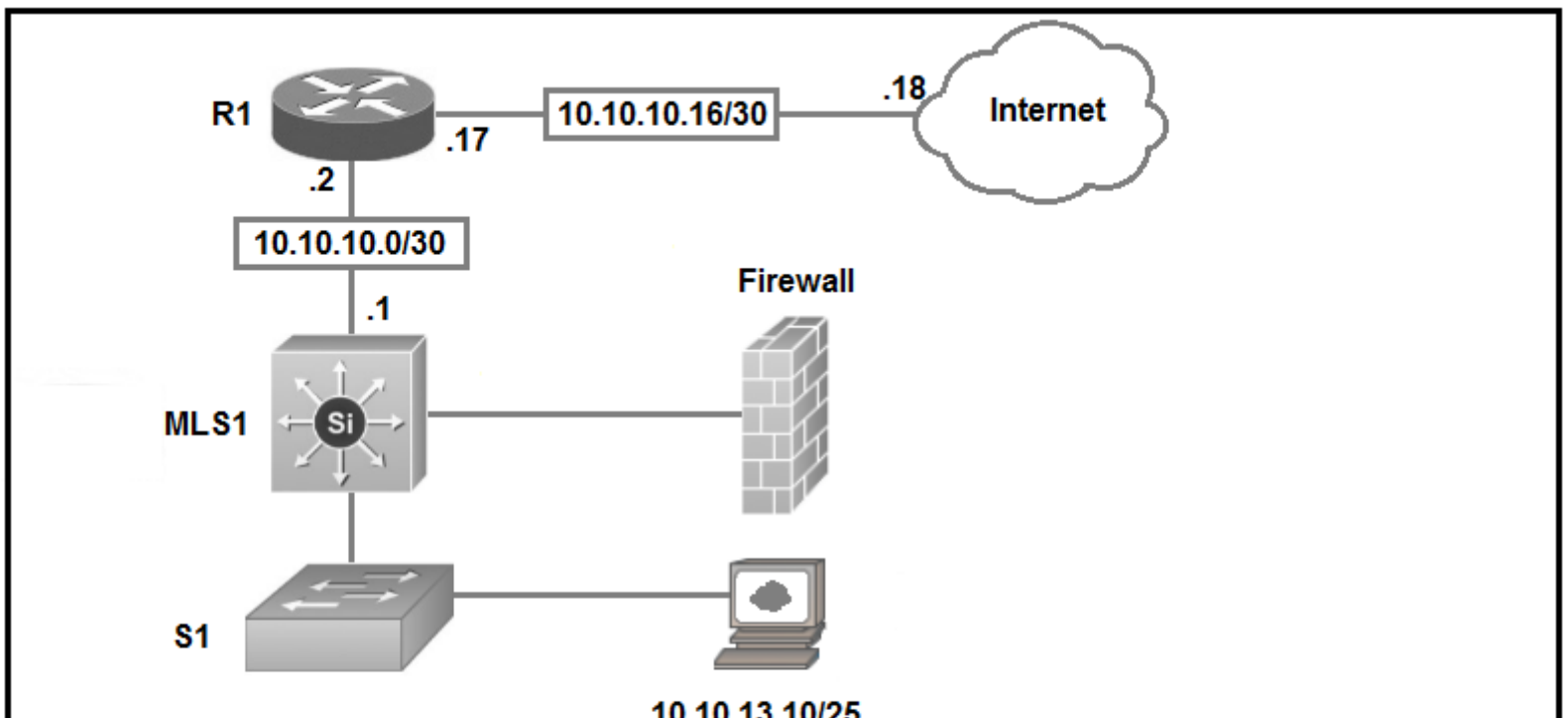
Topic 1 - Single Topic

Question #1 *Topic 1*




```
R1#sh ip ro
Gateway of last resort is 10.10.10.18 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C          10.10.10.0/30 is directly connected, FastEthernet0/1
O          10.10.13.0/25 [110/6576] via 10.10.10.1, 06:58:21, FastEthernet0/1
C          10.10.10.16/30 is directly connected, FastEthernet0/24
O          10.10.13.144/28 [110/110] via 10.10.10.1, 06:58:21, FastEthernet0/1
B*   0.0.0.0/0 [20/0] via 10.10.10.18, 01:17:58
```

Refer to the exhibit. Which type of route does R1 use to reach host 10.10.13.10/32?

A. default route

B. network route

C. host route

D. floating static route

Correct Answer: *B*

Community vote distribution

B (95%) 5%

LOST40 Highly Voted 1 year, 6 months ago

I passed my CCNA. Strangely, they don't show you your scores right away. I got that Credly badge and print out version of the cert. Some of the questions came from here and some were extremely different. So study really really hard.

upvoted 20 times

GreatDane Highly Voted 8 months, 3 weeks ago

Selected Answer: B

A. default route

The default route is 0.0.0.0/0, it is used to reach all destinations not included in the routing table. But the router already has a route to 10.10.13.10/32. The default route is not needed.
Wrong answer.

B. network route

The routing table includes a route to 10.10.13.0/25. This subnet has these characteristics:

7 bits in the host ID = (2^7 – 2) = 126 IP addresses
1st IP address = 10.10.13.1
Last IP address = 10.10.13.126

This route includes address 10.10.13.10 and is an OSPF route (see the leading O).
Correct answer.

C. host route

There's no host route in the routing table.
Wrong answer.

D. floating static route

A floating static route is used as a "backup" route to reach a subnet when the "main" route fails. But here the route to the host's subnet is already in the routing table, and it is working.
Wrong answer.

upvoted 18 times

Calladot Most Recent 2 days, 1 hour ago

Selected Answer: B

++++++++

upvoted 1 times

S089765 4 days, 2 hours ago

Selected Answer: B

Network

upvoted 1 times

gerardop 2 weeks, 2 days ago

Selected Answer: B

The host to reach is in the network 10.10.13.10/32 it means from 10.10.13.8 to 10.10.13.11 the accurate route shown in the table is 10.10.13.10/25 it means from 10.10.13.0 to 10.10.13.127 that includes 10.10.13.10/32

upvoted 1 times

ziyod2005 1 month ago

Selected Answer: B

It is not a floating route, because floating route is a route, which is not visible in routing table, if there are other routes to the same destination and lower AD. And, it is not a host route, because host route has a 32 bit network mask. And it is not a default route, because it's default route's destination address is not the same. Finally, there is the last answer - network route.

upvoted 1 times

Elther 1 month, 1 week ago

Selected Answer: B

Answer is B

upvoted 1 times

Justbewise 2 months, 2 weeks ago

The selected answer is B. The network is advertised in the routing table

upvoted 1 times

Humble1982 3 months, 1 week ago

B. Network route

upvoted 1 times

Hope_12 4 months, 2 weeks ago

Selected Answer: B

B. 10.10.13.0/25 From OSPF route(network route)
inc = 128
10.10.13.0 - 10.10.13.128 is in range for 10.10.13.10/32

upvoted 2 times

Mgardini 4 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

zeromoves 6 months, 3 weeks ago

Great!

upvoted 1 times

[Removed] 7 months, 3 weeks ago

Selected Answer: B

I think the answer is B

upvoted 1 times

rapide 9 months ago

How can i download in pdf ?

upvoted 1 times

rachidi07 7 months ago

by taking contributor access plan
upvoted 1 times

Request7108 9 months ago

Selected Answer: B

By process of elimination, the answer must be B, although I think the PC diagram with the /25 might be confusing some people.
The default route given is 10.10.10.18 for any traffic not matching a known route and the host 10.10.13.10/32 is known, therefore it cannot be A.
It cannot be C because there are no /32, single hosts in the table
It cannot be D because a floating static route is used for higher administrative distances are none are present in this scenario.
upvoted 2 times

javachip 9 months, 2 weeks ago

Selected Answer: B

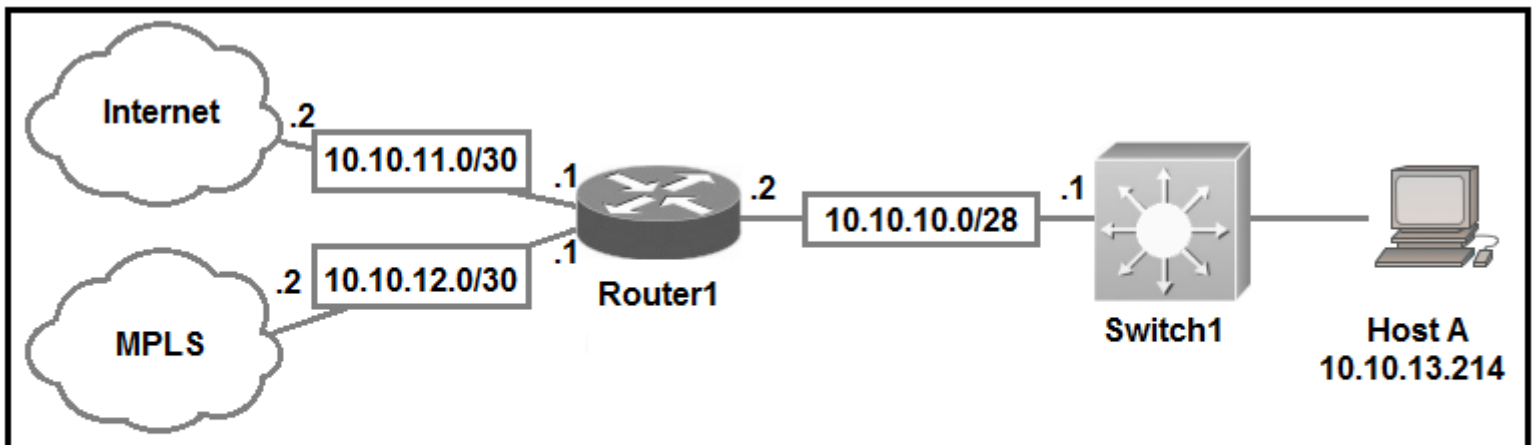
network is keyword
upvoted 1 times

cristip 10 months ago

Selected Answer: B

correct
upvoted 2 times

Question #2 *Topic 1*




```
Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0

      209.165.200.0/27 is subnetted, 1 subnets
B        209.165.200.224 [20/0] via 10.10.12.2, 03:22:14
      209.165.201.0/27 is subnetted, 1 subnets
B        209.165.201.0 [20/0] via 10.10.12.2, 02:26:33
      209.165.202.0/27 is subnetted, 1 subnets
B        209.165.202.128 [20/0] via 10.10.12.2, 02:26:03
      10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C        10.10.10.0/28 is directly connected, GigabitEthernet0/0
C        10.10.11.0/30 is directly connected, FastEthernet2/0
C        10.10.12.0/30 is directly connected, GigabitEthernet0/1
O        10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.128/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.144/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.160/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.208/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
S*    0.0.0.0/0 [1/0] via 10.10.11.2
```

Refer to the exhibit. Which prefix does Router1 use for traffic to Host A?

A. 10.10.10.0/28

B. 10.10.13.0/25

C. 10.10.13.144/28

D. 10.10.13.208/29

Correct Answer: *D*

The prefix with ג€longest prefixג€ will be matched first, in this case is ג29/€ג€.

Community vote distribution

D (100%)

mikachuu85 Highly Voted 1 year, 8 months ago

10.10.13.208/29 gives .208 for network, hmin 209, hmax 214, bcast 215. The correct answer will be D as this route gives the correct range.

upvoted 12 times

ZUMY Highly Voted 2 years, 5 months ago

D is correct:
*Router selects longest Prefix path from routing table.

upvoted 9 times

ZUMY 9 months, 3 weeks ago

It's a trick question but the obvious answer is D. In order to reach Host A, you need to be in its network.

upvoted 1 times

S089765 Most Recent 4 days, 2 hours ago

Selected Answer: D

D fall in range

upvoted 1 times

ziyod2005 1 month ago

Selected Answer: D

10.10.13.214 IPv4 address belongs to the 10.10.13.208/29 subnet and router will choose this one as the best route

upvoted 1 times

Hope_12 4 months, 2 weeks ago

Selected Answer: D

D.10.10.13.208/29
Host A = 10.10.13.214
10.10.13.208 has inc of 8 from /29 with highest subnet mask(Longest Prefix)
10.10.13.208 - 10.10.13.216 is in range for 10.10.13.214

upvoted 2 times

Mgardini 4 months, 3 weeks ago

Selected Answer: D

Answer is D

Due to Longest Prefix path

upvoted 1 times

GreatDane 8 months, 3 weeks ago

Selected Answer: D

Inside Router1's routing table, there are no host routes (/32 routes) leading directly to Host A. So, Router1 will use the route to the most specific subnet which includes Host A's IP address. That is, it will use the route with the longest prefix.

A. 10.10.10.0/28

This subnet includes IP addresses from 10.10.10.1 to 10.10.10.14.
Host A's IP address is not included.
Wrong answer.

B. 10.10.13.0/25

This subnet includes IP addresses from 10.10.13.1 to 10.10.13.126.
Host A's IP address is not included.
Wrong answer.

C. 10.10.13.144/28

This subnet includes IP addresses from 10.10.13.145 to 10.10.13.158.
Host A's IP address is not included.
Wrong answer.

D. 10.10.13.208/29

This subnet includes IP addresses from 10.10.13.209 to 10.10.13.214.
Host A's IP address is included.
Correct answer.

upvoted 5 times

Request7108 9 months ago

D is the correct answer because it is the most specific path with a match for the host. Other folks have mentioned the "longest prefix" but I prefer calling it the "most specific" path

upvoted 2 times

remoto 9 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

javachip 9 months, 2 weeks ago

Selected Answer: D

router selects longest prefix path

upvoted 1 times

NetworkRookie 10 months, 2 weeks ago

Selected Answer: D

Router selects longest Prefix path from routing table.

upvoted 1 times

keokkeo_123 11 months ago

Selected Answer: D

is correct

upvoted 1 times

nyasalandi123 1 year, 1 month ago

D is correct as it is in the same network range

upvoted 1 times

Chiefthings 1 year, 3 months ago

It's a trick question but the obvious answer is D. In order to reach Host A, you need to be in its network.

upvoted 3 times

aosroyal 1 year, 5 months ago

Selected Answer: D

correct

upvoted 1 times

Samir_123 1 year, 7 months ago

Selected Answer: D

correct

upvoted 2 times

vira5489 1 year, 9 months ago

Selected Answer: D

correct

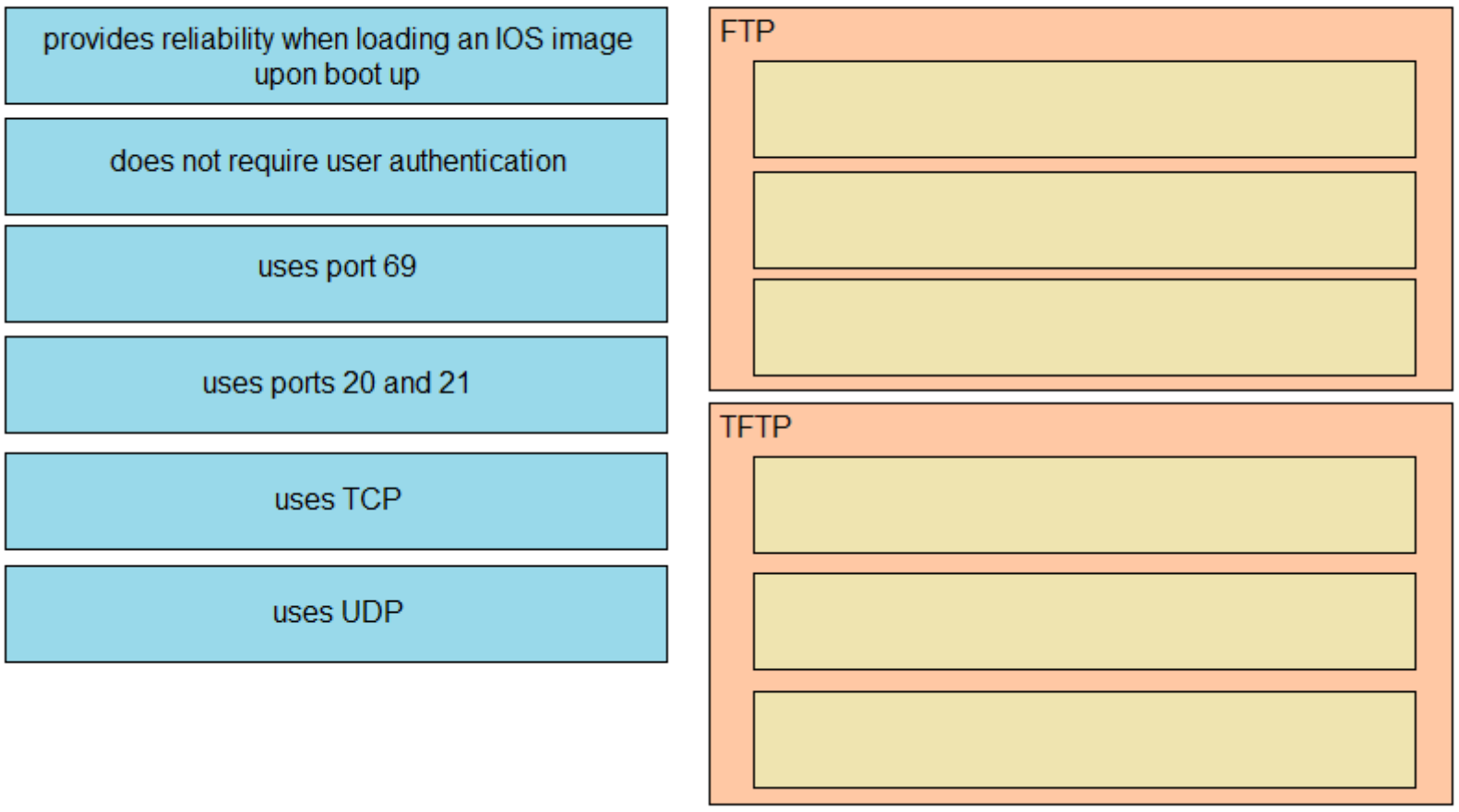
upvoted 3 times

DRAG DROP -

Drag and drop the descriptions of file-transfer protocols from the left onto the correct protocols on the right.

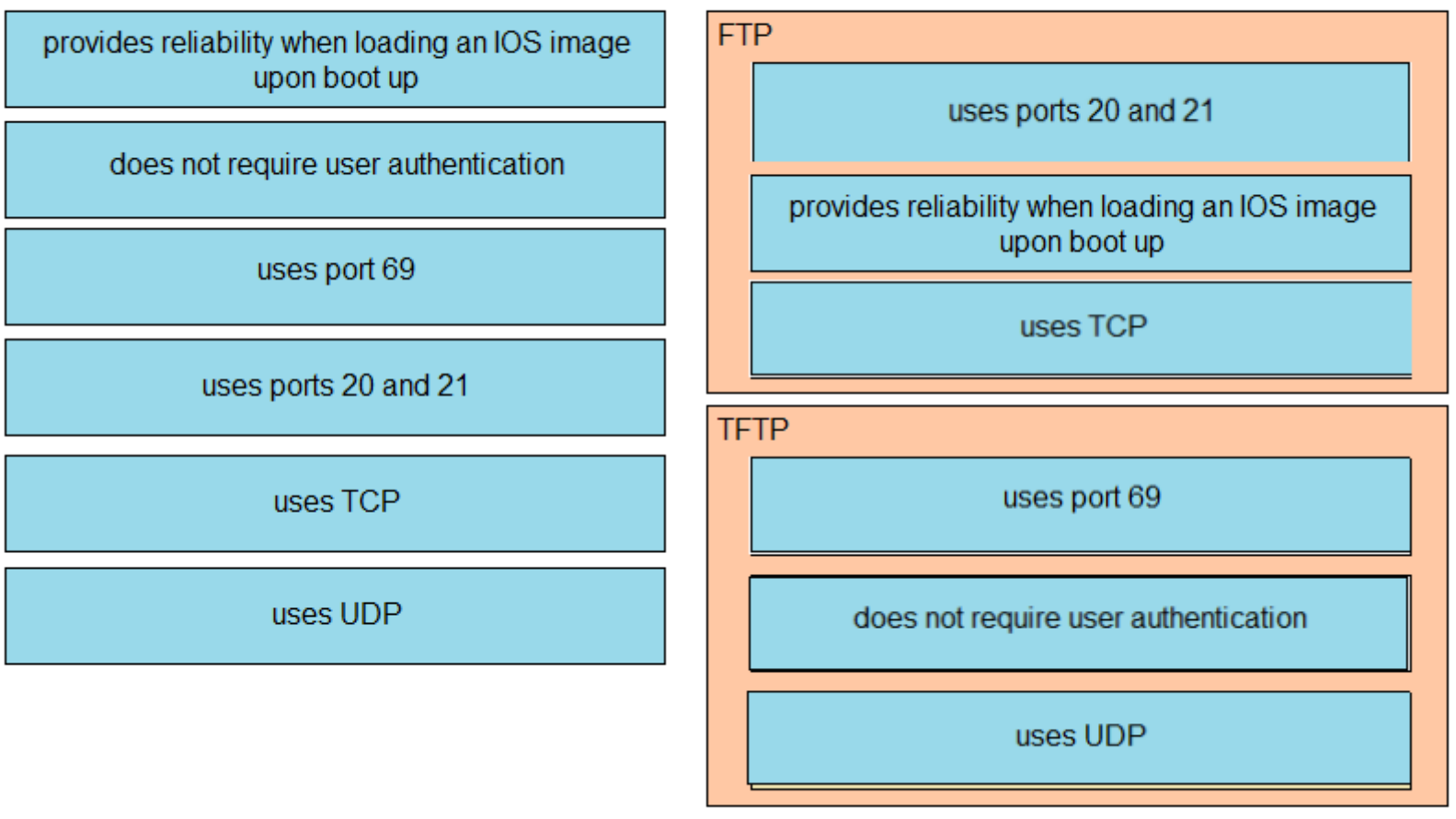
Select and Place:

Answer Area



Correct Answer:

Answer Area



Ali526 Highly Voted 2 years, 8 months ago

Correct.

upvoted 10 times

Request7108 Highly Voted 9 months ago

The current ordering is incorrect. The correct answers are:
FTP uses ports 20 and 21 over TCP by default and is more reliable for loading IOS images
TFTP uses port 69 and UDP by default and does not require user credentials

TFTP is aptly named for being trivial to configure and use. It is less reliable and you may often see failures or bad hashes when loading files or images instead of using FTP.

upvoted 7 times

ac89l 4 months ago

Drink coffee my friend

upvoted 3 times

GreatDane Most Recent 2 months, 2 weeks ago

Ref: Cisco IOS Cookbook, 2nd Edition (O'Reilly)

"...
Discussion
Several recipes in this chapter have shown how to transfer files between your router and server by using TFTP. However, Cisco routers also support FTP. We find that FTP is better suited for transferring files over busy and congested links. While TFTP file transfers tend to abort if they encounter persistent congestion, FTP appears to be more resilient.

FTP is also somewhat more secure than TFTP because it uses usernames and passwords. TFTP has no user-level security features.
..."

Ref: Difference between FTP and TFTP - GeeksforGeeks

"...
FTP stands for File Transfer Protocol.
...
FTP works on two ports: 20 and 21 One for data and another is for connection control.
...
TFTP stands for Trivial File Transfer Protocol.
...
TFTP works on 69 Port number and its service is provided by UDP.
..."

upvoted 1 times

SamuelSami 11 months, 2 weeks ago

https://slidetodoc.com/ftp-file-transfer-protocol-tftp-trivial-ftp-cisc-2/

upvoted 2 times

Rramos37 1 year, 11 months ago

Y como sabe el software si están o no en orden las respuestas?... Creo que lo importante es la respuesta o respuestas y no el orden de las mismas

upvoted 1 times

Apmgoqi 2 years ago

Answers are incorrect! ND: the Answers has to be in the correct order otherwise the system will mark you incorrect

upvoted 3 times

Jay2782 2 years ago

Do the answers have to be in a specific order to be considered correct?

upvoted 1 times

ZUMY 2 years, 5 months ago

Correct Answer

upvoted 4 times

Question #4 *Topic 1*

A frame that enters a switch fails the Frame Check Sequence. Which two interface counters are incremented? (Choose two.)

A. input errors

B. frame

C. giants

D. CRC

E. runts

Correct Answer: *AD*
Whenever the physical transmission has problems, the receiving device might receive a frame whose bits have changed values. These frames do not pass the error detection logic as implemented in the FCS field in the Ethernet trailer. The receiving device discards the frame and counts it as some kind of input error.
Cisco switches list this error as a CRC error. Cyclic redundancy check (CRC) is a term related to how the FCS math detects an error.
The ג€input errorsג€ includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
The output below show the interface counters with the ג€show interface s0/0/0ג€ command:

```
Router#show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is M4T
  Description: Link to R2
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  --output omitted--
  5 minute output rate 0 bits/sec, 0 packets/sec
     268 packets input, 24889 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     251 packets output, 23498 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Community vote distribution

AD (100%)

DatBroNZ Highly Voted 1 year, 6 months ago
input errors: total of many counters, including all below
frame: Frames on illegal format. Can be caused by collisions
giants: Frames that exceeded the maximum size (1518 bytes)
CRC: Received frames that did not pass the FCS math
runts: Frames that did not meet the minimum size (64 bytes). Can be caused by collisions
Therefore CRC and INPUT ERRORS will be increased.
upvoted 13 times

ZUMY Highly Voted 2 years, 5 months ago
A,D is correct.
upvoted 11 times

kilticespi Most Recent 4 months, 3 weeks ago
It is correct
upvoted 2 times

kilticespi 4 months, 3 weeks ago
It is correct
upvoted 1 times

jonathan126 4 months, 3 weeks ago
A and D is correct
upvoted 1 times

diegoherreras 6 months, 3 weeks ago
Selected Answer: AD
opciones a y d
upvoted 1 times

JORGED 7 months, 2 weeks ago

A,D options

upvoted 1 times

GreatDane 8 months, 3 weeks ago

Selected Answer: AD

Ref: Understand Cyclic Redundancy Check Errors on Nexus Switches - Cisco

"...
CRC Error Definition
...
Host-B will usually increment some sort of error counter on its Network Interface Card (NIC) as well, such as the "input errors", "CRC errors", or "RX errors" counters.
..."

A. input errors

Correct answer.

B. frame

Wrong answer.

C. giants

Wrong answer.

D. CRC

Correct answer.

E. runts

Wrong answer.

upvoted 1 times

NetStef 9 months ago

Selected Answer: AD

A,D is correct.

upvoted 1 times

NetworkRookie 10 months, 2 weeks ago

Selected Answer: AD

A,D is correct.

upvoted 2 times

aosroyal 1 year, 5 months ago

Selected Answer: AD

correct

upvoted 2 times

Bigc0ck 1 year, 7 months ago

Input Errors and Cycle Redundancy Check (CRC)
CRC errors mean that the frames didn't match what the Frame Check Sequence (FCS) says they should be.

This is where it might throw people off with input errors.

Description of input errors from Cisco
Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input error count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.

upvoted 1 times

ZUMY 2 years, 5 months ago

Switch port status
*Runts
*Gaint
*Input errors
*CRC
*Output errors
*Frame

upvoted 2 times

Question #5 *Topic 1*

DRAG DROP -

Drag and drop the IPv4 network subnets from the left onto the correct usable host ranges on the right.

Select and Place:

Answer Area

172.28.228.144/18	172.28.228.1 - 172.28.229.254
172.28.228.144/21	172.28.224.1 - 172.28.231.254
172.28.228.144/23	172.28.228.129 - 172.28.228.254
172.28.228.144/25	172.28.228.145 - 172.28.228.150
172.28.228.144/29	172.28.192.1 - 172.28.255.254

Correct Answer:

Answer Area

172.28.228.144/18	172.28.228.144/23
172.28.228.144/21	172.28.228.144/21
172.28.228.144/23	172.28.228.144/25
172.28.228.144/25	172.28.228.144/29
172.28.228.144/29	172.28.228.144/18

This subnet question requires us to grasp how to subnet very well. To quickly find out the subnet range, we have to find out the increment and the network address of each subnet. Let's take an example with the subnet 172.28.228.144/18:

From the /18 (= 1100 0000 in the 3rd octet), we find out the increment is 64. Therefore the network address of this subnet must be the greatest multiple of the increment but not greater than the value in the 3rd octet (228). We can find out the 3rd octet of the network address is 192 (because 192 = 64 * 3 and 192 < 228) -

> The network address is 172.28.192.0. So the first usable host should be 172.28.192.1 and it matches with the 5th answer on the right. In this case we don't need to calculate the broadcast address because we found the correct answer.

Let's take another example with subnet 172.28.228.144/23 -> The increment is 2 (as /23 = 1111 1110 in 3rd octet) -> The 3rd octet of the network address is 228

(because 228 is the multiply of 2 and equal to the 3rd octet) -> The network address is 172.28.228.0 -> The first usable host is 172.28.228.1. It is not necessary but if we want to find out the broadcast address of this subnet, we can find out the next network address, which is 172.28.(228 + the increment number).0 or

172.28.230.0 then reduce 1 bit -> 172.28.229.255 is the broadcast address of our subnet. Therefore the last usable host is 172.28.229.254.

freeknowledge123 Highly Voted 8 months, 2 weeks ago

when faced with this kind of questions, it's best not to waste time calculate the IP range of each subnet, but simply know that the smaller the mask the longer the range will be, so for example /18 will have the biggest range.

upvoted 27 times

paniaguavo Highly Voted 1 year ago

Subnet / Usable IPs
172.28.228.144/18 - 172.28.192.1 - 172.28.255.254

172.28.228.144/21 - 172.28.224.1 - 172.28.231.254

172.28.228.144/23 - 172.28.228.1 - 172.28.229.254

172.28.228.144/25 - 172.28.228.129 - 172.28.228.254

172.28.228.144/29 - 172.28.228.145 - 172.28.228.150

upvoted 12 times

StingVN Most Recent 2 months, 2 weeks ago

172.28.228.144/18: 172.28.192.1. – 172.28.255.254
172.28.228.144/21: 172.28.224.1 – 172.28.231.254
172.28.228.144/23 : 172.28.228.1 – 172.28.229.254
172.28.228.144/25 : 172.28.228.129 – 172.28.228.254
172.28.228.144/29 : 172.28.228.145 - 172.28.228.150

upvoted 1 times

GreatDane 2 months, 2 weeks ago

Do it like a router would:

1.
IP 172.28.228.144 -> 10101100.00011100.11 100100.10010000
Mask 255.255.192.0 -> 11111111.11111111.11 000000.00000000

2.
"Logical AND" between IP and Mask:

10101100.00011100.11 100100.10010000
11111111.11111111.11 000000.00000000

Result:

10101100.00011100.11 000000.00000000

172.28.192.0 -> Network ID

3.
1st usable IP address = Network ID + 1:

10101100.00011100.11 000000.00000000 +
00000000.00000000.00 000000.00000001 =
10101100.00011100.11 000000.00000001 -> 172.28.192.1

4.
Broadcast address = Net ID + all Host ID bits to 1:

10101100.00011100.11 111111.11111111 =
172.28.255.255 -> broadcast address

5. Last usable IP = broadcast address - 1:

10101100.00011100.11 111111.11111111 -
00000000.00000000.00 000000.00000001 =
10101100.00011100.11 111111.11111110 - > 172.28.255.254

Do the same for the other IPs/masks.

upvoted 1 times

Zafferano 5 months ago

D R
1 = 5 2 = 2 3 = 1 4 = 3 5 = 4

upvoted 1 times

Garfieldcat 10 months, 3 weeks ago

The question is somehow misleading. On the left hand side, those IP are addresses instead of subnet numbers.

upvoted 3 times

Request7108 9 months ago

It is poorly worded and should be what network range would be if it were in a /18, /21, etc. For example, if 172.28.228.144 were an IP in a classful /21, what would the usable network range be and the answer would be 172.28.224.1-172.28.231.254

upvoted 1 times

Question #6 *Topic 1*

How do TCP and UDP differ in the way that they establish a connection between two endpoints?

A. TCP uses the three-way handshake, and UDP does not guarantee message delivery.

B. TCP uses synchronization packets, and UDP uses acknowledgment packets.

C. UDP provides reliable message transfer, and TCP is a connectionless protocol.

D. UDP uses SYN, SYN ACK, and FIN bits in the frame header while TCP uses SYN, SYN ACK, and ACK bits.

Correct Answer: *A*

Community vote distribution

A (100%)

ZUMY Highly Voted 2 years, 5 months ago

A is correct

upvoted 9 times

Hanagaki_Shinjiro Most Recent 2 weeks, 3 days ago

Definitely A

upvoted 1 times

tester_20252 2 months, 1 week ago

A is correct

upvoted 1 times

Mgardini 4 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

Zafferano 5 months ago

La risposta corretta è A. TCP utilizza l'handshake a tre vie e UDP non garantisce la consegna dei messaggi

upvoted 1 times

Bilal1992 8 months, 2 weeks ago

A is right

upvoted 1 times

diudiuQIdama 9 months ago

Selected Answer: A

easy one

upvoted 1 times

Masquerade 9 months ago

The correct answer is A. TCP uses the three-way handshake, and UDP does not guarantee message delivery.

TCP and UDP are two different transport layer protocols that are commonly used in computer networks. Both protocols are used to establish a connection between two endpoints, but they differ in the way that they establish and maintain that connection.

upvoted 2 times

Ali526 2 years, 8 months ago

A is correct.

upvoted 3 times

SScott 2 years, 8 months ago

Yes, here is a good article supporting A....
https://www.guru99.com/tcp-vs-udp-understanding-the-difference.html#:~:text=TCP%20is%20a%20connection%2Doriented,UDP%20uses%20no%20handshake%20protocols&text=TCP%20has%20acknowledgment%20segments%2C%20but,not%20have%20any%20acknowledgment%20segment.

upvoted 3 times

Question #7 *Topic 1*

Which 802.11 frame type is Association Response?

A. management

B. protected frame

C. action

D. control

Correct Answer: *A*
There are three main types of 802.11 frames: the Data Frame, the Management Frame and the Control Frame. Association Response belongs to Management
Frame. Association response is sent in response to an association request.
Reference:
https://en.wikipedia.org/wiki/802.11_Frame_Types

Community vote distribution

A (100%)

hokieman91 Highly Voted 2 years, 7 months ago
"A" is correct - great video on the 3 types of 802.11 frames
https://www.youtube.com/watch?v=PCpnRqKCWCQ
upvoted 29 times

Nae_Kun 1 year, 9 months ago
wow this video is a must watch, if your coming from ccna v3
upvoted 4 times

SScott 2 years, 5 months ago
Yes A for sure. That is an excellent video and breakdown of the Management Sub-Frame with Association.
upvoted 4 times

AgustD Highly Voted 3 years ago
The answer is management if i'm not wrong
upvoted 6 times

Tester_2025 Most Recent 2 months, 1 week ago
"A" is correct
upvoted 1 times

nuridelon 6 months, 2 weeks ago
A is correct
upvoted 1 times

Alizadeh 9 months ago
Answer is : A
The Association Response frame is a type of management frame in the 802.11 wireless networking standard. It is used to respond to an Association Request frame that is sent by a client device during the association process.

The Association Response frame is sent by the access point (AP) and contains information about the status of the association request, as well as any additional parameters that are required for the client to connect to the network. If the association request is successful, the Association Response frame will include the association ID (AID) that is assigned to the client device, as well as the supported rates and other relevant information. If the association request is unsuccessful, the Association Response frame will contain an error code indicating the reason for the failure.

The Association Response frame is an important part of the 802.11 association process, which is used to establish a connection between a client device and an AP. It is used to confirm that the client device is allowed to join the network and to provide the necessary information for the client to communicate with the AP.
upvoted 2 times

Masquerade 9 months ago
The correct answer is A. management.

In the 802.11 wireless networking standard, there are several different frame types that can be used for different purposes. The Association Response frame is a type of management frame, which is used for managing the basic operations of the wireless network.

Management frames are used for a variety of purposes, including association, authentication, and power management. Association Response frames are used to respond to an Association Request frame from a client device, indicating whether the device is allowed to join the network.

upvoted 1 times

HansZ 1 year, 2 months ago

Selected Answer: A

A is correct

upvoted 1 times

ScorpionNet 1 year, 4 months ago

Management

upvoted 2 times

Ayie 2 years, 2 months ago

management

upvoted 2 times

ZUMY 2 years, 5 months ago

A is correct

upvoted 2 times

ZUMY 2 years, 5 months ago

802.11 is wireless specification of IEEE.
A mac frame consist of several fields.
Frame control is one of the feild
Under frame control there are other fields such as protocol versions, type, subtype etc
Under Subtype, 2bit protocol versions subtype attributes set to 0 all ways
Attributes are
01 Management - Association Response
02 control
03 Data
04 Extensions

upvoted 6 times

Question #8 *Topic 1*

In which way does a spine-and-leaf architecture allow for scalability in a network when additional access ports are required?

A. A spine switch and a leaf switch can be added with redundant connections between them.

B. A spine switch can be added with at least 40 GB uplinks.

C. A leaf switch can be added with connections to every spine switch.

D. A leaf switch can be added with a single connection to a core spine switch.

Correct Answer: *C*
Spine-leaf architecture is typically deployed as two layers: spines (such as an aggregation layer), and leaves (such as an access layer). Spine-leaf topologies provide high-bandwidth, low-latency, nonblocking server-to-server connectivity.
Leaf (aggregation) switches are what provide devices access to the fabric (the network of spine and leaf switches) and are typically deployed at the top of the rack. Generally, devices connect to the leaf switches. Devices can include servers, Layer 4-7 services (firewalls and load balancers), and WAN or Internet routers.
Leaf switches do not connect to other leaf switches. In spine-and-leaf architecture, every leaf should connect to every spine in a full mesh.
Spine (aggregation) switches are used to connect to all leaf switches and are typically deployed at the end or middle of the row. Spine switches do not connect to other spine switches.
Reference:
https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/guide-c07-733228.html

Community vote distribution
C (83%) A (17%)

ZUMY Highly Voted 2 years, 5 months ago
C is correct!
In Spine Leaf architecture...
To increase performance(bandwidth) - Add Spine switch connects to every Leaf Switch
To Increase Access switch ports count - Add leaf switch and connects to every Spine switch
Support:
https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/white-paper-c11-737022.html
upvoted 13 times

Hanagaki_Shinjiro Most Recent 2 weeks, 3 days ago
C is correct
upvoted 1 times

Mgardini 4 months, 3 weeks ago
Selected Answer: C
answer is c
upvoted 2 times

GreatDane 8 months, 3 weeks ago
Selected Answer: C
Ref: Cisco Data Center Spine-and-Leaf Architecture: Design Overview White Paper - Cisco

"...
Spine-and-leaf architecture
...
If device port capacity becomes a concern, a new leaf switch can be added by connecting it to every spine switch and adding the network configuration to the switch. The ease of expansion optimizes the IT department's process of scaling the network.
..."

A. A spine switch and a leaf switch can be added with redundant connections between them.

Wrong answer.

B. A spine switch can be added with at least 40 GB uplinks.

Wrong answer.

C. A leaf switch can be added with connections to every spine switch.

Correct answer.

D. A leaf switch can be added with a single connection to a core spine switch.

Wrong answer.
upvoted 3 times

Masquerade 9 months ago

Selected Answer: C

CORRECTION:
Answer: C. A leaf switch can be added with connections to every spine switch.
This allows for scalability in a network when additional access ports are required because each leaf switch can be connected to each spine switch, providing additional capacity and redundancy. This gives the network more flexibility in terms of scalability, making it easier to add more ports and expand the network as needed.
upvoted 4 times

Masquerade 9 months ago

Selected Answer: A

The correct answer is A. A spine switch and a leaf switch can be added with redundant connections between them.

In a spine-and-leaf architecture, the network is organized into two layers: the spine layer and the leaf layer. The spine layer consists of one or more core switches, which are connected to each other and form the backbone of the network. The leaf layer consists of access switches, which are connected to the spine switches and provide connectivity to end devices.

When additional access ports are required in a spine-and-leaf architecture, the network can be easily scaled by adding a new spine switch and a new leaf switch. The new spine switch is connected to the existing spine switches with redundant links, and the new leaf switch is connected to the new spine switch. This allows the network to accommodate more devices without disrupting the existing network.
upvoted 2 times

Request7108 9 months ago

Your answer is incorrect because it is not necessary to add a spine every time you add a leaf or vice versa. Leaf switches expand port capacity but a spine switch is necessary when its plane becomes oversubscribed.
upvoted 1 times

SamuelSami 1 year, 2 months ago

A spine switch and a leaf switch can be added with redundant connections between them
upvoted 1 times

Jbcrggddfhh 1 year, 4 months ago

"The leaf layer consists of access switches that connect to devices such as servers."

More leaf switches = more access switches = more access ports

https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/white-paper-c11-737022.html
upvoted 1 times

SollyMalwane 1 year, 7 months ago

Selected Answer: C

Is correct
upvoted 1 times

chosenone 2 years, 11 months ago

When a new leaf switch is added it will have connection to every spine switch
So the option (C) is the correct answer
upvoted 3 times

AgustD 3 years ago

Answer should be option A i think, if i make any mistakes pls correct me i'm a newbie :)
upvoted 4 times

Enycon 3 years ago

I think you dont use lacp between spine and leaf but Im a newbie myself
upvoted 2 times

pokemonmoon 2 years, 12 months ago

OCG doesnt say anything about it
upvoted 2 times

Demi_UY_Scuti 2 years, 10 months ago

If I remember correctly, you can add redundant links in a spine-leaf topology. However, C is the correct answer because it meets the necessary conditions for creating this type of topology, that is, one link between every spine and every leaf switches.
upvoted 4 times

ScorpionNet 1 year, 4 months ago

The answer is C because you can only connect leaf switches to more spine switches. Spine switches does the same but completely opposite
upvoted 1 times

Question #9 *Topic 1*

What identifies the functionality of virtual machines?

A. The hypervisor communicates on Layer 3 without the need for additional resources.

B. Each hypervisor supports a single virtual machine and a single software switch.

C. The hypervisor virtualizes physical components including CPU, memory, and storage.

D. Virtualized servers run efficiently when physically connected to a switch that is separate from the hypervisor.

Correct Answer: *C*

Community vote distribution

C (100%)

shomkin Highly Voted 1 year, 8 months ago

just me or is the question supposed to be "check the the most correct statement regarding hypervisors"?

upvoted 12 times

Yasin_Alsabah 1 year, 7 months ago

I agree with you :)

upvoted 2 times

sasquatchshrimp 1 year, 1 month ago

At this point I feel like I am just picking an answer that is not wrong, but also has nothing to do with the question.

upvoted 2 times

Bigc0ck Highly Voted 1 year, 7 months ago

This seems more like a MCSA question than CCNA...

upvoted 6 times

MSTAHIR Most Recent 1 month, 2 weeks ago

Correct Answer is C Hypervisor

upvoted 1 times

Mgardini 4 months, 3 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

namyou 5 months, 3 weeks ago

Selected Answer: C

I think it's c

upvoted 1 times

GreatDane 8 months, 3 weeks ago

Selected Answer: C

Ref: What is a virtual machine (VM) and how it works – Cisco

"...
How does a virtual machine work?

A virtual machine packages an operating system and application with a description of the compute resources needed to run it, such as the CPU, memory, storage, and networking. When this virtual machine is deployed to a host computer, a software called hypervisor reads the description and provides the requested compute resources.
..."

A. The hypervisor communicates on Layer 3 without the need for additional resources.

Wrong answer.

B. Each hypervisor supports a single virtual machine and a single software switch.

Wrong answer.

C. The hypervisor virtualizes physical components including CPU, memory, and storage.

Correct answer.

D. Virtualized servers run efficiently when physically connected to a switch that is separate from the hypervisor.

Wrong answer.
upvoted 1 times

Masquerade 9 months ago

Selected Answer: C

The hypervisor virtualizes physical components including CPU, memory, and storage. The hypervisor is a software layer that sits between the physical hardware of a computer and the operating system. It virtualizes physical components such as CPU, memory, and storage, allowing for multiple operating systems to run on a single physical machine. This allows for improved scalability, flexibility, and resource utilization.
upvoted 2 times

ZUMY 9 months, 3 weeks ago

C is ok
upvoted 1 times

DARKEDGE 1 year, 6 months ago

Selected Answer: C

C is the right answer
upvoted 2 times

Eric852 1 year, 7 months ago

Selected Answer: C

It's C
upvoted 1 times

SollyMalwane 1 year, 7 months ago

Selected Answer: C

I agree with you
upvoted 1 times

Question #10 *Topic 1*

Which command automatically generates an IPv6 address from a specified IPv6 prefix and MAC address of an interface?

A. ipv6 address dhcp

B. ipv6 address 2001:DB8:5:112::/64 eui-64

C. ipv6 address autoconfig

D. ipv6 address 2001:DB8:5:112::2/64 link-local

Correct Answer: *C*
The ג€ipv6 address autoconfigג€ command causes the device to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the EUI-64 based addresses to the interface. Addresses are configured depending on the prefixes received in Router Advertisement (RA) messages. The device will listen for RA messages which are transmitted periodically from the router (DHCP Server). This RA message allows a host to create a global IPv6 address from:
ג€¢ Its interface identifier (EUI-64 address)
ג€¢ Link Prefix (obtained via RA)
Note: Global address is the combination of Link Prefix and EUI-64 address

Community vote distribution
B (69%) C (25%) 3%

Wissba Highly Voted 3 years, 4 months ago
The needed is an IPv6 address generated from a specified prefix and not from a delegated one, so I think that B is the right answer
upvoted 39 times

JoJoRa33it 1 year, 10 months ago
CCNA 200-301 Official Cert Guide, Volume 1
Chapter 24: Implementing IPv6 Addressing on Routers

ipv6 address address/prefix-length: Static configuration of a specific address
ipv6 address prefix/prefix-length eui-64: Static configuration of a specific prefix and
prefix length, with the router calculating the interface ID using EUI-64 rules
ipv6 address dhcp: Dynamic learning on the address and prefix length using DHCP
ipv6 address autoconfig: Dynamic learning of the prefix and prefix length, with the router
calculating the interface ID using EUI-64 rules (SLAAC)
upvoted 18 times

Thodoris85 3 years, 3 months ago
The simplest method is to enable stateless autoconfiguration on the interface. Enabling stateless autoconfiguration on the interface configures IPv6 addresses based on prefixes received in Router Advertisement messages. A link-local address, based on the Modified EUI-64 interface ID, is automatically generated for the interface when stateless autoconfiguration is enabled. To enable stateless autoconfiguration, enter the following command:
hostname(config-if)# ipv6 address autoconfig
upvoted 15 times

iRodimusPrime 3 years, 2 months ago
That's as may, but the question states automatically I.E. upon entering the command the address is added without the need for further information to be acquired first.
upvoted 5 times

Kawan_Ali 1 year, 8 months ago
I think its B because it says "specified IPv6 prefix"
upvoted 12 times

JWMcInSC 3 years, 3 months ago
EUI-64 (Extended Unique Identifier) is a method we can use to automatically configure IPv6 host addresses. An IPv6 device will use the MAC address of its interface to generate a unique 64-bit interface ID. However, a MAC address is 48 bit and the interface ID is 64 bit.
upvoted 7 times

khalid86 Highly Voted 2 years, 11 months ago
Answer is B
upvoted 10 times

SudipSen Most Recent 4 weeks ago
B is correct
upvoted 1 times

binayD 1 month, 1 week ago

This question doesn't require you to think outside the given parameters. For instance, it suggests analyzing the question before considering the options. The term "Auto config" is linked to SLAAC, and if the question mentions SLAAC or hints at it, option C is probably the correct answer. In essence, the question is asking how you would generate an IPv6 address using a /64 prefix and the MAC address of the interface.

upvoted 2 times

dayogreats 1 month, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

Shri_Fcb10 1 month, 2 weeks ago

Guys I passed my CCNA cert. Most of the questions were this dump. A big thanks to everyone contributing on the discussion, it helped a lot. CHEERSSS!!!

upvoted 3 times

Natalie89 2 months, 2 weeks ago

I think the correct answer is B. A key word is 'specified', in spite of 'automatically '

upvoted 1 times

YaaYaaSEE 3 months ago

Selected Answer: C

The correct command to automatically generate an IPv6 address from a specified IPv6 prefix and MAC address of an interface is the "ipv6 address autoconfig" command.

upvoted 1 times

Dunedrifter 3 months, 4 weeks ago

Selected Answer: B

To generate an ipv6 address from a *SPECIFIED* prefix you will need to *SPECIFY* the prefix with eui-64 keyword. The answer is B.

upvoted 2 times

Ciscoparty 4 months ago

Selected Answer: B

The command used to automatically generate an IPv6 address from a specified IPv6 prefix and MAC address of an interface is called "EUI-64" (Extended Unique Identifier-64). EUI-64 is a method that combines a device's 48-bit MAC address with a 16-bit identifier derived from the IPv6 prefix to create a 64-bit interface identifier.

To generate an IPv6 address using EUI-64, you need the IPv6 prefix and the MAC address of the interface.

upvoted 2 times

cr0minus 4 months, 3 weeks ago

You are correct that the "ipv6 address autoconfig" command enables automatic configuration of the IPv6 address using the SLAAC mechanism, which generates an IPv6 address based on the prefix information advertised by the router. So, in a sense, this command does generate an IPv6 address automatically.

However, it is important to note that the IPv6 address generated using SLAAC is not based on the MAC address of the interface, unlike the IPv6 address generated using the "ipv6 address 2001:DB8:5:112::/64 eui-64" command.

So, to answer your question, if the requirement is to generate an IPv6 address based on the MAC address of an interface, then the correct command would be "ipv6 address 2001:DB8:5:112::/64 eui-64". On the other hand, if the requirement is to enable automatic configuration of the IPv6 address using the router-advertised prefix information, then the correct command would be "ipv6 address autoconfig".

upvoted 3 times

shumps 5 months ago

here they are requiring the command which is: ipv6 address autoconfig. Not the result, so the answer is C

upvoted 1 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: B

The command "ipv6 address 2001:DB8:5:112::/64 eui-64" automatically generates an IPv6 address from a specified IPv6 prefix and MAC address of an interface using the EUI-64 method. The EUI-64 method uses the MAC address of the interface to create an interface identifier (IID) that is used to complete the IPv6 address.

Option A ("ipv6 address dhcp") configures an interface to obtain an IPv6 address through DHCPv6.

Option C ("ipv6 address autoconfig") configures an interface to automatically obtain an IPv6 address using Stateless Address Autoconfiguration (SLAAC).

Option D ("ipv6 address 2001:DB8:5:112::2/64 link-local") configures an IPv6 link-local address on the interface.

upvoted 1 times

Ciscoman021 5 months, 4 weeks ago

Selected Answer: B

The EUI-64 method uses the MAC (Media Access Control) address of the network interface to generate a unique 64-bit identifier. The MAC address is a unique identifier assigned to the network interface by the manufacturer and is usually 48 bits long. The EUI-64 method takes the MAC address

and adds a 16-bit value to create a 64-bit identifier.

upvoted 1 times

lucantonelli93 6 months, 3 weeks ago

Selected Answer: B

The correct answer it's B

upvoted 1 times

oatmealturkey 6 months, 4 weeks ago

Selected Answer: C

The answer is C. Keyword is "automatically". If you input the prefix and type eui-64 and press enter, it is similar to using a calculator. There is no automation involved. So autoconfig fits better.

"Specified" is in there to throw us off, but it doesn't necessarily mean that WE must specify the prefix; it could simply mean that the prefix is specified in the RA.

upvoted 1 times

Nutanix_Dummy 6 months, 4 weeks ago

Selected Answer: B

The keyword is "specified IPv6 prefix and MAC address" thus answer is B

upvoted 2 times

Question #11 *Topic 1*

When configuring IPv6 on an interface, which two IPv6 multicast groups are joined? (Choose two.)

A. 2000::/3

B. 2002::5

C. FC00::/7

D. FF02::1

E. FF02::2

Correct Answer: *DE*
When an interface is configured with IPv6 address, it automatically joins the all nodes (FF02::1) and solicited-node (FF02::1:FFxx:xxxx) multicast groups. The all- node group is used to communicate with all interfaces on the local link, and the solicited-nodes multicast group is required for link-layer address resolution.
Routers also join a third multicast group, the all-routers group (FF02::2).
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/xe-3s/ipv6-xe-36s-book/ip6-multicast.html

Community vote distribution
DE (100%)

mazintaha Highly Voted 3 years, 2 months ago
All-nodes link-local multicast group FF02::1
All-routers link-local multicast group FF02::2
upvoted 22 times

Gelo29 Highly Voted 2 years, 12 months ago
Multicast - FF
Global Unicast - 2/3
Unique Local - FC/FD
Link Local - FE80
upvoted 22 times

Demi_UY_Scuti 2 years, 10 months ago
Global unicast includes all prefixes unless reserved for other purposes. Although 2 & 3 fall in that range, they are not the only assignable global unicast addresses.
upvoted 3 times

MSTAHIR Most Recent 1 month, 2 weeks ago
DE Selected FF is link-local multicast group
upvoted 1 times

Pupettolo9 2 months, 3 weeks ago
Selected Answer: DE
All-nodes link-local multicast group FF02::1
All-routers link-local multicast group FF02::2
upvoted 1 times

ricky1802 7 months, 2 weeks ago
Selected Answer: DE
D. FF02::1 - This is the all-nodes multicast address. It is used to reach all devices on a local-link (same subnet).

E. FF02::2 - This is the all-routers multicast address. It is used to reach all routers on a local-link.

A. 2000::/3 and C. FC00::/7 are not multicast addresses, 2000::/3 is an unicast address range, FC00::/7 is an unique-local address range, both are unicast address ranges. B. 2002::5 is not a multicast address either, it's an unicast address.

It's important to note that multicast addresses are used to reach a group of devices instead of a single device, unlike unicast addresses.
upvoted 1 times

GreatDane 8 months, 2 weeks ago
Selected Answer: DE
Ref: IP Multicast: PIM Configuration Guide, Cisco IOS Release 15SY

"C H A P T E R 3
...

Information About Configuring Basic IP Multicast in IPv6 Networks
...
IPv6 Multicast Groups

An IPv6 address must be configured on an interface before the interface can forward IPv6 traffic. Configuring a site-local or global IPv6 address on an interface automatically configures a link-local address and activates IPv6 for that interface. Additionally, the configured interface automatically joins the following required multicast groups for that link:
...
• All-nodes link-local multicast group FF02::1
• All-routers link-local multicast group FF02::2
..."

upvoted 1 times

Masquerade 9 months ago

Selected Answer: DE

Answer: D. FF02::1 and E. FF02::2
Explanation: IPv6 multicast groups are joined when configuring IPv6 on an interface. The two IPv6 multicast groups that are joined are FF02::1 and FF02::2. FF02::1 is the all-nodes multicast group and FF02::2 is the all-routers multicast group.

upvoted 1 times

cormorant 10 months, 2 weeks ago

FF02::1 - all nodes/hosts
FF02::2 - all routers

upvoted 2 times

Bram99 10 months, 3 weeks ago

DE correct answer

upvoted 1 times

exilify 11 months, 4 weeks ago

Selected Answer: DE

dedededededede

upvoted 1 times

lock12333 1 year, 3 months ago

Selected Answer: DE

dedededededede

upvoted 1 times

ZUMY 2 years, 5 months ago

When configure Ipv6 the interface will join multicast groups as follows
as per answer
If its a node :FF02::1
If its a router :FF02::2

upvoted 6 times

felixedmund 2 years, 9 months ago

For router to act like IPv6 router (to get it joined to FF02::2 is all-routers multicast group), we need to issue "ipv6 unicast-routing" command. That means configuring only interface with IPv6 address does not mean it will definitely join FF02::2 group unless you add "ipv6 unicast-routing" command on global config mode

upvoted 4 times

DRAG DROP -

```
[root@HostTest ~]# ip route
default via 192.168.1.193 dev eth1  proto static
192.168.1.0/26 dev eth1  proto kernel  scope link  src 192.168.1.200  metric 1

[root@HostTest ~]# ip addr show eth1
eth1:  mtu 1500 qdisc pfifo_fast qlen 1000
   link/ether 00:0C:22:83:79:A3 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.200/26 brd 192.168.1.255 scope global eth1
   inet6 fe80::20c:29ff:fe89:79b3/64 scope link
   valid_lft forever preferred_lft forever
```

Refer to the exhibit. Drag and drop the networking parameters from the left onto the correct values on the right.

Select and Place:

Answer Area

default gateway	00:0C:22
host IP address	00:0C:22:83:79:A3
NIC MAC address	192.168.1.193
NIC vendor OUI	192.168.1.200
subnet mask	255.255.255.192

Correct Answer:

Answer Area

default gateway	NIC vendor OUI
host IP address	NIC MAC address
NIC MAC address	default gateway
NIC vendor OUI	host IP address
subnet mask	subnet mask

The ג€ip routeג€ and ג€ip addr show eth1ג€ are Linux commands.

ג ¢€ג€ip routeג€: display the routing table

ג ¢€ג€ip addr show eth1ג€: get depth information (only on eth1 interface) about your network interfaces like IP Address, MAC Address information

Robertlars Highly Voted 11 months, 1 week ago

- default gateway = 192.168.1.193

- host IP address = 192.168.1.200

- NIC MAC address = 00:0C:22:83:79:A3

- NIC vendor OUI = 00:OC:22

- subnet mask = 255.255.255.192

upvoted 28 times

sirpsionics Most Recent 1 month, 1 week ago

How do you tell the difference between the host ip and default gateway in this question???

upvoted 1 times

christian321 1 month ago

The "ip route" command tells us the default gateway whereas the "ip addr show" command shows us the configs of the interface. Both commands are used on a host. So the ip of the host's interface is the host ip.

upvoted 1 times

Question #13 *Topic 1*

What is the default behavior of a Layer 2 switch when a frame with an unknown destination MAC address is received?

A. The Layer 2 switch forwards the packet and adds the destination MAC address to its MAC address table.

B. The Layer 2 switch sends a copy of a packet to CPU for destination MAC address learning.

C. The Layer 2 switch floods packets to all ports except the receiving port in the given VLAN.

D. The Layer 2 switch drops the received frame.

Correct Answer: *C*
If the destination MAC address is not in the CAM table (unknown destination MAC address), the switch sends the frame out all other ports that are in the same
VLAN as the received frame. This is called flooding. It does not flood the frame out the same port on which the frame was received.

Community vote distribution

C (100%)

therandman Highly Voted 3 years, 2 months ago

Sometimes called BUM traffic - Broadcast, Unknown Unicast, Multicast. These forms of traffic are "flooded" out all ports except the port the packet was received on.

upvoted 21 times

ZUMY Highly Voted 2 years, 5 months ago

C is correct.
Whenever a switch receive a frame, it look f MAC address table for a matching entry and if not found ,switch will forward to (Flood) all the ports in the switch except the port that received.

upvoted 12 times

Hanagaki_Shinjiro Most Recent 2 weeks, 3 days ago

C is corect, it can cause flooding

upvoted 1 times

MSTAHIR 1 month, 2 weeks ago

Selected Answer C, unknown destination address, switch flood the frame to its all ports except the received one in the same VLAN.

upvoted 1 times

BeautifulSmile 3 months, 2 weeks ago

I wrote the CCNA exam yesterday, and i passed. this site was really helpful and again reading through comment did help as well.

upvoted 3 times

Taju711 4 months, 3 weeks ago

did any have latest exam result for CCNA?

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: C

Ref: Introduction to Networks Companion Guide (CCNAv7)

"Chapter 7
Ethernet Switching
...
The MAC Address Table
...
Find the Destination MAC Address

If the destination MAC address is a unicast address, the switch looks for a match between the destination MAC address of the frame and an entry in its MAC address table. If the destination MAC address is in the table, the switch forwards the frame out the specified port. If the destination MAC address is not in the table, the switch forwards the frame out all ports except the incoming port. This is called an unknown unicast.
..."

upvoted 1 times

Masquerade 9 months ago

Selected Answer: C

Answer is C. The Layer 2 switch floods packets to all ports except the receiving port in the given VLAN. When a Layer 2 switch receives a frame with an unknown destination MAC address, it will flood the frame to all ports in the same VLAN, except for the port from which the frame was received. This is done so that the destination device can receive the frame and respond with its MAC address.

upvoted 1 times

everchosen13 11 months, 2 weeks ago

I believe its C
But shouldnt it say flood 'frames' not packets

upvoted 1 times

msomali 1 year, 4 months ago

Switches Flood traffic with unknown destination MAC Address out all ports apart from the one it received, They do not forward. They will only forward if the destination MAC Address is in the CAM Table.

So from the question the keyword is "UNKNOWN MAC ADDRESS" and Letter C has the Keyword "FLOOD" thus C is the correct answer

upvoted 1 times

npettijohn 1 year, 10 months ago

I would also like to add that if the source MAC address is not in the CAM table, then it will be added.

upvoted 1 times

DatBroNZ 2 years, 10 months ago

Option C. When there is no matching entry in the MAC address table, switches forward the frame out all interfaces (except the incoming interface) using a process called flooding.

upvoted 3 times

AgustD 3 years ago

Option C is the correct answer.

upvoted 3 times

Anton2020 3 years, 1 month ago

D would be correct if the question was about a router receiving an IP packet with an unknown destination.

upvoted 3 times

Enycon 3 years ago

The router would send the packet to the WAN port, usually the default gateway.

upvoted 2 times

rlelliott 2 years, 7 months ago

The Router would only send an unknown packet out another interface if it has a default route configured listing that interface or ip address on that connected network. Routers only use default gateways when ip routing is disabled

upvoted 2 times

szx 3 years, 1 month ago

Answer is C

upvoted 4 times

Question #14 *Topic 1*

An engineer must configure a /30 subnet between two routes. Which usable IP address and subnet mask combination meets this criteria?

A. interface e0/0 description to XX-AXXX:XXXXX ip address 10.2.1.3 255.255.255.252

B. interface e0/0 description to XX-AXXX:XXXXX ip address 192.168.1.1 255.255.255.248

C. interface e0/0 description to XX-AXXX:XXXXX ip address 172.16.1.4 255.255.255.248

D. interface e0/0 description to XX-AXXX:XXXXX ip address 209.165.201.2 225.255.255.252

Correct Answer: *D*

Community vote distribution

D (100%)

rugginic Highly Voted 3 years, 2 months ago

answer is D. The up in A is a broadcast

upvoted 40 times

dendio 1 year, 8 months ago

Right, A is the broadcast address - it is explained in better detail here: https://stackoverflow.com/questions/29034878/how-can-i-determine-network-and-broadcast-address-from-the-ip-address-and-subnet

upvoted 4 times

r8derfan33 Highly Voted 3 years, 3 months ago

Wait? What? Did you look at the subnet mask? 225.255.255.252?

upvoted 18 times

Ali526 2 years, 8 months ago

There is typo in D; should be 255.255.255.252.
Having said that, it's the correct answer.

upvoted 4 times

Smaritz 1 year, 5 months ago

To be honest, I didn't even notice the typo LOL

upvoted 3 times

Tengereni 2 years, 4 months ago

thats a typo

upvoted 3 times

SiliconeIT Most Recent 1 month, 1 week ago

The answer is A, I saw some saying that A is a broadcast address and would like to remind everyone that broadcast addresses can be reconfigured while the mistake of having subnet mask 225.255.255.251 eliminates it as a candidate

upvoted 1 times

bikila123 1 month, 2 weeks ago

A is Broadcast address of a given network , /30 have only 2 usable host so the correct answer is D.

upvoted 1 times

Da_Costa 2 months ago

Selected Answer: D

The correct answer is D although the subnet mask is strange

upvoted 1 times

Taku2023 4 months, 2 weeks ago

225.255.255.252 Is an invalid subnet mask

upvoted 1 times

Rydaz 4 months, 1 week ago

its a typo

upvoted 1 times

Taju711 4 months, 3 weeks ago

Did anyone have any latest exam re

upvoted 2 times

GreatDane 8 months, 2 weeks ago

Selected Answer: D

A. interface e0/0 description to XX-AXXX:XXXXX ip address 10.2.1.3 255.255.255.252

Given address belongs to subnet 10.2.1.0/30, and it's the broadcast address inside that subnet.
Wrong answer.

B. interface e0/0 description to XX-AXXX:XXXXX ip address 192.168.1.1 255.255.255.248

Given address belongs to subnet 192.168.1.0/29.
Wrong answer.

C. interface e0/0 description to XX-AXXX:XXXXX ip address 172.16.1.4 255.255.255.248

Given address belongs to subnet 172.16.1.0/29.
Wrong answer.

D. interface e0/0 description to XX-AXXX:XXXXX ip address 209.165.201.2 225.255.255.252

Given address belongs to subnet 209.165.201.0/30, which ranges from 209.165.201.1 to 209.165.201.2.
Correct answer.

upvoted 5 times

michael1001 9 months, 1 week ago

Need to fix the question as well, says routes instead of routers. Very confusing.

upvoted 2 times

Layfon 12 months ago

If these are updated questions how is this typo still here

upvoted 3 times

france60 1 year, 4 months ago

la réponse D est correcte

upvoted 2 times

rictorres333 1 year, 4 months ago

Selected Answer: D

It's posible a typing error letter D, just you must google by the question, the error in mask was written hear, 225.255.255.252 intead of 255.255.255.252. Please, examtopic correct it!!!

upvoted 2 times

country_rooted 1 year, 5 months ago

we're using a pf of /30 thus all we need to do is look at the class and it will tell us how much we need for network bits and the remaining would be subnet and host bits. for additional help use the sm.

upvoted 1 times

DatBroNZ 1 year, 6 months ago

Option D is the correct (the question has a typo, mask is 255.255.255.252)
Network: 209.165.201.0
Broadcast: 209.165.201.3
Usable IPs: 209.165.201.1 - 209.165.201.2

Option A not correct because that IP is broadcast
Network: 10.2.1.0
Broadcast: 10.2.1.3
Usable IPs: 10.2.1.1 - 10.2.1.2

Option B and C are wrong because they have a /29 mask

upvoted 6 times

Nagib 1 year, 6 months ago

mask of D is not correct start 225.255.255.252 so answer is A

upvoted 1 times

Nagib 1 year, 6 months ago

A is the correct because D mask not correct 225.255.255.252
and D will be the answer if the mask will be fixed

upvoted 1 times

saadboss2022 1 year, 6 months ago

First, D IP address isn't private.
Second, we can use /31 between router's connection.
the question not clear enough.

upvoted 1 times

Question #15 *Topic 1*

Which network allows devices to communicate without the need to access the Internet?

A. 172.9.0.0/16

B. 172.28.0.0/16

C. 192.0.0.0/8

D. 209.165.201.0/24

Correct Answer: *B*

This question asks about the private ranges of IPv4 addresses. The private ranges of each class of IPv4 are listed below:
Class A private IP address ranges from 10.0.0.0 to 10.255.255.255
Class B private IP address ranges from 172.16.0.0 to 172.31.255.255
Class C private IP address ranges from 192.168.0.0 to 192.168.255.255
Only the network 172.28.0.0/16 belongs to the private IP address (of class B).

Community vote distribution

B (100%)

Samitha Highly Voted 3 years, 2 months ago

Private Address Ranges

Class A 10.0.0.0 to 10.255.255.255
Class B 172.16.0.0 to 172.32.255.255
class C 192.168.0.0 to 192.168.255.255

So 172.28.0.0/16 in the range of Private IPs in Class B.
Answer is B.

upvoted 22 times

Sr_Moe 2 years, 11 months ago

Class B should be 172.16.0.0 to 172.31.255.255

upvoted 10 times

iRodimusPrime Highly Voted 3 years, 2 months ago

This question is really badly worded, it's asking what type of address SHOULD you use if you're not connecting to the internet I.E. to save on IPv4 addresses. Therefore the only private address is correct.

upvoted 13 times

MSTAHIR Most Recent 1 month, 2 weeks ago

B Class-B Private address

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: B

An IP network, which is not connected to the public Internet, uses private IP addresses.
There is a privare IP addresse range per each IP address class.

A. 172.9.0.0/16

A class B, public IP address range.
Wrong answer.

B. 172.28.0.0/16

A class B, private IP address range.
Correct answer.

C. 192.0.0.0/8

A class C, public IP address range.
Wrong answer.

D. 209.165.201.0/24

A class C, public IP address range.
Wrong answer.

upvoted 1 times

ismatdmour 1 year, 6 months ago

This is surely the kind of question which one has to think further and try to predict what the intention behind it actually is. Surely, any network if working isolated from the internet can work with any IP addresses whether private or public. If you will connect this isolated network later to the Internet, if private you will need a NAT and if public (and not assigned to you) you will encounter problems. In any case you can have as well any public ip addresses behind a a NAT as long as the NAT will translate them to a valid public addresses (assigned to you). Unfortunately, poorly written questions are copied from one web site to another. I like about this site that they give the opportunity to vote and discuss the questions. I wonder if CISCO itself had cases of poor questions. Any cases or experiences reported?

upvoted 7 times

soRwatches 6 months, 1 week ago

poorly written question like this is unfair for those who are not native English speaker. like me.

upvoted 1 times

ZUMY 2 years, 5 months ago

Private IP Address Range by IETF
Class A 10.0.0.0-10.255.255.255
Class B 172.16.0.0 - 172.31.255.255
Class C 192.168.0.0 - 192.168.255.255

upvoted 3 times

rlelliott 2 years, 7 months ago

ALL of the answers are correct for what this question ACTUALLY asks, however I believe what they are meaning to ask is which network belongs in the private address range and therefore CANNOT communicate across the internet. Therefore the answer is B. 172.28.0.0/16 which is the only private address range presented.

upvoted 7 times

admin1982 2 years, 7 months ago

Definitely B

upvoted 3 times

dcouch 2 years, 11 months ago

why wouldn't C work?

upvoted 1 times

Benonie 2 years, 11 months ago

in the class C private range start with 192.168 and not 192.0. This is why C wouldn't work

upvoted 2 times

JWMcInSC 3 years, 3 months ago

I agree with the 172.28 being a defined range in 1918, that does not mean the other addresses couldn't work I assure you. That question is not what is a valid 1918 range, the question is which would work if we didn't need public access and they all would.

upvoted 3 times

Marcelious 3 years, 3 months ago

this doesn't make sense to me and I cannot find anything when googling it, as far as I am aware any local network will work so unsure on why the answer is B?

upvoted 2 times

simonver 3 years, 3 months ago

172.28.0.0/16 is the only subnet part of the private address-range defined in RFC 1918. The private addresses are:
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
https://en.wikipedia.org/wiki/Private_network

upvoted 15 times

Boot20 2 years, 10 months ago

Using a private address doesn’t mean The device “doesn’t need to access the internet “ - You can still use NAT. this question Is poorly written

upvoted 1 times

Question #16 *Topic 1*

