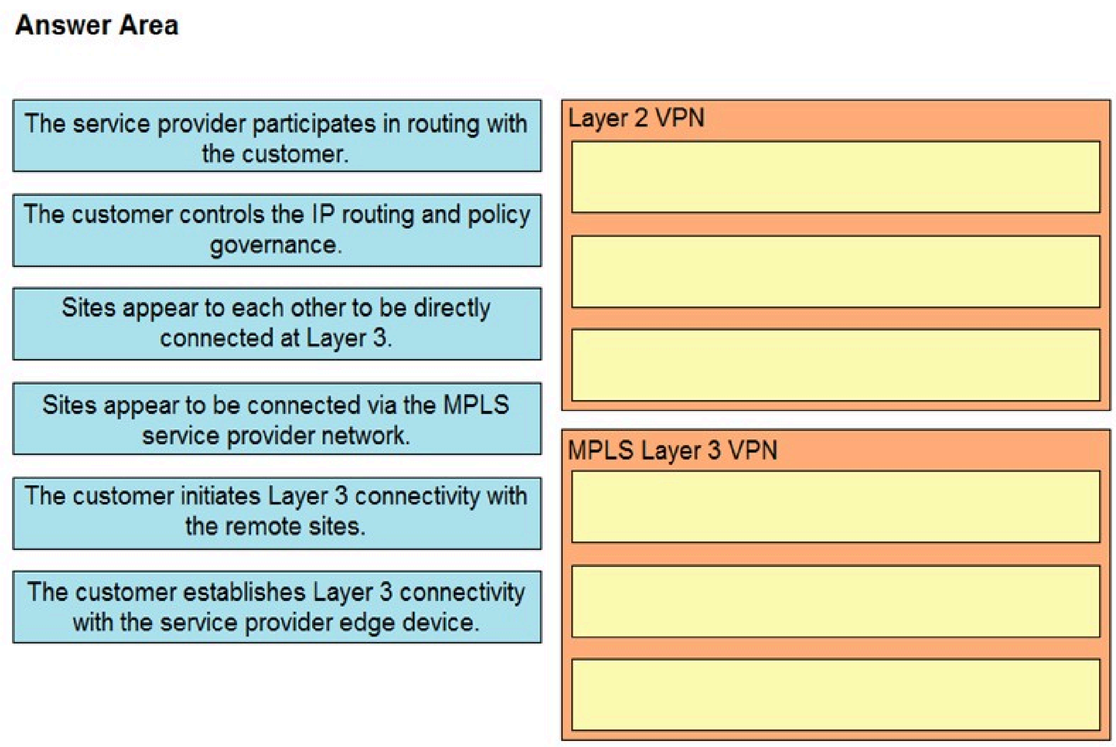
Question #112

Topic 1

DRAG DROP -

Drag and drop the descriptions from the left onto the corresponding VPN types on the right.

Select and Place:



Answer Area

The service provider participates in routing with the customer.

The customer controls the IP routing and policy governance.

Sites appear to each other to be directly connected at Layer 3.

Sites appear to be connected via the MPLS service provider network.

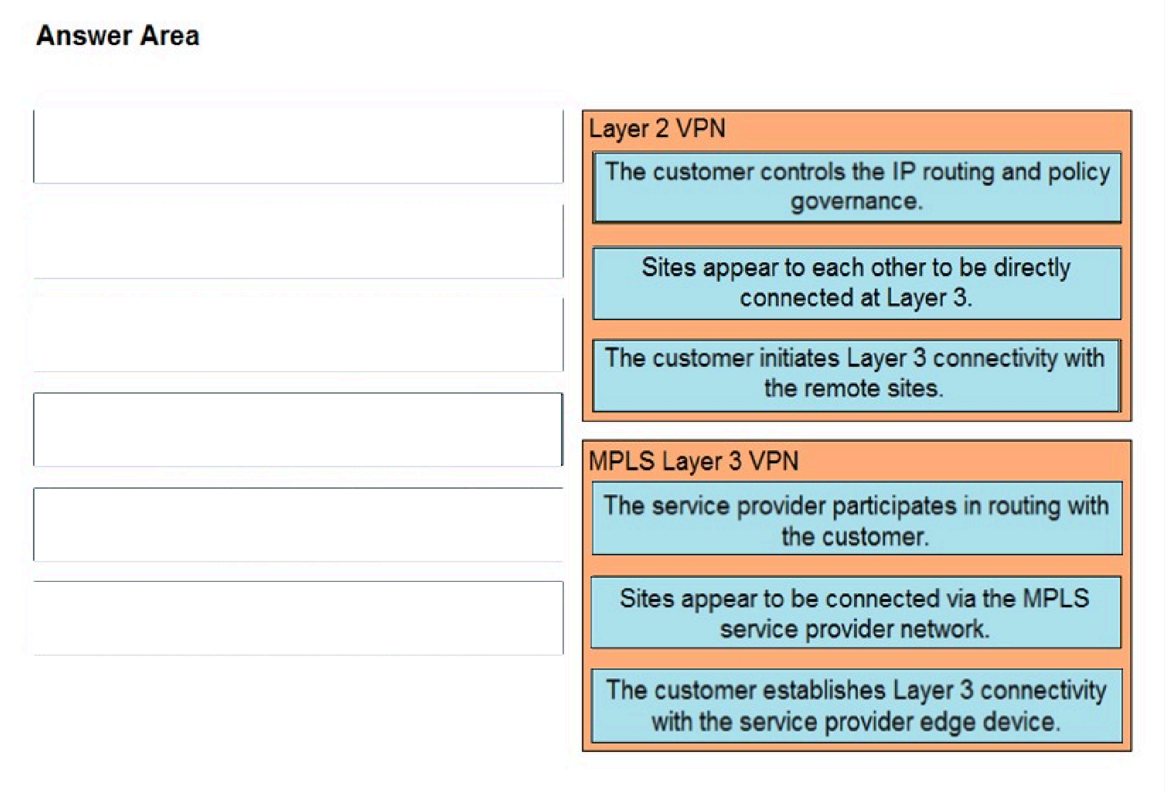
The customer initiates Layer 3 connectivity with the remote sites.

The customer establishes Layer 3 connectivity with the service provider edge device.

Layer 2 VPN

MPLS Layer 3 VPN

**Correct Answer:**



Answer Area

Layer 2 VPN

The customer controls the IP routing and policy governance.

Sites appear to each other to be directly connected at Layer 3.

The customer initiates Layer 3 connectivity with the remote sites.

MPLS Layer 3 VPN

The service provider participates in routing with the customer.

Sites appear to be connected via the MPLS service provider network.

The customer establishes Layer 3 connectivity with the service provider edge device.

**certstudent2016** 1 year, 4 months ago

Correct Answer!!

https://ipwithease.com/layer-2-vs-layer-3-vpn/#:~:text=Layer%202%20VPNs%20virtualize%20the,Internet%20or%20Service%20provider%20backbone.

upvoted 2 times

Question #113 *Topic 1*

A customer requests a VPN solution to connect multiple sites with the company headquarters. All the sites use the same IP subnet. The engineer plans to use
VPLS. Which solution must the engineer include in the design?

A. different VLANs on each site

B. address translation to hide overlapping subnets

C. 802.1Q connectivity on the LAN side of the CE

D. route exchange with the service provider

**Correct Answer:** *B*

*Community vote distribution*

B (50%) C (43%) 7%

**Beehurls** 11 months, 1 week ago

**Selected Answer: C**

VPLS is a way to share the same subnet at multiple sites. Using NAT to hide the overlapping subnets does not make sense and defeats the purpose. A few are caught up in the idea that the PE side should be configured with 802.1Q, but they must be looking at the configuration guide for the PE only. You are perfectly fine with configuring 802.1Q on the CE side, and it is required to use multiple VLANs.

upvoted 2 times

**Swiz005** 1 year, 6 months ago

**Selected Answer: B**

NAT is required for duplicate IPs - B

upvoted 1 times

**Beehurls** 11 months, 1 week ago

No one said anything about duplicate IPs. VPLS is a way to extend a L2 domain which means the design is meant to use the same subnet.

upvoted 1 times

**Abdulmw** 2 years, 4 months ago

**Selected Answer: D**

When connecting multiple sites that use the same IP subnet over a VPLS (Virtual Private LAN Service) network, it is essential to include route exchange with the service provider. VPLS is a Layer 2 VPN technology that extends the LAN segment across multiple sites, including the headquarters and remote locations. In such a scenario, the service provider plays a crucial role in ensuring that traffic is appropriately routed between the sites.

Route exchange with the service provider allows the service provider's network to understand the reachability of each site's IP subnets. This enables proper routing of traffic within the VPLS network, despite the overlapping IP subnets at different locations.

upvoted 1 times

**mgiuseppe86** 2 years, 5 months ago

**Selected Answer: B**

Cisco config guide states 802.1q should be configured on the PE side, not CE.. I am going with B

upvoted 1 times

**musclehamster** 2 years, 6 months ago

**Selected Answer: C**

Being in the same subnet does not mean there is an issue as long as there are no duplicate IPs

upvoted 2 times

**beskar** 2 years, 7 months ago

**Selected Answer: C**

VPLS is a L2 WAN technology therefore it makes sense that the answer be C and not B. NAT has nothing to do with this. The same IP subnet is nothing more than extending a subnet/vlan across a WAN to other sites.

upvoted 2 times

**Clauster** 2 years, 7 months ago

Selected Answer: C

Because VPLS is a L2 VPN topology, the best answer here is C, you need to configure VLAN on the CE side of the LANs at each site. This is the best answer. NAT can also be used but it will be way more work as you would have to manage several IP networks and handle all of those translations, and they are planning on scaling.

upvoted 2 times

**SpicyMochi** 2 years, 10 months ago

Selected Answer: B

B. address translation to hide overlapping subnets

When connecting multiple sites with the same IP subnet using VPLS, the engineer must include address translation to hide overlapping subnets. VPLS (Virtual Private LAN Service) is a Layer 2 VPN technology that allows multiple sites to appear as if they are connected to the same LAN segment, but each site must use a unique IP subnet. Address translation is used to map the overlapping IP subnets to unique subnets, allowing them to be transmitted across the VPLS network without conflicts.

upvoted 2 times

**cerifyme85** 2 years, 11 months ago

Selected Answer: B

Therefore LAn users would be on a different subnet behind CE and would still ned to NAT to ISP subnet... B

upvoted 1 times

**cerifyme85** 2 years, 11 months ago

I think the question meant all the CE routers on same subnet.

upvoted 1 times

> **cerifyme85** 2 years, 11 months ago
>
> Therefore LAn users would be on a different subnet behind CE and would still ned to NAT to ISP subnet... B
>
> upvoted 1 times

**jzzmth** 2 years, 11 months ago

I'm going with C.
The question states all sites use the same subnet... while answer "B" states [... NAT to hide overlapping subnetS ...]. To me this just doesn't sound correct because there is only 1 subnet in question and that answer uses the plural form of that word, also the question uses the words "must include" and you can absolutely get this working without any NAT involved if you treat it simply as a Layer2 extension (just don't have overlapping IPs).
"C" sounds more correct here because yeah if you use a VPLS circuit to extend a broadcast domain obviously you need to tag that traffic with a VLAN before you can even send it into the VPLS circuit.

upvoted 3 times

> **Clauster** 2 years, 7 months ago
>
> This is not correct, you cannot have overlapping subnets when using VLANs the router/switch won't allow you to configure overlapping subinterfaces. NAT is needed.
>
> upvoted 1 times

**iLikeHamburgers** 3 years, 2 months ago

Selected Answer: B

Question states "All the sites use the same IP subnet.", thus NAT is needed.

upvoted 2 times

**Reinier_veen** 3 years, 3 months ago

Selected Answer: C

"VPLS is a type of VPN that allows for the connection of multiple sites into a single L2 domain over a managed IP/MPLS network".
So the VPN represents a L2 "virtual switch".

upvoted 2 times

> **sylux** 3 years, 2 months ago
>
> It says here you should do it on the PE device not the CE
> Page 3-7
> https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-11/configuration_guide/mpls/b_1611_mpls_9300_cg/configuring_virtual___private_lan_service__vpls__and_vpls_bgp_based_autodiscovery.pdf
>
> upvoted 1 times

> **iLikeHamburgers** 3 years, 2 months ago

"All the sites use the same IP subnet."
We have to NAT the networks at each site because of this. Only answer that facilitates this requirement is B

upvoted 1 times

⊟ **Beehurls** 11 months, 1 week ago

You want to share the subnet with VPLS. So you should not hide it.

upvoted 1 times

⊟ **zzmejce** 3 years, 2 months ago

Don't we need 802.1q on the WAN side in this case...

upvoted 1 times

Question #114 *Topic 1*

An ISP provides Layer 3 VPN service over MPLS to a customer with four branches and multiple CE routers at each branch. To exchange the routes that are learned from the CE routers, which BGP address family should the ISP activate among the PE routers?

A. address-family multicast

B. L2VPN EVPN

C. VPNv4 unicast

D. IPv4 unicast

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**SpicyMochi** 1 year, 4 months ago

**Selected Answer: C**

C. VPNv4 unicast

To exchange routes learned from CE routers in a Layer 3 MPLS VPN service, the ISP should activate the VPNv4 unicast address family among the PE routers. VPNv4 unicast is the BGP address family used in MPLS VPN networks to exchange routing information between the PE routers. It carries the VPNv4 prefix, which includes both the customer IPv4 prefix and the route distinguisher (RD) value that identifies the VPN instance.

upvoted 1 times

**Reinier_veen** 1 year, 10 months ago

**Selected Answer: C**

http://www.mplsvpn.info/2009/11/difference-between-address-family-ipv4.html

" In short we can say that ipv4 address-family is being used for customers and vpnv4 address-family is used by SP core. "

upvoted 3 times

## Question #115 *Topic 1*

In the SD-WAN underlay network, which WAN Edge VPN ID is defined as the transport VPN and is used to carry control traffic?

A. VPN 0

B. VPN 512

C. VPN 128

D. VPN 256

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

⊟ **salmarin** 1 year, 7 months ago

**Selected Answer: A**

VPN0 is correct

upvoted 1 times

⊟ **Lungful** 2 years ago

**Selected Answer: A**

A is correct. Fresh from the ENCOR studies/exam.

upvoted 1 times

⊟ **Reinier_veen** 2 years, 9 months ago

VPN 0 = transport VPN

VPN 512 = management VPN for OOB-management

upvoted 4 times

⊟ **Hope66** 3 years ago

The answer provided is correct

upvoted 1 times

Question #116 *Topic 1*

A company's security policy requires that all connections between sites be encrypted in a manner that does not require maintenance of permanent tunnels. The sites are connected through a private MPLS-based service that uses a dynamically changing key and spoke-to-spoke communication. Which type of transport encryption must be used in this environment?

A. GETVPN

B. DMVPN

C. GRE VPN

D. standard IPsec VPN

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

⊟ **iLikeHamburgers** Highly Voted 2 years, 5 months ago

**Selected Answer: A**

Standard IPsec VPN isn't correct because it is not dynamic. It is a permanent VPN tunnel solution. The requirements state that "does not require maintenance of permanent tunnels"
DMVPN isn't correct because it is by design, a Hub and Spoke Architecture. The requirements state "spoke to spoke communication"
GRE VPN isn't correct because a GRE VPN doesn't encrypt to secure the packets during transport. The requirements state "all connections between sites be encrypted"
GETVPN is correct because it is the only one listed that is a "tunnel-less VPN". The requirements state "does not require maintenance of permanent tunnels.

upvoted 11 times

⊟ **XalaGyan** 2 years, 1 month ago

very well explained many thanks bro

upvoted 1 times

⊟ **chefexam** 1 year, 6 months ago

Doesn't DMVPN allow spoke-to-spoke as well!?

upvoted 3 times

⊟ **LSLS55** 1 year, 4 months ago

It does: "Dynamic spoke-to-spoke tunnels for partial scaling or fully meshed VPNs" - page 288 OCG.

upvoted 2 times

⊟ **bccabrera** Most Recent 1 year, 9 months ago

**Selected Answer: A**

https://www.routexp.com/2017/08/quick-comparison-ipsec-vs-dmvpn-vs.html

upvoted 3 times

⊟ **Hope66** 2 years, 6 months ago

I think that A is correct : please see CCNP Enterprise design ENSLD 300-420 pag.291

upvoted 4 times

Question #117 *Topic 1*

Which PIM mode uses a shared tree only?

A. bidirectional

B. sparse

C. dense

D. source-specific

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**goku2020** Highly Voted 5 years, 3 months ago

A BIDIR PIM use only shared tree.

upvoted 10 times

**XalaGyan** 3 years, 1 month ago

well said

upvoted 1 times

**PicoOstrava** Most Recent 1 year, 3 months ago

**Selected Answer: A**

the correct answer is A. bidirectional.

Bidirectional PIM exclusively uses the shared tree for all multicast communication, unlike Sparse Mode, which can switch between shared and source-specific trees.

upvoted 1 times

**TheGorn** 2 years, 2 months ago

Dense is Shortest Path

Sparse and SSM use RP (shared) then check for Shortest Path

BiDir uses RP (shared) and then forwards the data that way as well.

upvoted 1 times

**electro165** 2 years, 6 months ago

It's option C, because The PIM (Protocol Independent Multicast) mode that uses a shared tree only is "dense" mode. In PIM Dense Mode (PIM-DM), multicast traffic is initially flooded across the entire network, and routers prune back branches of the tree where no receivers are present. It's suitable for smaller networks or scenarios where multicast traffic is spread to most of the network.

upvoted 2 times

Question #118 *Topic 1*

Which two statements describe source trees in a multicast environment? (Choose two.)

A. Source trees guarantee the minimum amount of network latency for forwarding multicast traffic

B. Source trees create an optimal path between the source and the receivers

C. Source trees use a single common root placed at some chosen point in the network

D. Source trees can introduce latency in packet delivery

E. Source trees can create suboptimal paths between the source and the receivers

**Correct Answer:** *AB*

**certstudent2016** 1 year, 4 months ago

AB is correct

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

**Benzzyy** 2 years, 3 months ago

AB is correct

Source trees have the advantage of creating the optimal path between the source and the receivers. This advantage guarantees the minimum amount of network latency for forwarding multicast traffic.

upvoted 3 times

Question #119 *Topic 1*

Which two best practices must be followed when designing an out-of-band management network? (Choose two.)

A. Enforce access control

B. Facilitate network integration

C. Back up data using the management network

D. Ensure that the management network is a backup to the data network

E. Ensure network isolation

**Correct Answer:** *AE*

*Community vote distribution*

AE (100%)

**salmarin** 1 year, 7 months ago

**Selected Answer: AE**

provided answer is correct

upvoted 1 times

**XalaGyan** 2 years, 7 months ago

**Selected Answer: AE**

Answers A and E are correct. separate management access and control it tightly

upvoted 1 times

**certstudent2016** 3 years, 4 months ago

AE is correct!!

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/chap9.html

upvoted 1 times

## Question #120 *Topic 1*

What is a benefit of using VRRPv3 as compared to VRRPv2?

A. VRRPv3 supports IPv4 and IPv6

B. VRRPv3 supports authentication

C. VRRPv3 supports preemption

D. VRRPv3 supports stateful switchover

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Sickcnt** 1 year, 4 months ago

**Selected Answer: A**

"VRRPv3 supports usage of IPv4 and IPv6 addresses while VRRPv2 only supports IPv4 addresses"

upvoted 1 times

**certstudent2016** 1 year, 10 months ago

A is correct!!

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-e/fhp-15-e-book/VRRPv3-Protocol-Support.html

upvoted 1 times

## Question #121 *Topic 1*

A customer is discussing QoS requirements with a network consultant. The customer has specified that end-to-end path verification is a requirement. Which QoS solution meets this requirement?

A. IntServ model with RSVP to support the traffic flows

B. DiffServ model with PHB to support the traffic flows

C. marking traffic at the access layer with DSCP to support the traffic flows

D. marking traffic at the access layer with CoS to support the traffic flows

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Lungful** 1 year, 6 months ago

**Selected Answer: A**

A is correct. https://learningnetwork.cisco.com/s/question/0D53i00000KsqtXCAR/qos-architecture-models-intserv-vs-diffserv

upvoted 1 times

**vangio** 1 year, 7 months ago

Correct A

upvoted 1 times

**Sickcnt** 2 years, 4 months ago

**Selected Answer: A**

"The main difference between integrated services and differentiated services is that <<integrated services involve prior reservation of resources before achieving the required quality of service>>, (while differential services mark the packets with priority and send it to the network without prior reservation.) "

upvoted 2 times

**certstudent2016** 2 years, 10 months ago

A is correct

https://www.cisco.com/en/US/technologies/tk543/tk766/technologies_white_paper09186a00800a3e2f.html

upvoted 1 times

Question #122 *Topic 1*

Which nonproprietary mechanism can be used to automate rendezvous point distribution in a large PIM domain?

A. Embedded RP

B. BSR

C. Auto-RP

D. Static RP

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**J2J2J2J** 1 year, 8 months ago

**Selected Answer: B**

Multicast PIM Bootstrap (BSR)

upvoted 1 times

**Sickcnt** 2 years, 4 months ago

**Selected Answer: B**

Auto-RP could be an option as well (But its Cisco Proprietary)

So B is the correct answer

upvoted 1 times

**certstudent2016** 2 years, 10 months ago

B is correct

https://networklessons.com/cisco/ccie-routing-switching/multicast-pim-bootstrap-bsr#:~:text=BSR%20(Bootstrap)%20is%20similar%20to,is%20a%20Cisco%20proprietary%20protocol.

upvoted 1 times

Question #123 *Topic 1*

Which QoS feature responds to network congestion by dropping lower priority packets?

A. CBWFQ

B. tail drop

C. WRED

D. strict priority

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

⊟ **Benzzyy** Highly Voted 👍 3 years, 9 months ago

I think the answer is C
WRED can selectively discard lower priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/15-mt/qos-conavd-15-mt-book/qos-conavd-oview.html#:~:text=WRED%20can%20selectively%20discard%20lower,for%20different%20classes%20of%20service.

upvoted 5 times

⊟ **danieldarq** Most Recent 🕓 1 year, 8 months ago

is C:
Congestion Avoidance monitors network traffic loads in an effort to anticipate and avoid congestion. Congestion Avoidance is achieved through packet dropping. Typically, congestion avoidance is implemented on output interfaces where high-speed links intersect with low speed links. Congestion Avoidance in Cisco products uses Weighted Random Early Detection (WRED) to avoid congestion by dropping low priority packets and allowing high priority packets to continue on their path.

upvoted 1 times

⊟ **J2J2J2J** 1 year, 8 months ago

**Selected Answer: C**

WRED makes early detection of congestion possible and provides a means for handling multiple classes of traffic. WRED can selectively discard lower priority traffic when the router begins to experience congestion and provide differentiated performance characteristics for different classes of service.

upvoted 1 times

⊟ **roganjosh** 3 years ago

**Selected Answer: C**

Guys, It's C

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/15-mt/qos-conavd-15-mt-book/qos-conavd-oview.html#:~:text=WRED%20can%20selectively%20discard%20lower,for%20different%20classes%20of%20service.

upvoted 1 times

⊟ **Audie** 3 years ago

"Strict Priority (SP) - Engress traffic from the highest priority queue is transmitted first"
Must be "D"

upvoted 1 times

⊟ **Emily23** 1 year, 8 months ago

The question asks you which packet is dropped FIRST and the first thing that comes to you is to think about a mechanism which assures which packet goes first and assume that is correct ? Great logic mate...

upvoted 1 times

⊟ **danpho123** 3 years, 2 months ago

CBWFQ is a scheduling mechanism used to provide a minimum bandwidth guarantee to traffic classes during times of network congestion at an interface. Each of the CBWFQ queues is assigned a weight, and the packets are served from the queues based upon the weight of the queue.

WRED can selectively discard lower priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service.

https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book/congestion_avoidance.html

upvoted 1 times

⊟ **aymeric** 4 years ago

I think A is a better answer

upvoted 1 times

⊟ **CCNPWILL** 3 years, 8 months ago

Please research. IT IS NOT A!

upvoted 1 times

Question #124 *Topic 1*

What is an advantage of designing an out-of-band network management solution?

A. In the event of a production network outage, network devices can still be managed.

B. There is no separation between the production network and the management network.

C. In the event of a production network outage, it can be used as a backup network path.

D. It is less expensive than an in-band management solution.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Alberto5738** 1 year, 3 months ago

Do you have a reference or link to validate the answer?

Thanks

upvoted 1 times

**Lungful** 1 year, 6 months ago

**Selected Answer: A**

A is correct.

upvoted 1 times

## Question #125 *Topic 1*

An engineer is designing a QoS policy that queues excess packets for later transmission. Which mechanism must be included in the design?

A. shaping

B. WRED

C. policing

D. RED

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Lungful** 1 year, 6 months ago

**Selected Answer: A**

Definitely shaping. A is correct.

upvoted 1 times

**certstudent2016** 2 years, 10 months ago

A is correct!

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

upvoted 2 times

Question #126 *Topic 1*

An organization is designing a detailed QoS plan that limits bandwidth to specific rates. Which two parameters are supported by the traffic policing feature?
(Choose two.)

A. violating

B. marking

C. shaping

D. bursting

E. conforming

**Correct Answer:** *AE*

*Community vote distribution*

AE (100%)

**Ranx01** Highly Voted 👍 4 years, 7 months ago

I also think it's A & E, the question is asking for the traffic "policing" feature.

upvoted 12 times

**Hamele0n** Highly Voted 👍 4 years, 7 months ago

I think it's A and E.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/xe-3s/qos-plcshp-xe-3s-book/qos-plcshp-class-plc.html

upvoted 6 times

**Hermes76** Most Recent 1 year, 6 months ago

The parameters that are specifically associated with traffic policing in QoS are:
Conforming: Traffic policing categorizes packets as conforming if they adhere to the specified rate limit. Conforming packets are typically forwarded or treated according to the configured QoS policies.

Violating: Traffic policing categorizes packets as violating if they exceed the specified rate limit. Violating packets are often dropped or subjected to lower priority treatment.
Answer is A and E

upvoted 1 times

**Clauster** 2 years, 1 month ago

Selected Answer: AE

This answer is A and E
Straight out of the white pages to end the discussion
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/15-mt/qos-plcshp-15-mt-book/qos-plcshp-trfc-plc.html

upvoted 1 times

**cerifyme85** 2 years, 5 months ago

https://www.ipspace.net/kb/tag/QoS/QoS_Policing.html#:~:text=Police%20action,rate/burst%20size

upvoted 2 times

**Reinier_veen** 2 years, 10 months ago

conform
violate
exceed

upvoted 1 times

**certstudent2016** 3 years, 4 months ago

Selected Answer: AE

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

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/xe-17/qos-plcshp-xe-17-book/qos-plcshp-trfc-plc.pdf

upvoted 3 times

**certstudent2016** 3 years, 4 months ago

A&E Correct

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

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/xe-17/qos-plcshp-xe-17-book/qos-plcshp-trfc-plc.pdf

upvoted 1 times

**Bigmikemalta** 3 years, 4 months ago

**Selected Answer: AE**

Violating and conforming I think

upvoted 2 times

**Audie** 3 years, 6 months ago

Agree with A and E: police bps burst-normal burst-max conform-action action exceed-action action violate-action action

upvoted 3 times

**roganjosh** 3 years, 6 months ago

**Selected Answer: AE**

A and E are right,

upvoted 3 times

**Xavi07** 4 years, 1 month ago

to limit bandwith the better option is marking and shaping

upvoted 1 times

Question #127 *Topic 1*

An engineer must propose a QoS architecture model that allows an application to inform the network of its traffic profile and to request a particular type of service to support its bandwidth and delay requirements. The application requires consistent and dedicated bandwidth end to end. Which QoS architecture model meets these requirements?

A. DiffServ

B. LLQ

C. WRED

D. IntServ

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**Lungful** 1 year, 6 months ago

**Selected Answer: D**

D is correct. IntServ is the "hard" QoS method that reserves resources and bandwidth.

https://learningnetwork.cisco.com/s/question/0D53i00000KsqtXCAR/qos-architecture-models-intserv-vs-diffserv

upvoted 1 times

**namibdigger** 2 years, 7 months ago

**Selected Answer: D**

Integrated Services Model ....expects applications to signal their requirements to the network (Study Guide v.1.4 p224)

upvoted 3 times

Question #128 *Topic 1*

An engineer is designing a multicast network for a financial application. Most of the multicast sources also receive multicast traffic (many-to-many deployment model). To better scale routing tables, the design must not use source trees. Which multicast protocol satisfies these requirements?

A. PIM-SSM

B. PIM-SM

C. MSDP

D. BIDIR-PIM

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**goku2020** Highly Voted 3 years, 3 months ago

D => BIDIR PIM is a many-to-many multicast model.

upvoted 12 times

**Eards** Most Recent 1 year, 4 months ago

Selected Answer: D

D may to many bidirectional

upvoted 1 times

**namibdigger** 1 year, 7 months ago

Selected Answer: D

BIDIR-PIM: same tree for receiving and sending Multicast traffic & less stae in routers because many sources produce a single (*,G) only - examples: stock exchange. These meet the requirements best.

upvoted 1 times

**Hope66** 1 year, 11 months ago

In many-to-many applications, PM-SM is not ideal because in not bidirectional

Answer id D

upvoted 2 times

**roganjosh** 2 years ago

Selected Answer: D

Answer is D

upvoted 3 times

**Xavi07** 2 years, 8 months ago

Bidir-PIM is designed to be used for many-to-many applications within individual PIM domains. Multicast groups in bidirectional PIM mode can scale to an arbitrary number of sources without incurring overhead due to the number of sources.

So answer is D -> BIDIR PIM

upvoted 3 times

**luisjuradoledesma** 3 years, 1 month ago

In support of the use of BIDIR-PIM in financial applications:

https://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/multicast-enterprise/prod_white_paper0900aecd80310db2.pdf

upvoted 4 times

**luisjuradoledesma** 3 years, 1 month ago

D - Actually PIM-SM creates shared trees (not source trees). However, BDIR-PIM eliminates the need for a first-hop route to encapsulate data packets being sent to the RP - then scales better in a "many-to-many" deployment

upvoted 2 times

**lygris** 3 years, 2 months ago

D- Bidir PIM

Bidir PIM doesn't build source trees, PIM-SM does

upvoted 2 times

⊟ **helium** 3 years, 2 months ago

PIM-SM is correct. As there is two requirements that use Many-to-many model and no source tree. BIDIR PIM use source tree.

upvoted 1 times

⊟ **Kakat** 2 years, 7 months ago

https://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/multicast-enterprise/prod_white_paper0900aecd80310db2.pdf

BIDIR PIM uses shared tree.

upvoted 4 times

Question #129 *Topic 1*

An engineer is working for a large cable TV provider that requires multiple sources streaming video on different channels using multicast with no rendezvous point.

Which multicast protocol meets these requirements?

A. PIM-SM

B. PIM-SSM

C. any-source multicast

D. BIDIR-PIM

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**kudasay** Highly Voted 4 years, 3 months ago

PIM-SSM is correct

upvoted 13 times

**luisjuradoledesma** Highly Voted 4 years, 1 month ago

B - PIM-SSM is suitable for when well-known sources exist within the local PIM domain and for broadcast applications. Also, PIM-SSM eliminates the RPs and shared trees - then it could be correct.

upvoted 5 times

**nicolamazzoletti** Most Recent 1 year, 5 months ago

Selected Answer: B

With BIR-PIM all the traffic passes via the RP

upvoted 1 times

**Lungful** 1 year, 6 months ago

Selected Answer: B

B is correct.

upvoted 1 times

**vangio** 1 year, 7 months ago

Correct B

upvoted 1 times

**Dyks** 1 year, 10 months ago

Selected Answer: B

PIM-SSM utilizes the source tree and not the shared tree so there is no need for an RP.

BIR-PIM uses shared tree only (RP Required)

PIM-SM use both Source and Shared Tree (RP Required)

upvoted 3 times

**Eards** 2 years, 4 months ago

Selected Answer: B

PIM-SSM

upvoted 1 times

**namibdigger** 2 years, 7 months ago

Selected Answer: B

Agree with PIM-SSM: is the best one-to-many (=broadcast = TV) model which eliminates RP

upvoted 1 times

**roganjosh** 3 years ago

Selected Answer: B

PIM-SSM is correct , no RP or shared (*,G) tree, only SPT (S,G) to the sender.

upvoted 2 times

⊟ **Xavi07** 3 years, 8 months ago

SSM is the correct.

SSM eliminates the RP. In Bidir there is RP

upvoted 3 times

⊟ **luisjuradoledesma** 4 years, 1 month ago

In addition - please, note, the RP is required for BIDIR PIM - refer to:

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/16-12/configuration_guide/ip_mcast_rtng/b_1612_ip_mcast_rtng_9600_cg/configuring_pim.html#id_111801

upvoted 3 times

⊟ **Blipblop** 4 years, 1 month ago

I think BIDIR-PIM is correct because it’s used for when we have many sources and receivers talking to each other.

upvoted 1 times

> ⊟ **ejohnson7** 3 years, 1 month ago
>
> sorry my friend you are wrong the ans is SSM no RP
>
> upvoted 4 times

Question #130 *Topic 1*

What is the function of the multicast Reverse Path Forwarding check?

A. It allows for a loop-free distribution tree from the source to receivers.

B. It serves as an Auto RP Mapping agent.

C. It prevents bootstrap messages from reaching all routers.

D. It is used to discover and announce RP-set information.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Lungful** 1 year, 6 months ago

Selected Answer: A

A, preventing loops, is correct.

https://en.wikipedia.org/wiki/Reverse-path_forwarding

upvoted 1 times

**namibdigger** 2 years, 7 months ago

Selected Answer: A

Reverse Path... will ensure that the packet is forwarded....without routing loops (Student learning guide v1.4 p253)

upvoted 3 times

Question #131 *Topic 1*

An architect is designing a multicast solution for a network that contains over 100 routers. The architect plans to create several multicast domains and balance the
PIM-SM traffic within the network. Which technology should the architect include in the design?

A. DVMRP

B. IGMP

C. MOSPF

D. MSDP

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**J2J2J2J** 1 year, 8 months ago

**Selected Answer: D**

Multicast Source Discovery Protocol (MSDP)

upvoted 1 times

**namibdigger** 2 years, 7 months ago

**Selected Answer: D**

MSDP...is needed for interdomain multicast routing when regular PIM-SM is used within a domain (student guide v.1.4 p 264)

upvoted 2 times

**certstudent2016** 2 years, 10 months ago

**Selected Answer: D**

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book.pdf

upvoted 1 times

Question #132 *Topic 1*

An engineer must design a scalable QoS architecture that allows the separation of the traffic into classes based on predefined business requirements. The design must also utilize the differentiated services code points as the QoS priority descriptor value and support at least 10 levels of classification. Which QoS technology should the engineer include in the design?

A. RSVP

B. DiffServ

C. Best Effort

D. InterServ

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**Lungful** 1 year, 6 months ago

**Selected Answer: B**

B is correct. "Differentiated Services (Diffserv) model is also known as a soft QoS model. It's a model based in service classes and per hop behaviours associated to each class."

Reference: https://learningnetwork.cisco.com/s/question/0D53i00000KsqtXCAR/qos-architecture-models-intserv-vs-diffserv

upvoted 1 times

**namibdigger** 2 years, 7 months ago

**Selected Answer: B**

DSCP Values allow for > 10 classes and are used in DiffServ to discriminate traffic

upvoted 2 times

Question #133 *Topic 1*

A network engineer is redesigning a company's QoS solution. The company is currently using IP Precedence, but the engineer plans to move to DiffServ. It is important that the new solution provide backward compatibility with the current solution. Which technology should the design include?

A. expedited forwarding

B. assured forwarding

C. class selector code points

D. default per-hop behavior

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**Lungful** 1 year, 6 months ago

**Selected Answer: C**

C is correct. "To preserve backward-compatibility with any IP precedence scheme currently in use on the network, DiffServ has defined a DSCP value in the form xxx000, where x is either 0 or 1. These DSCP values are called Class-Selector Code Points. (The DSCP value for a packet with default PHB 000000 is also called the Class-Selector Code Point.)"

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_dfsrv/configuration/15-mt/qos-dfsrv-15-mt-book/qos-dfsrv.html

upvoted 1 times

**Reinier_veen** 2 years, 4 months ago

annoying that they use other terms.
" class selector code points" means "Differentiated Services Code Point" (DSCP)?

upvoted 1 times

**namibdigger** 2 years, 7 months ago

**Selected Answer: C**

FiffServ is backward compatible with IP Precedence (Ip-Precedence uses the 3 most signifcant bits of the ToS byte, whereas Diffserve uses the fost significant six bits - which includ the ones from IP precedence)

upvoted 4 times

Question #134 *Topic 1*

An enterprise customer has these requirements:

✑ end-to-end QoS for the business-critical applications and VoIP services based on CoS marking.

✑ flexibility to offer services such as IPv6 and multicast without any reliance on the service provider.

✑ support for full-mesh connectivity at Layer 2.

Which WAN connectivity solution meets these requirements?

A. VPWS

B. MPLS VPN

C. DMVPN

D. VPLS

**Correct Answer:** *D*

*Community vote distribution*

D (86%) 14%

⊟ **mgiuseppe86** 1 year, 5 months ago

**Selected Answer: D**

VPLS... currently use this at work. The second i saw "full-mesh" I knew it was VPLS right away.

upvoted 3 times

⊟ **J2J2J2J** 1 year, 8 months ago

**Selected Answer: D**

VPWS used on point to point (P2P) and the VPLS used on point to multi point (P2MP)

upvoted 2 times

⊟ **cerifyme85** 1 year, 11 months ago

**Selected Answer: D**

Full mesh VPLS.. VPWS ptp

https://community.cisco.com/t5/mpls/vpls-versus-vpws-what-are-the-differences/td-p/4428284#:~:text=%40Meddane%C2%A0%3A-,VPWS,point%20(P2P)%2C%20the%20VPLS%20used%20on%20point%20to%20multi%20point%20(P2MP),-View%20solution%20in

upvoted 1 times

⊟ **isa1010** 2 years ago

**Selected Answer: A**

Virtual Private Wire Service (VPWS) or PseudoWires offer quality of service (QoS) mechanisms to prioritize voice, video, and critical traffic

upvoted 1 times

⊟ **Lungful** 1 year, 6 months ago

The questions specifies full mesh as a requirement though and VPWS is p2p.

upvoted 2 times

Question #135 *Topic 1*

When designing interdomain multicast, which two protocols are deployed to achieve communication between multicast sources and receivers? (Choose two.)

A. IGMPv2

B. BIDIR-PIM

C. MP-BGP

D. MSDP

E. MLD

**Correct Answer:** *CD*

*Community vote distribution*

CD (75%) BD (25%)

**Lungful** 1 year, 6 months ago

**Selected Answer: CD**

I vote C+D based on: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/Phase_1/mcstmsdp/mcst_p1.html

upvoted 2 times

**Yeti56** 1 year, 7 months ago

**Selected Answer: CD**

Interdomain multicast networks such as PIM-SM, MBGP, and MSDP

upvoted 1 times

**cerifyme85** 1 year, 11 months ago

**Selected Answer: CD**

https://www.arista.com/en/um-eos/eos-multicast-source-discovery-protocol-msdp#:~:text=configuring%20MSDP%20speakers.-,Network%20Configuration,messages%20are%20MSDP%20control%20messages%20that%20peers%20excl

upvoted 1 times

**XalaGyan** 2 years, 1 month ago

**Selected Answer: BD**

Answers B and D

When designing interdomain multicast, two protocols that are typically deployed to achieve communication between multicast sources and receivers are:

BIDIR-PIM (Option B): BIDIR-PIM (Bi-Directional PIM) is a multicast routing protocol that allows multicast traffic to flow in both directions between domains. It uses a shared tree architecture to support interdomain multicast communication.

MSDP (Option D): MSDP (Multicast Source Discovery Protocol) is used to exchange information between domains about multicast sources. MSDP allows routers in one domain to learn about multicast sources in other domains and to forward traffic to those sources. MSDP operates at the edge of each domain and is used in conjunction with BIDIR-PIM.

In summary, BIDIR-PIM and MSDP are two protocols that are deployed to achieve interdomain multicast communication between multicast sources and receivers.

upvoted 2 times

**Clauster** 1 year, 7 months ago

You are incorrect, i just asked bard and it gave me B and C as the correct answers

upvoted 1 times

**Clauster** 1 year, 7 months ago

Sorry C and D

upvoted 1 times

**namibdigger** 2 years, 7 months ago

**Selected Answer: CD**

MSDP (Multicast interdomain discovery protocol) should exchange routing information using BGP (Student learning guide v1.4. p 274)

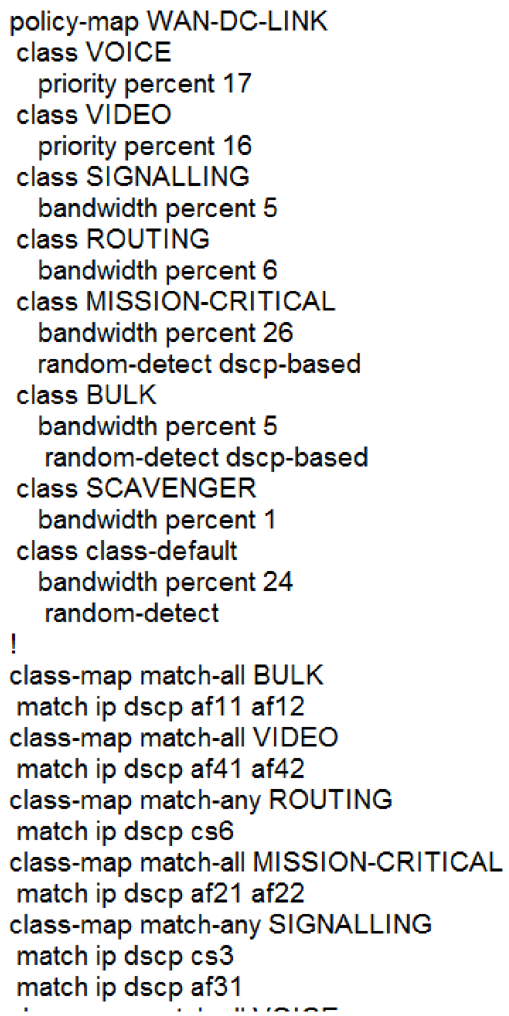
upvoted 2 times

**GustavoF** 1 year, 10 months ago

BGP itself differs from MP-BGP operation. In my option B and D are correct.

upvoted 1 times

Question #136 Topic 1



```
policy-map WAN-DC-LINK
 class VOICE
   priority percent 17
 class VIDEO
   priority percent 16
 class SIGNALLING
   bandwidth percent 5
 class ROUTING
   bandwidth percent 6
 class MISSION-CRITICAL
   bandwidth percent 26
   random-detect dscp-based
 class BULK
   bandwidth percent 5
    random-detect dscp-based
 class SCAVENGER
   bandwidth percent 1
 class class-default
   bandwidth percent 24
    random-detect
!
class-map match-all BULK
 match ip dscp af11 af12
class-map match-all VIDEO
 match ip dscp af41 af42
class-map match-any ROUTING
 match ip dscp cs6
class-map match-all MISSION-CRITICAL
 match ip dscp af21 af22
class-map match-any SIGNALLING
 match ip dscp cs3
 match ip dscp af31
```

Refer to the exhibit. A customer needs to apply QoS to the network management traffic passing through the GigabitEthernet 0/2 interface. All eight queuing classes are in use, so the new requirement must be integrated into the existing policy. Which solution must the customer choose?

A. Mark the traffic to DSCP CS6 and assign it to the ROUTING class. Then, prioritize traffic within the class.

B. Mark the traffic to DSCP CS2 and assign it to the ROUTING class. Then, baseline existing queue sizes to determine if additional bandwidth can be provisioned to the ROUTING class.

C. Mark the traffic to DSCP CS4 and assign it to the SIGNALLING class. Then, prioritize traffic within the class.

D. Mark the traffic to DSCP CS5 and assign it to the SIGNALLING class. Then, baseline existing queue sizes to determine if additional bandwidth can be provisioned to the SIGNALLING class.

**Correct Answer:** *B*

*Community vote distribution*

B (75%) A (25%)

**neiker45** 1 year, 7 months ago

Selected Answer: B

In the link provided before, in figure 15-5 you can see how in the control queue they are doing the same thing we are doing here. They are taking network control, Internetwork control and network management traffic and putting them in one slot including their respective DSCP category.