```
Router(config)#interface GigabitEthernet 1/0/1
Router(config-if)#ip address 192.168.16.143 255.255.255.240
Bad mask /28 for address 192.168.16.143
```

Refer to the exhibit. Which statement explains the configuration error message that is received?

A. It belongs to a private IP address range.

B. The router does not support /28 mask.

C. It is a network IP address.

D. It is a broadcast IP address.

Correct Answer: *D*

Community vote distribution

D (100%)

ZUMY Highly Voted 2 years, 5 months ago

For /28 network, There (2^4)=16 Subnets with each having (2^4-2)=14 host (14 +1 Network ID+ 1Broadcast ID)=16
Subnets are
192.168.16.0
192.168.16.16
.....
192.168.16.128
192.168.16.144 (Above this network ID there will be address 192.168.16.143 which is a broadcast ID of Network 192.168.16.128

upvoted 22 times

ZUMY 2 years, 5 months ago

Shortcut to find
1.First calculate subnets (barrowed 4 bits 2^4=16 subnets) or 256-240 (16)
2. Then do a math (256/16)=16 subnets, if so (144/16)=9 subnets
so 144 is a subnet address and 143 is a broadcast address of previous network ID (128)
it means (128+16)144

upvoted 16 times

Customexit Highly Voted 11 months ago

For anyone still confused, I break it down a bit easier:
grab 192.168.16.143/28
10001111 is 143 in binary (the last octet is all we're worried about since it's /28).
Draw your line at /28, 1000 | 1111.
You remember how to get your network/broadcast, first/last?
Notice all 1's at the right of the line. That usually means that's your broadcast right?
And all 0's is your network.
So we can see that this is actually a broadcast.

upvoted 11 times

MSTAHIR Most Recent 1 month, 2 weeks ago

Selected D

upvoted 1 times

tonyisabel 1 year, 5 months ago

Selected Answer: D

subnet address=192.168.16.128
Host address range = 192.168.16.129-192.168.16.142
broadcast address=192.168.16.143

upvoted 6 times

DatBroNZ 1 year, 6 months ago

D is correct

Network: 192.168.16.128/28
Broadcast: 192.168.16.143
Usable IPs: 192.168.16.129 - 192.168.16.142

upvoted 3 times

__sb 1 year, 6 months ago

Not A: it's possible to configure a private IP address on an interface
Not B: /28 is a prefix not a mask, and all routers support them

Not C: network addresses are always even numbers (host part all 0's)
D: broadcast addresses are always odd numbers (host part all 1's)

upvoted 7 times

kalistro 1 year, 8 months ago

According to the mask 255.255.255.240 we take the last octet as reference and subtract to see the subnet increment: 256-240= 16. Then a multiple of 16 close to 143 is searched, in this case it is 144 which would be the following address of network and therefore 143 would be a broadcast address.

upvoted 2 times

aman87 1 year, 12 months ago

D is correct

upvoted 2 times

Shaz313 2 years, 2 months ago

D is definitely correct.

upvoted 4 times

Micah_TENGWA 2 years, 3 months ago

D is correct because the next subnet address is 192.168.16.144

upvoted 7 times

Giuseppe_001 2 years, 4 months ago

zumy insegnami la via

upvoted 3 times

Alsaher 2 years, 4 months ago

D is correct

upvoted 4 times

ZUMY 2 years, 5 months ago

D is correct.
If list out the subnet for /28
It will be like
192.168.16.0
192.168.16.16
..
192.168. 16.128
-------> here the last IP is 192.168. 16.143 is a broadcast
192.168.16.144
192.168.16.160..
Last 192.168. 16.240

upvoted 3 times

ZUMY 2 years, 5 months ago

Dear moderator
Please remove this comment.Thx

upvoted 2 times

marcojmnez 2 years, 6 months ago

255.255.255.240 -->/28
Block size=256-240=16 Usable IPs.
las part of the IP is 143 and there are 144 IPs to 0 to 143.
144/16=9 and hence 192.168.16.143 is a broadcast IP.

Explained by Samitha

upvoted 5 times

Ali526 2 years, 8 months ago

D is definitely correct.

upvoted 4 times

Question #17 *Topic 1*

Which IPv6 address type provides communication between subnets and cannot route on the Internet?

A. link-local

B. unique local

C. multicast

D. global unicast

Correct Answer: *B*
A IPv6 Unique Local Address is an IPv6 address in the block FC00::/7. It is the approximate IPv6 counterpart of the IPv4 private address. It is not routable on the global Internet.
Note: In the past, Site-local addresses (FEC0::/10) are equivalent to private IP addresses in IPv4 but now they are deprecated.
Link-local addresses only used for communications within the local subnet. It is usually created dynamically using a link-local prefix of FE80::/10 and a 64-bit interface identifier (based on 48-bit MAC address).

Community vote distribution

B (100%)

ZUMY Highly Voted 2 years, 5 months ago

B is correct

upvoted 7 times

Alizadeh Most Recent 9 months ago

Selected Answer: B

An IPv6 address type that provides communication between subnets and cannot route on the Internet is a link-local address. Link-local addresses are used for communication within a single network segment or link, such as between devices on a local area network (LAN). They are not intended to be routable over the Internet and are not assigned to devices that need to communicate with devices on other networks.

Link-local addresses are identified by the prefix "FE80::/10" and are automatically generated by the device when it is connected to a network. They are usually used in conjunction with other types of IPv6 addresses, such as global unicast addresses, which are used for communication over the Internet.

It's important to note that link-local addresses are not the same as loopback addresses, which are used for communication between a device and itself and are identified by the prefix "::1/128". Loopback addresses are not used for communication with other devices.

upvoted 3 times

Vlad_Is_Love_ua 1 year ago

Selected Answer: B

Unique local unicast addresses are analogous to private IPv4 addresses in that they are used for local communications, intersite VPNs, and so on, except for one important difference – these addresses are not intended to be translated to a global unicast address. They are not routable on the internet without IPv6 NAT, but they are routable inside a limited area, such as a site.

upvoted 2 times

Jackie_Manuas12 1 year, 6 months ago

"A IPv6 Unique Local Address is an IPv6 address in the block FC00::/7"
I thought unique local addresses began with FD, not FC?

upvoted 1 times

DUMPledore 9 months, 1 week ago

Found this on Jeremy's IT Lan YT

- Uses the address block FCOO: : / 7 (FCOO: : to FDFF : FFF F : FFF F: FFFF: F FFF : FFF F: FFF F)
- However, a later update requires the 8th bit to be set to 1, so the first two digits must be FD.

upvoted 1 times

Dante_Dan 1 year, 7 months ago

Selected Answer: B

For the people asking about the link-local address. Extracted from Official Cert Guide CCNA 200-301 Volume 1 page 566:

IPv6 defines rules so the packets sent to any link-local addresses should not be forwarded by any router to another subnet...

upvoted 3 times

shakyak 1 year, 9 months ago

Keyword
Global-Public IP
Local-Private IP

upvoted 3 times

dave1992 2 years ago

why is A not the right answer? link local, isnt routable, unique local routable within the lan.

upvoted 1 times

ProgSnob 1 year, 10 months ago

A is not the right answer because link local addresses do not communicate with other subnets. They only communicate with devices on their local link. B is correct as it is similar to the private addresses in IPv4. They can be routed internally but not across the Internet.

upvoted 7 times

Coffeezw 1 year, 11 months ago

From my understanding, unique local is routable (inter-vlan) not across the internet.

upvoted 1 times

Jonasye 2 years, 7 months ago

so link local address can be routed to internet? why?

upvoted 3 times

Bubu3k 2 years, 7 months ago

no it doesn't, but the question asks about routing between subnets as well

upvoted 4 times

Jonfernz 2 years, 5 months ago

Link local addresses cannot be routed to the Internet but they cannot communicate beyond their own subnet.

upvoted 4 times

hippyjm 2 years, 7 months ago

B is correct

upvoted 4 times

Question #18 *Topic 1*

Which IPv6 address block sends packets to a group address rather than a single address?

A. 2000::/3

B. FC00::/7

C. FE80::/10

D. FF00::/8

Correct Answer: *D*
FF00::/8 is used for IPv6 multicast and this is the IPv6 type of address the question wants to ask.
FE80::/10 range is used for link-local addresses. Link-local addresses only used for communications within the local subnetwork (automatic address configuration, neighbor discovery, router discovery, and by many routing protocols). It is only valid on the current subnet. It is usually created dynamically using a link-local prefix of FE80::/10 and a 64-bit interface identifier (based on 48-bit MAC address).

Community vote distribution

D (100%)

Samitha Highly Voted 3 years, 2 months ago

IPV6

1.Unicast
2.Any Cast
3.Multicast(FF00::/8)

Uni-cast
---
i.Global Uni cast (Public IPs 2000::/3)
ii.Unique Local (Private IPs FD00::/8)
iii.Link Local (FE08::10)

group address means one to many(Multicast).
Answer is D
upvoted 24 times

Delajan 2 years, 4 months ago

Actually Unique Local: Assigned from the FC00::/7 range
upvoted 1 times

therandman Highly Voted 3 years, 2 months ago

Somehow the FF seemed to be a hint.
upvoted 11 times

cormorant Most Recent 10 months, 2 weeks ago

FC00::/7 - private networks (intranet)
FE80::/10 - private networks (intranets)
FF00::/8 - multicast
upvoted 1 times

Vlad_Is_Love_ua 1 year ago

Selected Answer: D
The following figure illustrates the format of an IPv6 multicast address. An IPv6 multicast address defines a group of devices known as a multicast group. IPv6 multicast addresses use the prefix ff00::/8, which is equivalent to the IPv4 multicast address 224.0.0.0/4.
upvoted 1 times

Hodicek 1 year, 10 months ago

FF AS MULTICAST
upvoted 3 times

Shamwedge 2 years, 2 months ago

I read the question as in block i.e. prevent
Do do that
upvoted 2 times

Question #19 *Topic 1*

What are two reasons that cause late collisions to increment on an Ethernet interface? (Choose two.)

A. when Carrier Sense Multiple Access/Collision Detection is used

B. when one side of the connection is configured for half-duplex

C. when the sending device waits 15 seconds before sending the frame again

D. when a collision occurs after the 32nd byte of a frame has been transmitted

E. when the cable length limits are exceeded

Correct Answer: *BE*
A late collision is defined as any collision that occurs after the first 512 bits (or 64th byte) of the frame have been transmitted. The usual possible causes are full- duplex/half-duplex mismatch, exceeded Ethernet cable length limits, or defective hardware such as incorrect cabling, non-compliant number of hubs in the network, or a bad NIC.
Late collisions should never occur in a properly designed Ethernet network. They usually occur when Ethernet cables are too long or when there are too many repeaters in the network.
Reference:
https://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1904.html

Community vote distribution
BE (75%) AE (25%)

Artengineer Highly Voted 3 years, 4 months ago
the right answer is B_E
cause the selected one . when Carrier Sense Multiple Access/Collision Detection is used was the result f the collision domain but not the reason
Join me to discuss more over my blog
https://wa.me/50947163627
upvoted 31 times

VictorCisco 5 months ago
half-duplex as it is, can't be a cause of collision.
upvoted 1 times

John248 Highly Voted 3 years, 2 months ago
Directly from a Cisco article.

What are two reasons that cause late collisions to increment on an Ethernet interface? (Choose two)
A. when the sending device waits 15 seconds before sending the frame again
B. when the cable length limits are exceeded
C. when one side of the connection is configured for half-duplex
D. when Carrier Sense Multiple Access/Collision Detection is used
E. when a collision occurs after the 32nd byte of a frame has been transmitted
Answer: B, C
A late collision is defined as any collision that occurs after the first 512 bits (or 64th byte) of the frame have Been transmitted. The usual possible causes are full-duplex/half-duplex mismatch, exceeded Ethernet cable length limits, or defective hardware such as incorrect cabling, non-compliant number of hubs in the network, or
a bad NIC. Late collisions should never occur in a properly designed Ethernet network. They usually occur when Ethernet cables are too long or when there are too many repeaters in the network.
Reference: https://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1904.html
upvoted 19 times

dendio 1 year, 8 months ago
This is correct, but the answers have been moved around
upvoted 5 times

vuhidus Most Recent 1 year, 1 month ago
Selected Answer: BE
The answer is BE
upvoted 1 times

whojabagooya 1 year, 2 months ago
Selected Answer: BE
I'm going to have to agree with the cited cisco literature. They specifically site long cables and repeaters which are half duplex.
upvoted 2 times

lohaN73 1 year, 3 months ago

CSMA/CD happens before any collision,not after. So,option A can be kicked out at first glance... option B & E are valid
upvoted 1 times

illuded03jolted 1 year, 3 months ago
B and E are correct options.
upvoted 1 times

lock12333 1 year, 3 months ago
Selected Answer: AE
a and e
upvoted 1 times

Hodicek 1 year, 9 months ago
B- E is the correct answer, search on google on the 2 reasons that cause late collision
B- E is the correct answer 100%
upvoted 3 times

Shaz313 2 years, 2 months ago
Late Collision is a collision on an Ethernet network that is detected late in the transmission of the packet. Late collisions can result from defective Ethernet transceivers, from having too many repeaters between stations, or from exceeding Ethernet specifications for maximum node-to-node distances
the right answer is B_E
upvoted 3 times

ZUMY 2 years, 5 months ago
Given Answer B & E are correct!
****
A late collision is defined as any collision that occurs after the first 512 bits (or 64th byte) of the frame have Been transmitted. The usual possible causes are full-duplex/half-duplex mismatch, exceeded Ethernet cable length limits, or defective hardware such as incorrect cabling, non-compliant number of hubs in the network, or
a bad NIC. Late collisions should never occur in a properly designed Ethernet network. They usually occur when Ethernet cables are too long or when there are too many repeaters in the network.
upvoted 5 times

admin1982 2 years, 7 months ago
Definitely B and E
upvoted 3 times

Lakshmi_200_301 2 years, 8 months ago
I think questions B and E are correct answers
upvoted 3 times

jowill 2 years, 9 months ago
B is not a correct answer because at CSMA/CD mode, end points cannot send and receive frames at the same time. Therefore end points(NIC) have to be in half-duplex mode. B is not a cause of late collision. But A can detect collision but also not the cause of late collision. All in all there is issue in the description of the question itself.
upvoted 2 times

siva_13 2 years, 9 months ago
B and E
upvoted 2 times

daslux4 2 years, 9 months ago
B and E certainly
upvoted 2 times

boghota 2 years, 10 months ago
But B (when one side of the connection is configured for half-duplex) leaves open if the other side of the connection is configured as half-duplex as well so this doesn´t necessarily mean a duplex missmacth or am I wrong here?
upvoted 2 times

boghota 2 years, 10 months ago
But on the other hand, as Wikipedia states:
"As a correctly set up CSMA/CD (Carrier-sense multiple access with collision detection) network link should not have late collisions, the usual possible causes are full-duplex/half-duplex mismatch, exceeded Ethernet cable length limits, or defective hardware such as incorrect cabling, non-compliant number of hubs in the network, or a bad NIC."
So I guess A can not be the right answer.

https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_detection#Late_collision
upvoted 1 times

ITstudent123 2 years, 10 months ago
B and E
upvoted 1 times

Question #20 *Topic 1*

What is a benefit of using a Cisco Wireless LAN Controller?

A. It eliminates the need to configure each access point individually.

B. Central AP management requires more complex configurations.

C. Unique SSIDs cannot use the same authentication method.

D. It supports autonomous and lightweight APs.

Correct Answer: *A*

Samitha Highly Voted 3 years, 2 months ago

A wireless LAN (or WLAN) controller is used in combination with the Lightweight Access Point Protocol (LWAPP) to "manage light-weight access points in large quantities" by the network administrator or network operations center.

upvoted 13 times

ZUMY Highly Voted 2 years, 5 months ago

A is correct:

D could also be correct if there is no autonomous wording. Autonomous doesn't support LWAPP protocol (Autonomous Ap's are standalone Ap's which does not support CAPWAP/LWAPP) that Wireless Lan Controller uses)

upvoted 12 times

MSTAHIR Most Recent 1 month, 1 week ago

A is Correct answer. It is the advantage of using CISCO controller.

upvoted 1 times

cormorant 10 months, 2 weeks ago

there is a dump floating around in the internet stating that the answer to thsi question is "Unique SSIDs cannot use the same authentication method. "

can someone well versed in this area chime in?

upvoted 1 times

Request7108 9 months ago

Unique SSIDs can utilize the same authentication methods. They can be identical in all aspects except the network name

upvoted 1 times

awashenko 1 year, 8 months ago

A is correct. That is one of the biggest benefits of using a controller.

upvoted 1 times

ragekod 1 year, 11 months ago

A incorect

upvoted 1 times

nav2802 2 years, 6 months ago

Option A & D seems to be correct But
for Option D :- Wireless LAN Controller not associated with Autonomous (Meaning of Autonomous is "Standalone access point are known as Autonomous Access Point")
Keyword Lightweight is correct
WLC supports Lightweight but not autonomous

So "A" is correct

upvoted 5 times

klaku1212 2 years, 7 months ago

Q. Can I connect an autonomous AP to a wireless LAN controller (WLC) and expect the AP to work?

A. No, only LAPs work when they are connected to a WLC. Autonomous APs do not understand the Lightweight AP Protocol (LWAPP) or the CAPWAP protocol that the WLC uses. In order to connect an autonomous AP to a WLC, you must first convert the autonomous AP to lightweight mode.

upvoted 3 times

ZayaB 2 years, 7 months ago

A and D are both correct. if there was option to select 2 answers, A and D would be correct. However, the best answer for this question I think, is option A.

upvoted 2 times

Request7108 9 months ago

D is not correct because autonomous APs can't connect to a WLC
upvoted 1 times

DatBroNZ 2 years, 10 months ago
Easy one, option A
upvoted 3 times

AgustD 2 years, 10 months ago
Option D is the answer
upvoted 1 times

sarsat 3 years, 1 month ago
answer is correct
upvoted 4 times

Question #21 *Topic 1*

Which action is taken by switch port enabled for PoE power classification override?

A. If a monitored port exceeds the maximum administrative value for power, the port is shutdown and err-disabled.

B. When a powered device begins drawing power from a PoE switch port, a syslog message is generated.

C. As power usage on a PoE switch port is checked, data flow to the connected device is temporarily paused.

D. If a switch determines that a device is using less than the minimum configured power, it assumes the device has failed and disconnects it.

Correct Answer: *A*
PoE monitoring and policing compares the power consumption on ports with the administrative maximum value (either a configured maximum value or the port's default value). If the power consumption on a monitored port exceeds the administrative maximum value, the following actions occur:
- A syslog message is issued.
- The monitored port is shut down and error-disabled.
- The allocated power is freed.
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/power_over_ethernet.pdf

John248 Highly Voted 3 years, 2 months ago
PoE monitoring and policing compares the power consumption on ports with the administrative maximum value (either a configured maximum value or the port's default value). If the power consumption on a monitored port exceeds the administrative maximum value, the following actions occur:
• A syslog message is issued.
• The monitored port is shut down and error-disabled.
• The allocated power is freed.
upvoted 24 times

SScott 2 years, 5 months ago
A is correct.
Complete articles for reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/power_over_ethernet.html#80693:~:text=IEEE%20802.3af%20power%20classification

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011010.html#:~:text=the%20request%20is%20denied

B would be the normal operation of the switch with syslog typically enabled by default
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/troubleshooting/g_power_over_ethernet.html#:~:text=the%20syslog%20message%20was%20an
upvoted 2 times

GreatDane Most Recent 1 year, 3 months ago
Ref: Release 15.4SY Supervisor Engine 6T Software Configuration Guide

"Power over Ethernet
...
Inline Power IEEE Power Classification Override
...
If the power consumption on a monitored port exceeds the administrative maximum value, the following actions occur:

• A syslog message is issued.
• The monitored port is shut down and error-disabled.
• The allocated power is freed.
..."

Answer A is correct.
upvoted 3 times

Alsaher 2 years, 4 months ago
A is correct
upvoted 2 times

Question #22 *Topic 1*

What occurs to frames during the process of frame flooding?

A. Frames are sent to all ports, including those that are assigned to other VLANs.

B. Frames are sent to every port on the switch that has a matching entry in MAC address table.

C. Frames are sent to every port on the switch in the same VLAN except from the originating port.

D. Frames are sent to every port on the switch in the same VLAN.

Correct Answer: *C*

Community vote distribution

C (100%)

ZUMY Highly Voted 2 years, 5 months ago

Given answer C is correct

upvoted 11 times

SScott Highly Voted 2 years, 5 months ago

C is right.
Frame flooding would be restricted to the devices that are in that VLAN. With a potential loop issue the flooding could occur from the switch NOT having a device match nor location in the MAC table. B would describe a broadcast.

upvoted 8 times

GreatDane Most Recent 8 months, 2 weeks ago

Selected Answer: C

Ref: Flooding vs Broadcast - Cisco Community

Post by Kristian Alexander Brown

"...
Flooding is sometimes known as an unknown unicast. This happens when a switch receives a frame with a destination mac address it does not have in the CAM table. It will flood it out all ports except the receiving port of the frame.
..."

A. Frames are sent to all ports, including those that are assigned to other VLANs.

Wrong answer.

B. Frames are sent to every port on the switch that has a matching entry in MAC address table.

Wrong answer.

C. Frames are sent to every port on the switch in the same VLAN except from the originating port.

Correct answer.

D. Frames are sent to every port on the switch in the same VLAN.

Wrong answer.

upvoted 2 times

Shamwedge 1 year, 8 months ago

D is correct.

FF00::/8 and FF00::/10 are both multicast addresses.

https://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=5

upvoted 1 times

Jay1324 1 year, 8 months ago

No C is correct, you provided IPV^ multicast addresses which operate at layer 3 and are known as packets. The question states layer 2 frames meaning mac addresses.

upvoted 2 times

Wong93 2 years ago

C is correct

upvoted 3 times

nav2802 2 years, 6 months ago

Ans is C
upvoted 4 times

Question #23 *Topic 1*

Which function does the range of private IPv4 addresses perform?

A. allows multiple companies to each use the same addresses without conflicts

B. provides a direct connection for hosts from outside of the enterprise network

C. ensures that NAT is not required to reach the Internet with private range addressing

D. enables secure communications to the Internet for all external hosts

Correct Answer: *A*

ZUMY Highly Voted 2 years, 5 months ago
A is correct!
upvoted 10 times

Bhrino Most Recent 4 months, 1 week ago
Since the traffic doesn't traverse the internet there shouldn't be any confit with multiple companies have the same private ips in different networks
upvoted 1 times

Alokbhai580 5 months ago
Option A is incorrect because the range of private IPv4 addresses is specifically designed to prevent conflicting IP addresses within a single company or organization. If multiple companies were to use the same private IP addresses, conflicts would arise.

Therefore, the correct answer is option C, which states that the range of private IPv4 addresses ensures that NAT (Network Address Translation) is not required to reach the Internet with private range addressing. This is because private IP addresses are not routable on the public Internet, so NAT is required to translate between private and public IP addresses. By using private IP addresses within an organization, NAT can be avoided for internal communication, which can reduce network complexity and improve security.
upvoted 1 times

arjune 5 months, 2 weeks ago
A is Correct.This is where NAT is used also.
upvoted 1 times

Bilal1992 8 months, 2 weeks ago
A is correct.
upvoted 1 times

Crazey 2 years, 11 months ago
Repeating question
upvoted 1 times

Question #24 *Topic 1*

Which action must be taken to assign a global unicast IPv6 address on an interface that is derived from the MAC address of that interface?

A. explicitly assign a link-local address

B. disable the EUI-64 bit process

C. enable SLAAC on an interface

D. configure a stateful DHCPv6 server on the network

Correct Answer: *C*

Community vote distribution

C (100%)

dave1992 Highly Voted 2 years ago

i love how you can literally click for the correct answer but theres still people that come here and leave a comment saying," C is the correct answer"

upvoted 19 times

ciscodj 1 year, 5 months ago

you must be new to these types of questions and answers. The reason it's done is because some answers can be incorrect and the more ppl input you get a better idea if the answer is valid or not.

upvoted 19 times

GangsterDady 1 year, 10 months ago

they leave correct answer comment cause some question's answers on this website are wrong.

upvoted 25 times

Brocolee 2 months ago

For anyone that read @dave1992 comment, don't worry! The reason people doing it is because there is a lot of INCORRECT answer especially from #423 - #1057 (I haven't check anything after that yet).
So the more people COMMENTING it, the more it help others validate the answer so when you sit on the actual exam you know you got it right.
this user @dave1992 here is just being a Smart As*.
the saying goes: if you can't contribute positively, then just shut the F up.

upvoted 8 times

maw619 2 years ago

The more people agreeing with the answer helps me sleep better at night.

upvoted 80 times

ZUMY Highly Voted 2 years, 5 months ago

C is the answer
https://howdoesinternetwork.com/2013/slaac-ipv6-stateless-address-autoconfiguration

upvoted 10 times

pass4future Most Recent 1 month, 1 week ago

I read your article is highly informative and will surely benefit aspiring professionals. In addition, my well-crafted guide offers valuable insights into obtaining actual 200-301 exam dumps for CCNA success. Get actual 200-301 exam dumps, The author emphasizes the importance of choosing reputable sources and verifying the authenticity of the dumps to ensure reliable content. The URL (https://havily.com/how-to-get-actual-200-301-exam-dumps/) provided in the article leads readers to a trustworthy platform for accessing genuine exam dumps. By following the advice in the article, candidates can enhance their preparation for the CCNA exam and increase their chances of success. It is a comprehensive guide that promotes responsible use of exam dumps and encourages candidates to focus on understanding the concepts rather than memorizing answers. A highly informative read for anyone aspiring to excel in the CCNA certification.

upvoted 1 times

rhylos 2 months, 3 weeks ago

Selected Answer: C

C is correct. SLAAC https://howdoesinternetwork.com/2013/slaac-ipv6-stateless-address-autoconfiguration

upvoted 1 times

Da_Costa 3 months, 2 weeks ago

Enable Stateless Address Auto-Configuration (SLAAC)

upvoted 2 times

dsolaide 3 months, 3 weeks ago

Selected Answer: C

SLAAC is designed to be a simple, automatic approach to assigning IPv6 addresses. It is defined in RFC4862 and is specifically used to assign only a global unicast IPv6 address, an IPv6 prefix length, and, optionally, a default router.

upvoted 1 times

Mosaccio 4 months ago

Has anyone done the exam recently?

upvoted 2 times

GreatDane 8 months, 2 weeks ago

Selected Answer: C

Ref: IPv6 Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

"C H A P T E R 5

...

SLAAC Address Assignment

The most common method for IPv6 client address assignment is Stateless Address Auto-Configuration (SLAAC). SLAAC provides simple plug-and-play connectivity where clients self-assign an address based on the IPv6 prefix. This process is achieved.

Stateless Address Auto-Configuration (SLAAC) is configured as follows:

...

• Hosts take the first 64 bits of the IPv6 prefix from the Router Advertisement message and combines it with the 64 bit EUI-64 address (in the case of ethernet, this is created from the MAC Address) to create a global unicast message. The host also uses the source IP address, in the IP header, of the Router Advertisement message, as its default gateway.

The last 64 bits of the IP v6 address can be learned based on the following 2 algorithms:

• EUI-64 which is based on the MAC address of the interface, or
• Private addresses that are randomly generated.

"

...

upvoted 6 times

[Removed] 1 year, 2 months ago

What is SLAAC? SLAAC stands for Stateless Address Autoconfiguration and the name pretty much explains what it does. It is a mechanism that enables each host on the network to auto-configure a unique IPv6 address without any device keeping track of which address is assigned to which node C is ok

upvoted 8 times

Nicocisco 1 year, 7 months ago

Selected Answer: C

C is right

upvoted 1 times

SScott 2 years, 5 months ago

C is right.
https://www.amarchaudhari.me/enable-ipv6-slaac-on-cisco-routers/

upvoted 2 times

MD100MD101FUCKER 2 years, 10 months ago

Correct Answer: C

upvoted 2 times

Crazey 2 years, 11 months ago

Repeating question

upvoted 1 times

emmet0713 3 years ago

https://howdoesinternetwork.com/2013/slaac-ipv6-stateless-address-autoconfiguration

upvoted 3 times

Question #25 *Topic 1*

Several new coverage cells are required to improve the Wi-Fi network of an organization. Which two standard designs are recommended? (Choose two.)

A. 5GHz provides increased network capacity with up to 23 nonoverlapping channels.

B. 5GHz channel selection requires an autonomous access point.

C. Cells that overlap one another are configured to use nonoverlapping channels.

D. Adjacent cells with overlapping channels use a repeater access point.

E. For maximum throughput, the WLC is configured to dynamically set adjacent access points to the channel.

Correct Answer: *CE*

Community vote distribution

AC (64%) CE (34%)

Raymond9 Highly Voted 2 years, 9 months ago

If I have understood correctly, C and E have somehow the same meaning: avoid signal overlapping, since E separate the channel to avoid using the same channel and having signal collision. See "Dynamic Channel Assignment" in https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/radio_resource_management.html

A and B are kind of tricky to mention 5GHz, which must have non-overlapping channels, and actually accomplish what C/E have done, but they're saying incorrect stuff.
For A: 2.4GHz has 11 Channels, 5GHZ has 45 Channels
For B: There are two types of APs: autonomous AP/controllerless AP/"Fat AP" and lightweight AP/AP with Controller.
Ref:https://stormwindstudios.com/wireless-access-points/
And lightweight AP can be applied to 2.4GHz and 5Hz (there's command for both in cisco lightweight AP, just google it....

For D: I think the repeater cannot solve the problem of "overlapping channels" since it just re-transmit or "repeat" the signal, aka the overlapping channels will still be overlapping!

upvoted 23 times

chr Highly Voted 2 years, 4 months ago

The correct answer is A and C.
https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Channel_Planning_Best_Practices#:~:text=APs%20should%20be%20deployed%20with%20overlapping%20coverage%20cells.,because%20this%20can%20lead%20to%20increased%20channel%20utilization.

upvoted 12 times

naise 2 years, 2 months ago

is it sure the AC are the correct ones?

upvoted 1 times

Nicocisco 1 year, 7 months ago

No because 5Ghz has 24 non-overlapping channels

upvoted 11 times

SScott 2 years, 1 month ago

Yes an informative article and supporting A

upvoted 1 times

davidmdlp85 Most Recent 1 day, 10 hours ago

Ill go with C and E

https://www.routerfreak.com/best-wifi-channel-width-for-5ghz/

upvoted 1 times

lamm 2 months ago

CE must be the correct answer, A propose an incorrrect definition of non overlapping channels.

upvoted 2 times

DRvisin 3 months ago

A is probably a typo - it's supposed to be 24 channels - A & C are the answers

upvoted 1 times

DRvisin 3 months ago

if you see 23channels on the exam choose the other combination

upvoted 2 times

dsolaide 3 months, 3 weeks ago

Selected Answer: CE

In A ,the statement mentioned is not entirely accurate. 5GHz can have more or less than 23 channels depending on the standard being used (such as 802.11a, 802.11n, 802.11ac, or 802.11ax) and regulatory restrictions in different countries.it's also important to note that not all these channels are available for use in Wi-Fi networks due to regulatory restrictions.

C is correct for obvious reasons.

E is also correct because Configuring the wireless LAN controller (WLC) to dynamically set adjacent access points to the same channel is a technique known as channel bonding or channel aggregation. It is commonly used to maximize throughput in a wireless network.

upvoted 4 times

lolungos 4 months ago

A and C are correct

E sounds like the you will set adjacent APs to the same channel that will decrease the througput
The rest are just lies :(
Source: CWNP curriculum

upvoted 1 times

dropspablo 4 months, 3 weeks ago

Selected Answer: CE

5Ghz has 23 non-overlapping channels, but that's not the point. At 5GHz, its waves are short with greater speed in smaller cells, but its signal does not reach long distances like at 2.4GHz, so depending on the design, one or the other can be used. Therefore, answer A would not be the most appropriate answer to the question. Correct C - E

upvoted 2 times

dropspablo 1 month ago

Correction, the correct answer is A and C. "standard designs recommended" a WLC would not be a "standard design". And "Several new coverage cells" could only be 5Ghz which contains 23 nonoverlapping channels to improve coverage, as 2 ,4Ghz has only 3 nonoverlapping channels, which would make several new coverage cells very difficult, as proposed.

upvoted 1 times

jonathan126 4 months, 3 weeks ago

Selected Answer: CE

Network capacity is the amount of traffic that the wireless network can support, which is affected primarily by the wifi standard, but it can also be affected by factors such as overlapping channels (wave interference), absorption, scattering,... For option A, it seems to say that 5 GHz does not lead to overlapping channels, thus improve the network capacity. But 2.4GHz does not necessarily lead to overlapping channels, as long as we choose the non-overlapping channels (1, 6, and 11). So I think option A is not the best. I would go for C and E.
Please correct me if I am wrong!

upvoted 1 times

virab4 5 months ago

5g ghz have 24 non-overlaping channels

upvoted 1 times

Alokbhai580 5 months ago

A and C.

A) 5GHz provides increased network capacity with up to 23 non-overlapping channels. Using the 5GHz frequency band, which is less congested than the 2.4GHz band, provides more capacity for Wi-Fi clients, and allows for up to 23 non-overlapping channels to be used.

C) Cells that overlap one another are configured to use non-overlapping channels. To minimize interference and ensure high performance, adjacent cells that overlap each other should use non-overlapping channels. This helps to reduce co-channel interference and increase throughput.

upvoted 1 times

VictorCisco 5 months ago

Selected Answer: CE

A is not correct. 5GHz has more then 23 non overlapping chanels depending of bandwith of a channel (even 20 MHz):
https://en.wikipedia.org/wiki/List_of_WLAN_channels#5_GHz_(802.11a/h/j/n/ac/ax)

upvoted 2 times

Rether16 5 months, 2 weeks ago

Tricky question but it can't be Answer A as 5Ghz actually has 24 Non overlapping channels NOT 23 as stated.

upvoted 1 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: AC

The two recommended standard designs for improving Wi-Fi network coverage by adding new cells are:

A. 5GHz provides increased network capacity with up to 23 non-overlapping channels. This design is recommended because the 5GHz frequency band provides more non-overlapping channels than the 2.4GHz band, which is often crowded and has only three non-overlapping channels. Using the 5GHz band can help reduce interference and improve network performance.

C. Cells that overlap one another are configured to use non-overlapping channels. This design is recommended to minimize interference between adjacent access points. When cells overlap, they should be configured to use non-overlapping channels to avoid interference and ensure optimal

network performance.

Therefore, options A and C are the correct answers.

upvoted 1 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: AC

The two recommended standard designs to improve the Wi-Fi network of an organization are:

A. 5GHz provides increased network capacity with up to 23 nonoverlapping channels. This is because 5GHz frequency bands have more channels than the 2.4GHz frequency bands, and the channels do not overlap as much, allowing for less interference and more capacity.

C. Cells that overlap one another are configured to use nonoverlapping channels. This helps to reduce interference and ensures that adjacent cells do not interfere with one another. By using nonoverlapping channels, the organization can maximize the use of available frequencies and improve the overall performance of the Wi-Fi network.

Therefore, options A and C are the recommended standard designs to improve the Wi-Fi network of an organization.

upvoted 1 times

Itsjoshuaaa 6 months, 3 weeks ago

chatgpt chose A and C

upvoted 3 times

keokkeo_123 7 months ago

Selected Answer: AC

correcto

upvoted 1 times

Question #26 *Topic 1*

How do TCP and UDP differ in the way they provide reliability for delivery of packets?

A. TCP does not guarantee delivery or error checking to ensure that there is no corruption of data, UDP provides message acknowledgement and retransmits data if lost.

B. TCP provides flow control to avoid overwhelming a receiver by sending too many packets at once, UDP sends packets to the receiver in a continuous stream without checking.

C. TCP is a connectionless protocol that does not provide reliable delivery of data; UDP is a connection-oriented protocol that uses sequencing to provide reliable delivery.

D. TCP uses windowing to deliver packets reliably; UDP provides reliable message transfer between hosts by establishing a three-way handshake.

Correct Answer: *B*

Community vote distribution

B (100%)

ZUMY Highly Voted 2 years, 5 months ago

B is correct

upvoted 8 times

GreatDane Most Recent 8 months, 2 weeks ago

Selected Answer: B

Ref: CCNA 200-301 Official Cert Guide, Volume 2

"Chapter 1. Introduction to TCP/IP Transport and Applications

...

Flow Control Using Windowing

TCP implements flow control by using a window concept that is applied to the amount of data that can be outstanding and awaiting acknowledgment at any one point in time.

...

User Datagram Protocol

UDP provides a service for applications to exchange messages. Unlike TCP, UDP is connectionless and provides no reliability, no windowing, no reordering of the received data, and no segmentation of large chunks of data into the right size for transmission.

..."

upvoted 2 times

splashy 11 months, 1 week ago

B is 50% correct, udp sends packets individually not as a stream, fix your effing answers cisco...

upvoted 4 times

rarehunter5 1 year, 2 months ago

why not c?

upvoted 1 times

Shanku97 2 months, 1 week ago

tcp is a connection-oriented protocol

upvoted 2 times

Knobbler 1 year, 6 months ago

A little bit confusing.....in a later question it becomes clear that TCP sends as a stream....not UDP.

upvoted 1 times

nuggetbutts 2 years ago

This is a question directly from the official Cisco review book "Do I know this already" section. Unlikely an actual exam question.

upvoted 2 times

Crazey 2 years, 11 months ago

Repeating question

upvoted 1 times

Shamwedge 2 years, 2 months ago

different answers

upvoted 3 times

jerry19 2 years, 4 months ago

Repeating response.

upvoted 6 times

Question #27 *Topic 1*

What are two differences between optical-fiber cabling and copper cabling? (Choose two.)

A. A BNC connector is used for fiber connections

B. The glass core component is encased in a cladding

C. The data can pass through the cladding

D. Light is transmitted through the core of the fiber

E. Fiber connects to physical interfaces using RJ-45 connections

Correct Answer: *BD*

Community vote distribution

BD (100%)

Raymond9 Highly Voted 2 years, 9 months ago

For lazy people who hate this kind of stupid question in CCNA but has a heart of curiosity, I do some simple research for you. Please correct me if any incorrect stuffy

1.There are 3 kind of wiring mainly when we talk about networking: Fiber, Coaxial cable, twisted pair. The last 2 are Copper wiring
2. BNC Connector is for Coaxial Cable, so A is wrong
3.the structure of fiber is: Jacket encase Buffer, Buffer encase Cladding, Cladding encase core. We uses light to transmit data through the core. Therefore B and D are right, C is wrong
4. RJ45 is a connector is for twisted pair, so E is wrong

upvoted 57 times

NICE_ANSWERS 3 months, 3 weeks ago

Thank you very much Raymond.. Very helpful👌

upvoted 1 times

XBfoundX 2 years, 8 months ago

Thanks for this responses, that's help me and yes we hate this type of questions because they are meaning less. I think you do to ;) Many thanks btw

upvoted 6 times

Ali526 2 years, 8 months ago

You are right; good research.

upvoted 4 times

SScott 2 years, 5 months ago

B & D for sure. E would require a media converter

upvoted 5 times

tigertoo Most Recent 3 months, 3 weeks ago

the question makes no sense. They are not differences but features of Optical fibre cabling

upvoted 3 times

Smaritz 7 months ago

B and D.

This is not a difficult question, but it is rather poorly worded.

upvoted 1 times

BakedPotato 7 months ago

While B is a correct statement, it is not a "difference" between copper and fiber. Someone with an elementary education wrote this question.

upvoted 2 times

GreatDane 8 months, 2 weeks ago

Selected Answer: BD

Ref: Core (optical fiber) - Wikipedia

“The core of a conventional optical fiber is the part of the fiber that guides the light. It is a cylinder of glass or plastic that runs along the fiber's length. The core is surrounded by a medium with a lower index of refraction, typically a cladding of a different glass, or plastic. Light travelling in the core reflects from the core-cladding boundary due to total internal reflection, as long as the angle between the light and the boundary is greater than the critical angle.
…”

A. A BNC connector is used for fiber connections

A BNC connector is a connector used for coaxial cable networking.
Wrong answer.

B. The glass core component is encased in a cladding

Correct answer.

C. The data can pass through the cladding

Wrong answer.

D. Light is transmitted through the core of the fiber

Correct answer.

E. Fiber connects to physical interfaces using RJ-45 connections

A RJ-45 connector is a modular connector commonly used to terminate twisted pair and multi-conductor flat cable.
Wrong answer.

upvoted 1 times

leafy 2 years ago

I thought C because current passes through the outer conductor in a coaxial cable but I guess that doesn't count as cladding

upvoted 1 times

ZUMY 2 years, 5 months ago

B & D are correct

upvoted 3 times

SUKABLED 2 years, 7 months ago

i guess all OSI layeres are covered...:) Answers are correct here!

upvoted 2 times

Futchihoore 2 years, 9 months ago

Yes it is, I had this question last time

upvoted 2 times

Bach999 2 years, 9 months ago

Is this a real CCNA exam question?

upvoted 3 times

Question #28 *Topic 1*

How does CAPWAP communicate between an access point in local mode and a WLC?

A. The access point must not be connected to the wired network, as it would create a loop

B. The access point must be connected to the same switch as the WLC

C. The access point must directly connect to the WLC using a copper cable

D. The access point has the ability to link to any switch in the network, assuming connectivity to the WLC

Correct Answer: *D*

Community vote distribution

D (100%)

Shamwedge Highly Voted 2 years, 2 months ago

A, B, and C all are connection related. D is the only answer that relates to "communication"

upvoted 14 times

Alokbhai580 Most Recent 5 months ago

"B" seems correct. For option "D" on the other hand, access point does not have the ability to link to any switch in the network assuming connectivity to the WLC. CAPWAP communication between an access point in local mode and a WLC typically occurs over the wired network infrastructure using the CAPWAP protocol. The access point must be able to reach the WLC's IP address, which can be configured statically or obtained dynamically through DHCP. The access point and WLC must be on the same IP subnet or have Layer 3 connectivity between their subnets.

upvoted 4 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: D

the correct answer is option D: "The access point has the ability to link to any switch in the network, assuming connectivity to the WLC." The AP can be connected to any switch in the network, as long as the switch has connectivity to the WLC. The AP and the WLC exchange CAPWAP messages over IP, using UDP port 5246 or 5247, depending on whether the messages are encrypted.

upvoted 4 times

GreatDane 1 year, 3 months ago

Ref: Understanding Local Switching on Access Points - TechLibrary - Juniper Networks

"...
How Does Local Switching Work?

When local switching is enabled on an access point, control traffic is managed by a controller and data traffic is handled by the local switches using CAPWAP.
..."

A. The access point must not be connected to the wired network, as it would create a loop

Wrong answer.

B. The access point must be connected to the same switch as the WLC

Wrong answer.

C. The access point must directly connect to the WLC using a copper cable

Wrong answer.

D. The access point has the ability to link to any switch in the network, assuming connectivity to the WLC

Correct answer.

upvoted 2 times

ismatdmour 1 year, 6 months ago

Selected Answer: D

D is most correct and is the general case.

upvoted 2 times

ostralo 1 year, 11 months ago

ref) CCNA 200-301 Cert guide
Cisco AP Modes.
■ Local: The default lightweight mode that offers one or more functioning BSSs on a specific channel. During times that it is not transmitting, the AP will scan the other channels
to measure the level of noise, measure interference, discover rogue devices, and match

against intrusion detection system (IDS) events.

■ FlexConnect: An AP at a remote site can locally switch traffic between an SSID and a VLAN if its CAPWAP tunnel to the WLC is down and if it is configured to do so.

I think this question should be asking the FlexConnect mode not the Local mode. In this sense, D is not really right but the other options are totally wrong.

upvoted 4 times

dave1992 2 years ago

CAPWAP doesnt communicate, the communcation is called CAPWAP. its a tunnel from the core layer that terminates on the access layer.

upvoted 4 times

Nhan 2 years, 6 months ago

This is split-Mac address topic

upvoted 3 times

martco 2 years, 7 months ago

Answer D
seems to be best answer here
the Control And Provisioning of Wireless Access Points is a point to point tunnel between the AP's you deploy out in the office space and the central WLC device sitting in your datacentre

upvoted 4 times

andiks 2 years, 7 months ago

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/ap_connectivity_to_cisco_wlc.html

upvoted 2 times

LTTAM 2 years, 8 months ago

Is this topic relevant in the CCNA? No where can I find CAPWAP (in detail) in the CCNA study material. Unless if this is new material added to the CCNA.

upvoted 2 times

dave1992 2 years ago

if you are reading the study material, you will 100% read the CAPWAP section in detail. refer to Wireless Lans chapter. all of it is in there. theres no way you can read the material without seeing this.

upvoted 3 times

Raymond9 2 years, 9 months ago

not found direct reference to support answer D, but reference to reject B, see the topology of https://rscciew.wordpress.com/2014/01/22/configure-ap-groups-on-wlc/, which has one layer-2 and one layer-3 switches between WLC and AP

upvoted 2 times

SScott 2 years, 5 months ago

Yes D. Good article Raymond with eliminating B.
Here is a further reference that helps illustrate the WLC and switch topology to the local mode AP
https://www.thenetworkdna.com/2020/10/wireless-infrastructure-analysis-local.html

upvoted 2 times

sandha 2 years, 11 months ago

i need the reference for capwap

upvoted 2 times

Question #29 *Topic 1*

Which IPv6 address block forwards packets to a multicast address rather than a unicast address?

A. 2000::/3

B. FC00::/7

C. FE80::/10

D. FF00::/12

Correct Answer: *D*

Community vote distribution

D (100%)

marcojmnez Highly Voted 2 years, 6 months ago

FF <- easiest way to remember multicast.

upvoted 38 times

cormorant 10 months, 2 weeks ago

'FF <- easiest way to remember multicast.'

i'm putting this on a shirt

upvoted 8 times

boghota Highly Voted 2 years, 9 months ago

Multicast: FF00/8 -- FF00:: - FFFF::
Global Unicast: 2000::/3, 2001::/3, 2002::/4, 2001:db8::/32
Link Local Unicast: FE80::/10 -- FE80:: - FEBF::
Unique Local Unicast: FC00::/7 -- FC00:: - FDFF::
Loopback: ::1/128

Correct Answer: C

upvoted 17 times

boghota 2 years, 9 months ago

A) Global Unicast
B) Unique Local Unicast
C) Link Local Unicast
D) Multicast

upvoted 6 times

boghota 2 years, 9 months ago

Sorry I mean Correct Answer: D

upvoted 8 times

Ciscoman021 Most Recent 5 months, 3 weeks ago

Selected Answer: D

In IPv6, multicast addresses are used to send a single packet to multiple hosts simultaneously. The IPv6 address block that forwards packets to a multicast address rather than a unicast address is the FF00::/8 address block. Therefore, the correct answer is option D.

upvoted 1 times

Kane4555 1 year, 8 months ago

Selected Answer: D

D is correct. Don't get thrown off by the /12 prefix, that's FF00-FF0F, which are valid multicast addresses.

upvoted 3 times

il_pelato_di_casalbruciato 2 years, 5 months ago

All nice, but we want visual feedback

upvoted 2 times

Bibi20 1 year ago

Bel nome😂😂

upvoted 1 times

ZUMY 2 years, 5 months ago

D is correct

upvoted 3 times

nenotronix 2 years, 6 months ago

https://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=5#:~:text=Well%2Dknown%20multicast%20addresses%20have,for%20assigned%20groups%20of%20devices.

upvoted 2 times

Raymond9 2 years, 9 months ago

https://ptgmedia.pearsoncmg.com/images/chap4_9781587144776/elementLinks/04fig11_alt.jpg

upvoted 2 times

dave369 3 years, 2 months ago

I understand Timothyng's confusion but on the exam I took, it had a /12 mask as is shown here on examtopics.

upvoted 4 times

Pras86 3 years ago

so which is the correct ans?

upvoted 2 times

Timothyng 3 years, 3 months ago

The answer should be changed to FF00::/8. FF00 is correct.

upvoted 10 times

Question #30 *Topic 1*

What is the difference regarding reliability and communication type between TCP and UDP?

A. TCP is reliable and is a connectionless protocol; UDP is not reliable and is a connection-oriented protocol.

B. TCP is not reliable and is a connectionless protocol; UDP is reliable and is a connection-oriented protocol.

C. TCP is not reliable and is a connection-oriented protocol; UDP is reliable and is a connectionless protocol.

D. TCP is reliable and is a connection-oriented protocol; UDP is not reliable and is a connectionless protocol.

Correct Answer: *D*

Community vote distribution

D (100%)

Hanagaki_Shinjiro 2 weeks, 3 days ago

Selected Answer: D

There's no doubt about D is correction

upvoted 1 times

Hanagaki_Shinjiro 2 weeks, 3 days ago

There's no doubt about D is correction

upvoted 1 times

Abdulrahman94 3 months, 1 week ago

d is the right answer

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: D

Ref: Difference between TCP and UDP: Comparison in 2022 - IP With Ease

"...
Key points of difference between TCP and UDP
...
• TCP is the connection-oriented protocol while UDP is connectionless protocol.
• TCP is more reliable than UDP.
..."

A. TCP is reliable and is a connectionless protocol; UDP is not reliable and is a connection-oriented protocol.

Wrong answer.

B. TCP is not reliable and is a connectionless protocol; UDP is reliable and is a connection-oriented protocol.

Wrong answer.

C. TCP is not reliable and is a connection-oriented protocol; UDP is reliable and is a connectionless protocol.

Wrong answer.

D. TCP is reliable and is a connection-oriented protocol; UDP is not reliable and is a connectionless protocol.

Correct answer.

upvoted 4 times

braeiv123 11 months, 3 weeks ago

D is correct

upvoted 2 times

Hansain 12 months ago

Selected Answer: D

D is correct

upvoted 3 times

Kaizer5 1 year, 3 months ago

Selected Answer: D

D is correct

upvoted 2 times

kentsing 1 year, 4 months ago

D is correct

upvoted 2 times

DARKK 1 year, 4 months ago

Selected Answer: D

D is correct

upvoted 1 times

Nebulise 1 year, 7 months ago

D is correct

upvoted 1 times

mrb23 1 year, 8 months ago

D is correct

upvoted 1 times

ragekod 1 year, 11 months ago

D is correct

upvoted 1 times

Giuseppe_001 2 years, 4 months ago

D is correct

upvoted 1 times

ZUMY 2 years, 5 months ago

D is correct

upvoted 1 times

SScott 2 years, 5 months ago

D is correct

upvoted 1 times

Question #31 *Topic 1*

What are two descriptions of three-tier network topologies? (Choose two.)

A. The distribution layer runs Layer 2 and Layer 3 technologies

B. The network core is designed to maintain continuous connectivity when devices fail

C. The access layer manages routing between devices in different domains

D. The core layer maintains wired connections for each host

E. The core and distribution layers perform the same functions

Correct Answer: *AB*

Community vote distribution

AB (100%)

alexiro Highly Voted 3 years, 1 month ago

Access: Provides a connection point (access) for end-user devices. Does not forward frames between two other access switches under normal circumstances.

Distribution: Provides an aggregation point for access switches, providing connectivity to the rest of the devices in the LAN, forwarding frames between switches, but not connecting directly to end-user devices.
The distribution layer is where redistribution of routing protocols should be performed. It should never be performed at the core or access layer.

Core: Aggregates distribution switches in very large campus LANs, providing very high forwarding rates for the larger volume of traffic due to the size of the network.
Only switching between campus (distribution) switches should be performed at the core layer. Nothing should be done to slow down forwarding of traffic, such as using ACLs, supporting clients, or routing between VLANs
Core layer switches are commonly set up in a star topology. This is because core layer switches connect multiple campuses via distribution layer switches

upvoted 26 times

Ali526 2 years, 8 months ago

You have written a long story, but no answer.
AB is correct.

upvoted 44 times

Jazzy_147369 2 years, 7 months ago

I think copy and paste is more like it

upvoted 11 times

netlol Highly Voted 1 year, 7 months ago

A correct because distribution layer has multilayer switches (L2 and L3 technologies)
B correct oore provides reliability
C incorrect because it must be core layer, not access
D incorrect because it must be access layer, not core
E incorrect because core & distribution only perform same functions in 2-tier model (since they are aggregated)

upvoted 11 times

Ciscoman021 Most Recent 5 months, 3 weeks ago

Selected Answer: AB

The correct answers are A and B.

upvoted 1 times

MSTAHIR 8 months ago

AB correct.

upvoted 1 times

jnanofrancisco 8 months, 1 week ago

AB is the correct here

upvoted 1 times

Vile_Yogabear 10 months, 1 week ago

I was confused with this one because I don't normally use L3 switches at the distribution layer. However, what layer 3 function would run on the distribution layer. The routing usually happens that the core layer.

upvoted 2 times

Isuzu 4 months, 3 weeks ago

FYI: https://www.geeksforgeeks.org/2-tier-and-3-tier-architecture-in-networking/

upvoted 1 times

keokkeo_123 10 months, 2 weeks ago

Selected Answer: AB

AB is the answer

upvoted 1 times

Bram99 10 months, 3 weeks ago

A,B Is correct

upvoted 1 times

Xcape 1 year, 3 months ago

AB IS THE BEST CHOICE

upvoted 1 times

LingLingW 1 year, 8 months ago

Is that mean even the core are down but the connectivity are still flowing for statement B?

upvoted 1 times

ZUMY 2 years, 5 months ago

A&B are ok.
Core: Aggregates distribution switches in very large campus LANs, providing very high forwarding rates for the larger volume of traffic due to the size of the network.
Only switching between campus (distribution) switches should be performed at the core layer. Nothing should be done to slow down forwarding of traffic, such as using ACLs, supporting clients, or routing between VLANs
Core layer switches are commonly set up in a star topology. This is because core layer switches connect multiple campuses via distribution layer switches

upvoted 5 times

marcojmnez 2 years, 6 months ago

The Distribution Layer (1.1.2.3)
The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. In Figure 1-6, the distribution layer is the boundary between the Layer 2 domains and the Layer 3 routed network.

The core should be highly available and redundant. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly.

https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

upvoted 2 times

Question #32 *Topic 1*

Which type of IPv6 address is publicly routable in the same way as IPv4 public addresses?

A. multicast

B. unique local

C. link-local

D. global unicast

Correct Answer: *D*

Community vote distribution

D (100%)

Shaz313 Highly Voted 2 years, 2 months ago

Global unicast addresses (GUAs), also known as aggregatable global unicast addresses, are globally routable and reachable in the IPv6 Internet. They are equivalent to public IPv4 addresses. They play a significant role in the IPv6 addressing architecture

upvoted 10 times

EDO243 Most Recent 1 week, 6 days ago

D is a correct answer

upvoted 1 times

Lego_Las 4 months, 2 weeks ago

Selected Answer: D

what?! yessirr

upvoted 1 times

gugugulo 7 months ago

The type of IPv6 address that is publicly routable in the same way as IPv4 public addresses is D. global unicast.

Global unicast addresses are similar to public IPv4 addresses in that they are globally unique and can be routed on the public Internet. They are the equivalent of public IPv4 addresses and are assigned to organizations by Regional Internet Registries (RIRs). Global unicast addresses begin with the prefix 2000::/3 and are the most commonly used type of IPv6 address on the Internet.

Multicast addresses are used for one-to-many communication and are not routable in the same way as unicast addresses. Unique local addresses (ULA) are used for local communication within an organization and are not meant to be routed on the public Internet. Link-local addresses are used for communication within a local network segment and are not meant to be routed outside of the segment.

upvoted 1 times

MSTAHIR 8 months ago

D is correct

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: D

Ref: IPv6 address - Wikipedia

A. multicast

A multicast address doesn’t compare to an IPv4 public address.
Wrong answer.

B. unique local

Unique local addresses are addresses analogous to IPv4 private network addresses.
Wrong answer.

C. link-local

A link-local address is also based on the interface identifier, but uses a different format for the network prefix. The prefix field contains the binary value 1111111010. The 54 zeroes that follow make the total network prefix the same for all link-local addresses (fe80::/64 link-local address prefix), rendering them non-routable.
Wrong answer.

D. global unicast

Unicast and anycast addresses are typically composed of two logical parts: a 64-bit network prefix used for routing, and a 64-bit interface identifier used to identify a host's network interface.
Correct answer.

upvoted 2 times

Alizadeh 9 months ago

Selected Answer: D

The type of IPv6 address that is publicly routable in the same way as IPv4 public addresses is a global unicast address. Global unicast addresses are unique, globally reachable addresses that are assigned to devices that need to communicate with other devices over the Internet. They are similar to IPv4 public addresses in that they can be used to reach devices on other networks, but they are structured differently and use a different address space.

Global unicast addresses are identified by the prefix "2000::/3" and are assigned to devices by their network administrator or by an Internet service provider (ISP). They are used for communication between devices on different networks, such as between a device on a LAN and a device on the Internet.

It's important to note that global unicast addresses are not the same as link-local addresses, which are used for communication within a single network segment or link and are not intended to be routable over the Internet. Link-local addresses are identified by the prefix "FE80::/10" and are automatically generated by the device when it is connected to a network.

upvoted 1 times

ScorpionNet 1 year, 4 months ago

I agree because Global Unicast is similar to Public IPv4 addresses because they are in the same page like 2001::/64 and 209.165.202.0/30

upvoted 2 times

ragekod 1 year, 11 months ago

D is correct

upvoted 1 times

kadamske 1 year, 12 months ago

Correct answer "D"

upvoted 1 times

Harry0210 2 years, 2 months ago

D is correct

upvoted 1 times

ZUMY 2 years, 5 months ago

D is correct

upvoted 1 times

marcojmnez 2 years, 6 months ago

Global unicast: A routable address in the IPv6 Internet, similar to a public IPv4 address.

https://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=4

upvoted 3 times

Ali526 2 years, 8 months ago

D is correct.

upvoted 4 times

Question #33 *Topic 1*

What is the expected outcome when an EUI-64 address is generated?

A. The interface ID is configured as a random 64-bit value

B. The characters FE80 are inserted at the beginning of the MAC address of the interface

C. The seventh bit of the original MAC address of the interface is inverted

D. The MAC address of the interface is used as the interface ID without modification

Correct Answer: *C*

Community vote distribution

C (91%) 9%

ZUMY Highly Voted 2 years, 5 months ago

C is correct!
EUI-64 Process
01.Split Mac Address in to two (00:BB:CC | DD:11:22)
02. Insert FFFE Hexa in the middle
Eg: 00:BB:CC:DD:11:22 --> 02BB:CCFF:FEDD:1122
03.Invert the 7th Bit of the MAC address (0 to 1)
Ref:
https://geek-university.com/ccna/ipv6-eui-64-calculation/

upvoted 22 times

examcol Highly Voted 3 years, 1 month ago

C is correct. https://geek-university.com/ccna/ipv6-eui-64-calculation/

upvoted 12 times

ajuniad Most Recent 4 weeks, 1 day ago

C IS CORRECT

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: C

Ref: Understanding IPv6 EUI-64 Bit Address - Cisco Community

Post by SunilKhanna

"...
The IPv6 EUI-64 format address is obtained through the 48-bit MAC address. The MAC address is first separated into two 24-bits, with one being OUI (Organizationally Unique Identifier) and the other being NIC specific. The 16-bit 0xFFFE is then inserted between these two 24-bits for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the an EUI-48 MAC address.
...
Next, the seventh bit from the left, or the universal/local (U/L) bit, needs to be inverted. This bit identifies whether this interface identifier is universally or locally administered.
...
Once the above is done, we have a fully functional EUI-64 format address.
..."

upvoted 3 times

rick0813 11 months, 1 week ago

Selected Answer: C

a is wrong because its not random, its based on the MAC address
b is wrong because FF:FE is inserted in the middle
c is correct

upvoted 1 times

Hansain 12 months ago

Selected Answer: C

C is correct

upvoted 2 times

Vlad_Is_Love_ua 1 year ago

The EUI-64 format interface ID is derived from the 48-bit MAC address by inserting the hexadecimal number fffe between the upper 3 bytes (OUI field) and the lower 3 vendor assigned bytes of the MAC address. Then, the seventh bit of the first octet is inverted. (In a MAC address, this bit indicates the scope and has a value of 1 for global scope and 0 for local scope; it will be 1 for globally unique MAC addresses. In the EUI-64 format,

the meaning of this bit is opposite, so the bit is inverted.)
C- correct

upvoted 1 times

vuhidus 1 year, 1 month ago

Selected Answer: C

C is the answer

upvoted 2 times

GohanF2 1 year, 1 month ago

It can't be B due that the value that it's inserted in the Mac address is : FFFE. not FF80.
We use FF80 when we want to create a multicast address.

upvoted 1 times

hardwiredman 1 year, 1 month ago

Selected Answer: C

FFFE goes in the middle, then the 7th bit is inverted

upvoted 1 times

saeed_huhu 1 year, 1 month ago

Selected Answer: B

EUI-64

upvoted 1 times

onikafei 1 year, 7 months ago

Selected Answer: C

C is correct

upvoted 1 times

Shaz313 2 years, 2 months ago

EUI-64 (Extended Unique Identifier) is a method we can use to automatically configure IPv6 host addresses. An IPv6 device will use the MAC address of its interface to generate a unique 64-bit interface ID. However, a MAC address is 48 bit and the interface ID is 64 bit. What are we going to do with the missing bits?

IPv6 MAC address vs Interface ID

Here's what we will do to fill the missing bits:

We take the MAC address and split it into two pieces.
We insert "FFFE" in between the two pieces so that we have a 64 bit value.
We invert the 7th bit of the interface ID.

upvoted 4 times

Belinda 1 year, 6 months ago

Thanks for the expanciation.

upvoted 1 times

nenotronix 2 years, 6 months ago

Thanks "examcol"

upvoted 2 times

ZayaB 2 years, 7 months ago

Thanks

upvoted 2 times

Question #34 *Topic 1*

A corporate office uses four floors in a building.

☞ Floor 1 has 24 users.

☞ Floor 2 has 29 users.

Floor 3 has 28 users.

▪

☞ Floor 4 has 22 users.

Which subnet summarizes and gives the most efficient distribution of IP addresses for the router configuration?

A. 192.168.0.0/24 as summary and 192.168.0.0/28 for each floor

B. 192.168.0.0/23 as summary and 192.168.0.0/25 for each floor

C. 192.168.0.0/25 as summary and 192.168.0.0/27 for each floor

D. 192.168.0.0/26 as summary and 192.168.0.0/29 for each floor

Correct Answer: *C*

Community vote distribution

C (100%)

Bne_Pradhan Highly Voted 2 years, 3 months ago

network summary each floor,
max user to each floor=30<=2^H-2
H=5, will give N=3 therefore /27

For Network Summary,
Total Users,= 103
103<=2^H-2
H=7
will give N=1
Therefore/25,,, i hope u got ans in short, tht is C

upvoted 24 times

Danielki 1 year, 4 months ago

Where did N came from? I'm lost....

upvoted 1 times

Hanagaki_Shinjiro 1 week, 5 days ago

8-7=1 BRO

upvoted 1 times

ScorpionNet 1 year, 4 months ago

N is the Network, U is the usable host, H is the host

upvoted 2 times

Customexit Highly Voted 10 months, 4 weeks ago

write this down first thing in the exam:

/32 1
/31 2
/30 4
/29 8
/28 16
/27 32
/26 64
/25 128
/24 256
/23 512
/22 1024
/21 2048

upvoted 22 times

NICE_ANSWERS 3 months, 3 weeks ago

please, what's it's significance?

upvoted 1 times

hayo 3 months, 2 weeks ago

Number of addresses per subnet

upvoted 1 times

flash93933 8 months, 1 week ago

love you

upvoted 1 times

habbey2080 Most Recent 5 days, 13 hours ago

The answer is c

upvoted 1 times

MSTAHIR 8 months ago

total user 103, must be /25 Mask as for all floors, /27 Mask for each floor, refer to 2^5 = 32 - NW ID and Broad cast address, total usable IP 30.

upvoted 2 times

keokkeo_123 10 months, 2 weeks ago

Selected Answer: C

ccccccccccccccccc

upvoted 2 times

lock12333 1 year, 3 months ago

Selected Answer: C

ccccccccccccc

upvoted 1 times

GreatDane 1 year, 3 months ago

4 floors = 4 subnets. And you have a total of 103 users.

How many bits do you need to have 103 addresses? You need 7 bits: (2^7 – 2) = 126 addresses.
Starting from the 192.168.0.0 subnet that you're given, you must use a /25 subnet mask:

255.255.255.1xxxxxxx = 255.255.255.128

How many bits do you need to configure 4 subnets? You need 2 bits: (2^2) = 4 subnets. You have to borrow the two bits from the host ID. This way, the subnet mask, which is a /25 now, becomes a /27:

255.255.255.111xxxxx = 255.255.255.224

There are 5 bits remaining on the host ID. You have (2^5 – 2) = 30 addresses, and it fits the subnet on which you have the most users (floor 2).

You started with a 192.168.0.0/25 subnet and you ended up with a 192.168.0.0/27 subnet.
Answer C is correct.

upvoted 5 times

kentsing 1 year, 4 months ago