(https://www.ciscopress.com/articles/article.asp?p=2159353&seqNum=3).

upvoted 1 times

**CKL_SG** 2 years, 3 months ago

Selected Answer: B

Twelve-Class Egress Queuing Model
Network control traffic (marked CS6), signaling traffic (marked CS3) and network
management traffic (marked CS2) is all assigned to a dedicated nonpriority queue with a 10 percent bandwidth allocation; optionally, CS7 traffic may also be mapped to this queue.
https://www.ciscopress.com/articles/article.asp?p=2159353&seqNum=3

upvoted 2 times

**Eards** 2 years, 10 months ago

**Selected Answer: B**

CS2 = mangement

upvoted 2 times

**XalaGyan** 2 years, 7 months ago

Application PHB DSCP CoS
Network Control - CoS 7
Internetwork Control CS6 48 CoS 6
Voice EF 46 CoS 5
Interactive-Video AF41 34 CoS 4
Streaming-Video CS4 32 CoS 4
Mission-Critical Data 25 CoS 3
Call-Signaling CS3 24 CoS 3
AF31 26
Transactional Data AF21 18 CoS 2
Network-Management CS2 16 CoS 2
Bulk Data AF11 10 CoS 1
Scavenger CS1 8 CoS 1
Best-Effort 0 0 0

upvoted 1 times

**XalaGyan** 2 years, 7 months ago

Application PHB DSCP CoS
Network Control - CoS 7
Internetwork Control CS6 48 CoS 6
Voice EF 46 CoS 5
Interactive-Video AF41 34 CoS 4
Streaming-Video CS4 32 CoS 4
Mission-Critical Data 25 CoS 3
Call-Signaling CS3 24 CoS 3
AF31 26
Transactional Data AF21 18 CoS 2
Network-Management CS2 16 CoS 2
Bulk Data AF11 10 CoS 1
Scavenger CS1 8 CoS 1
Best-Effort 0 0 0

upvoted 1 times

**namibdigger** 3 years, 1 month ago

**Selected Answer: A**

If i understand correctly i am asked to use the given classes and integrate it to the new policy - given I am not asked to alter the traffic values but to 'map' the network traffic to those values that are in the exibit it must be answer A. Answer B would be correct if i was allowed to alter the garantueed bandwith of the ROUTING class. I Think i am not allowed to do that so i would align with the given value of CS6 which is not 'normal' network mgmt but that value is due to alteration according to the customers requirements - so not sure what answer is expected

upvoted 2 times

**iLikeHamburgers** 2 years, 8 months ago

You make an interesting point. I hate this question because as you eluded to, it is not clear as to whether we can make changes to the existing config, the question only states that "it has to be integrated". I don't know how i'm supposed to interpret that. In the real world, you would be told explicitly whether changes can be implemented or not. The only other thing that comes to mind would be if you had to make changes throughout the entire network. Marking the mgmt traffic to CS6 would alleviate you from having to go into each and every device to make changes to the config. However the other side to that argument is you still have to go into every device to mark the mgmt traffic as CS6.

Could we not just add this config class-map match-any ROUTING??
match ip dscp CS2
upvoted 1 times

⊟ **XalaGyan** 2 years, 7 months ago

Great thinking but since CS6 is pretty much high prio or almost highest prio, i would refrain from using CS6 and CS7 entirely no matter what question or customer says. CS6 and CS7 should be left for the device to do its vital things.

Eventhough Answer A looks good and namibdigger explained it well, i stick to Option B as it is less evil and gets the job done.
upvoted 1 times

⊟ **certstudent2016** 3 years, 4 months ago

Selected Answer: B

B seems correct
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/hcs/12_5/HCS_Solution/SRND/HCS_12_5_SRND/chcs_m_quality-of-service-considerations.pdf
upvoted 1 times

⊟ **Hope66** 3 years, 4 months ago

I think that the answer is B, CS2 is management.
upvoted 1 times

⊟ **cwoolie** 3 years, 4 months ago

I am reading CS2 is management so must be B
upvoted 1 times

⊟ **cwoolie** 3 years, 5 months ago

Is answer B?
upvoted 1 times

⊟ **cwoolie** 3 years, 5 months ago

I have answer as D?
upvoted 1 times

Question #137 *Topic 1*

An architect must address sustained congestion on the access and distribution uplinks of a network. QoS has already been implemented and optimized, but it is no longer effective in ensuring optimal network performance. Which two solutions should the architect use to improve network performance. (Choose two.)

A. Configure selective packet discard to drop noncritical network traffic.

B. Bundle additional uplinks into logical EtherChannels.

C. Utilize random early detection to manage queues.

D. Implement higher-speed uplink interfaces.

E. Reconfigure QoS based on the IntServ model.

**Correct Answer:** *BD*

*Community vote distribution*

BD (75%) AC (25%)

**Marinheiro** 2 years, 1 month ago

**Selected Answer: BD**

B and D are correct.

upvoted 1 times

**andrewChan** 2 years, 10 months ago

**Selected Answer: BD**

As the question mentioned that QoS has been implemented and optimized, I can assumed A and C had been done. So I prefer B & D to upgrade the link and add new uplinks

upvoted 4 times

**Eards** 2 years, 10 months ago

**Selected Answer: AC**

AC would love to say BD throw more bandwidth at it but make most questions on QOS pointless...

upvoted 1 times

**26d13e9** 1 year, 4 months ago

Since we are talking about access and distribution switches, these are normally in close proximity and adding links should not be much of an issue. From that point, BD.

I completely see your point.....but may be at the core level where adding more may be hard.

upvoted 1 times

**namibdigger** 3 years, 1 month ago

**Selected Answer: BD**

I went for B and D straight away because the question states that 'QoS has already been... optimized' which rules out any more fiddling with QoS. Dropping noncritical network traffic (A) to me is far from being optimal network performance

upvoted 1 times

**zlimvos** 3 years, 2 months ago

**Selected Answer: AC**

For me also A and C make sense.

upvoted 1 times

**cwoolie** 3 years, 5 months ago

I have answers as A and C???

upvoted 1 times

## Question #138 *Topic 1*

An engineer must design a QoS solution for a customer that is connected to an ISP over a 1Gbps link with a 100Mbps CIR. The ISP aggressively drops all traffic received over the CIR, which is causing numerous TCP retransmissions. The customer is not using any RTP applications but wants to maximize bandwidth usage up to the CIR. Which QoS solution should the engineer choose?

A. policing

B. queuing

C. traffic shaping

D. policer with markdown

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**26d13e9** 1 year, 4 months ago

No RTP applications.....then surely shaping

upvoted 1 times

**namibdigger** 3 years, 1 month ago

**Selected Answer: C**

Shaping prevents the provider from dropping traffic that exceeds the contracted rate (Official Cert guide P.313)

upvoted 4 times

**certstudent2016** 3 years, 4 months ago

however the issue is retransmission which can be avoided by Shaping - 'C' is correct

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

upvoted 4 times

**cwoolie** 3 years, 5 months ago

Answer is A. Policing is for inbound traffic like questions states.

upvoted 1 times

**iLikeHamburgers** 2 years, 8 months ago

Policing is used for inbound traffic. The question states "The ISP aggressively drops all traffic RECEIVED.." so the traffic being dropped is traffic sent from the customer to the ISP. The ISP is using policing to drop traffic, but if wanted to control the amount of traffic being sent OUT of your network, you would use traffic shaping.

upvoted 2 times

Question #139 *Topic 1*

The customer solution requires QoS to support streaming multimedia over a WAN. An architect chooses to use Per-Hop Behavior. Which solution should the engineer use to classify and mark traffic traveling between branch sites?

A. CBWFQ with DSCP AF2

B. LLQ with DSCP EF

C. CBWFQ with DSCP AF3

D. LLQ with DSCP AF4

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**TheGorn** 1 year, 8 months ago

Recommendations by Cisco and the RFC. Looks like multimedia would be AF3x.

https://ptgmedia.pearsoncmg.com/images/chap16_9781587144622/elementLinks/16fig04_alt.jpg

upvoted 1 times

**kejvi** 1 year, 8 months ago

it is question, whether AF3 meen AF31 AF32 AF33, or AF3 class doesn't exist, therefore only existing DSCP would be EF

upvoted 1 times

**vangio** 2 years, 1 month ago

correct C

upvoted 1 times

**iLikeHamburgers** 2 years, 8 months ago

**Selected Answer: C**

The DSCP value for Multimedia Streaming is AF3

upvoted 2 times

**namibdigger** 3 years, 1 month ago

**Selected Answer: C**

i go for 'C' - Official Cert Guide states 'Multimedia Streaming = AF3' (p. 311) and LLQ is too strong for Multimedia to implement (only for 'real time' like Voice or videoconferencing)

upvoted 3 times

**cwoolie** 3 years, 4 months ago

This is from Cisco Learning Space...

"Broadcast video traffic should be marked to CS5 /DSCP 40"

"Multimedia Streaming AF21 Per Hop Behavior"

upvoted 1 times

**Hope66** 3 years, 5 months ago

I think that the answer is C:

AF3 = multimedia streaming

upvoted 3 times

**cwoolie** 3 years, 5 months ago

I think answer is correct....Low Latency Queuing (LLQ) is the preferred queuing policy for VoIP audio. Given the stringent delay/jitter sensitive requirements of TP and the need to synchronize audio and video for CUVA, priority (LLQ) queuing is the recommended for all video traffic as well. Note that, for video, priority bandwidth is generally fudged up by 20% to account for the overhead.

upvoted 1 times

**Audie** 3 years, 6 months ago

C. LLQ is mainly for Voice and other Critical Controls. See the link below which states that Multimedia is AF3. https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/Borderless_Campus_Network_1-0/Borderless_Campus_1-0_Design_Guide/BN_Campus_QoS.html

upvoted 1 times

⊟ **cryptonite** 3 years, 6 months ago

Streaming multimedia should not be on the LLQ, the LLQ is for real-time traffic. I am not very sure but I will go for CBWFQ with DCP AF2 (lower drop probability).

upvoted 1 times

⊟ **cryptonite** 3 years, 6 months ago

https://www.ciscopress.com/articles/article.asp?p=357102&seqNum=2 CS4 is closer to AF3 than AF2

upvoted 1 times

⊟ **bogd** 3 years, 6 months ago

**Selected Answer: C**

LLQ with EF seems way too strict for STREAMING multimedia (where one can actually take advantage of buffering).

Judging by the various Cisco QoS baseline docs (even though the ones below are quite old), streaming video should be somewhere at AF3x/CS4. So I would go with C.

https://www.cisco.com/en/US/technologies/tk543/tk759/technologies_white_paper0900aecd80295a9b.pdf

https://community.cisco.com/t5/collaboration-voice-and-video/cisco-qos-baseline-classification-and-marking-and-mapping/ta-p/3108355

upvoted 2 times

Question #140 *Topic 1*

An engineer must design an in-band management solution for a customer with branch sites. The solution must allow remote management of the branch sites using management protocols over an MPLS WAN. Queueing is implemented at the remote sites using these classes:
✑ Class1 equals voice traffic
✑ Class2 equals mission-critical traffic
✑ Class3 equals default traffic
How must the solution prioritize the management traffic over the WAN?

A. Mark the traffic with DSCP EF and map into Class1 with a minimum bandwidth assigned by reducing the bandwidth available to Class2.

B. Mark the traffic with DSCP CS1 and map into Class2 with a minimum bandwidth assigned by reducing the bandwidth available to Class3.

C. Mark the traffic with DSCP CS6 and map into Class1 with a minimum bandwidth assigned by reducing the bandwidth available to Class2.

D. Mark the traffic with DSCP CS2 and map into Class2 with a minimum bandwidth assigned by reducing the bandwidth available to Class3.

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**iLikeHamburgers** 1 year, 8 months ago

**Selected Answer: D**

in the OCG, pg 311, CS2 is labeled as Network Management. Since non of the other answers suggest marking the management traffic as CS2, and you wouldn't want to reduce the bandwidth to any other Classes except for Class 3, D is the obvious choice.

upvoted 2 times

**namibdigger** 2 years, 1 month ago

**Selected Answer: D**

NW-Mgmt is the traffic in question i guess which equals CF2 (recommendation) and is to be placed in class 2 which and reduces less important class3 bandwith.

upvoted 2 times

**cwoolie** 2 years, 4 months ago

Why not "B"? Although network management traffic may not be considered as critical as voice and video traffic, it does merit some prioritization. In Cisco QOS classification and marking recommendations, network management traffic is given a Layer 3 classification of CS1 PHB (DSCP16) or Layer 2 CoS of 2. That is from the Cisco design book...

upvoted 1 times

**cwoolie** 2 years, 4 months ago

Disregard. CiscoPress says management traffic is classified as CS2. So I agree Answer is D

upvoted 2 times

**morlu** 2 years, 8 months ago

**Selected Answer: D**

It's D. CS2 is for OAM ('management'). Also, you wouldn't want to reduce the bandwidth for Class2 since it is specifically labeled mission-critical.

upvoted 4 times

**cryptonite** 2 years, 6 months ago

You don put management traffic in the same class as voice!!

upvoted 1 times

**cryptonite** 2 years, 6 months ago

I agree the answer is D

upvoted 1 times

## Question #141 *Topic 1*

An engineer is designing a multicast network for a company specializing in VoD content. Receivers are across the Internet, and for performance reasons, the multicast framework must be close to the receivers within each AS. For high availability, if the sources in one AS are no longer available, the receivers of that AS must be able to receive the VoD content from the sources in another AS. Which feature must the design include?

A. SSM

B. anycast RP

C. bidirectional PIM

D. MSDP

**Correct Answer:** *B*

*Community vote distribution*

B (60%) D (40%)

⊟ **iSDA69** 4 months, 3 weeks ago

**Selected Answer: B**

I Think the right answer should be B Anycast RP.
That's because this is the feature that has to be enabled to allow the clients of one AS to contact the same (other AS) RP IP address when the local RP fails. This will allow the clients to join the multicast sources of the other AS.
MSDP in this question is considered enabled because we are in a multiple AS scenario and has the function (as usual) to advertise the sources between AS.

upvoted 1 times

⊟ **NoHombre** 5 months, 3 weeks ago

**Selected Answer: D**

You have receivers spread across multiple ASes (interdomain) and you want the multicast control plane close to the receivers in each AS (i.e., each AS runs its own PIM-SM with a local RP). For high availability, if sources in AS1 fail, receivers in AS1 must be able to learn and join sources in AS2 automatically.

That is exactly what MSDP does: it peers the RPs of different domains and advertises Source-Active (SA) messages. Using SA information, an RP in one AS learns about active sources in the other AS and can trigger joins toward those sources. This enables interdomain source discovery and failover while keeping the PIM framework (RP) local to each AS for performance.

upvoted 1 times

⊟ **sola123** 7 months, 2 weeks ago

**Selected Answer: B**

it says multicast feature not multicast mode

upvoted 1 times

⊟ **anaq87** 9 months ago

**Selected Answer: D**

The correct answer is D. MSDP (Multicast Source Discovery Protocol).
Why MSDP is required:

The design involves multiple PIM-Sparse Mode domains (one in each AS), where the RPs are local to each receiver AS for performance. When sources in one AS fail, receivers in that AS must still be able to get VoD streams from sources in a different AS. MSDP connects multiple PIM-SM domains by allowing RPs to share active source information (the “(S,G)” state) across AS boundaries. With MSDP, if a source goes down in one AS, the RP in that AS can learn about active sources in another AS via MSDP, allowing receiver RPs to join alternate sources dynamically.

upvoted 2 times

⊟ **PicoOstrava** 1 year, 3 months ago

**Selected Answer: B**

option D, is also used to propagate multicast sources across different domains. However, it is primarily used for source discovery, and it does not directly handle high availability as effectively as anycast RP in this context.

upvoted 2 times

**TheGorn** 2 years, 1 month ago

This questions sucks. Looks like both B and D could be considered pieces of the same solution.

https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/anycast.html

upvoted 1 times

> **TheGorn** 2 years, 1 month ago
>
> Going with D though as one is dependent on the other and the wording states "must include".
>
> upvoted 1 times

**neiker45** 2 years, 2 months ago

**Selected Answer: D**

MSDP is required for inter-domain multicasting

upvoted 3 times

**vangio** 2 years, 7 months ago

Correct B

upvoted 1 times

**Reinier_veen** 3 years, 4 months ago

Info about AnycastRP:

https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/anycast.html

upvoted 1 times

**namibdigger** 3 years, 7 months ago

**Selected Answer: B**

Difficult - it reminds me of anycast in general with BGP 'close to nearest' - thats why i opt for B

upvoted 1 times

Question #142 *Topic 1*

An organization plans to deploy multicast across two different autonomous systems. Their solution must allow RPs to:
➾ discover active sources outside their domain
➾ use the underlying routing information for connectivity with other RPs
➾ announce sources joining the group
Which solution supports these requirements?

A. SSM

B. MSDP

C. PIM-DM

D. PIM-SM

**Correct Answer:** *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-10/configuration_guide/ip_mcast_rtng/b_1610_ip_mcast_rtng_9500_cg/b_1610_ip_mcast_rtng_9500_cg_chapter_010001.pdf

*Community vote distribution*
B (100%)

**Lungful** 1 year, 6 months ago

**Selected Answer: B**

B is correct.

"MSDP is also used to announce sources sending to a group. These announcements must originate at the RP of the domain."

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

MSDP is a mechanism to connect multiple PIM-SM domains. 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 a common shared tree).

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book.pdf
upvoted 2 times

Question #143 *Topic 1*

Which type of rendezvous point deployment is standards-based and supports dynamic RP discovery?

A. bootstrap router

B. Anycast-RP

C. Auto-RP

D. static RP

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Lungful** 1 year, 6 months ago

**Selected Answer: A**

A is correct.

BSR (Bootstrap) is similar to Cisco's AutoRP, it's a protocol that we use to automatically find the RP (Rendezvous Point) in our multicast network. BSR however, is a standard and included in PIMv2, unlike AutoRP which is a Cisco proprietary protocol.

Reference: https://networklessons.com/cisco/ccie-routing-switching/multicast-pim-bootstrap-bsr#:~:text=BSR%20(Bootstrap)%20is%20similar%20to,is%20a%20Cisco%20proprietary%20protocol

upvoted 1 times

**Reinier_veen** 2 years, 4 months ago

**Selected Answer: A**

Auto-RP = Cisco Propriatary

BSR (bootstrap Router) = standards based

upvoted 1 times

**zlimvos** 2 years, 8 months ago

**Selected Answer: A**

RP standards-based + dynamic RP discovery = bootstrap router

upvoted 1 times

Question #144 *Topic 1*

An engineer must design a QoS solution for a customer. The network currently supports data only, but the customer will roll out VoIP and IP video in conjunction with the new QoS solution. The engineer plans to use DiffServ. To ensure priority for voice services, which model must the design include?

A. 8-class model

B. 4-class model

C. 6-class model

D. 12-class model

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Lungful** 1 year, 6 months ago

Selected Answer: A

A is correct. 8-class also uses multimedia categories and the question mentioned IP video.

upvoted 1 times

**cerifyme85** 1 year, 11 months ago

why not 12?

upvoted 1 times

**bccabrera** 1 year, 9 months ago

The 12-class QoS strategy model builds upon the 8-class model and includes the following additional classes:

Real-time Interactive
Broadcast Video
Management/OAM
Bulk Data

https://www.ciscopress.com/articles/article.asp?p=2756478&seqNum=8

upvoted 1 times

**Reinier_veen** 2 years, 4 months ago

got it.
Ignore my previous comment.
4-class has one queue for both voice and data.
8-class has different queues for voice and data.
question states that voice has to get priority over all other (including voice) data. So we need 8-class (at least).

upvoted 1 times

**Hope66** 2 years, 4 months ago

I'm prone for 8-class model

https://www.ciscopress.com/articles/article.asp?p=2756478&seqNum=8

upvoted 2 times

**Reinier_veen** 2 years, 4 months ago

why not 4-class model? In 4-class is a seperate class for voice (EF). Is nog that the question?

upvoted 1 times

**mgiuseppe86** 1 year, 5 months ago

It is also asking for IP Video.. you get that in 8-class

8-class: 4-class + Multimedia Streaming | Multimedia conferencing | Network control | scavenger

upvoted 1 times

Question #145 *Topic 1*

Which NETCONF operation creates filtering that is specific to the session notifications?

A. <create-subscription>

B. <commit>

C. <notification>

D. <logging>

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**bccabrera** 1 year, 3 months ago

**Selected Answer: A**

2.1.1. <create-subscription>

Description:

This operation initiates an event notification subscription that
will send asynchronous event notifications to the initiator of the
command until the subscription terminates.

upvoted 1 times

**namibdigger** 2 years, 1 month ago

**Selected Answer: A**

Agreed -after reading the RFC (in parts :) ) - it's neither in the online learning guide nor in the CertGuide book

upvoted 2 times

**certstudent2016** 2 years, 4 months ago

https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/5672j-docs-dev-nso/87/1/rfc5277.pdf

A is correct

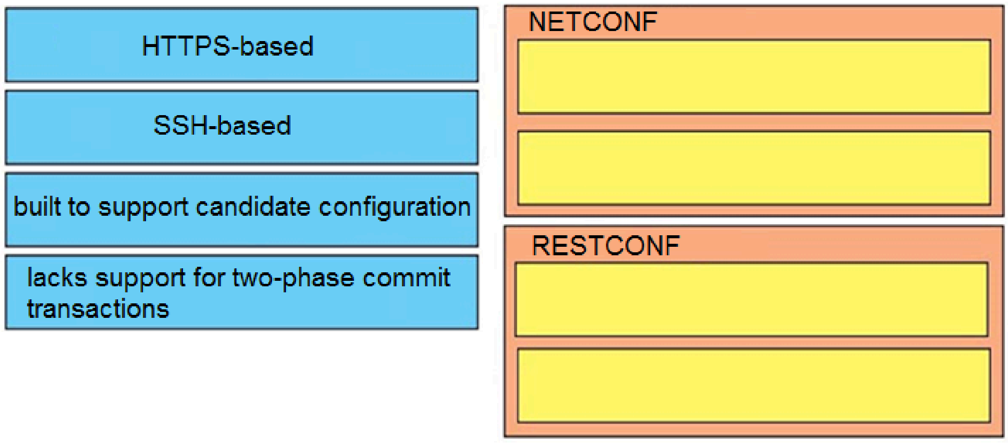
upvoted 1 times

Question #146 *Topic 1*

DRAG DROP -

Drag and drop the properties from the left onto the protocols they describe on the right.

Select and Place:



HTTPS-based

SSH-based

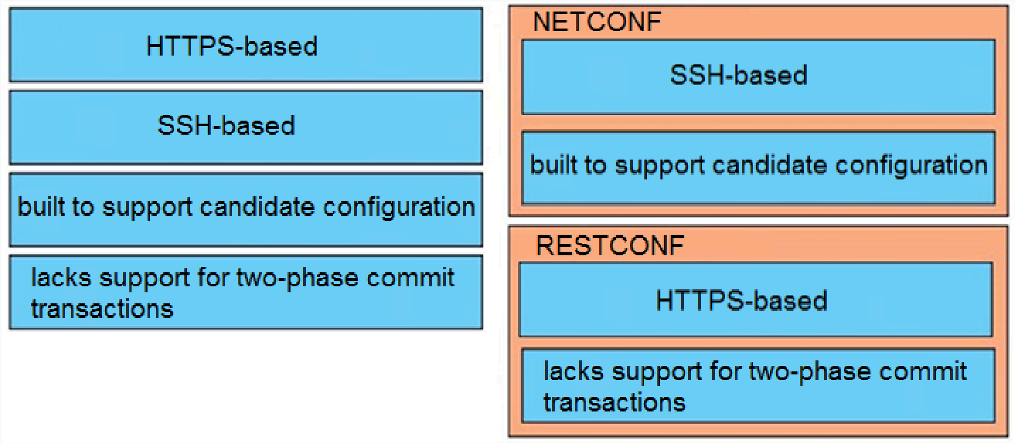
built to support candidate configuration

lacks support for two-phase commit transactions

NETCONF

RESTCONF

**Correct Answer:**



HTTPS-based

SSH-based

built to support candidate configuration

lacks support for two-phase commit transactions

NETCONF

SSH-based

built to support candidate configuration

RESTCONF

HTTPS-based

lacks support for two-phase commit transactions

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

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/169/b_169_programmability_cg/configuring_yang_datamodel.html

**Lungful** 1 year, 6 months ago

The answer is correct.

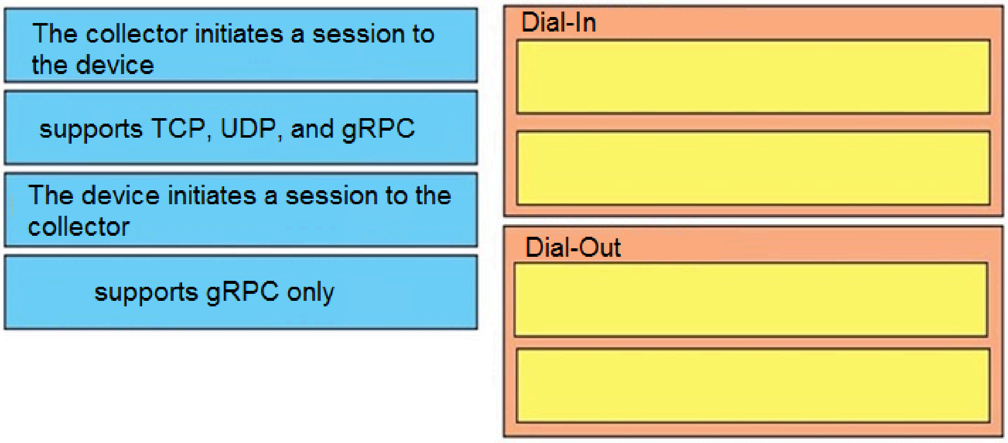
upvoted 1 times

Question #147 Topic 1

DRAG DROP -

Drag and drop the characteristics from the left onto the telemetry mode they apply to on the right.

Select and Place:



The collector initiates a session to the device

supports TCP, UDP, and gRPC

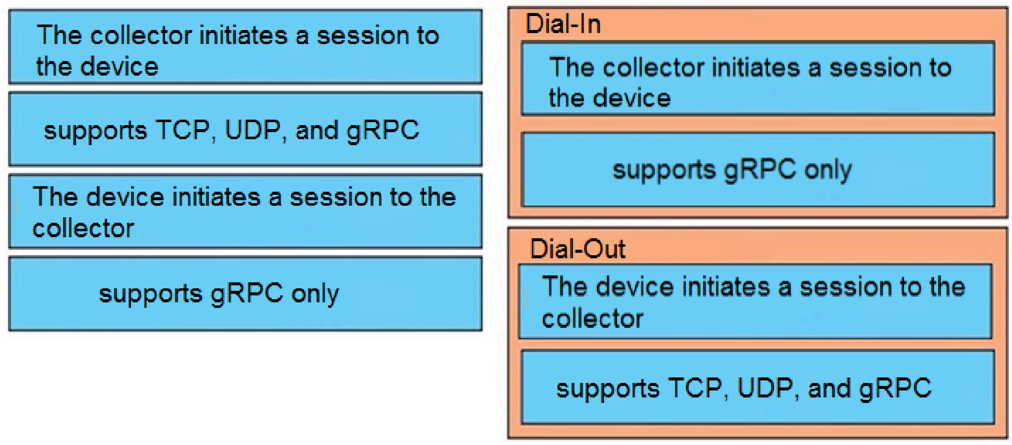
The device initiates a session to the collector

supports gRPC only

Dial-In

Dial-Out

**Correct Answer:**



The collector initiates a session to the device

supports TCP, UDP, and gRPC

The device initiates a session to the collector

supports gRPC only

Dial-In

The collector initiates a session to the device

supports gRPC only

Dial-Out

The device initiates a session to the collector

supports TCP, UDP, and gRPC

In a dial-in mode, the destination initiates a session to the router and subscribes to data to be streamed. Dial-in mode is supported over gRPC in only 64-bit platforms.

In a dial-out mode, the router initiates a session to the destinations based on the subscription. All 64-bit IOS XR platforms (except for NCS 6000 series routers) support gRPC and TCP protocols. All 32-bit IOS XR platforms support only TCP.

Reference:

https://www.cisco.com/c/en/us/td/docs/iosxr/asr9000/telemetry/b-telemetry-cg-asr9000-61x/b-telemetry-cg-asr9000-61x_chapter_010.html#id_36445

**iLikeHamburgers** 1 year, 8 months ago

The answer is correct.

Model-Driven Telemetry (MDT) data is streamed through :

Transmission Control Protocol (TCP): used for only dial-out mode.

User Datagram Protocol (UDP): used for only dial-out mode.

See Transport and Encoding

https://www.cisco.com/c/en/us/td/docs/iosxr/asr9000/telemetry/b-telemetry-cg-asr9000-61x/b-telemetry-cg-asr9000-61x_chapter_011.html

upvoted 1 times

**namibdigger** 2 years, 1 month ago

I guess the answer is correct, since gRCP needs to be configured and maintained - there is a 3-Way handshake (TCP) in every direction but gRPC means that this is the way to retrieve/stream data which works if 'Pulling' via gRPC configures only ...closest to what i can explain

upvoted 1 times

**Hope66** 2 years, 4 months ago

I think that the answer is right:

https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/telemetry/70x/b-telemetry-cg-ncs5500-70x/b-telemetry-cg-ncs5500-70x_chapter_01.html pag.26

upvoted 1 times

⊟ **cwoolie** 2 years, 4 months ago

The answer is wrong. Dial in Supports TCP, UDP, and GRPC, the device initiates a session to the collector. Dial out is the other two options.

upvoted 1 times

⊟ **XalaGyan** 1 year, 7 months ago

Dial-In (Dynamic)

1.Telemetry updates are sent to the initiator or subscriber.

2.Life of the subscription is tied to the connection (session) that created it, and over which telemetry updates are sent. No change is observed in the running configuration.

3.Dial-in subscriptions need to be reinitiated after a reload, because established connections or sessions are killed during stateful switchover.

4.Subscription ID is dynamically generated upon successful establishment of a subscription.

upvoted 2 times

⊟ **XalaGyan** 1 year, 7 months ago

Dial-Out (Static or Configured)

1.Telemetry updates are sent to the specified receiver or collector.

2.Subscription is created as part of the running configuration; it remains as the device configuration till the configuration is removed.

3.Dial-out subscriptions are created as part of the device configuration, and they automatically reconnect to the receiver after a stateful switchover.

4.Subscription ID is fixed and configured on the device as part of the configuration.

upvoted 2 times

Question #148 *Topic 1*

An engineer needs a standards-driven YANG model to manage a multivendor network environment. Which model should the engineer choose?

A. Native

B. OpenConfig

C. IETF

D. IEEE NETCONF

**Correct Answer:** *B*

*Community vote distribution*

B (62%) C (38%)

**LearnMachine** 6 months, 3 weeks ago

Selected Answer: B

IETF - Models developed by the Internet Engineering Task Force (Standards)

OpenConfig - Community-driven models led by major network operators (fast updates, but not standards)

upvoted 1 times

**Seb82** 1 year, 4 months ago

Selected Answer: B

IETF is not a YANG model per se, it is an org that creates YANG models. Question asked for a "standard YANG model"

upvoted 1 times

**bz_boy** 2 years ago

Answer B

https://blogs.cisco.com/networking/solving-multi-vendor-network-management-complexity-with-openconfig

upvoted 1 times

**salmarin** 2 years, 1 month ago

Selected Answer: B

OpenConfig for multi vendor devices.

upvoted 2 times

**neiker45** 2 years, 2 months ago

Selected Answer: B

I say B

upvoted 1 times

**mgiuseppe86** 2 years, 5 months ago

Why do half the comments say B yet only 2 votes? People need to use the voting system more.

upvoted 2 times

**akbntc** 2 years, 5 months ago

Selected Answer: B

It's B: Openconfig.

upvoted 2 times

**electro165** 2 years, 6 months ago

The correct answer is B: OpenConfig

For managing a multivendor network environment with a standards-driven YANG model, the engineer should choose the "OpenConfig" model.

OpenConfig is an industry initiative that aims to provide a vendor-neutral and standardized YANG data model for network device configuration and monitoring. It's designed to work across different vendors' equipment and to promote interoperability in a heterogeneous network environment.

upvoted 1 times

**Clauster** 2 years, 7 months ago

Selected Answer: B

Answer is 100% B
Page 387 OCG Book:

OpenConfig is a group of network operators working on developing programmable interfaces
and tools for managing networks in a vendor-neutral way using software-defined
networking concepts and model-driven management and operations. OpenConfig focuses
on building consistent sets of vendor-neutral data models written in YANG to support
operational needs and requirements from various network operators

upvoted 2 times

**J2J2J2J** 2 years, 8 months ago

**Selected Answer: C**

YANG is a data modeling language developed in the IETF. It is used to model configuration and state data manipulated by protocols such as NETCONF and RESTCONF. YANG enables easier management of network elements, such as routers, and is widely used and deployed by many network equipment vendors and network operators.

upvoted 2 times

**Emily23** 2 years, 8 months ago

The YANG Model Coordination Group, for example, has been spending time on the inventory of YANG models in the industry, tooling aspects, training and education of NETCONF, YANG, pyang, and the model coordination for the IETF.

OpenConfig focuses on building consistent sets of vendor-neutral data models written in YANG to support operational needs and requirements from various network operators.

upvoted 1 times

**namibdigger** 3 years, 7 months ago

According to Student learning guide and Cert Guide C is correct - where it's stating that IETF is developing and updating several YANG models - which means they are vendor independant. So C seems right.

upvoted 2 times

**python_tamer** 3 years, 9 months ago

**Selected Answer: C**

I believe it's C.
"We support a comprehensive set of IOS XR native models as well as industry-driven OpenConfig models and standards-driven IETF models"
https://blogs.cisco.com/sp/advancing-your-programmability-journey-with-latest-ios-xr-innovations

upvoted 3 times

**Hope66** 3 years, 10 months ago

I think that the answer is OpenConfig too.
Pag. 387 ENSLD-420 book
and
https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-741518.html (find the word "Multivendor")

upvoted 1 times

**namibdigger** 3 years, 7 months ago

Your answer refers to OpenConfig BGP YANG - which is a model for routing protocol BGP. The question asks for a network management model; the article you refer to also contains an introduction to _generalö_ data models - citing IETF. That's why i think its C

upvoted 1 times

**cwoolie** 3 years, 11 months ago

Why not OpenConfig? Openconfig support all vendors of network gear

upvoted 1 times

Question #149 *Topic 1*

An engineer is working with NETCONF and Cisco NX-OS based devices. The engineer needs a YANG model that supports a specific feature relevant only to
Cisco NX-OS. Which model should the engineer choose?

A. Native

B. IEEE

C. OpenConfig

D. IETF

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**alphatag** Highly Voted 👍 2 years, 4 months ago

The correct answer is NATIVE model, that in this case are specific to the IOS-XR, NX-OS and IOS-XE Cisco platforms. Cisco data models are available on GitHub, at: https://github.com/YangModels/yang/tree/master/vendor/cisco

upvoted 7 times

**Eards** Most Recent ◷ 1 year, 4 months ago

Selected Answer: A

Native - vendor specific

upvoted 1 times

**namibdigger** 1 year, 7 months ago

Selected Answer: A

While D is not wrong Cisco NX-OS brings a Native YANG model along: 'For more a complete set of feature support, and for support of specific Cisco NX-OS Software features, using a native YANG model with NX-OS is recommended (https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-741518.html#_Toc528621677)

upvoted 1 times

**zlimvos** 1 year, 8 months ago

Selected Answer: A

Native ofcourse

upvoted 1 times

**bogd** 2 years ago

Selected Answer: A

https://blogs.cisco.com/developer/which-yang-model-to-use

"Models created by Vendors are often referred to as “Native” models – as in they are Native to the devices/software for which they are associated with."

upvoted 4 times

Question #150 Topic 1

A client is moving to Model-Driven Telemetry and requires periodic updates. What must the network architect consider with this design?

A. Updates that contain changes within the data are sent only when changes occur.

B. Empty data subscriptions do not generate empty update notifications.

C. Periodic updates include a full copy of the data that is subscribed to.

D. The primary push update is sent immediately and cannot be delayed.

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**goku2020** Highly Voted 4 years, 3 months ago

C is correct.

upvoted 6 times

**Clauster** Most Recent 1 year, 7 months ago

**Selected Answer: C**

Answer is C

I was able to find the documentation on Cisco WhitePages

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/173/b_173_programmability_cg/model_driven_telemetry.html

upvoted 2 times

**namibdigger** 2 years, 7 months ago

**Selected Answer: C**

I Agree on C but find it difficult to see the difference in A (ENSLD Cert Guide p 390: on-change subscription streams out data only when a change in the data has occured' -differnce may be in 'Periodic subscription' which is not the usual approach for A

upvoted 2 times

**Xavi07** 3 years, 8 months ago

C is correct. Periodic updates contain a full copy of the subscribed data element or table.

upvoted 1 times

**luisjuradoledesma** 4 years, 1 month ago

Agree - C is correct - Periodic updates contain a full copy of the subscribed data element or table for all supported transport protocols

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b_166_programmability_cg/model_driven_telemetry.html

upvoted 4 times

## Question #151 *Topic 1*

An infrastructure team is concerned about the shared memory utilization of a device, and for this reason, they need to monitor the device state. Which solution limits impact on the device and provides the required data?

A. IPFIX

B. static telemetry

C. on-change subscription

D. periodic subscription

**Correct Answer:** *D*

*Community vote distribution*

D (75%) C (25%)

**goku2020** Highly Voted 5 years, 3 months ago

C is correct Change-on subscription have less impact, more specific to obtain information.

upvoted 10 times

**zzmejce** Highly Voted 3 years, 2 months ago

**Selected Answer: D**

Memory usage is measured in bytes and changes very frequently. On-change subscription will send data almost non-stop. In this case periodic change is more suitable.

upvoted 7 times

**NoHombre** Most Recent 5 months, 3 weeks ago

**Selected Answer: D**

It is not recommended to use on-change subscriptions for frequently changing data values such as counters
incrementing on an interface.

upvoted 1 times

**guerreroa25** 9 months, 2 weeks ago

**Selected Answer: C**

On-change subscription is the solution that limits the impact on the device and provides the required data. On-change subscription allows for monitoring specific data in real-time, only sending the data when it changes, and not continuously. This can help limit the impact on device resources, such as shared memory utilization.

upvoted 2 times

**PicoOstrava** 1 year, 3 months ago

**Selected Answer: D**

Creating an on-change subscription for a data node value that is known to change constantly would send excess data to the MDT stream, and could be detrimental to the data collection process. It is highly recommended to use periodic subscriptions for data node values that are constantly changing.

upvoted 1 times

**PicoOstrava** 1 year, 3 months ago

**Selected Answer: D**

If the main goal is to have comprehensive, real-time updates on memory utilization with less impact, D (periodic subscription) could be more suitable since it ensures regular state data collection

upvoted 1 times

**mithradel** 1 year, 9 months ago

D. periodic ->
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/model-driven-telemetry-wp.html

upvoted 1 times

**akbntc** 2 years, 5 months ago

**Selected Answer: C**

C (On-Change) is correct solution for monitoring device state, for example, when an interface goes down, or when an OSPF adjacency goes down.

upvoted 2 times

**Lungful** 2 years, 6 months ago

Selected Answer: D

D is correct. Periodic is more suitable for memory usage. "Periodic publication is perfect for counters or measures that constantly change, such as the current bandwidth utilization of your network interfaces."

https://community.dataminer.services/simplify-network-operations-with-telemetry-streaming-data/

upvoted 1 times

**magicrushb76** 2 years, 6 months ago

Answer is C. With on-change subscriptions, the first push update is the entire set of subscribed to data (the initial sychronization as defined in the IETF documents). This is not controllable. Subsequent updates are sent when the data changes, and consist of only the changed data. However, the minimum data resolution for a change is a row. So, if an on-change subscription is to a leaf within a row, if any item in that row changes, an update notification is sent. The exact contents of the update notification depend on the transport protocol.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1612/b_1612_programmability_cg/model_driven_telemetry.html

upvoted 1 times

**SomKeat** 2 years, 7 months ago

answer is C

upvoted 1 times

**CKL_SG** 2 years, 9 months ago

Selected Answer: D

concerned about the shared memory utilization of a device, and for this reason, they need to monitor the device state
question mention they are concerned and need to monitor, thus i believe D which is periodic subscription more suitable as they want to know memory utilization from time to time and For periodic subscriptions the update trigger is specified by time interval and an time for the report to be sent.
rather than on-change subscription an update trigger occurs whenever a change in the subscribed information is detected

upvoted 2 times

**namibdigger** 3 years, 7 months ago

Selected Answer: C

Aggree on C as correct, that's exactly what on-change subscription is meant for (they monitor the state of the device (e.g. operational/non-operational) not the amount of memory used which might work with A (in SDA)

upvoted 2 times

**bogd** 4 years ago

Selected Answer: C

Less impact ==> on-change subscription

upvoted 1 times

**Xavi07** 4 years, 8 months ago

I agree, C is correct. On change subscription

upvoted 1 times

**luisjuradoledesma** 5 years, 1 month ago

C (change-on subscription) looks correct
There are two types of subscriptions: periodic and on-change. With periodic subscription, data is streamed out to the destination at the configured interval. It continuously sends data for the lifetime of that subscription. With on-change, data is published only when a change in the data occurs such as when an interface or OSPF neighbor goes down.
https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming-telemetry

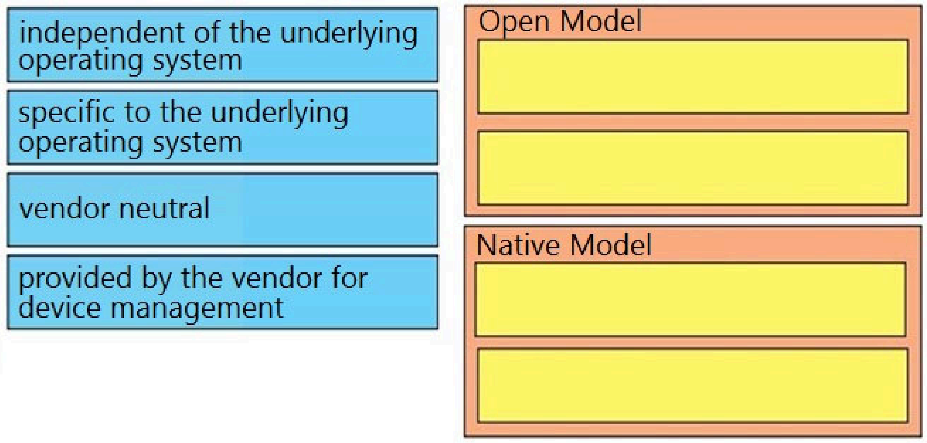
upvoted 3 times

Question #152 Topic 1

DRAG DROP -

Drag and drop the characteristics from the left onto the YANG model they describe on the right.

Select and Place:



independent of the underlying operating system

specific to the underlying operating system

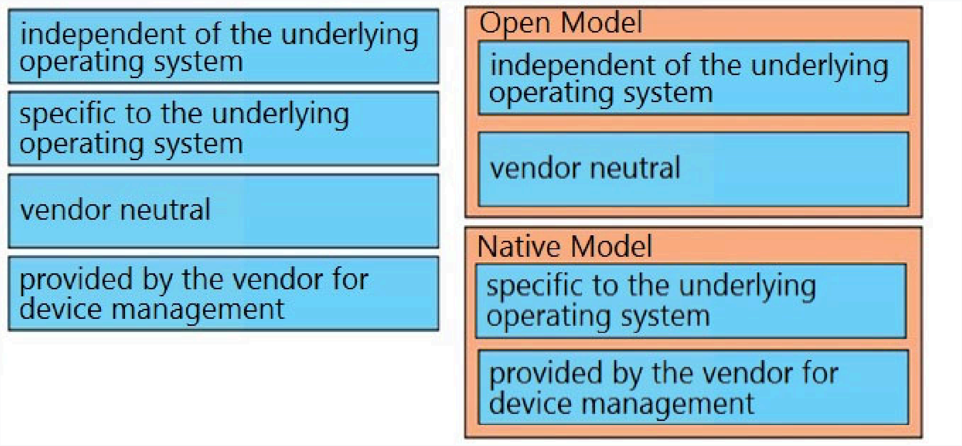
vendor neutral

provided by the vendor for device management

Open Model

Native Model

**Correct Answer:**



independent of the underlying operating system

specific to the underlying operating system

vendor neutral

provided by the vendor for device management

Open Model

independent of the underlying operating system

vendor neutral

Native Model

specific to the underlying operating system

provided by the vendor for device management

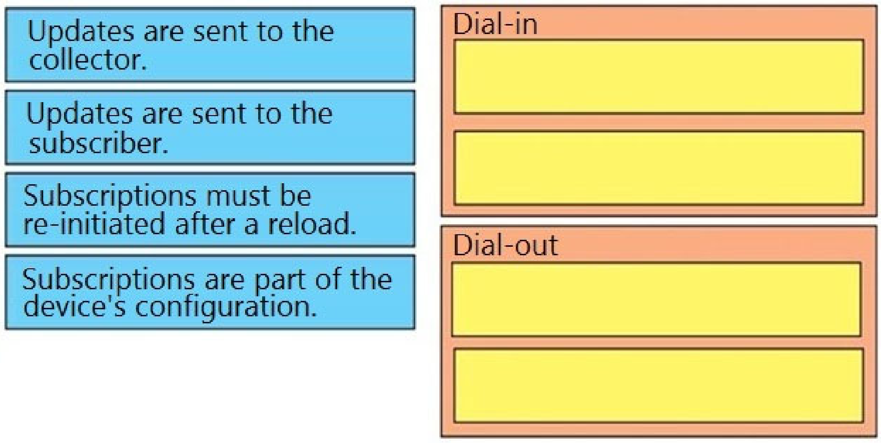
Currently there are no comments in this discussion, be the first to comment!

## Question #153 *Topic 1*

DRAG DROP -

Drag and drop the model driven telemetry characteristics from the left onto the mode they belong to on the right.

Select and Place:



Updates are sent to the collector.

Updates are sent to the subscriber.

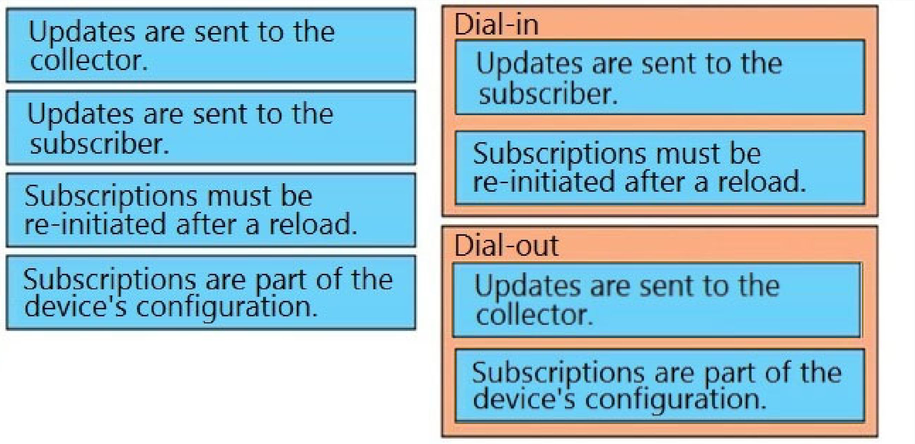
Subscriptions must be re-initiated after a reload.