16 addresses per floor is not enough so 32 per floor is needed
simply count from /32=1 /31=2 /30=4...../27=32
/27 per floor is the answer

upvoted 5 times

DaveDaSpade 1 year, 3 months ago

That's how I got the answer quickly :)

upvoted 1 times

Shamwedge 1 year, 10 months ago

Subnet Mask: 128 192 224 240
Hosts: 128 64 32 16
/Cider 25 26 27 28

/27 is the smallest number that will meet the number of hosts required for all the floors

upvoted 3 times

Alibaba 2 years, 4 months ago

here should be add vlan also, in this situation question was a little misunderstand, but its cisco tricky question

upvoted 2 times

ZUMY 2 years, 5 months ago

C is correct
/27 mask will give 30 host for each subnet (2^5-2)=30

upvoted 3 times

ZUMY 2 years, 5 months ago

/25 gives us 126 maximum hosts per subnet (Total no. hosts in the building)
C. 192.168.0.0/25 as summary and 192.168.0.0/27 for each floor

upvoted 3 times

bigbux 2 years, 5 months ago

We are Keeping in mind not to waste IPs.
/27 gives us 30 maximum hosts per subnet (per floor)
/25 gives us 126 maximum hosts per subnet (Total no. hosts in the building)
C. 192.168.0.0/25 as summary and 192.168.0.0/27 for each floor

upvoted 5 times

hokieman91 2 years, 7 months ago

C. 192.168.0.0/25 as summary and 192.168.0.0/27 for each floor
This gives each floor separate networks with 30 hosts (plus network id and plus BC address).
/25 allows us to summarize the four /27 networks with 30 hosts

upvoted 2 times

admin1982 2 years, 7 months ago

C is correct. given a /27 mask

upvoted 2 times

jasten 2 years, 8 months ago

The main goal is always to make efficient use of IPs (Waste as little as possible). "B" & "D" it is not enough to cover all the users for each floor. "A" waste many IPs. In my opinion the correct answer is C, due to a /27 gives 30 usable ip per floor.

upvoted 10 times

Ali526 2 years, 8 months ago

This question does not have sufficient information to reach at a unique conclusion.

upvoted 3 times

Ali526 2 years, 7 months ago

Sorry. It does. C is correct.

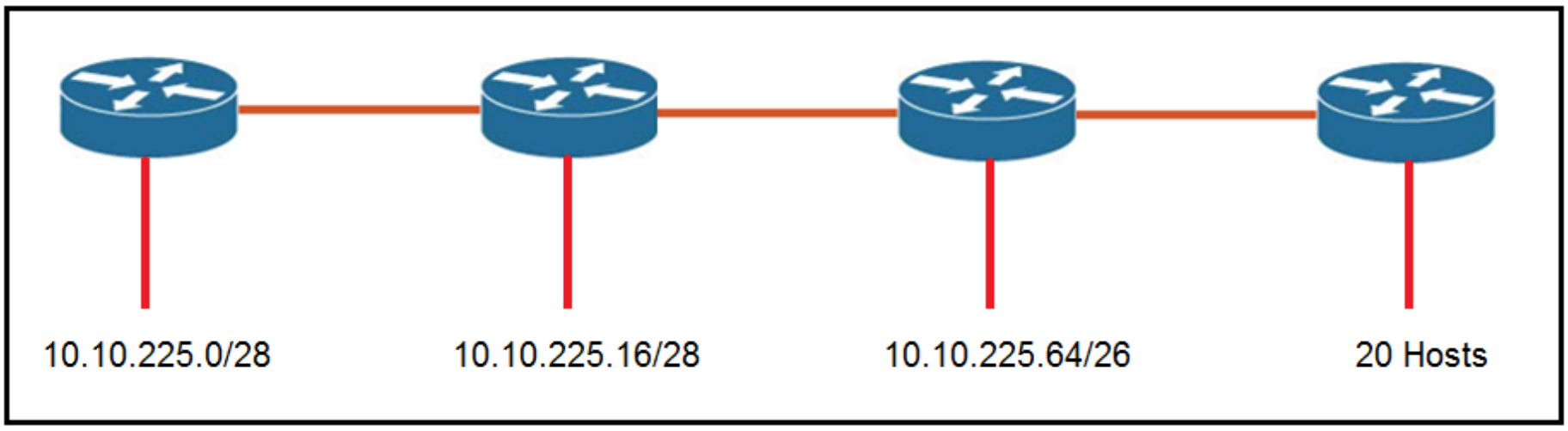
upvoted 3 times

Siegfried 1 year, 9 months ago

Not really. Chose C but in real scenario that would be really dumb thing to do as you want to have at least little bit of free IPs for scalability. That's why they completely missed /26 subnet as an option as that one would be ideal - so I clicked C of course. But in reality If I was forced - from some dumb reason - to choose from wasting some IPs and scalability I would go for scalability 100% (and choosing /25 then).

upvoted 1 times

Question #35 *Topic 1*



Refer to the exhibit. An engineer must add a subnet for a new office that will add 20 users to the network. Which IPv4 network and subnet mask combination does the engineer assign to minimize wasting addresses?

A. 10.10.225.48 255.255.255.240

B. 10.10.225.32 255.255.255.240

C. 10.10.225.48 255.255.255.224

D. 10.10.225.32 255.255.255.224

Correct Answer: *D*

Community vote distribution

D (100%)

ZUMY Highly Voted 2 years, 5 months ago

D is correct!

Find the subnet mask
*To have 20 User in a subnet We have to use /27 prefix
* So Host count for /27 prefix is (2^5-2)=30
* Subnet Mask for /27 prefix is (sum of Network bits (128+64+32)=224 , so 255.255.255.224

Find the network ID

*As per the /27 prefix each subnet has 30 host and 32 including network ID & Broadcast ID
* so first network ID is 10.10.255.0 and the second will be 10.10.255.32

upvoted 41 times

diudiuQIdama 9 months ago

I think there is a gap between the second and the third subnets, so we use .32 for the required network id, if more than 30, we need to use .64 as there are more space

upvoted 1 times

diudiuQIdama 9 months ago

Sorry .128

upvoted 1 times

suriyaprakash 1 year, 6 months ago

Thank you

upvoted 1 times

GreatDane Highly Voted 1 year, 3 months ago

A. 10.10.225.48 255.255.255.240

This is a /28 subnet. 4 bits in the host ID. You have (2^4 – 2) = 14 addresses. But you need 20 more IP addresses.
Wrong answer.

B. 10.10.225.32 255.255.255.240

This is a /28 subnet. 4 bits in the host ID. You have (2^4 – 2) = 14 addresses. But you need 20 more IP addresses.
Wrong answer.

C. 10.10.225.48 255.255.255.224

This looks like a /27 subnet. 5 bits in the host ID. You have (2^5 – 2) = 30 addresses. Could be the right answer, but there's a mismatch between the subnet ID and the subnet mask.

If you perform the logical AND between the subnet ID and the subnet mask, you should obtain the subnet ID:

Subnet ID 00001010.00001010.11111111.00110000
Subnet mask 11111111.11111111.11111111.11100000

Result 00001010.00001010.11111111.00100000

Decimal 10.10.255.32

This is not the subnet ID. Wrong answer.

D. 10.10.225.32 255.255.255.224

This is a /27 subnet. 5 bits in the host ID. You have (2^5 – 2) = 30 addresses. No mismatches between subnet ID and subnet mask. Correct answer.

upvoted 10 times

eng_sakher Most Recent 1 month, 1 week ago

D CORRECT :)
BLOCKS SIZE = 2^#OF ZEROS IN WORK OCTET 2^5=32
10.10.225.0 / 10.10.225.32 / 10.10.225.64/ 10.10.225.96 >>> ETC >>>>

upvoted 1 times

hoisin 7 months, 2 weeks ago

That is a good explanation for this question.

upvoted 1 times

HeinyHo 11 months, 4 weeks ago

Selected Answer: D

Definitely D

upvoted 2 times

bhurishravas 1 year, 9 months ago

C - write. Because D - do not contain 20 propered host`s: IP range D = 15 (63-48)

upvoted 1 times

bhurishravas 1 year, 9 months ago

I apologize)). Confuse myself!
D - write. Because C - do not contain 20 propered host`s: IP range C = 15 (63-48)

upvoted 1 times

taku03 1 year, 9 months ago

It is quite confusing especially if you are not really careful 10.10.225.48 is a host in network 10.10.225.32-10.10.225.63 as broadcast

upvoted 3 times

dave1992 1 year, 10 months ago

The keyword is which “network” technically C is a host ip and D is the network id so D is correct

upvoted 2 times

SUKABLED 2 years, 7 months ago

Simple maths - D!

upvoted 1 times

BurekMaster1 2 years, 8 months ago

Why not C?

upvoted 3 times

Roberts132 2 years, 2 months ago

It is not valid because by vlsm they are subnetting from 28 bit to 28 bit leaving a 27 bit network and finally using a 26 bit network.

upvoted 2 times

BurekMaster1 2 years, 8 months ago

got it!

upvoted 2 times

rlelliott 2 years, 7 months ago

Because 10.10.225.48 255.255.255.224 is not a valid network ID. the valid network IDs for a /27 network are 0, 32, 64, 96, 128 etc in the 4th octet.

upvoted 12 times

Ali526 2 years, 8 months ago

D is correct.

upvoted 4 times

Question #36 *Topic 1*

What is a characteristic of spine-and-leaf architecture?

A. Each link between leaf switches allows for higher bandwidth.

B. It provides greater predictability on STP blocked ports.

C. It provides variable latency.

D. Each device is separated by the same number of hops.

Correct Answer: *D*

GreatDane Highly Voted 1 year, 3 months ago

Ref: Cisco Data Center Spine-and-Leaf Architecture: Design Overview White Paper – Cisco

"...
Spine-and-leaf architecture
...
With a spine-and-leaf architecture, no matter which leaf switch to which a server is connected, its traffic always has to cross the same number of devices to get to another server (unless the other server is located on the same leaf).
..."

A. Each link between leaf switches allows for higher bandwidth.

Wrong answer.

B. It provides greater predictability on STP blocked ports.

Wrong answer.

C. It provides variable latency.

Wrong answer.

D. Each device is separated by the same number of hops.

Correct answer.

upvoted 9 times

ajuniad Most Recent 4 weeks, 1 day ago

A. Each link between leaf switches allows for higher bandwidth.
The spine-and-leaf architecture is a network topology commonly used in data centers to provide high bandwidth, low latency, and scalability. In this architecture, network switches are organized into two layers: the spine layer and the leaf layer.

In a spine-and-leaf architecture, each leaf switch is connected to every spine switch, and the connections between these switches provide high bandwidth. This is in contrast to traditional network topologies like hierarchical designs, where not all devices are directly connected to each other.

The statement "Each link between leaf switches allows for higher bandwidth" is correct because every leaf switch is connected to every spine switch, forming multiple parallel paths for data to travel between devices. This arrangement ensures that the available bandwidth is effectively aggregated and distributed across all the links, resulting in increased overall network capacity.

upvoted 1 times

Ryan2theGuy 2 months, 1 week ago

From what I understand A) but I'm open to opinions
Spine-and-leaf architecture is a type of network topology in which switches are arranged in a leaf layer that connects to a spine layer. The spine layer acts as the core of the network, while the leaf layer provides access to endpoints such as servers or storage devices. A characteristic of this architecture is that it allows for high bandwidth and low latency, as well as scalability and flexibility in adding or removing leaf switches.

upvoted 1 times

jonathan126 4 months, 3 weeks ago

A - Incorrect since leaf switches do not connect to each other
B - Incorrect. It might help a bit on the port role due to uniform structure, but the blocked ports still depends on the MAC address, so different MAC address will affect the blocked ports -> not predictable
C - incorrect. I think the latency would be quite predictable as the hop count is uniform. The latency will also affect by the transmission medium and has nothing to do with the LAN architecture.
D - Each "end" device is separated by the same number of hops would be better, as hop count between leaf switch is 2 but hop count between leaf and spine switch is 1.
Correct me if I am wrong..

upvoted 2 times

ManKilla 2 years ago

D is the answer because Leaf switches do not connect each other

upvoted 2 times

Shaz313 2 years, 2 months ago

A solution that has been proposed is a spine and leaf topology, a topology that ensures that all devices are the same number of network hops away, thereby providing predictable and consistent network latency.

upvoted 4 times

ZUMY 2 years, 5 months ago

D is correct!

Find the subnet mask
*To have 20 User in a subnet We have to use /27 prefix
* So Host count for /27 prefix is (2^5-2)=30
* Subnet Mask for /27 prefix is (sum of Network bits (128+64+32)=224 , so 255.255.255.224

Find the network ID

*As per the /27 prefix each subnet has 30 host and 32 including network ID & Broadcast ID
* so first network ID is 10.10.255.0 and the second will be 10.10.255.32

upvoted 4 times

ZUMY 2 years, 5 months ago

Moderator Please delete this comment.

upvoted 11 times

IxlJustinlxl 2 years, 4 months ago

^^ for Q35

upvoted 2 times

admin1982 2 years, 7 months ago

D is correct.

upvoted 3 times

jasten 2 years, 8 months ago

There are no direct links between leaf nor between spine

upvoted 3 times

Miskoolak 3 years ago

Correct answer is "A"
bc. of absence of stp all links are active and pass the traffic .

upvoted 1 times

smote 2 years, 11 months ago

But there are no direct links between leaf switches, so D is correct.

upvoted 8 times

Chenet 2 years ago

no, you are wrong mate

upvoted 1 times

Question #37 *Topic 1*

An office has 8 floors with approximately 30-40 users per floor. One subnet must be used. Which command must be configured on the router Switched Virtual
Interface to use address space efficiently?

A. ip address 192.168.0.0 255.255.0.0

B. ip address 192.168.0.0 255.255.254.0

C. ip address 192.168.0.0 255.255.255.128

D. ip address 192.168.0.0 255.255.255.224

Correct Answer: *B*

Community vote distribution

B (100%)

GreatDane Highly Voted 1 year, 3 months ago

8 floors and 40 user per floor means 320 users (approx.). How many bits do you need to have 320 IP addresses?

8 bits = (2^8 – 2) =254 IP addresses, and it's not enough.
9 bits = (2^9 – 2) = 510 IP addresses, and this is enough.

You have a class C subnet (192.168.0.0). This means a subnet mask like this:

255.255.255.0

But you need 9 bits for the hosts, so you've got left with a subnet mask like this:

255.255.1111111x.xxxxxxxx =255.255.254.0

This means you will use VLSM subnetting.
Answer B is correct.

upvoted 42 times

bikila123 1 month, 2 weeks ago

very good explanation!!!

upvoted 2 times

HMaw 11 months, 1 week ago

Reading your explain make me hearing Jeremy voice saying "Save the hosts". Nicely done.

upvoted 8 times

re__roy 12 months ago

Well explained brother

upvoted 1 times

AKA1987 Highly Voted 2 years ago

40*8<=2^H-2, will give H=9 which is a /23 OR 255.255.254.0 = Answer B

upvoted 9 times

HakamCnna 1 year, 3 months ago

how you give H=9 .?

upvoted 2 times

Freitas512 Most Recent 1 week ago

Selected Answer: B

To get a subnet to support 40 users we need at least 6 bits. 32-6 = /26
but we want to be able to get 8 different subnets so we need 3 more bits.
/26-3 = /23 .
We just need to find the subnet mask of /23

upvoted 1 times

blackcisco 1 month, 3 weeks ago

B is correct because i quote "One subnet must be used" one subnet is needed for all 8 floors and only A and B provide this with B uses must less address space

upvoted 1 times

Naetan0809 4 months, 2 weeks ago

8 FLOORS = 8 SUBNET
"APPROX" 30-40 USERS = HOST NEEDED
192.168.0.0 = Old Subnet Mask =/24

8 SUBNET= 2,4,8 = 3 BITS BORROWED

NewSubnetMask= OldSubnetMask + BITS BORROWED = 24+3 = 27

USABLE HOST = 2^(32-NSM)- 2 =2^(32-27) - 2 = 30 USABLE HOST

With "192.168.0.0 255.255.255.224" we have 8 subnets:
- + First subnet: 192.168.0.0 to 192.168.0.31
- + Second subnet: 192.168.0.32 to 192.168.0.63
- + Third subnet: 192.168.0.64 to 192.168.0.95
- + Fourth subnet: 192.168.0.96 to 192.168.0.127
- + Fifth subnet: 192.168.0.128 to 192.168.0.159
- + Sixth subnet: 192.168.0.160 to 192.168.0.191
- + Seventh subnet: 192.168.0.192 to 192.168.0.223
- + Eighth subnet: 192.168.0.224 to 192.168.0.255

upvoted 1 times

timtgh 7 months ago

They most likely meant one subnet per floor, not just one big subnet for the whole office. It's a judgement call. They didn't say "per floor," but they often word things poorly, and that is probably what they meant. If the whole office is one subnet, then it's a flat network and no subnetting is needed at all, and the mask doesn't matter.

upvoted 1 times

oatmealturkey 6 months, 3 weeks ago

But subnetting is still needed if they want only one subnet, because with their allocated Class C address that we can see in the answer choices, they do not have enough space for that many hosts on a single subnet.

upvoted 2 times

Maycao 8 months ago

Correct

upvoted 1 times

Vile_Yogabear 10 months, 1 week ago

I managed to solve it by I didn't like the way I did it.

8 x 40 = 320 hosts
I manually tried to find which subnet can support this many hosts.

512, 254, 128, 64, 32, 16,8 , 4, 2, 1
If a /24 can support 254 - 2 hosts then
/23 can support 512 - 2 hosts so its must be a /23 network.
I just counted the subnet my memorizing the numbers
128, 192, 224,240,248, 252,254, 255
/17, /18, /19, /20, /21, /22, /23, /24
So the subnet mask for /23 is 255.255.254.0

upvoted 2 times

keokkeo_123 10 months, 2 weeks ago

Selected Answer: B

BBBBBBB

upvoted 1 times

Vishalb86 1 year, 8 months ago

For a class C network, the default subnet mask is 255.255.255.0. In CIDR the lowest is a /25 which supports 126 hosts. To answer this question there is supposed to be a class B address with a subnet mask of 255.255.254.0 or /23 which will support 9 subnets and 510 host.

upvoted 2 times

Hodicek 1 year, 10 months ago

Sorry B is the correct answer as 8 X40 = 320 so it should to be B not C

upvoted 2 times

Hodicek 1 year, 10 months ago

Answer is C

upvoted 1 times

SScott 2 years ago

It's between A and B. B /23 waste less addresses and there are plenty of subnets to cover the host address range per floor.
C /25 255.255.255.128 does not work. Insufficient floor coverage with subnet range.
D /27 255.255.255.224 will work for 30 users per all eight floors but not when staffing is 31 up to 40 users per floor at times.

upvoted 2 times

Bne_Pradhan 2 years, 3 months ago

40*8<=2^H-2, will give H=8
hence in between A and B, but As A will waste lot of addresses, correct will be B

upvoted 2 times

Bne_Pradhan 2 years, 3 months ago

i suppose B was meant to be 255.255.255.0,, but in anyways thts the most favoured ans

upvoted 1 times

Shamwedge 2 years, 2 months ago

No. 255.255.254.0 is correct. 256 = /24 but you need to use at least 512 to cover the 320 users. 512 hosts is /23 and 255.255.254.0 is the subnet mask for /23

upvoted 10 times

Adaya 2 years, 2 months ago

Thanks for your explanation

upvoted 2 times

Doad 2 years, 3 months ago

Answer must be 255.255.255.128 as at last octet bits will 10000000-- only then it can occupy 40 hosts otherwise not.

upvoted 4 times

Heymannicerouter 2 years ago

That would be correct if the question said one subnet per floor, however since it's only one in total, you need a subnet that covers at least 320 users, therefore B is correct.

upvoted 2 times

timtgh 7 months ago

As stated above, the question probably did mean per floor, and they just worded it badly. There's no way to know for sure.

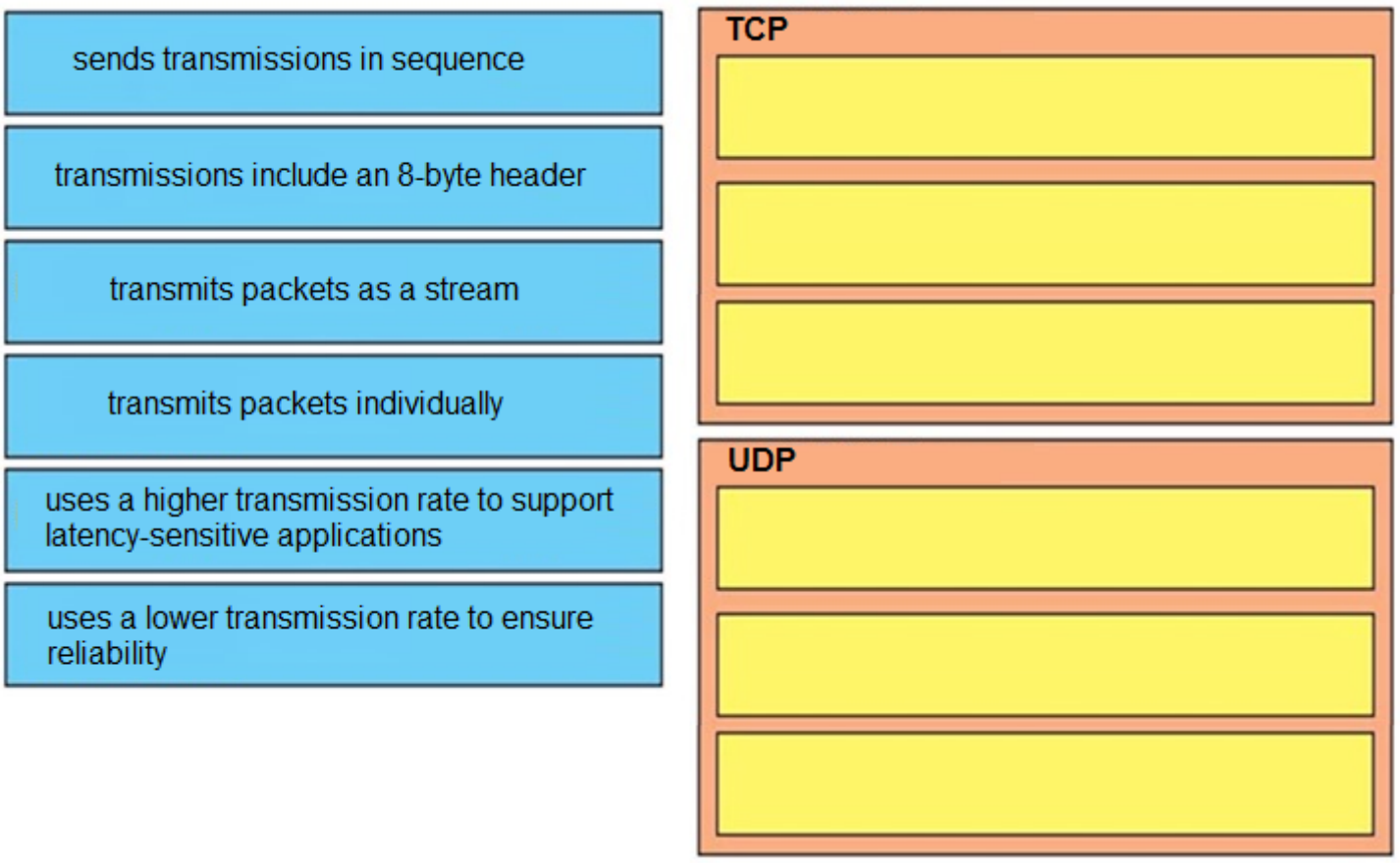
upvoted 1 times

Question #38 *Topic 1*

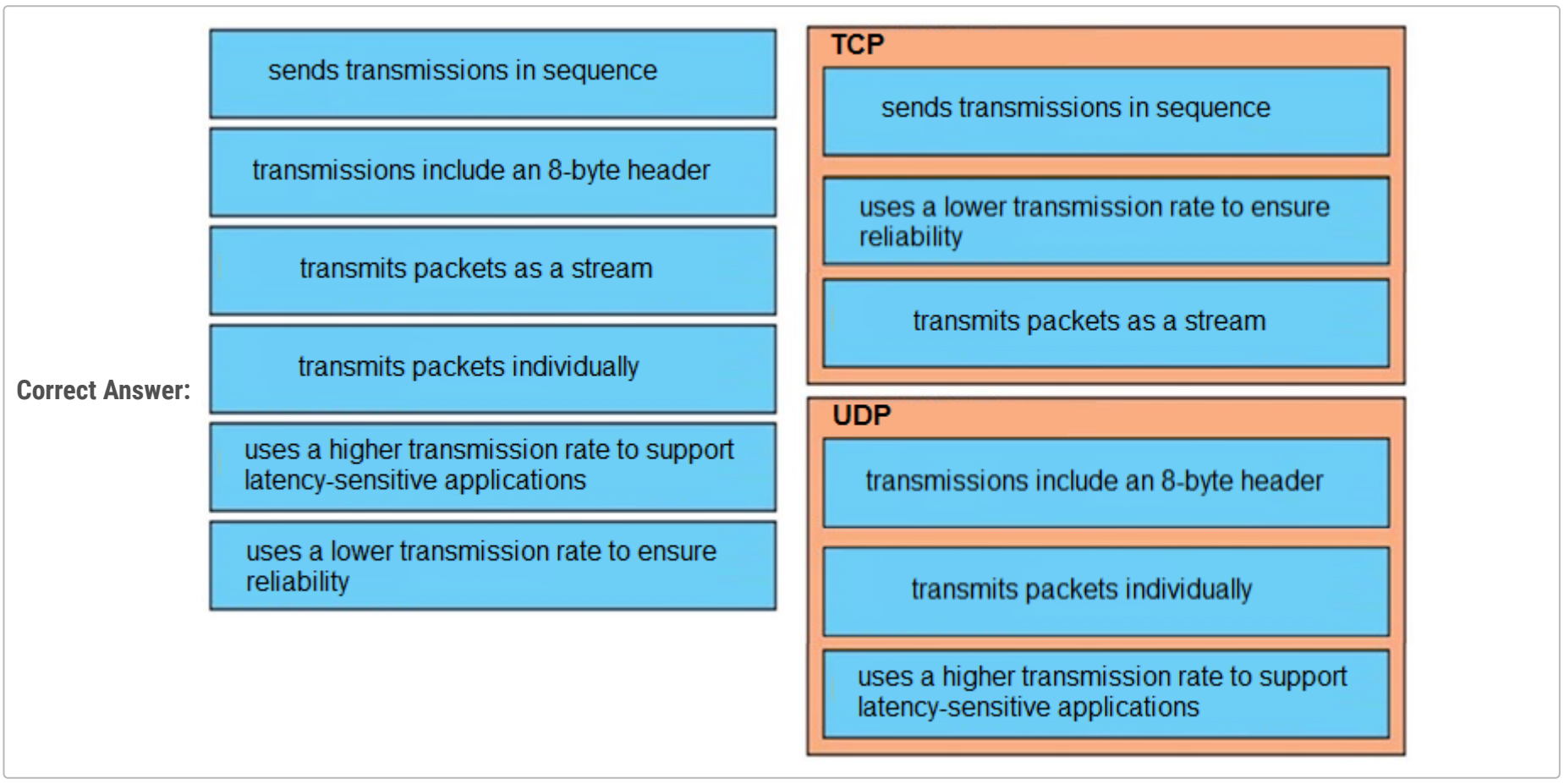
DRAG DROP -

Drag and drop the descriptions of IP protocol transmissions from the left onto the IP traffic types on the right.

Select and Place:



Correct Answer:



Racaine Highly Voted 2 years, 8 months ago

error on the answer, transmits a packets as a stream is UDP fonction not TCP

upvoted 33 times

HippoMonarch 6 days, 7 hours ago

TCP indeed transmits data as an ordered, flow-controlled "stream," whereas UDP sends each data packet individually and without sequencing, more like a "stream" of independent packets rather than a true "stream."

upvoted 2 times

rlelliott 2 years, 7 months ago

"Stream Versus Packet — TCP/IP is a stream-oriented protocol, while UDP is a packet-oriented protocol. This means that TCP/IP is considered to be a long stream of data that is transmitted from one end of the connection to the other end, and another long stream of data flowing in the opposite direction." https://www.mathworks.com/help/instrument/tcpip-and-udp-comparison.html#:~:text=Stream%20Versus%20Packet%20%E2%80%94%20TCP%2FIP,flowing%20in%20the%20opposite%20direction.

upvoted 20 times

amrith501 2 years, 8 months ago

Answers are correct
https://www.vpnmentor.com/blog/tcp-vs-udp/#:~:text=TCP%20sends%20out%20a%20stream,individual%20packets%20possess%20proper%20boundaries

upvoted 9 times

SScott 2 years, 5 months ago

Yes, good link with highlight. Answers are correct.
TCP is reliable and the transmission is a stream. UDP is unreliable because the packets are sent individually with no recovery nor acknowledgement which help provide the higher transmission rate.

upvoted 7 times

ProgSnob 1 year, 10 months ago

If you've ever used Wireshark you would know that viewing a TCP stream is an important part of troubleshooting.

upvoted 5 times

itsmeJB Most Recent 2 weeks, 3 days ago

Do we really need to answer it in this order?

upvoted 1 times

aymanmk 2 months ago

stream it was for udp

upvoted 1 times

MadKisa 2 months ago

It is not, read previous comments

upvoted 2 times

Shabeth 2 months, 1 week ago

this is the answer from question#26., its just confusing
B. TCP provides flow control to avoid overwhelming a receiver by sending too many packets at once, UDP sends packets to the receiver in a continuous stream without checking.

upvoted 1 times

Dunedrifter 2 months, 2 weeks ago

Given answers are correct.

upvoted 1 times

no_blink404 3 months ago

TCP/IP is a stream-oriented protocol, while UDP is a packet-oriented protocol. Suggested Answer is correct.

upvoted 2 times

ProgSnob 8 months, 2 weeks ago

TCP is considered a stream. It does send packets individually but it sends them continually until the stream of data is completed. UDP sends packets individually in an unorganized manner while a stream is a continuous flow. I don't think of a flow when I think of UDP.

upvoted 1 times

Dante_Dan 1 year, 7 months ago

For the TCP/UDP - stream discussion:
Extracted directly from the Official Cert Guide CCNA 200-301 Volume 2 Page 7 Table 1-2:
It mentions some of the features that TCP has:
Ordered data transfer and data segmentation.- Continuous stream of bytes from an upper-layer process that is "segmented" for transmission and delivered to upper-layer processes at the receiving device, with the bytes in the same order

upvoted 1 times

adli1984 1 year, 9 months ago

TCP/IP is a stream-oriented protocol, while UDP is a packet-oriented protocol

upvoted 1 times

dabears 1 year, 10 months ago

To get this answer correct on the exam do the answers provided have to be in this order? For instance, TCP - sends transmissions in sequence, use a lower transmission rate to ensure reliability, transmits packets as a stream. Any order will give you the correct answer?

upvoted 2 times

coolapple 1 year, 11 months ago

answers are up to scratch

upvoted 1 times

Duketernity 2 years, 1 month ago

using the windowing technique of TCP, it allows a stream of packets to be trafficked at once..in the event a packet within the stream drops or is lost, the sequencing of the TCP will allow the packet to be resent as the packet sequence will not be acknowledged. So answer is correct. TCP packets are streamed within the allowable window.

upvoted 2 times

ZUMY 2 years, 5 months ago

Given answers are correct

upvoted 2 times

Robin999 2 years, 6 months ago

Answers are correct

upvoted 2 times

Question #39 *Topic 1*

A device detects two stations transmitting frames at the same time. This condition occurs after the first 64 bytes of the frame is received. Which interface counter increments?

A. runt

B. collision

C. late collision

D. CRC

Correct Answer: *C*

Community vote distribution

B (67%) C (33%)

Raooff Highly Voted 2 years, 8 months ago

C is right
Collision happens after 512 bits =64 byte =late collision
upvoted 19 times

initialdg 1 month, 4 weeks ago

Thanks for confirming
upvoted 1 times

oooMooo Highly Voted 2 years, 4 months ago

Collision occurs in the first 64 bytes
A late collision occurs after the 512th bit (64th byte) of a frame has been transmitted by a device.
Anything under 64byte frame is considered a runt.
upvoted 15 times

picho707 Most Recent 1 month ago

late collisions are not about detecting collisions after receiving a specific amount of data within a frame, but rather about detecting collisions that occur after a certain time has passed since the start of the frame transmission.
upvoted 2 times

Dunedrifter 2 months, 2 weeks ago

Selected Answer: B

A late collision is a collision that occurs after the first 64 bytes of the frame have been transmitted. Late collisions typically indicate a problem with the network, such as excessive cable length or a misconfiguration. However, In this scenario, the collision is detected after the first 64 bytes of the frame have been received, not transmitted. Therefore, it is not considered a late collision.
upvoted 3 times

mda2h 2 months, 3 weeks ago

C is right.

"To allow collision detection to work properly, the period in which collisions are detected is restricted (512 bit-times). For Ethernet, this is 51.2us (microseconds), and for Fast Ethernet, 5.12us. For Ethernet stations, collisions can be detected up to 51.2 microseconds after transmission begins, or in other words up to the 512th bit of the frame.

When a collision is detected by a station after it has sent the 512th bit of its frame, it is counted as a late collision."

https://www.cisco.com/c/en/us/support/docs/interfaces-modules/port-adapters/12768-eth-collisions.html#topic4
upvoted 1 times

dsolaide 3 months, 3 weeks ago

Selected Answer: B

Ethernet interfaces often have a general collision counter that increments whenever collisions are detected. This collision counter tracks the total number of collisions that occur during the transmission of frames. It does not differentiate between early collisions (which occur at the beginning of frame transmission) and late collisions (which occur after a specific point).
upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: C

Ref: Late collision errors - Cisco Community

Post by okopp

“i think, that late collisions are caused collisions after first 64 bytes,this mean that the cable is too long. You could check cable length”

A. runt

Wrong answer.

B. collision

Wrong answer.

C. late collision

Correct answer.

D. CRC

Wrong answer.

upvoted 1 times

Alizadeh 9 months ago

Selected Answer: C

If a device detects two stations transmitting frames at the same time after the first 64 bytes of the frame is received, this is an indication of a collision on the network. When a collision occurs, the device's interface counter for collisions will increment.

The collision counter is a metric that is used to track the number of collisions that occur on a network interface. It is one of several counters that can be used to monitor the performance of a network interface and identify potential problems. Other counters that may be used to monitor the performance of a network interface include counters for transmitted and received frames, errors, and discards.

If the collision counter is consistently high, it may indicate that there is a problem with the network, such as a high level of contention for network resources or a configuration issue. In this case, it may be necessary to troubleshoot the issue and take steps to reduce the number of collisions on the network. This could involve optimizing network configuration, adding additional network resources, or implementing other strategies to improve network performance.

upvoted 1 times

Japucip12 1 year, 11 months ago

Hate this question, since a spanish native speaker I am, always get confuse with "after" and "before" - that leads me to give the wrong answer

upvoted 7 times

AiR1994 1 week ago

As a spanish native speaker that happens to me as well. Just think on what happens when a party ends? yes, the AFTER-party ... lol

upvoted 1 times

aferiver 2 months, 2 weeks ago

Think about "Afterhour" xD

upvoted 1 times

mariodesa 1 year, 8 months ago

Whenever you come across this, remember Adobe's "After Effects" post-production software. It is used "after" the video is recorded, not "before". :)

upvoted 3 times

ZUMY 2 years, 5 months ago

C is correct

upvoted 3 times

Aval0n1 2 years, 6 months ago

C is correct
https://www.cisco.com/c/en/us/support/docs/interfaces-modules/port-adapters/12768-eth-collisions.html

upvoted 4 times

Raymond9 2 years, 9 months ago

"If the distance between two transmitting stations exceeds the particular Ethernet specification, the stations might not become aware soon enough that another station already has control of the wire. The resulting collision of signals results in a data packet that is more than 64 bytes in length, which is allowable but which contains cyclical redundancy check (CRC) errors, resulting in unreliable communication."
Ref: https://networkencyclopedia.com/late-collision/

So it seems to have CRC incremented as well?

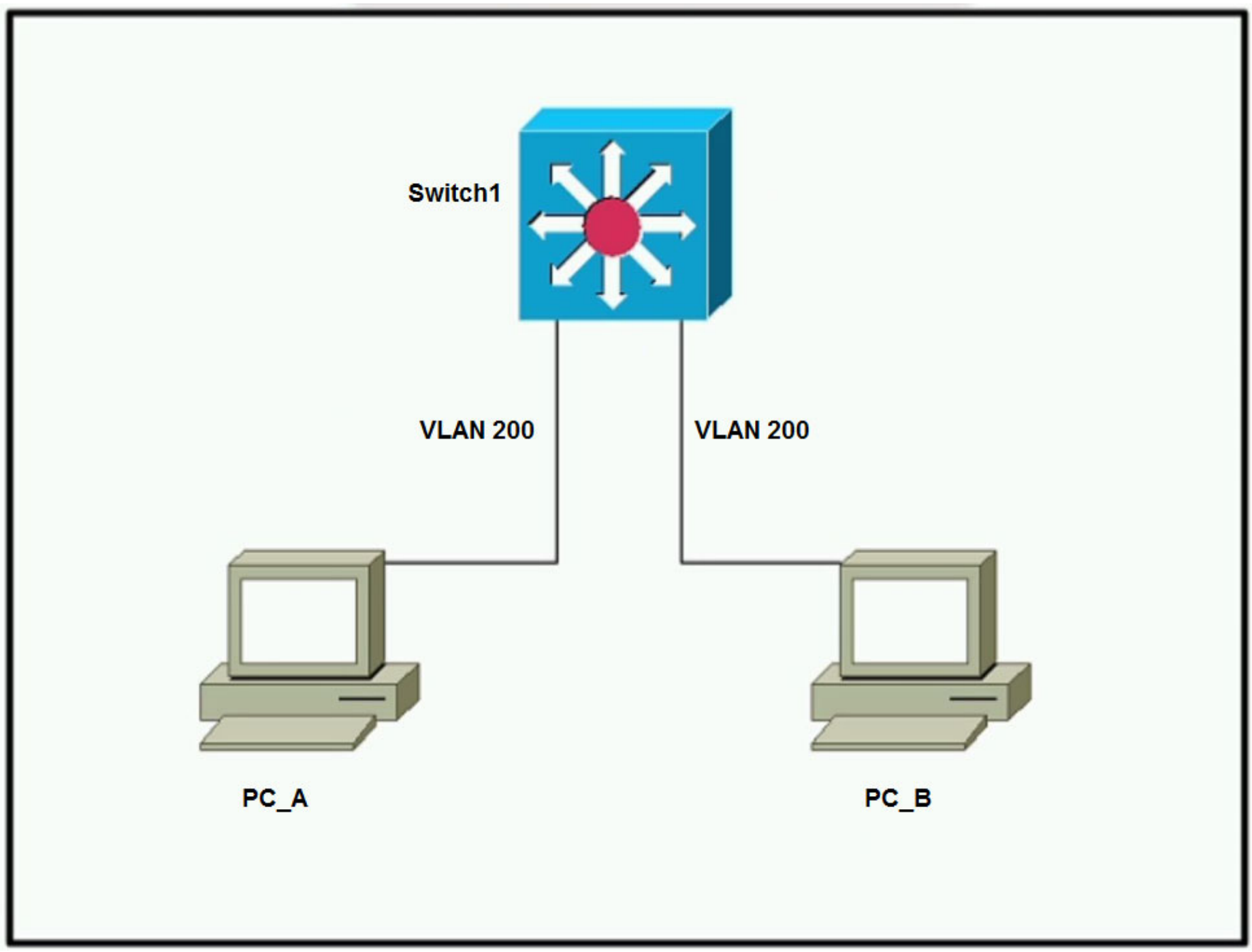
upvoted 4 times

SScott 2 years, 5 months ago

C is right. That is true CRC is also a counter to consider. However, the 64 bytes (512 bits) would relate specifically with a late collision. The late-col counter corresponds mainly with a duplex speed mismatch rather than defective cabling, card or corruption issue with transmission and CRC errors.

upvoted 2 times

Question #40 *Topic 1*



Refer to the exhibit. Which outcome is expected when PC_A sends data to PC_B after their initial communication?

A. The source MAC address is changed.

B. The destination MAC address is replaced with ffff.ffff.ffff.

C. The source and destination MAC addresses remain the same.

D. The switch rewrites the source and destination MAC addresses with its own.

Correct Answer: *C*

Cyberops Highly Voted 1 year, 4 months ago
key work is after their initial communication
upvoted 19 times

laurvy36 1 year, 3 months ago
good point noted
upvoted 2 times

GreatDane Highly Voted 1 year, 3 months ago
You have a TCP/IP network. This means that PC A and PC B have an IP address each. PC A knows PC B's address and creates an IP packet for PC B. Then, the packet (Layer 3) becomes an Ethernet frame (Layer 2): PC A gets PC B's MAC address and uses it as the destination L2 address.

When the frame arrives at SW1, the switch looks at the destination MAC address and controls (in its MAC table) to which port that address is associated. Then, the switch sends the frame to PC B through that port (forwarding phase).

The switch leaves unchanged BOTH the source and the destination MAC addresses inside the frame.
Answer C is correct.
upvoted 14 times

Question #41 *Topic 1*

Using direct sequence spread spectrum, which three 2.4-GHz channels are used to limit collisions?

A. 5, 6, 7

B. 1, 2, 3

C. 1, 6, 11

D. 1, 5, 10

Correct Answer: *C*

Community vote distribution

C (100%)

1234Rob5678 Highly Voted 2 years, 5 months ago

C. 1,6,11 is correct. Question poorly worded, collisions happen in a wired network, congestion happens in a wireless network.

upvoted 8 times

Ali526 Highly Voted 2 years, 8 months ago

C is correct. 1,6,11 don't overlap.

upvoted 6 times

habbey2080 Most Recent 5 days, 13 hours ago

1,6,11

upvoted 1 times

eng_sakher 1 month, 1 week ago

1+6+11 :) ♥
C IS CORRECT

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: C

Ref: Channel Planning Best Practices - Cisco Meraki

"...
802.11 RF Spectrum

2.4 GHz

The 802.11 standard defines fourteen 20MHz wide channels in the 2.4 GHz industrial, scientific, and medical (ISM) band. Wireless devices specified as 802.11b/g/n are capable of operating within this band. The channels available within different countries/regions is dictated by local governing authorities. In the United States, channels 1 through 11 are permitted. This provides three non-overlapping channels 1, 6 and 11.
..."

A. 5, 6, 7

Wrong answer.

B. 1, 2, 3

Wrong answer.

C. 1, 6, 11

Correct answer.

D. 1, 5, 10

Wrong answer.

upvoted 1 times

Alizadeh 9 months ago

Selected Answer: C

In the 2.4 GHz frequency band, the three channels that are commonly used to limit collisions when using direct sequence spread spectrum (DSSS) are channels 1, 6, and 11. These channels are spaced far enough apart in the spectrum to minimize the likelihood of interference between devices operating on different channels.

DSSS is a spread spectrum technique that is used to reduce the impact of interference on wireless communication. It involves spreading the data signal over a wide frequency band by modulating the data with a high-frequency code, or "chipping" code. This chipping code is used to spread

the signal over a wide frequency range, making it less vulnerable to interference and more resistant to noise.

By using DSSS and selecting channels 1, 6, and 11, it is possible to limit collisions and improve the performance of the wireless network. It's important to note, however, that other factors, such as the number of devices on the network, the type of devices, and the distance between devices, can also impact the performance of the network and may require additional strategies to optimize network performance.

upvoted 4 times

cormorant 10 months, 2 weeks ago

2.4 Ghz uses 5-hop metrics for limiting collisions

upvoted 2 times

keokkeo_123 10 months, 2 weeks ago

Selected Answer: C

CCCCCCCC

upvoted 1 times

ZUMY 1 year, 4 months ago

1,6,11 is correct

upvoted 1 times

Gaurabdon 1 year, 4 months ago

Depends on the region/country where you are residing but most commonly it is 1, 6 and 11.

upvoted 1 times

1234Rob5678 2 years, 5 months ago

congestion and interference happen in a wireless network

upvoted 2 times

marcojmnez 2 years, 6 months ago

1, 6, 1

https://www.sciencedirect.com/topics/engineering/direct-sequence-spread-spectrum

upvoted 3 times

Question #42 *Topic 1*

How do TCP and UDP differ in the way they guarantee packet delivery?

A. TCP uses retransmissions, acknowledgment, and parity checks, and UDP uses cyclic redundancy checks only

B. TCP uses two-dimensional parity checks, checksums, and cyclic redundancy checks, and UDP uses retransmissions only

C. TCP uses checksum, acknowledgements, and retransmissions, and UDP uses checksums only

D. TCP uses checksum, parity checks, and retransmissions, and UDP uses acknowledgements only

Correct Answer: *C*

Community vote distribution

C (100%)

GreatDane 8 months, 2 weeks ago

Selected Answer: C

Ref: TCP vs UDP - Difference and Comparison | Diffen

"...
Comparison chart
...
Error Checking

TCP does error checking and error recovery. Erroneous packets are retransmitted from the source to the destination.

UDP does error checking but simply discards erroneous packets. Error recovery is not attempted.
..."

A. TCP uses retransmissions, acknowledgment, and parity checks, and UDP uses cyclic redundancy checks only

Wrong answer.

B. TCP uses two-dimensional parity checks, checksums, and cyclic redundancy checks, and UDP uses retransmissions only

Wrong answer.

C. TCP uses checksum, acknowledgements, and retransmissions, and UDP uses checksums only

Correct answer

D. TCP uses checksum, parity checks, and retransmissions, and UDP uses acknowledgements only

Wrong answer.

upvoted 2 times

keokkeo_123 10 months, 2 weeks ago

Selected Answer: C

CCCCCCCCCc

upvoted 3 times

Jackie_Manuas12 1 year, 6 months ago

C is the only answer that makes sense. "Parity checks" isn't mentioned in the OCG.

upvoted 3 times

reagan_donald 1 year, 7 months ago

Selected Answer: C

100% is correct

upvoted 2 times

ZUMY 2 years, 5 months ago

C is correct

upvoted 3 times

AvalOn1 2 years, 6 months ago

C is right. UDP has only checksums
https://en.wikipedia.org/wiki/User_Datagram_Protocol#Checksum_computation

upvoted 3 times

dave1992 1 year, 10 months ago

C. TCP uses checksum, acknowledgements, and retransmissions, and UDP uses checksums only

explain yourself.

upvoted 2 times

Question #43 *Topic 1*

A wireless administrator has configured a WLAN; however, the clients need access to a less congested 5-GHz network for their voice quality. Which action must be taken to meet the requirement?

A. enable Band Select

B. enable DTIM

C. enable RX-SOP

D. enable AAA override

Correct Answer: *A*

Community vote distribution

A (100%)

GreatDane Highly Voted 8 months, 2 weeks ago

Selected Answer: A

Ref: Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Gibraltar 16.12.x

"C H A P T E R 47

Information About Configuring Band Selection, 802.11 Bands, and Parameters

Band Select

Band select enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the device.
..."

A. enable Band Select

Correct answer

B. enable DTIM

Wrong answer.

C. enable RX-SOP

Wrong answer.

D. enable AAA override

Wrong answer.

upvoted 7 times

Goh0503 Most Recent 10 months, 3 weeks ago

A is Correct
https://community.cisco.com/t5/wireless-mobility-knowledge-base/load-balancing-and-band-select-on-the-cisco-wireless-lan/ta-p/3128513#:~:text=You%20can%20use%20this%20feature%20to%20combat%20these%20sources%20of%20interference%20and%20improve%20overall%20network%20performance

upvoted 2 times

kalistro 1 year, 7 months ago

A is correct,
https://rscciew.wordpress.com/2014/10/26/cisco-band-select-feature/#:~:text=We%20can%20configure%20this%20feature,applications%20(Like%3A%20Voice).

upvoted 4 times

kalistro 1 year, 7 months ago

reewrewrwe

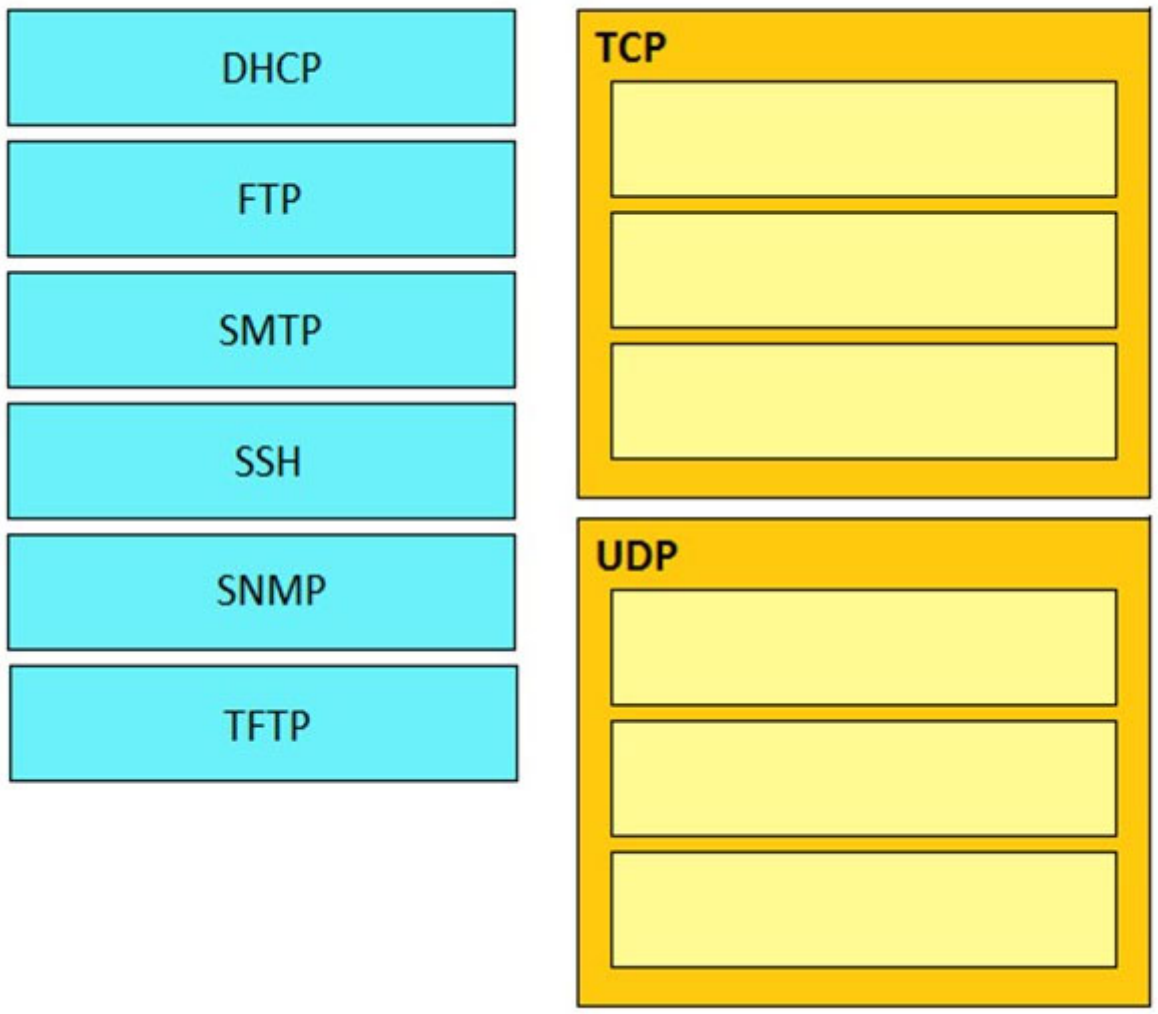
upvoted 2 times

Question #44 *Topic 1*

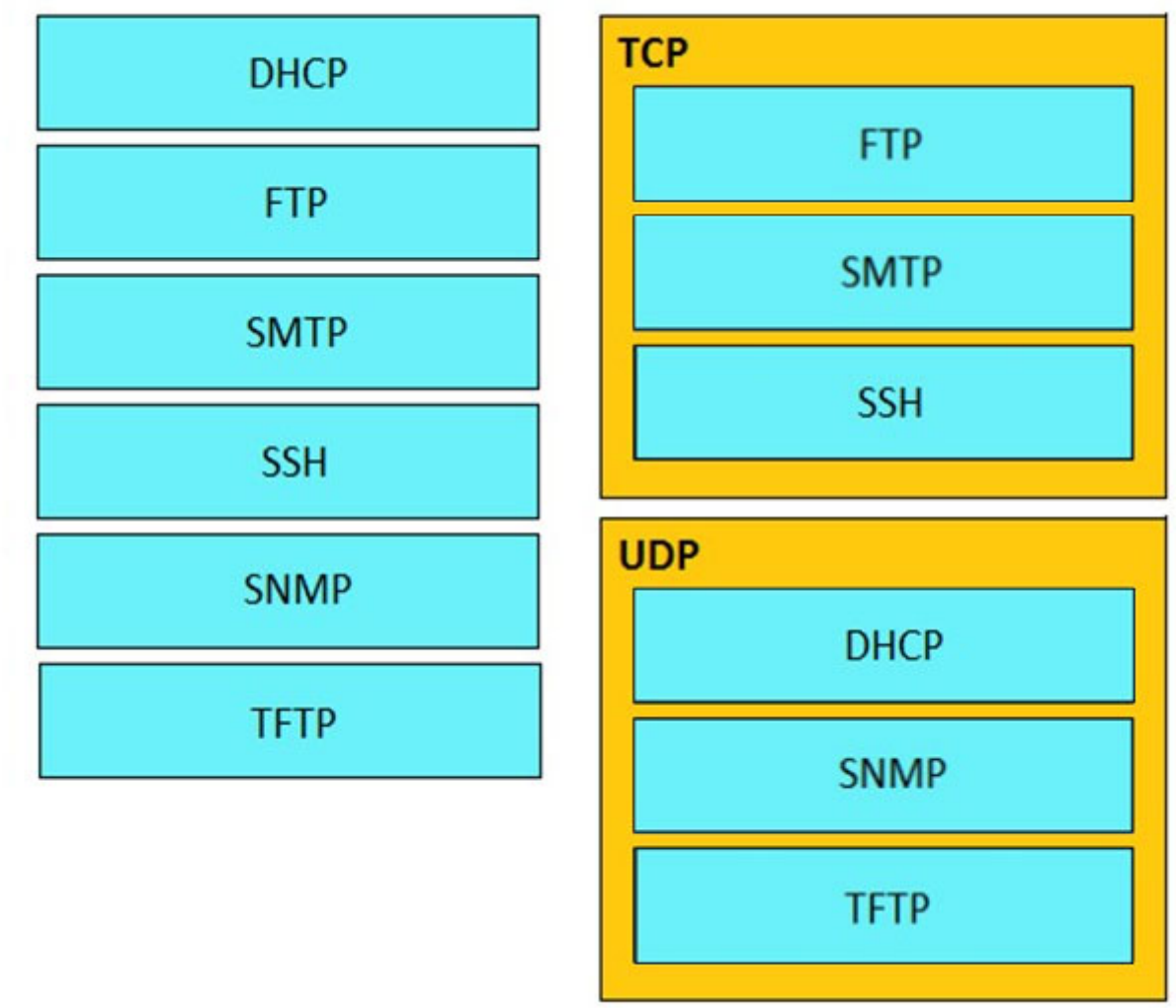
DRAG DROP -

Drag and drop the application protocols from the left onto the transport protocols that it uses on the right.

Select and Place:



Correct Answer:



Mani_Baarathi Highly Voted 2 years, 1 month ago

FTP -TCP 20,21
SSH - TCP 22
SMTP - TCP 25
TFTP - UDP 69
SNMP - UDP 161
DHCP - UDP 67

upvoted 24 times

Luinus Most Recent 9 months, 2 weeks ago

Coorect

upvoted 3 times

creaguy 11 months, 1 week ago

This was an actual question on my test. but DHCP was replaced with RIP and SSH was replaced with telnet

upvoted 2 times

Cabassi 7 months ago

In that case, RIP and SSH what did you do? .
Thanks in advance!!

upvoted 4 times

john1247 5 months ago

RIP-UDP-520.Telnet-TCP-23.

upvoted 2 times

NICE_ANSWERS 3 months, 3 weeks ago

Please must you specify the port number?

upvoted 2 times

dabears 1 year, 9 months ago

Do the answers have to be in a specific order to be considered correct?

upvoted 2 times

SasithCCNA 1 year, 9 months ago

Nope, it can be in any order.

upvoted 5 times

ZUMY 2 years, 5 months ago

Given answers are correct

upvoted 3 times

wirlernenman 2 years, 6 months ago

Correct

upvoted 3 times

Ali526 2 years, 8 months ago

This is correct.

upvoted 3 times

SScott 2 years, 1 month ago

That's right DHCP, SNMP, and TFTP all use UDP.
http://web.deu.edu.tr/doc/oreily/networking/tcpip/ch11_09.htm
https://www.reddit.com/r/ccna/comments/5jst64/why_does_tftp_use_udp/

upvoted 1 times

Question #45 *Topic 1*

What is the destination MAC address of a broadcast frame?

A. 00:00:0c:07:ac:01

B. ff:ff:ff:ff:ff:ff

C. 43:2e:08:00:00:0c

D. 00:00:0c:43:2e:08

E. 00:00:0c:ff:ff:ff

Correct Answer: *B*

Community vote distribution

B (100%)

Ali526 Highly Voted 2 years, 8 months ago

This is correct.

upvoted 7 times

abdelkader163 Most Recent 2 months, 4 weeks ago

Answer BBBBBBB

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: B

Ref: Broadcast Frame - an overview | ScienceDirect Topics

"...
Cisco IOS Switch Basics

Switch Concepts
...
• Broadcasts... Layer 2 broadcast frames have a destination Media Access Control (MAC) address of FF:FF:FF:FF:FF:FF and Layer 3 broadcast addresses have a destination Internet Protocol (IP) address that is set for the broadcast of that particular network (the address varies, so don't always assume that an IP address ending with 255 is the broadcast address).
..."

A. 00:00:0c:07:ac:01

Wrong answer.

B. ff:ff:ff:ff:ff:ff

Correct answer.

C. 43:2e:08:00:00:0c

Wrong answer.

D. 00:00:0c:43:2e:08

Wrong answer.

E. 00:00:0c:ff:ff:ff

Wrong answer.

upvoted 3 times

keokkeo_123 10 months, 2 weeks ago

Selected Answer: B

BBBBBBBBBB

upvoted 3 times

cortib 2 years ago

Answer is correct, related question to this could be the address' range used by HRSP : 0000.0C9F.F000 to 0000.0C9F.FFFF.

upvoted 4 times

ZUMY 2 years, 5 months ago

Correct Answer

upvoted 4 times

hippyjm 2 years, 5 months ago

https://www.ciscopress.com/articles/article.asp?p=3089352&seqNum=5

upvoted 2 times

Question #46 *Topic 1*

For what two purposes does the Ethernet protocol use physical addresses?

A. to uniquely identify devices at Layer 2

B. to allow communication with devices on a different network

C. to differentiate a Layer 2 frame from a Layer 3 packet

D. to establish a priority system to determine which device gets to transmit first

E. to allow communication between different devices on the same network

F. to allow detection of a remote device when its physical address is unknown

Correct Answer: *AE*

Community vote distribution

AE (100%)

Nhan Highly Voted 2 years, 7 months ago

Physical address is MAC address

upvoted 12 times

ZUMY Highly Voted 2 years, 5 months ago

A & E are correct

upvoted 11 times

Junior_Network Most Recent 23 hours, 8 minutes ago

Selected Answer: AE

A,E is correct

upvoted 1 times

virab4 5 months ago

how shall i know what i need to choose 2 answers?

upvoted 1 times

moooosi 4 weeks, 1 day ago

It^s written in the question. Choose two

upvoted 1 times

ViShawnn 3 months, 2 weeks ago

That's the fun part, you don't :)

upvoted 1 times

daddydagoth 6 months, 4 weeks ago

Specify that we need to choose 2, thank you

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: AE

Ref: Ethernet Address - an overview | ScienceDirect Topics

"...
Transmission Control Protocol/Internet Protocol Packet Analysis
...
In a LAN, each node is assigned a physical address, also known as a MAC/Ethernet address. This address is unique to each of the nodes on the LAN and is 6 bytes (48 bits) long, which is burned on the Ethernet card (also known as the network interface card). Ethernet is a byte-count protocol. A node on a LAN broadcasts a frame that is heard by all other nodes; only the node whose Ethernet address matches with the DA in the Ethernet frame copies the frame into its buffer.
..."

upvoted 3 times

jossyda 1 year, 3 months ago

Selected Answer: AE

Are correct

upvoted 3 times

ian77ex 1 year, 7 months ago

A and E are correct but the question doesn't specify "Select two answers"

A. to uniquely identify devices at Layer 2
- This is the most Accurate answer

E. to allow communication between different devices on the same network
- This is OK, but physical addresses is just the FIRST thing needed, not the ONLY thing needed to allow communication in the same broadcast network.

So if the question does not specify "select two answers" I would go with A.

upvoted 4 times

Tunz 1 year, 4 months ago

The questions says for what two purpose
So that's saying select two

upvoted 4 times

youtri 2 years, 5 months ago

I think (F) is incorrect, because remote device means it belongs to other network, please correct me if someone knows thank you

upvoted 5 times

ZayaB 2 years, 7 months ago

F is not correct. F states that when physical address (MAC address) is not known, it use broadcast address of all Fs. Correct answers are AE as MAC addr are used on L2 and used for communication within the network (LAN).

upvoted 4 times

Ali526 2 years, 8 months ago

AF is also correct. In a way, this Q has 3 answers: AEF

upvoted 3 times

sinear 2 years, 8 months ago

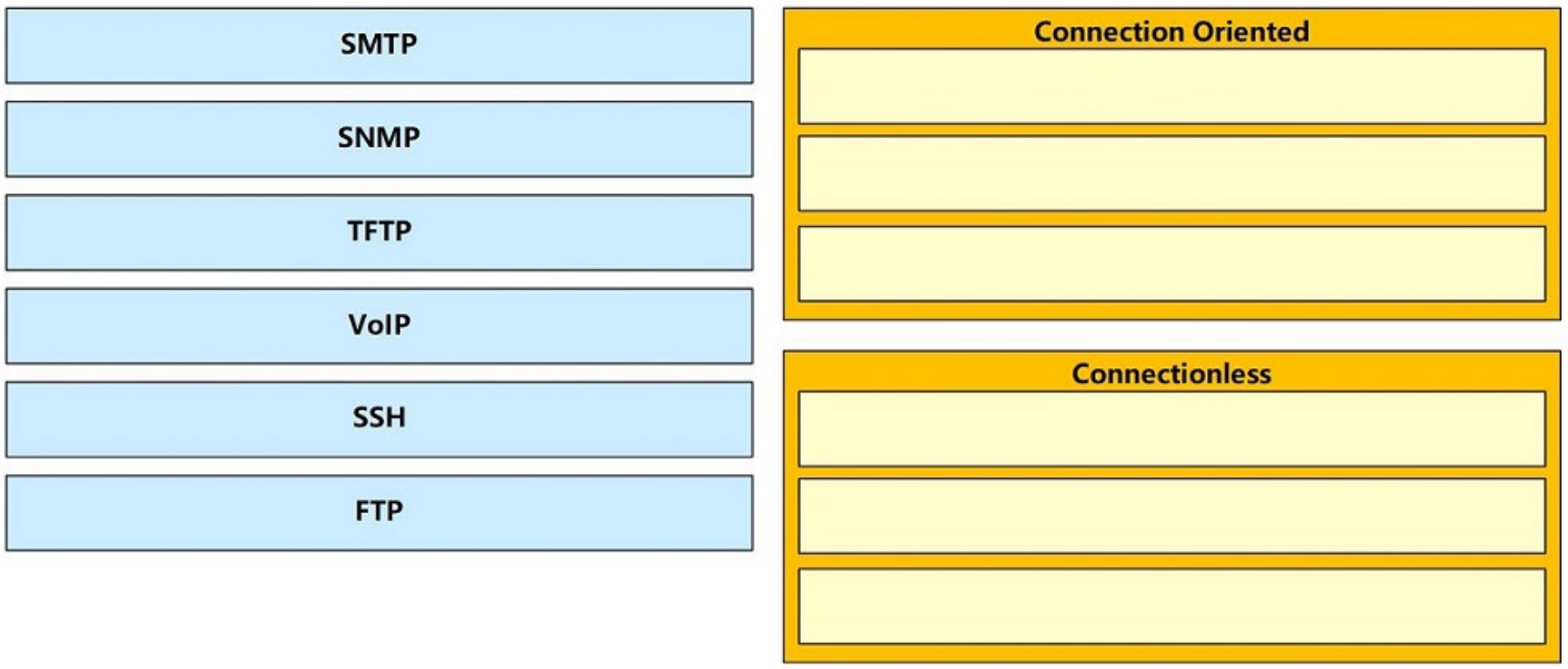
Don't think so. F describes the ARP protocol.

upvoted 3 times

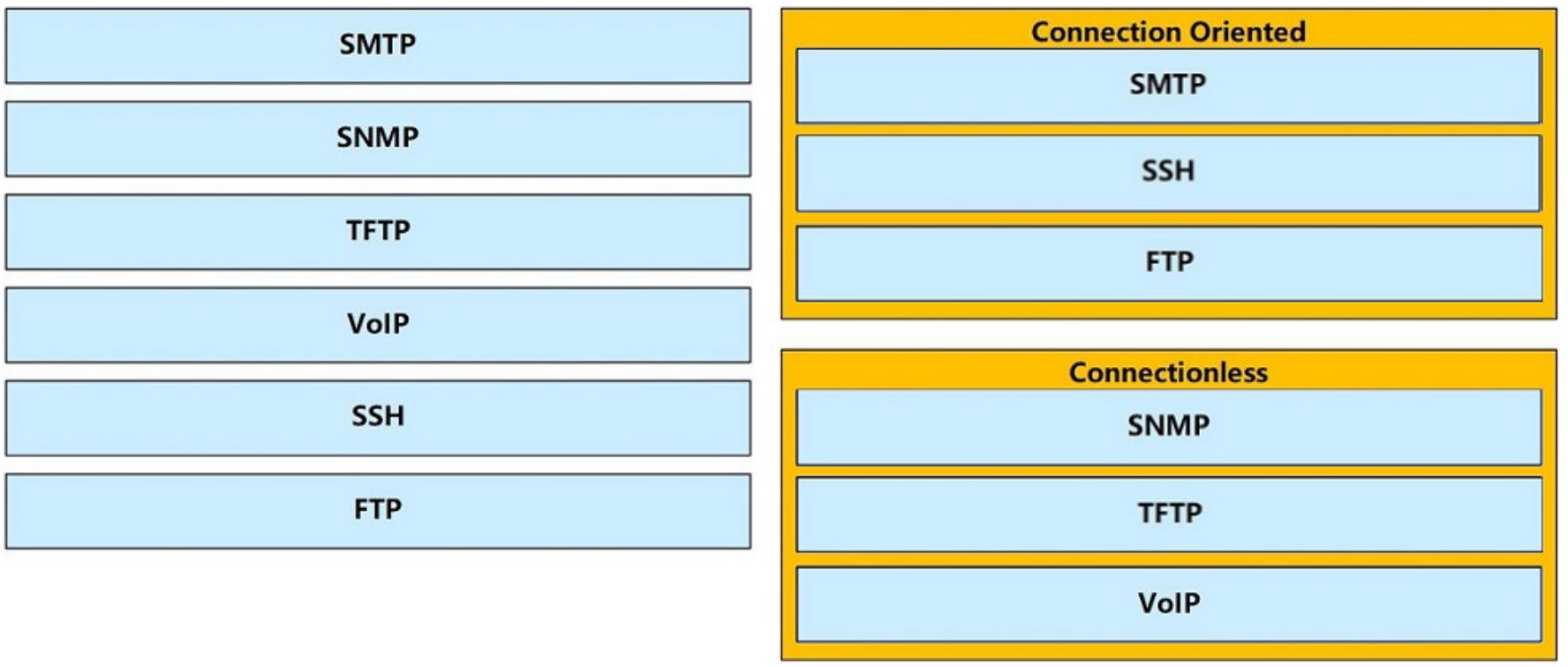
DRAG DROP -

Drag and drop the networking parameters from the left on to the correct values on the right.

Select and Place:



Correct Answer:



SSH uses TCP port 22 while SNMP uses UDP port 161 and 162.

Tengereni Highly Voted 2 years, 4 months ago

generally if you know the protocols used by TCP and UDP this question should not be difficult for you

its the same question asked in a different format

upvoted 13 times

BlackO Most Recent 1 year, 10 months ago

literally UDP and TCP protocol grouping

upvoted 1 times

MMAXY 2 years, 4 months ago

yea correct

upvoted 3 times

ZUMY 2 years, 5 months ago

Given answer is correct

upvoted 4 times

Ali526 2 years, 8 months ago

This is correct.

upvoted 3 times

Question #48 *Topic 1*

Which component of an Ethernet frame is used to notify a host that traffic is coming?

A. start of frame delimiter

B. Type field

C. preamble

D. Data field

Correct Answer: *C*
Preamble is a 7 Byte field in the Ethernet frame which helps to receiver to know that it is an actual data (Ethernet Frame) and not some random noise in the transmission medium. It acts like a doorbell telling about the incoming data.

Community vote distribution

C (88%) 12%

Alizadeh Highly Voted 9 months ago

Selected Answer: C

The component of an Ethernet frame that is used to notify a host that traffic is coming is the preamble. The preamble is a sequence of bits that is transmitted at the beginning of an Ethernet frame and is used to alert the receiving host that a frame is about to be transmitted.

The preamble consists of a series of alternating 1s and 0s, followed by a start-of-frame delimiter (SFD). The SFD is a unique pattern of bits that indicates the start of the frame and allows the receiving host to synchronize its clock with the sender's clock. The preamble and SFD together make up the preamble field of the Ethernet frame.

After the preamble, the Ethernet frame consists of several other fields, including the destination and source MAC addresses, the type field, and the data field. The data field contains the payload of the frame, which can be a variety of different types of data, such as IP packets or application data.

The preamble is important because it allows the receiving host to prepare for the arrival of the frame and ensures that the frame is properly received and processed. Without the preamble, the receiving host may not be aware that a frame is being transmitted, which could result in lost or corrupted data.

upvoted 7 times

ajuniad Most Recent 4 weeks, 1 day ago

Imagine you have a special code that you want to send to your friend using a walkie-talkie. Before you start talking in your code, you want to make sure your friend is listening and ready to hear your message. So, you and your friend decide on a special clapping pattern that you'll do before you start talking.

In the same way, in a computer network, before sending important information, devices use a special pattern of signals called a "preamble." This preamble works like the clapping pattern. It helps the devices get ready to listen to the upcoming message and understand it correctly. It's like a little signal that says, "Hey, get ready, some important stuff is about to come!"

upvoted 1 times

ajuniad 4 weeks, 1 day ago

C. Preamble

The preamble is a sequence of alternating ones and zeros that serves as a synchronization signal at the beginning of an Ethernet frame. It notifies a host that traffic is coming and helps the receiving device synchronize its clock with the sender's clock. This synchronization is essential for correctly interpreting the subsequent data in the frame.

upvoted 1 times

Dutch012 7 months ago

If it says the "actual" traffic is coming the answer would be "A".
otherwise is C.

upvoted 1 times

iMo7ed 7 months, 1 week ago

Selected Answer: C

C is correct

upvoted 2 times

ProgSnob 8 months, 2 weeks ago

For a bit I thought it could possibly be A but the correct answer is C. All the SFD does is let the destination device know the important part of the frame is about to begin. The Preamble is when it actually starts receiving the frame so it known something is about the come.

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: C

Ref: Ethernet Frame - an overview | ScienceDirect Topics

"...
Frame Format
...
The 64-bit preamble allows the receiver to synchronize with the signal; it is a sequence of alternating 0s and 1s.
..."

A. start of frame delimiter

Wrong answer.

B. type field

Wrong answer.

C. Preamble

Correct answer.

D. data field

Wrong answer
upvoted 3 times

Panda_man 9 months ago

Selected Answer: C

C is correct
upvoted 1 times

Ioannis_Vos 9 months ago

The Preamble (7 bytes) and Start Frame Delimiter (SFD), also called the Start of Frame (1 byte), fields are used for synchronization between the sending and receiving devices. These first eight bytes of the frame are used to get the attention of the receiving nodes. Essentially, the first few bytes tell the receivers to get ready
to receive a new frame.
This is from netacad. Propably the correct answer is C.
upvoted 1 times

Panda_man 10 months ago

Selected Answer: C

C is correct
upvoted 2 times

keokkeo_123 10 months, 2 weeks ago

Selected Answer: A

PREEEEE
upvoted 2 times

seeemo 1 year ago

PRE (Preamble) indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.
upvoted 2 times

Hodicek 1 year, 9 months ago

PREAMBLE IS THE CORRECT ANSWER 100% ,SORRY FOR CONFUSION
upvoted 3 times

ProgSnob 1 year, 9 months ago

The Preamble is 7 bytes and provides synchronization. The SFD is 1 byte and supposedly lets the user know that data is incoming. That's what I read.
upvoted 4 times

Hodicek 1 year, 10 months ago

A is correct
upvoted 1 times

DonnerKomet 2 years ago

According to CISCO preamble is 8 Bytes
upvoted 1 times

Godfather2022 11 months ago

7 bytes and not 8
upvoted 1 times

cormorant 10 months, 2 weeks ago

you mean it's 7 bytes + 1 byte from the SFD
upvoted 1 times

ZUMY 2 years, 5 months ago

C is correct

upvoted 4 times

Question #49 *Topic 1*

You are configuring your edge routers interface with a public IP address for Internet connectivity. The router needs to obtain the IP address from the service provider dynamically.
Which command is needed on interface FastEthernet 0/0 to accomplish this?

A. ip default-gateway

B. ip route

C. ip default-network

D. ip address dhcp

E. ip address dynamic

Correct Answer: *D*

Community vote distribution

D (100%)

xsp Highly Voted 2 years, 7 months ago

D is correct, means that the router will act as a DHCP client.
Should a router be set as a DHCP server commands are as follows:
conf t
service dhcp
ip dhcp pool <pool name>
network <network to be use as pool>
default-router <default gateway or the ip address of the ethernet interface facing the host>
dns-server <ip add of your dns server, say: 8.8.8.8 which is a google dns>
exit

upvoted 13 times

Jacob_Davis18 2 years, 6 months ago

Not correct, review again. The answer is C.
R1(config)#int Gi0/0
R1(config-if)#ip address dhcp

upvoted 2 times

Snellers 2 years, 6 months ago

think you may have misjudged where your answers are. ip address dhcp is answer D.

upvoted 7 times

ZUMY Highly Voted 2 years, 5 months ago

D is the answer
R1(config)#int Gi0/0
R1(config-if)#ip address dhcp

upvoted 6 times

ajuniad Most Recent 4 weeks, 1 day ago

D. ip address dhcp

To obtain an IP address dynamically from a service provider for Internet connectivity, you would use the "ip address dhcp" command on the interface. This command tells the router to request an IP address from a DHCP (Dynamic Host Configuration Protocol) server, which is usually provided by the Internet service provider (ISP). DHCP is a method for devices to automatically receive network configuration settings, including IP addresses, from a central server.

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: D

“obtain the IP address from the service provider dynamically” means obtaining an IP address from a DHCP server.

A. ip default-gateway

Wrong answer.

B. ip route

Wrong answer.

C. ip default-network

Wrong answer.

D. ip address dhcp

Correct answer.

E. ip address dynamic

Wrong answer.

upvoted 4 times

MrBadger 1 year, 5 months ago

I am sure I have seen "ip address dynamic or negotiate" somewhere? Anyway I picked dhcp which is correct.

upvoted 1 times

BlackO 1 year, 10 months ago

right answer

upvoted 1 times

Ali526 2 years, 8 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/config-dhcp-client.html

upvoted 2 times

Ali526 2 years, 8 months ago

D is correct.

upvoted 2 times

Question #50 *Topic 1*

Which two statements about the purpose of the OSI model are accurate? (Choose two.)

A. Defines the network functions that occur at each layer

B. Facilitates an understanding of how information travels throughout a network

C. Changes in one layer do not impact other layer

D. Ensures reliable data delivery through its layered approach

Correct Answer: *AB*

Community vote distribution

AB (100%)

Dante_Dan Highly Voted 2 years, 1 month ago

A & B are correct

C is incorrect because changes in one layer definitely affects others; imagine affecting layer 1 (disconnect a cable, plug it incorrectly, administer the incorrect amount of voltage, etc), it would affect other layers.
D is incorrect because OSI model is not meant to ensure anything, it simply explains some of the features of each layer it defines.

upvoted 16 times

Belinda 1 year, 6 months ago

Thanks

upvoted 4 times

Joe_Q Highly Voted 2 years, 5 months ago

The keyword is "Purpose".

upvoted 6 times

Dutch012 Most Recent 7 months ago

B is wrong, it does not tell us how are packets and frames forwarded by using a router and switch.
I believe A & C are right.

upvoted 3 times

CheMetto 3 months ago

Yes me too. Changes, i think they are talking about protocol, doesn't affect other layers. That is one of the purpose of the layer

upvoted 1 times

timtgh 7 months ago

C is correct. People are misinterpreting it. Yes, if a layer has a failure, this will definitely break all of the layers above it. But all documentation of the OSI model tells you that a primary goal of using the model is that change at one layer (meaning change in specs, not a broken cable in your network) does not affect other layers. The URL below is just one example. It says "The layers of isolation concept means that changes made in one layer of the architecture generally don't impact or affect components in other layers: the change is isolated to the components within that layer..." Most likely that is what the question is referring to.

https://www.oreilly.com/library/view/software-architecture-patterns/9781491971437/ch01.html

upvoted 2 times

GreatDane 8 months, 2 weeks ago

Selected Answer: AB

Ref: OSI Model Advantages and Basic Purpose Explained - Computer Networking Notes and Study Guides

"...
The layered approach
...
OSI model uses this approach. It divides the entire communication process into seven layers. Each layer describes a particular functionality along with the protocols and devices which are required to perform that functionality.
...
Advantages of the OSI Model
...
• Provide a teaching tool to understand the communication process used between networking components.
..."

A. Defines the network functions that occur at each layer

Correct answer.

B. Facilitates an understanding of how information travels throughout a network

Correct answer.

C. Changes in one layer do not impact other layer

Wrong answer.

D. Ensures reliable data delivery through its layered approach

Wrong answer.

upvoted 1 times

Anyc 1 year ago

This question is quite confusing. There is too much ambiguity about the word "change". The official definition of this word refers to a modification, a replacement, a substitution and not to something broken, deteriorated, damaged or incorrectly made. Moreover "Changes in one layer do not impact other layer" is not only written in netacad courses but it is a very strong message taught in all good courses on the CCNA exam. If this assertion is correct, it risks concealing that one of the fine qualities of the OSI model is to allow changes in one layer without impacting the other layers. We must also come back to the definition of the word "impact". Impact does not necessarily imply shutdown, failure or any other negative event.

upvoted 1 times

Nicocisco 1 year, 6 months ago

In my netacad courses i have:
These are the benefits of using a layered model to describe network protocols and operations:

-Assisting in protocol design because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below
-Fostering competition because products from different vendors can work together
-Preventing technology or capability changes in one layer from affecting other layers above and below
-Providing a common language to describe networking functions and capabilities

So i don't know if it can be A and C

upvoted 2 times

ismatdmour 1 year, 6 months ago

Answer C says "Changes in one layer do not impact other layer" is incorrect, for example a broken wire (physical layer disconnected) will result in Data-link layer protocol to be down (down down state) and no communication at all layers will occur. This means that a change in one layer impacts other layers and C is incorrect.
At the same time, this does not contradict with that in your course:"Preventing technology or capability changes in one layer from affecting other layers above and below". For example, for the same leased line (physical layer) they came up with many data link layer protocols, e.g HDLC and PPP. As another example, the Ethernet (which spans over physical and data-link layers) started with 10BaseT, with IP, ARP, IGMP and ICMP protocols on top at layer3. However, later on, the Ethernet Protocol continued to evolve with many variants, e.g. 100BaseT, 1000BaseT, Fuber Ethernet of many variants and so on while the L3 Protocols of IP and its colleagues remain untouched.
Hence, the answer (C) talks about operational changes while the Netacademy talks about design changes. I hope this clarified the difference.

upvoted 1 times

chr 2 years, 4 months ago

B. Facilitates an understanding of how information travels throughout a network
Because it is a conceptual tool used to understand networking.
C. Changes in one layer do not impact other layer.
Each layer provides services to the layer above. Changes within a layer should therefore not impact the layer above (ie the same service is provided to the layer above though it may be performed in a different way if the layer is changed).

upvoted 4 times

ZUMY 2 years, 5 months ago

A & B are correct
OSI model is an structure for Both TCP and UDP. So it doesn't ensure reliabile delivery always (For UDP)

upvoted 5 times

Claudiu1 2 years, 6 months ago

"C. Changes in one layer do not impact other layer " I also find this true, as, for example, L2 Ethernet protocol can support both IPv4 and IPv6 protocols without changes to its structure. However, this is why layered models exist in general, it is not particular to OSI, nor it defines its purpose. I'd say AB are correct

upvoted 4 times

ronanncirl 2 years, 6 months ago

Not D as its not always reliable delivery

upvoted 3 times

ZayaB 2 years, 7 months ago

Yes, I also see D is also somehow right. But best and relevant answer is AB

upvoted 2 times

Ali526 2 years, 8 months ago

AB is good, D maybe.

upvoted 2 times

Question #51 *Topic 1*

Which three statements about MAC addresses are correct? (Choose three.)

A. To communicate with other devices on a network, a network device must have a unique MAC address

B. The MAC address is also referred to as the IP address

C. The MAC address of a device must be configured in the Cisco IOS CLI by a user with administrative privileges

D. A MAC address contains two main components, the first of which identifies the manufacturer of the hardware and the second of which uniquely identifies the hardware

E. An example of a MAC address is 0A:26:B8:D6:65:90

F. A MAC address contains two main components, the first of which identifies the network on which the host resides and the second of which uniquely identifies the host on the network

Correct Answer: *ADE*

Community vote distribution

ADE (100%)

Ali526 Highly Voted 2 years, 8 months ago

ADE are the answers.

upvoted 14 times

Junior_Network Most Recent 22 hours, 57 minutes ago

Selected Answer: ADE

Easy one

upvoted 1 times

Hanagaki_Shinjiro 1 week, 3 days ago

Selected Answer: ADE

So easy

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: ADE

A. To communicate with other devices on a network, a network device must have a unique MAC address

Correct answer.

B. The MAC address is also referred to as the IP address

Wrong answer.

C. The MAC address of a device must be configured in the Cisco IOS CLI by a user with administrative privileges

Wrong answer.

D. A MAC address contains two main components, the first of which identifies the manufacturer of the hardware and the second of which uniquely identifies the hardware

Correct answer.

E. An example of a MAC address is 0A:26:B8:D6:65:90

Correct answer.

F. A MAC address contains two main components, the first of which identifies the network on which the host resides and the second of which uniquely identifies the host on the network

Wrong answer.

upvoted 3 times

keokkeo_123 10 months, 2 weeks ago

Selected Answer: ADE

ADE is coorrect ans

upvoted 3 times

WINDSON 1 year, 3 months ago

I agree ADE are correct. But why C is wrong ?
upvoted 1 times

Dezun 1 year, 2 months ago
administrator cannot assign mac address.
upvoted 1 times

Adaya 2 years, 3 months ago
Yes correct answers
upvoted 3 times

ZUMY 2 years, 4 months ago
ADE are correct!
upvoted 4 times

Question #52 *Topic 1*

Which technique can you use to route IPv6 traffic over an IPv4 infrastructure?

A. NAT

B. 6 to 4 tunneling

C. L2TPv3

D. dual-stack

Correct Answer: *B*

Community vote distribution

B (100%)

ZUMY Highly Voted 2 years, 4 months ago

B is correct!
Overlay tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure (a core network or the figure below). By using overlay tunnels, you can communicate with isolated IPv6 networks without upgrading the IPv4 infrastructure between them. Overlay tunnels can be configured between border devices or between a border device and a host; however, both tunnel endpoints must support both the IPv4 and IPv6 protocol stacks. IPv6 supports the following types of overlay tunneling mechanisms:

1 Manual
2 Generic routing encapsulation (GRE)
3 IPv4-compatible
4 6to4
5 Intrasite Automatic Tunnel Addressing Protocol (ISATAP)

upvoted 25 times

virab4 5 months ago

yes inner and outer ip addresses

upvoted 2 times

ajuniad Most Recent 4 weeks, 1 day ago

B. 6 to 4 tunneling
Imagine you have two groups of friends, one group that talks using a secret code with letters and numbers (IPv6), and another group that talks using regular words (IPv4). But you want these two groups to talk to each other, even though they use different ways of talking.

Now, think of a big tunnel that connects these two groups. When someone from the first group wants to send a message to someone in the second group, they put their message in a special envelope and send it through the tunnel. When the message comes out of the tunnel on the other side, it looks like a message from the second group, even though it started with the first group's way of talking.

In the same way, 6 to 4 tunneling helps the two different ways of talking, IPv6 and IPv4, to understand each other. It wraps the IPv6 message in an IPv4 wrapper and sends it through a tunnel. This way, they can communicate even though they use different codes.

upvoted 2 times

soRwatches 6 months, 1 week ago

is this type of question is in the scope of CCNA?

upvoted 3 times

GreatDane 8 months, 2 weeks ago

Selected Answer: B

Ref: IPv6 Tunnel through an IPv4 Network – Cisco

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

A. NAT

Wrong answer.

B. 6 to 4 tunneling

Correct answer.

C. L2TPv3

Wrong answer.

D. dual-stack

Wrong answer.

upvoted 3 times

marcojmnez 2 years, 6 months ago

An automatic 6to4 tunnel allows isolated IPv6 domains to be connected over an IPv4 network to remote IPv6 networks

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-6to4-tunls-xe.pdf

upvoted 4 times

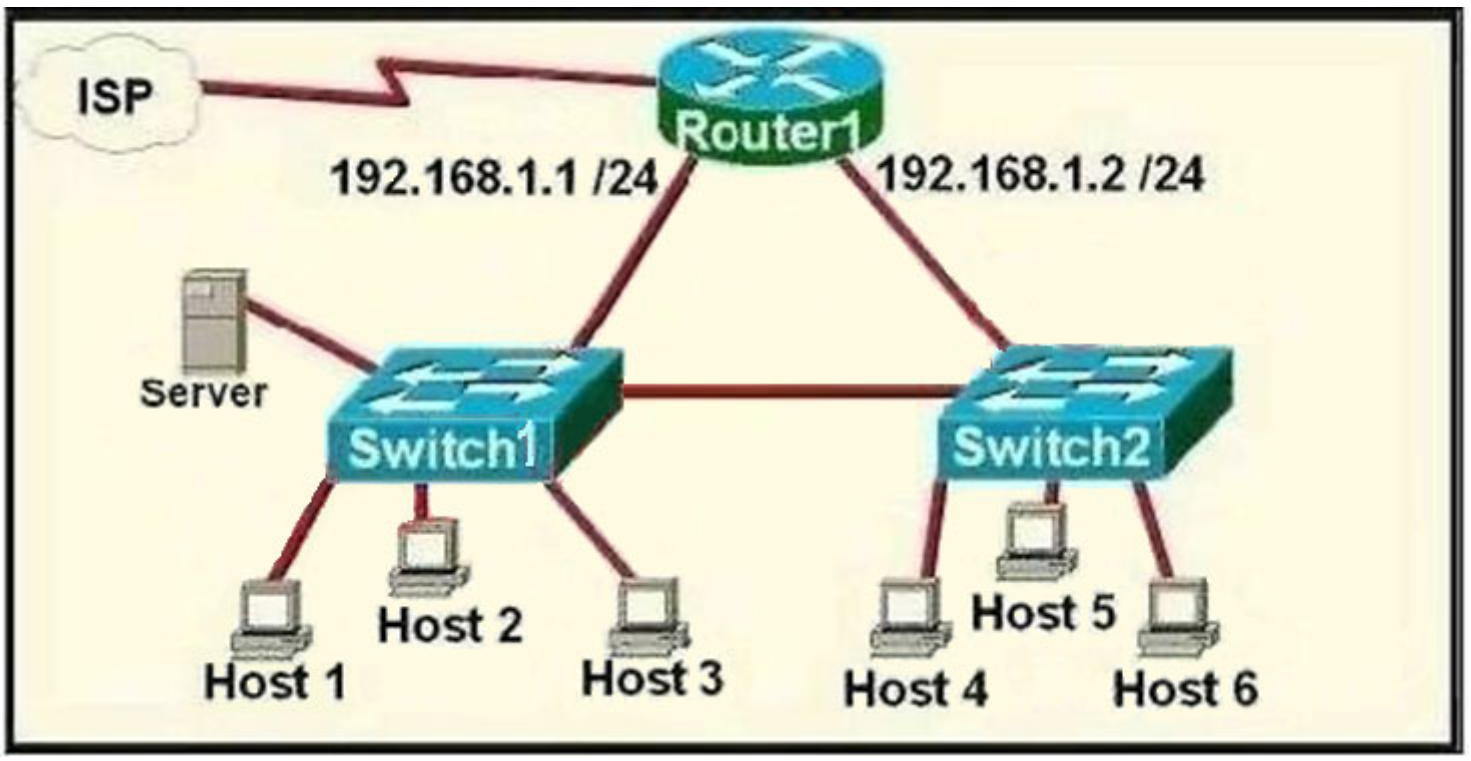
echarles10 2 years, 8 months ago

B is the correct answer... 6 to 4
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/15-mt/ir-15-mt-book/ip6-ipoverip6-tunls.html#:~:text=Generic%20routing%20encapsulation%20(GRE)%20IPv4,%2Dto%2Dpoint%20encapsulation%20scheme.

upvoted 4 times

Question #53 *Topic 1*

Refer to the exhibit. A network technician is asked to design a small network with redundancy. The exhibit represents this design, with all hosts configured in the same VLAN. What conclusions can be made about this design?



A. This design will function as intended.

B. Spanning-tree will need to be used.

C. The router will not accept the addressing scheme.

D. The connection between switches should be a trunk.

E. The router interfaces must be encapsulated with the 802.1Q protocol.

Correct Answer: *C*

Each interface on a router must be in a different network. If two interfaces are in the same network, the router will not accept it and show error when the administrator assigns it.

Community vote distribution

C (100%)

ZUMY Highly Voted 2 years, 4 months ago

C is correct!
Each router interface Must be in different network.

upvoted 9 times

SScott 2 years, 3 months ago

Yes C is right. A possible exception to this scenario would be a bridge group which is not referenced
https://community.cisco.com/t5/switching/two-interfaces-same-subnet-r/td-p/3076045

upvoted 1 times

agazi Highly Voted 1 year, 7 months ago

I think we should reveal the designer name for future references. He has done terrible job in designing like this. Just to lighten up the mood. on serious not what if we have switch interface (SVI) on the router it could work but not as intended

upvoted 8 times

timtgh Most Recent 7 months ago

Badly worded question. Not enough info is given. If these are L2 switches, then C is correct. That was probably the author's intention. However, if they are L3 switches, then C would be wrong, so D would be the answer. I think C is the answer they want.

upvoted 2 times

megaa 1 month, 4 weeks ago

By the switch diagram, it is clear as L2 switch, if it is an L3 switch you would find the icon of multilayer switch.

upvoted 1 times

elixirwell 5 months, 3 weeks ago

If it was an L3 SW why would they show a router? I guess it was safe to assume.

upvoted 1 times

ECisco 1 month, 4 weeks ago

also L3 switch has a different icon used by Cisco so

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: C

The link between the two switches creates a single broadcast domain. And a broadcast domain maps to a subnet.
Any interface on Router1 must be assigned to a subnet which is distinct from every other interface. But, in this case, the network design doesn't comply with such requirement.

A. This design will function as intended.

Wrong answer.

B. Spanning-tree will need to be used.

Wrong answer.

C. The router will not accept the addressing scheme.

Correct answer.

D. The connection between switches should be a trunk.

Wrong answer.

E. The router interfaces must be encapsulated with the 802.1Q protocol.

Wrong answer.

upvoted 3 times

ScorpionNet 1 year, 4 months ago

C is right because Routers are meant to route through different networks

upvoted 2 times

CISCO2022 2 years, 3 months ago

will not work. one vlan, no STP needed router stop broadcast. need router on stick and 2 vlan to work. C is correct.

upvoted 5 times

marcojmnez 2 years, 6 months ago

Both Rs interfaces overlaping.

upvoted 4 times

sinear 2 years, 8 months ago

Why not also B ? STP is needed as there are 2 SW no ?

upvoted 2 times

lordnano 2 years, 6 months ago

STP is needed to avoid packet loops on layer 2. The router does not forward layer 2 broadcast on routed interfaces, so there is no loop created, which would makes STP necessary.

upvoted 11 times

Chun9 2 years, 7 months ago

I believe L2 switches with different IP subnet can't create the link and they don't know how to route.

upvoted 2 times

ZayaB 2 years, 7 months ago

The network needs to be designed properly before STP (PVST+ or other) can be used. According to the diagram, best answer that fits is C as router will not accept multiple IPs from the same subnet.

upvoted 2 times

pianetaperez 2 years, 8 months ago

ip address overlaps

upvoted 3 times

Question #54 *Topic 1*

Which two statements are true about the command ip route 172.16.3.0 255.255.255.0 192.168.2.4? (Choose two.)

A. It establishes a static route to the 172.16.3.0 network.

B. It establishes a static route to the 192.168.2.0 network.

C. It configures the router to send any traffic for an unknown destination to the 172.16.3.0 network.

D. It configures the router to send any traffic for an unknown destination out the interface with the address 192.168.2.4.

E. It uses the default administrative distance.

F. It is a route that would be used last if other routes to the same destination exist.

Correct Answer: *AE*

Community vote distribution

AE (100%)

SScott Highly Voted 2 years, 3 months ago

A and E are correct. The tricky part to the question is the prefix subnet 172.16.3.0 which is the destination network. B is wrong. The 192.168.2.0 network is the next hop used to reach the static route destination. No metric is set so the default value of 6 will be used for the administrative distance.
https://www.cisco.com/c/en/us/td/docs/routers/nfvis/switch_command/b-nfvis-switch-command-reference/ip_route_commands.pdf

upvoted 10 times

liselsia 1 year, 10 months ago

i think the static route should have default AD of 1

upvoted 12 times

Ali526 Highly Voted 2 years, 8 months ago

AE are correct.

upvoted 8 times

Junior_Network Most Recent 22 hours, 47 minutes ago

it has default 1

upvoted 1 times

ajuniad 4 weeks, 1 day ago

correct answer is A&D
A. The command "ip route 172.16.3.0 255.255.255.0 192.168.2.4" establishes a static route to the 172.16.3.0 network. This means that the router knows how to reach the devices in the 172.16.3.0 network, and it will use the interface with the address 192.168.2.4 to reach them.

D. The command "ip route 172.16.3.0 255.255.255.0 192.168.2.4" also configures the router to send any traffic for an unknown destination out the interface with the address 192.168.2.4. This is because it's a default route (also known as the gateway of last resort), which means if the router doesn't have a specific route for a destination, it will send the traffic out through this interface.

The other options (B, C, E, and F) do not accurately describe the behavior of the given command.

upvoted 1 times

MauroC19 4 weeks, 1 day ago

Selected Answer: AE

ip route command has the following order: (destination IP) (mask) (next hop) (AD)
as the AD is not specified in the question, I asume that is using its default AD, so answer E is correct.

upvoted 1 times

gabyslim 2 months, 1 week ago

Selected Answer: AE

A and E are correct.

upvoted 1 times

PacketFapper 3 months, 3 weeks ago

so does the inverse applies here as well. Could i reverse the cmd and yield the same result
if

ip route 192.168.2.4 255.255.255.0 172.16.3.0

Will destination be to the 172.16.3.0 network from 192.168.2.4?

upvoted 1 times

CheMetto 3 months ago

as first, as ip route you need to follow network rules, so it's not 192.168.2.4 but it is 192.168.2.0. As second, if you invert it, it means that you'll reach 192.168.2.4 through 172.16.3.0

upvoted 1 times

Bhrino 4 months, 1 week ago

Selected Answer: AE

The command for static routes are “ip route (destination) (subnet mask) (next hop)” making 3.0 the destination network (A). E also is correct because the question did not add a custom administrative distance making it the default of 1.

upvoted 2 times

GreatDane 8 months, 2 weeks ago

Selected Answer: AE

A. It establishes a static route to the 172.16.3.0 network.

Correct answer.

B. It establishes a static route to the 192.168.2.0 network.

Wrong answer.

C. It configures the router to send any traffic for an unknown destination to the 172.16.3.0 network.

Wrong answer.

D. It configures the router to send any traffic for an unknown destination out the interface with the address 192.168.2.4.

Wrong answer.

E. It uses the default administrative distance.

Correct answer.

F. It is a route that would be used last if other routes to the same destination exist.

Wrong answer.

upvoted 2 times

cormorant 10 months, 2 weeks ago

ip route destination_address + subnet mask + next hop
it's a static route. the administrative distance for static routes is 1

upvoted 1 times

keokkeo_123 10 months, 2 weeks ago

Selected Answer: AE

AE answer

upvoted 2 times

VarDav 11 months, 2 weeks ago

A&E
See floating static route:
https://www.ciscopress.com/articles/article.asp?p=2180209&seqNum=7#:~:text=A%20floating%20static%20route%20is,connectivity%20to%20the%20primary%20route.

upvoted 1 times

AWSEMA 1 year, 1 month ago

Router(config)#int f1/0
Router(config-if)#ip ad
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

Router(config-if)#
Router(config-if)#int f2/0
Router(config-if)#ip ad
Router(config-if)#ip address 192.168.2.2 255.255.255.0
% 192.168.2.0 overlaps with FastEthernet1/0

upvoted 1 times

RedSeven4 1 year, 10 months ago

Why is D not correct?

upvoted 2 times

shiv3003 4 months, 3 weeks ago

yes it can be D.. AD can be manually be set
upvoted 1 times

Taku2023 7 months ago
D is correct for me also. it is the next hop ip.
upvoted 1 times

laurvy36 1 year, 9 months ago
unknown destination means that the router will send the packet most probably to the gateway of last resort 0.0.0.0/0 if it doesnt know the destination
upvoted 2 times

Coffeezw 1 year, 10 months ago
Coz it says unknown destination, of which the question gives us the known destination network address (172.....)
upvoted 4 times

Alsaher 2 years, 4 months ago
AE is correct
upvoted 2 times

ZUMY 2 years, 4 months ago
A & E are correct!
upvoted 2 times

jerry19 2 years, 4 months ago
Keep trying. This is a recursive ip route which essentially says, any traffic going to this network and this subnet, go here!
upvoted 1 times

UmbertoReed 2 years, 5 months ago
A is correct because "ip route" works with the format "destination-address mask [exit-interface | next-hop-address].

B is correct because it doesn't explicitly specify an administrative distance at the end of the command, so it uses the default AD of 1.
upvoted 5 times

Question #55 *Topic 1*

What are two benefits of private IPv4 IP addresses? (Choose two.)

A. They are routed the same as public IP addresses.

B. They are less costly than public IP addresses.

C. They can be assigned to devices without Internet connections.

D. They eliminate the necessity for NAT policies.

E. They eliminate duplicate IP conflicts.

Correct Answer: *BC*

Community vote distribution

BC (78%) AB (22%)

ZUMY Highly Voted 2 years, 4 months ago

B & C are correct!

upvoted 13 times

lucky1559 Highly Voted 2 years ago

E is not quite that wrong. If not the private adresses, there would be less adresses overall to use, so it would increase the chance of someone assigning address that is already in use. By using private IPs, there is no chance, someone assigns diplicate public address inside LAN cuz there is a special IP scope for that.
Therefore I would say B&E.

C is like yes and no. 0 is always less that something grater than it, but here it suggests that privates costs something which is wrong.

upvoted 8 times

Utshav Most Recent 2 weeks, 6 days ago

The correct answers are:

B. They are less costly than public IP addresses.
C. They can be assigned to devices without Internet connections.

upvoted 1 times

Utshav 2 weeks, 6 days ago

. Correct. Private IPv4 addresses are less costly because they are not globally unique and can be used within private networks without requiring registration or assignment from Internet authorities.
Correct. Private IPv4 addresses can be assigned to devices within a local network that do not require direct Internet access. This is useful for internal communication or isolated network segments

upvoted 1 times

AndreaGambera 3 weeks, 4 days ago

B e C are correct !

upvoted 1 times

Iamm 2 months ago

A and C are correct, or better answer considering other options.
B refers to private address with some kind of cost, but unlike public squeme, there is no cost at all for private addressing squeme. So i believe this is a trick option.

upvoted 1 times

Marius_Mario 3 months, 3 weeks ago

I think the right answer are C and E.

upvoted 1 times

Jorro99404 4 months ago

Selected Answer: BC

B and C are correct

upvoted 1 times

Isuzu 4 months, 3 weeks ago

AI Say
The two benefits of private IPv4 IP addresses are:

C. They can be assigned to devices without Internet connections: Private IPv4 addresses can be assigned to devices that do not need to connect to the internet, such as devices that only need to communicate with other devices on the same local network. This conserves public IP addresses for devices that need to connect to the internet.

E. They eliminate duplicate IP conflicts: Private IPv4 addresses are used within a local network, so there is no possibility of a conflict with public IP addresses used on the internet. Using private IP addresses eliminates the need for organizations to coordinate with other organizations to ensure that their IP addresses are unique.

upvoted 1 times

Bhrino 4 months, 1 week ago

While it helps to eliminate duplicate up problems it doesn't fix it completely and using private address are free making b correct instead of e

upvoted 1 times

dearc 5 months, 2 weeks ago

AI answered: The correct two benefits of private IPv4 IP addresses are:

B. They are less costly than public IP addresses. C. They can be assigned to devices without Internet connections.

Private IPv4 addresses are not routed the same as public IP addresses and do not eliminate the necessity for NAT . Private IP addresses are used within local area networks and are not directly accessible from the Internet. They are a way to conserve and reuse public IP addresses by allowing multiple devices to share a single public IP address. Private IPs are also useful for assigning addresses to devices that do not need to access the internet, such as printers or security cameras.

upvoted 2 times

daddydagoth 6 months, 4 weeks ago

"they are less costly" Is an absolute awful answer considering that they cost nothing but it is technically correct...

upvoted 6 times

timtgh 7 months ago

Another bad question. B,C, and E are all correct, but B,C are probably the expected answer. E is also true because private addresses do eliminate duplicate IP address conflicts. Note that don't eliminate the duplicate addresses, but they do stop them from causing conflicts. However, this usually requires NAT, while B and C are accomplished without requiring NAT, so are better answers.

upvoted 2 times

remoto 9 months, 1 week ago

Selected Answer: BC

B and C

upvoted 1 times

RougePotatoe 10 months ago

Selected Answer: AB

A. They are routed the same as public ipv4 addresses
B. They are less costly than public ipv4 addresses

There is no difference in routing procedures between public and private ipv4 addresses. If the router doesn't have the IP address in the routing table it will send it to the default route.
C. They can be assigned to devices without Internet connections.
Makes no sense because you can assign public ipv4 addresses to devices that do not have internet connections as well.

upvoted 2 times

siredobu 7 months, 3 weeks ago

They are NOT routed the same way as public ipv4 addresses, they are not route-able on the internet

upvoted 6 times

RougePotatoe 10 months, 2 weeks ago

Anyone knows why A. They are routed the same as public IP addresses. couldn't be an answer?

upvoted 1 times

diudiuQIdama 9 months ago

public router will drop those packets from private addresses so they are not routable on puiblic network

upvoted 5 times

ian77ex 1 year, 7 months ago

Selected Answer: BC

B is correct, but It's not seriuos, way too many possible answers could have made this a better question.

upvoted 5 times

Shamwedge 1 year, 10 months ago

This one is easy to overthink.
B is correct because they're free.
C is correct because local devices can still communicate with private IP's without internet
D is not correct because a duplicate IP address can still be configured by accident via human error

upvoted 3 times

Marius_Mario 3 months, 3 weeks ago

But duplicate private IP are not a problem because of NAT, and the fact that each address remain in it own place

upvoted 1 times

etx 2 years ago

should be C + E imo

upvoted 6 times

Question #56 *Topic 1*

What are two benefits that the UDP protocol provide for application traffic? (Choose two.)

A. UDP traffic has lower overhead than TCP traffic

B. UDP provides a built-in recovery mechanism to retransmit lost packets

C. The CTL field in the UDP packet header enables a three-way handshake to establish the connection

D. UDP maintains the connection state to provide more stable connections than TCP

E. The application can use checksums to verify the integrity of application data

Correct Answer: *AE*

Community vote distribution

AE (100%)

Ali526 Highly Voted 2 years, 8 months ago

AE are correct.

upvoted 9 times

ZUMY Highly Voted 2 years, 4 months ago

A & E are correct!

upvoted 7 times

Hanagaki_Shinjiro Most Recent 1 week, 3 days ago

Selected Answer: AE

There's no doutb about A&E

upvoted 1 times

BehEARD 2 months, 2 weeks ago

AE Correct

upvoted 1 times

Tobilest 4 months, 1 week ago

AE are correct

upvoted 1 times

MSTAHIR 7 months, 4 weeks ago

A & E are correct

upvoted 2 times

Nebulise 1 year, 7 months ago

A and E are correct!

upvoted 4 times

SUKABLED 2 years, 7 months ago

AEsy...

upvoted 2 times

Nicocisco 1 year, 6 months ago

EAsy :D

upvoted 1 times

Zerotime0 2 years, 7 months ago

Deff not bcd those describe tcp. Another way to answer.

upvoted 3 times

Question #57 *Topic 1*

Which two goals reasons to implement private IPv4 addressing on your network? (Choose two.)

A. Comply with PCI regulations

B. Conserve IPv4 address

C. Reduce the size of the forwarding table on network routers

D. Reduce the risk of a network security breach

E. Comply with local law

Correct Answer: *BD*

Community vote distribution

BD (100%)

CiscoTerminator Highly Voted 2 years, 1 month ago

I think the answer B should be more specific like "To conserve IPv4 Public Addresses" - otherwise you cant conserve IPv4 addresses by using IPv4 addresses.

upvoted 19 times

nastynasty 1 year, 8 months ago

haha true

upvoted 2 times

ZUMY Highly Voted 2 years, 4 months ago

B & D are correct!

upvoted 7 times

Junior_Network Most Recent 22 hours, 41 minutes ago

B and D are correct but reducing routing table is also true. I'm not sure

upvoted 1 times

djflexyb 1 month, 3 weeks ago

C and D, the question asks why do you implement it, you don't implement something to conserve it

upvoted 1 times

[Removed] 3 months, 1 week ago

Selected Answer: BD

B and D are correct

upvoted 1 times

cpinac 6 months, 1 week ago

I'm a little confused, per The CCNA Official Cert Guide Vol1 (page 278):

■Avoiding/Delaying IPv4 Address Exhaustion: To delay the day in which all public IPv4 addresses were assigned to organizations as public addresses, RFC 1918 calls for the use
of NAT along with private networks for the addresses internal to an organization.

■ Reducing Internet Routers' Routing Table Size: Using private networks also helps reduce the size of the IP routing tables in Internet routers. For instance, routers in the Internet do not need routes for the private IP networks used inside organizations (in fact, ISPs filter those routes)

upvoted 5 times

properchad 4 months ago

Question is asking the benefits of using private ipv4 on OUR NETWORK . From this perspective it doesn't matter to us whether the size of routing table of ISP or other public routers are less or large.
We need to assess the benefits it provides to us. And on that note security is one good reason as our networks can't be accessed from internet unless NAT is in use.
And it does save the ipv4 address exhaustion.

upvoted 1 times

properchad 4 months ago

and also the forwarding tables of routers in our network won't be any less. We do need to route packets using routing table.

upvoted 1 times

Salvador_dali 5 months, 3 weeks ago

I was thinking the same, I'm using the same book to study for exam and it seems a lot of answers contradict what is in Cisco's OFFICIAL cert guide.

upvoted 1 times

MrBadger 1 year, 5 months ago

Terribly worded question, the answers actually tell you what the question is.

upvoted 4 times

setarehsabz 1 year, 7 months ago

B and D are correct

upvoted 3 times

Doopfenel 1 year, 9 months ago

Why does it reduce the breach security?

upvoted 6 times

Chupacabro 1 year, 8 months ago

In a scenario that the network isn't connected to the internet.

upvoted 5 times

WINDSON 1 year, 3 months ago

if your network don't have internet connectivity, how can i hack you ?

upvoted 5 times

ismatdmour 1 year, 6 months ago

private addresses are hidden behund a Nat hence they are not exposed to external reconnaissance attacks from outside the network

upvoted 2 times

AlexMD 1 year, 10 months ago

B & D are correct

upvoted 1 times

DavidFitzgerald 2 years, 4 months ago

Think there is a typo in the question shouldn't it be: "which two goals ARE reasons..?"

upvoted 2 times

Ali526 2 years, 8 months ago

BD are correct.

upvoted 4 times

il_pelato_di_casalbruciato 2 years, 4 months ago

grazie ar cazzo

upvoted 6 times

Question #58 *Topic 1*

Which WAN access technology is preferred for a small office / home office architecture?

A. broadband cable access

B. frame-relay packet switching

C. dedicated point-to-point leased line

D. Integrated Services Digital Network switching

Correct Answer: *A*
Service providers provide Internet access using broadband services such as DSL, cable, and satellite access. Broadband connections are typically used to connect small offices and telecommuting employees to a corporate site over the Internet. Data traveling between corporate sites over the public WAN infrastructure should be protected using VPNs.

Community vote distribution

A (100%)

ZUMY Highly Voted 2 years, 4 months ago

A is correct!
upvoted 10 times

[Removed] Most Recent 3 months, 1 week ago

Selected Answer: A
A is correct.
upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: A
Ref: Connecting Networks v6 Companion Guide

"Chapter 4
WAN Concepts
...
Selecting a WAN Technology
...
WAN Link Connection Options
...
Public WAN infrastructure:... Broadband connections are typically used to connect small offices and telecommuting employees to a corporate site over the Internet.
..."

A. broadband cable access

Correct answer

B. frame-relay packet switching

Wrong answer.

C. dedicated point-to-point leased line

Wrong answer.

D. Integrated Services Digital Network switching

Wrong answer.
upvoted 3 times

Marcos9410 1 year, 2 months ago

I think D is the correct answer.
Integrated services digital network (ISDN) is a WAN technology that offers increments of 64-Kbps connections most often used by SOHO (small office/home office) users.

https://the-definition.com/term/integrated-services-digital-network-isdn
upvoted 2 times

flash93933 8 months, 1 week ago

ISDN is dial up man....
upvoted 5 times

all4one 8 months ago

hahaha

upvoted 1 times

hippyjm 2 years, 6 months ago

Public WAN infrastructure: Service providers provide Internet access using broadband services such as DSL, cable, and satellite access. Broadband connections are typically used to connect small offices and telecommuting employees to a corporate site over the Internet. Data traveling between corporate sites over the public WAN infrastructure should be protected using VPNs.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/15-mt/ir-15-mt-book/ip6-ipoverip6-tunls.html#:~:text=Generic%20routing%20encapsulation%20(GRE)%20IPv4,%2Dto%2Dpoint%20encapsulation%20scheme.

upvoted 3 times

echarles10 2 years, 8 months ago

A .broadband is correct for Small office.

upvoted 3 times

Question #59 *Topic 1*

Which two WAN architecture options help a business scalability and reliability for the network? (Choose two.)

A. asychronous routing

B. single-homed branches

C. dual-homed branches

D. static routing

E. dynamic routing

Correct Answer: *CE*
Reference:
https://www.cisco.com/c/dam/en/us/td/docs/nsite/wan_optimization/WANoptSolutionGd.pdf

Community vote distribution

CE (72%) AC (28%)

sinear Highly Voted 2 years, 8 months ago

Should be C and E for me.
Dynanic routing serves scalability as compared to static routing.

upvoted 27 times

Zerotime0 2 years, 7 months ago

Agree here too e provides and defines scalability in this scenario.

upvoted 2 times

SUKABLED Highly Voted 2 years, 7 months ago

C and E for me too..who the hell come up with those questions

upvoted 16 times

SUKABLED 2 years, 7 months ago

However, I guess in the real exam, A and C will count for correct..

upvoted 6 times

Natalia89_er Most Recent 3 weeks, 2 days ago

Selected Answer: CE

A is not correct

A. asynchronous routing isn't a standard term related to WAN architecture. You might be thinking of "asymmetric routing," where packets between two points might take different paths for the outbound and return traffic. While this can happen in complex networks, it's not specifically a method for improving scalability and reliability.

upvoted 1 times

BJ221 1 month ago

Selected Answer: AC

I think A and C are corresc answers. In WAN architecture with dual-homed branches it is not problem and it can even increased network capacity and improved load balancing

upvoted 1 times

xbololi 2 months, 3 weeks ago

Selected Answer: CE

Based on scalability you need dynamic not static its too much work. Dual-homed is necessery for relaibilty. So C&E sounds more accurate for these rules.

upvoted 1 times

lsuzu 4 months, 3 weeks ago

C&E are correct
C. Dual-homed branches: This architecture involves connecting each branch office to two different routers or switches, allowing for redundancy in case of a network failure. This design ensures that if one of the network connections fails, the other can take over without any disruption, providing high availability and improved network reliability.

E. Dynamic routing: Dynamic routing is a type of routing protocol that allows routers to dynamically exchange information about network topology changes. This capability enables routers to adapt to network changes automatically and select the most efficient path for data transmission. Dynamic routing ensures network scalability, as new routers or network segments can be added without manual intervention, and it also improves network reliability by automatically rerouting traffic in the event of a network outage.

upvoted 5 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: CE

The two WAN architecture options that help a business scalability and reliability for the network are:

C. Dual-homed branches: Dual-homing involves connecting each branch office to two or more different WAN links, such as two different service providers, in order to provide redundancy and increase reliability. This architecture option enables the business to maintain network connectivity even if one of the WAN links fails. In addition, it can also provide better performance and scalability by balancing traffic across the multiple links.

E. Dynamic routing: Dynamic routing protocols enable routers to dynamically exchange information about the network topology and find the best path for data to travel. This allows for faster convergence in case of network changes and improves network scalability by automatically adjusting to changes in the network. Dynamic routing protocols also increase network reliability by providing redundancy and failover mechanisms.

upvoted 1 times

ipvoice 7 months, 2 weeks ago

Selected Answer: CE

I am guessing this answer; but I do not think dynamic routing is not an architecture

upvoted 3 times

Kosheema 9 months ago

Should be A and C

upvoted 1 times

HMaw 9 months, 1 week ago

Selected Answer: CE

Question: Which two WAN architecture options help a business scalability and reliability for the network?
Keyword: Reliability

Here is some reading to consider for Asynchronous routing

Issues to Consider with Asymmetric Routing

Asymmetric routing is not a problem by itself, but will cause problems when Network Address Translation (NAT) or firewalls are used in the routed path. For example, in firewalls, state information is built when the packets flow from a higher security domain to a lower security domain. The firewall will be an exit point from one security domain to the other. If the return path passes through another firewall, the packet will not be allowed to traverse the firewall from the lower to higher security domain because the firewall in the return path will not have any state information. The state information exists in the first firewall.
Ref: https://www.cisco.com/web/services/news/ts_newsletter/tech/chalktalk/archives/200903.html

upvoted 2 times

rivera82 9 months, 2 weeks ago

Selected Answer: AC

According to Google

upvoted 2 times

TR3Y 4 months, 1 week ago

Asynchronous routing is not *reliable* according to the keyword of the questions here. The wording almost got me too. Comparing the definitions with each other can provide more clarity. @HMaw posted the def. above.

upvoted 1 times

dick3311 10 months, 4 weeks ago

Selected Answer: AC

I prefer A and C

upvoted 2 times

esther18 11 months ago

A & C is the correct answer, you guys can google it

upvoted 2 times

AWSEMA 1 year, 2 months ago

Selected Answer: CE

I guess c&e

upvoted 1 times

ScorpionNet 1 year, 4 months ago

A and C are correct because it's asking for 2 WAN architecture

upvoted 3 times

SelamB 1 year, 6 months ago

Selected Answer: CE

The answer is C and E. Before the emergency of GRE and When WAN was using IPSec the main problem was its inability not being able to support multicast address for routing protocol to work. This leads to labor intensive manual configuration of IPSec tunnel. So they came up with GRE to make it support dynamic routing intern improving the scalability of WAN links.
I don't think anyone has a problem with the answer Dual homed for reliability

upvoted 2 times

agazi 1 year, 7 months ago

WAN technologies are very difficult to assign dynamic routing so A,C are correct answers

upvoted 3 times

Question #60 *Topic 1*

What is the binary pattern of unique ipv6 unique local address?

A. 00000000

B. 11111100

C. 11111111

D. 11111101

Correct Answer: *B*

A IPv6 Unique Local Address is an IPv6 address in the block FC00::/7, which means that IPv6 Unique Local addresses begin with 7 bits with exact binary pattern as 1111 110 -> Answer B is correct.

Note: IPv6 Unique Local Address is the approximate IPv6 counterpart of the IPv4 private address. It is not routable on the global Internet.

Community vote distribution

B (57%) D (43%)

Santhoshabraham1969 Highly Voted 2 years, 7 months ago

According to latest RFC, unique local address is FD00::/8. Hence option should be D

upvoted 31 times

Rob2000 Highly Voted 1 year, 11 months ago

Correct answer: B
IANA actually reserves prefix FC00::/7, and not
FD00::/8, for these addresses. FC00::/7 includes all addresses that begin with hex FC
IPv6 Unique local address are in the block of FC00::/7
So , the pattern is composed of the bits that don´t change
F - 1111
C - 1100
/7 - 1111110 Letter B
Letter D is
11111101 - FD , not a Unique Local Address

upvoted 19 times

dearc 5 months, 2 weeks ago

AI said: Thank you for providing the search results. Based on the majority of search results, the correct answer to this question is B. 11111100, as it refers to the first 7 bits of an IPv6 Unique Local Address which have an exact binary pattern of 1111 1100

upvoted 1 times

Junior_Network Most Recent 22 hours, 24 minutes ago

Just to be completely exact, IANA actually reserves prefix FC00::/7, and not
FD00::/8, for these addresses. FC00::/7 includes all addresses that begin with hex FC and
FD. However, an RFC (4193) requires the eighth bit of these addresses to be set to 1, which
means that in practice today, the unique local addresses all begin with their first two digits
as FD.

upvoted 1 times

Yinxs 2 weeks, 4 days ago

Selected Answer: D

The key bit is the eth bit, only according to the prefix that is 7, B and D are all correct.But, according to eh Cisco docuemnt, because the only legitimate value for the L flag(8th bit) is 1, the only valid ULA addresses today are in the fd00::/8 prefix.
https://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=4

upvoted 1 times

OrwellMB 2 months, 1 week ago

Selected Answer: B

The first 7 bits are set to "1111110," represented by "FC" in hexadecimal. This prefix identifies the address as a ULA.

The next bit, the 8th bit, is set to "0." This indicates that the address is not globally unique and is intended for private use within a specific organization or network.

upvoted 1 times

Natalie89 2 months, 2 weeks ago

Selected Answer: B

https://www.rfc-editor.org/rfc/rfc4193

FC00::/7 prefix to identify Local IPv6 unicast
addresses.

upvoted 1 times

Dunedrifter 2 months, 2 weeks ago

Selected Answer: B

ULAs are defined within the fd00::/8 prefix. The first 7 bits (binary pattern: 1111110) are fixed for ULAs. The next 1 bit (binary pattern: 1) is reserved for future use and should be set to 0.

So, the correct answer would be:

B. 1111110

upvoted 2 times

zbeugene7 3 months, 1 week ago

CCNA 200-301 Official Cert Guide , Volume 1, page 551 states it's 8 bits long and should have value FD, however RFC https://www.rfc-editor.org/rfc/rfc4193 stipulates:
Prefix FC00::/7 prefix to identify Local IPv6 unicast
addresses.
This last 8th bit makes the difference , it's FD if it's 8 bit long and FC if it's 7 , the question is is 8 or 7 ?

upvoted 1 times

Jorro99404 4 months ago

Selected Answer: B

B) FC00 = 11111100

upvoted 2 times

jonathan126 4 months, 3 weeks ago

Either FC (1111 1100) or FD (1111 1101). As per RFC 4193, local unicast address should satisfy below:
1) FC::/7 prefix (1111 1100)
2) The 8th bit should set to 1 if the prefix is locally assigned (1111 1101)
*Set to 0 may be defined in the future

Thus, the answer is D

upvoted 3 times

Zortex 6 months ago

Selected Answer: D

According to latest RFC, unique local address is FD00::/8.

upvoted 3 times

Nutanix_Dummy 6 months, 3 weeks ago

Selected Answer: D

according to https://www.apnic.net/wp-content/uploads/arin/assets/arin-vx-v6-ula.pdf states FD00::/8 is locally assigned and FC00::/8 is centrally assigned.

upvoted 1 times

SamuelSami 11 months, 1 week ago

OTE

For more information on ULA addresses with NAT66 or NPTv6, see Ed Horley's excellent articles on the topic, at www.howfunky.com. Horley has also written an excellent book, Practical IPv6 for Windows Administrators.

L Flag and Global ID

ULA addresses have the prefix fc00::/7, or the first 7 bits as 1111 110x. As shown in Figure 4-10, the eighth bit (x) is known as the L flag, or the local flag, and it can be either 0 or 1. This means that the ULA address range is divided into two parts:

fc00::/8 (1111 1100): When the L flag is set to 0, may be defined in the future.

fd00::/8 (1111 1101): When the L flag is set to 1, the address is locally assigned.

Because the only legitimate value for the L flag is 1, the only valid ULA addresses today are in the fd00::/8 prefix.

Another difference between ULA addresses and private IPv4 addresses is that ULA addresses can also be globally unique. This is helpful for ensuring that there won't be any conflicts when combining two sites using ULA addresses or just in case they get leaked out into the Internet.

upvoted 1 times

splashy 11 months, 3 weeks ago

Selected Answer: B

I think it's about range -> where do the 1's stop

11111100 FC00::/6 does not exclude FD
11111101 FD00::/8 excludes everything below FD

Netacad 7.02 Module 1 12.3.4
Unique local addresses range fc00::/7 to fdff::/7 ...

sorry for double post.

upvoted 1 times

splashy 11 months, 3 weeks ago

I think it's about range -> where do the 1's stop

11111100 FC00::/6 does not exclude FD
11111101 FD00::/8 excludes everything below FD

Netacad 7.02 Module 1 12.3.4
Unique local addresses range fc00::/7 to fdff::/7 ...

upvoted 1 times

shubhambala 1 year ago

Selected Answer: D

Answer is D

upvoted 2 times

g_mindset 1 year ago

Selected Answer: D

The answer is D. This is the current Unique Local Address being used. Check Official Certification Guide Volume 1, page 551(Unique Local Addresses).

upvoted 2 times

g_mindset 1 year ago

EXTRACT FROM FROM CERT GUIDE:

Just to be completely exact, IANA actually reserves the prefix FC00::/7, and not FD00::/8, for these addresses. FC00::/7 includes all addresses that begin with hex FC and FD. However, an RFC (4193) requires the eighth bit of these addresses to be set to 1, which means that in practice today, the unique local addresses all begin with their first two digits as FD.

upvoted 2 times

Question #61 *Topic 1*

Which two options are the best reasons to use an IPV4 private IP space? (Choose two.)

A. to enable intra-enterprise communication

B. to implement NAT

C. to connect applications

D. to conserve global address space

E. to manage routing overhead

Correct Answer: *AD*

Community vote distribution

AD (75%) AB (25%)

Ali526 Highly Voted 2 years, 8 months ago

AD correct.

upvoted 9 times

Utshav Most Recent 2 weeks, 6 days ago

A. Correct In an organization, using private IP space allows for communication within the enterprise without the need for globally unique IP addresses. Private IP addresses are not routable on the public Internet, so they are suitable for internal network communication.
C. Incorrect. Connecting applications does not specifically require the use of private IP space. Applications can use IP addresses from public or private address spaces, depending on the scenario

upvoted 1 times

Utshav 2 weeks, 6 days ago

D. Correct. One of the key reasons for using private IP space is to conserve global address space. IPv4 addresses are limited, and using private IP space for internal communication reduces the consumption of publicly routable addresses.

upvoted 1 times

BarkingSpider 1 month, 2 weeks ago

Selected Answer: AD

NAT does indeed solve the problem of non-routable private addresses on the public internet, which serves a purpose related to the question. But it is not, in and of itself, a REASON to implement private IPv4 addresses. So it is definitely not the correct answer. A&D are correct.

upvoted 1 times

kyleptt 2 months ago

Can't intra-enterprise communication be done with IPV6 ?

upvoted 1 times

Isuzu 4 months, 3 weeks ago

I see no one is looking at E.... Correct Answer: D & E

upvoted 1 times

dearc 5 months, 2 weeks ago

Selected Answer: AD

AI said:The correct answers to the question "Which two options are the best reasons to use an IPv4 private IP space?" are:

A. To enable intra-enterprise communication D. To conserve global address space

Private IP addresses can be used within an organization for communication between devices without the need for unique public addresses . This helps to conserve the limited supply of IPv4 addresses available globally, which is a finite resource. Private IP addresses are not routable on the public internet and can be used within an organization without conflicts with public addresses. Therefore, options A and D are the best reasons to use an IPv4 private IP space.

Option B- to implement NAT , option C- to connect applications, and option E- to manage routing overhead don't refer to the use of private IP addresses directly. However, NAT can be used to translate private addresses to public addresses for access to the internet.

upvoted 2 times

iMo7ed 7 months, 1 week ago

Selected Answer: AD

A and D are correct

upvoted 2 times

Bilal1992 7 months, 3 weeks ago

AD IS CORRECT

upvoted 2 times

DB_Cooper 8 months ago

Selected Answer: AB

A. To enable intra-enterprise communication: Private IP spaces allow devices within an enterprise to communicate with one another without the need to have globally unique IP addresses. This makes it easier to manage the internal network, and reduces the risk of IP address conflicts.

B. To implement Network Address Translation (NAT): NAT allows devices on a private IP network to communicate with devices on a public IP network. It allows a device on a private network to use a single unique public IP address to connect to the internet or other public IP networks.

Using private IP space in conjunction with NAT allows organization to keep their internal network private, while still providing access to the internet or other public IP network. It conserve global address space as it is not needed to use globally unique IP addresses for all internal devices.

upvoted 2 times

DB_Cooper 8 months ago

i change my answer to AD. disregard my comment

upvoted 9 times

jnanofrancisco 8 months, 1 week ago

A & D are correct

upvoted 1 times

onikafei 1 year, 6 months ago

Selected Answer: AD

A and D are correct

upvoted 1 times

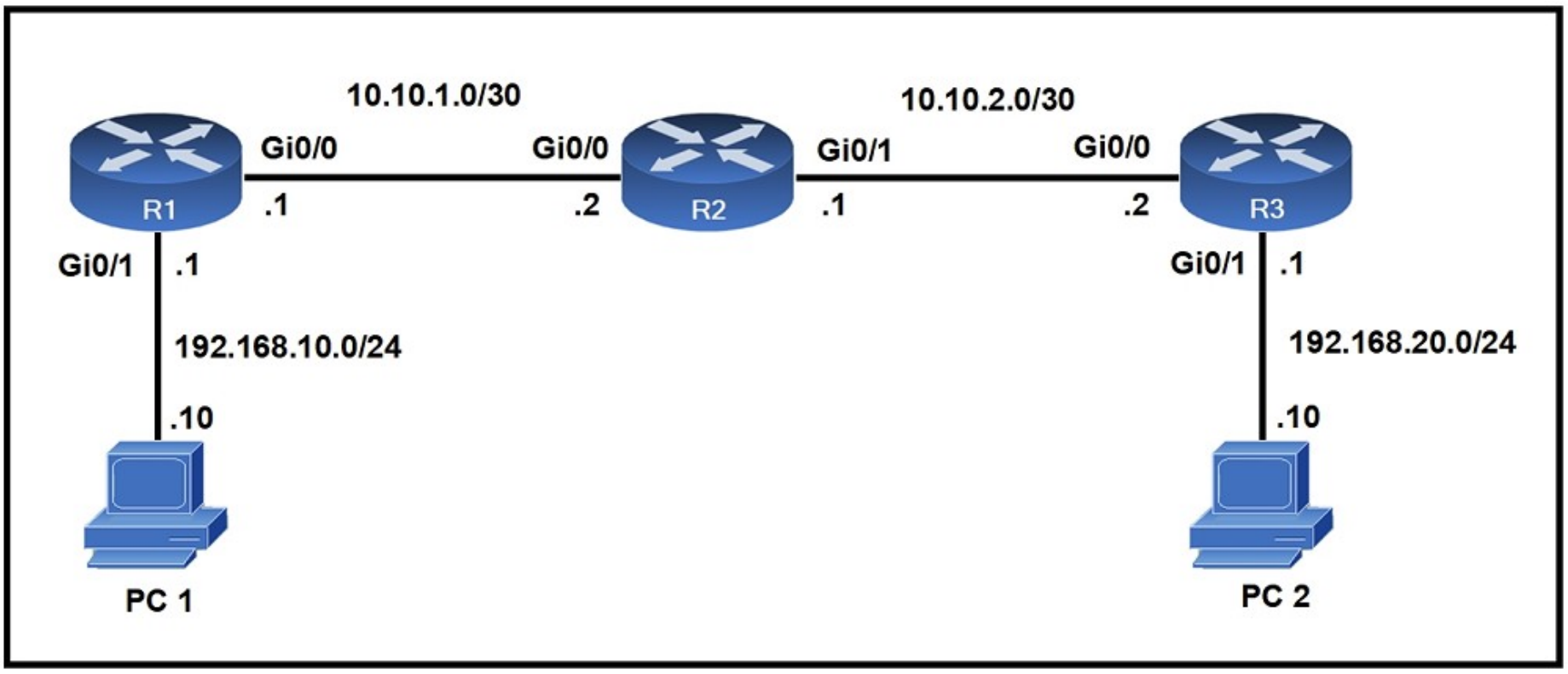
ZUMY 2 years, 4 months ago

A & D are correct

upvoted 3 times

Question #62 *Topic 1*

Refer to the exhibit. When PC1 sends a packet to PC2, the packet has which source and destination IP address when it arrives at interface Gi0/0 on router R2?



A. source 192.168.10.10 and destination 10.10.2.2

B. source 192.168.20.10 and destination 192.168.20.1

C. source 192.168.10.10 and destination 192.168.20.10

D. source 10.10.1.1 and destination 10.10.2.2

Correct Answer: *C*

The source and destination IP addresses of the packets are unchanged on all the way. Only source and destination MAC addresses are changed.

Community vote distribution

C (100%)

Hanagaki_Shinjiro 1 week, 2 days ago

Selected Answer: C

ONLY C

upvoted 1 times

Aie_7 8 months, 1 week ago

Selected Answer: C

C is the only one correct. MAC source and destination change, not ip source destination.

upvoted 1 times

LeeBlack 1 year, 3 months ago

C is the correct answer

upvoted 2 times

Cyberops 1 year, 4 months ago

c is correct answer

upvoted 1 times

sovafal192 1 year, 7 months ago

Selected Answer: C

No NAT in place, so C is OK.

upvoted 2 times

Heymannicerouter 2 years ago

C is correct

upvoted 4 times

Question #63 *Topic 1*

What is the same for both copper and fiber interfaces when using SFP modules?

A. They support an inline optical attenuator to enhance signal strength

B. They accommodate single-mode and multi-mode in a single module

C. They provide minimal interruption to services by being hot-swappable

D. They offer reliable bandwidth up to 100 Mbps in half duplex mode

Correct Answer: *C*

Community vote distribution

C (100%)

ZUMY Highly Voted 2 years ago

C is correct
Hot-Swap-Component that of device can be removed or install without powering down the device.
upvoted 11 times

peplegal 5 months ago

Yes, C is correct "HOT-SWAPPABLE" - just to complement, see bellow link with other types of SFP - Small Form-Factor Pluggable:

https://en.wikipedia.org/wiki/Small_Form-factor_Pluggable
Tks Zumy!
upvoted 1 times

Utshav Most Recent 2 weeks, 6 days ago

C. They provide minimal interruption to services by being hot-swappable.

Explanation:
SFP (Small Form-factor Pluggable) modules are used to provide flexibility in connecting networking equipment, such as switches and routers, to various types of network media, including both copper and fiber interfaces. One of the key features of SFP modules, whether they are used with copper or fiber connections, is their hot-swappable nature. Hot-swappability means that you can remove or replace the SFP module while the equipment is powered on, minimizing interruption to network services. This is a significant advantage for maintenance and upgrades in a network environment.
upvoted 1 times

Utshav 2 weeks, 6 days ago

The other options are not universally true for both copper and fiber interfaces with SFP modules:

A. Inline optical attenuators are typically used in fiber connections to reduce the signal strength and avoid overloading the receiver. This is not a common practice for copper connections with SFP modules.

B. SFP modules for fiber connections come in both single-mode and multi-mode variants, but the same module doesn't typically accommodate both types. Copper interfaces use different types of SFP modules altogether.

D. The bandwidth capability mentioned here (up to 100 Mbps in half duplex mode) doesn't accurately represent SFP modules. SFP modules can support a wide range of data rates, from 100 Mbps to 10 Gbps or even higher, depending on the specific module and the type of interface (copper or fiber).
upvoted 1 times

dearc 5 months, 2 weeks ago

Selected Answer: C

Based on the search results, the correct answer to the question "What is the same for both copper and fiber interfaces when using SFP modules?" is:

C. They provide minimal interruption to services by being hot-swappable

The other options mentioned in the search results refer to specific features of SFP modules , such as supporting an inline optical attenuator (option A), accommodating single-mode and multi-mode (option B), offering reliable bandwidth up to 100 Mbps in half duplex mode (option D).
upvoted 1 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: C

right answer is c
upvoted 1 times

erikkkkkka 1 year, 3 months ago

This tells u why c is correct
https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-

gbic-sfp-modules/datasheet-c78-366584.html
upvoted 1 times

Jbcrggddfhh 1 year, 4 months ago
"SFP modules are hot swappable and contain ID and system information for the switch."

https://www.pcmag.com/encyclopedia/term/sfp
upvoted 3 times

theRock2022 1 year, 5 months ago
A hot swap describes the act of removing components from or plugging them into a computer system while the power remains switched on. This means that parts can be changed without shutting down or rebooting a computer or server.
upvoted 4 times

Question #64 *Topic 1*

What are two functions of a server on a network? (Choose two.)

A. handles requests from multiple workstations at the same time

B. achieves redundancy by exclusively using virtual server clustering

C. housed solely in a data center that is dedicated to a single client achieves redundancy by exclusively using virtual server clustering

D. runs the same operating system in order to communicate with other servers

E. runs applications that send and retrieve data for workstations that make requests

Correct Answer: *AE*

Community vote distribution
AE (100%)

Sutokuto Highly Voted 9 months ago
Selected Answer: AE
If an answer choice has definitive language like "exclusively" or "solely" it's usually wrong.
upvoted 5 times

Utshav Most Recent 2 weeks, 6 days ago
The correct answers are:

A. Handles requests from multiple workstations at the same time.
E. Runs applications that send and retrieve data for workstations that make requests.

A. Correct .Servers are designed to handle requests from multiple clients or workstations simultaneously. This is one of their primary functions in a network environment. Examples of server types include web servers, file servers, and database servers.

E. Correct. One of the main functions of a server is to run applications that serve data and services to workstations that request them. This can include applications like web servers, email servers, and database servers.
upvoted 1 times

Utshav 2 weeks, 6 days ago
B. Incorrect. Virtual server clustering involves grouping multiple virtual servers together for improved availability and fault tolerance. While it can achieve redundancy, it's not the exclusive way to achieve redundancy, and it's not a direct function of a server.

C. Incorrect. This option does not describe a general function of servers on a network. While dedicated data centers and virtual server clustering might be strategies used for redundancy, this option is not a common function of servers.

D. Incorrect. Servers on a network can run different operating systems depending on their roles and the needs of the network. Communication between servers does not necessarily require them to run the same operating system.
upvoted 1 times

huykg009 9 months, 2 weeks ago
the Correct Answer is B and C
upvoted 1 times

huykg009 9 months, 2 weeks ago
Sorry the correct Answer is A and E
upvoted 3 times

Question #65 *Topic 1*

Which function is performed by the collapsed core layer in a two-tier architecture?

A. enforcing routing policies

B. marking interesting traffic for data policies

C. applying security policies

D. attaching users to the edge of the network

Correct Answer: *A*

Community vote distribution

A (100%)

Benjamin8189 Highly Voted 2 years ago

low cost at first but will be difficult to scale in future, because cable requirement increase, each new site require full mash to other building due no to centralize core, also increase routing complexity and addition routing peer needed in new protocol. Three-tier will be more efficient.

upvoted 10 times

Ciscoman021 Highly Voted 5 months, 3 weeks ago

Selected Answer: A

In a two-tier network architecture, the collapsed core layer typically combines the core and distribution layers of a three-tier architecture into a single layer. The main function of the collapsed core layer is to provide high-speed switching and routing of traffic between the distribution layer switches and the access layer switches. Therefore, the answer to your question is A. enforcing routing policies.

upvoted 5 times

Utshav Most Recent 2 weeks, 6 days ago

D. Attaching users to the edge of the network.

Explanation:

In a network design that follows a collapsed core architecture, the core and distribution layers are combined into a single layer. This design is often used in smaller networks to simplify the network architecture and reduce complexity.

The collapsed core layer primarily focuses on connecting end-user devices or access switches to the network. It aggregates traffic from the access layer and provides connectivity for users, servers, and other network devices. It's responsible for attaching users and devices to the edge of the network.

The other options (A, B, and C) are not typically specific functions performed by the collapsed core layer in a two-tier architecture. They may be associated with other layers or components in the network architecture.

upvoted 2 times

Isuzu 4 months, 3 weeks ago

Correct Answer is D. Attaching users to the edge of the network.
In a two-tier network architecture, the collapsed core layer serves as the middle layer between the access layer and the distribution layer. Its primary function is to provide high-speed connectivity for the distribution layer switches and to attach the users to the edge of the network.

Option A is incorrect because enforcing routing policies is typically done at the distribution layer.

Option B is incorrect because marking interesting traffic for data policies is also typically done at the distribution layer.

Option C is incorrect because applying security policies is typically done at the access layer, distribution layer, and sometimes the core layer, depending on the network design.

upvoted 1 times

xbololi 2 months, 3 weeks ago

There is no distribution layer at tier2... So collapsed core layer works as core and distribution.
https://i.ytimg.com/vi/ZmLxb8HzQX4/maxresdefault.jpg

upvoted 1 times

moise_amo 7 months, 2 weeks ago

Selected Answer: A

A is the corect answer

upvoted 3 times

JulietaMT98 1 year, 6 months ago

Selected Answer: A

In collapsed core architecture, the core and distribution layers are combined, simplifying the design.

upvoted 5 times

ZUMY 2 years ago

A is correct

upvoted 2 times

SScott 2 years ago

A is correct.

upvoted 1 times

Question #66 *Topic 1*

What is the primary function of a Layer 3 device?

A. to transmit wireless traffic between hosts

B. to analyze traffic and drop unauthorized traffic from the Internet

C. to forward traffic within the same broadcast domain

D. to pass traffic between different networks

Correct Answer: *D*

Community vote distribution

D (100%)

Bhrino 4 months, 1 week ago

Layer 3 = different network
Layer 2: same network

upvoted 2 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: D

The primary function of a Layer 3 device is to pass traffic between different networks.

upvoted 1 times

Aie_7 8 months, 1 week ago

Selected Answer: D

You could be wrong answering A thinking about firewalls, but the primary function of layer 3 devices is precisely to forward traffic between networks.

upvoted 2 times

kenCapt 11 months, 1 week ago

Layer 3 devices are Routers which is used to pass traffic between different LANs, whereas layer 2 devices are Switches that only broadcast traffic in its domain but not to other LANS.D is absolutely correct

upvoted 3 times

ScorpionNet 1 year, 4 months ago

Basically functions between Routers, Layer 3 switches especially the Firewall enabled

upvoted 1 times

RichyES 1 year, 7 months ago

Selected Answer: D

D is the the answer

upvoted 4 times

Hodicek 1 year, 10 months ago

ROUTER FUNSTION IN SUMMARY

upvoted 3 times

ZUMY 2 years ago

D is correct

upvoted 2 times

Question #67 *Topic 1*

Which two functions are performed by the core layer in a three-tier architecture? (Choose two.)

A. Provide uninterrupted forwarding service

B. Inspect packets for malicious activity

C. Ensure timely data transfer between layers

D. Provide direct connectivity for end user devices

E. Police traffic that is sent to the edge of the network

Correct Answer: *AC*
Reference:
https://www.mcmcse.com/cisco/guides/hierarchical_model.shtml

Community vote distribution

AC (100%)

Jbcrggddfhh Highly Voted 1 year, 4 months ago

"Core layer: This layer is considered the backbone of the network and includes the high-end switches and high-speed cables such as fiber cables. This layer of the network does not route traffic at the LAN. In addition, no packet manipulation is done by devices in this layer. Rather, this layer is concerned with speed and ensures reliable delivery of packets."

https://www.mcmcse.com/cisco/guides/hierarchical_model.shtml

upvoted 7 times

ricky1802 Highly Voted 7 months, 2 weeks ago

Selected Answer: AC

In a three-tier architecture, the core layer is the central part of the network that provides high-speed switching and routing services to other network segments. The core layer is responsible for forwarding data between distribution layers and other network segments, and for ensuring efficient and reliable data transmission.

The core layer is designed to be highly available, scalable, and redundant, and typically uses high-speed network switches and routers. The core layer provides the backbone for the network, and is critical to the overall performance and reliability of the system. It is usually placed at the center of the network, and is optimized for speed and low latency to provide high-speed connectivity between the distribution layers. The core layer also provides a centralized point for network management and monitoring.

upvoted 5 times

sany11 Most Recent 4 months, 3 weeks ago

Selected Answer: AC

this layer is concerned with speed and ensures reliable delivery of packets.

upvoted 2 times

Sauceboyzzjp 1 year, 7 months ago

this design is very clear it only meant to forward traffic as fast as possible

upvoted 4 times

ZUMY 2 years ago

A,C Correct

upvoted 3 times

ZUMY 2 years ago

Core – also referred to as the network backbone, this layer is responsible for transporting large amounts of traffic quickly. The core layer provides interconnectivity between distribution layer devices it usually consists of high speed devices, like high end routers and switches with redundant links.

upvoted 2 times

Shaz313 2 years, 2 months ago

Core – also referred to as the network backbone, this layer is responsible for transporting large amounts of traffic quickly. The core layer provides interconnectivity between distribution layer devices it usually consists of high speed devices, like high end routers and switches with redundant links.

upvoted 2 times

Shaz313 2 years, 2 months ago

The function of the core layer is to provide fast and efficient data transport. Characteristics of the core layer include the following: The core layer is a high-speed backbone that should be designed to switch packets as quickly as possible to optimize communication transport within the network

upvoted 2 times

4guysgaming 2 years, 2 months ago

given answers are correct

upvoted 2 times

lordnano 2 years, 6 months ago

Things like packet inspection is a separate network service and is not part of the 3-tier architecture model.
Also think about network design with network virtualization. The inspection of the workload traffic can be completely decoupled of the the physical layers.

I would stick to A and C. That fits also to the reference link.

upvoted 4 times

1Mohit1 2 years, 2 months ago

Agreed A and C make the most sense.

upvoted 2 times

SScott 2 years ago

That is right. A & C would be the primary two functions of core w/three-tier. I'd have to say B inspection/ATP would fall more under the immediate Distribution Layer following Core traffic management.
https://blog.router-switch.com/2012/05/cisco-network-the-cisco-3-layered-hierarchical-model/

upvoted 1 times

Shaaaaane 2 years, 6 months ago

Agreed, answer is A and B

upvoted 2 times

Nicocisco 1 year, 6 months ago

Policy is in distribution layer

upvoted 1 times

imad 2 years, 6 months ago

correct answers are a and b

upvoted 3 times

Nicocisco 1 year, 6 months ago

Policy is in distribution layer

upvoted 1 times

Question #68 *Topic 1*

What is a recommended approach to avoid co-channel congestion while installing access points that use the 2.4 GHz frequency?

A. different nonoverlapping channels

B. one overlapping channel

C. one nonoverlapping channel

D. different overlapping channels

Correct Answer: *A*

Community vote distribution

A (70%) C (30%)

Scooter96 Highly Voted 2 years, 1 month ago

I agree, A. it is. Each AP operates in one channel. The goal is that neighboring APs don't use the same channel, so you need multiple non-overlapping channel, or you have co-channel interference, which slows down your wireless operation. (Adjacent channel interference causes collisions)

upvoted 15 times

ZUMY Highly Voted 2 years ago

A is correct

upvoted 8 times

dearc Most Recent 5 months, 2 weeks ago

Selected Answer: A

The correct answer to the question "What is a recommended approach to avoid co-channel congestion while installing access points that use the 2.4 GHz frequency?" is:

A. different non-overlapping channels

This is a commonly recommended approach to avoid co-channel interference when deploying multiple access points that use the 2.4 GHz frequency band . Channels 1, 6, and 11 are non-overlapping channels that are commonly used for this purpose.

Options B, C, and D are not recommended because they involve using overlapping channels, which can lead to interference and reduced performance.

upvoted 2 times

vnn777 7 months ago

Selected Answer: A

1,6,11 channels to avoid co-channel interruption.

upvoted 1 times

Mokonyana 7 months, 1 week ago

i think the keyword is "co-channel". I would say the right answer is A.

upvoted 2 times

Fab79 8 months, 4 weeks ago

Selected Answer: A

A correct

upvoted 4 times

Abdullahalbsheesh 9 months, 1 week ago

Selected Answer: C

C is correct

upvoted 2 times

dendentester 11 months, 1 week ago

C IS CORRECT

upvoted 1 times

saeed_huhu 1 year, 1 month ago

Selected Answer: C

The question said " co-channel " so 1-6-11 is already in use
best answer is C .

upvoted 1 times

BitterOldMan 1 year, 4 months ago

Seems like C is a better choice, as 2.4Ghz uses one channel and A refences channels. So, basically move it to one other nonoverlapping channel.

upvoted 1 times

Smaritz 1 year, 3 months ago

I think they are referring to multiple access points, not just 2.

upvoted 2 times

Nebulise 1 year, 7 months ago

Channels 1, 6 and 11 are the non-overlapping channels used in the 2.4GHz range

upvoted 2 times

Question #69 *Topic 1*

A manager asks a network engineer to advise which cloud service models are used so employees do not have to waste their time installing, managing, and updating software that is only used occasionally. Which cloud service model does the engineer recommend?

A. infrastructure-as-a-service

B. platform-as-a-service

C. business process as service to support different types of service

D. software-as-a-service

Correct Answer: *D*

Community vote distribution

D (100%)

mugtaba 4 months, 1 week ago

aswer D

upvoted 1 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: D

The cloud service model that the network engineer would recommend for employees to avoid wasting time installing, managing, and updating software that is only used occasionally is "software-as-a-service" (SaaS).

upvoted 1 times

Peterpiper 1 year, 11 months ago

D is the right answer.

upvoted 2 times

Hanagaki_Shinjiro 1 week, 2 days ago

TELL ME WHY

upvoted 1 times

ZUMY 2 years ago

D is correct

upvoted 3 times

DonnerKomet 2 years ago

SaaS provides te required Software, operating system and network:
Provides ready-to-use application or software

upvoted 3 times

SScott 2 years ago

Yes D occasional hosted application is SaaS
https://www.cloudflare.com/learning/cloud/what-is-saas/

upvoted 1 times

shakyak 1 year, 10 months ago

Occasionally has nothing to do with Saas. It's just there to trick you.

upvoted 2 times

Question #70 *Topic 1*

What are two functions of a Layer 2 switch? (Choose two.)

A. acts as a central point for association and authentication servers

B. selects the best route between networks on a WAN

C. moves packets within a VLAN

D. moves packets between different VLANs

E. makes forwarding decisions based on the MAC address of a packet

Correct Answer: *CE*

Community vote distribution

CE (100%)

ismatdmour Highly Voted 1 year, 6 months ago

Selected Answer: CE

C and E. Little confusion at first about E because of the use of the word "Packet" which is a layer 3 term rather than using "Frame" for a layer 2 concept. However, we need to remember that packet is a general term that is also used to replace other terms like a "frame" of other layers. CISCO questions like this tend to use it as well. Also, a L3 packet encapsulates a L2 frame which in turn embed a frame.

upvoted 10 times

Hanagaki_Shinjiro Most Recent 1 week, 2 days ago

Selected Answer: CE

C and E are correct. If you want to move packets between many VLANs, you have to use layer 3 devices.

upvoted 1 times

bikila123 1 month, 2 weeks ago

not a packet its frame...since its layer 2

upvoted 1 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: CE

C. Moves packets within a VLAN, and E. makes forwarding decisions based on the MAC address of a packet.

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: CE

Even if no answer talks about “frames”, but only “packets” are mentioned, just focus on what a Layer 2 switch DOES, not ON WHAT a Layer 2 switch operates.

A. acts as a central point for association and authentication servers

I think a WLC does this: “association” means a wireless device which associates with a lightweight AP, and an “authentication server” can be a RADIUS server configured on a WLC to authenticate wireless users.
To me, wrong answer.

B. selects the best route between networks on a WAN

A router’s job.
Wrong answer.

C. moves packets within a VLAN

Yes, a Layer 2 switch does this.
Correct answer.

D. moves packets between different VLANs

Well, inter-VLANs routing implies a Layer 3 switch, not a Layer 2 one.
Wrong answer.

E. makes forwarding decisions based on the MAC address of a packet

Yes, the typical use of a Layer 2 switch.
Correct answer.

upvoted 4 times

saeed_huhu 1 year, 1 month ago

Selected Answer: CE

You need Router On Stick to route VLAN - so A-E
D is incorrect

upvoted 1 times

ismatdmour 1 year, 6 months ago

I meant to say "encapsulates a L2 frame which in turn embed a MAC address"

upvoted 2 times

panagiss 1 year, 10 months ago

Is it not possible to transfer packets between different VLANs? In case a 2 Vlans are in the same Subnet of course

upvoted 1 times

Nicocisco 1 year, 6 months ago

We need L3 switches to transfer different VLAN

upvoted 3 times

ScorpionNet 1 year, 4 months ago

Or a Router with subinterfaces configured

upvoted 1 times

babaKazoo 1 year, 10 months ago

C and E are correct put a switch moves frames and not packets.

upvoted 3 times

ZUMY 2 years ago

C,E are correct

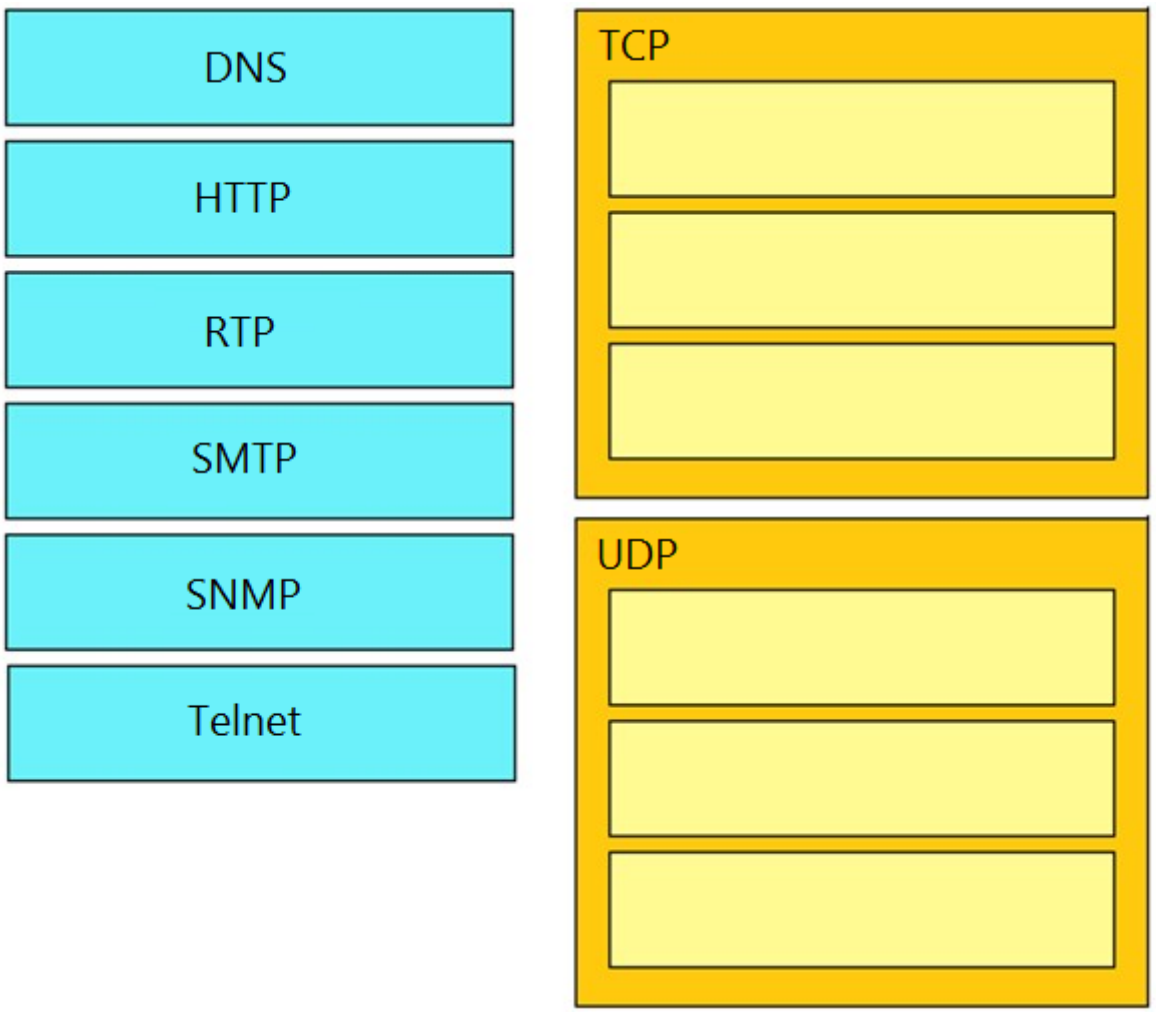
upvoted 2 times

Question #71 *Topic 1*

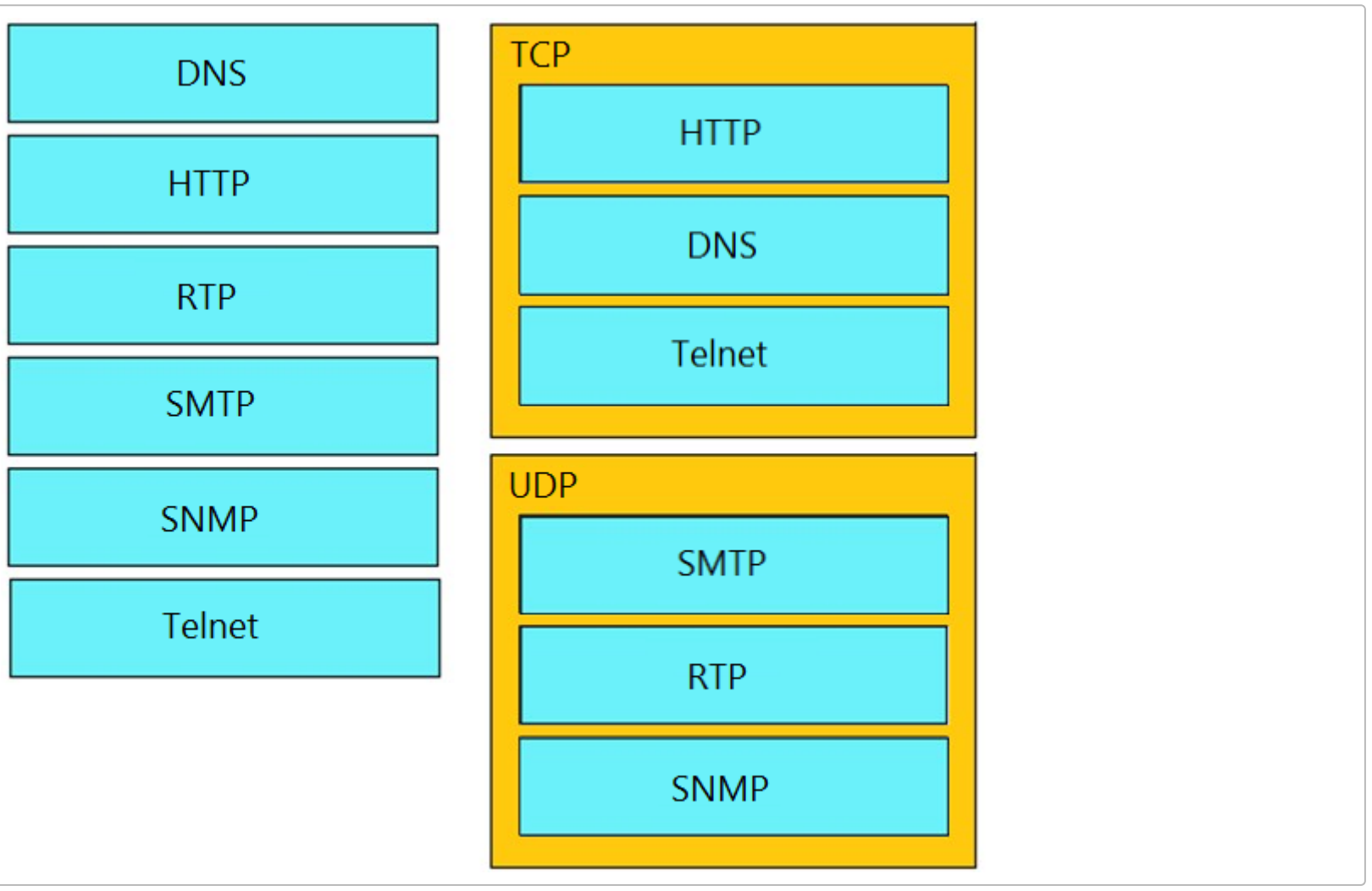
DRAG DROP -

Drag and drop the TCP/IP protocols from the left onto their primary transmission protocols on the right.

Select and Place:



Correct Answer:



splashy Highly Voted 1 year ago

HTTP
SMTP
Telnet (can be used to test tcp connectivity not udp)

DNS
RTP
SNMP

DNS is mostly UDP Port 53, but as time progresses, DNS will rely on TCP Port 53 more heavily. DNS has always been designed to use both UDP and TCP port 53 from the start1 , with UDP being the default, and fall back to using TCP when it is unable to communicate on UDP, typically when the packet size is too large to push through in a single UDP packet.

upvoted 56 times

esther18 Highly Voted 11 months ago

TCP- HTTP, SMTP, Telnet

UDP- DNS, RTP, SNMP

upvoted 22 times

Koda88 Most Recent 1 day, 16 hours ago

The question reads "primary transfer protocol". I am certain DNS would have UDP considered as its primary.

Also, SMTP uses TCP for its protocol. So I believe the DNS (under TCP) and SMTP (under UDP) need to be swapped in the Correct Answer for it to be actually correct.

upvoted 1 times

xbololi 2 months, 3 weeks ago

"primary transmission protocols" DNS uses UDP firstly then uses TCP in case.
HTTP
SMTP
Telnet/SSH

DNS
RTP
SNMP

upvoted 1 times

Bingchengchen236 3 months ago

RTP use UDP, the answer is incorrect. correct me if i am wrong.

upvoted 3 times

Danishh 4 months, 1 week ago

TCP - HTTP, SMTP, Telnet,FTP, SSH, POP3, HTTPS

UDP - DHCP, DHCP(client), TFTP, SNMP,

TCP & UDP - DNS (53)

upvoted 3 times

Hope_12 4 months, 2 weeks ago

SMTP is TCP port 25. SMTP should be in TCP bracket not in UDP.
DNS is UDP/TCP port 53. However it is initially UDP unless the messages are larger than 512 bytes then it will use TCP.

upvoted 1 times

jnanofrancisco 8 months, 1 week ago

HTTP, SMTP, TELNET

DNS, RTP, SNMP

upvoted 2 times

freeknowledge123 8 months, 2 weeks ago

smtp use tcp please correct the answer

upvoted 6 times

Kosheema 8 months, 4 weeks ago

TCP:SMTP, Telnet, HTTP
UDP: RTP, DNS, SNMP

upvoted 2 times

Kosheema 8 months, 4 weeks ago

SMTP is a TCP. Are the answers of this pool correct?

upvoted 2 times

Garfieldcat 10 months, 3 weeks ago

SMTP is TCP

upvoted 4 times

santoshSre 11 months ago

SMTP and DNS are TCP right?

upvoted 3 times

SamuelSami 11 months, 1 week ago

Is RTP port TCP or UDP?

RTP applications can use the Transmission Control Protocol (TCP), but most use the User Datagram protocol (UDP) instead because UDP allows for faster delivery of data.

upvoted 1 times

J0_e 11 months, 4 weeks ago

SMTP is TCP
upvoted 2 times

j6 11 months, 3 weeks ago
thank you i thought it was
upvoted 1 times

Danielki 1 year, 4 months ago
Isn't it DNS use both UDP AND TCP?
upvoted 3 times

ZUMY 1 year, 4 months ago
Given answers are correct!
upvoted 1 times

Bibi20 1 year ago
Nope SMTP is TCP
upvoted 3 times

Question #72 *Topic 1*

An engineer observes high usage on the 2.4GHz channels and lower usage on the 5GHz channels. What must be configured to allow clients to preferentially use
5GHz access points?

A. Client Band Select

B. Re-Anchor Roamed Clients

C. OEAP Spilt Tunnel

D. 11ac MU-MIMO

Correct Answer: *A*

Community vote distribution

A (100%)

Shaz313 Highly Voted 2 years, 2 months ago

Band Select is Cisco's terminology for Band Steering. When enabled it encourages stations onto the 5 GHz band. This is achieved by suppressing 2.4 GHz probe response frames to station probe requests and by responding with 5 GHz probe response frames first.

upvoted 18 times

GreatDane Highly Voted 8 months, 2 weeks ago

Selected Answer: A

Ref: Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Gibraltar 16.12.x

"C H A P T E R 47

Information About Configuring Band Selection, 802.11 Bands, and Parameters

Band Select

Band select enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the device.
..."

upvoted 5 times

Utshav Most Recent 2 weeks, 5 days ago

A. Client Band Select
To encourage clients to preferentially use 5GHz access points over 2.4GHz access points, the "Client Band Select" feature should be configured. This feature helps in steering clients to the less congested and higher-performance 5GHz frequency band, which typically offers more available channels and less interference compared to the often crowded 2.4GHz band.

upvoted 1 times

geober 10 months, 3 weeks ago

Band select enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point so the answer is A

upvoted 2 times

Vlad_Is_Love_ua 1 year ago

What is client band select?
Band Select is Cisco's terminology for Band Steering. When enabled it encourages stations onto the 5 GHz band. This is achieved by suppressing 2.4 GHz probe response frames to station probe requests and by responding with 5 GHz probe response frames first.

upvoted 2 times

ZUMY 1 year, 4 months ago

A is correct

upvoted 2 times

AlexMD 1 year, 10 months ago

A is correct answer

upvoted 1 times

Shaz313 2 years, 2 months ago

Band select enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested.

upvoted 4 times

Question #73 *Topic 1*

Which networking function occurs on the data plane?

A. processing inbound SSH management traffic

B. sending and receiving OSPF Hello packets

C. facilitates spanning-tree elections

D. forwarding remote client/server traffic

Correct Answer: *D*

Community vote distribution

D (90%) 10%

Shaz313 Highly Voted 2 years, 2 months ago

Networking devices operate in two planes; the data plane and the control plane. The control plane maintains Layer 2 and Layer 3 forwarding mechanisms using the CPU. The data plane forwards traffic flows

upvoted 15 times

DonnerKomet 2 years ago

I think, this question refers to SDN terminology, so the data plane takes care of forwarding ans uses the tables created by control plane to do it.

upvoted 3 times

Kane002 Highly Voted 1 year, 8 months ago

The data plane is also sometimes referred to as the "Forwarding plane".

upvoted 11 times

Utshav Most Recent 2 weeks, 5 days ago

D. forwarding remote client/server traffic

The data plane, also known as the forwarding plane or user plane, is responsible for the actual forwarding and processing of network traffic. This includes forwarding user data packets between network devices. Option D, "forwarding remote client/server traffic," is the networking function that occurs on the data plane. It involves moving data packets from one interface to another based on their destination addresses, without involving decisions related to network management or control protocols.

upvoted 1 times

Ciscoman021 5 months ago

Selected Answer: D

The networking function that occurs on the data plane is forwarding remote client/server traffic.

The data plane is responsible for forwarding user traffic through the network, and it is implemented by forwarding devices such as switches and routers. The other options listed, such as processing inbound SSH management traffic, sending and receiving OSPF Hello packets, and facilitating spanning-tree elections, are functions that occur on the control plane, which is responsible for managing and configuring the network devices.

upvoted 3 times

iMo7ed 7 months, 1 week ago

Selected Answer: D

It is D

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: D

Ref: IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols

"Chapter 3
Planes of Operation
...
• The data plane: The data plane is the forwarding plane, which is responsible for the switching of packets through the router (that is, process switching and CEF switching). In the data plane, there could be features that could affect packet forwarding such as quality of service (QoS) and access control lists (ACLs).
..."

upvoted 2 times

Fab79 8 months, 4 weeks ago

Selected Answer: D

D is correct

upvoted 3 times

guynetwork 1 year ago

It is D

upvoted 1 times

sasquatchshrimp 1 year, 1 month ago

Selected Answer: C

I am reading the question as "What network operation operates on the data plane(osi layer 2). STP is strictly a layer 2 protocol. So I would go with that since the other options are vague and D includes remote client/server forwarding, and those connections would be TCP which is layer 3. Crappy question, but STP is the only option that strictly adhears to layer 2, unless the question needs to be "interpreted" by aliens and "technically" means something no one would ever intent those words to mean.

upvoted 1 times

sasquatchshrimp 1 year, 1 month ago

I recant my answer. D sounds better with how silly the question and answers are worded.

upvoted 2 times

splashy 1 year, 1 month ago

Dont answer this questions with the osi layers, its not about that. Its about functions in the data plan vs control plane. Nothing to do with osi layers.

upvoted 5 times

Jbcrggddfhh 1 year, 4 months ago

D is correct since traffic forwarding is in the data plane:
"The data plane is the forwarding plane, which is responsible for the switching of packets through the router (that is, process switching and CEF switching)."
Reference: https://www.ciscopress.com/articles/article.asp?p=2272154&seqNum=3

upvoted 1 times

Jbcrggddfhh 1 year, 4 months ago

A is incorrect since SSH management traffic is in the management plane:
"The management plane is used to manage a device through its connection to the network.
Examples of protocols processed in the management plane include Simple Network Management Protocol (SNMP), Telnet, File Transfer Protocol (FTP), Secure FTP, and Secure Shell (SSH)."
Reference: https://www.ciscopress.com/articles/article.asp?p=2272154&seqNum=3

B is incorrect since OSPF is in the control plane:
"The control plane is the brain of the router. It consists of dynamic IP routing protocols (that is OSPF, IS-IS, BGP, and so on)"
Reference: https://www.ciscopress.com/articles/article.asp?p=2272154&seqNum=3

C is incorrect since STP is in the control plane:
"Typically, STP, VTP, and routing protocols are used in the control plane to create routing tables, forwarding tables, and other tables."
Reference: https://www.ciscopress.com/articles/article.asp?p=2928193&seqNum=3

upvoted 10 times

Question #74 *Topic 1*

Under which condition is TCP preferred over UDP?

A. UDP is used when low latency is optimal, and TCP is used when latency is tolerable.

B. TCP is used when dropped data is more acceptable, and UDP is used when data is accepted out-of-order.

C. TCP is used when data reliability is critical, and UDP is used when missing packets are acceptable.

D. UDP is used when data is highly interactive, and TCP is used when data is time-sensitive.

Correct Answer: *C*

Community vote distribution

C (87%) 13%

i_am_confused Highly Voted 1 year, 2 months ago

Selected Answer: C

C explains why you would pick TCP over UDP. A explains why you would pick UDP over TCP.

upvoted 10 times

kevy250 Most Recent 4 weeks, 1 day ago

C is correct

upvoted 1 times

iMo7ed 7 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

remoto 9 months, 1 week ago

Selected Answer: C

ok the answer

upvoted 1 times

santoshSre 11 months ago

Both A and C are correct, since udp is connection less the latency will be much lower compared to TCP.

upvoted 2 times

hammy1924 1 year ago

I think while A and C are both true, C is correct in this context as the question asks for when TCP is preferred.

upvoted 3 times

Cyberops 1 year, 4 months ago

C is the correct answer

upvoted 1 times

ZUMY 1 year, 4 months ago

C : is correct

upvoted 1 times

JonCCNA12 1 year, 5 months ago

I hate how A is worded ...What do you mean by optimal ? But C is correct.I look at UDP as gaming and TCP as simply browsing the internet.

upvoted 3 times

DuncanDUNC 1 year, 6 months ago

C is the most correctness.

upvoted 1 times

chrisp31 1 year, 6 months ago

Selected Answer: C

C is most correct. Connection based, need to get packets and verify.

upvoted 1 times

ismatdmour 1 year, 6 months ago

Selected Answer: C

C is correct for the current question context "Under which condition is TCP preferred over UDP?". However, A will be the answer for alternative question context of "Under which condition is UDP preferred over TCP?". Be ware

upvoted 3 times

onikafei 1 year, 6 months ago

Selected Answer: C

A and C are both correct, however in this case your going to want to tcp to transmit critical data. You arent going to pick TCP or UDP over latency

upvoted 2 times

Namek 1 year, 7 months ago

Selected Answer: C

The correct answer is C

upvoted 1 times

Nicocisco 1 year, 7 months ago

Selected Answer: C

It's C, it can't be A because you're not going to choose TCP just because you have latency

upvoted 1 times

Dante_Dan 1 year, 7 months ago

Selected Answer: A

I think the answer must be A: an application such as VoIP it is imperative that the latency is minimal; and we know tha in TCP latency is tolerable as it uses retransmission in case it loses packets, which it could cause latency.

In the given answer C: well indeed in TCP data reliability is important, but in UDP missing packets could be catastrophic, let's take a look at the VoIP example again: missing packets during a call, or worse, in a videocall will cause severe communication problems.

upvoted 3 times

awashenko 1 year, 6 months ago

I think you're overthinking the question. Option C would be the best response as TCP is is for critical applications and when you do not want any drops. UDP can be used when you need fast and "mostly reliable" transmissions like VOIP.

upvoted 1 times

Chupacabro 1 year, 8 months ago

tcp PREFERRED over udp, meaning the advantages of TCP. A might be right but UDP preference isn't being asked.

upvoted 3 times