Subscriptions are part of the device's configuration.

Dial-in

Dial-out

**Correct Answer:**



Updates are sent to the collector.

Updates are sent to the subscriber.

Subscriptions must be re-initiated after a reload.

Subscriptions are part of the device's configuration.

Dial-in

Updates are sent to the subscriber.

Subscriptions must be re-initiated after a reload.

Dial-out

Updates are sent to the collector.

Subscriptions are part of the device's configuration.

**XalaGyan** 1 year, 7 months ago

Dial-In (Dynamic)

1.Telemetry updates are sent to the initiator or subscriber.

2.Life of the subscription is tied to the connection (session) that created it, and over which telemetry updates are sent. No change is observed in the running configuration.

3.Dial-in subscriptions need to be reinitiated after a reload, because established connections or sessions are killed during stateful switchover.

4.Subscription ID is dynamically generated upon successful establishment of a subscription.

Dial-Out (Static or Configured)

1.Telemetry updates are sent to the specified receiver or collector.

2.Subscription is created as part of the running configuration; it remains as the device configuration till the configuration is removed.

3.Dial-out subscriptions are created as part of the device configuration, and they automatically reconnect to the receiver after a stateful switchover.

4.Subscription ID is fixed and configured on the device as part of the configuration.

upvoted 2 times

Question #154 *Topic 1*

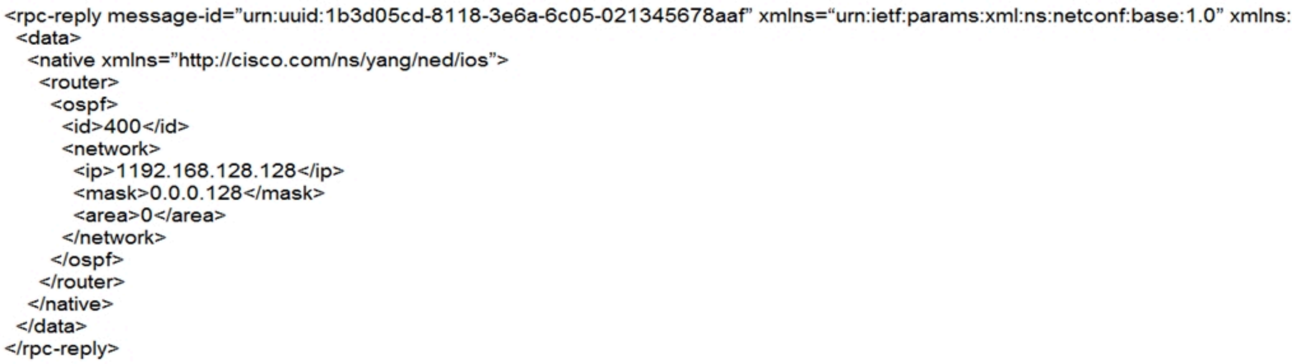
An engineer uses Postman and YANG to configure a router with:

⊸ OSPF process ID 400

⊸ network 192.168.128.128/25 enabled for Area 0

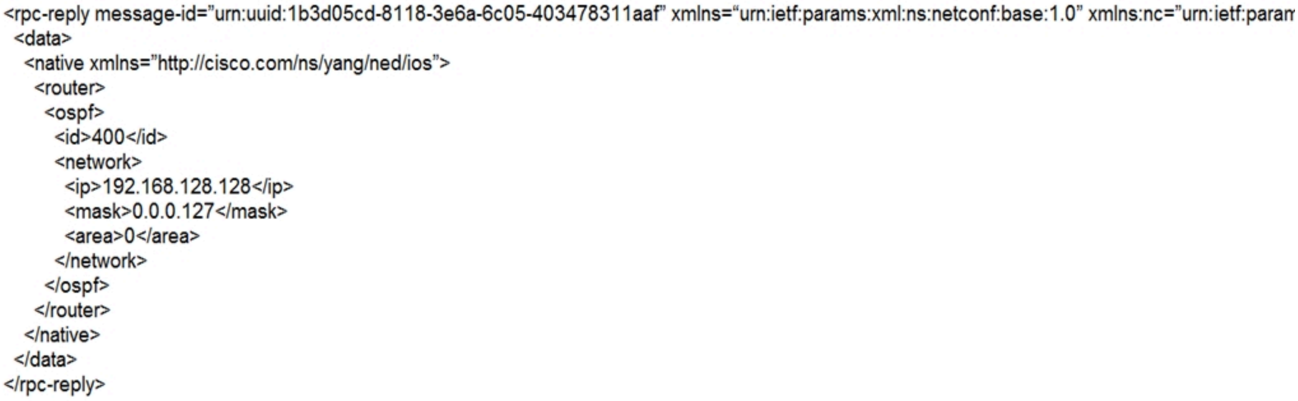
Which get-config reply verifies that the model set was designed correctly?

A.



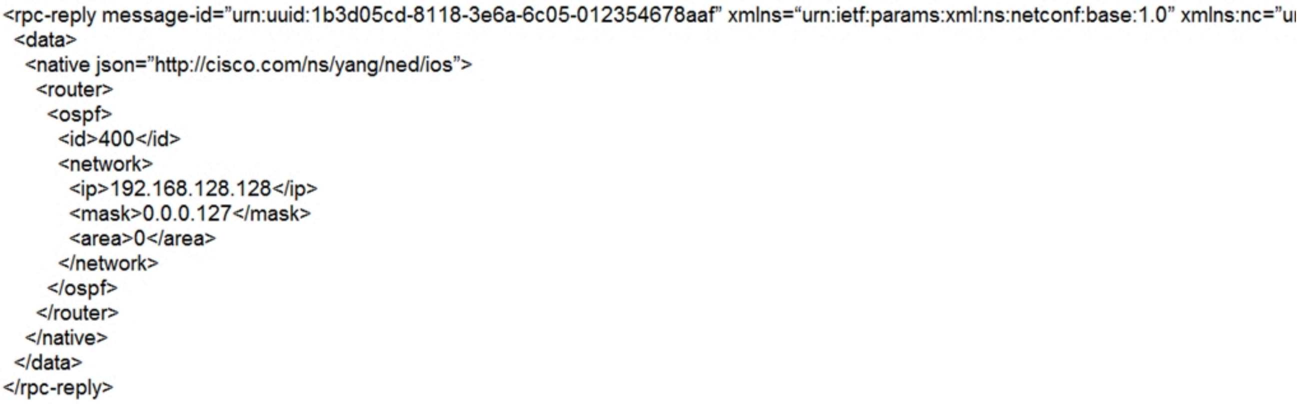
```
<rpc-reply message-id="urn:uuid:1b3d05cd-8118-3e6a-6c05-021345678aaf" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:
 <data>
  <native xmlns="http://cisco.com/ns/yang/ned/ios">
   <router>
    <ospf>
     <id>400</id>
     <network>
      <ip>1192.168.128.128</ip>
      <mask>0.0.0.128</mask>
      <area>0</area>
     </network>
    </ospf>
   </router>
  </native>
 </data>
</rpc-reply>
```

B.



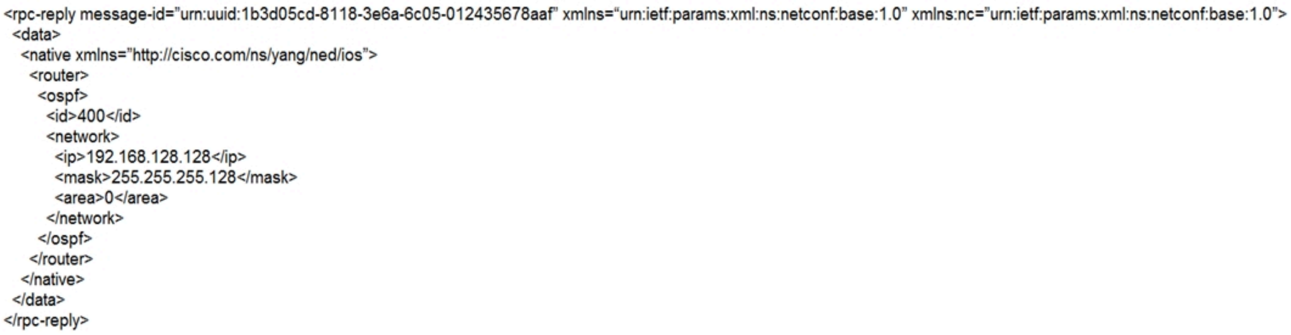
```
<rpc-reply message-id="urn:uuid:1b3d05cd-8118-3e6a-6c05-403478311aaf" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:nc="urn:ietf:param
 <data>
  <native xmlns="http://cisco.com/ns/yang/ned/ios">
   <router>
    <ospf>
     <id>400</id>
     <network>
      <ip>192.168.128.128</ip>
      <mask>0.0.0.127</mask>
      <area>0</area>
     </network>
    </ospf>
   </router>
  </native>
 </data>
</rpc-reply>
```

C.



```
<rpc-reply message-id="urn:uuid:1b3d05cd-8118-3e6a-6c05-012354678aaf" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:nc="u
 <data>
  <native json="http://cisco.com/ns/yang/ned/ios">
   <router>
    <ospf>
     <id>400</id>
     <network>
      <ip>192.168.128.128</ip>
      <mask>0.0.0.127</mask>
      <area>0</area>
     </network>
    </ospf>
   </router>
  </native>
 </data>
</rpc-reply>
```

D.



```
<rpc-reply message-id="urn:uuid:1b3d05cd-8118-3e6a-6c05-012435678aaf" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
 <data>
  <native xmlns="http://cisco.com/ns/yang/ned/ios">
   <router>
    <ospf>
     <id>400</id>
     <network>
      <ip>192.168.128.128</ip>
      <mask>255.255.255.128</mask>
      <area>0</area>
     </network>
    </ospf>
   </router>
  </native>
 </data>
</rpc-reply>
```

**Correct Answer:** *B*

**Clauster** 1 year, 7 months ago

Ok guys so i got the answer right

Let's start by process of elimination, on OSPF we use WildCard Masks, so immediately A and D are out of the question and invalid.

Second thing is with C, NETCONF does not use JSON, and there's a JSON on one of the lines which makes this answer invalid and the only answer left is B

upvoted 4 times

⊟ **vangio** 1 year, 7 months ago

Correct B. XML

upvoted 1 times

⊟ **zlimvos** 2 years, 8 months ago

B (or C) are correct due to the mask. There is a small part not visible which makes one question wrong (param:json instead of xml)

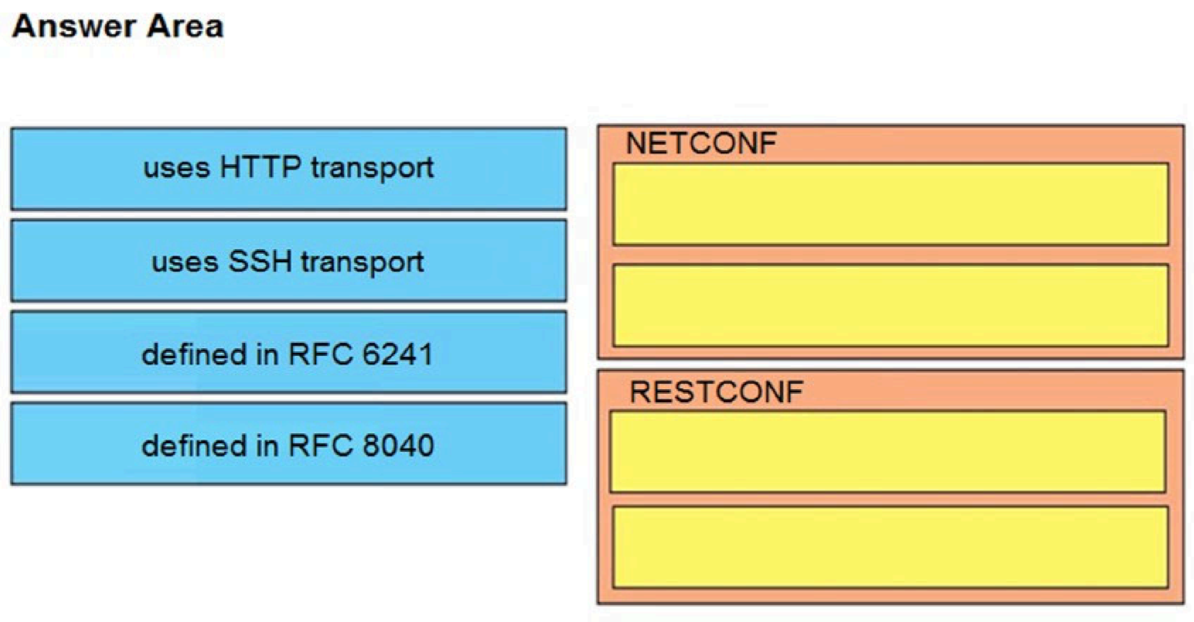
upvoted 1 times

Question #155 Topic 1

DRAG DROP -

Drag and drop the characteristics from the left onto the configuration protocols they describe on the right.

Select and Place:



Answer Area

uses HTTP transport

uses SSH transport

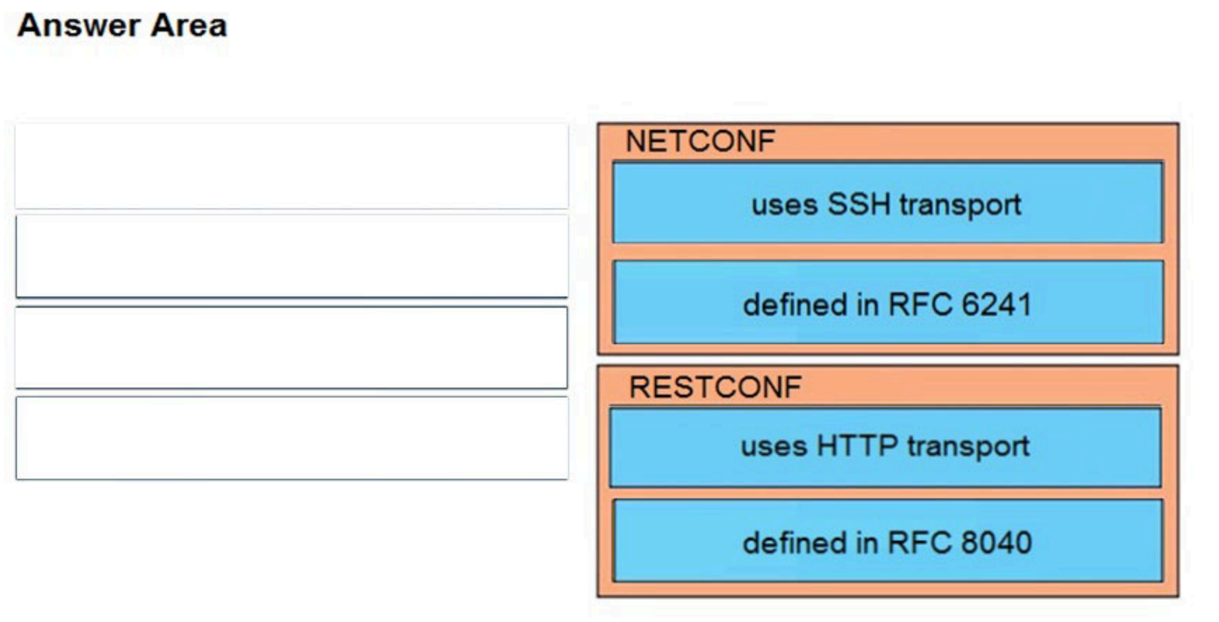
defined in RFC 6241

defined in RFC 8040

NETCONF

RESTCONF

**Correct Answer:**



Answer Area

NETCONF

uses SSH transport

defined in RFC 6241

RESTCONF

uses HTTP transport

defined in RFC 8040

**Clauster** Highly Voted 1 year, 7 months ago

So remember that NETCONF was created before RESTCONF, RESTCONF works in conjunction with NETCONF it was created to basically help NETCONF, if you remember this you will make the obvious choice 6241 comes first

upvoted 8 times

**certstudent2016** Most Recent 2 years, 10 months ago

https://www.ipspace.net/kb/CiscoAutomation/070-netconf.html#:~:text=NETCONF%20provides%20mechanisms%20to%20install,on%20top%20of%20HTTP%2FHTTPS.

upvoted 1 times

Question #156 *Topic 1*

A company must automate a set of complex changes aligned with DR testing in the network. These changes are specific, and the DR playbook will be adjusted in the future. The playbook has diverse routing and switching assets in scope as well as multiple vendor and hardware platforms. A developer will create a thin, web front-end microservice and integrate with an Open Daylight controller to push changes to the network. Which YANG model should be used?

A. Use an open YANG model to allow the reuse of code and standardize the implementation across platforms.

B. Develop an individualized YANG model to minimize development resources and time to market.

C. Use multiple native vendor YANG models to provide code consistency.

D. Use a single native vendor YANG model to minimize development time.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**neiker45** 1 year, 8 months ago

Standardization is always good for coding. Don't need to re-invent the wheel unless needed.

upvoted 1 times

**namibdigger** 3 years, 1 month ago

**Selected Answer: A**

Considering all the requirements in the question A seems obvious

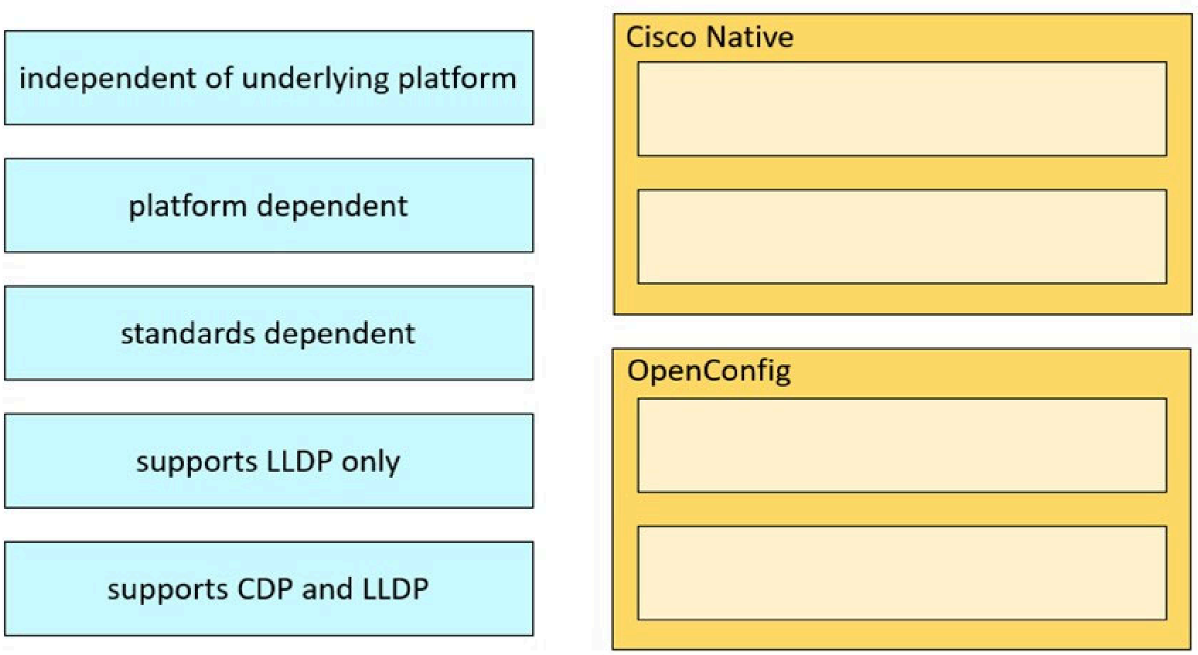
upvoted 2 times

Question #157 *Topic 1*

DRAG DROP -

Drag and drop the characteristics from the left onto the YANG models they describe on the right. Not all options are used.

Select and Place:



independent of underlying platform

platform dependent

standards dependent

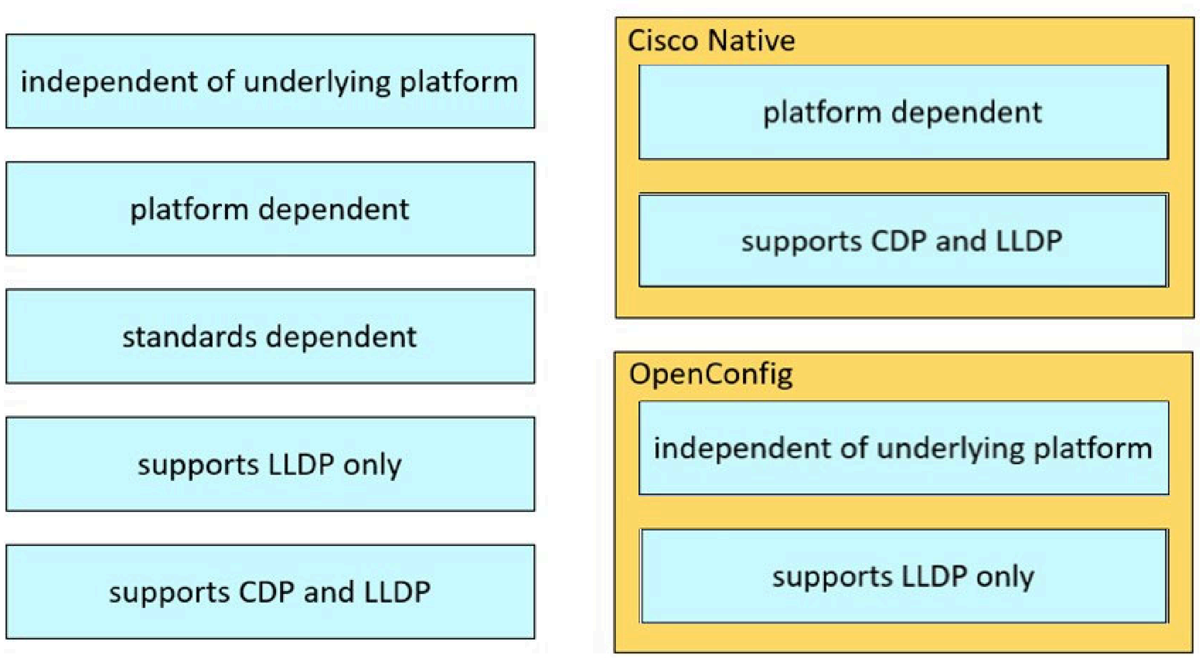
supports LLDP only

supports CDP and LLDP

Cisco Native

OpenConfig

**Correct Answer:**



independent of underlying platform

platform dependent

standards dependent

supports LLDP only

supports CDP and LLDP

Cisco Native

- platform dependent
- supports CDP and LLDP

OpenConfig

- independent of underlying platform
- supports LLDP only

Currently there are no comments in this discussion, be the first to comment!