```
SiteA#show interface TenGigabitEthernet0/1/0
TenGigabitEthernet0/1/0 is up, line protocol is up
  Hardware is BUILT-IN-EPA-8x10G, address is 780c.f02a.db91 (bia 780a.f02b.db91)
  Description: Connection to SiteB
  Internet address is 10.10.10.1/30
  MTU 8146 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 166/255, txload 1/255, rxload 1/255
  Full Duplex, 10000Mbps, link type is force-up, media type is SFP-LR
  5 minute input rate 264797000 bits/sec, 26672 packets/sec
  5 minute output rate 122464000 bits/sec, 15724 packets/sec

SiteB#show interface TenGigabitEthernet0/1/0
TenGigabitEthernet0/1/0 is up, line protocol is up
  Hardware is BUILT-IN-EPA-8x10G, address is 780c.f02c.db26 (bia 780c.f02c.db26)
  Description: Connection to SiteA
  Internet address is 10.10.10.2/30
  MTU 8146 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Full Duplex, 10000Mbps, link type is force-up, media type is SFP-LR
  5 minute input rate 122464000 bits/sec, 15724 packets/sec
  5 minute output rate 264797000 bits/sec, 26672 packets/sec
```

Refer to the exhibit. Shortly after SiteA was connected to SiteB over a new single-mode fiber path, users at SiteA report intermittent connectivity issues with applications hosted at SiteB. What is the cause of the intermittent connectivity issue?

A. Interface errors are incrementing.

B. High usage is causing high latency.

C. An incorrect SFP media type was used at SiteA.

D. The sites were connected with the wrong cable type.

Correct Answer: *A*

The only indicator of any issues here is the reliability 166/255 on SiteA. When the input and output errors increase, they affect the reliability counter. This indicates how likely it is that a packet can be delivered or received successfully. Reliability is calculated like this: reliability = number of packets / number of total frames.
The value of 255 is the highest value meaning that the interface is very reliable at the moment. The calculation above is done every 5 minutes.

Community vote distribution

A (71%) B (29%)

Zara2stra Highly Voted 2 years, 3 months ago

reliability 255/255: When the input and output errors increase, they affect the reliability counter. This indicates how likely it is that a packet can be delivered or received succesfully. Reliability is calculated like this: reliability = number of packets / number of total frames. The value of 255 is the highest value meaning that the interface is very reliable at the moment. The calculation above is done every 5 minutes.
So answer A is correct.

upvoted 17 times

LordScorpius 1 year, 4 months ago

Yes but, this definition is for "Reliability" which could be composed of unknown factors, none of which are specifically stating, "Interface Errors". Could be. What is the CAUSE? The only indication is throughput is blowing up the link. High volume of frames.

upvoted 1 times

zbeugene7 3 months, 1 week ago

Interface errors could be the cause for whatever unknown reason, , because of problems with the interface, it's not saying counter is the cause

upvoted 1 times

SScott 2 years ago

The output shows many interface errors within the past five minutes and A is correct. The txload/rxload are not experiencing any performance or utilization issues so not B.

https://www.linkedin.com/pulse/get-know-cisco-ios-show-interfaces-command-basic-network-kumari#:~:text=When%20the%20input,at%20the%20moment.

https://packetlife.net/blog/2011/jul/8/evaluating-txload-and-rxload/#:~:text=txload%20and%20rxload%20roughly%20measure%20the%20amount%20of%20traffic%20passing%20out%20of%20and%20into%20an%20interface%2C%20respectively%2C%20relative%20to%20its%20perceived%20bandwidth

upvoted 3 times

RougePotatoe Highly Voted 10 months, 4 weeks ago

Why aren't people reading the question? It asks what is causing the issue not can you confirm the issue. Yes the reliability is down BUT WHY IS IT DOWN? That is the question not if there is an issue with reliability. We know there is a problem with reliability the question stated it and is confirmed by the reliability counter.

upvoted 7 times

Hope_12 Most Recent 4 months, 1 week ago

Selected Answer: B

A is result not the cause which is the one asked in the question.

upvoted 2 times

Rydaz 4 months, 1 week ago

txload and rxload are low... so it can't be high usage right?

upvoted 1 times

VictorCisco 5 months ago

Error increase is not the cause of the issue is the consequence/result of the issue!! A wrong cabel could be an issue...

upvoted 2 times

gc999 6 months, 1 week ago

I think A is the outcome, not the cause. So answer is B

upvoted 1 times

shutie 7 months ago

I had had an confusing idea why A is correct, not B because of what the question says UNTIL I found rx/rxload indicatior show 1/255, which refers to very low amount of traffic you are sending/receiving.
Therefore it's safely said that In/Output rate is not problematic at all.

upvoted 2 times

iMo7ed 7 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: A

Shortly after SiteA was connected to SiteB over a new single-mode fiber path, users at SiteA report intermittent connectivity issues with applications hosted at SiteB. What is the cause of the intermittent connectivity issue?

All parameters are equal between SiteA and SiteB, except for “reliability”.

Ref: Cisco IOS Show Interface Explained - networklessons.com

“…
reliability 255/255: When the input and output errors increase, they affect the reliability counter. This indicates how likely it is that a packet can be delivered or received succesfully. Reliability is calculated like this: reliability = number of packets / number of total frames. The value of 255 is the highest value meaning that the interface is very reliable at the moment. The calculation above is done every 5 minutes.
…”

This means that “reliability = 255/255” indicates a perfectly working interface (SiteB), while “reliability = 166/255” means that the interface is experiencing transmission/reception errors (SiteA).

upvoted 3 times

Elidor 10 months, 2 weeks ago

Selected Answer: A

The question is written in a confusing manner. They ask what is the cause, not the PROBABLE cause. We can't know for sure through the exhibit that B is really the cause. Therefore, answer is A.

upvoted 3 times

splashy 1 year ago

Selected Answer: A

166/255 reliability is going down = errors increasing

txload & rxload 1/255 which means low sent/transfer and received traffic = so definitely not high usage

upvoted 3 times

ptfish 1 year, 1 month ago

I think B is a trap answer. Not sure if this is the reason, maybe the quality of the SFP connector or something else.
But in the show interface command we can clearly see that there are some issues with reliability counter (reliability 166/255).

upvoted 1 times

sasquatchshrimp 1 year, 1 month ago

Selected Answer: B

The question is asking the cause, and the cause can very well be high volume, the other options are either potential facts or not related. I am going with B.

upvoted 1 times

iGlitch 1 year, 3 months ago

Selected Answer: A

A, 166/255

upvoted 2 times

LordScorpius 1 year, 4 months ago

Selected Answer: B

Again, not what is the problem but, what is the cause: B.

upvoted 1 times

LordScorpius 1 year, 4 months ago

However, I really, really wanna say "Force-up" on an incompatible SFP. In the field, THAT would be the cause but, we can't know it here.

upvoted 1 times

jahinchains 1 year, 4 months ago

Selected Answer: B

reliability does show us that there is a input output discrepancy due to high volume of frames

reliability 255/255: When the input and output errors increase, they affect the reliability counter. This indicates how likely it is that a packet can be delivered or received succesfully. Reliability is calculated like this: reliability = number of packets / number of total frames. The value of 255 is the highest value meaning that the interface is very reliable at the moment. The calculation above is done every 5 minutes.

https://networklessons.com/cisco/ccnp-tshoot/cisco-ios-show-interface-explained

upvoted 1 times

ZUMY 1 year, 4 months ago

A is correct
Reliability 255/255 = no input/out put errors in the interface
Reliability 166/255 = yes. some problem with input/output in the interface

upvoted 4 times

jahinchains 1 year, 4 months ago

and the question is what causes it? B!

upvoted 3 times

Vinarino 1 year, 8 months ago

"Shortly after Site-A was connected to Site-B..." What happened and why?
WHY a failure occurs is sought (and the answer) = 1000 users click on the new link (to SiteB to play with the app there) simultaneously = NO BANDWIDTH / utilization / the pipe is clogged.

upvoted 1 times

Question #76 *Topic 1*

A network engineer must configure the router R1 GigabitEthernet1/1 interface to connect to the router R2 GigabitEthernet1/1 interface. For the configuration to be applied, the engineer must compress the address 2001:0db8:0000:0000:0500:000a:400F:583B. Which command must be issued on the interface?

A. ipv6 address 2001::db8:0000::500:a:400F:583B

B. ipv6 address 2001:db8:0::500:a:4F:583B

C. ipv6 address 2001:db8::500:a:400F:583B

D. ipv6 address 2001:0db8::5:a:4F:583B

Correct Answer: *C*

Community vote distribution

C (100%)

SScott Highly Voted 2 years ago

C is the right compressed address.
https://iplocation.io/ipv6-compress

upvoted 5 times

Jorro99404 Most Recent 3 months, 2 weeks ago

Selected Answer: C

The correct one

upvoted 2 times

cormorant 10 months, 2 weeks ago

at last a question with a correct answer that makes sense

upvoted 4 times

keokkeo_123 10 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 3 times

ZUMY 1 year, 4 months ago

C is correct!

upvoted 2 times

onikafei 1 year, 7 months ago

Dumbed it down to c or a, a however was incorrect. 0000 should have been shortened

upvoted 1 times

priya17 1 year, 10 months ago

C correct answer

upvoted 1 times

Sonieta 1 year, 11 months ago

Yes, C is the better way to compress

upvoted 1 times

NZIAKOU 2 years ago

Good "C"

upvoted 2 times

Question #77 *Topic 1*

What is a network appliance that checks the state of a packet to determine whether the packet is legitimate?

A. Layer 2 switch

B. LAN controller

C. load balancer

D. firewall

Correct Answer: *D*

Community vote distribution

D (100%)

hp2wx Highly Voted 1 year, 1 month ago

Answer is D as a firewall is used for stateful packet inspection.

upvoted 5 times

dearc Most Recent 5 months, 2 weeks ago

Selected Answer: D

D is correct!

upvoted 2 times

ZUMY 1 year, 4 months ago

D is correct!

upvoted 3 times

AlexMD 1 year, 10 months ago

D is correct answer

upvoted 3 times

ABIboyscorner 1 year, 11 months ago

I believe that this is where security comes into play.

upvoted 4 times

Question #78 *Topic 1*

What is a role of access points in an enterprise network?

A. integrate with SNMP in preventing DDoS attacks

B. serve as a first line of defense in an enterprise network

C. connect wireless devices to a wired network

D. support secure user logins to devices on the network

Correct Answer: *C*

YoniEth Highly Voted 2 years, 2 months ago

C is correct.

upvoted 10 times

Petermwathe Most Recent 7 months, 3 weeks ago

C is correct

upvoted 1 times

ZUMY 1 year, 4 months ago

C is correct!

upvoted 3 times

Nebulise 1 year, 9 months ago

Easiest question in the exam

upvoted 3 times

Question #79 *Topic 1*

An implementer is preparing hardware for virtualization to create virtual machines on a host. What is needed to provide communication between hardware and virtual machines?

A. router

B. hypervisor

C. switch

D. straight cable

Correct Answer: *B*

Community vote distribution

B (100%)

ABIboyscorner Highly Voted 1 year, 11 months ago

A computer that hosts VMs requires specialized software called a hypervisor. The hypervisor emulates the computer's CPU, memory, hard disk, network and other hardware resources, creating a pool of resources that can be allocated to the individual VMs according to their specific requirements. The hypervisor can support multiple virtual hardware platforms that are isolated from each other, enabling VMs to run Linux and Windows Server OSes on the same physical host.

upvoted 14 times

Hanagaki_Shinjiro Most Recent 1 week, 2 days ago

Selected Answer: B

B is 100% correct

upvoted 1 times

iMo7ed 7 months, 1 week ago

Selected Answer: B

It is B

upvoted 2 times

sasquatchshrimp 1 year, 1 month ago

read it as, "what give a virtual computer access to physical hardware?" Hypervisor.

upvoted 1 times

ZUMY 1 year, 4 months ago

B is correct

upvoted 2 times

Question #80 *Topic 1*

How does a Cisco Unified Wireless Network respond to Wi-Fi channel overlap?

A. It allows the administrator to assign the channels on a per-device or per-interface basis.

B. It segregates devices from different manufactures onto different channels.

C. It analyzes client load and background noise and dynamically assigns a channel.

D. It alternates automatically between 2.4 GHz and 5 GHz on adjacent access points.

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/dca.html

Community vote distribution
C (81%) D (19%)

SScott Highly Voted 2 years ago
Best answer is C relates more to Dynamic Channel Assignment DCA

https://packet6.com/configuring-cisco-rrm-dca-dynamic-channel-assignment/

Do not agree with D, which is more about Band Select and Band Direction but the feature does not alternate AP's automatically, this is wrong with the wording.

With the question specific to channel overlap, analyzing AP load with client associations, managing channel assignments per RF group

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper_chapter_0100.pdf

https://community.cisco.com/t5/wireless/how-to-deal-with-channel-overlapping-channel-interferences/td-p/2465741
upvoted 25 times

SScott 2 years ago
Alternating between 2.4 and 5 frequencies will not directly address channel overlap experience concerns.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_wireless_high_client_density_design_guide.html#:~:text=In%20general%2C%202.4,venue%20help%20desk.
upvoted 6 times

hker 2 years ago
I agree with you SScott.
upvoted 5 times

Da_Costa Most Recent 3 weeks, 5 days ago
Selected Answer: C
dynamic channel assignment, manual channel assignment by the administrator, alternating channels, and device segregation.
upvoted 1 times

Ciscoman021 5 months, 3 weeks ago
Selected Answer: C
The Cisco Unified Wireless Network is designed to dynamically manage and optimize wireless coverage and performance by constantly monitoring and adjusting to changing conditions. In the case of Wi-Fi channel overlap, the network will analyze client load and background noise and dynamically assign channels to minimize interference and optimize throughput. This ensures that the network can provide reliable and high-performance Wi-Fi connectivity to all clients, even in challenging environments with high levels of interference.
upvoted 4 times

oatmealturkey 7 months ago
Selected Answer: C
These questions are often worded in a very deliberate way. Because this asks how the Cisco Unified Wireless Network RESPONDS to channel overlap, I go with C over D. The way Band Select works is to cause 5ghz-capable clients to join the 5ghz band, but it does this all the time when Band Select is enabled, not as a response to any conditions. DCA is a response to channel overlap.
upvoted 2 times

moise_amo 7 months, 2 weeks ago
Selected Answer: C
the question is for channel overlapps principaly, not for band select
upvoted 1 times

Anas_Ahmad 7 months, 4 weeks ago

Selected Answer: C

A Cisco Unified Wireless network does not alternate automatically between 2.4 GHz and 5 GHz on adjacent access points. The network instead analyzes the client load and background noise on different channels and dynamically assigns a channel that will provide the best performance for the wireless network. It does not make use of switching between 2.4 and 5GHz as this is not how it's designed to handle channel overlap. This helps to ensure that there is minimal channel overlap and that the wireless network is operating at optimal performance. that is why D is not correct

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: C

Ref: Enterprise Mobility 8.1 Design Guide – Cisco

"C H A P T E R 3
WLAN RF Design Considerations
…
Radio Resource Management – RRM
…
What RRM Does

RRM consists of four algorithms:

1. RF Grouping
2. DCA (Dynamic Channel Assignment)
…
DCA – Dynamic Channel Assignment

Dynamic Channel Assignment is responsible for monitoring the spectrum, and choosing the best channel plan to place the AP's on. Interference is the primary concern, the less interference there is the more bandwidth (airtime) we can use. To do this DCA monitors four parameters

• Signal—any Wi-Fi signal created by my network/RF Group
• Noise—any RF signal that is not identified as Wi-Fi; this includes collisions and packets to low to be demodulated as well.
• Interference—any Wi-Fi signal that is from Rogue devices or devices not part of my RF Group
• Load—The relative channel utilization of AP's in the RF Group
…"

upvoted 2 times

Yunus_Empire 9 months, 3 weeks ago

C is the Best

upvoted 1 times

mzu_sk8 10 months ago

D on another site without explanation

upvoted 1 times

splashy 1 year ago

Selected Answer: C

I think it's C... Can be found in provided link: DCA Algorithm
Same Channel Contention—other AP's/clients on the same channel - also known as Co-Channel interference or CCI
Foreign Channel - Rogue—Other non RF Group AP's operating on or overlapping with the AP's served channel
Noise—Non-Wi-Fi sources of interference such as Bluetooth, analog video, or cordless phones - see CleanAir for useful information on using CleanAir to detect noise sources
Channel Load—through the use of industry standard QBSS measurements - these metrics are gathered from the Phy layer - very similar to CAC load measurements.
DCA Sensitivity—A sensitivity threshold selectable by the user that applies hysteresis to the evaluation on channel changes

Answer D doesn't fix problem 2 and 3 resulting in overlap.

upvoted 1 times

GohanF2 1 year, 1 month ago

It Must be option C due that for accomplish option D the feature of "band select " needs to be enabled and that it's not enabled by default

upvoted 1 times

vuhidus 1 year, 1 month ago

Selected Answer: D

I think it's D

upvoted 1 times

saeed_huhu 1 year, 1 month ago

Selected Answer: C

C - Dynamic Channel Assignment DCA

upvoted 1 times

SH_ 1 year, 2 months ago

Selected Answer: C

Best choice is C. Dynamic Channel Assignment (DCA)
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/dca.html

upvoted 1 times

LordScorpius 1 year, 4 months ago

Selected Answer: C

Dynamic Channel Assignment DCA. Cisco is a for-profit company. Teaching us about all their features is part of our "Certification".

upvoted 2 times

jahinchains 1 year, 4 months ago

Selected Answer: D

the paramater on C are client load and background noise? how does it conncern in channel overlap? D is good...

upvoted 1 times

D0nkey_h0t 1 year, 3 months ago

when channels overlap the noise level is high

upvoted 1 times

ZUMY 1 year, 4 months ago

Going with Answer C:
Ref: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/dca.html

upvoted 2 times

Question #81 *Topic 1*

In which situation is private IPv4 addressing appropriate for a new subnet on the network of an organization?

A. The network has multiple endpoint listeners, and it is desired to limit the number of broadcasts.

B. The ISP requires the new subnet to be advertised to the Internet for web services.

C. There is limited unique address space, and traffic on the new subnet will stay local within the organization.

D. Traffic on the subnet must traverse a site-to-site VPN to an outside organization.

Correct Answer: *C*

Community vote distribution

C (83%) Other

Marcos9410 Highly Voted 1 year, 2 months ago

Selected Answer: C

C is correct

upvoted 5 times

ZUMY Most Recent 1 year, 4 months ago

Going with C:

upvoted 3 times

Bigc0ck 1 year, 5 months ago

Isn't private IP addressing just the same as saying NAT?

upvoted 2 times

DoBronx 10 months, 3 weeks ago

ur name tho]

upvoted 5 times

awashenko 1 year, 6 months ago

Selected Answer: C

Best answers is C

upvoted 2 times

ian77ex 1 year, 7 months ago

Selected Answer: C

C is correct.
A is also good, but when you have two possible answers you should select the best one.

upvoted 3 times

hector255 1 year, 7 months ago

Selected Answer: C

Sorry, I checked that the correct one is C.

upvoted 2 times

hector255 1 year, 7 months ago

Selected Answer: D

Sorry, I checked that the correct one is C.

upvoted 1 times

hector255 1 year, 7 months ago

Selected Answer: A

Option A is the correct.

upvoted 1 times

kijken 1 year, 7 months ago

Selected Answer: C

C is almost the definition of the reason why we subnet and why we use private addresses with NAT

upvoted 2 times

babaKazoo 1 year, 7 months ago

A. Use separate VLAN to reduce broadcast traffic.
C. Use separate subnet to conserve address space.

So for this question C.
upvoted 4 times

chin_rao 1 year, 7 months ago

Selected Answer: C

Private IP address are used to conserve IP addresses
upvoted 1 times

gvofke 1 year, 9 months ago

Selected Answer: A

Subnetting is used to limit the broadcast domain, i think the right answer is A
upvoted 1 times

eddy_bigirwa 1 year, 9 months ago

i thin c is the correct answer since private ip are used only on local network and cant be used over the internet(WAN0
upvoted 2 times

marked 1 year, 10 months ago

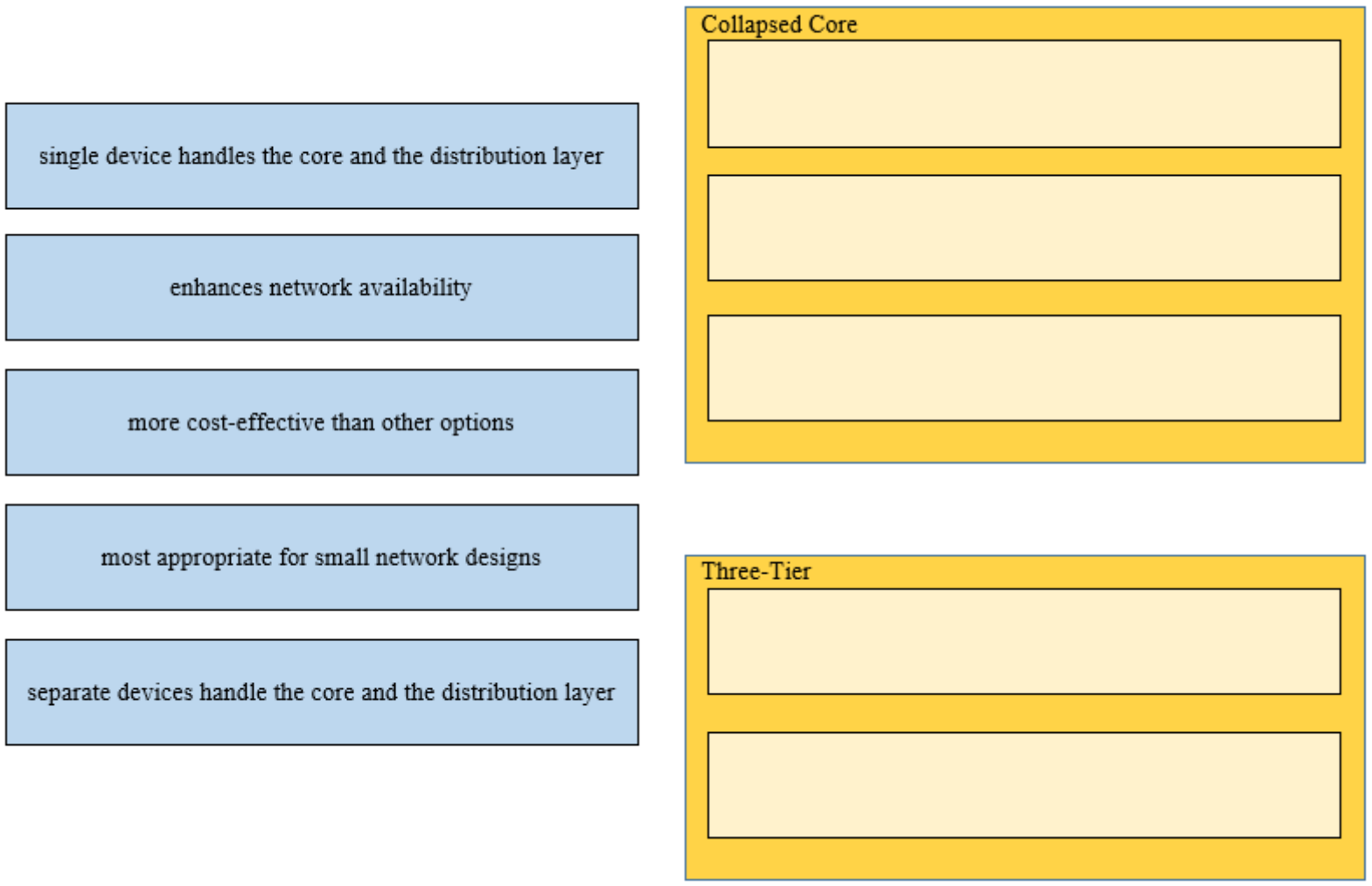
As far I know subnet is done to save and utilise address space in the network. So I opt C
upvoted 1 times

Question #82 *Topic 1*

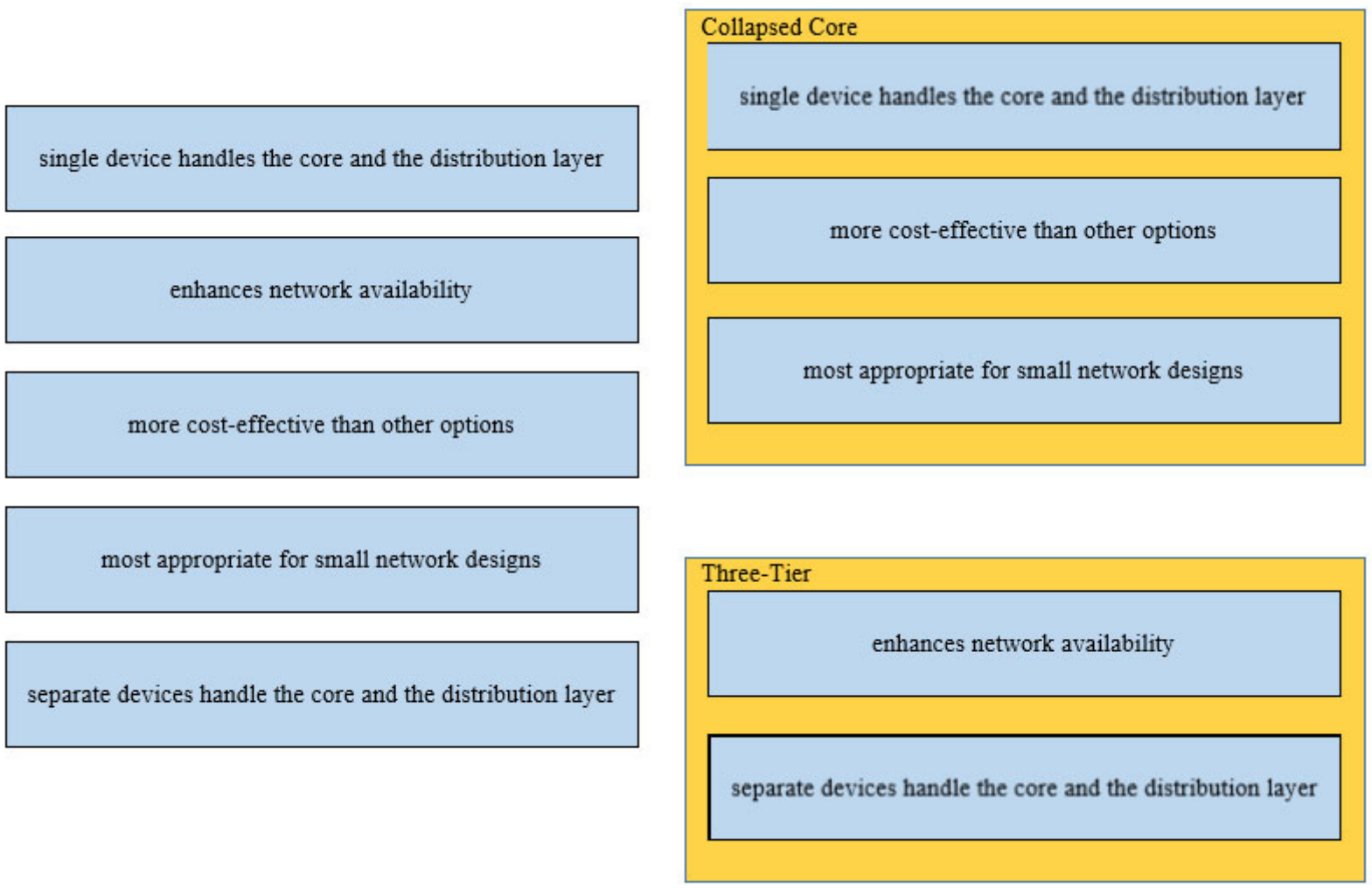
DRAG DROP -

Drag and drop the characteristics of network architectures from the left onto the type of architecture on the right.

Select and Place:



Correct Answer:



Yunus_Empire Highly Voted 9 months, 2 weeks ago

Given Answers Are Correct....

upvoted 7 times

Junior_Network Most Recent 20 hours, 8 minutes ago

more cost effective than other option -> This is not totally true because of wiring cost

upvoted 1 times

ELHAZ 5 months, 4 weeks ago

Collapsed core :
Single device handles the core and the distribution layer
more cost-effective than other opton
most appropriate for small network designs

Tree-Thier:

enhances network availability
separate devices handles the core and the distribution layer

upvoted 1 times

harkindeylee 6 months, 2 weeks ago

Correct

upvoted 2 times

Question #83 *Topic 1*

Which 802.11 frame type is indicated by a probe response after a client sends a probe request?

A. data

B. management

C. control

D. action

Correct Answer: *B*

Community vote distribution

B (100%)

ZUMY Highly Voted 1 year, 4 months ago

B is correct

Management frames: Used for joining and leaving a wireless cell. Management frame types include association request, association response, and reassociation request, just to name a few. (See Table 7-2 for a complete list.)
Control frames: Used to acknowledge when data frames are received.
Data frames: Frames that contain data.

upvoted 22 times

TA77 1 year, 3 months ago

Thank you

upvoted 2 times

VirtuaTech Most Recent 4 months, 1 week ago

repeated question

upvoted 1 times

harkindeylee 6 months, 2 weeks ago

B is correct

upvoted 1 times

GreatDane 8 months, 2 weeks ago

Selected Answer: B

Ref: 802.11 Association Process Explained - Cisco Meraki

"...
1. A mobile station sends probe requests to discover 802.11 networks within its proximity. Probe requests advertise the mobile stations supported data rates and 802.11 capabilities such as 802.11n. Because the probe request is sent from the mobile station to the destination layer-2 address and BSSID of ff:ff:ff:ff:ff:ff all AP's that receive it will respond.

2. APs receiving the probe request check to see if the mobile station has at least one common supported data rate. If they have compatible data rates, a probe response is sent advertising the SSID (wireless network name), supported data rates, encryption types if required, and other 802.11 capabilities of the AP.
..."

upvoted 3 times

TinKode 10 months ago

Selected Answer: B

Duplicate with question nr. 7
A guy posted this link
https://www.youtube.com/watch?v=PCpnRqKCWCQ

upvoted 4 times

Marcos9410 1 year, 2 months ago

Selected Answer: B

B is correct

upvoted 2 times

[Removed] 1 year, 7 months ago

https://www.ciscopress.com/articles/article.asp?p=1271797&seqNum=2

upvoted 3 times

Question #84 *Topic 1*

What is the difference in data transmission delivery and reliability between TCP and UDP?

A. TCP transmits data at a higher rate and ensures packet delivery. UDP retransmits lost data to ensure applications receive the data on the remote end.

B. TCP requires the connection to be established before transmitting data. UDP transmits data at a higher rate without ensuring packet delivery.

C. UDP sets up a connection between both devices before transmitting data. TCP uses the three-way handshake to transmit data with a reliable connection.

D. UDP is used for multicast and broadcast communication. TCP is used for unicast communication and transmits data at a higher rate with error checking.

Correct Answer: *B*
UDP speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party. As a result, UDP is beneficial in time- sensitive communications, including voice over IP (VoIP), domain name system (DNS) lookup, and video or audio playback.

Community vote distribution

B (100%)

ZUMY Highly Voted 1 year, 4 months ago
B is correct
upvoted 9 times

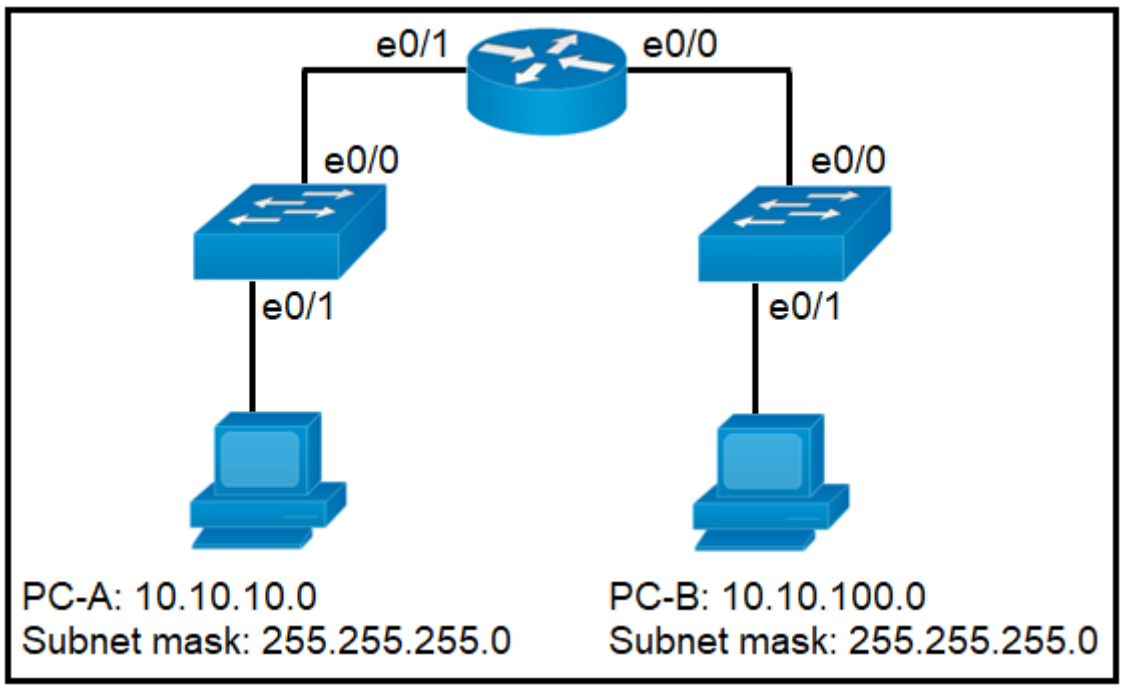
Smaritz Highly Voted 1 year, 6 months ago
B is correct
upvoted 6 times

Hanagaki_Shinjiro Most Recent 1 week, 2 days ago
Selected Answer: B
UDP speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party. As a result, UDP is beneficial in time- sensitive communications, including voice over IP (VoIP), domain name system (DNS) lookup, and video or audio playback.
upvoted 1 times

[Removed] 3 months, 1 week ago
Selected Answer: B
B is the correct answer.
upvoted 1 times

Yunus_Empire 9 months, 2 weeks ago
B is correct
upvoted 4 times

Question #85 *Topic 1*



Refer to the exhibit. When PC-A sends traffic to PC-B, which network component is in charge of receiving the packet from PC-A, verifying the IP addresses, and forwarding the packet to PC-B?

A. router

B. Layer 2 switch

C. load balancer

D. firewall

Correct Answer: *A*

Community vote distribution

A (100%)

SparkySM Highly Voted 1 year, 7 months ago

the key point is "verifying the IP addresses," it is done by router .since the sw do things with MAC

upvoted 11 times

harkindeylee Most Recent 6 months, 2 weeks ago

Packet is recieved by the router. A is perfect

upvoted 2 times

country_rooted 1 year, 4 months ago

From the time the question asks to verify you already know the answer is A.

upvoted 2 times

ZUMY 1 year, 4 months ago

A is correct!

upvoted 3 times

rictorres333 1 year, 4 months ago

Selected Answer: A

The key word is "packet".

upvoted 3 times

Belinda 1 year, 7 months ago

A IS CORRECT. PC--A and PC-B are not in the same network. Switches send traffic in layer 2 and within the same VLA while routers route traffic to different subnet and at layer 3.

upvoted 3 times

Question #86 *Topic 1*

What is the maximum bandwidth of a T1 point-to-point connection?

A. 1.544 Mbps

B. 2.048 Mbps

C. 34.368 Mbps

D. 43.7 Mbps

Correct Answer: *A*

Community vote distribution

A (100%)

Chupacabro Highly Voted 1 year, 8 months ago

A. T1
B. E1
C. E3
D. T3
https://www.ciscopress.com/articles/article.asp?p=2202411&seqNum=7

upvoted 11 times

Vlad_Is_Love_ua Most Recent 1 year ago

Selected Answer: A

What Does Point-to-Point T1 Mean? Point-to-point T1 is a direct and/or a private T1 network connection between two or more networks or locations. It is a secure, private and unshared network connection that provides a T1 network at a speed of 1.544 mbps between multiple networks/locations.

upvoted 2 times

shauntilyard 1 year, 3 months ago

Why is this even tested if it is specific to the US?

upvoted 4 times

sasquatchshrimp 1 year, 1 month ago

They got to make their money somehow, and real questions would allow all network admins to get the ccna with no study.

upvoted 7 times

Hanagaki_Shinjiro 1 week, 2 days ago

that's true

upvoted 1 times

Smaritz 1 year, 6 months ago

Correct answer is A. This is old technology, also discussed in the Networking Essentials module in MCSE that I did in 1999

upvoted 4 times

hassanhhady 1 year, 8 months ago

what is T1 means ?

upvoted 2 times

Yasin_Alsabah 1 year, 7 months ago

a T1 link supports 1.544 Mbps, an E1 supports 2.048 Mbps, a T3 supports 43.7 Mbps, and an E3 connection supports 34.368 Mbps. Optical Carrier (OC) transmission rates are used to define the digital transmitting capacity of a fiber-optic network.

upvoted 7 times

Question #87 *Topic 1*

What are two similarities between UTP Cat 5e and Cat 6a cabling? (Choose two.)

A. Both support speeds up to 10 Gigabit.

B. Both support speeds of at least 1 Gigabit.

C. Both support runs of up to 55 meters.

D. Both support runs of up to 100 meters.

E. Both operate at a frequency of 500 MHz.

Correct Answer: *BD*

Community vote distribution

BD (100%)

Marcos9410 Highly Voted 1 year, 2 months ago

B and D are correct.

UTP Cables CAT 5e:
Frecuency: 100 MHz
Max. Bandwidth: 1 Gbps
Max. Distance: 100 m

UTP Cables CAT 6a:
Frecuency: 500 MHz
Max. Bandwidth: 10 Gbps
Max. Distance: 100 m

upvoted 13 times

Smaritz Highly Voted 1 year, 6 months ago

At least 1 Gbps is a bit misleading, they support at least 10 Mbps also.

upvoted 7 times

ricky1802 Most Recent 7 months, 2 weeks ago

Selected Answer: BD

Here are the common specifications for some popular UTP categories:

Cat5:

Frequency: Up to 100 MHz
Bandwidth: 100 Mbps (Fast Ethernet)
Max Distance: 100 meters (328 feet)
Cat5e:

Frequency: Up to 100 MHz
Bandwidth: 1 Gbps (Gigabit Ethernet)
Max Distance: 100 meters (328 feet)
Cat6:

Frequency: Up to 250 MHz
Bandwidth: 10 Gbps (10 Gigabit Ethernet)
Max Distance: 55 meters (180 feet) for 10 Gbps, 100 meters (328 feet) for 1 Gbps
Cat6a:

Frequency: Up to 500 MHz
Bandwidth: 10 Gbps (10 Gigabit Ethernet)
Max Distance: 100 meters (328 feet)
Cat7:

Frequency: Up to 600 MHz
Bandwidth: 10 Gbps (10 Gigabit Ethernet)
Max Distance: 100 meters (328 feet)
Cat8:

Frequency: Up to 2 GHz
Bandwidth: 25/40 Gbps (25/40 Gigabit Ethernet)
Max Distance: 30 meters (98 feet)

upvoted 5 times

RougePotatoe 10 months, 4 weeks ago

Ahh another bad question. Cat5e can support 10gig at shorter distances so both could support 10gig. Both could support 100 meter runs. So Technically A,B, and D are correct.

upvoted 2 times

iGlitch 1 year, 4 months ago

B should be: Both support a maximum speed of 1 Gigabit.

upvoted 3 times

Bonesaw 11 months, 4 weeks ago

The maximum speed on Cat6a is 10G, so that would be incorrect

upvoted 1 times

ZUMY 1 year, 4 months ago

B & D are fine.

upvoted 1 times

Question #88 *Topic 1*

What is a characteristic of cloud-based network topology?

A. onsite network services are provided with physical Layer 2 and Layer 3 components

B. wireless connections provide the sole access method to services

C. physical workstations are configured to share resources

D. services are provided by a public, private, or hybrid deployment

Correct Answer: *D*

Community vote distribution

D (100%)

Vlad_Is_Love_ua 10 months ago

D is correct

upvoted 2 times

ZUMY 1 year, 4 months ago

D is fine

upvoted 3 times

AvroMax 1 year, 7 months ago

Selected Answer: D

D correct

upvoted 3 times

onikafei 1 year, 7 months ago

D would be correct

Definitly not A as its physical when we are talking about cloud services
B talks about access to a service but doesn't talk about topologies.
C feels like its refering to shared resources on a network between workstations and not on cloud.

upvoted 3 times

onikafei 1 year, 7 months ago

Correctme if im wrong :)

upvoted 2 times

Question #89 *Topic 1*

Which network action occurs within the data plane?

A. reply to an incoming ICMP echo request

B. make a configuration change from an incoming NETCONF RPC

C. run routing protocols (OSPF, EIGRP, RIP, BGP)

D. compare the destination IP address to the IP routing table

Correct Answer: *D*

Community vote distribution

Dante_Dan Highly Voted 1 year, 7 months ago

Selected Answer: D

Extracted from Book #2, page 359:

"... the following list details some of the more common actions that a networking device does that fit into the data plane:
- De-encapsulating and re-encapsulating a packet in a data-link frame (routers, layer 3 switches).
- Adding or removing an 802.1Q trunking header (routers and switches).
- Matching an ethernet frame's destination MAC address to the MAC address table (layer 2 switches).
- Matching an IP packet's destination IP address to the IP routing table (routers, layer 3 switches).
- Encrypting the data and adding a new IP header (for VPN processing).
- Changing the source or destination IP address (for NAT) processing).
- Discarding a message due to a filter (ACLs, port security).

All the items in the list make up the data plane, because the data plane includes all actions done per message."

upvoted 18 times

sgashashf 1 year, 6 months ago

This blows my mind, considering I've read from multiple different sources that "the Control plane refers to all functions and processes that determine which path to use to send the packet or frame." I now have no idea how to differentiate between these two planes.

upvoted 9 times

jose01210 1 year, 4 months ago

igual me pasa a mi

upvoted 1 times

MDK94 Highly Voted 1 year, 2 months ago

ICMP = internet CONTROL message protocol

"The role of ICMP is to provide information about the path the data is taking from its point of origin to its destination. It has the same basic structure as an IP packet, but despite that, it's not really goodput. It's there to control 'how things are done', therefore, is part of the control plane."

Source: https://blog.apnic.net/2021/06/21/what-are-ping-and-traceroute-really/#:~:text=The%20role%20of%20ICMP%20is,part%20of%20the%20control%20plane.

upvoted 12 times

michael1001 9 months, 1 week ago

Underrated

upvoted 1 times

Hangulmal Most Recent 1 month ago

The data plane is accountable for the actual transmission of data packets across a network. It entails determining, based on a packet's destination address, the appropriate outgoing interface for it. This procedure typically involves looking up the destination IP address in the routing table to ascertain the next network hop for the packet. The comparison of the destination IP address with the IP routing table is a crucial data plane operation.

Answer: D

upvoted 1 times

davidmdlp85 2 months ago

The Idea is that the question is not referring to the layer two in the OSI model, is just about the networks planes Data, Control, and Management Planes. For that case, yes, Matching an IP packet's destination IP address to the IP routing table occurs in Data Plane.

upvoted 1 times

iMo7ed 7 months, 1 week ago

Selected Answer: D

It's D

upvoted 2 times

splashy 8 months ago

Selected Answer: D

https://ipwithease.com/cisco-express-forwarding-cef/

I think it's a CEF question: FIB and adjacency tables are in data plane, once these are "established" the data won't pass through the cpu any more.

upvoted 5 times

LordScorpius 1 year, 4 months ago

Selected Answer: D

If you can subnet from /20 to /30 and you know the contrast between TCP and UDP, and you learn the data types for the three planes...you WILL pass the CCNA.

upvoted 4 times

xbololi 2 months, 2 weeks ago

DHCP, ipv6, DTP, VTP, ACL, Static Routing: Am i a joke to you? xD

upvoted 1 times

ZUMY 1 year, 4 months ago

Going with D

Think of the control plane as being like the stoplights that operate at the intersections of a city. Meanwhile, the data plane (or the forwarding plane) is more like the cars that drive on the roads, stop at the intersections, and obey the stoplights.

upvoted 3 times

pagamar 1 year, 5 months ago

Tumbative: I saw this question in a recent Exam, and the RIGHT answer is D, 100% correct in Topic 6 of the Exam.

upvoted 2 times

Bigc0ck 1 year, 5 months ago

Another wonderful example of bad test writing.... I thought Data plane was about forwarding packets between layer 2 > 3

upvoted 1 times

Knobbler 1 year, 6 months ago

Selected Answer: A

I'm going with A :)

upvoted 1 times

debut01 1 year, 7 months ago

je pense que c'est la B

upvoted 1 times

Nicocisco 1 year, 7 months ago

Selected Answer: A

C'est la A car la dataplane forward le trafic

upvoted 1 times

reagan_donald 1 year, 7 months ago

The role of ICMP is to provide information about the path the data is taking from its point of origin to its destination. It has the same basic structure as an IP packet, but despite that, it's not really goodput. It's there to control 'how things are done', therefore, is part of the control plane.

Correct answer is D

upvoted 1 times

daanderud 1 year, 7 months ago

Selected Answer: D

Agree. RESPONDING to ICMP is in the data pane

upvoted 1 times

daanderud 1 year, 7 months ago

I meant A!

upvoted 1 times

AndersonMr 1 year, 8 months ago

Selected Answer: D

icmp is control plane

upvoted 1 times

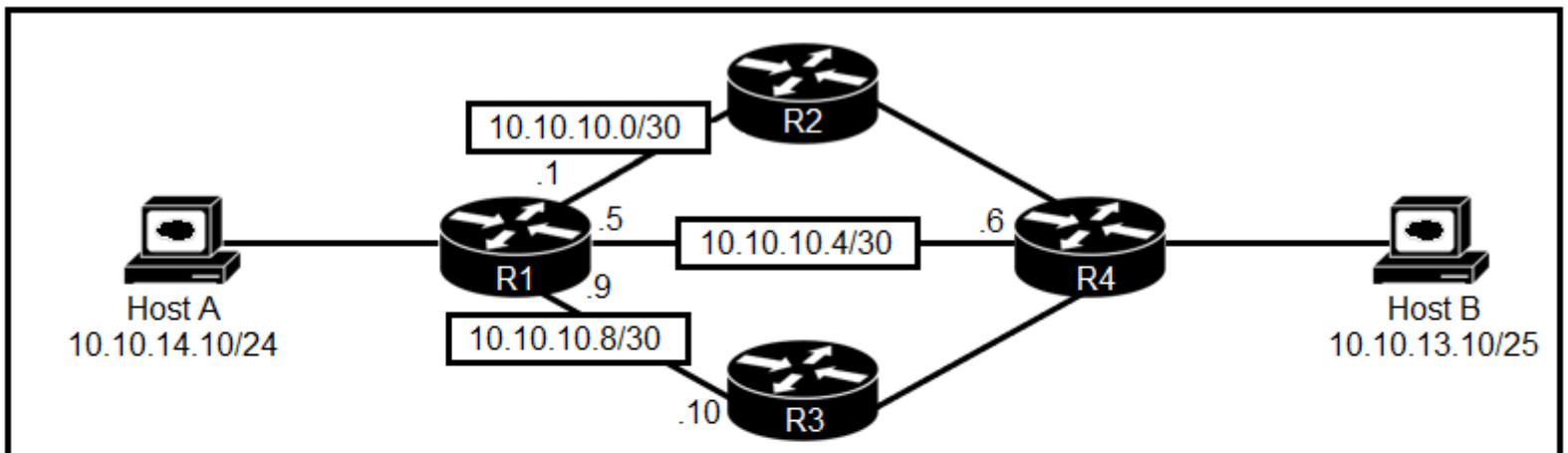
Kane002 1 year, 8 months ago

Selected Answer: A

Actual management of data is data plane, hence responding to an ICMP message is within the data plane, whereas routing decisions are made by the control plane, hence A not D.

upvoted 3 times

Question #90 *Topic 1*




```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
R1(config)#ip route 10.10.13.0 255.255.255.128 10.10.10.2 111
R1(config)#ip route 10.10.13.0 255.255.255.128 10.10.10.6 112
R1(config)#ip route 10.10.13.0 255.255.255.128 10.10.10.10 108
R1(config-router)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 10.10.10.5 0.0.0.0 area 0
R1(config-router)#network 10.10.10.1 0.0.0.0 area 0
R1(config-router)#network 10.10.14.1 0.0.0.0 area 0
```

Refer to the exhibit. R1 has just received a packet from host A that is destined to host B. Which route in the routing table is used by R1 to reach host B?

A. 10.10.13.0/25 [1/0] via 10.10.10.2

B. 10.10.13.0/25 [108/0] via 10.10.10.10

C. 10.10.13.0/25 [110/2] via 10.10.10.6

D. 10.10.13.0/25 [110/2] via 10.10.10.2

Correct Answer: *B*

Community vote distribution

B (83%) A (17%)

Jbcrggddfhh Highly Voted 1 year, 4 months ago

B is correct; it uses the lowest AD out of all the routes presented that go to the 10.10.13.0/25 subnet. A is a default route and would only be used if there wasn't a route to that subnet in the routing table.

upvoted 17 times

Cynthia2023 Most Recent 1 month ago

Selected Answer: A

Since the network 10.10.10.8/30 is not advertised in the OSPF configuration and there is no specific route to 10.10.10.10 in the routing table, R1 wouldn't have a direct route to reach 10.10.10.10. In this scenario, R1 would typically follow the default behavior of selecting the best match in its routing table. The best match among the routes listed would be the default route

upvoted 1 times

bikila123 1 month, 1 week ago

different routing protocol to the same destination will be selected by AD so the answer is B

upvoted 1 times

properchad 4 months ago

Longest prefix match is preferred over any AD value.
Here, although the default route uses AD of 1 ,it isn't the proper match for the destination.
Destination address is 10.10.13.10 and the longest prefix match for that is 10.10.13.0/25.
There are currently 3 routes configured for that destination each with different AD value and also OSPF is running.
Now when you first have the longest prefix match then only you check the AD value. So that would make the route with AD of 108 the perfect path for the destination.
Router make decision based on the following checklist in order.
1. Longest prefix match
2. AD
3. Metric
This is just a high level overview but for the CCNA I think this will suffice.

upvoted 2 times

Nutanix_Dummy 6 months, 3 weeks ago

Selected Answer: B

Route Source Default Distance Values
Connected interface 0
Static route 1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route 5
External Border Gateway Protocol (BGP) 20
Internal EIGRP 90
IGRP 100
OSPF 110
Intermediate System-to-Intermediate System (IS-IS) 115
Routing Information Protocol (RIP) 120
Exterior Gateway Protocol (EGP) 140
On Demand Routing (ODR) 160
External EIGRP 170
Internal BGP 200
Unknown* 255

upvoted 1 times

freeknowledge123 8 months, 1 week ago

what a question, first you might think it's the route with the lowest AD value, then when you see the conf you realise it's a default route and only used when there is no matching route

upvoted 3 times

AbiZ17 8 months, 2 weeks ago

Choice B coz it has lowest AD and it is the most specific one

upvoted 1 times

BlkWatches 9 months, 2 weeks ago

Very tricky haha

upvoted 2 times

RougePotatoe 10 months, 4 weeks ago

Selected Answer: B

OSFP routing, indicated by area 0 routing command, has AD of 110. There is a floating static route configured with 108 AD. As the configured static route's AD is lower (108) than the OSPF's default AD (110) it will route the traffic via 10.10.10.10 because it has the lowest AD and thus will be put into the routing table.

upvoted 3 times

ptfish 1 year, 1 month ago

Selected Answer: B

Because all routes point to the same subnet (10.10.13.0/25). So the route with the smallest AD value will be added to the routing table.
AD: OSPF (110), 10.10.10.10 (108), 10.10.10.6 (110), 10.10.10.2 (110)

upvoted 1 times

hp2wx 1 year, 1 month ago

Know your default routing protocol ADs!

upvoted 1 times

ZUMY 1 year, 3 months ago

B is correct!
Router prefers static route over dynamic route
Router prefers Lowest AD

upvoted 1 times

timskis2 1 year, 3 months ago

IT WILL USE THE DEFAULT / STATIC ROUTE 10.10.10.2 IT'S THE ONLY ONE ON THE DIAGRAM

upvoted 4 times

TA77 1 year, 3 months ago

The default route will only be used If there's no entry in the routing table for a specific subnet. Hence, in this question 10.10.10.2 will not be used.

upvoted 2 times

mytime 1 year, 4 months ago

this just throws me off because i look at the routing diagram and I don't see most of the multiple choice answers in the diagram. I guess i just have to go with the ad / metric in the answer bank.

upvoted 2 times

Question #91 *Topic 1*

Which two network actions occur within the data plane? (Choose two.)

A. Run routing protocols.

B. Make a configuration change from an incoming NETCONF RPC.

C. Add or remove an 802.1Q trunking header.

D. Match the destination MAC address to the MAC address table.

E. Reply to an incoming ICMP echo request.

Correct Answer: *CD*

Community vote distribution

CD (89%) 6%

mantest Highly Voted 1 year, 4 months ago

C&D are correct ans..

upvoted 11 times

Anas_Ahmad Highly Voted 9 months, 2 weeks ago

– De-encapsulating and re-encapsulating a packet in a data-link frame (routers, Layer 3 switches)
– Adding or removing an 802.1Q trunking header (routers and switches)
– Matching an Ethernet frame's destination Media Access Control (MAC) address to the MAC address table (Layer 2 switches)
– Matching an IP packet's destination IP address to the IP routing table (routers, Layer 3 switches)
– Encrypting the data and adding a new IP header (for virtual private network [VPN] processing)
– Changing the source or destination IP address (for Network Address Translation [NAT] processing)
– Discarding a message due to a filter (access control lists [ACLs], port security

upvoted 8 times

Da_Costa Most Recent 3 weeks, 5 days ago

Selected Answer: DE

ABC are not associated with dataplane

upvoted 1 times

Da_Costa 1 month, 2 weeks ago

Selected Answer: CE

My opinion

upvoted 1 times

kyleptt 1 month, 2 weeks ago

Just adding some though into this topic ICMP won't be the forwarding of traffic ? I understand C & D are correct but E seems correct to me

upvoted 1 times

Isuzu 4 months, 3 weeks ago

Is E can also be Correct... Reply to an incoming ICMP echo request: occurs when a device receives an ICMP echo request (ping) and needs to send an ICMP echo reply back to the source IP address.

Correct me if am wrong

upvoted 2 times

WOP_TO 1 year, 1 month ago

Selected Answer: CD

https://www.ciscopress.com/articles/article.asp?p=2995354&seqNum=2
De-encapsulating and re-encapsulating a packet in a data-link frame (routers, Layer 3 switches)

Adding or removing an 802.1Q trunking header (routers and switches)

Matching an Ethernet frame's destination Media Access Control (MAC) address to the MAC address table (Layer 2 switches)

Matching an IP packet's destination IP address to the IP routing table (routers, Layer 3 switches)

Encrypting the data and adding a new IP header (for virtual private network [VPN] processing)

Changing the source or destination IP address (for Network Address Translation [NAT] processing)

Discarding a message due to a filter (access control lists [ACLs], port security)

All the items in the list make up the data plane, because the data plane includes all actions done per message.

upvoted 4 times

saeed_huhu 1 year, 1 month ago

Selected Answer: CD

C and D
Please currect it

upvoted 1 times

MDK94 1 year, 2 months ago

The correct answers are C and D 100% (there are 2 other questions that are part of this dump that are very similar to this question and the answers have never used ICMP as part of the control plane. Also remember that ICMP means internet CONTROL message protocol.

"The role of ICMP is to provide information about the path the data is taking from its point of origin to its destination.

It has the same basic structure as an IP packet, but despite that, it's not really goodput. It's there to control 'how things are done', therefore, is part of the control plane."

Reference: https://blog.apnic.net/2021/06/21/what-are-ping-and-traceroute-really/#:~:text=The%20role%20of%20ICMP%20is,part%20of%20the%20control%20plane.

upvoted 2 times

MDK94 1 year, 2 months ago

Apologies I meant that there are 2 other questions that are part of this dump that are very similar to this question and the answers have never used ICMP as part of the DATA plane)

upvoted 1 times

ZUMY 1 year, 3 months ago

Going with C & D

upvoted 2 times

jossyda 1 year, 3 months ago

Selected Answer: CD

Data Plane:
■ De-encapsulating and re-encapsulating a packet in a data-link frame (routers, Layer 3 switches)
■ Adding or removing an 802.1Q trunking header (routers and switches)
■ Matching an Ethernet frame's destination Media Access Control (MAC) address to the MAC address table (Layer 2 switches)
■ Matching an IP packet's destination IP address to the IP routing table (routers, Layer 3 switches)
■ Encrypting the data and adding a new IP header (for virtual private network [VPN] processing)
■ Changing the source or destination IP address (for Network Address Translation [NAT] processing)
■ Discarding a message due to a filter (access control lists [ACLs], port security)

upvoted 3 times

mytime 1 year, 4 months ago

ALL of the explanations that people have posted do not say anything about ICMP (weather it's replying or sending) so is that a correct answer or not? I understand the mac thing that is spelled out very well but, it does not say anything about ICMP specifically

upvoted 1 times

MikeNY85 1 year, 4 months ago

C&D are the answers. ICMP is part of control plane

upvoted 1 times

msomali 1 year, 4 months ago

Correct answers are CD

Here are the actions that occur at the Data Plane:-
– De-encapsulating and re-encapsulating a packet in a data-link frame (routers, Layer 3 switches)
– Adding or removing an 802.1Q Trunking header (routers and switches).
– Matching an Ethernet frame's destination Media Access Control (MAC) address to the MAC address table (Layer 2 switches).
– Matching an IP packet's destination IP address to the IP routing table (routers, Layer 3 switches).
– Encrypting the data and adding a new IP header (for virtual private network [VPN] processing).
– Changing the source or destination IP address (for Network Address Translation [NAT] processing).
– Discarding a message due to a filter (access control lists [ACLs], port security.

upvoted 3 times

iGlitch 1 year, 4 months ago

Selected Answer: CD

ICMP is part of the control plane, therefor E is wrong.

upvoted 1 times

Scvrfvce 1 year, 4 months ago

Selected Answer: CD

C&D should be the right answer

upvoted 3 times

gamergoddess123 1 year, 4 months ago

Selected Answer: CD

Extracted from Book #2, page 359:
"... the following list details some of the more common actions that a networking device does that fit into the data plane:
- De-encapsulating and re-encapsulating a packet in a data-link frame (routers, layer 3 switches).
- Adding or removing an 802.1Q trunking header (routers and switches).
- Matching an ethernet frame's destination MAC address to the MAC address table (layer 2 switches).
- Matching an IP packet's destination IP address to the IP routing table (routers, layer 3 switches).
- Encrypting the data and adding a new IP header (for VPN processing).
- Changing the source or destination IP address (for NAT) processing).
- Discarding a message due to a filter (ACLs, port security).

All the items in the list make up the data plane, because the data plane includes all actions done per message."

upvoted 4 times

Question #92 *Topic 1*

What are network endpoints?

A. support inter-VLAN connectivity

B. a threat to the network if they are compromised

C. act as routers to connect a user to the service provider network

D. enforce policies for campus-wide traffic going to the Internet

Correct Answer: *B*

Community vote distribution

B (100%)

Smaritz Highly Voted 1 year, 3 months ago

Strangely worded question and answer

upvoted 17 times

TA77 1 year, 3 months ago

Indeed

upvoted 1 times

everchosen13 Highly Voted 11 months, 2 weeks ago

I mean, essentially any portion of your network is a threat if it is compromised...

upvoted 13 times

kyleptt Most Recent 2 weeks, 1 day ago

This a silly question

upvoted 2 times

xbololi 2 months, 3 weeks ago

Definetely not a question for knowledge more like a verbal test.

upvoted 1 times

Wes_60 5 months, 3 weeks ago

The most useless question so far

upvoted 7 times

GreatDane 8 months, 2 weeks ago

Selected Answer: B

A. support inter-VLAN connectivity

A Layer 3 switch's job.
And an L3 switch is an intermediary device.
Wrong answer.

B. a threat to the network if they are compromised

Your PC is an end device. Another user retrieves your username and your password, and has unauthorized access to your computer.
What could happen to your network?
Correct answer.

C. act as routers to connect a user to the service provider network

A router is an intermediary device.
Wrong answer.

D. enforce policies for campus-wide traffic going to the Internet

A firewall's job.
And a firewall is an intermediary device.
Wrong answer.

upvoted 5 times

Marcos9410 1 year, 2 months ago

Selected Answer: B

The correct answer is B.

Here you can find the exactly explanation:

https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint

upvoted 2 times

ZUMY 1 year, 3 months ago

Going with B

upvoted 1 times

jose01210 1 year, 4 months ago

I think that is A

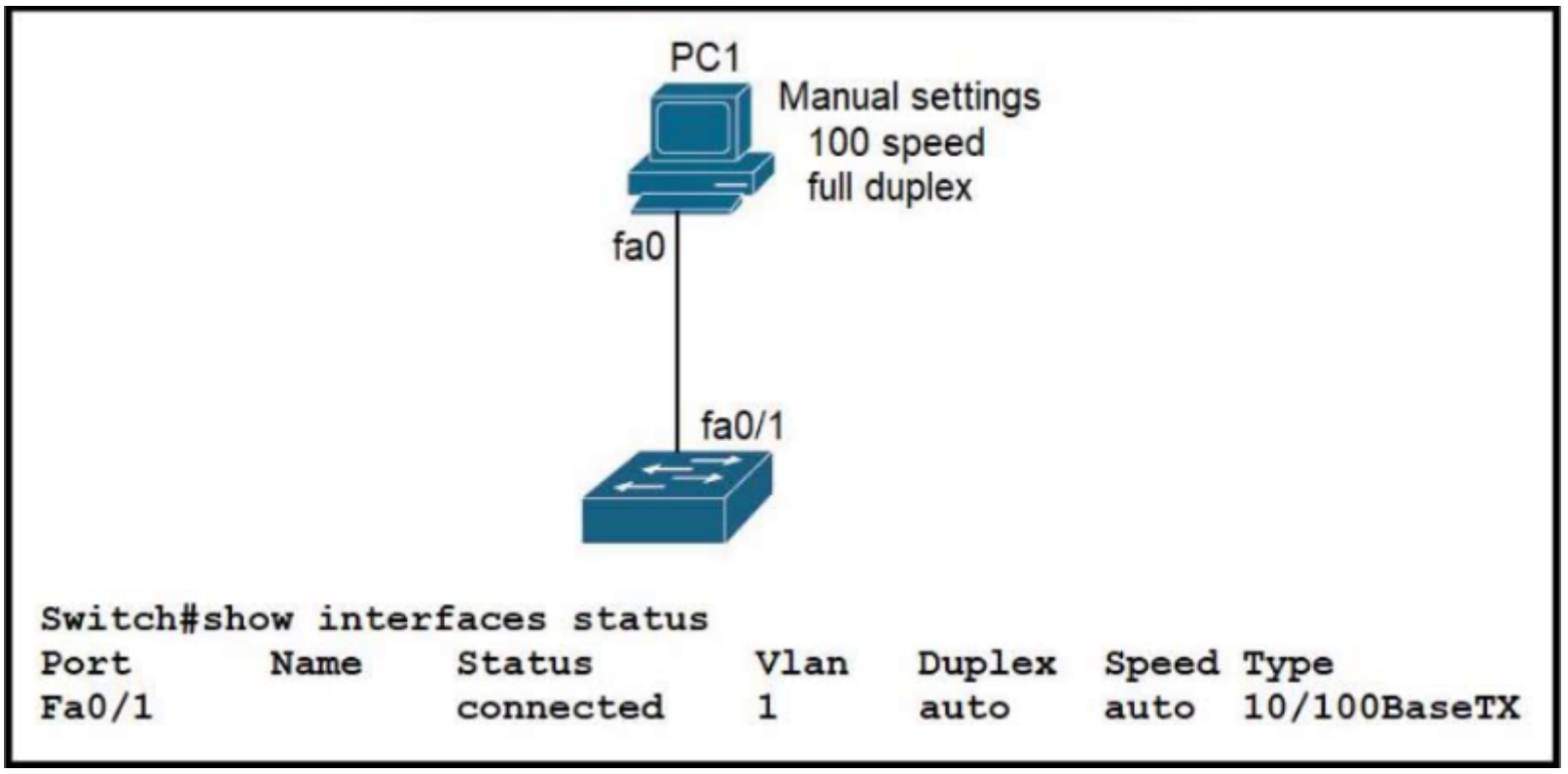
upvoted 2 times

CCAL 1 year, 4 months ago

aucun sens

upvoted 3 times

Question #93 *Topic 1*



Refer to the exhibit. The link between PC1 and the switch is up, but it is performing poorly. Which interface condition is causing the performance problem?

A. There is an issue with the fiber on the switch interface.

B. There is a duplex mismatch on the interface.

C. There is an interface type mismatch.

D. There is a speed mismatch on the interface.

Correct Answer: *B*

Community vote distribution

B (100%)

Jbcrggddfhh Highly Voted 1 year, 4 months ago

The answer is B.

The PC's port runs in full duplex, while the Fa0/1 port on the switch is in auto-negotiate mode.
This results in a duplex mismatch that causes the switchport to operate as half-duplex, which culminates in poor performance on the link.

"A duplex mismatch occurs when two connected devices are configured in different duplex modes.
This may happen, for example, if one is configured for autonegotiation while the other one has a fixed mode of operation that is full duplex (no autonegotiation). In such conditions, the autonegotiation device correctly detects the speed of operation, but is unable to correctly detect the duplex mode.
As a result, it sets the correct speed but assumes half-duplex mode.
When a device is operating in full duplex while the other one operates in half duplex, the connection works reliably only at a very low throughput."

Reference: https://en.wikipedia.org/wiki/Autonegotiation#Duplex_mismatch

upvoted 17 times

GreatDane Most Recent 8 months, 2 weeks ago

Selected Answer: B

Ref: Autonegotiation – Wikipedia

"...
Duplex mismatch

A duplex mismatch occurs when two connected devices are configured in different duplex modes. This may happen, for example, if one is configured for autonegotiation while the other one has a fixed mode of operation that is full duplex (no autonegotiation). In such conditions, the autonegotiation device correctly detects the speed of operation, but is unable to correctly detect the duplex mode. As a result, it sets the correct speed but assumes half-duplex mode.

When a device is operating in full duplex while the other one operates in half duplex, the connection works reliably only at a very low throughput.
..."

upvoted 4 times

hp2wx 1 year, 1 month ago

B is correct. Had there been a speed mis-match, the port would be in the down/down state and traffic would not be able to flow at all over the link.

upvoted 4 times

ZUMY 1 year, 3 months ago

B is correct!

upvoted 2 times

Question #94 *Topic 1*

Why was the RFC 1918 address space defined?

A. conserve public IPv4 addressing

B. support the NAT protocol

C. preserve public IPv6 address space

D. reduce instances of overlapping IP addresses

Correct Answer: *A*

Community vote distribution

A (100%)

MauroC19 1 month ago

Selected Answer: A

Answer is A. RFC 1918 was about private ipv4 addressing

upvoted 2 times

hp2wx 1 year, 1 month ago

A is correct. Private IPv4 addresses were developed to conserve IPv4 address space. NAT was developed as a way to use private addresses and allow for them to be able to communicate with other hosts outside of their LAN. C & D do not deal at all with private IP addresses

upvoted 4 times

ZUMY 1 year, 3 months ago

A is correct!

upvoted 2 times

erikkkkkka 1 year, 3 months ago

A is correct

An RFC1918 address is an IP address that is assigned by an enterprise organization to an internal host. These IP addresses are used in private networks, which are not available, or reachable, from the Internet.

upvoted 2 times

Jbcrggddfhh 1 year, 4 months ago

Answer is A.

"With the described scheme many large enterprises will need only a relatively small block of addresses from the globally unique IP address space."

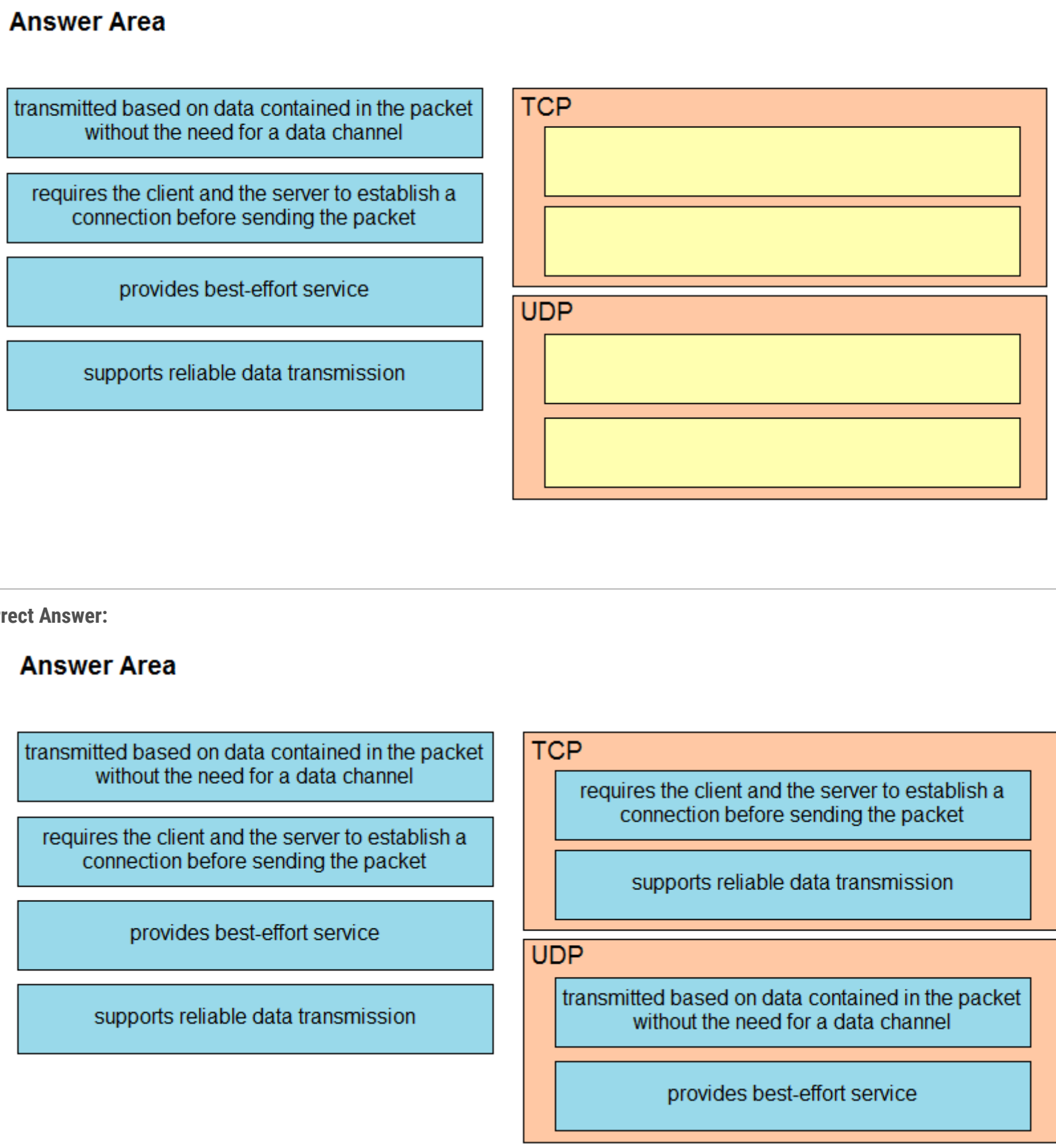
Reference: https://datatracker.ietf.org/doc/html/rfc1918

upvoted 4 times

DRAG DROP -

Drag and drop the TCP or UDP details from the left onto their corresponding protocols on the right.

Select and Place:



Correct Answer:

[Removed] 3 months, 1 week ago

The answer is correct

upvoted 1 times

yousfs1212 5 months, 4 weeks ago

The question is simple and the answer is correct

upvoted 2 times

NetStef 9 months ago

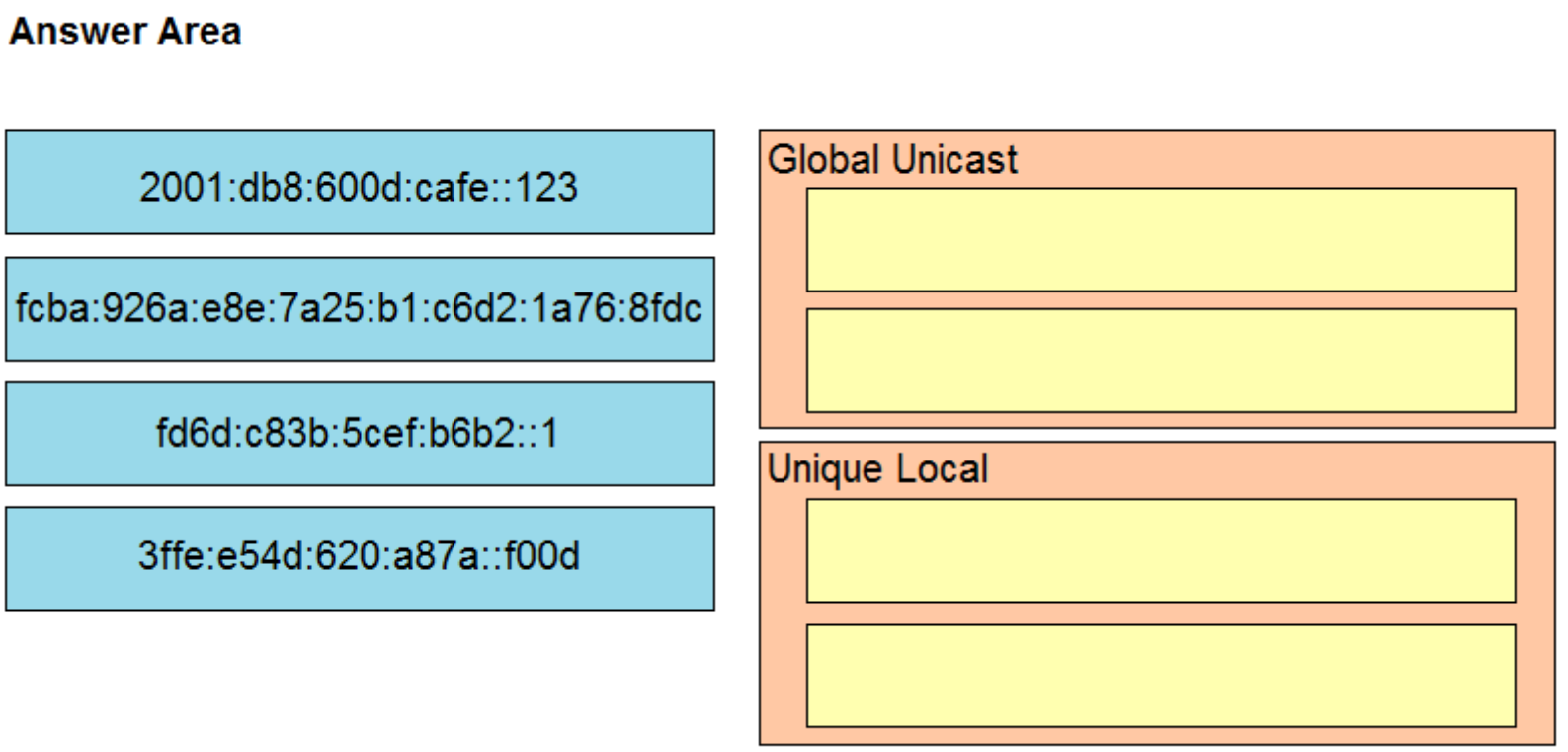
Answer is correct

upvoted 4 times

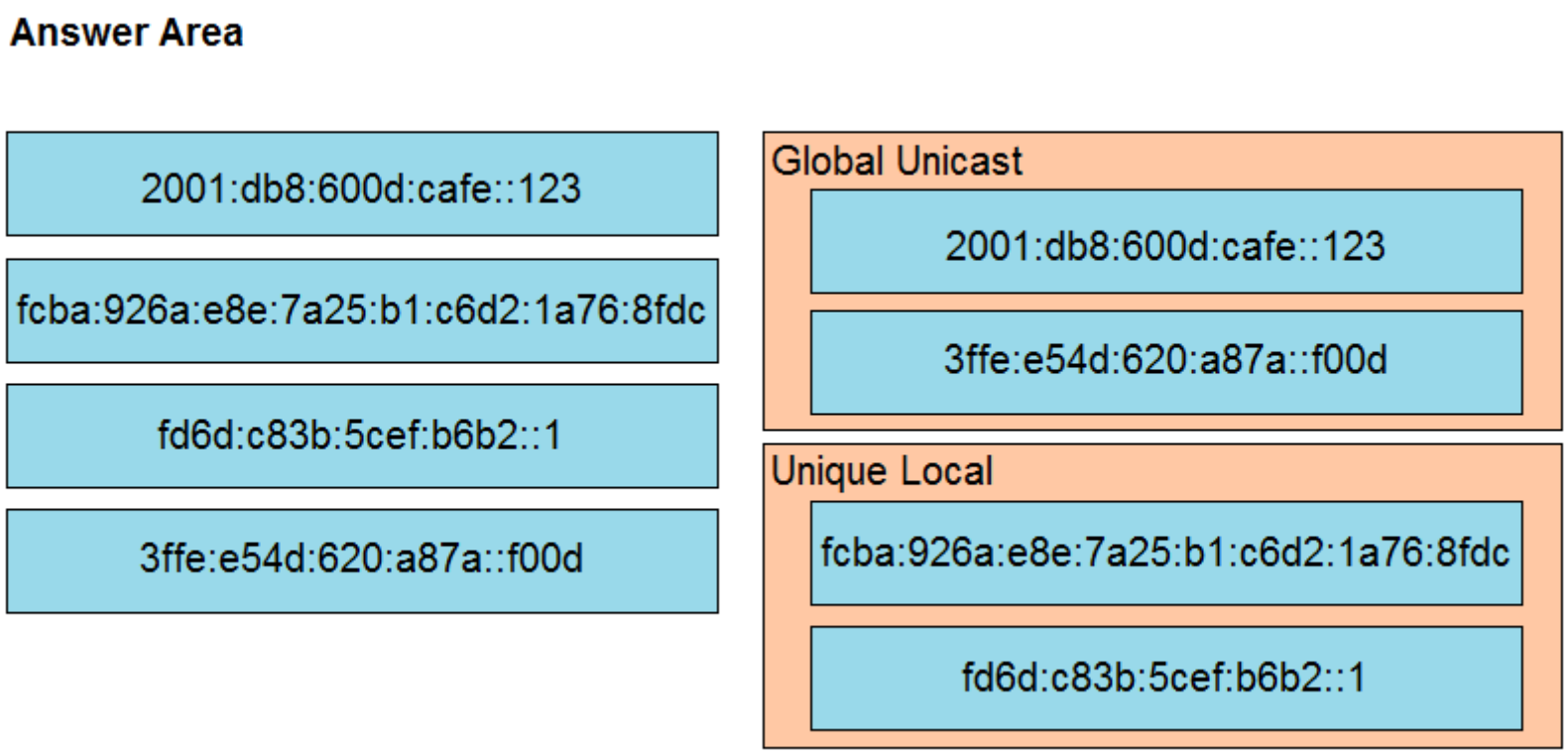
DRAG DROP -

Drag and drop the IPv6 addresses from the left onto the corresponding address types on the right.

Select and Place:



Correct Answer:



Reference:

https://learningnetwork.cisco.com/s/question/0D53i00000Kt6kl/ipv6-unique-local-addresses

netzwork Highly Voted 11 months, 3 weeks ago

Unique local addresses will begin with either FC or FD:

The first 7 bits indicate that we have a unique local address. 1111 110 in binary is FC in hexadecimal. However, the L bit (8th bit) has to be set to 1 so we end up with 1111 1101 which is FD in hexadecimal.

https://networklessons.com/ipv6/ipv6-address-types

upvoted 12 times

NetStef Most Recent 9 months ago

Answer is correct

upvoted 4 times

Question #97 *Topic 1*

Which type of organization should use a collapsed-core architecture?

A. small and needs to reduce networking costs

B. large and must minimize downtime when hardware fails

C. large and requires a flexible, scalable network design

D. currently small but is expected to grow dramatically in the near future

Correct Answer: *A*
It is ideal for small companies: The collapsed core model is a reduced version of the three-tier model. The deduction was made to create a network for small and medium-sized campuses. Therefore, smaller institutions can get the advantage of using a collapsed core network while still gaining the same benefits they would if they were using a three-tier model. Small organizations often cannot afford the hardware and human resources to run the network can benefit greatly with less oversight necessary.
And reduces cost: In a traditional three-tier campus network, the core layer is typically a complex and expensive piece of hardware. This layer is eliminated with collapsed core architecture, reducing both cost and complexity.

Community vote distribution

A (100%)

ZUMY 1 year, 3 months ago

A is correct

upvoted 2 times

Jbcrggddfhh 1 year, 4 months ago

Selected Answer: A

A is correct.

It is ideal for small companies: "The collapsed core model is a reduced version of the three-tier model. The deduction was made to create a network for small and medium-sized campuses. Therefore, smaller institutions can get the advantage of using a collapsed core network while still gaining the same benefits they would if they were using a three-tier model. Small organizations often cannot afford the hardware and human resources to run the network can benefit greatly with less oversight necessary."

And reduces cost: "In a traditional three-tier campus network, the core layer is typically a complex and expensive piece of hardware. This layer is eliminated with collapsed core architecture, reducing both cost and complexity."

Reference: https://www.insightssuccess.com/what-is-collapsed-core-architecture-and-how-its-useful/

upvoted 3 times

Question #98 *Topic 1*

A network administrator is setting up a new IPv6 network using the 64-bit address 2001:0EB8:00C1:2200:0001:0000:0000:0331/64. To simplify the configuration, the administrator has decided to compress the address. Which IP address must the administrator configure?

A. ipv6 address 2001:EB8:C1:22:1::331/64

B. ipv6 address 21:EB8:C1:2200:1::331/64

C. ipv6 address 2001:EB8:C1:2200:1:0000:331/64

D. ipv6 address 2001:EB8:C1:2200:1::331/64

Correct Answer: *D*

Community vote distribution

D (100%)

Junior_Network 19 hours, 44 minutes ago

Selected Answer: D

D is correct

upvoted 1 times

soe_life 3 months ago

Selected Answer: D

d is correct

upvoted 1 times

Eyad_Alotaibi 9 months ago

Selected Answer: D

Correct answer is D

upvoted 3 times

Yunus_Empire 9 months, 2 weeks ago

Selected Answer: D

Correct D

upvoted 4 times

MisterK_77 1 year ago

Selected Answer: D

DDDDDDDD

upvoted 3 times

[Removed] 1 year, 1 month ago

Only leading zero (not trailing zeros) are removed
https://www.ciscopress.com/articles/article.asp?p=2803866#:~:text=Rule%201%3A%20Omit%20Leading%200s,the%20address%20to%20be%20ambiguous.

upvoted 1 times

Quantum14 1 year, 1 month ago

are these the real answers? or are answers given in this forum?,
I want to know if this is a forum error or the real test has this same error
The correct answer is the letter D, without a doubt

upvoted 1 times

vuhidus 1 year, 1 month ago

Selected Answer: D

DDDDDDDDD

upvoted 3 times

coralreef 1 year, 1 month ago

The correct answer is the letter D.
In The suggested answer or letter A there is an error in the fourth field because trailing zeros were omitted.
The rule in IPv6 addresses for omitting zeros indicates that only leading zeros can be omitted.

upvoted 1 times

hp2wx 1 year, 1 month ago

The given answer is 100% wrong. You are not allowed to remove non-leading/floating 0s in an IPv6 address. D is the only answer choice that properly abbreviates the IPv6 Address as it only removes leading 0s and uses :: notation properly.

upvoted 1 times

Haider660 1 year, 2 months ago

Selected Answer: D

It's 2200. D

upvoted 1 times

ratu68 1 year, 2 months ago

Selected Answer: D

D 100% sure !

upvoted 4 times

SH_ 1 year, 2 months ago

Selected Answer: D

D because 2200 cannot be shortened to 22

upvoted 3 times

MDK94 1 year, 2 months ago

D is 100% correct, no way its wrong

upvoted 1 times

battery1979 1 year, 2 months ago

A would be correct if the fourth octet was 0022.

upvoted 2 times

Patrick69 1 year, 2 months ago

Selected Answer: D

D only!

upvoted 3 times

Marcos9410 1 year, 2 months ago

Selected Answer: D

D is the correct answer.

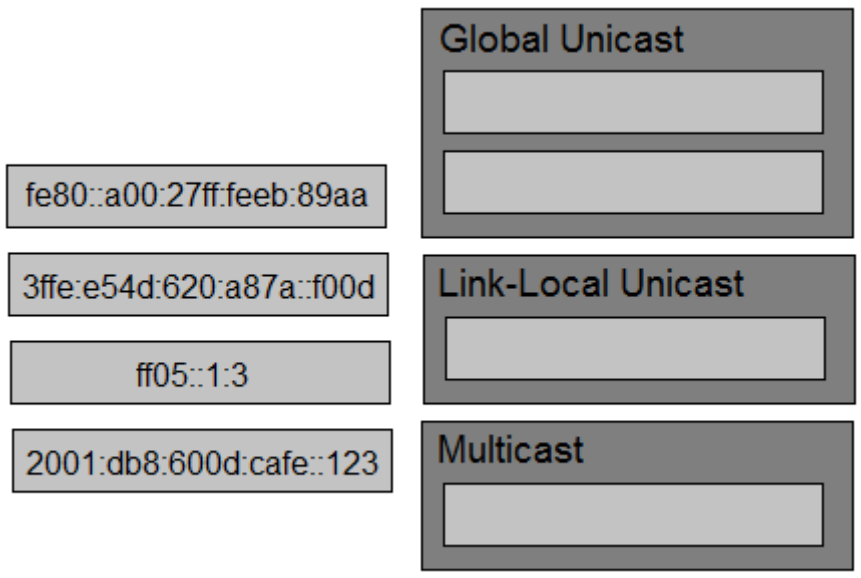
Only LEADING 0s can be removed (compressed)

upvoted 2 times

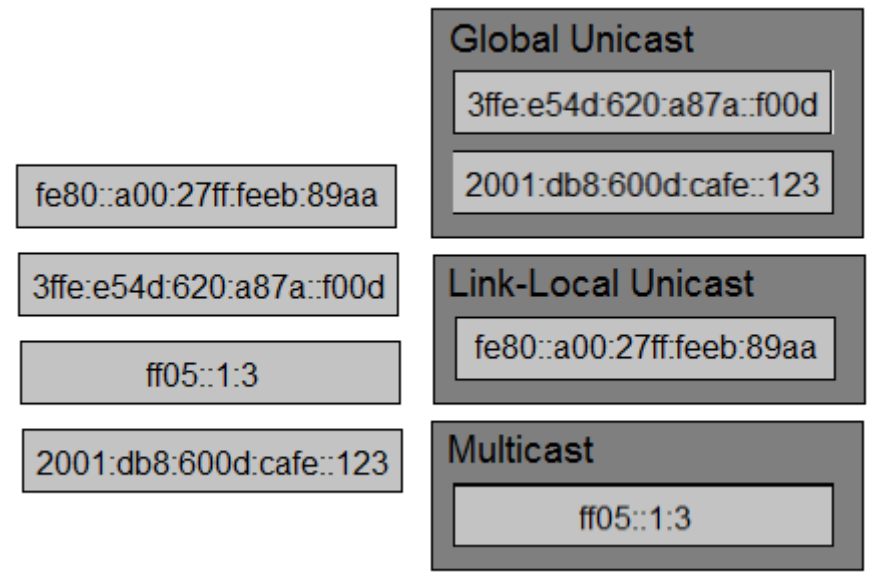
DRAG DROP -

Drag and drop the IPv6 addresses from the left onto the corresponding address types on the right.

Select and Place:



Correct Answer:



Danielki 5 months, 2 weeks ago

the address 3ffe:e54d:620:a87a::f00d might have been considered a global unicast address during the 6bone testing period, it is not considered a valid global unicast address in the current IPv6 address space.

upvoted 1 times

NetStef 9 months ago

Answer is correct

upvoted 4 times

DoBronx 10 months, 3 weeks ago

Im just going to assume Link Local starts with FE cuz of SNEAKEEEE Link

upvoted 3 times

Question #100 *Topic 1*

What is an appropriate use for private IPv4 addressing?

A. to allow hosts inside to communicate in both directions with hosts outside the organization

B. on internal hosts that stream data solely to external resources

C. on the public-facing interface of a firewall

D. on hosts that communicate only with other internal hosts

Correct Answer: *D*

Community vote distribution

D (100%)

GreatDane Highly Voted 8 months, 2 weeks ago

Selected Answer: D

A. to allow hosts inside to communicate in both directions with hosts outside the organization

Host inside a LAN may also use public IP addresses to communicate with hosts inside and outside the organization.
Wrong answer.

B. on internal hosts that stream data solely to external resources

Look at answer A.
Wrong answer.

C. on the public-facing interface of a firewall

Since private IP addresses can not be used on the public Internet, how can you configure a private IP address on the public-facing interface of a firewall?
Wrong answer.

D. on hosts that communicate only with other internal hosts

Would you buy and use public IP addresses for hosts that communicate only inside your LAN?
Correct answer.

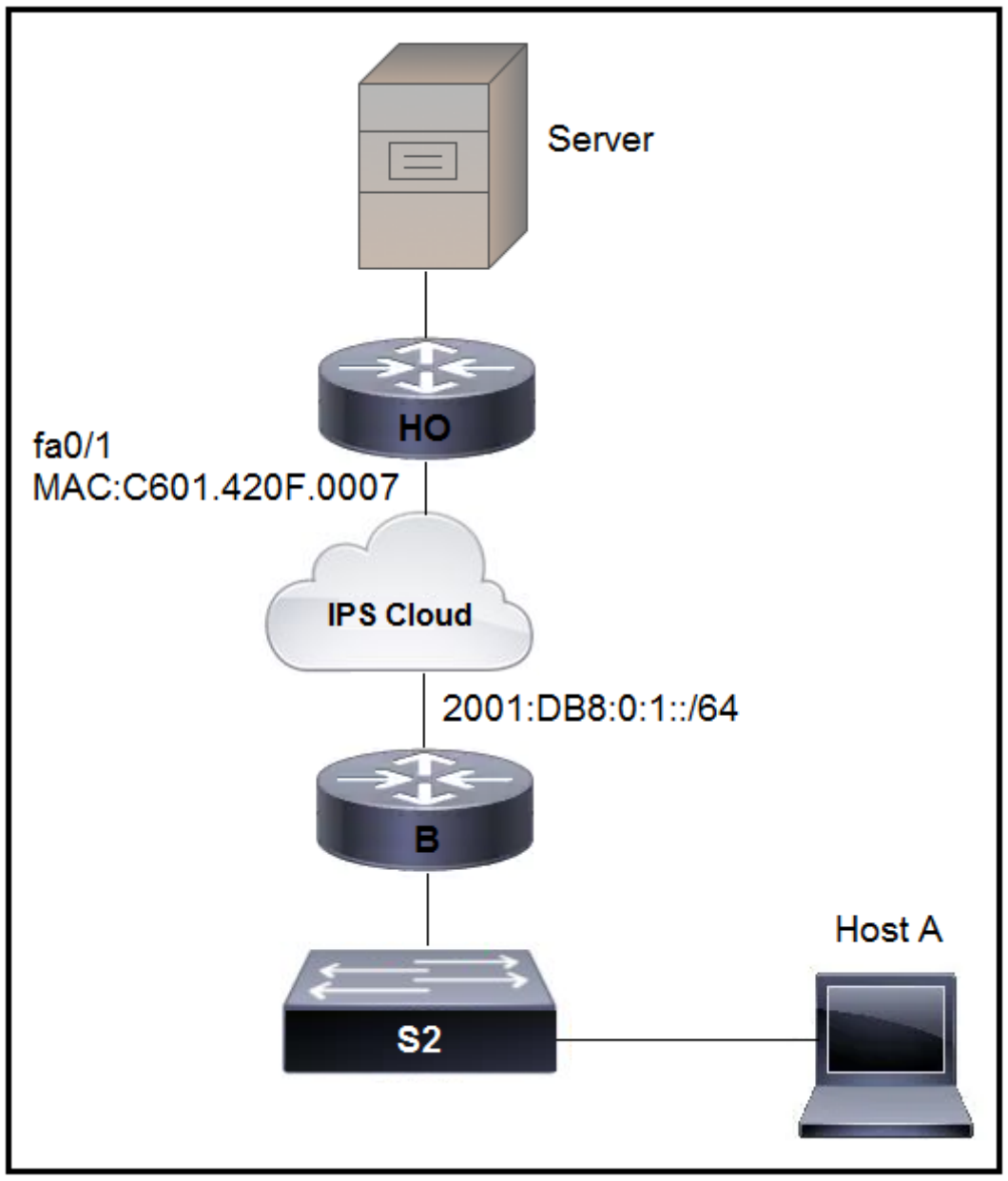
upvoted 6 times

ridhoc Highly Voted 10 months, 1 week ago

It's obviously D!!

upvoted 6 times

Question #101 *Topic 1*



Refer to the exhibit. An engineer is configuring the HO router. Which IPv6 address configuration must be applied to the router fa0/1 interface for the router to assign a unique 64-bit IPv6 address to itself?

A. ipv6 address 2001:DB8:0:1:FFFF:C601:420F:7/64

B. ipv6 address 2001:DB8:0:1:FE80:C601:420F:7/64

C. ipv6 address 2001:DB8:0:1:C601:42FF:FE0F:7/64

D. ipv6 address 2001:DB8:0:1:C601:42FF:800F:7/64

Correct Answer: *B*

Community vote distribution

C (83%) B (17%)

coralreef Highly Voted 10 months, 1 week ago

LETTER C IS THE CORRECT ANSWER
although IPv6 SLAAC (EUI-64) process is missing:
48 bit MAC Address = C6-01-420F:0007
split address in the middle = C6-01-42 0F-00-07
insert FF:FE = C6-01-42-FF:FE-0F-00-07
hexadecimal = C"6"-01-42-FF:FE-0F-00-07
7th bit in binary = 6 = 0000 0110
7th bit flip changes 6 to 4 = 0000 0100
64 bit host interface ID = C401:42FF:FE0F:0007

LETTER C IS THE CORRECT ANSWER
so,
ipv6 address 2001:DB8:0:1:C601.42FF:FE0F:7 /64

upvoted 20 times

Equiano Highly Voted 11 months, 3 weeks ago

Selected Answer: C

The correct answer here should be C even though the 7th bit was not inverted. The other options are no good.

upvoted 8 times

Junior_Network Most Recent 19 hours, 36 minutes ago

Selected Answer: C

it's C with ipv6 address 2001:DB8:0:1:C401:42FF:FE0F:7/64

upvoted 1 times

kyleptt 2 days, 17 hours ago

Selected Answer: C

I think they are asking for EUI 64 so FFFE should be in the ipv6 config

upvoted 1 times

kyleptt 2 weeks, 1 day ago

Selected Answer: C

Horrible question the answer is C add FFFE in the middle of the MAC and flip the 7th bit is how to obtain the EUI-64 Address

upvoted 1 times

bikila123 1 month, 1 week ago

the correct answer is C split into two and add FF FE into it and the invent the 7th bit if its 1 to 0 or if its 0 to 1

upvoted 1 times

raptuz 1 month, 2 weeks ago

Selected Answer: C

The letter C is correct, the flip of the 7th bit is only necessary when it is 0

upvoted 1 times

SAB5106 2 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

[Removed] 4 months, 1 week ago

Letter C should be the closest answer. The eui-64 process was not followed though.

upvoted 1 times

Vikramaditya_J 4 months, 1 week ago

Why Cisco asks such questions where none of the options is correct.
To generate an EUI-64 address, after converting the MAC, it will become: C401:42FF:FE0F:7
And IPv6 address will become: 2001:DB8:0:1:C401:42FF:FE0F:7

upvoted 5 times

kyleptt 1 month, 2 weeks ago

Correct the command for the creation of the EUI-64 Address was not given.

upvoted 1 times

HSong 4 months, 4 weeks ago

Selected Answer: C

The correct answer is C

upvoted 1 times

JBORBON 5 months ago

C is correct

upvoted 1 times

dearc 5 months, 2 weeks ago

Selected Answer: C

LETTER C IS THE CORRECT ANSWER

upvoted 1 times

elixirwell 5 months, 2 weeks ago

Selected Answer: C

ChatGPT says,
Based on the information provided, the answer would be option C: ipv6 address 2001:DB8:0:1:C601:42FF:FE0F:7/64. This is because the address configuration includes the interface identifier in the form of C601:42FF:FE0F:7 which is necessary to ensure that the router assigns a unique 64-bit IPv6 address to itself.

Option A (ipv6 address 2001:DB8:0:1:FFFF:C601:420F:7/64) does not include an interface identifier, so it would not provide a unique address.

Option B (ipv6 address 2001:DB8:0:1:FE80:C601:420F:7/64) is a link-local address, which is used for communication within the local network segment only, and cannot be used for communication outside of it.

Option D (ipv6 address 2001:DB8:0:1:C601:42FF:800F:7/64) does not have the correct format for the interface identifier, which should include the EUI-64 format, indicated by the FF:FE section in option C.

upvoted 2 times

joyboy92 7 months, 3 weeks ago

It should be C because:
- classic EUI-64 --> just splits the mac and insert FFFE
- modified EUI-64 (that now is the standard)--> splits the mac address, insert FFFE and inverts the 7th bit

upvoted 5 times

uditpatel1 4 months, 4 weeks ago

Yes, you are right but if the we invert 7th bit then 6 = 0110 so no 0100 = 4
So, thechniclly as per my suggestion there is no option to C4 like answers.

upvoted 1 times

ProgSnob 8 months, 1 week ago

Looking at the possibilities, it's definitely not A or D. It could be B or C. I believe it only flips the 7th bit if you configure the address with the "eui-64" command. In answers B and C they are manually entering the addresses so the bit wouldn't be flipped unless you did it manually. Option C manually enters the FFFE in the middle of the MAC address which gives the illusion that one would need to flip the 7th bit as well.

upvoted 1 times

freeknowledge123 8 months, 2 weeks ago

seems to me someone forgot to invert the 7 bit, there is no other explanation

upvoted 1 times

Question #102 *Topic 1*

What is a similarity between 1000BASE-LX and 1000BASE-T standards?

A. Both use the same data-link header and trailer formats.

B. Both cable types support RJ-45 connectors.

C. Both support up to 550 meters between nodes.

D. Both cable types support LR connectors.

Correct Answer: *A*

Community vote distribution

A (100%)

ricky1802 Highly Voted 7 months, 2 weeks ago

Selected Answer: A

1000BASE-LX:
Used for Gigabit Ethernet over optical fiber
Supports distances up to 10 km
Uses a single-mode fiber (SMF)

1000BASE-T:
Used for Gigabit Ethernet over copper cable
Supports distances up to 100 meters
Uses 4 pairs of copper wires
Supports speeds up to 1000 Mbps (1 Gbps)

upvoted 7 times

Fermento Most Recent 11 months, 1 week ago

Selected Answer: A

A is fine.

upvoted 3 times