Question #158 Topic 1

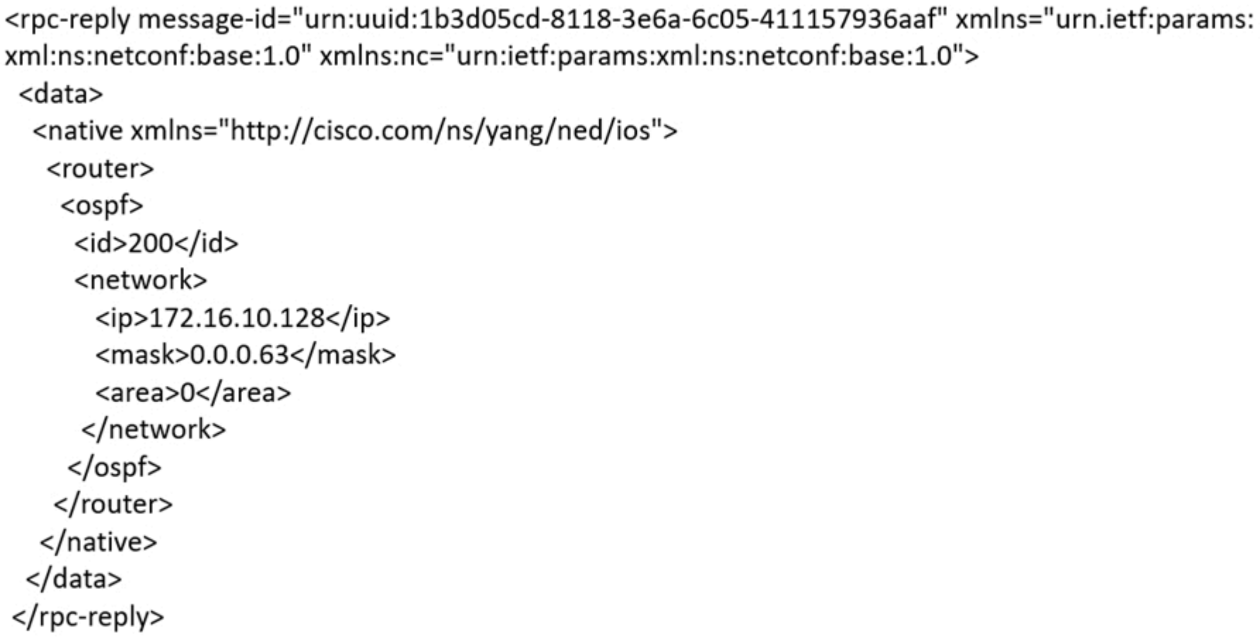
An engineer uses Postman and YANG to configure a router with:

✑ OSPF process ID 200

✑ network 172.16.10.128/26 enabled for Area 0

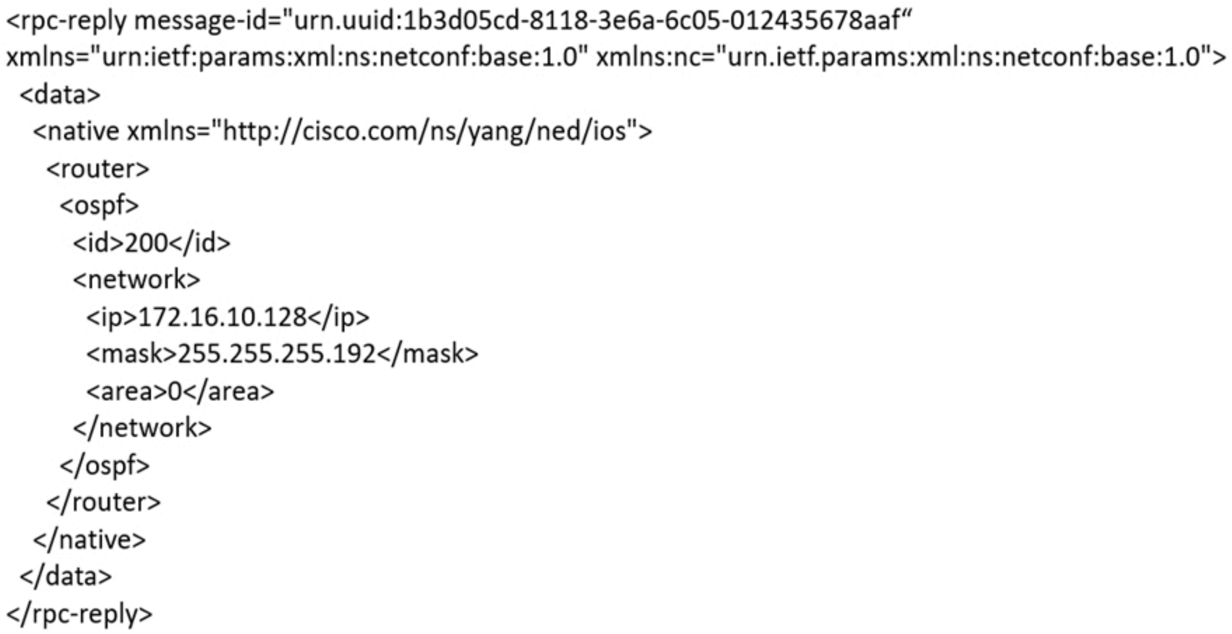
Which get-config reply verifies that the model set was designed correctly?

A.



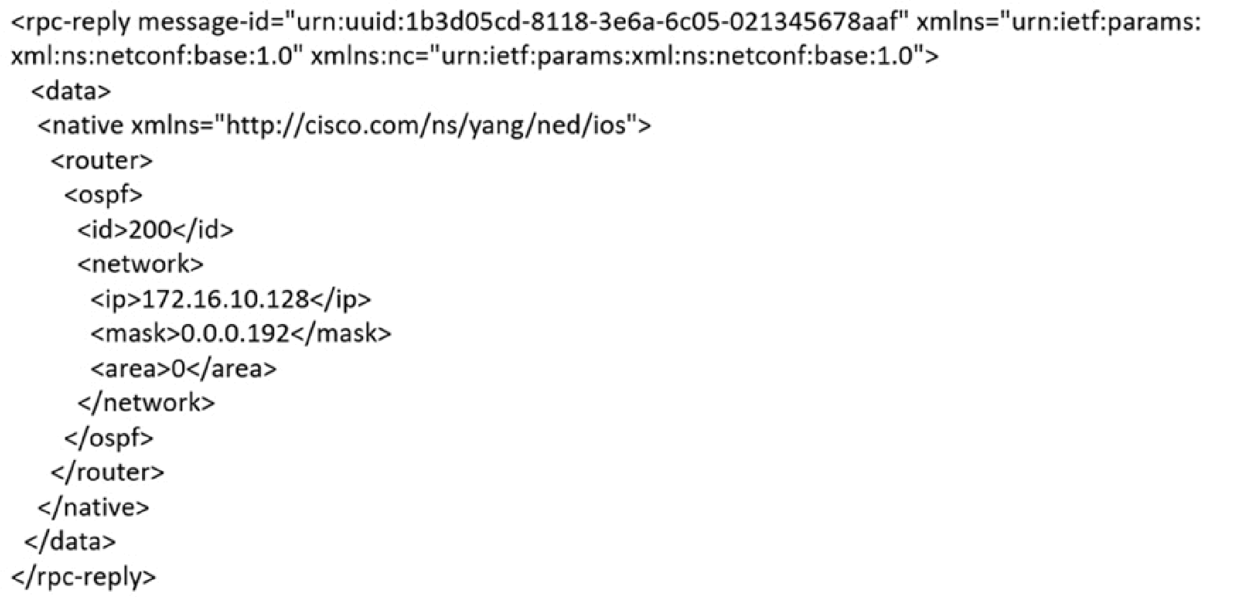
```
<rpc-reply message-id="urn:uuid:1b3d05cd-8118-3e6a-6c05-411157936aaf" xmlns="urn.ietf:params:
xml:ns:netconf:base:1.0" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
 <data>
  <native xmlns="http://cisco.com/ns/yang/ned/ios">
   <router>
    <ospf>
     <id>200</id>
     <network>
       <ip>172.16.10.128</ip>
       <mask>0.0.0.63</mask>
       <area>0</area>
      </network>
     </ospf>
    </router>
   </native>
  </data>
 </rpc-reply>
```

B.



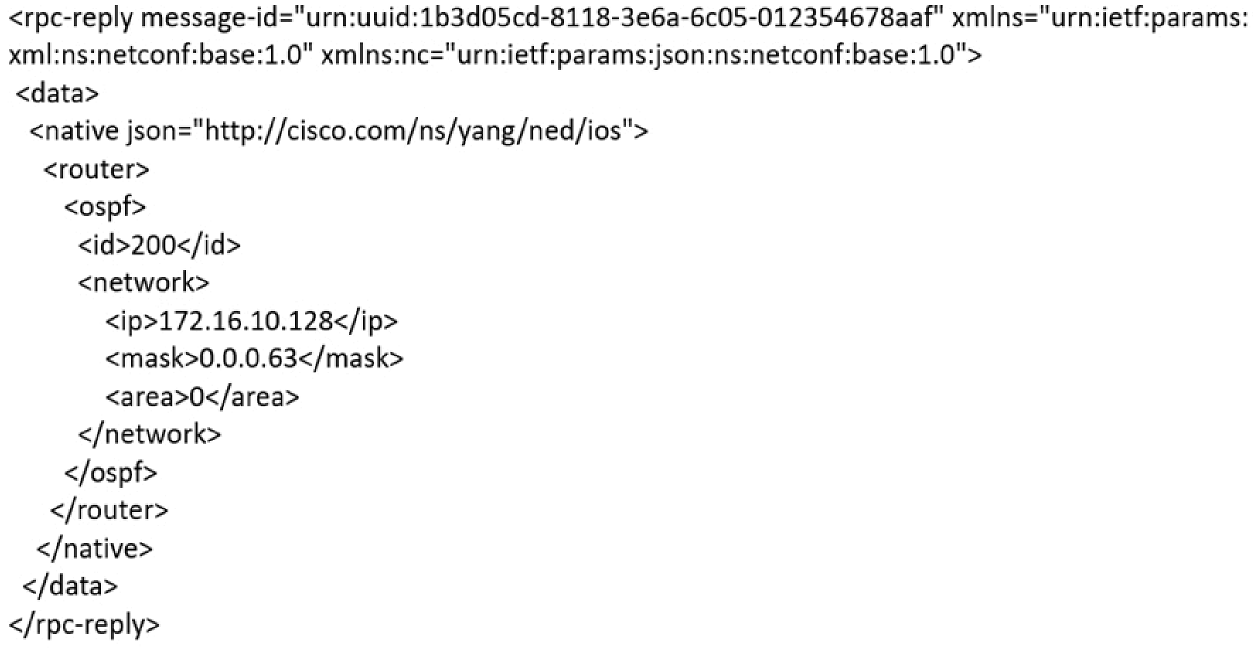
```
<rpc-reply message-id="urn.uuid:1b3d05cd-8118-3e6a-6c05-012435678aaf“
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:nc="urn.ietf.params:xml:ns:netconf:base:1.0">
 <data>
  <native xmlns="http://cisco.com/ns/yang/ned/ios">
   <router>
    <ospf>
     <id>200</id>
     <network>
      <ip>172.16.10.128</ip>
      <mask>255.255.255.192</mask>
      <area>0</area>
     </network>
    </ospf>
   </router>
  </native>
 </data>
</rpc-reply>
```

C.



```
<rpc-reply message-id="urn:uuid:1b3d05cd-8118-3e6a-6c05-021345678aaf" xmlns="urn:ietf:params:
xml:ns:netconf:base:1.0" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
   <native xmlns="http://cisco.com/ns/yang/ned/ios">
    <router>
     <ospf>
      <id>200</id>
      <network>
       <ip>172.16.10.128</ip>
       <mask>0.0.0.192</mask>
       <area>0</area>
      </network>
     </ospf>
    </router>
   </native>
  </data>
</rpc-reply>
```

D.



```
<rpc-reply message-id="urn:uuid:1b3d05cd-8118-3e6a-6c05-012354678aaf" xmlns="urn:ietf:params:
xml:ns:netconf:base:1.0" xmlns:nc="urn:ietf:params:json:ns:netconf:base:1.0">
 <data>
   <native json="http://cisco.com/ns/yang/ned/ios">
     <router>
       <ospf>
         <id>200</id>
         <network>
           <ip>172.16.10.128</ip>
           <mask>0.0.0.63</mask>
           <area>0</area>
         </network>
       </ospf>
     </router>
   </native>
 </data>
</rpc-reply>
```

**Correct Answer:** *A*

**Reinier_veen** Highly Voted 2 years, 4 months ago

two things to check:

1) does the subnetmask add-up?

2) correct combination of protocol and encoding? (netconf ==> XML)

upvoted 5 times

**Clauster** Most Recent 1 year, 7 months ago

The correct answer is A, it's got the right encoding (XML) plus the right subnet.
The other answer that has a correct Subnet (Wildcard) has JSON encoding which is not supported on NETCONF, please know that get-config is a NETCONF command and this is XML output.

upvoted 2 times

## Question #159 *Topic 1*

An engineer must use YANG with an XML representation to configure a Cisco IOS XE switch with these specifications:

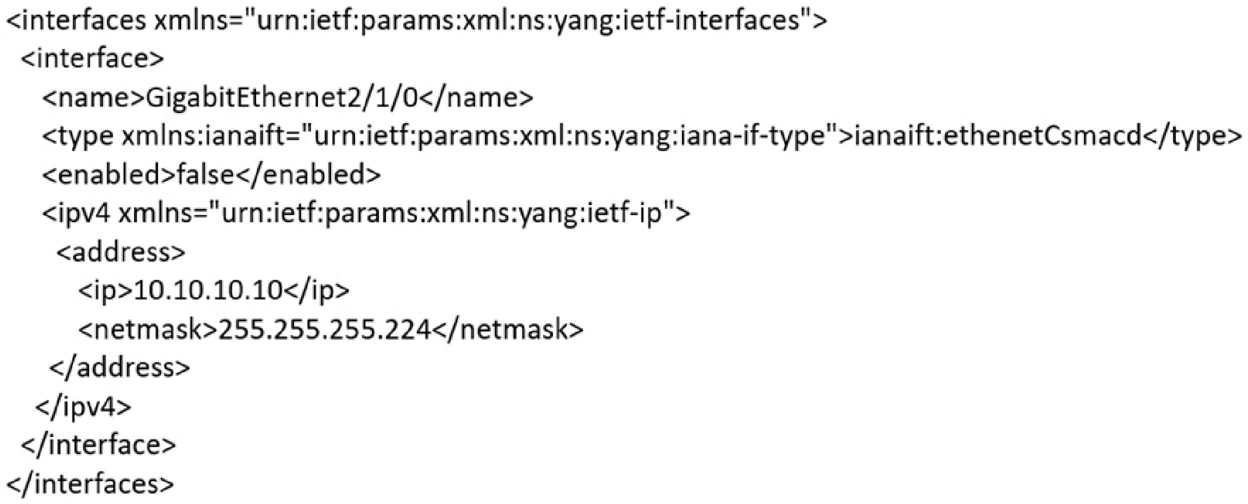
IP address 10.10.10.10/27 configured on the interface GigabitEthernet2/1/0

▪

☞ connectivity from a directly connected host 10.10.10.1/27

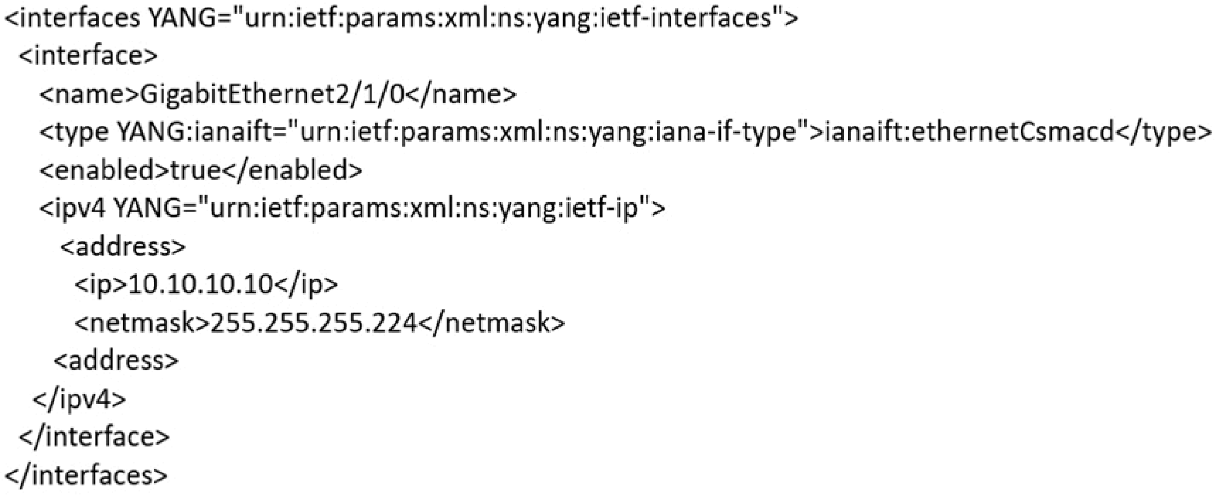
Which YANG data model set must the engineer choose?

A.



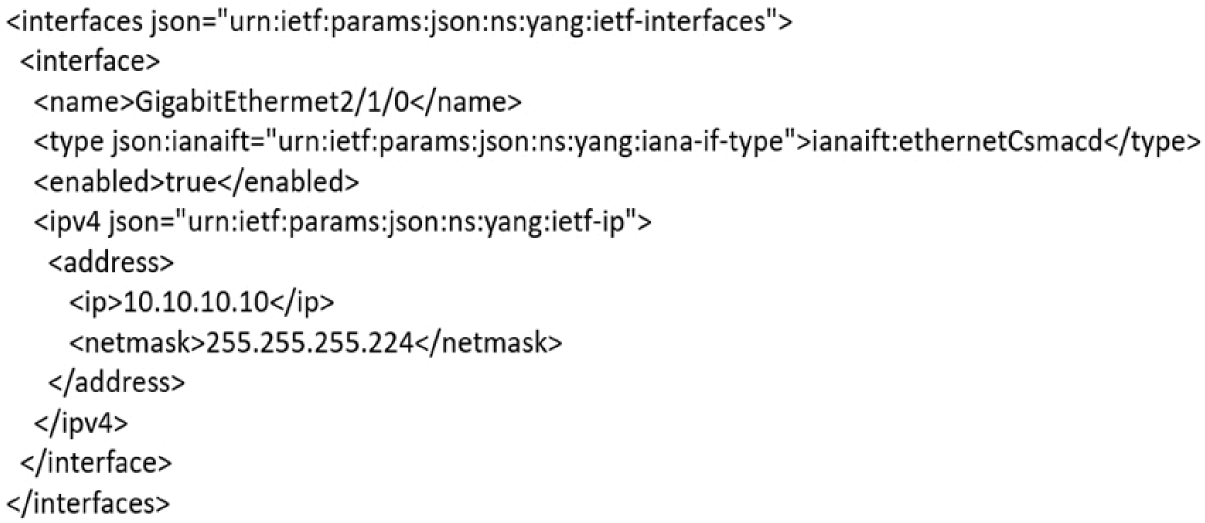
```
<interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
 <interface>
   <name>GigabitEthernet2/1/0</name>
   <type xmlns:ianaift="urn:ietf:params:xml:ns:yang:iana-if-type">ianaift:ethenetCsmacd</type>
   <enabled>false</enabled>
   <ipv4 xmlns="urn:ietf:params:xml:ns:yang:ietf-ip">
    <address>
      <ip>10.10.10.10</ip>
      <netmask>255.255.255.224</netmask>
    </address>
   </ipv4>
 </interface>
</interfaces>
```

B.



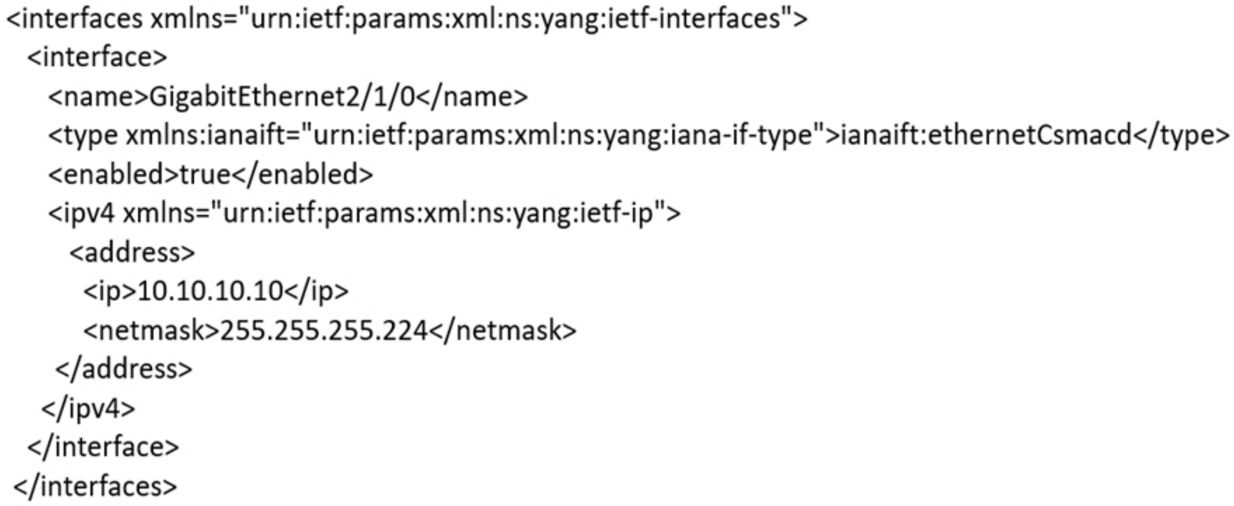
```
<interfaces YANG="urn:ietf:params:xml:ns:yang:ietf-interfaces">
 <interface>
   <name>GigabitEthernet2/1/0</name>
   <type YANG:ianaift="urn:ietf:params:xml:ns:yang:iana-if-type">ianaift:ethernetCsmacd</type>
   <enabled>true</enabled>
   <ipv4 YANG="urn:ietf:params:xml:ns:yang:ietf-ip">
    <address>
      <ip>10.10.10.10</ip>
      <netmask>255.255.255.224</netmask>
    <address>
   </ipv4>
 </interface>
</interfaces>
```

C.



```
<interfaces json="urn:ietf:params:json:ns:yang:ietf-interfaces">
  <interface>
    <name>GigabitEthermet2/1/0</name>
    <type json:ianaift="urn:ietf:params:json:ns:yang:iana-if-type">ianaift:ethernetCsmacd</type>
    <enabled>true</enabled>
    <ipv4 json="urn:ietf:params:json:ns:yang:ietf-ip">
      <address>
        <ip>10.10.10.10</ip>
        <netmask>255.255.255.224</netmask>
      </address>
    </ipv4>
  </interface>
</interfaces>
```

D.



```
<interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
  <interface>
    <name>GigabitEthernet2/1/0</name>
    <type xmlns:ianaift="urn:ietf:params:xml:ns:yang:iana-if-type">ianaift:ethernetCsmacd</type>
    <enabled>true</enabled>
    <ipv4 xmlns="urn:ietf:params:xml:ns:yang:ietf-ip">
      <address>
        <ip>10.10.10.10</ip>
        <netmask>255.255.255.224</netmask>
      </address>
    </ipv4>
  </interface>
</interfaces>
```

**Correct Answer:** *D*

**XalaGyan** Highly Voted 1 year, 7 months ago

Watchout for answer A as the interface is left ENABLED=false, while is the same but enabled=true.