```
C:\Users\ciscoadmin>ipconfig /all

Windows IP Configuration
   Host Name.....................: DESKTOP-480J88T
   Primary Dns Suffix............:
   Node Type.....................: Hybrid
   IP Routing Enabled............: No
   WINS Proxy Enabled............: No
   DNS Suffix Search List........: arcep.se

Ethernet adapter Ethernet:
   Media State...................: Media disconnected
   Connection-specific DNS Suffix :
   Description...................: Realtek PCIe GBE Family
Controller
   Physical Address..............: 3C-52-82-33-F3-BF
   DHCP Enabled..................: Yes
   Autoconfiguration Enabled.....: Yes
Wireless LAN adapter Wi-Fi
   Connection-specific DNS Suffix : arcep.se
   Description...................: Intel (R) Dual Band
Wireless-AC 7265
   Physical Address..............: C8-21-58-B4-F3-EF
   DHCP Enabled..................: Yes
   Autoconfiguration Enabled.....: Yes
   Link-local IPv6 Address.......: fe80::45a1:b3fa:2f37:bf37%2 (Preferred)
   IPv4 Address..................: 192.168.1.226 (Preferred)
   Subnet Mask...................: 255.255.255.0
   Lease Obtained................: October 3, 2019 12:28:08 PM
   Lease Expires.................: October 3, 2019 7:18:37 PM
   Default Gateway...............:  192.168.1.100
   DHCP Server...................: 192.168.1.254
   DHCPv6 IAID...................:  46670168
   DHCPv6 Client DUID............: 00-01-00-01-20-FF-05-55-3C-52-82-33-D3-84
   DNS Servers...................: 192.168.1.253
   NetBIOS over Tcpip............: Enabled
   Connection-specific DNS Suffix Search List :
                                   arcep.se
```

Refer to the exhibit. The given Windows PC is requesting the IP address of the host at www.cisco.com. To which IP address is the request sent?

A. 192.168.1.253

B. 192.168.1.100

C. 192.168.1.226

D. 192.168.1.254

Correct Answer: *A*

Community vote distribution

A (100%)

kyleptt 3 months ago

While I get that the DNS sever does this won't that be for local translations ? and the gateway to reach external DNS ?

upvoted 2 times

christian321 2 weeks, 2 days ago

The client is always using the DNS server within its network settings to resolve names into IPs. It does not matter wether the DNS server is internal or external; however if it was external, yes the request flows through the default gateway. But a local DNS server would also sent a request to another DNS server via the default gateway.

The questions just aims to point out the DNS server.

upvoted 1 times

Da_Costa 4 months, 3 weeks ago

DNS server resolves addresses such as www.cisco.com

upvoted 4 times

Ka_09 7 months ago

the given answer was wrong the correct option is DHCP server ip

upvoted 1 times

Fermento 11 months, 1 week ago

Selected Answer: A

Send for DNS serve, because url should be translate to IP address.

upvoted 4 times

j6 11 months, 2 weeks ago

Selected Answer: A

A correct - web address uses DNS server

upvoted 3 times

goms12 1 year ago

www.cisco.com request goes to the DNS server..Given option s the right one

upvoted 3 times

Question #104 *Topic 1*

Which function forwards frames to ports that have a matching destination MAC address?

A. frame flooding

B. frame filtering

C. frame pushing

D. frame switching

Correct Answer: *D*

Community vote distribution

D (100%)

Goh0503 Highly Voted 11 months, 4 weeks ago

Answer is D
Flooding means that the switch sends the incoming frame to all occupied and active ports (except for the one from which it was received

In forwarding , it first looks up the destination address in the MAC Address Table. It then forwards the frame to that specific port.

upvoted 7 times

dearc Highly Voted 5 months, 2 weeks ago

Selected Answer: D

The function that forwards frames to ports that have a matching destination MAC address is D. frame switching. As per the search results, a switch has four functions: learning, flooding, filtering, and switching. Specifically, switching is the function that allows a switch to forward frames to the proper Layer 2 port based on the destination MAC address . This is achieved by using a MAC address table to keep track of which MAC addresses are connected to which switch ports, and then forwarding frames only to the appropriate port based on the destination MAC address .

upvoted 5 times

bikila123 Most Recent 1 month, 1 week ago

D is correct
since its unicasting the known mac address

upvoted 1 times

Question #105 *Topic 1*

Which type of IPv6 address is similar to a unicast address but is assigned to multiple devices on the same network at the same time?

A. global unicast address

B. link-local address

C. anycast address

D. multicast address

Correct Answer: *C*

Community vote distribution

C (100%)

ricky1802 Highly Voted 7 months, 2 weeks ago

Selected Answer: C

An anycast address is similar to a unicast address but is assigned to multiple devices on the same network at the same time. When a device sends a packet to an anycast address, it is delivered to one of the devices with that address, selected based on the routing protocol's best-effort algorithm. This is useful for applications like load balancing and failover, where multiple devices provide the same service and it doesn't matter which one handles a particular request.

upvoted 8 times

dropspablo Most Recent 1 month, 3 weeks ago

An anycast address is more similar to a unicast address than a multicast address, as like a unicast an anycast can be assigned (configured) (eg DNS) on multiple devices in different geographic locations or parts of the network. Now a multicast is not a configurable address (assigned), it only sends to a group of devices on the same network.

upvoted 2 times

sol_ls95 8 months ago

why not multicast?

upvoted 1 times

manaoming 3 months ago

Multicast addresses refer to the entire group of hosts in that packets will be sent to all hosts that are members of the multicast group. Anycast addresses refer to one of the group of hosts in that packets will be sent to the host that is nearest, which is useful for servers in different geographical regions that serve the same service

upvoted 1 times

mrgreat 1 year ago

Answers is C
An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices.

upvoted 3 times

mzu_sk8 10 months, 2 weeks ago

in the same network? examples in books are a server in New york and a server in San Francesco ....

upvoted 1 times

Question #106 *Topic 1*

What is a characteristic of private IPv4 addressing?

A. composed of up to 65,536 available addresses

B. issued by IANA in conjunction with an autonomous system number

C. used without tracking or registration

D. traverse the Internet when an outbound ACL is applied

Correct Answer: *C*

Community vote distribution

C (100%)

iMo7ed 7 months, 1 week ago

Selected Answer: C

C is correct

upvoted 3 times

Request7108 9 months ago

A is incorrect because there are 65000 addresses in the 192s private range but there are 16 million in the 10.0.0.0 and 1 million in the 172s

upvoted 3 times

SVN05 7 months, 2 weeks ago

And If you combine all of IPv4 address spaces, you'll get 4,294,967,296 addresses to be exact.

upvoted 3 times

Question #107 *Topic 1*

What is a function of an endpoint on a network?

A. provides wireless services to users in a building

B. connects server and client device to a network

C. allows users to record data and transmit to a file server

D. forwards traffic between VLANs on a network

Correct Answer: *C*

An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Examples of endpoints include:

☞ Desktops
☞ Laptops
☞ Smartphones
☞ Tablets
☞ Servers
☞ Workstations

Internet-of-things (IoT) devices

▪

Community vote distribution

C (67%) B (33%)

Wwnz4 Highly Voted 11 months, 3 weeks ago

Terribly written answer for C

upvoted 12 times

Junior_Network Most Recent 19 hours, 25 minutes ago

another bad question... I'm not sure it's B or C

upvoted 1 times

PlsLetMePass 1 month ago

Selected Answer: B

The answer is B. connects server and client device to a network.

An endpoint is a device that is connected to a network. It can be a server, a client device, or a network appliance. The function of an endpoint is to connect to other devices on the network and to transmit and receive data.

Option A is incorrect because an endpoint does not provide wireless services to users in a building. This is the function of a wireless access point.

Option C is incorrect because an endpoint does not allow users to record data and transmit to a file server. This is the function of a file server.

Option D is incorrect because an endpoint does not forward traffic between VLANs on a network. This is the function of a Layer 3 switch.

upvoted 1 times

Coachof2 1 month, 1 week ago

C is the answer
B is an access switch no a endpoint

upvoted 1 times

hamish88 5 months, 1 week ago

B. connects server and client device to a network.

An endpoint is a device or software application that acts as a point of origin or destination for data transmitted over a network. Endpoints can include computers, smartphones, servers, printers, and other networked devices.

The function of an endpoint on a network is to connect a client device or a server to a network so that it can send or receive data. Endpoints can also provide additional functionality such as security, data backup, or remote access.

Option A is incorrect as providing wireless services is typically the function of a wireless access point (WAP) rather than an endpoint.

Option C is incorrect as recording data and transmitting it to a file server is a task that can be performed by a client device, but not necessarily by an endpoint.

Option D is incorrect as forwarding traffic between VLANs is typically the function of a layer 3 switch or a router, rather than an endpoint.

upvoted 4 times

j6 11 months, 2 weeks ago

Selected Answer: C

end point AKA host - written okay imo

upvoted 2 times

j6 11 months, 2 weeks ago

and other options would not make sense

upvoted 1 times

Question #108 *Topic 1*

What is the function of a controller in controller-based networking?

A. It serves as the centralized management point of an SDN architecture

B. It is a pair of core routers that maintain all routing decisions for a campus

C. It centralizes the data plane for the network

D. It is the card on a core router that maintains all routing decisions for a campus.

Correct Answer: *A*

Community vote distribution

A (100%)

dearc 5 months, 2 weeks ago

Selected Answer: A

The function of a controller in controller-based networking is A. It serves as the centralized management point of an SDN (Software-Defined Networking) architecture . The controller is responsible for managing network devices and implementing network policies, as well as providing a central point of control and visibility for the entire network. It enables dynamic, programmatically efficient network configuration through the use of software-based controllers or a centralized controller with open APIs (Application Programming Interfaces) that communicate with network devices and applications . This promotes increased network agility, scalability, and flexibility in response to changing business needs.

upvoted 3 times

[Removed] 11 months, 2 weeks ago

Selected Answer: A

Answer A is correct because a controller, or SDN controller, centralizes the control of the networking devices.

https://www.ciscopress.com/articles/article.asp?p=2995354&seqNum=2#:~:text=A%20controller%2C%20or%20SDN%20controller,the%20devices'%20distributed%20control%20plane.

upvoted 1 times

rick0813 10 months, 4 weeks ago

but A says that "centralized management point" , isn't it management plane and control plane is different in SDN Architecture?

upvoted 1 times

soRwatches 6 months, 1 week ago

it also confused me, this is a very tricky question if you don't read it at least twice.

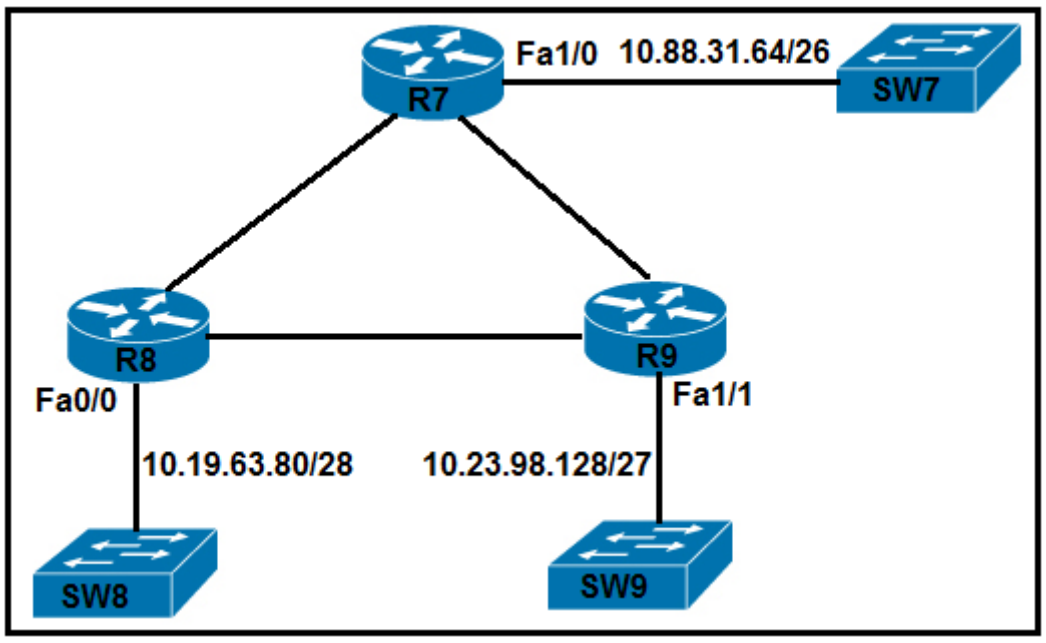
upvoted 1 times

RougePotatoe 10 months, 3 weeks ago

"What is the function of a controller in controller-based networking?" You might wanna read the question again no where does it mention control plane. It just asks what is the point of the controller.

upvoted 1 times

Question #109 *Topic 1*



Refer to the exhibit. Each router must be configured with the last usable IP address in the subnet. Which configuration fulfills this requirement?

A. R7# interface FastEthernet1/0 ip address 10.88.31.127 255.255.255.192 R8# interface FastEthernet0/0 ip address 10.19.63.95 255.255.255.240 R9# interface FastEthernet1/1 ip address 10.23.98.159 255.255.255.224

B. R7# interface FastEthernet1/0 ip address 10.88.31.126 255.255.255.240 R8# interface FastEthernet0/0 ip address 10.19.63.94 255.255.255.192 R9# interface FastEthernet1/1 ip address 10.23.98.158 255.255.255.248

C. R7# interface FastEthernet1/0 ip address 10.88.31.127 255.255.255.240 R8# interface FastEthernet0/0 ip address 10.19.63.95 255.255.255.192 R9# interface FastEthernet1/1 ip address 10.23.98.159 255.255.255.248

D. R7# interface FastEthernet1/0 ip address 10.88.31.126 255.255.255.192 R8# interface FastEthernet0/0 ip address 10.19.63.94 255.255.255.240 R9# interface FastEthernet1/1 ip address 10.23.98.158 255.255.255.224

Correct Answer: *D*

Community vote distribution

D (83%) B (17%)

Customexit Highly Voted 10 months, 3 weeks ago

You can do this fairly easily by process of elimination.

Starting with R7, a /26 is .192, so that leaves us with A or D.
The first difference between A and D is the last octet, 127 or 126 (respectively).

Do whatever process you prefer for subnetting and we figure that .126 is the last usable. .127 is the broadcast.

Answer is D.

upvoted 13 times

Junior_Network Most Recent 19 hours, 18 minutes ago

it's enough to look only R7 and answer is D

upvoted 1 times

Bhrino 4 months, 1 week ago

Selected Answer: D

Just look at the subnets mask.for r7 “/26” = .192 because 128 plus 64. Then for r8 “/28 “ = .240 because 128+64+32+16 that only leaves option d

upvoted 1 times

Bhrino 4 months, 1 week ago

Regarding the last usable up address for r7 because it’s /26 the subnets are going to be every 64 numbers specifically r7 .128 is the network up for the next subnet .127 is the broadcast and .126 is the last useable ip

upvoted 1 times

Hope_12 4 months, 1 week ago

Selected Answer: D

10.88.31.64 - 10.88.31.127/26 (FUH 10.88.31.65-10.88.31.126 LUH) inc = 64
Last usable host for R7(fa1/0)
10.88.31.126 255.255.255.192

10.19.63.80 - 10.19.63.95/28 (FUH 10.19.63.81-10.19.63.94 LUH) inc = 16
Last usable host for R8(fa0/0)

10.19.63.94 255.255.255.240

10.23.98.128 - 10.23.98.159/27 (FUH 10.23.98.129 - 10.23.98.158 LUH) inc = 32
Last usable host for R9(fa1/1)
10.23.98.158 255.255.255.224
upvoted 2 times

iMo7ed 7 months, 1 week ago

Selected Answer: D

it's D
upvoted 3 times

Tropicalsohot 8 months ago

Selected Answer: D

Subnet Mask of R7 is /26 thus 255.255.255.192
upvoted 1 times

binrayelias 8 months ago

I agree that D is the right answer
upvoted 1 times

joyboy92 8 months ago

Selected Answer: D

it's D
the subnet of first address in B is Wrong
upvoted 2 times

flash93933 8 months, 1 week ago

Selected Answer: D

Its D
the subnet masks in B are incorrect
upvoted 1 times

shubhambala 1 year ago

Selected Answer: B

The right answer is B. As for R9 the last usable address should be .158.
upvoted 2 times

EliasM 11 months, 4 weeks ago

I think its D. Check the answers again. The only difference between B and D is that in B, R9 subnet mask ends with .248, but it should be .224, because its a /27 network.
upvoted 3 times

EEGentle 11 months, 1 week ago

But why it has to be 224 and not 248 ?
upvoted 1 times

Customexit 10 months, 4 weeks ago

Because a /27 is .224

A .248 would be /29. R9 is not /29.
upvoted 2 times

rick0813 10 months, 4 weeks ago

because if 248 then i t will be /29.
upvoted 2 times

guynetwork 1 year ago

It is D
upvoted 4 times

Question #110 *Topic 1*

How do TCP and UDP fit into a query-responsible model?

A. TCP avoids using sequencing and UDP avoids using acknowledgments

B. TCP establishes a connection prior to sending data, and UDP sends immediately

C. TCP encourages out-of-order packet delivery, and UDP prevents re-ordering

D. TCP uses error detection for packets, and UDP uses error recovery.

Correct Answer: *B*

Community vote distribution

B (100%)

Xhuzepe 2 months, 4 weeks ago

Selected Answer: B

Out of the 4 answers, B is the correct one as it mentions 2 real properties (one for TCP and one for UPD).

upvoted 1 times

Prometheus_72 4 months, 3 weeks ago

B is the winner!

upvoted 4 times

Question #111 *Topic 1*

What provides centralized control of authentication and roaming in an enterprise network?

A. a lightweight access point

B. a wireless LAN controller

C. a firewall

D. a LAN switch

Correct Answer: *B*

Community vote distribution

B (100%)

StingVN 4 months, 2 weeks ago

Agree with B

upvoted 1 times

dearc 5 months, 2 weeks ago

Selected Answer: B

The correct answer to the question "What provides centralized control of authentication and roaming in an enterprise network?" is B - a wireless LAN controller.

A wireless LAN (Local Area Network) controller (WLC) is a device that provides centralized control and management of multiple wireless access points (APs) in a wireless network . It is responsible for configuring and monitoring the access points, managing the wireless traffic, and providing security protocols such as authentication and encryption. The WLC also enables seamless roaming between the access points without the need for reauthentication, as it maintains a centralized database of user credentials and authentication information.

Therefore, in an enterprise network, a wireless LAN controller provides centralized control of authentication and roaming for wireless clients .

upvoted 3 times

bruno0147 10 months, 4 weeks ago

B is correct

upvoted 4 times

Question #112 *Topic 1*

Which set of 2 4 GHz nonoverlapping wireless channels is standard in the United States?

A. channels 1, 6, 11, and 14

B. channels 2, 7, 9, and 11

C. channels 2, 7, and 11

D. channels 1, 6, and 11

Correct Answer: *D*

mrgreat 1 year ago

D is correct
https://www.metageek.com/training/resources/why-channels-1-6-11/

upvoted 3 times

Eagleswing 1 year ago

Answer D
https://community.cisco.com/t5/wireless/overlapping-v-s-non-overlapping-channels/td-p/601900

upvoted 2 times

Question #113 *Topic 1*

A network engineer is installing an IPv6-only capable device. The client has requested that the device IP address be reachable only from the internal network.
Which type of IPv6 address must the engineer assign?

A. IPv4-compatible IPv6 address

B. unique local address

C. link-local address

D. aggregatable global address

Correct Answer: *C*

Community vote distribution

B (97%)

mrgreat Highly Voted 1 year ago

It should be B! Only reachable from the internal network, not the internet.
https://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=4

Global unicast: A routable address in the IPv6 Internet, similar to a public IPv4 address.

Link-local: Used only to communicate with devices on the same local link.

Loopback: An address not assigned to any physical interface that can be used for a host to send an IPv6 packet to itself.

Unspecified address: Used only as a source address and indicates the absence of an IPv6 address.

Unique local: Similar to a private address in IPv4 (RFC 1918) and not intended to be routable in the IPv6 Internet. However, unlike RFC 1918 addresses, these addresses are not intended to be statefully translated to a global unicast address.

IPv4 embedded: An IPv6 address that carries an IPv4 address in the low-order 32 bits of the address.

upvoted 13 times

splashy Highly Voted 11 months, 1 week ago

If "the internal network" is 1 subnet for all nodes = C
If "the internal network" is more than 1 subnet for all nodes = B
Best practice is probably B, easier to for scaling by implementing more subnets in the future.
But it's still a Cisco question...

upvoted 8 times

sniek Most Recent 22 hours, 54 minutes ago

How can they get this wrong? Its most definitely not Link local as the only communication possible would be with the device that connects directly to it. Not other hostS from the network.

upvoted 1 times

kyleptt 2 days, 12 hours ago

Selected Answer: B

100 % B

upvoted 1 times

aymanmk 2 months ago

Selected Answer: B

unique local address

upvoted 1 times

abdelkader163 2 months, 3 weeks ago

Selected Answer: B

It's most likely to B

upvoted 1 times

Xhuzepe 2 months, 4 weeks ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

VanessaR05 3 months ago

Selected Answer: B

C SHOULD BE the answer

upvoted 1 times

VanessaR05 3 months ago

SORRY B SHOULD BE THE CORRECT ANSWER

upvoted 1 times

Friday_Night 4 months ago

So if this comes up in the Cisco exam, they will consider C as the correct answer?

upvoted 1 times

TR3Y 4 months ago

Selected Answer: C

Im going with C here. from this site I have found: Link-local addresses can be used to reach the neighboring nodes attached to the SAME LINK. Unique local can do the same but multiple (still not publicly routable). let me know If I am missing something here.
https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113328-ipv6-lla.html

upvoted 1 times

Isuzu 4 months, 2 weeks ago

To ensure that the device is reachable only from the internal network, the engineer must assign a unique local address. Unique local addresses (ULAs) are private IPv6 addresses that are not globally routable and are intended for use within a specific organization. They are similar to IPv4 private addresses in that they provide a way to address devices within a private network without exposing them to the public internet.

upvoted 1 times

shumps 4 months, 3 weeks ago

C is the answer,
Link local addresses are used in one single network segment, they can't be routed. Unique local addresses can be routed, but only within one routing domain.

upvoted 1 times

HSong 4 months, 4 weeks ago

The answer is C??? How come.

upvoted 1 times

thomson_johnson 6 months ago

How can engineer assign a link-local address, if it is generated automatically on IPv6 enabled interfaces using EUI-64 rules?
Plus it also depends as others have mentioned on what internal means, single subnet or entire internal site network.

upvoted 1 times

tubirubs 1 month, 1 week ago

wHAT??? utilize the comand ipv6 address x:x:x:x:x:x:x:x link-local

lol

upvoted 1 times

harkindeylee 6 months, 2 weeks ago

The answer should be unique local

upvoted 2 times

Cue_The_Joy 6 months, 3 weeks ago

Selected Answer: B

The IPv6 unique local addresses have some similarity to RFC 1918 private addresses for IPv4, but there are significant differences:

Unique local addresses are used for local addressing within a site or between a limited number of sites.
Unique local addresses can be used for devices that will never need to access another network.
Unique local addresses are not globally routed or translated to a global IPv6 address.

An IPv6 link-local address (LLA) enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet).
Packets with a source or destination LLA cannot be routed beyond the link from which the packet originated.

upvoted 2 times

Yaqub009 7 months, 1 week ago

Selected Answer: B

Unique Local Addresses (ULA) may eventually be used to address devices that should not be accessible from the outside, such as internal servers and printers. - CISCO

upvoted 1 times

Question #114 *Topic 1*

What is a requirement for nonoverlapping Wi-Fi channels?

A. different security settings

B. discontinuous frequency ranges

C. unique SSIDs

D. different transmission speeds

Correct Answer: *B*

Community vote distribution

B (100%)

Isuzu 4 months, 2 weeks ago

The requirement for non-overlapping Wi-Fi channels is that they must use discontinuous frequency ranges. Wi-Fi channels are defined by a specific frequency range, and adjacent channels overlap with each other. If two access points are using channels that overlap, they will cause interference and reduce the quality of the Wi-Fi network.

To avoid interference, it's necessary to choose Wi-Fi channels that don't overlap. The most common Wi-Fi channels in use are 1, 6, and 11, and they don't overlap with each other. This means that if you have multiple access points in the same area, you can assign each access point a different channel from this set of channels to avoid interference.

Different security settings, unique SSIDs, and different transmission speeds are not requirements for non-overlapping Wi-Fi channels, but they are important considerations for setting up a secure and efficient Wi-Fi network.

upvoted 1 times

StingVN 4 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

freeknowledge123 8 months, 2 weeks ago

can a guru explain the answer?

upvoted 1 times

laurvy36 8 months, 2 weeks ago

you have 1, 6 and 11 as channels, as nonoverlapping ones, not 123 or 456 etc

upvoted 1 times

laurvy36 8 months, 2 weeks ago

those channels are discontinuous

upvoted 1 times

Question #115 *Topic 1*

A network engineer must implement an IPv6 configuration on the vlan 2000 interface to create a routable locally-unique unicast address that is blocked from being advertised to the internet. Which configuration must the engineer apply?

A. interface vlan 2000 ipv6 address ff00:0000:aaaa::1234:2343/64

B. interface vlan 2000 ipv6 address fd00::1234:2343/64

C. interface vlan 2000 ipv6 address fe80:0000:aaaa::1234:2343/64

D. interface vlan 2000 ipv6 address fc00:0000:aaaa::a15d:1234:2343:8aca/64

Correct Answer: *D*

Community vote distribution

B (86%) 14%

cyborg7 Highly Voted 11 months, 2 weeks ago

D is incorrect as it contains :: which replaced with 0000.0000 will make the address longer than 128bits
Correct is B

upvoted 13 times

Sacuxipo 7 months, 2 weeks ago

fc00 : 0000 : aaaa :: a15d : 1234 : 2343 : 8aca
1st 2nd 3rd 5th 6th 7th 8th
I separated in this way to show you that it´is missing the 4th hextet. Guess where it must be?
D is correct man.

upvoted 2 times

FALARASTA 5 months ago

From slide notes

A double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros.
Example:
2001:db8:cafe:1:0:0:0:1 (leading 0s omitted) could be represented as 2001:db8:cafe:1::1

Note: The double colon (::) can only be used once within an address, otherwise there would be more than one possible resulting address

upvoted 2 times

Xhuzepe 2 months, 4 weeks ago

This is wrong. A double colon represents 2 or more all 0 quartets, not just one all 0 quartet. If it's only one quartet with all 0s, you simply put one 0.

upvoted 1 times

FALARASTA 5 months ago

You should refer the use of :: it means a a whole hextet but all are zeros

upvoted 1 times

Dutch012 7 months ago

if there is one all-0 quartet, don't use '::', just put one 0 instead.
so the correct one is B.

upvoted 2 times

molly_zheng 5 months, 1 week ago

RFC4291 recommended that " The use of "::" indicates one or more groups of 16 bits of zeros." refer to https://www.rfc-editor.org/rfc/rfc4291.html

upvoted 3 times

Madzonga 2 weeks, 3 days ago

it should also be the leftmost if there are two sets of 0s of equal length and in this address there's a group of 16 bits of zeros to the left of ::

upvoted 1 times

Bl1024 Highly Voted 11 months ago

Selected Answer: B

D is wrong address is too long

upvoted 8 times

Junior_Network Most Recent 19 hours, 1 minute ago

Selected Answer: B

I think it's B
upvoted 1 times

Cynthia2023 1 month ago

Selected Answer: B

Unique local addresses use prefix fc00::/7. The first bit following the prefix indicates, if set, that the address is locally assigned. This splits the address block in two equally sized halves, fc00::/8 and fd00::/8.

The block with L = 0, fc00::/8, is currently not defined.[1] It has been proposed that an allocation authority manage it, but this has not gained acceptance in the IETF.[8][9][10]
The block with L = 1, fd00::/8 follows the following format.
https://en.wikipedia.org/wiki/Unique_local_address#:~:text=unique%20local%20addresses.-,Definition,8%20and%20fd00%3A%3A%2F8.

SO, Unique Local Addresses (ULAs) are defined in RFC 4193, and the prefix range for ULA is indeed fd00::/8 to fdff::/8.
upvoted 2 times

raptuz 1 month, 2 weeks ago

Selected Answer: B

B is correct because the RFC 4193 tell the bit after the prefix FC00::/7 must be 1 so unique local addresses all begin with their first two digits as FD
upvoted 2 times

Xhuzepe 2 months, 4 weeks ago

Selected Answer: B

B is the correct answer.
If you decompress the IPv6 address fc00:0000:aaaa::a15d:1234:2343:8aca/64 it will have more than 8 hexadectets or quartets. It has a double colon between aaaa and a15d, which means it's a block of 2 or more continuous quartets of 0s. That leads to 9 or more quartets which is not the format of an IPv6 address. Max is 8 quartets (128 bits.)
upvoted 2 times

HM01 3 months, 1 week ago

D. interface vlan 2000 ipv6 address fc00:0000:aaaa::a15d:1234:2343:8aca/64

Option A (ff00::/8) represents a multicast address range, not a ULA.

Option B (fd00::/8) is the correct ULA prefix, but the specific address provided (fd00::1234:2343/64) is not within the recommended ULA prefix range (fd00::/8).

Option C (fe80::/10) represents a link-local address range, which is automatically assigned to interfaces but is not routable beyond the local link.

Therefore, option D is the most suitable choice for the given requirements.
upvoted 2 times

LexKin 3 months, 3 weeks ago

B is the best option. When assigning the unique local address, the bit after the seventh bit is always activated/ set to 1 hence it becomes FD.
upvoted 1 times

Friday_Night 4 months ago

yeah I think D is incorrect as well....
fc00:0000:aaaa::a15d:1234:2343:8aca
if you used :: then the :0000: must also be simplified to just :0: right?
upvoted 1 times

liviuml 5 months ago

Selected Answer: B

Correct answer is B.
Both B and D seems to be Unique Local but in D the problem isnot that double collon exist (can be used as short version of a sigle or multi 0000 valus.
The problem with D is there double collon should be used to replace first set of 0000 not the second as is in the answer.
Regards,
upvoted 1 times

elixirwell 5 months, 3 weeks ago

ChatGPT says:
To create a routable locally-unique unicast address that is blocked from being advertised to the internet on the vlan 2000 interface, the network engineer should apply a Unique Local Address (ULA) that starts with the prefix fd.

Therefore, the correct configuration for the vlan 2000 interface is:

B. interface vlan 2000 ipv6 address fd00::1234:2343/64

Option A is a multicast address (starts with FF00::/8) and cannot be assigned to an interface as a unicast address.

Option C is a link-local address (starts with FE80::/10) and cannot be routed outside of the local network.

Option D is also a ULA, but it uses a randomly generated Interface ID which may not be necessary and could be more difficult to manage. Additionally, it is a longer prefix (fc00::/7) which includes other types of addresses that are not necessarily meant to be used as locally-unique addresses.

upvoted 3 times

tal10 6 months, 3 weeks ago

Selected Answer: B

D is wrong address is too long

upvoted 1 times

Cue_The_Joy 6 months, 3 weeks ago

I'm not sure which answer is correct. However, here's verbatim what Cisco has to say about the use of the double colon; a double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros. Therefore, D would not be too long.

upvoted 6 times

TR3Y 4 months ago

Exactly I cant argue with the facts here. There is also no rule stating that the "::" must be used at the first 16BitHex. Tt can be in the front or in the back (wherever you want) but you can't use more than once on either side.

upvoted 1 times

jnanofrancisco 8 months, 1 week ago

B is the correct one

upvoted 2 times

freeknowledge123 8 months, 1 week ago

Selected Answer: D

i think FC is reserved FD is correct.

upvoted 1 times

ProgSnob 8 months, 1 week ago

A is for multicast
B is correct
C is for link-local
D is too long

The first 7 bits of FC00::/7 are 1111 110 which means that eighth bit can be a 0 or 1. If you make it a 1 then you can have FD00 which falls within the correct range.

upvoted 2 times

JohnJacobJr 9 months, 2 weeks ago

Selected Answer: B

Answer is B. D is incorrect because the double colon :: is only used to abbreviate MULTIPLE quartets of 0s. In the case of D, only ONE quartet is missing. Additionally, single quartets of 0's are represented by a sigle 0. D should be abbreviated as fc00:0:aaaa:0:a15d:1234:2343:8aca/64

upvoted 5 times

Question #116 *Topic 1*

What are two characteristics of an SSID? (Choose two.)

A. It uniquely identifies a client in a WLAN.

B. It is at most 32 characters long

C. It uniquely identifies an access point in a WLAN

D. It provides secured access to a WLAN.

E. It can be hidden or broadcast in a WLAN.

Correct Answer: *CD*

Community vote distribution

BE (96%) 2%

DixieNormus Highly Voted 1 year ago

Selected Answer: BE

Agree with B, E

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1300/12-2_15_JA/configuration/guide/o13ssid.html

States they contain up to 32 alphanumeric characters which supports B.
States multiple access points can use the same SSID so C is wrong.

The OCG on page 681 explains that an SSID can be broadcast or hidden by checking the "Broadcast SSID" checkbox.

upvoted 16 times

MonsieurP Highly Voted 4 months ago

An SSID is not an identifier of an Access Point. You can configure more than one SSID on an Access Point.

upvoted 5 times

Junior_Network Most Recent 18 hours, 56 minutes ago

Selected Answer: BE

Definitely wrong answers are A-C-D

upvoted 1 times

sniek 22 hours, 49 minutes ago

B E
B at most is correct. It cannot be longer,... But can be shorter.
E yes it can be shown and hidden. All other answers make no sense. Especially not the identifier of an accesspoint. An SSID can live on many AP's at once.

upvoted 1 times

4Lucky711 1 month, 2 weeks ago

Selected Answer: CE

Agree with @MohammedRafiq
B. It is at most 32 characters long. >> No, not 32 characters long. The SSID can consist of up to 32 alphanumeric, case-sensitive, characters.

I think CE is correct.
C. It uniquely identifies an access point in a WLAN (Other question)
E. It can be hidden or broadcast in a WLAN

upvoted 1 times

Yoyomax 2 months, 2 weeks ago

Selected Answer: BE

BE is the answer

upvoted 1 times

Rami1996 3 months, 2 weeks ago

IT'S B & E

upvoted 1 times

Isuzu 4 months, 2 weeks ago

B. It is at most 32 characters long: The SSID is a string of up to 32 characters that is used to identify a wireless network. It is case sensitive and can include letters, numbers, and special characters.

upvoted 1 times

StingVN 4 months, 2 weeks ago

Selected Answer: BE

I also agree with BE. But why correct answer from Cisco is CD? really do not understand.

upvoted 2 times

[Removed] 3 months, 1 week ago

From Cisco?

upvoted 1 times

MohammedRafiq 4 months, 3 weeks ago

B is incorrect, "SSID is not most 32 characters long, maximum 32 characters "

upvoted 3 times

christian321 2 weeks, 1 day ago

Look at the definition of "at most". It means "up to" so it is correct.

upvoted 1 times

thomson_johnson 6 months ago

Selected Answer: BE

C must be absolutely incorrect, you can make two or more WLANs coexist with the same SSID, you can then enable roaming if they overlap to make clients always have access when they move around

upvoted 1 times

cuenca73 7 months, 2 weeks ago

A - an SSID identifies an Access Point, no a client. Wrong.
B - True
C - two WLANs can coexist with the same SSID. Wrong.
D - the SSID is not related with security. Wrong
E - True

upvoted 4 times

lucantonelli93 7 months, 3 weeks ago

For me it's agree B and E.

upvoted 1 times

hasbulla01 10 months, 1 week ago

SSID it's only for identification... not have security for default

upvoted 2 times

Garfieldcat 10 months, 3 weeks ago

yeah, I agree BE

upvoted 3 times

rick0813 10 months, 4 weeks ago

Selected Answer: BE

BE , it can't be C because an ESS(extended service set) can have multiple access points with same SSID.

upvoted 3 times

RougePotatoe 10 months, 3 weeks ago

That's a horrible to explain it C is what the BSSID (MAC address) suppose to do.

upvoted 1 times

Sam7007 11 months, 1 week ago

Selected Answer: BE

B and E

upvoted 2 times

Question #117 *Topic 1*

When a switch receives a frame for a known destination MAC address, how is the frame handled?

A. flooded to all ports except the one from which it originated

B. forwarded to the first available port

C. sent to the port identified for the known MAC address

D. broadcast to all ports

Correct Answer: *C*

Community vote distribution

C (100%)

ccnanoob 1 month, 3 weeks ago

Selected Answer: C

The answer is C

upvoted 1 times

manaoming 3 months ago

I can see what the setter did... try to trick our eyes think it is an unknown address LOL

upvoted 2 times

Firewall2022 11 months, 4 weeks ago

The answer is C, "a frame for a known destination MAC address"

upvoted 4 times

IFBBPROSALCEDO 4 weeks ago

They are tricky!

upvoted 1 times

Cracked76 1 year ago

C it is

upvoted 2 times

Cracked76 1 year ago

A must be

upvoted 1 times

j6 11 months, 2 weeks ago

question says "known" not "unknown" so answer is C
if was "unknown" would be A

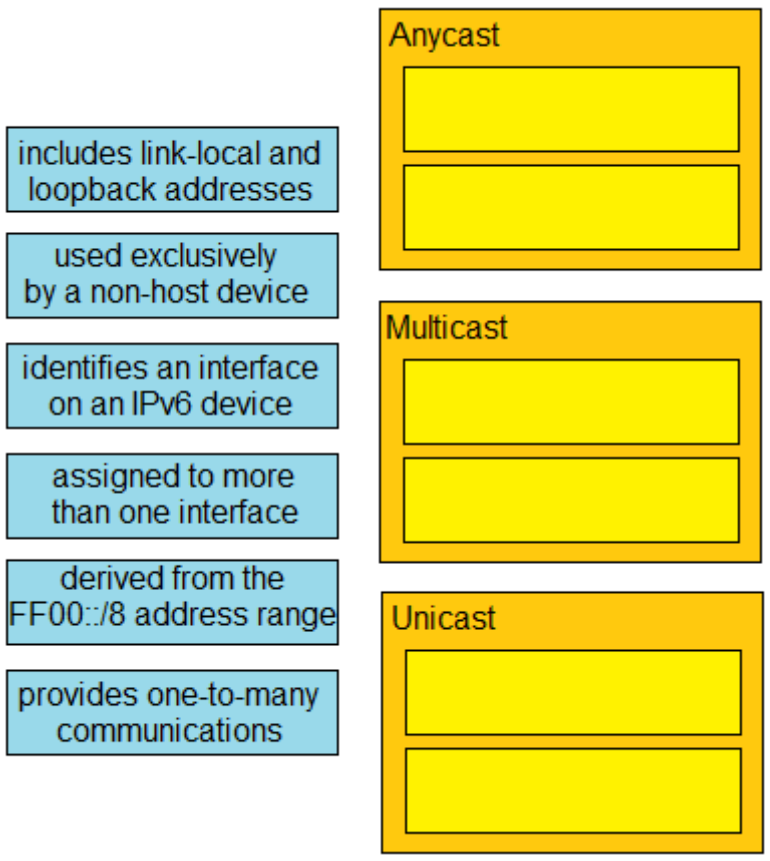
upvoted 1 times

Question #118 *Topic 1*

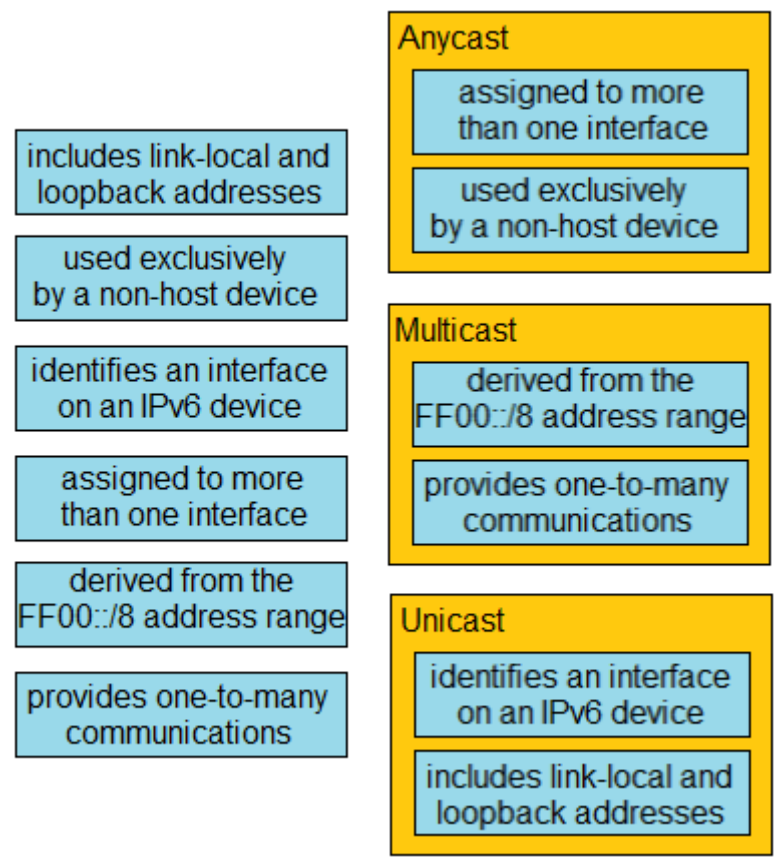
DRAG DROP -

Drag and drop the IPv6 address details from the left onto the corresponding types on the right.

Select and Place:



Correct Answer:



Yinxs 4 weeks ago

Official answer is correct.

upvoted 1 times

PlsLetMePass 1 month ago

Here is how I would categorize the descriptions into the 3 categories with only 2 descriptions per category:

Anycast
Assigned to more than one interface
Provides one to many communication
Multicast
Derived from the ff00::/8 address range
Used exclusively by a non-host device
Unicast
Identifies an interface on an IPv6 device
Includes link-local and loopback addresses

upvoted 2 times

AtousaF 1 month ago

Anycast addresses can be used only by a device, not a host, and anycast addresses must not be used as the source address of an IPv6 packet.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-3se/5700/ip6-anycast-add-xe.html#:~:text=Anycast%20addresses%20can%20be%20used,address%20of%20an%20IPv6%20packet.

upvoted 1 times

vnn777 2 months, 3 weeks ago

Why any-cast is used exclusively by non-host devices? It seems to me the opposit is correct.
Also one-to-many communication is a description of anycast, not multicast.

upvoted 3 times

Danny7 7 months, 2 weeks ago

Can link-local be considered as Uni cast?

upvoted 2 times

cuenca73 7 months, 2 weeks ago

Actually a link-local address is a type of unicast address

upvoted 5 times

Question #119 *Topic 1*

What is the collapsed layer in collapsed core architectures?

A. Core and distribution

B. access and WAN

C. distribution and access

D. core and WAN

Correct Answer: *A*

Community vote distribution

A (100%)

mrgreat Highly Voted 1 year ago

Answer A Correct
https://www.juniper.net/documentation/en_US/release-independent/nce/topics/concept/nce-182-evpn-collapsed-core-evpn-multihoming-campus-overview.html#:~:text=A%20collapsed%20core%20architecture%20takes,layer%20on%20a%20single%20switch.

A collapsed core architecture takes the normal three-tier hierarchical network and collapses it into a two-tier network. In a two-tier network, the function of the switches in the core layer and distribution layer are “collapsed” into a combined core and distribution layer on a single switch.

upvoted 6 times

AlexFordly Most Recent 11 months, 1 week ago

https://study-ccna.com/collapsed-core-and-three-tier-architectures/

upvoted 3 times

Vlad_Is_Love_ua 1 year ago

Selected Answer: A

If you choose a hierarchical tiered architecture, the exact number of tiers that you would implement in a network depends on the characteristics of the deployment site. For example, a site that occupies a single building might only require two layers while a larger campus of multiple buildings will most likely require three layers. In smaller networks, core and distribution layers are combined and the resulting architecture is called a collapsed core architecture.

upvoted 3 times

Question #120 *Topic 1*

What is a characteristic of a SOHO network?

A. includes at least three tiers of devices to provide load balancing and redundancy

B. connects each switch to every other switch in the network

C. enables multiple users to share a single broadband connection

D. provides high throughput access for 1000 or more users

Correct Answer: *C*

Community vote distribution

C (100%)

mrgreat Highly Voted 1 year ago

Answer C is correct
https://www.cisco.com/c/en/us/products/collateral/routers/soho-90-series-secure-broadband-routers/product_data_sheet09186a008014ede3.html
upvoted 8 times

ricky1802 Most Recent 7 months, 2 weeks ago

Selected Answer: C

SOHO stands for Small Office/Home Office, and a SOHO network refers to a network set up for a small office or home environment. It typically consists of a few computers, printers, and other devices connected together to allow for local file sharing, internet access, and other networking needs. A SOHO network can be set up using wired or wireless connections and can include a router, switch, and/or access point to manage the network and control access to resources. The main goal of a SOHO network is to provide a simple and cost-effective solution for small businesses or home users to connect their devices and share resources.

upvoted 3 times

Question #121 *Topic 1*

What is the role of disaggregation in controller-based networking?

A. It divides the control-plane and data-plane functions.

B. It streamlines traffic handling by assigning individual devices to perform either Layer 2 or Layer 3 functions

C. It summarizes the routes between the core and distribution layers of the network topology

D. It enables a network topology to quickly adjust from a ring network to a star network

Correct Answer: *A*

Community vote distribution

A (100%)

therandomjoke 5 months ago

Selected Answer: A

A its the way, in the SDN architecture the control plane and data plane are decouple.

upvoted 2 times

dearc 5 months, 2 weeks ago

Selected Answer: A

The answer to the question "What is the role of disaggregation in controller-based networking?" is:

A. It divides the control-plane and data-plane functions.

This answer is mentioned in multiple search results , including [1], [2], [3], and [4]. Answer B is also mentioned in some search results as a description of controller-based networking, but it is not the specific role of disaggregation within that architecture. Answers C and D are not mentioned in any relevant search results for this question.

upvoted 1 times

Radhie 8 months, 3 weeks ago

Taken literally, “network disaggregation” means to separate the network into its component parts. What we’re talking about here is the ability to source switching hardware and network operating systems separately. This is like buying a server from almost any manufacturer and then loading an OS of your choice.

Combining SDN and Disaggregation:
https://packetpushers.net/simplified-approach-sdn-network-disaggregation/

upvoted 2 times

RougePotatoe 10 months, 2 weeks ago

Does anyone know what disaggregation means? Its not in the OCCG.

upvoted 2 times

Cynthia2023 1 month, 1 week ago

Disaggregation in controller-based networking refers to the separation or division of control-plane and data-plane functions in a network architecture. In traditional networking, these functions are often tightly integrated into single devices like routers or switches. However, with disaggregation, the control-plane functions, responsible for making routing decisions and maintaining network information, are centralized in a controller, while the data-plane functions, which handle actual data forwarding, are distributed across the network devices.

upvoted 1 times

GhostWolf 10 months, 1 week ago

Network Function Disaggregation (NFD) defines the evolution of switching and routing appliances from proprietary, closed hardware and software sourced from a single vendor, towards totally decoupled, open components which are combined to form a complete switching and routing device.

this is what I found but it has nothing to do with the answers.

upvoted 1 times

Question #122 *Topic 1*

What is a function performed by a web server?

A. send and retrieve email from client devices

B. securely store files for FTP access

C. authenticate and authorize a user's identity

D. provide an application that is transmitted over HTTP

Correct Answer: *D*

Community vote distribution

D (100%)

mrgreat Highly Voted 1 year ago

Answer D is correct
https://www.techtarget.com/whatis/definition/Web-server#:~:text=The%20main%20job%20of%20a,email%2C%20file%20transfer%20and%20storage.

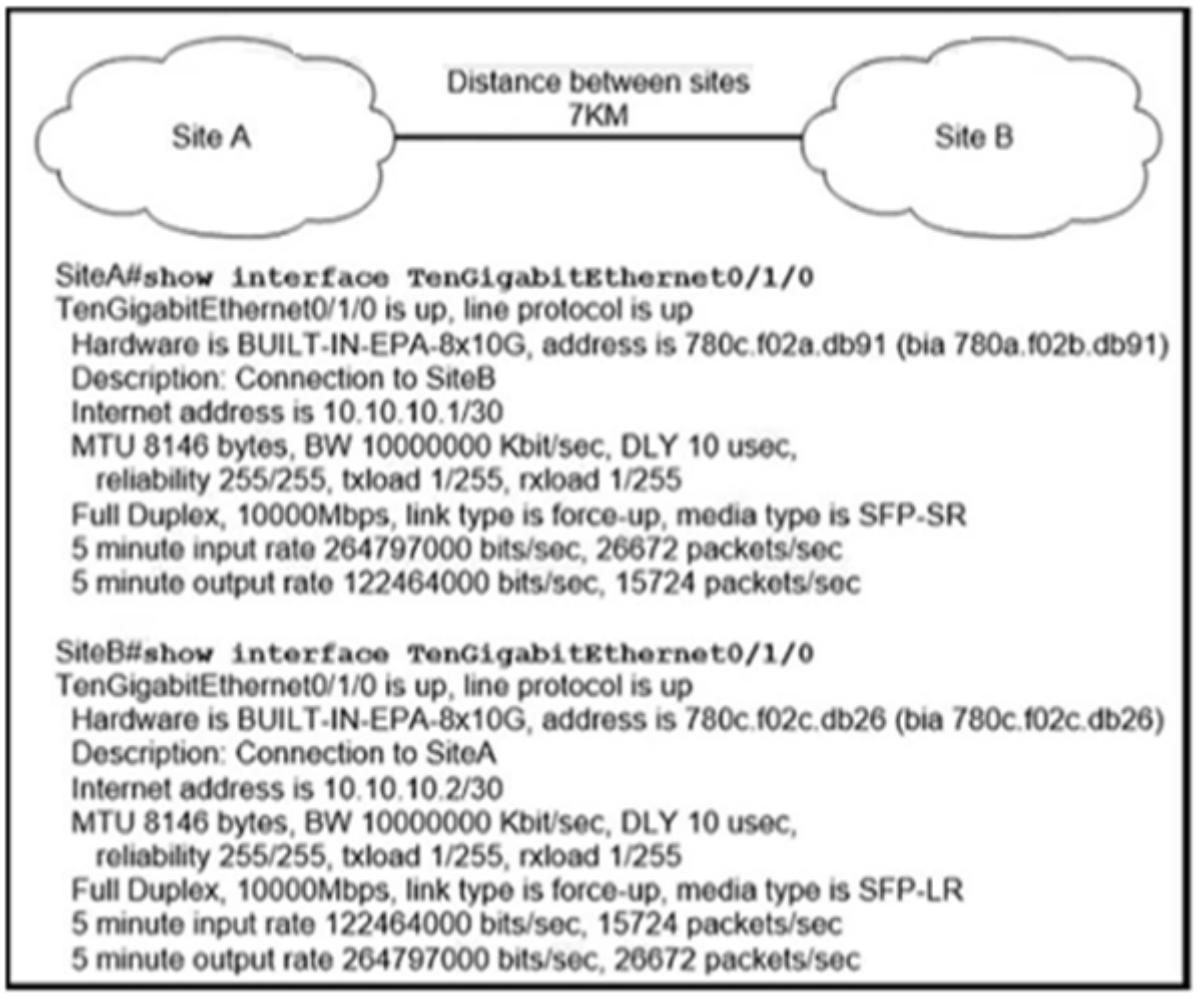
upvoted 6 times

Dutch012 Most Recent 7 months ago

Selected Answer: D

The web server uses HTTP/HTTPS

upvoted 4 times



Refer to the exhibit. Site A was recently connected to site B over a new single-mode fiber path. Users at site A report intermittent connectivity issues with applications hosted at site B. What is the reason for the problem?

A. Physical network errors are being transmitted between the two sites.

B. Heavy usage is causing high latency.

C. The wrong cable type was used to make the connection.

D. An incorrect type of transceiver has been inserted into a device on the link

Correct Answer: *D*

Community vote distribution

D (100%)

Bonesaw Highly Voted 12 months ago

Selected Answer: D

D is correct. The -SR stands for a short reach transceiver and is used for short range applications up to 300 meters, while the -LR can achieve up to 10km

upvoted 29 times

Bonesaw 11 months, 2 weeks ago

I'm back after taking my test and passing and would you believe this was question 101 of 101. Keep studying everyone

upvoted 46 times

[Removed] 3 months, 1 week ago

Wow! Thanks for letting us know. There are so many things to remember. I've been studying very hard for 15 months and i'm still not ready! But yes, i'll keep studying, there's no choice!

upvoted 4 times

NICE_ANSWERS 3 months, 3 weeks ago

Please how many questions are there on the standard exam?

upvoted 1 times

[Removed] 3 months, 1 week ago

Approximately 100 from what i've heard. Can be 94,97,101 but yes, about100.

upvoted 3 times

Wes_60 5 months, 3 weeks ago

Thanks for the feed back. My exam in less than 2 weeks. This gives me more confidence.

upvoted 3 times

Question #124 *Topic 1*

Which protocol uses the SSL?

A. SSH

B. HTTPS

C. HTTP

D. Telnet

Correct Answer: *B*

Community vote distribution

B (100%)

Vlad_Is_Love_ua Highly Voted 1 year ago

Selected Answer: B

HTTPS (port 443, TCP): HTTPS combines HTTP with a security protocol (Secure Sockets Layer [SSL]/Transport Layer Security[TLS]). DNS (port 53, TCP, and UDP): DNS is used to resolve Internet names to IP addresses.

upvoted 7 times

DixieNormus Highly Voted 1 year ago

Selected Answer: B

Trick question, nothing uses SSL anymore.

From the OCG page 325
SSL has been deprecated (see RFC 7568) and has been replaced by TLS.

also from the same page
TLS has many uses today, but most commonly, TLS provides the security features of HTTP Secure (HTTPS).

So the answer is technically B.

upvoted 5 times

mrgreat Most Recent 1 year ago

Answer B is correct.
https://www.acunetix.com/blog/articles/tls-security-what-is-tls-ssl-part-1/#:~:text=SSL%20and%20TLS%20are%20commonly,VoIP%2C%20VPN%2C%20and%20others.

upvoted 2 times

Question #125 *Topic 1*

Why is UDP more suitable than TCP for applications that require low latency such as VoIP?

A. UDP reliably guarantees delivery of all packets: TCP drops packets under heavy load

B. UDP uses sequencing data for packets to arrive in order TCP offers the capability to receive packets in random order

C. TCP uses congestion control for efficient packet delivery: UDP uses flow control mechanisms for the delivery of packets

D. TCP sends an acknowledgement for every packet received: UDP operates without acknowledgments

Correct Answer: *D*

Community vote distribution

D (100%)

everchosen13 Highly Voted 11 months, 2 weeks ago

Selected Answer: D

It is D just cause all the other answers are wrong but it doesn't really give an answer to the question.

upvoted 8 times

Yunus_Empire 9 months, 2 weeks ago

TCP sends acknowledgement packets back to the sender that the (For Example Packet#54 is received) but UDP does not acknowledge the sender whether the message received or not thats why UDP has low latency becz acknowledgements consume bandwidth....

upvoted 2 times

peplegal Most Recent 5 months ago

Selected Answer: D

Ther correct answer is "D", - But there is a typo in "every *packet* received". It should be ("every *segments* received" - Layer 4 - Transport) - Even though, letter "D" is a correct Answer.

1. The PDU of "Transport" Layer is called as a "Segment".
2. The PDU of "Network" Layer is called as a "Packet".
3. The PDU of the "Data-Link" Layer is called "Frames".

More information on source:
https://www.geeksforgeeks.org/difference-between-segments-packets-and-frames/

upvoted 3 times

ike110 8 months, 2 weeks ago

Should it be "segments" and not "packets"?

upvoted 2 times

peplegal 5 months ago

Yes, Ike !! You are Right !! Answer "D", It should be ("Segments" Layer 4 - Transport) instead of ("Packets" Layer 3 - Network) - Even though, letter "D" is a correct Answer.

upvoted 1 times

Question #126 *Topic 1*

What are the two functions of SSIDs? (Choose two.)

A. uses the maximum of 32 alphanumeric characters

B. controls the speed of the Wi-Fi network

C. used exclusively with controller-based Wi-Fi networks

D. supports a single access point

E. broadcasts by default

Correct Answer: *AD*
The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. The SSID can consist of up to 32 alphanumeric, case-sensitive, characters. Wireless clients connect using the SSID for secure communications. The SSID is a unique token that identifies an
802.11 wireless network. It is used by wireless devices to identify a network and to establish and maintain wireless connectivity. An SSID must be configured and assigned to a wireless client device interface before the device can associate with an access point.

Community vote distribution

AE (98%)

DixieNormus Highly Voted 1 year ago

Selected Answer: AE

Terrible question

A. uses the maximum of 32 alphanumeric characters
This is not a function, its a requirement, but it is true.
B. controls the speed of the Wi-Fi network
SSID has nothing to do with speed.
C. used exclusively with controller-based Wi-Fi networks
Any WLAN can have an SSID including autonomous which are not controller based.
D. supports a single access point
Multiple access points can share the same SSID.
E. broadcasts by default
The checkbox for broadcast is checked by default so this is true, still not a function.

A and E are true but are not functions.

upvoted 63 times

kyleptt 3 months ago

I second this comment

upvoted 1 times

DoBronx 10 months, 3 weeks ago

w comment.

upvoted 3 times

Yunus_Empire Highly Voted 9 months, 3 weeks ago

Selected Answer: AE

These are correct

upvoted 6 times

Junior_Network Most Recent 18 hours, 39 minutes ago

Selected Answer: AE

AE is correct but also they are not function :)

upvoted 1 times

BarkingSpider 1 month, 2 weeks ago

Selected Answer: DE

A isn't correct. The maximum of 32 *can* be used, but doesn't have to be 32.
B isn't correct. SSID has nothing to do with speed
C isn't correct. whether controller based or stand-alone APs, SSIDs are used either way.
D is correct. SSIDs support a single access point. They also support multiple APs. But a single is also supported, so this is a true statement.
E is correct. It broadcasts by default. Although it can be hidden.

upvoted 1 times

dropspablo 4 months, 2 weeks ago

Selected Answer: AD

Explanation of D
The SSID string must be consistent across all APs so that wireless clients can roam from one AP to another connected to their WLAN SSID. But when you have two SSIDs on an AP, a unique BSSID (logical AP) is generated for each SSID and its WLAN on the AP. So perhaps the answer is referring to the unique AP that is created by each SSID. The same AP can be composed of several logical APs with their independent BSSID (DFWMAC) for each SSID created. Being a single (logical) AP for each SSID on the AP. Remembering that in another AP the same SSID will have a different BSSID (DFWMAC).

upvoted 1 times

dropspablo 4 months, 2 weeks ago

The "broadcasts by default" function is a property of the BSSID, which is a unique identifier assigned to each wireless access point (AP), not the SSID. The BSSID is an essential part of the wireless communication protocol and is used to uniquely identify each AP on a wireless network. The SSID, on the other hand, is the name given to the wireless network, which is used by client devices to connect to it. Therefore, answer E can be considered incorrect, as it refers to a property of the BSSID and not the SSID.

upvoted 1 times

dropspablo 2 months, 2 weeks ago

Correcting, today I see that the correct answer would be the letter A and E. Because the letter D (supports a single access point) is wrong because we can have the same SSID in more than one AP, different from the BSSID that is unique in each AP (and SSID on the same AP). About the letter E (broadcasts by default) it is correct, because in the GENERAL Tab exactly when we create the SSID, the BROADCAST SSID option is enabled by default. I was trying to justify the ExamTopics answer but then I realized that you can't trust these wrong answers which just confuses us. In this link we can see that the broadcast is a function of the SSID that comes by default, and not the BSSID as I had informed. Therefore, the letter A and E I believe are correct as my colleagues claim!

https://mrncciew.com/2013/05/16/wlan-config-via-cli-part-1/

upvoted 1 times

beerbisceps1 5 months, 1 week ago

D is definitely not true.. I have 8 APs at my work place and they all connect through the same ssid.

upvoted 1 times

VictorCisco 5 months ago

There is no word ONLY. If there was an answer "support ONLY a single access point" you would be right, but in this case not! It could be one or many AP with the same SSID.

upvoted 3 times

elixirwell 5 months, 3 weeks ago

ChatGPT says:
The two functions of SSIDs (Service Set Identifiers) are:

Identification: An SSID is used to identify a specific wireless network, allowing devices to connect to the correct network.

Authentication: An SSID is also used to authenticate devices attempting to connect to the wireless network. Devices must provide the correct SSID along with any required credentials (such as a password or certificate) in order to connect.

Therefore, options A and E are partially correct as they relate to the characteristics of SSIDs, but they do not accurately describe the functions of an SSID.

Option B is not a function of SSIDs. The speed of the Wi-Fi network is primarily determined by the wireless standard and the capabilities of the devices connected to it.

Option C and D are also not accurate as SSIDs are used in both controller-based and controller-less Wi-Fi networks, and can be used to support multiple access points.

upvoted 1 times

rick0813 10 months, 2 weeks ago

Selected Answer: AE

C is wrong because its not only used in SDN ,

upvoted 2 times

RougePotatoe 10 months, 3 weeks ago

Selected Answer: AE

I follow with the sentiment question is bad but A,E are facts as I haven't heard of any APs that come with broadcast off by default. D is debatable because when multiple APs use the same SSID it become ESSID.
Can multiple APs use the same SSID? Yes.
Is it it called something different when multiple APs use the same SSID? Yes.
Would that mean an SSID support only one access point no.

Thus the conundrum of by definition yes but in practice no.

upvoted 2 times

everchosen13 11 months, 2 weeks ago

Selected Answer: AE

An SSID can be supported by MULTIPLE access points

upvoted 4 times

netzwork 11 months, 3 weeks ago

Selected Answer: AE

Definitely uses a max of 32 alphanumeric characters. Doesn't control the speed of the Wi-Fi network, it's not exclusive to controller-based networks, and SSID can be used in many access points. I would go with A and E

upvoted 1 times

Question #127 *Topic 1*

Which two characteristics describe the access layer in a three-tier network architecture? (Choose two.)

A. serves as the network aggregation point

B. physical connection point for a LAN printer

C. designed to meet continuous redundant uptime requirements

D. layer at which a wireless access point connects to the wired network

E. provides a boundary between Layer 2 and Layer 3 communications

Correct Answer: *BD*

The Access Layer is the one closer to the users. In fact, at this layer, we find the users themselves and the access-layer switches. The main purpose of this layer is to physically connect users to the network. In other words, there is just a cable between end-user PCs, printers, and wireless access points and access-layer switches.

Community vote distribution

BD (80%) AE (20%)

Junior_Network 18 hours, 37 minutes ago

Selected Answer: BD

BE for access layer

upvoted 1 times

Junior_Network 18 hours, 37 minutes ago

Sorry it was BD

upvoted 1 times

Hope_12 4 months, 1 week ago

Selected Answer: BD

B and D are for access layer.
A and E are description for distribution layer.
Question asks for access layer so answer is B and D.

upvoted 2 times

Isuzu 4 months, 2 weeks ago

B. physical connection point for a LAN printer and D. layer at which a wireless access point connects to the wired network are the two characteristics that describe the access layer in a three-tier network architecture.

Option A is incorrect because the aggregation point is typically found in the distribution layer, which aggregates traffic from the access layer.

Option C is incorrect because continuous redundant uptime requirements are typically associated with the core layer, which is responsible for providing high-speed connectivity and fault tolerance.

Option E is incorrect because the boundary between Layer 2 and Layer 3 communications is typically found in the distribution layer.

upvoted 1 times

harkindeylee 6 months, 2 weeks ago

I read the question wrong at first

. It for access layer. BD is correct. For distribution layer. AE is correct

upvoted 1 times

Dutch012 7 months ago

Selected Answer: BD

A & E for the distribution layer

upvoted 1 times

hoisin 7 months, 1 week ago

Now, which one is the correct answer BD or AE because Community vote distribution BD (60%) and AE (40%).

upvoted 2 times

Christopherjd20 7 months, 2 weeks ago

Selected Answer: BD

This question is asking for the characteristics for the access layer not the distribution.

So B & D

upvoted 1 times

DB_Cooper 8 months ago

Selected Answer: BD

The aggregation (or distribution) layer aggregates the uplinks from the access layer to the data center core.
From CCNA Data Center DCICT 640-916 Official Cert Guide.
access layer is closet to users

upvoted 3 times

freeknowledge123 8 months ago

Selected Answer: AE

AE seems correct and self explanatory

upvoted 1 times

DPAD 9 months ago

is A and E correct?

upvoted 1 times

binrayelias 8 months ago

B and D is correct for access layer while A and E is for distribution layer.

upvoted 2 times

Yunus_Empire 9 months, 3 weeks ago

What are two characteristics of the distribution layer in a three-tier network architecture? (Choose two.)

A. serves as the network aggregation point
B. provides a boundary between Layer 2 and Layer 3 communications
C. designed to meet continuous, redundant uptime requirements
D. is the backbone for the network topology
E. physical connection point for a LAN printer
A & B Correct

upvoted 4 times

Yunus_Empire 9 months, 3 weeks ago

What are two characteristics of the distribution layer in a three-tier network architecture? (Choose two.)

A. serves as the network aggregation point
B. provides a boundary between Layer 2 and Layer 3 communications
C. designed to meet continuous, redundant uptime requirements
D. is the backbone for the network topology
E. physical connection point for a LAN printer

upvoted 1 times

Olly123 11 months ago

Selected Answer: AE

A and E are both 'characteristics' that describe the access layer and also are correct.

upvoted 1 times

RougePotatoe 10 months, 3 weeks ago

Incorrect, distribution layer is the network aggregation point.
The aggregation (or distribution) layer aggregates the uplinks from the access layer to the data center core.
From CCNA Data Center DCICT 640-916 Official Cert Guide
https://learning.oreilly.com/library/view/ccna-data-center/9780133860429/ch01lev3sec2.html#ch01lev3sec2

upvoted 5 times

Customexit 10 months, 3 weeks ago

That sounds like Distribution Layer.

upvoted 6 times

Question #128 *Topic 1*

Which PoE mode enables powered-devices detection and guarantees power when the device detected?

A. auto

B. static

C. dynamic

D. active

Correct Answer: *A*

Community vote distribution

B (64%) A (33%)

BATSIE Highly Voted 8 months, 1 week ago

auto - Enables powered-device detection; if enough power is available, automatically allocates power to the PoE port after device detection (default setting).
max max-wattage - limits the power allowed on the port; range is 4000 to 30000 mW; if no value is specified, the maximum is allowed.
never - disables device detection, and disable power to the port.
Note:
If a port has a Cisco powered device connected to it, do not use the power inline never command to configure the port. A false link-up can occur, placing the port into the error-disabled state.

static - Enables powered-device detection; pre-allocate (reserve) power for a port before the switch discovers the powered device; the switch reserves power for this port even when no device is connected and guarantees that power will be provided upon device detection.
The switch allocates power to a port configured in static mode before it allocates power to a port configured in auto mode.

upvoted 12 times

mrgreat Highly Voted 1 year ago

Answer B is correct. Not A

https://www.thinlabs.com/faq/configure-cisco-switch-for-powering-poe-client#:~:text=static%20%2D%20Enables%20powered%2Ddevice%20detection,be%20provided%20upon%20device%20detection.

upvoted 8 times

MonsieurP Most Recent 1 week, 4 days ago

B is correct, not A
Refer to Cisco documentation titled "Configuring PoE"

upvoted 1 times

Da_Costa 3 weeks, 1 day ago

Selected Answer: B

Static is the correct answer

upvoted 1 times

Yinxs 4 weeks ago

Selected Answer: B

The key word is "guarantee".
A. auto mode can't guarantee, if enough power is available, the connected device can get the power.
B. static mode can pre-allocate the power, so it can guarantee the power to the device.

upvoted 1 times

MauroC19 4 weeks, 1 day ago

Selected Answer: A

Key word is "detection". For me, the correct answer is A
Check:
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011010.html

upvoted 1 times

Bili123 1 month ago

What is the correct answer?

upvoted 1 times

akareem999 1 month, 4 weeks ago

Selected Answer: B

Answer is B

static—Enables powered-device detection. Pre-allocate (reserve) power for a port before the switch discovers the powered device.

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011010.html#:~:text=static%E2%80%94Enables%20powered%2Ddevice%20detection,switch%20discovers%20the%20powered%20device.

upvoted 1 times

davidmdlp85 2 months ago

static : The device preallocates power to the port (even when no powered device is connected) and guarantees that power will be available for the port. The device allocates the port-configured maximum wattage, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is preallocated, any powered device that uses less than or equal to the maximum wattage, is guaranteed to be powered when it is connected to the static port. The port no longer participates in the first-come, first-served model.

However, if the powered device's IEEE class is greater than the maximum wattage, the device does not supply power to it. If the device learns through CDP messages that the powered device is consuming more than the maximum wattage, the device shuts down the powered device.

If you do not specify a wattage, the device preallocates the maximum value. The device powers the port only if it discovers a powered device. Use the static setting on a high-priority interface.

upvoted 2 times

zFlyingLotusz 2 months ago

Everyone... Everyone... It's D, Active.

For those who think "Static" has detection is wrong. The question states it requires gurenteed power and device detection, and the only one that provides both is Active.

Auto does not guarantee power if another port is allocated to Active.
Static does not have device detection.

upvoted 1 times

zFlyingLotusz 2 months ago

Everyone... Everyone... It's D, Active.

For those who think "Static" has detection is wrong. The question states it requires guaranteed power and device detection, and the only one that provides both is Active.

upvoted 1 times

Natalie89 2 months, 2 weeks ago

Selected Answer: B

static - Enables powered-device detection; pre-allocate (reserve) power for a port before the switch discovers the powered device; the switch reserves power for this port even when no device is connected and guarantees that power will be provided upon device detection

upvoted 1 times

xbololi 2 months, 3 weeks ago

Selected Answer: B

Configures the PoE mode on the port. Keywords and meanings:

auto - Enables powered-device detection; ""if enough power is available"", automatically allocates power to the PoE port after device detection (default setting).

static - Enables powered-device detection; pre-allocate (reserve) power for a port before the switch discovers the powered device; the switch reserves power for this port even when no device is connected and guarantees that power will be provided upon device detection.

"if enough power is available" means its not a guarenteed method as the question... So definetly not Auto... " the switch reserves power for this port even when no device is connected and guarantees that power" this is guarenteed method.

https://www.thinlabs.com/faq/configure-cisco-switch-for-powering-poe-client#:~:text=static%20%2D%20Enables%20powered%2Ddevice%20detection,be%20provided%20upon%20device%20detection.

upvoted 1 times

VanessaR05 3 months ago

Selected Answer: B

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011010.html#:~:text=static%E2%80%94Enables%20powered%2Ddevice%20detection,be%20provided%20upon%20device%20detection.

static—Enables powered-device detection. Pre-allocate (reserve) power for a port before the switch discovers the powered device. The switch reserves power for this port even when no device is connected and guarantees that power will be provided upon device detection.

upvoted 1 times

Danishh 3 months, 1 week ago

static—Enables powered-device detection. Pre-allocate (reserve) power for a port before the switch discovers the powered device. The switch reserves power for this port even when no device is connected and guarantees that power will be provided upon device detection.

upvoted 1 times

JJY888 3 months, 3 weeks ago

It's a bit unethical to put the term auto-detect and it is intentionally misleading. Auto mode will detect the device's power specs but cannot guarantee power. Static mode will detect the device power specs and guarantee power. Typical Cisco question. I have to go with B.

upvoted 1 times

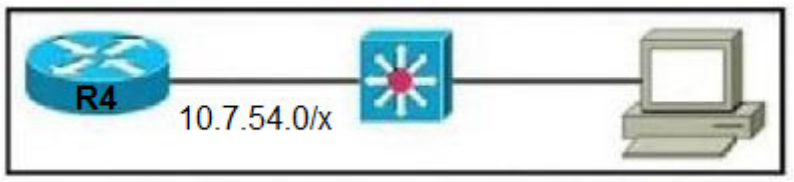
TR3Y 4 months ago

Selected Answer: B

From this cisco site itself. Please correct me if I am wrong. The definition has the same wording as the question. "Guarantees power will be available upon detection."
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011010.html

upvoted 2 times

Question #129 *Topic 1*



Refer to the exhibit. The router has been configured with a super net to accommodate the requirements for 380 users on a Subnet. The requirement already considers 30% future growth. Which configuration verifies the IP subnet on router R4?

A. Subnet: 10.7.54.0 Subnet mask: 255.255.128.0 Broadcast address: 10.5.55.255 Usable IP address range: 10.7.54.1 10.7.55.254 "€ƛ

B. Subnet: 10.7.54.0 Subnet mask: 255.255.255.0 Broadcast address: 10.7.54.255 Usable IP address range: 10.7.54.1 10.7.55.254 "€ƛ

C. Subnet: 10.7.54.0 Subnet mask: 255.255.254.0 Broadcast address: 10.7.54.255 Usable IP address range: 10.7.54.1 10.7.55.254 "€ƛ

D. Subnet: 10.7.54.0 Subnet mask: 255.255.254.0 Broadcast address: 10.7.55.255 Usable IP address range: 10.7.54.1 10.7.55.254 "€ƛ

Correct Answer: *D*

Community vote distribution

D (100%)

Customexit Highly Voted 10 months, 3 weeks ago

Questions like this can be process of elimination.
I highly recommend watching Subnetting Mastery playlist by Practical Networking on Youtube. You learn a very handy chart.

Need 380 users. A /23 works. /23 is 254. So either C or D.
Broadcast address is always odd. So D.

upvoted 10 times

Goh0503 Highly Voted 11 months, 3 weeks ago

Answer C
IP Address: 10.7.54.0
Network Address: 10.7.54.0
Usable Host IP Range: 10.7.54.1 - 10.7.55.254
Broadcast Address: 10.7.55.255
Total Number of Hosts: 512
Number of Usable Hosts: 510
Subnet Mask: 255.255.254.0
Wildcard Mask: 0.0.1.255
Binary Subnet Mask: 11111111.11111111.11111110.00000000
IP Class: B
CIDR Notation: /23

upvoted 7 times

Freddy01 10 months ago

You meant D right? Answer C has an incorrect broadcast address. You have listed the correct broadcast address 10.7.55.255, but chose option C with 10.7.54.255, which is not correct.

upvoted 4 times

MauroC19 Most Recent 4 weeks, 1 day ago

Selected Answer: D

Discarding process is key. You need at min a /23 to satisfied 380 hosts. Subnet mask in 3rd octet is then .254 (so you can discard A and B). The IP range given for C and D is the same, so you can easily detect which one is the broadcast address by adding +1 to the last usable host.
D is the final answer

upvoted 1 times

harkindeylee 6 months, 2 weeks ago

D IS CORRECT

upvoted 1 times

netzwork 11 months, 3 weeks ago

D is right.

upvoted 2 times

Goh0503 11 months, 3 weeks ago

Answer D

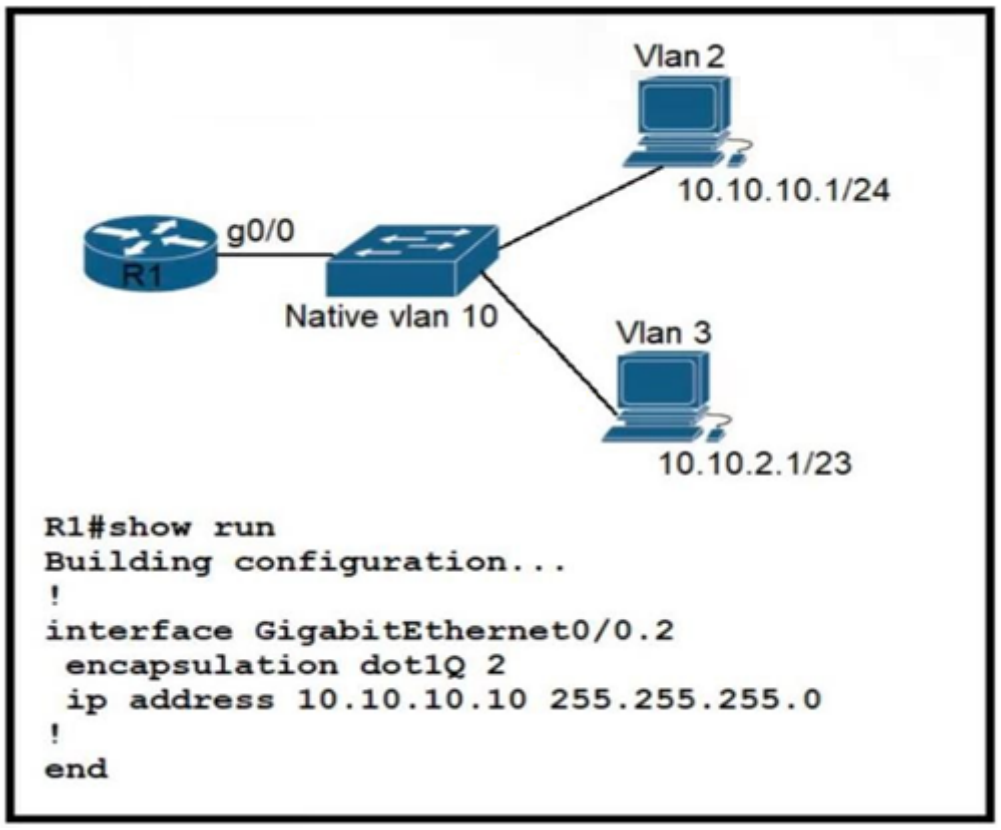
upvoted 2 times

mrgreat 1 year ago

D is correct

upvoted 1 times

Question #130 *Topic 1*



Refer to the exhibit. Configurations for the switch and PCs are complete. Which configuration must be applied so that VLANs 2 and 3 communicate back and forth?

A. interface GigabitEthernet0/0 ip address 10.10.2.10 255.255.252.0

B. interface GigabitEthernet0/0.10 encapsulation dot1Q 3 ip address 10.10.2.10 255.255.254.0

C. interface GigabitEthernet0/0.3 encapsulation dot1Q 3 native ip address 10.10.2.10 255.255.252.0

D. interface GigabitEthernet0/0.3 encapsulation dot1Q 10 ip address 10.10.2.10 255.255.255.252

Correct Answer: *B*

Community vote distribution

B (100%)

HMaw Highly Voted 11 months, 1 week ago

B is correct.
Question gave 3 hints to work on. (RoS, VLAN 3, and /23)
RoS require matching VLAN ID which is 3 and /23 = 254.
So dot1Q=3 and 255.255.254.0 = B
Hope this help

upvoted 13 times

RougePotatoe Highly Voted 10 months, 3 weeks ago

Selected Answer: B

They threw a curve ball. What you name the sub interface doesn't matter, although it is not best practice doesn't follow logic, as long as you have the correct encapsulation and ip address configured.

upvoted 11 times

Goh0503 Most Recent 1 year ago

Answer is B
R1 Subinterface Configuration (4.2.4)
The router-on-a-stick method requires you to create a subinterface for each VLAN to be routed.

A subinterface is created using the interface interface_id.subinterface_id global configuration mode command. The subinterface syntax is the physical interface followed by a period and a subinterface number. Although not required, it is customary to match the subinterface number with the VLAN number.
https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=5

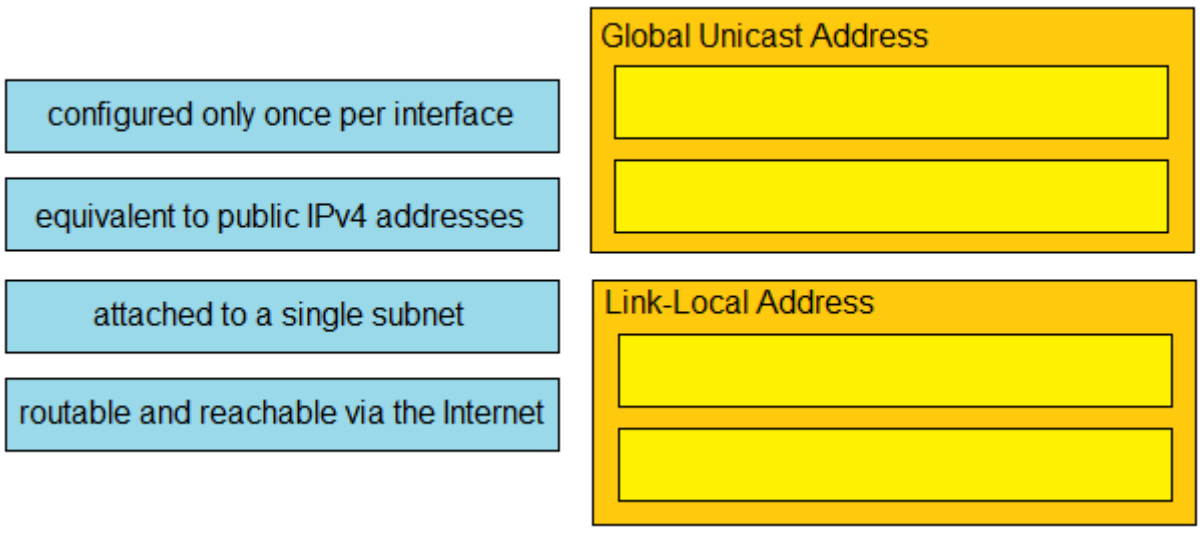
upvoted 4 times

Question #131 *Topic 1*

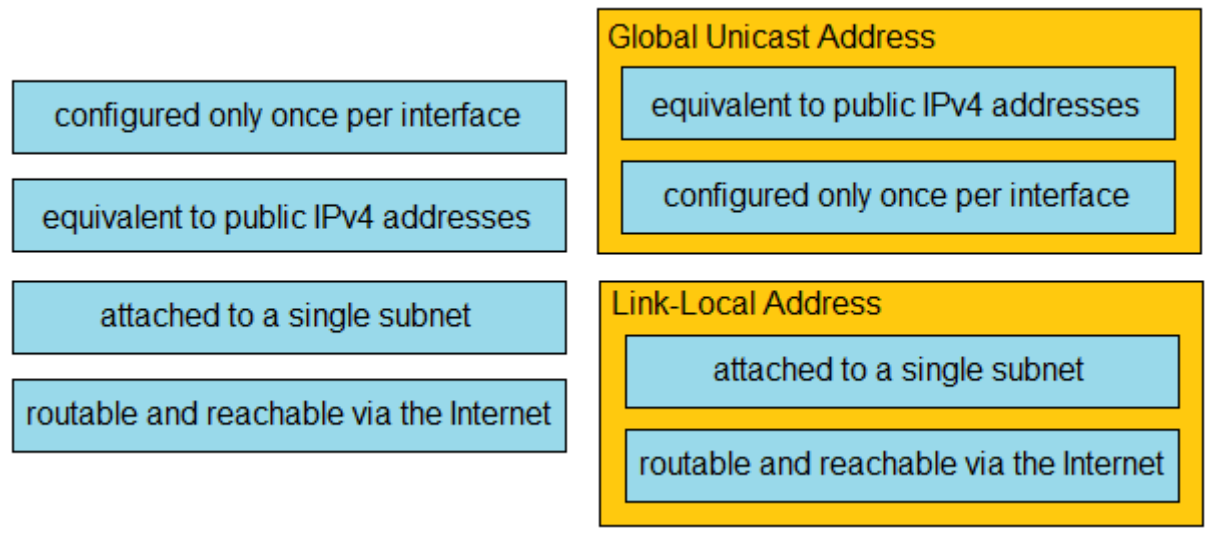
DRAG DROP -

Drag and drop the IPv6 address type characteristics from the left to the right.

Select and Place:



Correct Answer:



foreach Highly Voted 1 year ago

Wrong. Link-local addresses are not routable nor reachable via Internet. And you can have only one link-local address per interface.
So it should be :
- Global Unicast Address :
. equivalent to public IPv4 addresses
. routable and reachable via the Internet
- Link-Local Address :
. configured only once per interface
. attached to a single subnet

Source : https://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=4

upvoted 128 times

bikila123 1 month, 1 week ago

correct..

upvoted 1 times

mda2h 2 months, 3 weeks ago

Up! This answer makes more sense

upvoted 3 times

g_h_97 1 year ago

Thanks man, that was a weird mistake tbh

upvoted 12 times

GhostWolf 10 months, 1 week ago

Bro I was questioning my sanity.

upvoted 19 times

Tony5000 Highly Voted 9 months, 3 weeks ago

Wrong, it should be :
- Global Unicast Address :
. equivalent to public IPv4 addresses
. routable and reachable via the Internet
- Link-Local Address :
. configured only once per interface
. attached to a single subnet

upvoted 11 times

Danishh Most Recent 3 months, 1 week ago

The correct answer is :-
Global Unicast Address :
. equivalent to public IPv4 addresses
. routable and reachable via the Internet
- Link-Local Address :
. configured only once per interface
. attached to a single subnet

upvoted 3 times

UnbornD9 5 months, 1 week ago

WTF, who configure the correct answer for this questions? Sometimes I doubt the correctness of this site...

upvoted 3 times

jahzz 4 months ago

theyre not legally allowed to put the correct answer for every question, hence why they implement a discussion post for us users to vote on the correct answer to verify the validity of the answer

upvoted 2 times

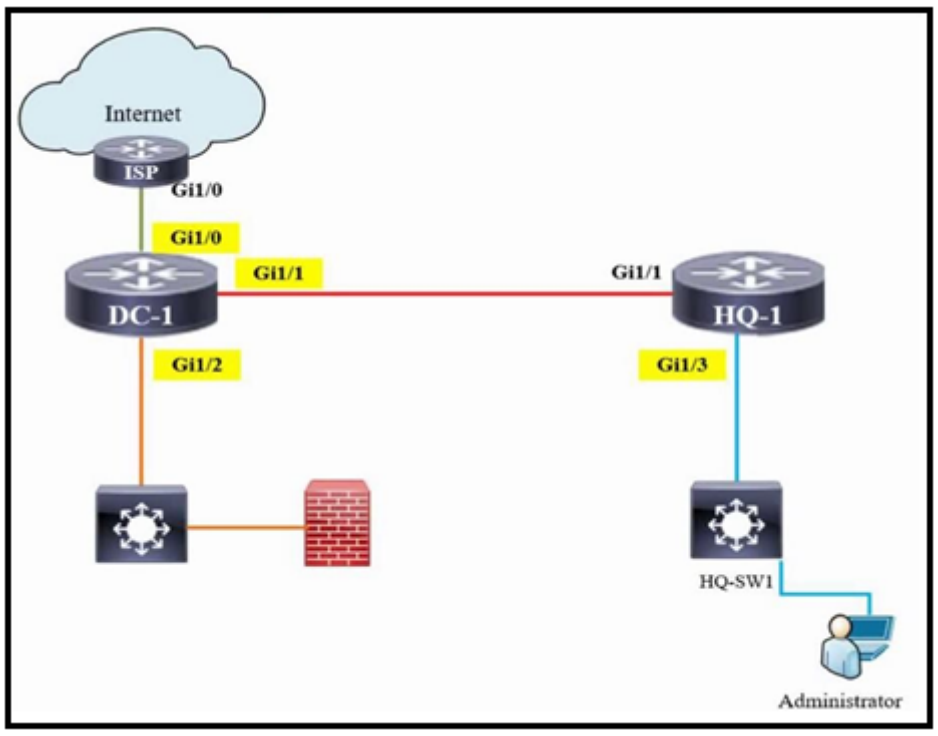
binrayelias 8 months ago

Global Unicast add
routable and reachable via internet
equivalent to public ipv4 add
Link-local add
attached to single subnet
config only once per interface

upvoted 1 times

Question #132 *Topic 1*

DRAG DROP -



Refer to the exhibit. The IP address configurations must be completed on the DC-1 and HQ-1 routers based on these requirements:

- ☞ DC-1 Gi1/0 must be the last usable address on a /30
- ☞ DC-1 Gi1/1 must be the first usable address on a /29
- ☞ DC-1 Gi1/2 must be the last usable address on a /28
- ☞ HQ-1 Gi1/3 must be the last usable address on a /29

Drag and drop the commands from the left onto the destination interfaces on the right. Not all commands are used.

Select and Place:

ip address 192.168.4.9 255.255.255.248
ip address 192.168.3.14 255.255.255.240
ip address 209.165.202.129 255.255.255.252
ip address 192.168.4.13 255.255.255.240
ip address 209.165.202.130 255.255.255.252
ip address 209.165.202.131 255.255.255.252
ip address 192.168.3.14 255.255.255.248

DC-1
Gi1/0
Gi1/1
Gi1/2

HQ-1
Gi1/3

Correct Answer:

ip address 192.168.4.9 255.255.255.248
ip address 192.168.3.14 255.255.255.240
ip address 209.165.202.129 255.255.255.252
ip address 192.168.4.13 255.255.255.240
ip address 209.165.202.130 255.255.255.252
ip address 209.165.202.131 255.255.255.252
ip address 192.168.3.14 255.255.255.248

DC-1
ip address 209.165.202.130 255.255.255.252
ip address 192.168.4.9 255.255.255.248
ip address 192.168.3.14 255.255.255.240

HQ-1
ip address 192.168.3.14 255.255.255.248

Customexit Highly Voted 10 months, 3 weeks ago

Broadcast: odd
Network: even
1st usable: odd
last usable: even

upvoted 22 times

HippoMonarch 1 week, 2 days ago

Really appreciate!!! It's really a magic method.

upvoted 1 times

jamesgavin 5 months ago

This is the best answer here.
This way you can resolve the question very fast without doing all the math, and save time.
upvoted 3 times

NICE_ANSWERS 3 months, 3 weeks ago
Please, what's the significance of this coded info
upvoted 1 times

picho707 Most Recent 4 weeks ago
I think the question should have read => HQ-1 Gi1/1 must be the last usable address on a /29 instead of HQ-1 Gi1/3. There are options from the selections to make the two switches non-overlapping.
upvoted 1 times

picho707 4 weeks ago
I meant to say:
I think the question should have read => HQ-1 Gi1/1 must be the last usable address on a /29 instead of HQ-1 Gi1/3. There are "NO" options from the selections to make the two switches non-overlapping.
upvoted 1 times

MelbourneJin 2 months, 3 weeks ago
G1/2 and G1/3 have the same IP address. Is that okay???
upvoted 2 times

Request7108 8 months, 4 weeks ago
If this question appears on the exam, I will likely skip it because of the time required to do the math. If possible, I would save it to the end to attempt only if I have extra time.
upvoted 3 times

UnbornD9 5 months, 1 week ago
It's something I'm trying to understand: you CAN skip it and review it in a second time? Someone know the answer?
upvoted 1 times

beerbisceps1 5 months, 1 week ago
I think once you skip and click next you can't go back
upvoted 2 times

GigaGremlin 11 months, 1 week ago
Sorry, for the confusion,...
just figured out, that I had a little miscalculation with the /30 .252
Network Address is 209.165.202.128 so 130 will be fine.
But I guess that's intended to be...
upvoted 1 times

GigaGremlin 11 months, 1 week ago
IMHO someone should correct the 1st Questinon from
"DC-1 Gi1/0 must be the last usable address on a /30"
to this Q & A
"DC-1 Gi1/0 must be the first usable address on a /30"
then you can choose IP-Address 209.165.202.131 255.255.255.252,
otherwise it simply doesn't make sense to me...
upvoted 2 times

F103 11 months, 3 weeks ago
Key word is "last usable address/ first usable addrss", check all possible subnet addresses then find if that is the last or first.
upvoted 1 times

DUMPledore 11 months, 3 weeks ago
can someone help to explain how the answers were get? I'm confused.
upvoted 1 times

netzwork 11 months, 3 weeks ago
/30 means the subnet will be .252 hosts will go in groups of 4
/29 means subnet will be .248 hosts will go in groups of 8
/28 means subnet will be .240 hosts will go in groups of 16

Now if you need to see how to get first host, last host and broadcast addresses, I recommend you study that separately.

To practice those exercises, go here:
https://www.subnetting.net/Subnetting.aspx?mode=practice
upvoted 2 times

Question #133 *Topic 1*

How is RFC 1918 addressing used in a network?

A. They are used to access the Internet from the internal network without conversion.

B. They are used in place of public addresses for Increased security.

C. They are used with NAT to preserve public IPv4 addresses.

D. They are used by Internet Service Providers to route over the Internet.

Correct Answer: *C*

Community vote distribution

C (100%)

mrgreat Highly Voted 1 year ago

C is correct
https://www.techtarget.com/whatis/definition/RFC-1918#:~:text=Along%20with%20NAT%20(network%20address,before%20the%20adoption%20of%20IPV6.

upvoted 6 times

RougePotatoe Most Recent 10 months, 3 weeks ago

Selected Answer: C

"This document describes address allocation for private internets. The allocation permits full network layer connectivity among all hosts inside an enterprise as well as among all public hosts of different enterprises. The cost of using private internet address space is the potentially costly effort to renumber hosts and networks between public and private."

https://datatracker.ietf.org/doc/html/rfc1918

upvoted 1 times

everchosen13 11 months, 3 weeks ago

I think its actually B the RFC 1918 was published in 1996. RFC 2663 (NAT) was published in 1999. It is not clear in the RFC 1918 that it was developed with NAT in mind

upvoted 2 times

RougePotatoe 10 months, 3 weeks ago

Comment makes no sense it literally says it in the introduction.

"This document describes address allocation for private internets. The allocation permits full network layer connectivity among all hosts inside an enterprise as well as among all public hosts of different enterprises. The cost of using private internet address space is the potentially costly effort to renumber hosts and networks between public and private."

https://datatracker.ietf.org/doc/html/rfc1918

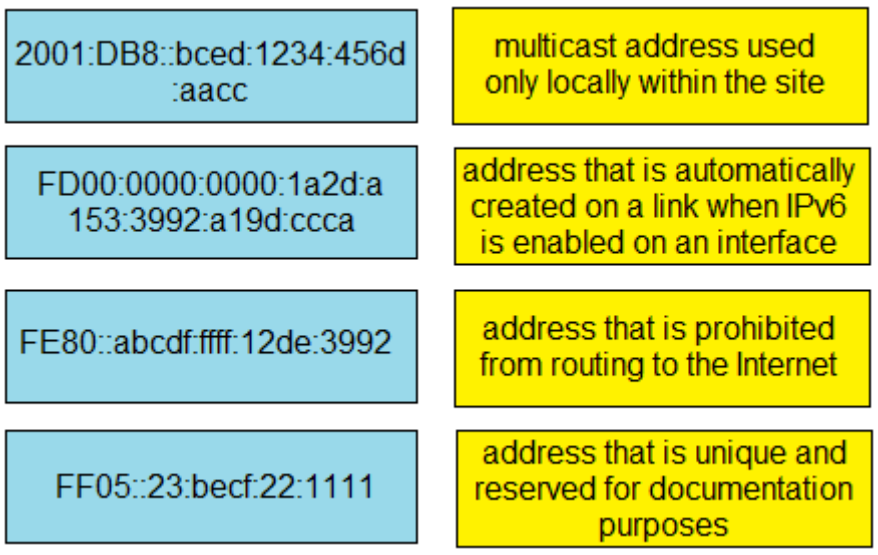
upvoted 2 times

Question #134 *Topic 1*

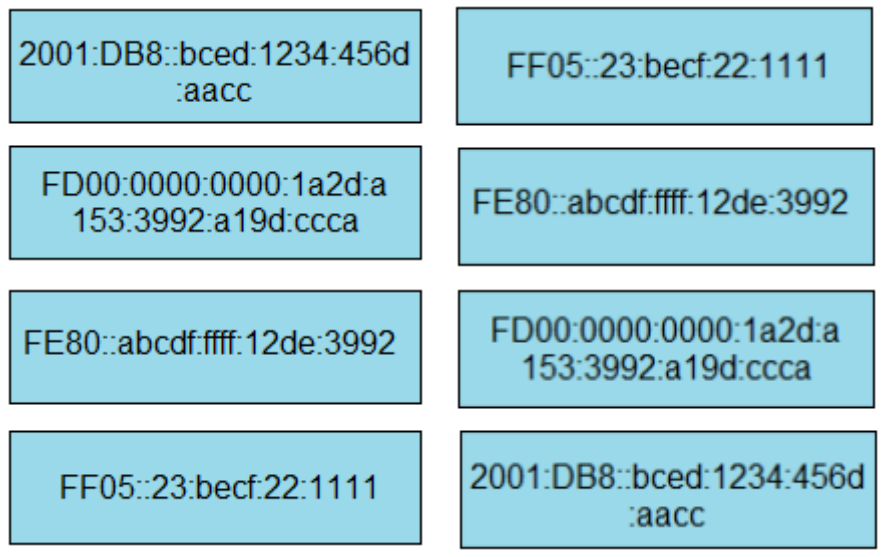
DRAG DROP -

Drag and drop the IPv6 address types from the left onto their descriptions on the right.

Select and Place:



Correct Answer:



Dutch012 Highly Voted 7 months ago

"prohibited"..... Cisco, please use simpler words in your questions, not all of us are born in the US.

upvoted 20 times

Junior_Network 16 hours, 59 minutes ago

you are extremly right

upvoted 1 times

sol_ls95 Highly Voted 7 months, 4 weeks ago

FF: MULTICAST

FD: UNIQUE LOCAL

FE: LINK LOCAL

2001: GLOBAL UNIQUE

upvoted 10 times

xbololi Most Recent 2 months, 3 weeks ago

reserved for documentation???? they really try to confuse people...

upvoted 1 times

Dunedrifter 2 months, 2 weeks ago

yup. 2001:0DB8::/32 is reserved to be used in tutorials and examples..

upvoted 1 times

[Removed] 3 months, 1 week ago

2001:db8 can't be used? I'm lost now...the more i study the more i get confused. I'm really about to give up

upvoted 2 times

iMo7ed 7 months, 1 week ago

2001:DB8 = Address that is unique and reserved for documentation purposes

FD00 = Address that is prohibited from routing to the Internet

FE80 = Address that is automatically created on a link when IPv6 is enabled on an Interface

FF05 = Multicast address used only locally within the site
upvoted 8 times

binrayelias 8 months ago
The soln is correct:
multicast site-local is ff05::.

fe80:: is unicast link local that is automatically generated on ipv6-enabled int

fc00:: is unique local and can't be routed over internet. Similar to ipv4 rfc 1918 private address.

2001:: is global unicast reserved prefix for use in documentation.
https://www.rfc-editor.org/rfc/rfc3849.txt
upvoted 3 times

binrayelias 8 months ago
https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113328-ipv6-lla.html. reference for fe80::
upvoted 1 times

Choquete 9 months ago
Then the solution is wrong?
upvoted 1 times

sol_ls95 7 months, 4 weeks ago
the solution is correct
upvoted 1 times

Robertlars 9 months, 1 week ago
- 2001 = multicast address used only locally within the site

- FD00 = address that is automatically created on a link when IPv6 is enabled on an interface

- FE80 = address that is prohibited from routing to the Internet

- FF05 = address that is unique and reserved for documentation purposes
upvoted 2 times

freeknowledge123 8 months, 2 weeks ago
FF05: is a multicast address used only for local scopehttps://learningnetwork.cisco.com/s/question/0D53i00000Z9uywCAB/what-about-address-of-ff052
upvoted 3 times

sol_ls95 7 months, 4 weeks ago
2001 its not multicast
upvoted 2 times