Both will work but only D will leave the ip configured AND NO SHUT the interface

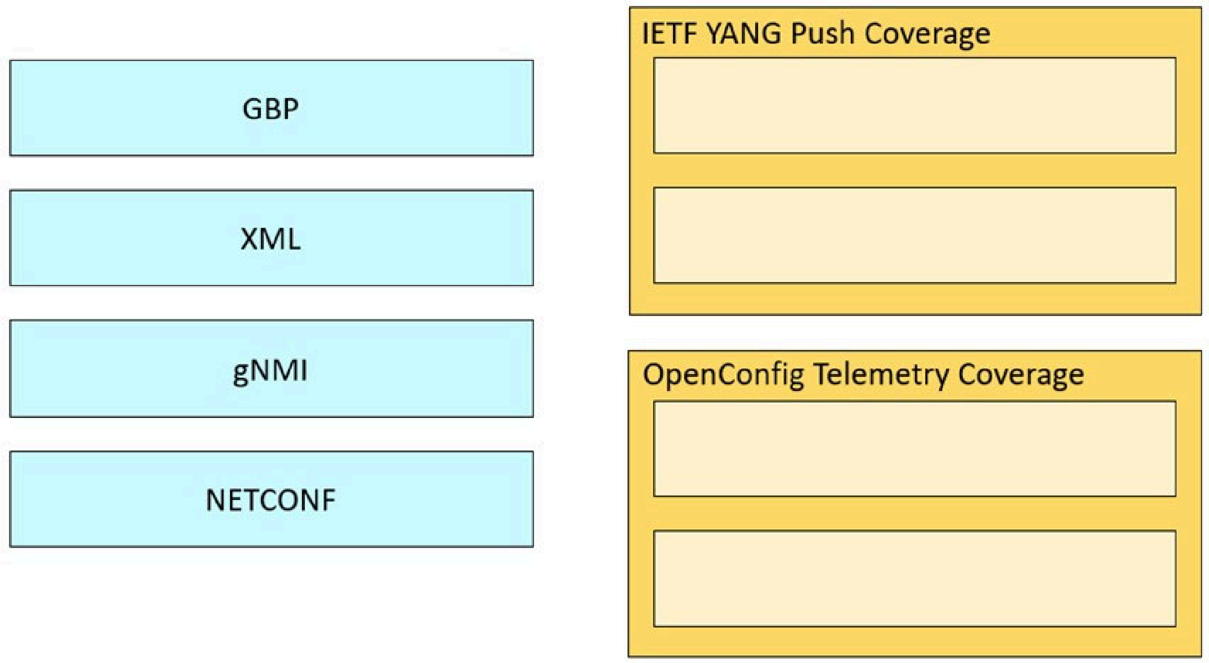
upvoted 7 times

Question #160 *Topic 1*

DRAG DROP -

Drag and drop the elements from the left onto the YANG models where they and used on the right.

Select and Place:



GBP

XML

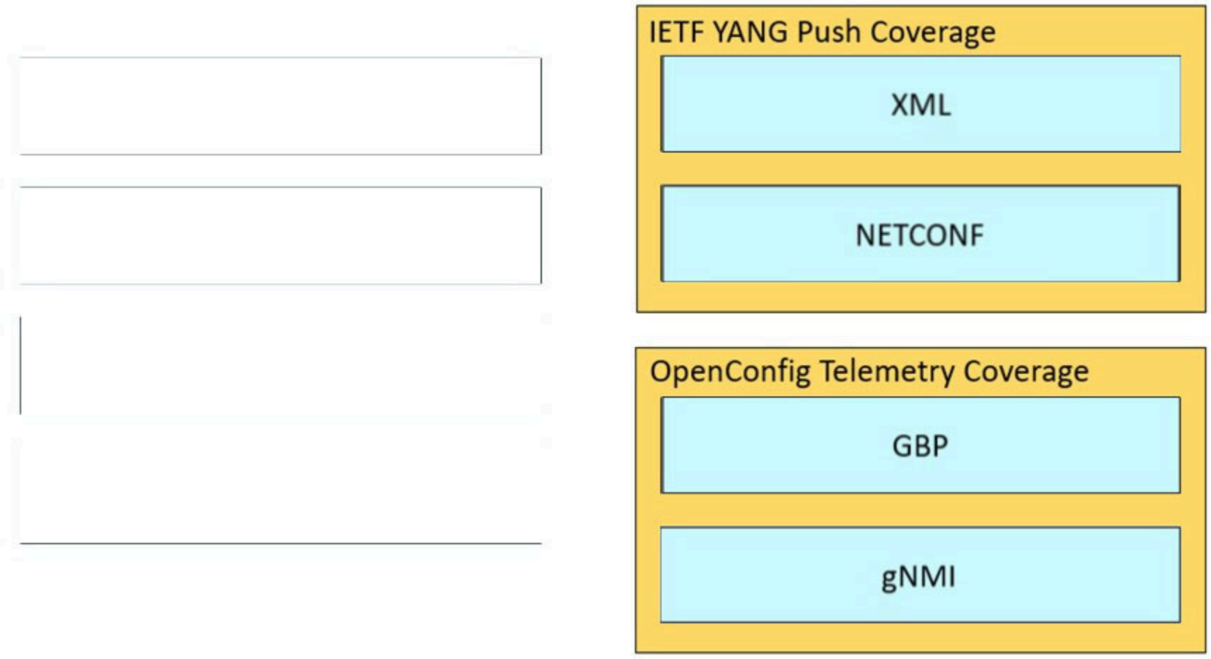
gNMI

NETCONF

IETF YANG Push Coverage

OpenConfig Telemetry Coverage

**Correct Answer:**



IETF YANG Push Coverage

XML

NETCONF

OpenConfig Telemetry Coverage

GBP

gNMI

Currently there are no comments in this discussion, be the first to comment!

Question #161 *Topic 1*

An architect must create a QoS solution for a customer to ensure that a 40 Mbps Internet connection is shared between four subnets based on these requirements:
* Each subnet must receive no less than 10 Mbps of download bandwidth during peak traffic times.
* A subnet can use up to 40 Mbps during nonpeak traffic times if the other subnets are idle.
* Download traffic must never experience a delay.
Which solution must the architect choose?

A. rate-limiting and shaping

B. bandwidth percentage and policing

C. shaping and policing

D. bandwidth percentage and rate-limiting

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**Clauster** 1 year, 6 months ago

**Selected Answer: B**

A - Shaping = Delays
C - Shaping = Delays
D - Rate - Limiting = Delays

Answer B: is the correct answer, you use Bandwidth percentage to each subnet and Policing to cut off traffic. The answer never said we needed to worry about packet loss or packet drops when Link is congested.

upvoted 1 times

**vangio** 1 year, 7 months ago

Correct B

upvoted 1 times

**CKL_SG** 1 year, 9 months ago

**Selected Answer: B**

It cannot be shaping as traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time

It cannot be Rate Limiting as well as it refer to both shaping and policing

What is Rate Limiting? Network rate limiting is used to limit the amount of traffic on a network. There are two main methods of rate limiting: traffic policing and traffic shaping. Traffic policing measures the rate of incoming traffic and drops packets that exceed the maximum allowed rate.

upvoted 4 times

**DOSKIM** 1 year, 11 months ago

It is C

upvoted 1 times

**Sickcnt** 2 years, 4 months ago

**Selected Answer: B**

"Download traffic must never experience a delay."

This means we shouldn't be using Shaping at any point (since that puts packets into a buffer and sends them out later on when congestion has been reduced)

Also: "Rate-limiting" is a bigger term and under it we have 2 things: "Policing" and "Shaping"

So since Rate-limiting also refers to "shaping" we cannot go with that option

B should be the correct answer

upvoted 3 times

⊟ **XalaGyan** 2 years, 1 month ago

This is the key indicator: "So since Rate-limiting also refers to "shaping" we cannot go with that option"

Policing and bandwidth percentage can do bandwidth fixed amount

upvoted 1 times

Question #162 *Topic 1*

An engineer is designing a network for a customer running a wireless network with a common VLAN for all APs. The customer is experiencing unicast flooding in the Layer 2 network between the aggregation and access layers. The customer wants to reduce the flooding and improve convergence time. Which solution meets these requirements?

A. Migrate all APs to a common Layer 2 access layer switch and run Layer 3 from the aggregation layer to all remaining access layer switches.

B. Align HSRP primary and STP root bridges and reduce ARP timers to match CAM timers on the aggregation layer switches.

C. Migrate to a Layer 3 access campus design if the APs can run on separate VLANs.

D. Align HSRP primary and STP root bridges if the APs cannot run on separate VLANs.

**Correct Answer:** *B*

*Community vote distribution*

B (57%) C (43%)

⊟ **Hope66** Highly Voted 👍 3 years, 5 months ago

I think B

The default ARP table aging time is 4 hours while the CAM holds the entries for only 5 minutes. The switch sends out a frame to all forwarding ports within tl respective VLAN when the destination MAC address is aged out from the CAM table. You need a CAM aging timer greater or equal to the ARP timeout in orde prevent unicast flooding.

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/71079-arp-cam-tableissues.html#:~:text=The%20default%20ARP%20table%20aging%20time%20is%204,ARP%20timeout%20in%20order%20to%20prevent%20unicast%20floo

upvoted 15 times

⊟ **rted** 1 year, 8 months ago

But B says "reduce ARP timers to match CAM timers". The flooding will still happen at same interval.

upvoted 2 times

⊟ **adcym** Most Recent ⊙ 1 year, 2 months ago

Selected Answer: B

Answer is B.

upvoted 2 times

⊟ **muffedtrims** 1 year, 4 months ago

Selected Answer: B

Voting B based on Hope66 explanation.

upvoted 1 times

⊟ **Swiz005** 1 year, 6 months ago

Selected Answer: C

Answer is C

upvoted 1 times

⊟ **beskar** 2 years, 7 months ago

Selected Answer: C

L3 Access Layer design will eliminate STP along with providing better convergence times than traditional L2 design.

upvoted 3 times

⊟ **SomKeat** 2 years, 7 months ago

Answer is B

upvoted 1 times

⊟ **CKL_SG** 2 years, 9 months ago

Selected Answer: B

Spanning-tree protocol looping behavior, including blocked links, slow convergence, asymmetric forwarding, and switch CAM and ARP table tuning to address unicast flooding

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

upvoted 1 times

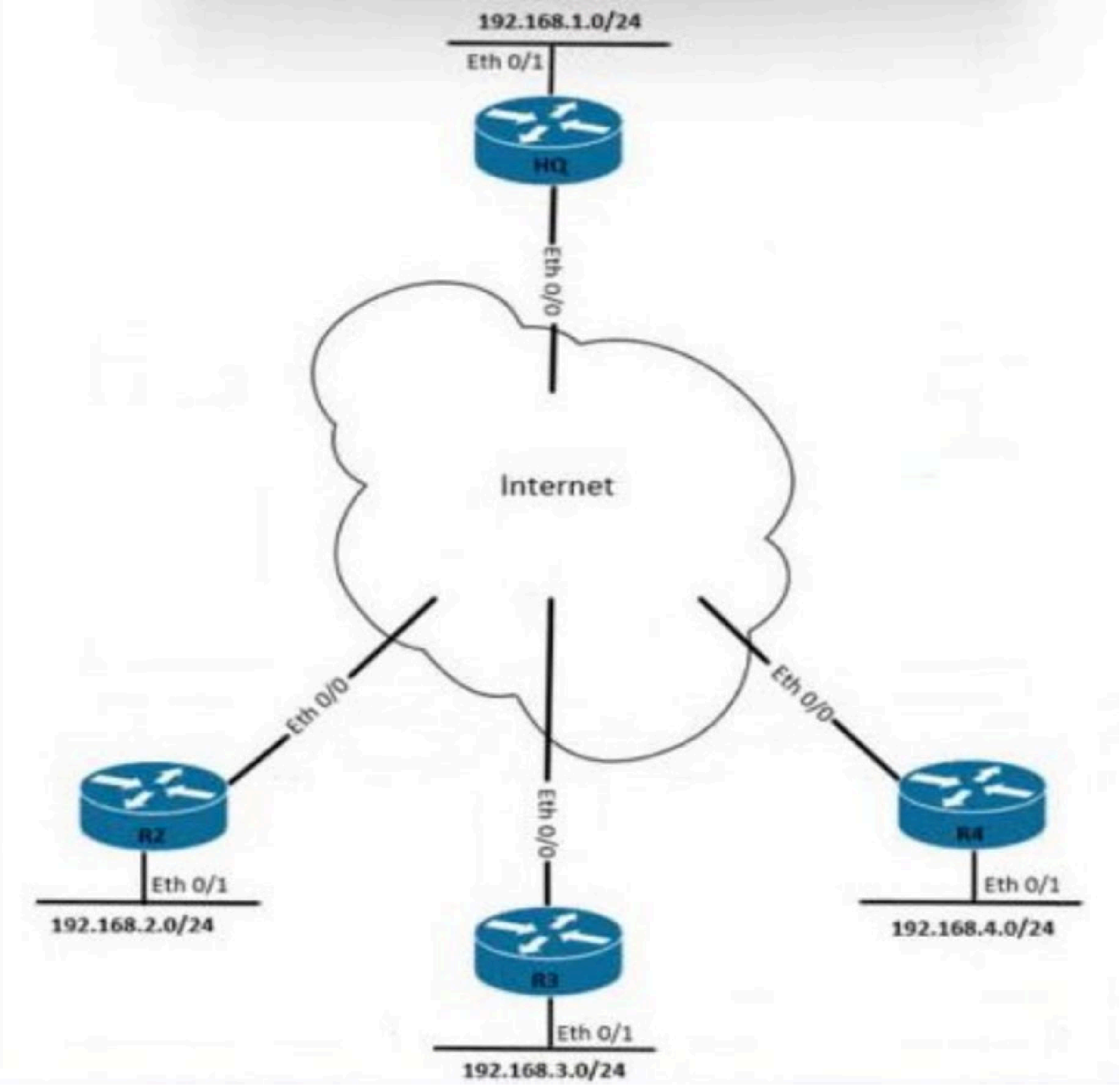
⊟ **XalaGyan** 3 years, 1 month ago

**Selected Answer: B**

Answer B is correct based on explanations provided by Hope66

upvoted 1 times

Question #163 Topic 1



Refer to the exhibit. A customer wants to adopt a dynamic site-to-site VPN solution to secure communication for VoIP, video, and FTP traffic between the remote branches and the headquarters. The customer also wants the branches to communicate directly, thereby reducing traffic at the headquarters location. The solution most consider that the branch routers are limited in available memory. Which VPN solution meets these requirements?

A. DMVPN Phase 2 Hub and Spoke design

B. DMVPN Phase 3 Hub and Spoke design

C. DMVPN Phase 3 Hierarchical design

D. DMVPN Phase 1 Hub and Spoke design

**Correct Answer:** *B*

*Community vote distribution*

B (89%) 11%

mgiuseppe86 1 year, 4 months ago

Selected Answer: B

Why is everyone typing A but no one is voting A?

I agree it should be A as well. It says nothing about requiring additional services and limited memory is a factor. But now I think about it, you will need ospf or EIGRP to route to other spokes. Maybe it is B afterall.

upvoted 1 times

⊟ **J2J2J2J** 1 year, 8 months ago

**Selected Answer: B**

DMVPN Phase 1: All traffic flows through the hub. The hub is used in the network's control and data plane paths.

DMVPN Phase 2: Allows spoke-to-spoke tunnels. Spoke-to-spoke communication does not need the hub in the actual data plane. Spoke-to-spoke tunnels are on-demand based on spoke traffic triggering the tunnel. Routing protocol design limitations exist. The hub is used for the control plane but, unlike phase 1, not necessarily in the data plane.

DMVPN Phase 3: Improves scalability of Phase 2. We can use any Routing Protocol with any setup. "NHRP redirects" and "shortcuts" take care of traffic flows.

upvoted 1 times

⊟ **314_pi** 1 year, 9 months ago

**Selected Answer: B**

DMVPN Phase 3 is the final and most scalable phase in DMVPN as it combines the summarisation benefits of phase 1 with the spoke-to-spoke traffic flows achieved via phase 2.

https://learningnetwork.cisco.com/s/article/dmvpn-concepts-amp-configuration

upvoted 1 times

⊟ **bccabrera** 1 year, 9 months ago

**Selected Answer: A**

A, because the solution most consider that the branch routers are limited in available memory.

upvoted 1 times

⊟ **dgonzalezexamtopics** 1 year, 10 months ago

As I understand, communications must be Spoke2Spoke and slso reduce the overhead due to the lack of memory. Then, L2 DMVPN: S2S routing via NHRP under the hood implies Spoke to Spoke communication al well as reducing traffic overhead. Should not be A?

upvoted 1 times

⊟ **bccabrera** 1 year, 9 months ago

It should be A.

upvoted 1 times

⊟ **jzzmth** 1 year, 11 months ago

**Selected Answer: B**

I'm going wth B.

DMVPN Phase 3 increases scalability of the network by minimizing the amount of routing information that the spokes need to maintain, thus greatly reducing the routing table overhead vs Phase 2...

upvoted 3 times

⊟ **XalaGyan** 2 years, 1 month ago

**Selected Answer: B**

Correct answer is B.

Level 1 - All routing via Hub

Level 2 - Spoke to Spoke Routing via NHRP under the hood

Level 3 - all to all communication with a routing protocol on top.

We have limited resources, therefore i chose to go with A.

Level 2 gets the job done and i dont need an additional memory overhead of routing protocol.

HTH

upvoted 2 times

⊟ **Tasabgd90** 2 years, 1 month ago

Wait, is it A or B then?

upvoted 1 times

⊟ **XalaGyan** 2 years, 1 month ago

Correct answer is B.

Level 1 - All routing via Hub
Level 2 - Spoke to Spoke Routing via NHRP under the hood
Level 3 - all to all communication with a routing protocol on top.

We have limited resources, therefore i chose to go with A.

Level 2 gets the job done and i dont need an additional memory overhead of routing protocol.

HTH
upvoted 2 times

Question #164 *Topic 1*

Which node performs the LISP Map-Server and Map-Resolver functions in the Cisco SD-Access network architecture?

A. control plane node

B. fabric edge node

C. border node

D. intermediate node

**Correct Answer:** *A*

**NoHombre** 5 months, 3 weeks ago

**Selected Answer: A**

From Official Guide Book:

It does this by moving remote destination information to a centralized mapping database called the LISP map server (MS) (a control plane node in SD-Access), which allows each router to manage only its local routes and query the map system to locate destination EIDs.

upvoted 1 times

Question #165 *Topic 1*

An engineer must design a management network that enables SSH, NTP, FTP, and SNMP over the production network. The design requires the management of routers and switches that exist across different networks. Which feature must the design include?

A. Management Plane Protection

B. dedicated management console connection per device

C. terminal server

D. dedicated management VRF connection per device

**Correct Answer:** *D*

**NoHombre** 5 months, 2 weeks ago

**Selected Answer: D**

Provided answer is correct, from OCG:
"One common solution is to use a loopback address for network management, separate from the loopback address used for routing. An in-band solution is not segmented from the primary traffic and address bandwidth usage. One possible way to segment the management traffic is to use a dedicated management VRF and assign the management interface of network devices to this VRF."

upvoted 1 times

Question #166 *Topic 1*

A network engineer must design a multicast solution to prevent the spoofing of multicast streams and ensure efficient bandwidth utilization. The network will be merged with another multicast domain in the future, and the merge must require minimum effort. Which two solutions meet the customer requirements? (Choose two.)

A. PIM-SSM

B. IGMPv3

C. IGMPv2

D. PIM-SM

E. MSDP

**Correct Answer:** *AB*

*Community vote distribution*

AB (53%) DE (40%) 7%

⊟ **jzzmth** Highly Voted 2 years, 5 months ago

**Selected Answer: AB**

I too think it's A and B:

"The ease of installation and operation of SSM makes it ideal for network operators, especially in those cases where content needs to be forwarded between multiple independent PIM domains (because there is no need to manage MSDP for SSM between PIM domains)."

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-ssm.html

And without IGMPv3 you can't setup PIM-SSM

upvoted 5 times

⊟ **NoHombre** Most Recent 5 months, 3 weeks ago

**Selected Answer: AB**

PIM-SSM (Source-Specific Multicast)

Prevents spoofing: Receivers join (S,G), i.e., a specific source and group. Traffic from any other source is ignored, so a rogue sender can't "spoof" the stream.

Efficient bandwidth: No shared tree, no RP, no register encapsulation. Joins go directly to the source (SPT from the start), minimizing unnecessary traffic/state.

Easy future merge: Inter-domain SSM needs only unicast reachability to the source; there's no RP and no MSDP to stitch domains—so merging multicast domains is much simpler.

And IGMPv3 cause it's required for PIM-SSM

upvoted 1 times

⊟ **neiker45** 1 year, 8 months ago

**Selected Answer: AE**

How about A and E. Using PIM-SSM provides us with the spoofing prevention and efficient bandwidth utilization and MSDP provides us with the inter-domain operability that we need after the merge.

upvoted 1 times

⊟ **neiker45** 1 year, 8 months ago

Nevermind, as per Jzzmth's documentation there is no need to manage MSDP for SSM between PIM domains.

upvoted 1 times

⊟ **neiker45** 1 year, 8 months ago

Since MSDP helps with RP information spreading, and SSM doesn't use RPs, it would not work.

upvoted 1 times

**dgonzalezexamtopics** 2 years, 2 months ago

Selected Answer: DE

I would say MSDP for sure and, thus, should be also PIM-SM because of the domains that are interconnected.

upvoted 2 times

**Emily23** 2 years, 2 months ago

It is B & D

upvoted 2 times

**Tasabgd90** 2 years, 7 months ago

Selected Answer: AB

I think it's A and B. Referring to this:

https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/Phase_2/mcst_p2.html

https://www.researchgate.net/publication/221081564_IGMPv3-Based_Method_for_Avoiding_DoS_Attacks_in_Multicast-Enabled_Networks

upvoted 3 times

**andrewChan** 2 years, 10 months ago

Selected Answer: DE

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#GUID-4B201DB3-2C27-4F98-977A-A1AE9DC39C21

MSDP is a mechanism to connect multiple PIM-SM domains. 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 a common shared tree).

upvoted 2 times

**Reinier_veen** 2 years, 10 months ago

Selected Answer: DE

I would opt for MSDP (for interconnecting multiple domains) and PIM-SM (for efficiency in bandwidth)

upvoted 2 times

**Eards** 2 years, 10 months ago

IGMPv3 to prevent spoofing ?

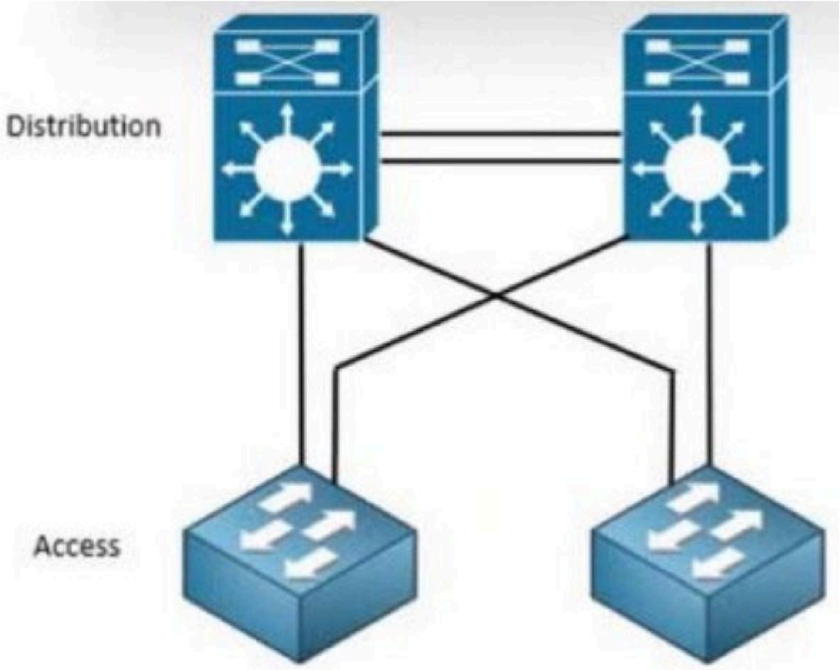
upvoted 2 times

**SirPeter** 2 years ago

YES, IGMPv3 supports SSM, whitch is source specific and thus prevent spoofing of source IP address.

upvoted 1 times

Question #167 Topic 1



Refer to the exhibit. An engineer is designing a Layer 2 campus network. The design must support fast convergence and leverage as much bandwidth as possible between layers. Distribution switches do support VSS; unfortunately, not all routing protocols are available for use due to license limitations. Which solution must the engineer choose?

A. EtherChannel

B. MEC

C. RSTP

D. ECMP

**Correct Answer:** *B*

*Community vote distribution*

B (86%) 14%

**mgiuseppe86** 1 year, 5 months ago

**Selected Answer: B**

Multi-Chassis EtherChannel. With inter-chassis SSO, the total switchover time is within a second and when a chassis fails or during a switchover event, all the links on that chassis go down. External switches that are single-homed into the failed chassis experience an outage. It is recommended to dual-home all connections to the SV pair using MEC technology, which primarily load-balances traffic across links, and keeps the traffic impact minimal in the event of chassis or link failure.

upvoted 2 times

**vangio** 1 year, 7 months ago

Correct B

upvoted 1 times

**J2J2J2J** 1 year, 8 months ago

**Selected Answer: B**

MEC (Multi Chassis Etherchannel)

upvoted 2 times

**andrewChan** 2 years, 4 months ago

**Selected Answer: B**

configure StackWise Virtual on distribution layer and then configure MEC
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html

upvoted 2 times

⊟ **beuzec** 2 years, 4 months ago

For me the answer is A: Etherchannel

upvoted 1 times

⊟ **Sickcnt** 2 years, 4 months ago

Could be but theres a reason they wrote "Distribution switches do support VSS"

So it means we should be doing MEC (Multi Chassis Etherchannel)

Answer B is 100% correct.

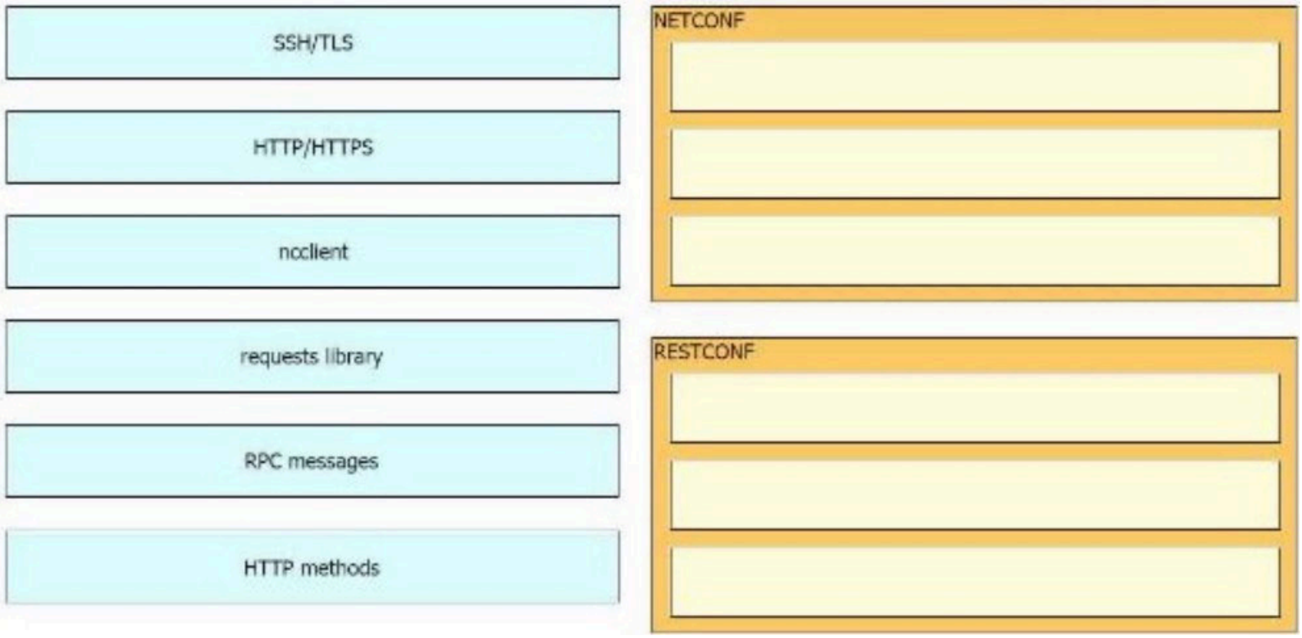
upvoted 2 times

Question #168 *Topic 1*

DRAG DROP -

Drag and drop the elements from the left onto the protocols where they are used on the right.

Select and Place:



SSH/TLS

HTTP/HTTPS

ncclient

requests library

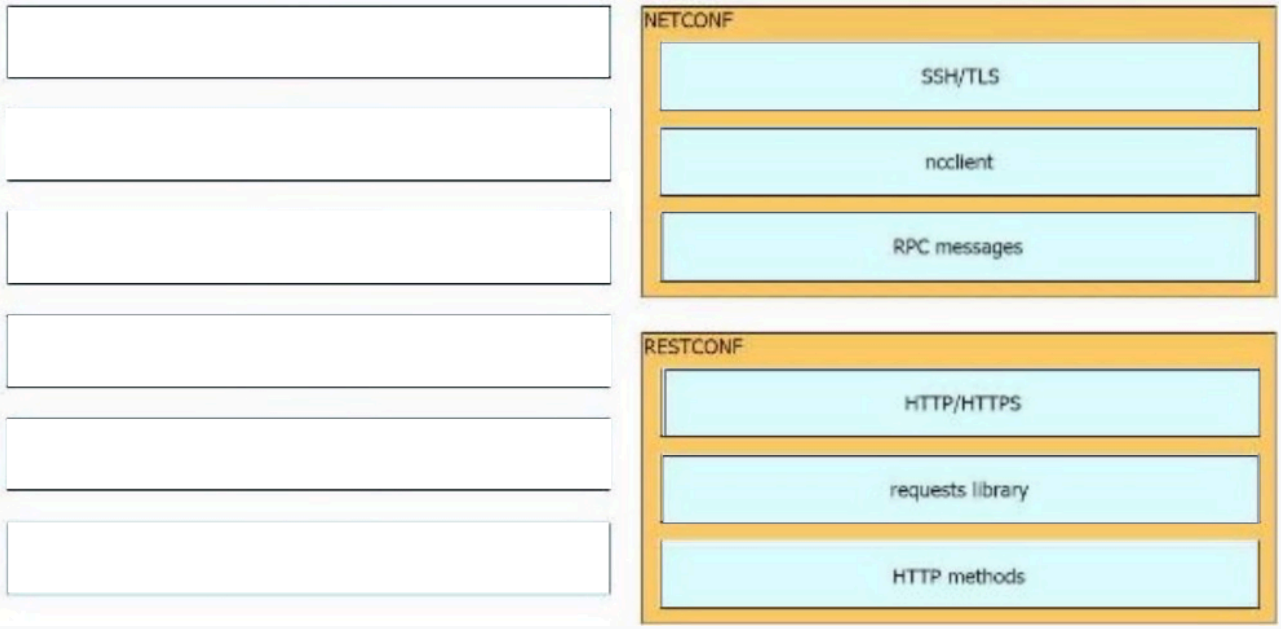
RPC messages

HTTP methods

NETCONF

RESTCONF

**Correct Answer:**



NETCONF

SSH/TLS

ncclient

RPC messages

RESTCONF

HTTP/HTTPS

requests library

HTTP methods

⊟ **StandAlone** 1 year, 4 months ago

ncclient -> Python library ( Use XML to create NetCONF message )

request library -> Python HTTP Library

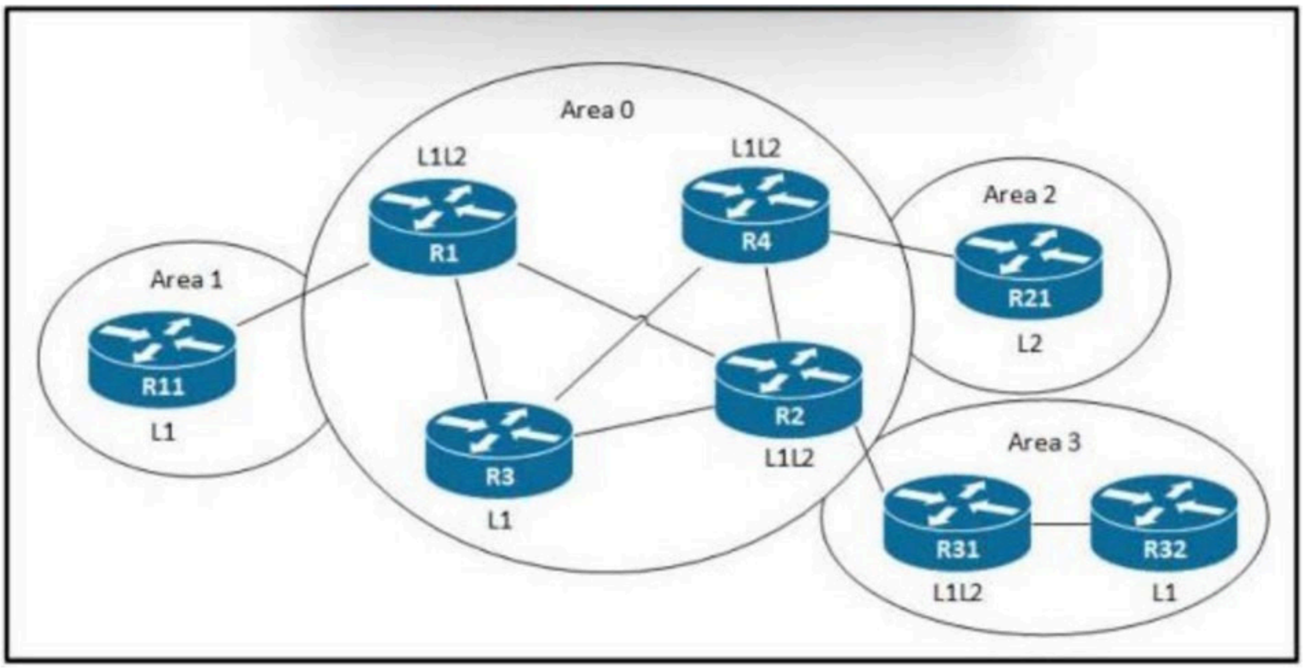
upvoted 1 times

⊟ **Lungful** 2 years ago

The answer is correct.

upvoted 1 times

Question #169 Topic 1



Refer to the exhibit. A customer experienced an unexpected network outage when the link between R1 and R2 went down. An architect must design a solution to ensure network continuity in the event the link tails again. Which solution should the design include?

A. Make R3 an L1L2 router.

B. Make R31 an L1 router.

C. Make Area 0 L2-only.

D. Make R11 an L2 router.

**Correct Answer:** *A*

*Community vote distribution*

A (64%) C (36%)

**mgiuseppe86** 1 year, 5 months ago

How is Area0-R11 forming any adjacency with Area0-R1?

It cant. L1 cannot form adjacency to L1/L2 from another area.

Doing this in a lab, i get

```
*Oct 7 01:00:02.864: ISIS-Adj: Area mismatch, level 1 IIH on GigabitEthernet0/0
*Oct 7 01:00:04.153: ISIS-Adj: Sending L1 LAN IIH on GigabitEthernet0/0, length 1497
*Oct 7 01:00:04.837: ISIS-Adj: Rec L2 IIH from 5254.001e.d934 (GigabitEthernet0/0), cir type L1L2, cir id 0000.0000.0011.01, length 1497, ht(30)
*Oct 7 01:00:04.837: ISIS-Adj: is-type mismatch
```

upvoted 1 times

**Marinheiro** 1 year, 7 months ago

Selected Answer: A

C It's wrong because area 1 would not comunicate with area 0

upvoted 2 times

**314_pi** 1 year, 9 months ago

Selected Answer: A

R11 is L1

upvoted 1 times

**Dyks** 1 year, 10 months ago

Selected Answer: A

You cannot connect an L1 router to a L2 router so converting the entire Area to L2 will cause an issue between R1 and R11. Converting R3 into an L1/L2 provides the right solution.

upvoted 1 times

**dgonzalezexamtopics** 1 year, 10 months ago

Ok, u r right, but then u would be choosing 2 answers. As it to be just one, I would go with A, because it would make R3 a L1L2 router and, consequently, it would have also a L2 domain

upvoted 2 times

**jzzmth** 1 year, 11 months ago

Selected Answer: C

This is a tricky question... because technically answers A and C will both work.

I'm going with answer C because I'm assuming Area 0 here is a backbone area and as such best practice is to make all routers in the backbone area L2 only. Doing this prevents default routes from being propagated and creating sub-optimal routing.

upvoted 2 times

**zzmejce** 2 years, 2 months ago

Selected Answer: C

Area 0 should be L2, R11 should be L2...

upvoted 2 times

**Reinier_veen** 2 years, 4 months ago

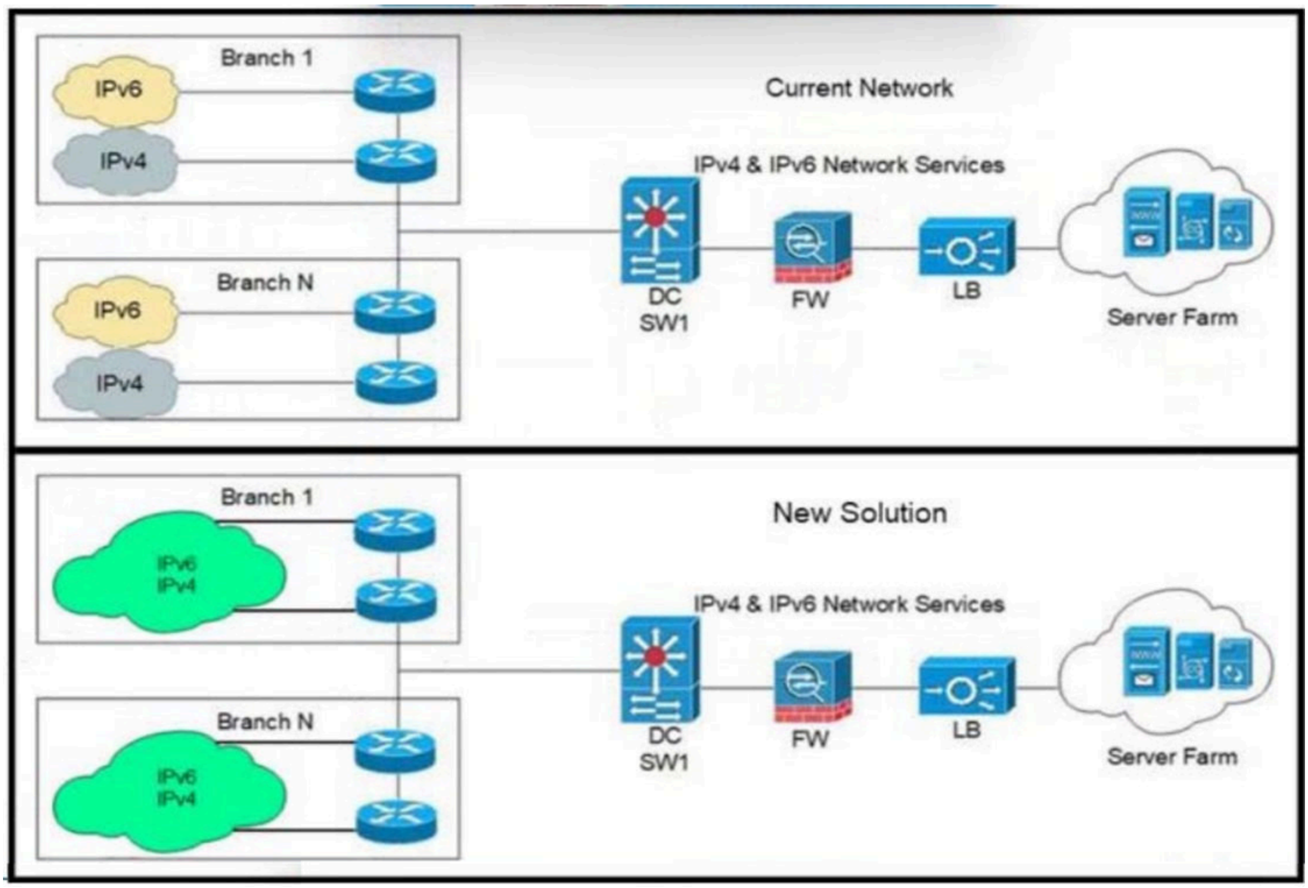
Selected Answer: A

answer is correct.

ENSLD 300-420 cert guide page 117. When creating a backbone there should never be L1 routers between (L2 only, or) L1/L2 routers.

upvoted 4 times

Question #170 *Topic 1*



Refer to the exhibit. An architect is developing a solution to consolidate networks while retaining device redundancy. The routing protocol for the WAN routers must be open standard, ensure high availability, and provide the fastest convergence time. Which solution must the design include?

A. both routers running EIGRP

B. one router running OSPFv2 and other OSPF v3

C. one router running ISIS and other OSPF v3

D. both routers running OSPFv2

**Correct Answer:** *A*

*Community vote distribution*

A (75%) B (25%)

**Sickcnt** Highly Voted 3 years, 4 months ago

**Selected Answer: A**

EIGRP is an open standard protocol for years now,

Also If we go with Answer B -> How could we guarantee "High availability" of one router is running OSPFv2 (for IPv4) and one running OSPFv3 (for IPv6)
... If one router failes (for example the OSPFv2 one) -> Then the IPv4 traffic would have to go through the OSPFv3 router, but since that is not configured up for IPv4 it would drop the packets.

EIGRP has a function called "EIGRP Ipv6" (But that can still be called "EIGRP")
So I guess it should be Answer A

But shame on Cisco for asking bad questions like these...
Its not about knowing the answer, its about seeing into the guys head who wrote the question and try to guess his thoughts.

upvoted 7 times

**79dbffe** Most Recent 1 month, 3 weeks ago

Selected Answer: A

Wanna feel old?

EIGRP has been an open standard for about 10 years now.

upvoted 1 times

**244afa3** 1 year, 7 months ago

eigrp is not open standard. so the realistic solution should be using both ospfv2 and ospfv3 on all routers.

upvoted 1 times

**salmarin** 2 years, 1 month ago

option E , both routers running OSPFV3.

upvoted 2 times

**mgiuseppe86** 2 years, 4 months ago

Idk man this question sucks. Coming back to it a month later I still don't know the answer.

Open standard: could mean OSPF or EIGRP

High availability: we are only using a single router per IP space. hA doesn't apply here

Fastest convergence: what convergence are we covering? There is only one router. If the ipv4 router goes down, goodnight. Same with ipv6. There is nothing to converge.

Furthermore, "both routers running EIGRP" is an unfair answer. "both routers running OSPF" should then also be an answer.

Yes opsfv3 is synonymous with ipv6 and EIGRP doesn't contain that nomenclature

But this is all so ridiculous. The word games in this question and answers takes away from the fundamentals of a network engineer. We shouldn't be tested on how well we can understand Cisco English.

upvoted 2 times

**mgiuseppe86** 2 years, 5 months ago

Selected Answer: A

No 3rd party vendor is going to support EIGRP on their network. what a dumb question. This is a marketing question and not a real-world question. Because of that, I am regretfully going with A, because Cisco is trying to market EIGRP now as Open. but we all know the real world answer is B.

upvoted 1 times

**Clauster** 2 years, 6 months ago

Selected Answer: B

The Answer is B.

EIGRP is an open standard and it it provides faster convergence times than OSPF, HOWEVER, the term EIGRP is meant to be for IPv4 and in this case we need EIGRP for IPv6, unfortunately i don't see an option in the answers that say EIGRP for IPv6, the book explains this a lot, the safer answer is OSPFv2 for IPv4 and OSPFv3 which handles IPv6

upvoted 2 times

> **mgiuseppe86** 2 years, 5 months ago
>
> What crack have you smoked lately? EIGRP is Cisco proprietary.
>
> upvoted 1 times
>
> > **TheGorn** 2 years, 2 months ago
> >
> > https://networklessons.com/eigrp/introduction-to-eigrp#:~:text=EIGRP%20stands%20for%20Enhanced%20Interior,it's%20now%20an%20open%20standard.
> >
> > upvoted 1 times

**Clauster** 2 years, 7 months ago

Selected Answer: B

B is correct for me.

It would of Specified EIGRP for IPv6 and it did not in the answers, i cannot accept A as the correct answer.

upvoted 1 times

**andrewChan** 3 years, 4 months ago

Selected Answer: A