```
Router# show interface gi0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
   Hardware is ISR4331-3x1GE, address is 5486.bc25.1f70 (bia 5486.bc25.1f70)
   Description: << WAN Link >>
   Internet address is 192.0.2.2/30
   MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive not supported
   Full Duplex, 1000Mbps, link type is auto, media type is RJ45
   output flow-control is off, input flow-control is off
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input 00:00:00, output 00:00:11, output hang never
   Last clearing of "show interface" counters never
   Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
   Queueing strategy: fifo
   Output queue: 0/40 (size/max)
   5 minute input rate 7000 bits/sec, 4 packets/sec
   5 minute output rate 4000 bits/sec, 4 packets/sec
      22579370 packets input, 8825545968 bytes, 0 no buffer
      Received 67 broadcasts (0 IP multicasts)
      0 runts, 0 giants, 0 throttles
      3612699 input errors, 3612699 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 10747057 multicast, 0 pause input
      12072167 packets output, 1697953637 bytes, 0 underruns
      0 output errors, 0 collisions, 1 interface resets
      6 unknown protocol drops
      0 babbles, 0 late collision, 0 deferred
      5 lost carrier, 0 no carrier, 0 pause output
      0 output buffer failures, 0 output buffers swapped out
```

Refer to the exhibit. What is a reason for poor performance on the network interface?

A. The interface is receiving excessive broadcast traffic.

B. The bandwidth setting of the interface is misconfigured.

C. The cable connection between the two devices is faulty.

D. The interface is operating at a different speed than the connected device.

Correct Answer: *C*

Here we see a large number of input errors and CRC errors.

Media Problem	Suggested Actions
Excessive noise	**1.** Use the **show interfaces ethernet** exec command to determine the status of the router's Ethernet interfaces. The presence of many CRC errors but not many collisions is an indication of excessive noise. **2.** Check cables to determine whether any are damaged. **3.** Look for badly spaced taps causing reflections. **4.** If you are using 100BaseTX, make sure you are using Category 5 cabling and not another type, such as Category 3.

Community vote distribution

C (100%)

Robertlars Highly Voted 9 months ago

What does lost carrier mean Cisco?

The "lost carrier" is when we do sense "something" coming towards the local receiver, but we cannot see our own data looped back on the medium. This is also detected by the local receiver and probably indicates a problem in the transmit direction of the cable or the loopback circuitry at the remote side.

Since we have 5 lost carriers as shown on the show interface command, this is indicative of a bad cable.
Ref: https://community.cisco.com/t5/switching/the-difference-between-quot-lost-carrier-quot-and-quot-no/td-p/1242625

upvoted 6 times

Yunus_Empire Most Recent 9 months, 2 weeks ago

Selected Answer: C

Given Answer is Correct...

upvoted 1 times

NICE_ANSWERS 3 months, 3 weeks ago

From the output, how do you know the cable connection is faulty?

upvoted 3 times

xbololi 2 months, 2 weeks ago

As far i know if the CRC counter is that high there is a highly chance of physical issue in that connection... Either cable or the socket has a problem.

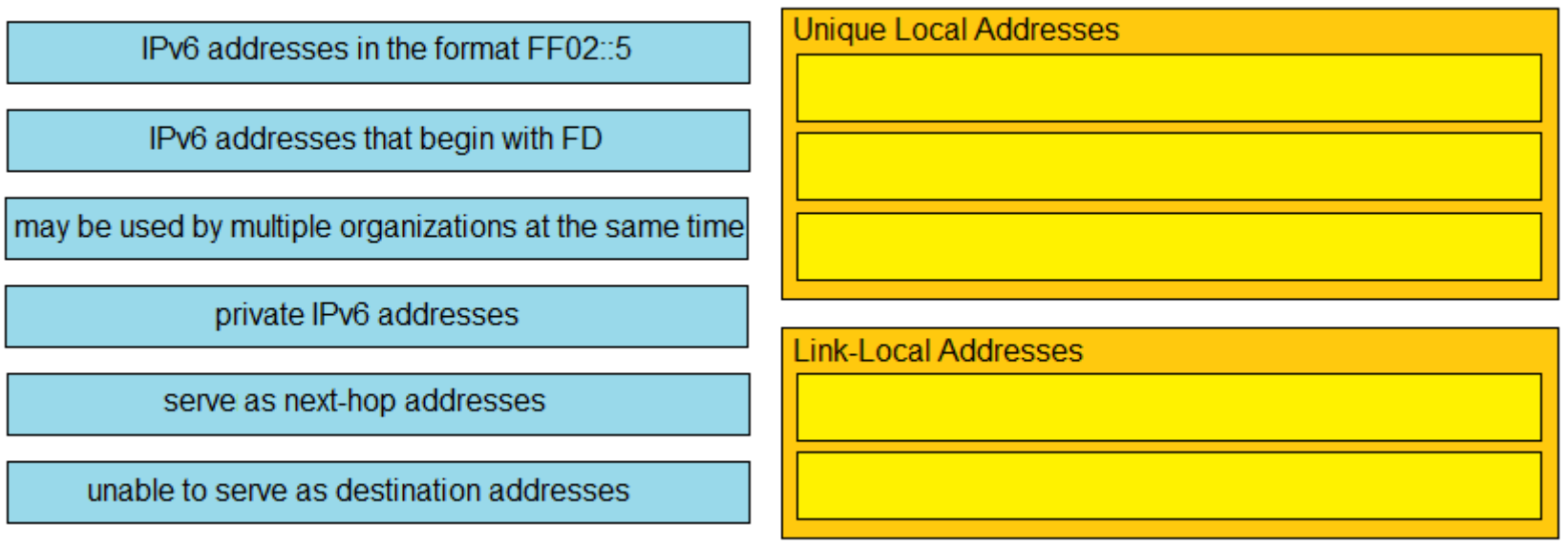
upvoted 2 times

Question #136 *Topic 1*

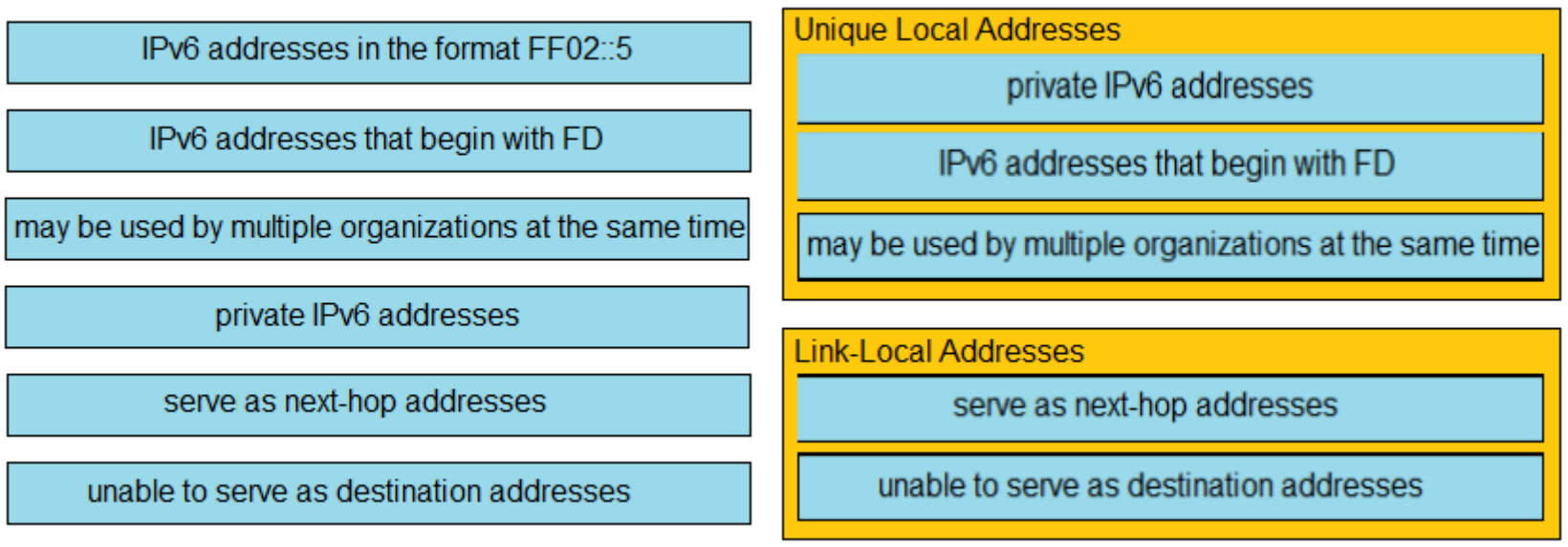
DRAG DROP -

Drag and drop the IPv6 address descriptions from the left onto the IPv6 address types on the right. Not all options are used.

Select and Place:



Correct Answer:



HippoMonarch 5 days, 9 hours ago

●Unique Local Addresses：
IPv6 addresses that begin with FD,
may be used by multiple organizations at the same time,
private IPv6 addresses

●Link-Local Addresses：
serve as next-hop addresses,
IPv6 addresses in the format FF02::5,

"FF02::5 is used for all Designated Routers (DRs) within the OSPF (Open Shortest Path First) protocol. In OSPF networks, this multicast address is used for specific link-local communication."

"Link-Local Addresses can serve as destination addresses for communication between nodes within the same subnet, but they cannot serve as destination addresses across different subnets."

upvoted 1 times

no_blink404 2 months, 3 weeks ago

Not a good question.

upvoted 1 times

manaoming 3 months ago

Why link-local address cannot be used as destination? Within the local link they can be used...

upvoted 3 times

lamm 2 months ago

Because is not routable, so when you said destination it happens to be in the same network space, so that communication occurrs in layer 2 rather than layer 3, so it was not destine to an IP.

upvoted 2 times

bikila123 1 month, 1 week ago

it can be routable with in subnet!

upvoted 1 times

Mikeabo 7 months, 1 week ago

Also FF is a multicast not a Unicast which encompasses global, unique local, Link Local

upvoted 2 times

Mikeabo 7 months, 1 week ago

ff02::5 all OSPF (Open Shortest Path First) routers ... https://www.menandmice.com/blog/ipv6-reference-multicast, I guess thats the reason

upvoted 3 times

lololss 8 months, 1 week ago

Why not IPv6 addresses in the format FF02::5?
FF02::5 I know it's a link-local scope.

upvoted 1 times

freeknowledge123 8 months ago

ff02 is a multicast address, check the documentation

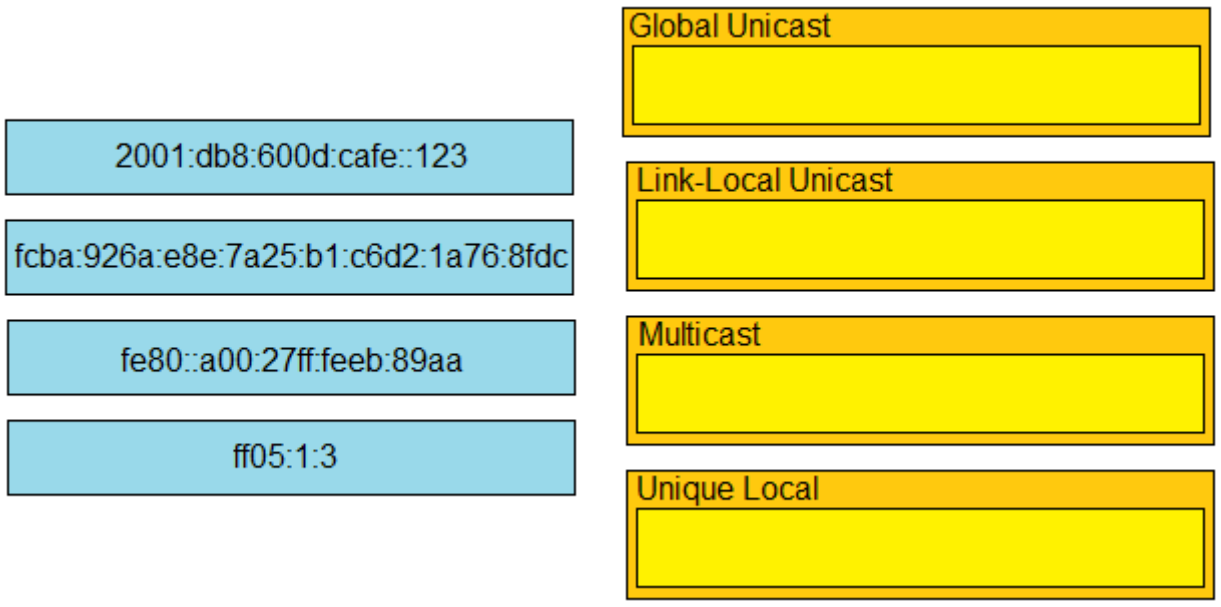
upvoted 5 times

Question #137 *Topic 1*

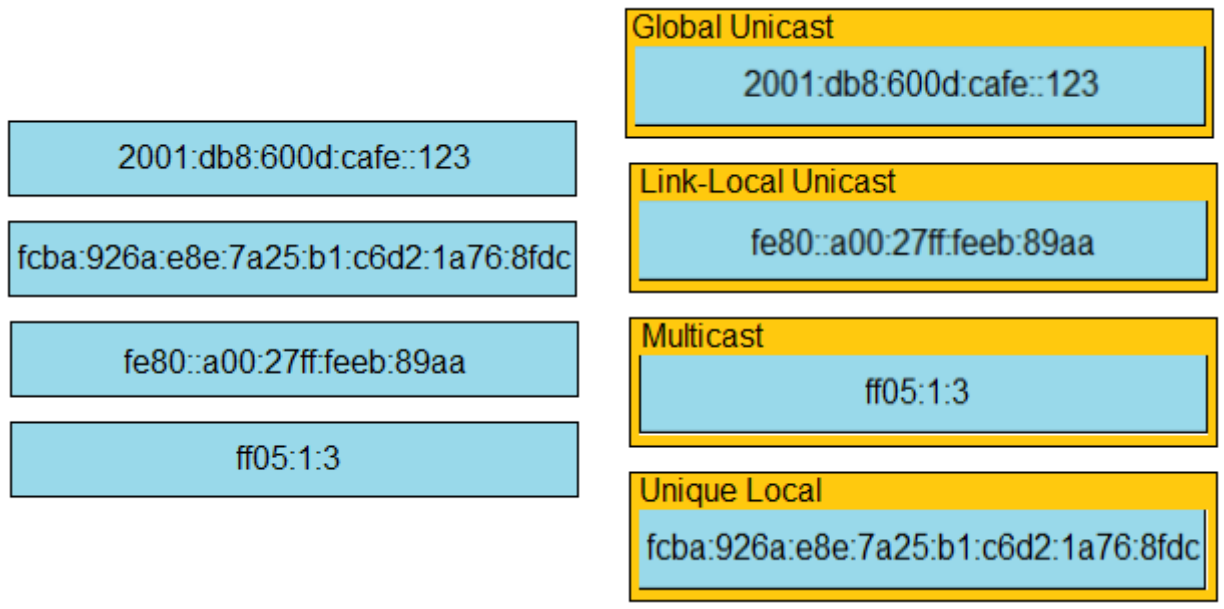
DRAG DROP -

Drag and drop the IPv6 addresses from the left onto the corresponding address types on the right.

Select and Place:



Correct Answer:



arjune Highly Voted 5 months, 1 week ago

All answers are correct

upvoted 11 times

juneq888 Most Recent 1 week, 3 days ago

This is the only answer I am 100% sure of

upvoted 2 times

Question #138 *Topic 1*

Which WAN topology has the highest degree of reliability?

A. point-to-point

B. router-on-a-stick

C. full mesh

D. hub-and-spoke

Correct Answer: *C*

Community vote distribution

C (100%)

lamm 2 months ago

Selected Answer: C

better answer

upvoted 1 times

Destructo 6 months, 1 week ago

Reliabilty = Redundancy, Full Mesh is the only option that gives you that.

upvoted 3 times

harkindeylee 6 months, 2 weeks ago

Full mesh obviously

upvoted 1 times

Robertlars 9 months ago

https://ipcisco.com/wan-topology-types/ (yes, full mesh is the correct answer)

upvoted 2 times

mrgreat 1 year ago

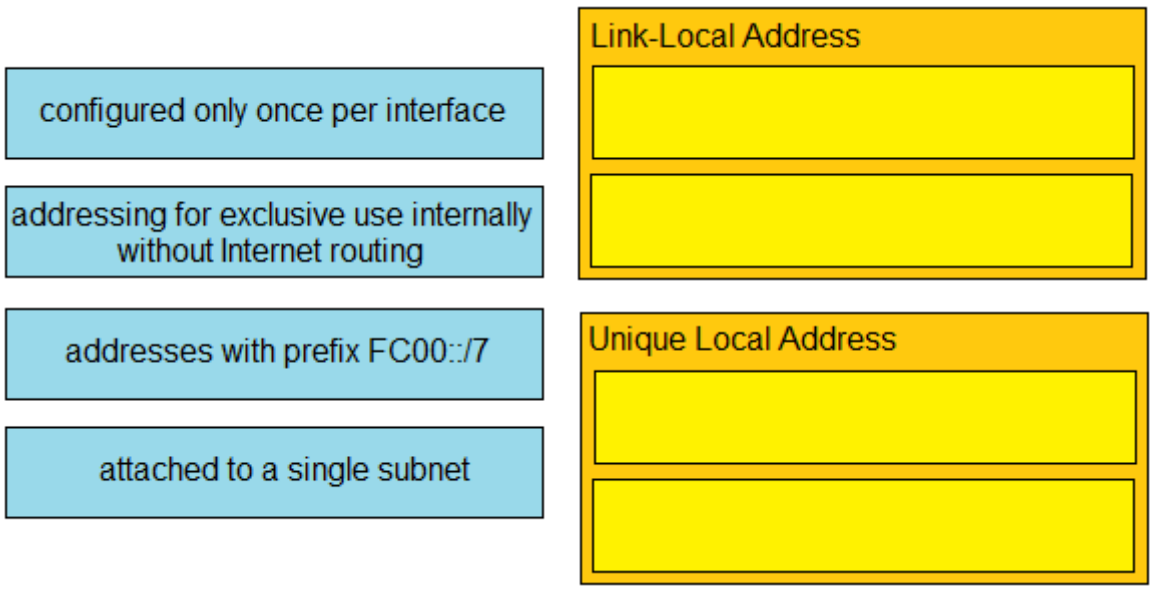
C is correct
https://www.sciencedirect.com/topics/computer-science/mesh-topology

upvoted 3 times

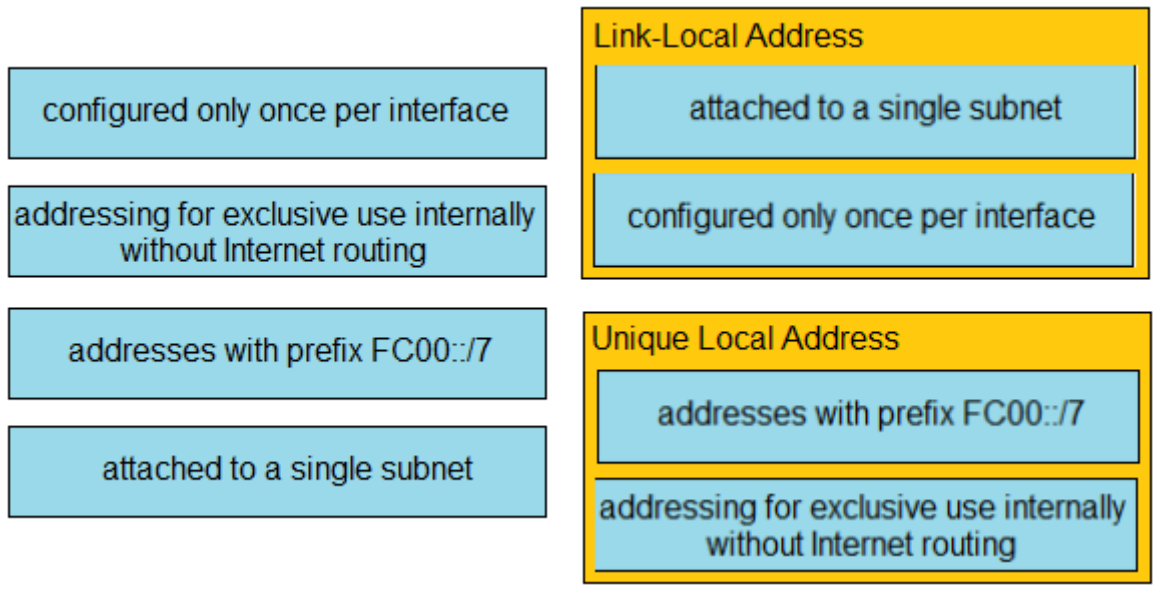
DRAG DROP -

Drag and drop the IPv6 address type characteristics from the left to the right.

Select and Place:



Correct Answer:



dropspablo 1 month, 3 weeks ago

Correct answers. In IPv4 you can configure only one address per interface, in IPv6 more than one is possible (Tested in Packet Tracer).

upvoted 1 times

no_blink404 3 months ago

Wrong. I think the answer should be:

Link Local Address:
- Attached to a single subnet
- Addressing for exclusive use internally without internet routing

Unique Local Address:
-Addresses with prefix FC00:/7
-Configured only once per interface

upvoted 3 times

everchosen13 11 months, 3 weeks ago

Link-local addresses are not routable on the internet. Answer given is incorrect

upvoted 4 times

BieLey 11 months, 3 weeks ago

There is no answer about routing to the internet. Given answers are correct.

upvoted 14 times

Webfat 7 months, 3 weeks ago

I think what he means is that both address is not routable on the internet

upvoted 3 times

Question #140 *Topic 1*

What causes a port to be placed in the err-disabled state?

A. nothing plugged into the port

B. link flapping

C. latency

D. shutdown command issued on the port

Correct Answer: *B*

Community vote distribution

B (100%)

RougePotatoe Highly Voted 10 months, 3 weeks ago

Selected Answer: B

There are various reasons for the interface to go into errdisable. The reason can be:

Duplex mismatch
Port channel misconfiguration
BPDU guard violation
UniDirectional Link Detection (UDLD) condition
Late-collision detection
Link-flap detection
Security violation
Port Aggregation Protocol (PAgP) flap
Layer 2 Tunneling Protocol (L2TP) guard
DHCP snooping rate-limit
Incorrect GBIC / Small Form-Factor Pluggable (SFP) module or cable
Address Resolution Protocol (ARP) inspection

https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html#anc8

upvoted 20 times

Hanagaki_Shinjiro 5 days, 21 hours ago

Thank you so much bro

upvoted 1 times

Vlad_Is_Love_ua Highly Voted 1 year ago

The Errdisable error disable feature was designed to inform the administrator when there is a port problem or error. The reasons a catalyst switch can go into Errdisable mode and shutdown a port are many and include:

Duplex Mismatch

Loopback Error

Link Flapping (up/down)
Port Security Violation
Unicast Flodding
UDLD Failure
Broadcast Storms
BPDU Guard

upvoted 6 times

Vlad_Is_Love_ua Most Recent 1 year ago

Selected Answer: B

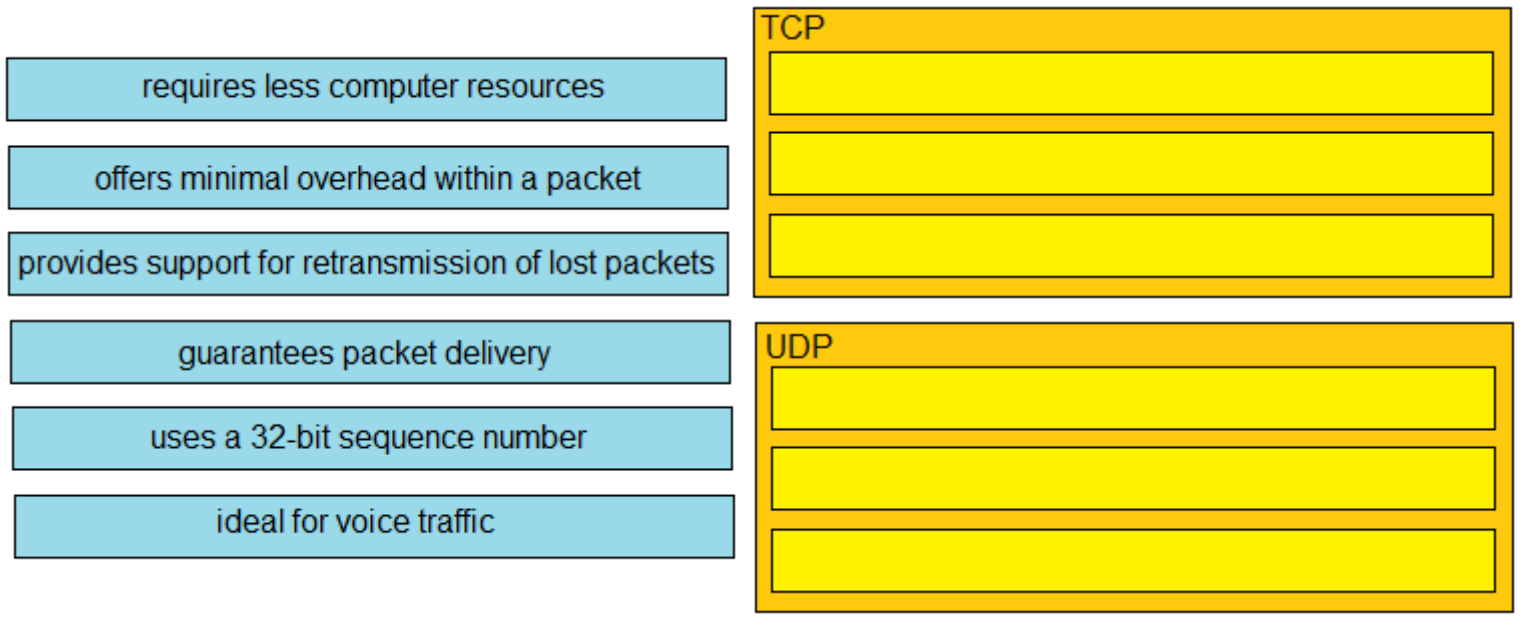
https://learningnetwork.cisco.com/s/question/0D53i00000Kt17xCAB/error-disable-port-state

upvoted 1 times

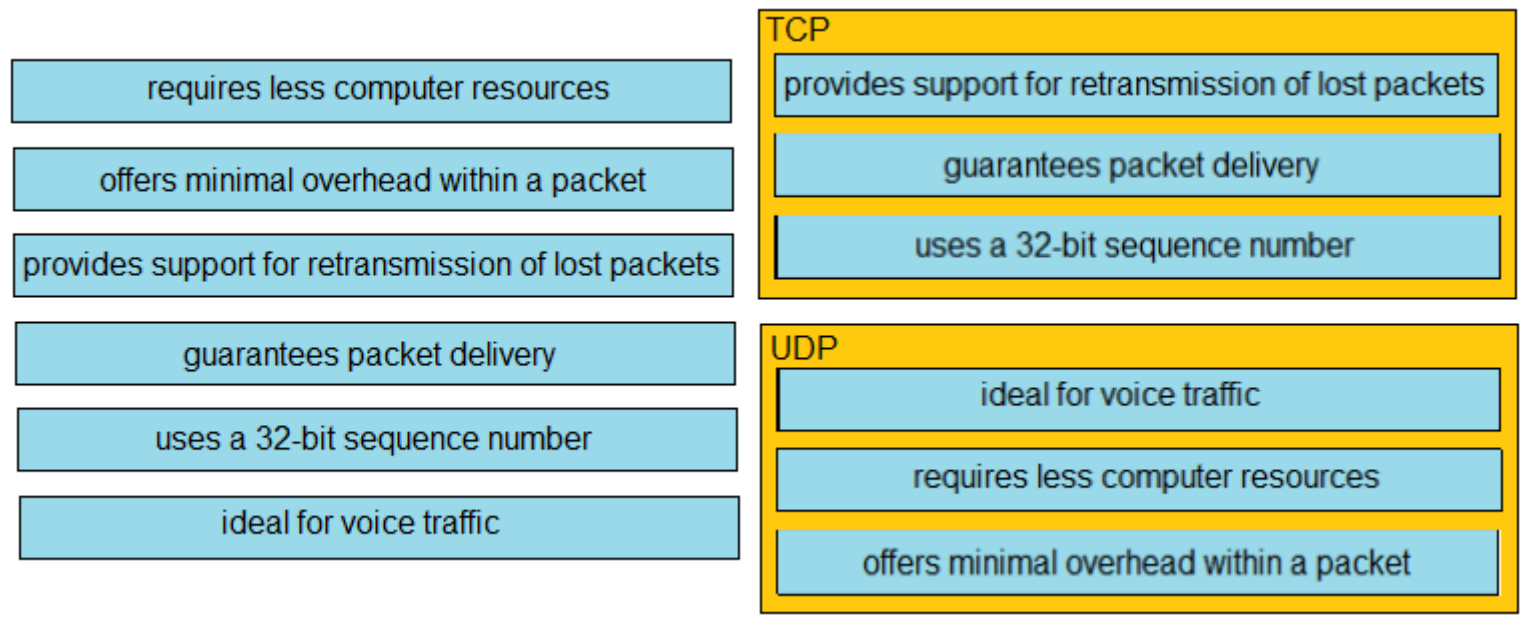
DRAG DROP -

Drag and drop the characteristics of transport layer protocols from the left onto the corresponding protocols on the right.

Select and Place:



Correct Answer:



Fermento Highly Voted 11 months, 1 week ago

This solution is right

upvoted 9 times

Junior_Network Most Recent 16 hours, 39 minutes ago

correct

upvoted 1 times

Question #142 *Topic 1*

A network engineer must configure an interface with IP address 10.10.10.145 and a subnet mask equivalent to 11111111.11111111.11111111.11111000. Which subnet mask must the engineer use?

A. /29

B. /30

C. /27

D. /28

Correct Answer: *A*

Community vote distribution

A (94%) 6%

Dutch012 Highly Voted 7 months ago

I hope hundreds of questions like this in my next week exam

upvoted 11 times

harkindeylee 6 months, 2 weeks ago

ikr the joy of bonus mark

upvoted 4 times

Fermento Highly Voted 11 months, 1 week ago

Selected Answer: A

Correct

upvoted 8 times

Da_Costa Most Recent 3 months, 3 weeks ago

/29 just calculate or add the number of bits

upvoted 1 times

Jorro99404 4 months ago

Selected Answer: A

A. /29

upvoted 1 times

Bhrino 4 months, 1 week ago

Selected Answer: A

If it's not obvious enough just count the ones in the last octed

upvoted 1 times

StingVN 4 months, 2 weeks ago

Selected Answer: A

This is free point from Cisco i guess.
A

upvoted 2 times

deluxeccna 5 months ago

Selected Answer: A

A is correct

upvoted 2 times

Jack67 5 months, 3 weeks ago

Selected Answer: A

A ist correct

upvoted 2 times

musi0 7 months ago

Selected Answer: C

Correct

upvoted 1 times

Isuzu 4 months, 2 weeks ago

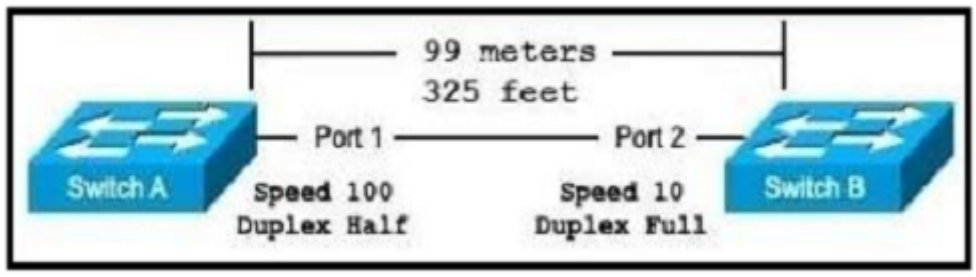
The subnet mask equivalent to 11111111.11111111.11111111.11111000 in dotted decimal notation is 255.255.255.248.

To determine the appropriate subnet mask for the given IP address and subnet mask, we need to identify the number of bits in the network portion of the address.

In this case, the first 29 bits of the IP address are used for the network portion, and the remaining 3 bits are used for the host portion. Therefore, the correct subnet mask is /29.

upvoted 2 times

Question #143 *Topic 1*



Refer to the exhibit. The switches are connected via a Cat5 Ethernet cable that is tested successfully. The interfaces are configured as access ports and are both in a down status. What is the cause of the issue?

A. The speed settings on the switches are mismatched

B. The distance between the two switches is not supported by Cat5

C. The switches are configured with incompatible duplex settings

D. The portfast command is missing from the configuration

Correct Answer: *A*

Community vote distribution

A (88%) 13%

zohar7471 Highly Voted 1 year ago

In speed mismatch, the link simply won't come up. In contrast to this, in duplex mismatch, the link will come up, but with poor performance.

upvoted 33 times

RougePotatoe 10 months, 2 weeks ago

I've seen this claim from cisco as well but when I change one side to full and the other side to half the link doesn't come up either. Does anyone know why?

upvoted 6 times

christian321 1 week, 6 days ago

Did you try that with real iOS devices or within a simulator such as Packet Tracer? The latter sometimes behaves different from real world usage.

upvoted 1 times

guynetwork Highly Voted 1 year ago

Selected Answer: A

It is A

upvoted 7 times

Junior_Network Most Recent 16 hours, 32 minutes ago

down down = No cable; bad cable; wrong cable pinouts; speed mismatch; neighboring device is (a) powered off,
(b) shutdown, or (c) error disabled.

upvoted 1 times

Hanagaki_Shinjiro 5 days, 21 hours ago

Selected Answer: C

How about C ?

upvoted 1 times

kyleptt 1 week, 2 days ago

Speed mismatch will cause them to go down.

upvoted 1 times

Question #144 *Topic 1*

Which two IP addressing schemes provide internet access to users on the network while preserving the public IPv4 address space? (Choose two.)

A. IPv6 addressing

B. PAT with private internal addressing

C. single public Class A network

D. private networks only

E. custom addresses from ARIN

Correct Answer: *AB*

PAT with private internal addressing is the usual method of allowing Internet access while preserving IPv4 addresses. Another alternative is using IPV6, which will allow internet access without using any IPv4 addresses. The other answer choices will consume a great deal of public IPV4 addresses, or will not allow for internet access.

Community vote distribution

AB (61%) BE (35%) 4%

Rether16 Highly Voted 5 months, 2 weeks ago

Selected Answer: AB

What better way than reserving IPv4 address space than not use it at all by using IPv6. I think its A & B.

upvoted 11 times

kenCapt Highly Voted 10 months, 3 weeks ago

Port Address Translation (PAT) is an extension of Network Address Translation (NAT) that permits multiple devices on a LAN to be mapped to a single public IP address to conserve IP addresses.

upvoted 11 times

Junior_Network Most Recent 16 hours, 23 minutes ago

This is from official book :
The Internet community worked hard during the 1990s to solve this problem, coming up with several solutions, including the following:
■ A new version of IP (IPv6), with much larger addresses (128 bit)
■ Assigning a subset of a public IP network to each company, instead of an entire public IP network, to reduce waste, using a feature called “Classless Interdomain Routing” (CIDR)
■ Network Address Translation (NAT), which allows the use of private IP networks

So A, B and E are correct. I think the question is wrong.

upvoted 1 times

Shanku97 3 weeks, 6 days ago

SO guys what would be the correct answer for the exam ??

upvoted 1 times

Nvthekid 1 month, 1 week ago

Selected Answer: AB

I would say AB

upvoted 1 times

Da_Costa 1 month, 2 weeks ago

Selected Answer: AC

I would go for A and C

upvoted 1 times

Natalie89 1 month, 4 weeks ago

Selected Answer: BE

BE are correct

upvoted 1 times

mda2h 2 months, 3 weeks ago

Selected Answer: AB

E) custom ARIN addresses are not Public IP addresses (or are they?), so this answer is still viable

upvoted 1 times

Da_Costa 3 months ago

BC are the best options

upvoted 3 times

hayo 3 months, 1 week ago

Selected Answer: AB

I'm going for A+B

Pure IPV6 doesn't use v4 address

PAT is an extension of NAT, so that with private addresses conserve IPv4

E would be an acceptable answer if it was paired with PAT/NAT , but it does not specify like it does in B. This means that they will not be able to access the interne, and that was a part of the question.

upvoted 1 times

Isuzu 4 months, 2 weeks ago

Selected Answer: BE

The two IP addressing schemes that provide internet access to users on the network while preserving the public IPv4 address space are:

B. PAT with private internal addressing: This approach uses Network Address Translation (NAT) to translate the private internal IP addresses of devices on the network to a single public IP address when accessing the Internet. This allows many devices to share a single public IP address, preserving the public IPv4 address space.

E. Custom addresses from ARIN: Organizations can request their own unique address space from the American Registry for Internet Numbers (ARIN) to use on their internal networks. This address space can be used in combination with NAT to provide Internet access to users on the network while preserving public IPv4 address space.

Therefore, the correct answers are B. PAT with private internal addressing and E. Custom addresses from ARIN.

upvoted 2 times

dearc 5 months, 2 weeks ago

Selected Answer: BE

The correct answers to the given question are B and E. PAT (Port Address Translation) with private internal addressing and custom addresses from ARIN (American Registry for Internet Numbers) are two IP addressing schemes that provide internet access to users on the network while preserving the public IPv4 address space . PAT allows multiple devices on a private network to share a single public IP address, while custom IP addresses can be assigned to private networks by ARIN to reduce the use of public IPv4 addresses. Therefore, the correct options are B and E.

upvoted 5 times

NICE_ANSWERS 3 months, 3 weeks ago

But what happens to IPv6 adressing then? Can you please help explain that also for me?

upvoted 1 times

Question #145 *Topic 1*

The address block 192.168.32.0/24 must be subnetted into smaller networks. The engineer must meet these requirements:

☞ Create 8 new subnets.

☞ Each subnet must accommodate 30 hosts.

☞ Interface VLAN 10 must use the last usable IP in the first new subnet.

☞ A Layer 3 interface is used.

Which configuration must be applied to the interface?

A. no switchport mode trunk ip address 192.168.32.97 255.255.255.224

B. switchport ip address 192.168.32.65 255.255.255.240

C. no switchport ip address 192.168.32.30 255.255.255.224

D. no switchport mode access ip address 192.168.32.62 255.255.255.240

Correct Answer: *C*

Community vote distribution

C (100%)

HMaw Highly Voted 11 months, 1 week ago

C is correct. Requirement is 8 networks with 30 hosts
255.255.255.0 = 11111111.11111111.11111111.00000000
8 networks = 1111 with increment of 16 which is less host number than require.
30 hosts = 11100000 with increment of 32
255.255.255.224 or 11111111.11111111.11111111.11100000
8 networks for /27 are 0,32,64,96,128,160,192,224
upvoted 10 times

SVN05 7 months, 2 weeks ago

Could someone please explain to us what does these 2 lines mean. Thank you.

8 networks = 1111 with increment of 16 which is less host number than require.
30 hosts = 11100000 with increment of 32
upvoted 2 times

raul_kapone Most Recent 1 month, 1 week ago

192.168.32.0/24
#s = 3 -> 2'3 = 8 subnets
#h = 5 -> 2'5 - 2 = 30 host/subnet

Subnets:
192.168.32.0/27
192.168.32.32/27
192.168.32.64/27
192.168.32.96/27

1st Subnet - Last useable IP address:
192.168.32.30/27
192.168.32.30 255.255.255.224

So, the answer is "C".
upvoted 1 times

rubzal 3 months, 3 weeks ago

What does layer 3 interface used means in this question?
upvoted 1 times

studying_1 3 months, 2 weeks ago

it means it is multilayer switch, need to write the subinterface command "no switchport" in order to be able to configure an IP address
upvoted 3 times

Bhrino 4 months, 1 week ago

The question ask for a sub that can hold 30 host meaning you would need a /27 which equals .224.
The question also said that this must use the last available ip in the first subnet. Because this is a /27 the subnet will be in increments on 32

With this in mind the
network address : .0
Broadcast : .31
The range is from .1 to .30 of usable ip addresses

upvoted 3 times

iMo7ed 7 months, 1 week ago

Selected Answer: C

C is correct

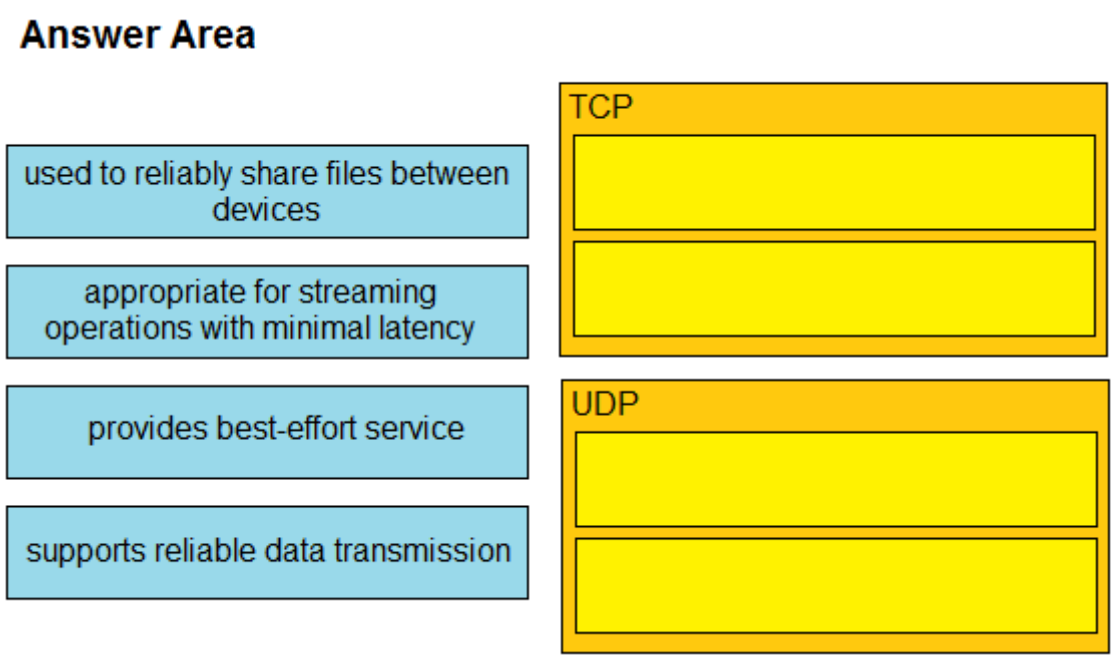
upvoted 2 times

Question #146 *Topic 1*

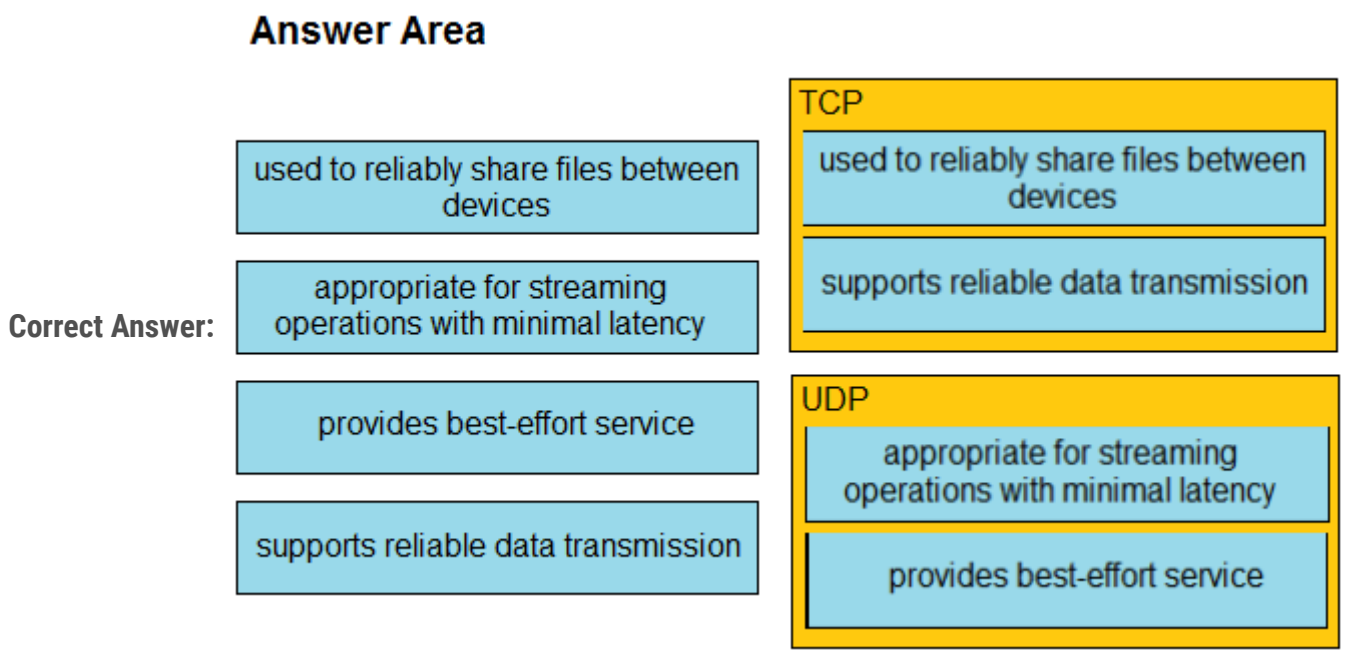
DRAG DROP -

Drag and drop the TCP or UDP details from the left onto their corresponding protocols on the right.

Select and Place:



Correct Answer:



alejandro12 10 months ago

correct answer is given

upvoted 4 times

joanb2s 10 months, 2 weeks ago

MAL MAL MAL. Correct TCP: provides... & supports. UDP: used to... & appropiate...

upvoted 1 times

xWhosNext 9 months, 2 weeks ago

The provided answer is correct. UDP provides 'best effort' not TCP.

UDP provides a best-effort datagram delivery service. This mechanism is best-effort because the underlying IP network does its best to deliver the datagram, but does not guarantee that the datagrams are delivered at the destination.

upvoted 1 times

Question #147 *Topic 1*

What are two reasons to deploy private addressing on a network? (Choose two.)

A. to subnet addresses in an organized hierarchy

B. to reduce network maintenance costs

C. to segment local IP addresses from the global routing table

D. to hide sensitive data from access users within an enterprise

E. to route protected data securely via an Internet service provider

Correct Answer: *AC*

Community vote distribution

BC (64%) AD (29%) 7%

DoBronx Highly Voted 10 months, 3 weeks ago

This bum ah question

upvoted 14 times

RougePotatoe Highly Voted 10 months, 3 weeks ago

Selected Answer: BC

A makes no sense as you could subnet public addresses into an organized hierarchy as well if you had reserved ipv4 addresses.
As ipv4 addresses cost money it definitely will reduce the cost of maintaining your network.

upvoted 7 times

lamm 2 months ago

make sense, this two options: public space cost money, private space none. You can't route private space to internet, but you can route to other private segment inside your organization (this vlan inter-routing as well). So i'm going with this two options.

upvoted 1 times

freeknowledge123 8 months, 1 week ago

can"t subnet an address when you have a limited address pool

upvoted 1 times

splashy 10 months, 2 weeks ago

You can also argue if you need to subnet your public ip addresses, you are using a lot of them, which is not really cost effective... .
You need to look at it from the enterprise perspective, they pay for a public IP or IP range from the ISP. The ISP will do the subnetting and will provide you with what you need if possible/available from their side (WAN) and if affordable for the enterprise. Enterprise does LAN subnetting, ISP manages WAN side i would say in most cases.

upvoted 1 times

RougePotatoe 10 months ago

I don't think the ISP is going to subnet for a company because it wouldn't make sense to. If they needed to resize one of their subnets they would have to first contact the ISP? That doesn't seem logical nor practical when ISP are servicing hundreds or thousands of companies. It's more likely that the ISP would just allocate a range of IP addresses and let the companies have free reign over those IP addresses so the ISP wouldn't have to do anything when the companies reorganize their networks. But going back to your example you still had cost as a major decision factor.

upvoted 1 times

melmiosis 10 months, 3 weeks ago

yea that was weird man.. i could smell that bs from a mile away.

upvoted 2 times

dropspablo Most Recent 1 month, 3 weeks ago

Correct B and C. We think of the logic of IPv6 where public addresses (global unicast) have no cost to be used and we can create hierarchies of subnets with only public addresses. The question does not say which version of the IP, so we could use IPv6 for hierarchy with subnets of public addresses, but it would have a whole migration to IPv6 which could be unfeasible. In this case the letters "A" and "B" would not be the reasons for using private addresses, if this were the case with IPv6 referring to the cost. Now even with IPv6 having public addresses at no cost, we need to use a private address (unique-local unicast) in cases of confidentiality (security) of sensitive user information on an internal network, against external threats from the Internet in conjunction with a firewall, as security is always a determining factor for using a Unique Local, or even a range of private IPv4 addresses. However, it lacked information about the external network, leaving D half incorrect. (he follows...)

upvoted 1 times

dropspablo 1 month, 3 weeks ago

Now let's see the letter C, which describes the NAT process (PAT) of the inside global table that with just one (or more) public IPs we can already segment to several inside local addresses (private IPs) in the internal network. Because the answer to the letter C is correct for IPv4 use, I believe that the question is about IPv4 and not IPv6, so reducing maintenance costs for public IPs would make sense in IPv4, public IPv4 addresses have significant costs in an "end-to-end" user project, and this awareness is necessary, so I choose letter B. "to reduce network maintenance costs" and letter C. "to segment local IP from the global".

upvoted 2 times

Kyoxi 5 months ago

Selected Answer: BC

chat gpt

upvoted 2 times

Isuzu 4 months, 2 weeks ago

its C&D

upvoted 3 times

dearc 5 months, 2 weeks ago

Selected Answer: AD

The answer to the question "What are two reasons to deploy private addressing on a network? (Choose two.)" is: A. to subnet addresses in an organized hierarchy D. to hide sensitive data from access users within an enterprise

Private addressing is the use of IP addresses that are not globally routable over the Internet . The two common reasons for deploying private addressing on a network are to subnet addresses in an organized hierarchy and to hide sensitive data from access users within an enterprise . Using private addressing allows for efficient use of available IP address space and provides a level of security by keeping private IP addresses hidden from public view.

upvoted 1 times

oatmealturkey 7 months, 1 week ago

"Global routing table" , in Cisco documentation at least, does not refer to some routing table of the whole Internet, it seems to refer to the routing table on a router that contains routes from different sources. Someone knowledgeable please correct me if I'm wrong, otherwise, segmenting private IP addresses from the global routing table makes no sense and therefore it can't be C. Cisco is trying to trick us with that one!

Absolutely using private addressing saves money!!! Companies have to pay their ISP for public address space, what companies choose to do with the address space is up to them to subnet but they have to buy the space from their ISP just the same.

upvoted 1 times

ricky1802 7 months, 2 weeks ago

Selected Answer: CD

C. to segment local IP addresses from the global routing table
D. to hide sensitive data from access users within an enterprise

Explanation:
C. Segmenting local IP addresses from the global routing table helps to improve network security by isolating internal network traffic from the public Internet and reducing the risk of unauthorized access.

D. Hiding sensitive data from access users within an enterprise helps to maintain the confidentiality and security of confidential information, as internal private IP addresses are not publicly accessible. This helps to reduce the risk of unauthorized access to sensitive information by external parties.

upvoted 1 times

ODZA 2 months, 1 week ago

But the users data can be accessed by someone within the LAN

upvoted 1 times

ricky1802 7 months, 2 weeks ago

A. to subnet addresses in an organized hierarchy is not a reason for deploying private addressing on a network because subnetting can be performed with either public or private IP addresses. The use of private addresses does not inherently provide a more organized hierarchy for subnetting IP addresses. The decision to use private addresses is typically driven by security and privacy considerations, rather than organizational considerations.

B. to reduce network maintenance costs is not a reason for deploying private addressing on a network because deploying private addressing does not necessarily lead to cost savings for network maintenance. In fact, the use of private addresses can add complexity to network management and require additional resources for proper configuration and maintenance.

upvoted 1 times

DB_Cooper 8 months ago

Selected Answer: AD

"to subnet addresses in an organized hierarchy" and "to hide sensitive data from access users within an enterprise" are common reasons for deploying private addressing on a network. Subnetting allows for better organization and management of IP addresses within a network, while private addressing can be used to protect sensitive data by limiting access to specific IP ranges.

upvoted 3 times

freeknowledge123 8 months, 2 weeks ago

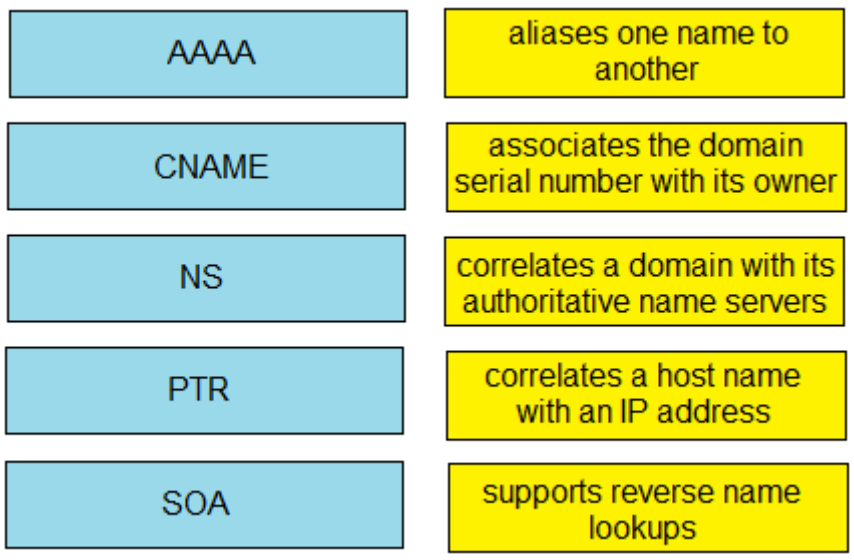
AD, private ip addresses are easy to use and create highly organised network because you need the IANA approval and you're not limited on how much addresses you use.
security because no one can access you're network from outside. the answer mention securtiy within a network it doesnt indicate where teh attack come from

upvoted 3 times

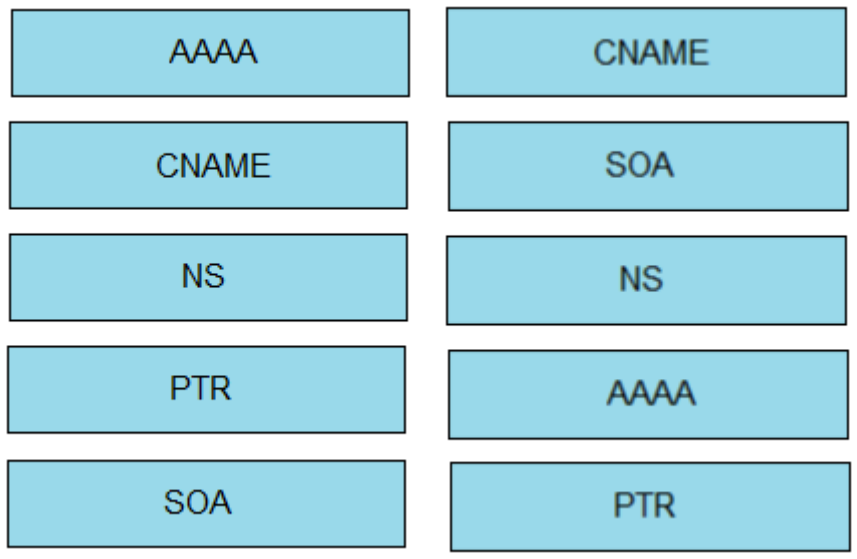
DRAG DROP -

Drag and drop the IPv6 DNS record types from the left onto the description on the right.

Select and Place:



Correct Answer:



TMT91 Highly Voted 12 months ago

Is this related CCNA 200-301 ?

upvoted 14 times

daddydagoth 6 months, 3 weeks ago

I am almost 99% sure that it is not

upvoted 4 times

cormorant Highly Voted 9 months, 2 weeks ago

SSSSSSSSSSOAAAAA - asssssssssssociatesss the domain sssssssssssserial number with itsss ownaaaaaaaa -

upvoted 7 times

dropspablo Most Recent 4 months, 2 weeks ago

CNAME: aliases one name to another

SOA: associates the domain serial number with its owner

NS: correlates a domain with its authoritative name servers

AAAA: correlates a host name with an IP address

PTR: supports reverse name lookups

upvoted 1 times

Saleem360 5 months, 3 weeks ago

I think this is not related CCNA 200-301

upvoted 2 times

cpinac 6 months, 1 week ago

This is correct!

upvoted 2 times

ricky1802 7 months, 1 week ago

AAAA: Stands for "Address Record", it maps a hostname to a IPv6 address.

CNAME: Stands for "Canonical Name", it is used to alias one name to another. For example, www.example.com can be an alias to example.com.

NS: Stands for "Name Server", it specifies the authoritative DNS servers for a particular zone.

PTR: Stands for "Pointer Record", it maps an IP address to a hostname. This is used for reverse DNS lookups.

SOA: Stands for "Start of Authority", it defines the start of a DNS zone and contains information about the zone's properties such as the domain name, primary name server, and the domain administrator's email address.

upvoted 5 times

ccna_goat 11 months, 3 weeks ago

another stupid question. not mentioned in blueprints, but you can encounter such questions more and more often recently - configuring AAA, configuring QoS, SNMP commands etc. not fair.

upvoted 5 times

soRwatches 6 months, 1 week ago

yeah, technically a robbery.

upvoted 2 times

mrgreat 1 year ago

Answers are correct

upvoted 3 times

Question #149 *Topic 1*

Which property is shared by 10GBase-SR and 10GBase-LR interfaces?

A. Both use the single-mode fiber type.

B. Both require UTP cable media for transmission.

C. Both require fiber cable media for transmission.

D. Both use the multimode fiber type.

Correct Answer: *C*

Community vote distribution

C (100%)

ricky1802 Highly Voted 7 months, 2 weeks ago

Selected Answer: C

10GBase-SR and 10GBase-LR are two types of 10 Gbps Ethernet standards for optical fiber communication.

10GBase-SR (Short Reach) is a 10 Gbps Ethernet standard for short-distance optical fiber communication, typically used for data center and campus network applications. It supports distances up to 300 meters over multi-mode fiber (MMF) cable.

10GBase-LR (Long Reach) is a 10 Gbps Ethernet standard for long-distance optical fiber communication, typically used for WAN (Wide Area Network) applications. It supports distances up to 10 kilometers over single-mode fiber (SMF) cable, making it well suited for high-speed inter-building or inter-data center connections.

upvoted 10 times

reeeda Highly Voted 1 year ago

C is right
Model Wave length F.O.Mode Distance Standard
SFP-10G-SR 850 nm Multimode 300 m Duplex LC 10GBASE-SR
SFP-10G-LR 1310 nm Singlemode 10 km Duplex LC 10GBASE-LR

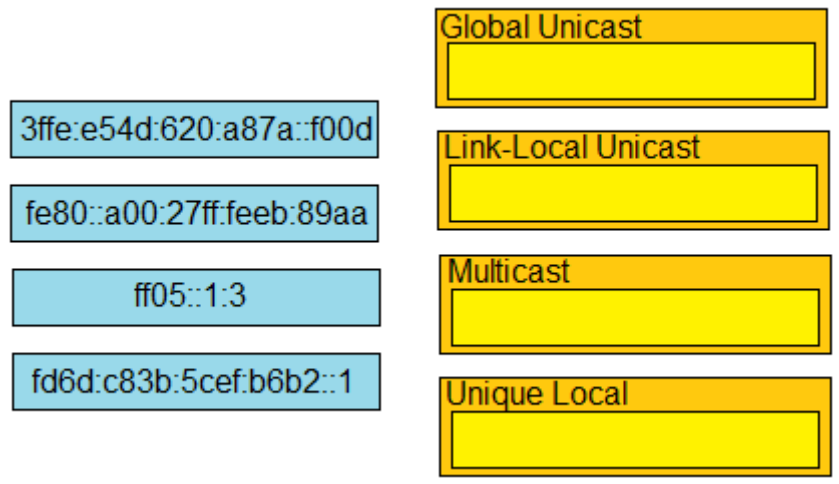
upvoted 6 times

Question #150 *Topic 1*

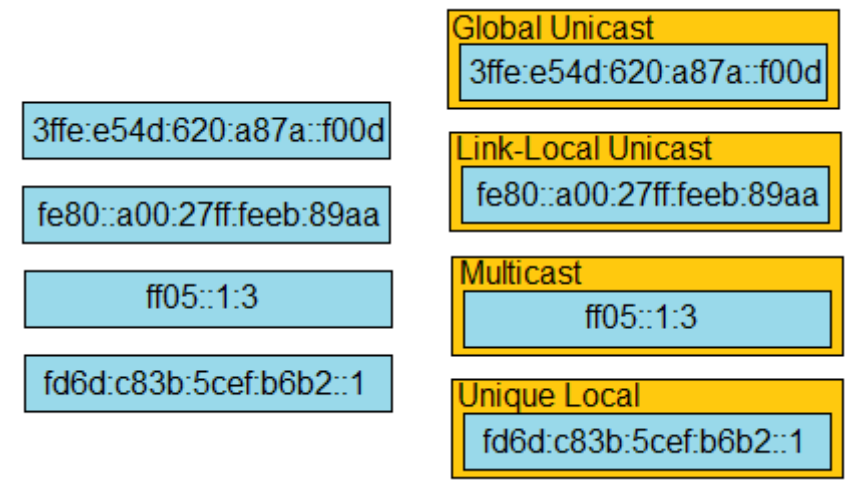
DRAG DROP -

Drag and drop the IPv6 addresses from the left onto the corresponding address types on the right.

Select and Place:



Correct Answer:



FlyingBanana Highly Voted 6 months, 2 weeks ago

remember that. unique local is my friend. (short form: fd)

upvoted 7 times

ahedalikhan87 Most Recent 23 hours, 21 minutes ago

same order, i like it xD

upvoted 1 times

cormorant 9 months, 1 week ago

link local- fe80
multicast- ff
unique local- fd

upvoted 3 times

Question #151 *Topic 1*

Which device permits or denies network traffic based on a set of rules?

A. switch

B. firewall

C. wireless controller

D. access point

Correct Answer: *B*

gorigorimmm 1 year ago

Why not D?
Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks

upvoted 1 times

Hanagaki_Shinjiro 5 days, 21 hours ago

Damn, you misunderstood seriously bro. ACLs are rules, not a DEVICE

upvoted 1 times

Taku2023 6 months, 3 weeks ago

Device is the keyword

upvoted 1 times

TMT91 12 months ago

D is Access Points not ACL !

upvoted 9 times

Dutch012 7 months ago

+ ACL is a set of rules, not a device

upvoted 1 times

Question #152 *Topic 1*

What is the role of a firewall in an enterprise network?

A. determines which packets are allowed to cross from unsecured to secured networks

B. processes unauthorized packets and allows passage to less secure segments of the network

C. forwards packets based on stateless packet inspection

D. explicitly denies all packets from entering an administrative domain

Correct Answer: *A*

Community vote distribution

A (100%)

ricky1802 Highly Voted 7 months, 2 weeks ago

Selected Answer: A

The role of a firewall in an enterprise network is to determine which packets are allowed to cross from unsecured to secured networks.

upvoted 5 times

DRAG DROP -

Refer to the exhibit.

```
C:\ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Inspiron15
   Primary DNS Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 1A-76-3F-7C-57-DF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Dell Wireless 1703 802.11b/g/n <2.4GHz>
   Physical Address. . . . . . . . . : B8-76-3F-7C-57-DF
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-Local IPv6 Address . . . . . : fe80::e09f:9839:6e86:f755x12<Preferred>
                  . . . . . . . . . . : 192.168.1.20<Preferred>
                  . . . . . . . . . . : 255.255.255.0
                  . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 263747135
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-18-E6-32-43-B8-76-3F-7C-57-DF

                  . . . . . . . . . . : 192.168.1.15
                                        192.168.1.16
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

An engineer is tasked with verifying network configuration parameters on a client workstation to report back to the team lead. Drag and drop the node identifiers from the left onto the network parameters on the right.

Select and Place:

192.168.1.1	broadcast address
192.168.1.20	default gateway
192.168.1.254	host IP address
192.168.1.255	last assignable IP address in the subnet
B8-76-3F-7C-57-DF	MAC address

Correct Answer:

192.168.1.1	192.168.1.255
192.168.1.20	192.168.1.1
192.168.1.254	192.168.1.20
192.168.1.255	192.168.1.254
B8-76-3F-7C-57-DF	B8-76-3F-7C-57-DF

Robertlars Highly Voted 9 months ago

broadcast address = 192.168.1.255

default gateway = 192.168.1.1

host IP address = 192.168.1.20

last assignable IP address in the subnet = 192.168.1.254

MAC address = B8-75-3F-7C-57-DF

upvoted 7 times

Fermento Highly Voted 11 months, 1 week ago

It's correct

upvoted 5 times

NICE_ANSWERS Most Recent 3 months, 3 weeks ago

Please, how do you know this is the broadcast address and the default gateway?

upvoted 1 times

manaoming 3 months ago

The broadcast address is 1 address before the next subnet's network address. With a subnet mask of 255.255.255.0, network addresses will be in the format of 192.168.1.0, 192.168.2.0, etc. Thus 192.168.1.255 is 1 address before the next subnet address of 192.168.2.0, making it a broadcast address.

As for the default gateway, I guess Cisco blanked out the row names that state which address is the host address or the default gateway. I don't like that, but either way I remembered that <Preferred> is next to the host IP address in the Windows ipconfig command output. By process of elimination the other one is the default gateway.

upvoted 4 times

Yunus_Empire 9 months, 2 weeks ago

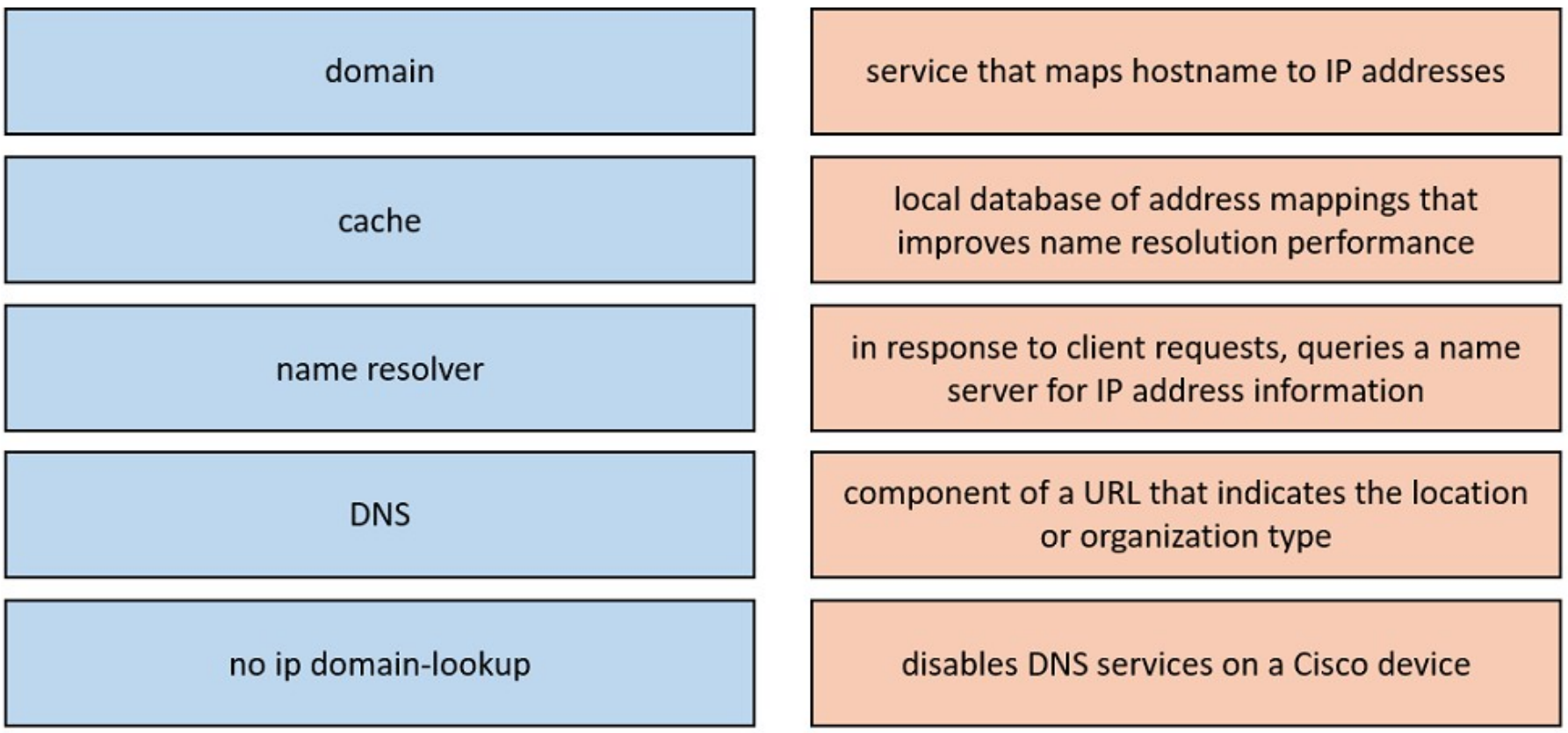
Simplest Question Ever😍😍

upvoted 4 times

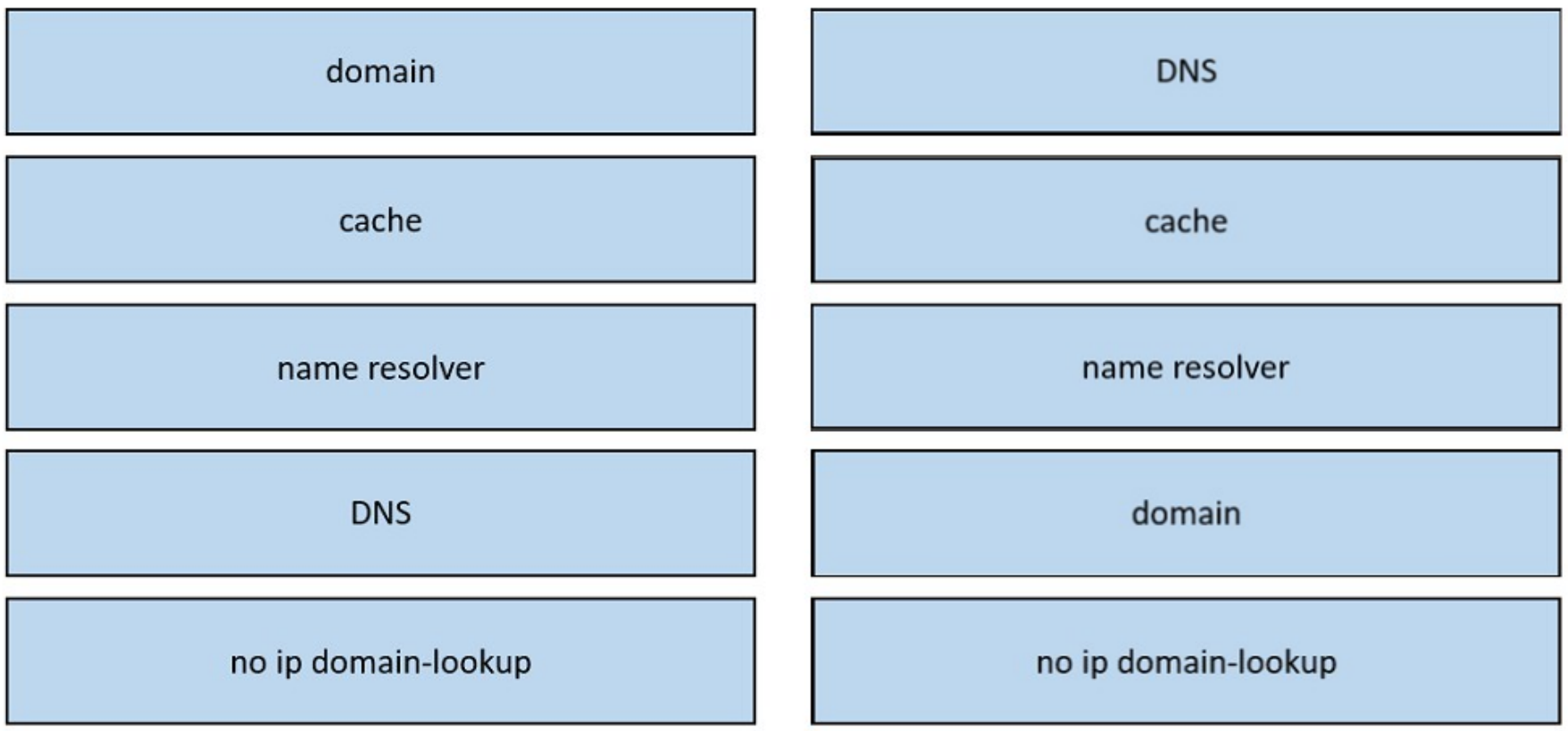
DRAG DROP -

Drag and drop the DNS lookup components from the left onto the functions on the right.

Select and Place:



Correct Answer:



Jhinminent 4 months, 3 weeks ago

Answer is correct

upvoted 4 times

Robertlars 9 months ago

domain = component of a URL that indicate the lcoation or organization type

cache = local database of address mappings that improves name resolution performance (on the end device's [PC's] "host" file)

name resolver = in response to client request, queries a name server for IP address information

DNS = service that maps hostname to IP address

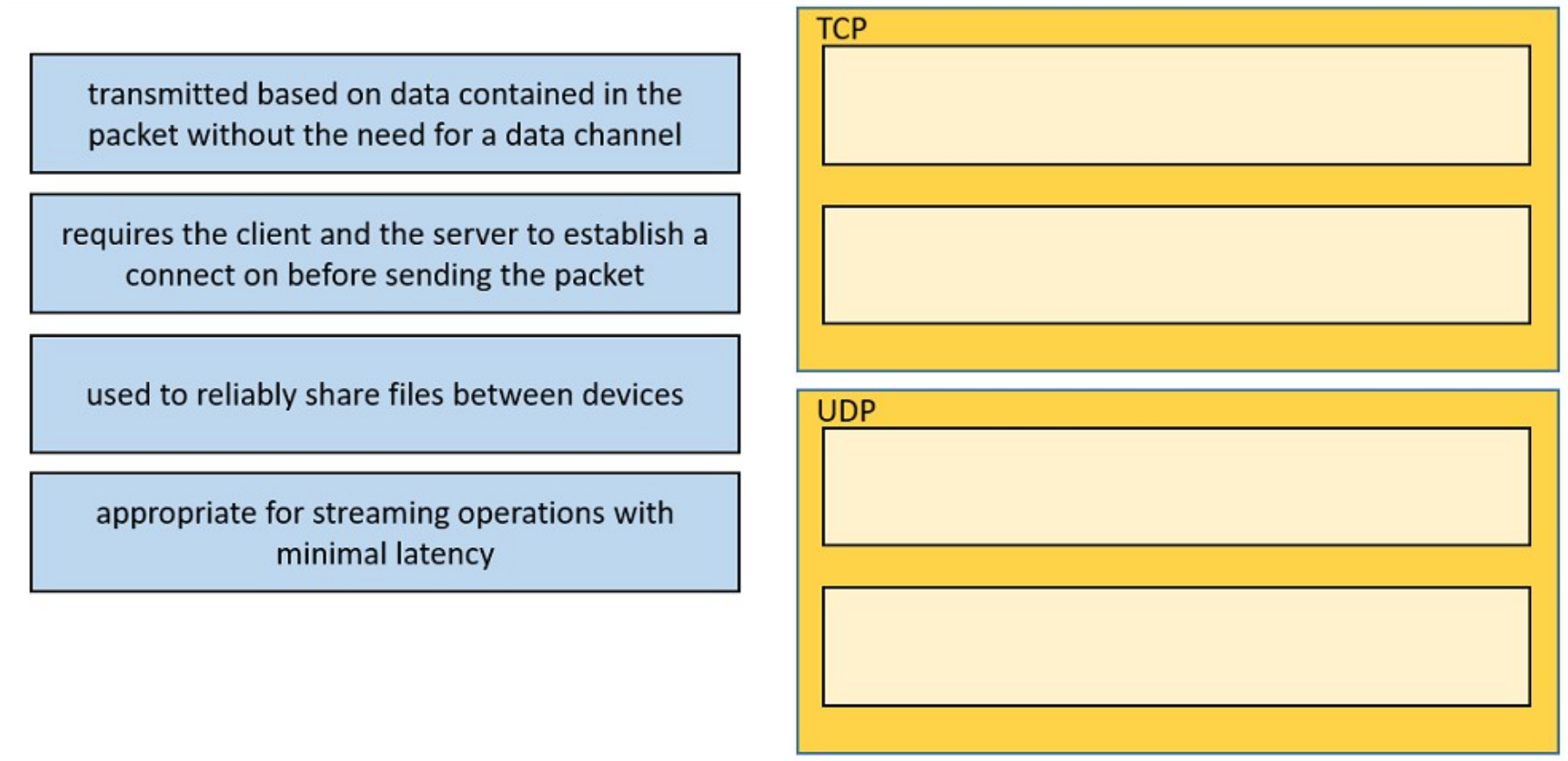
no ip domain-lookup = disables DNS services on a Cisco device

upvoted 2 times

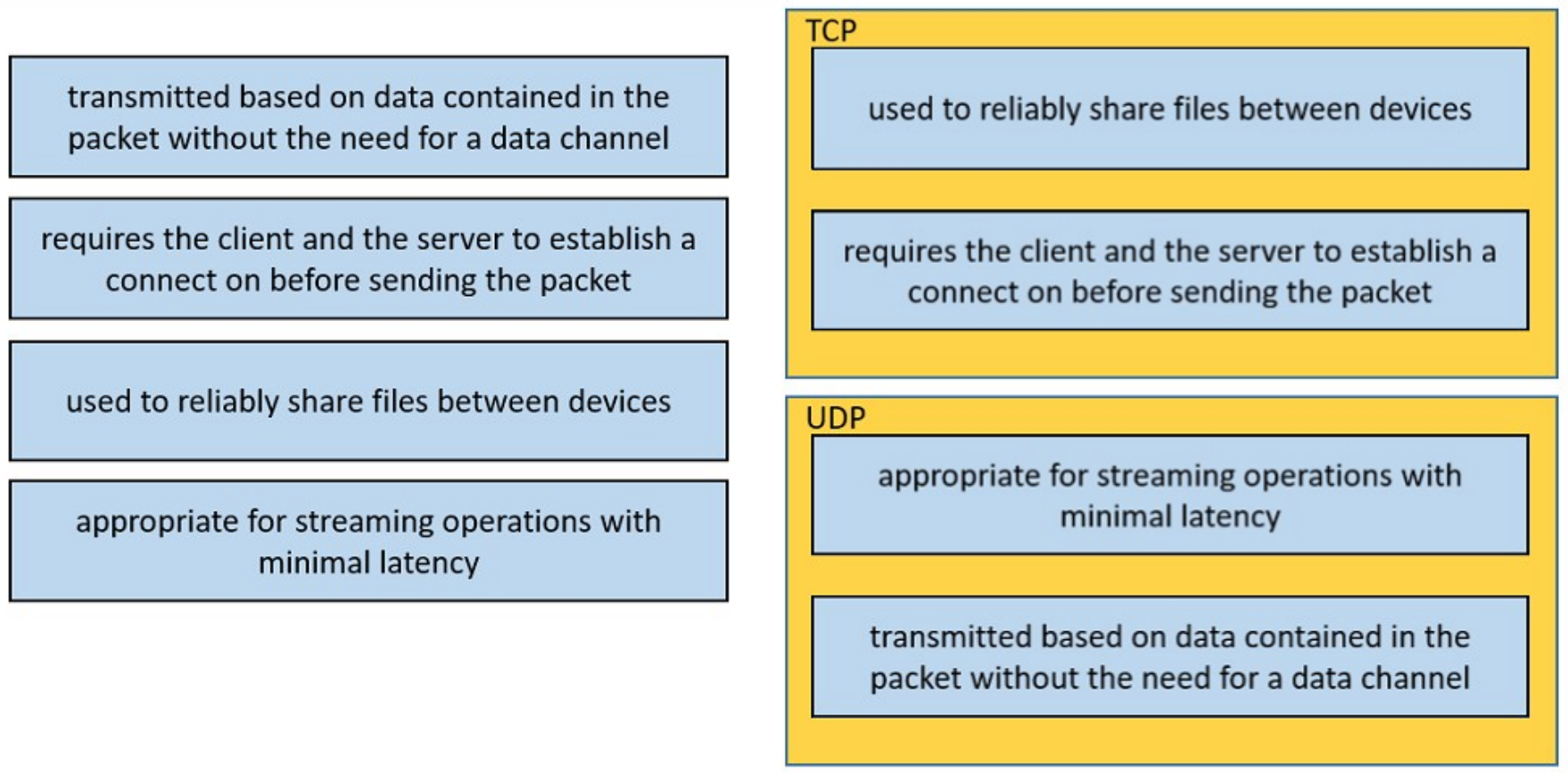
DRAG DROP -

Drag and drop the TCP or UDP details from the left onto their corresponding protocols on the right.

Select and Place:



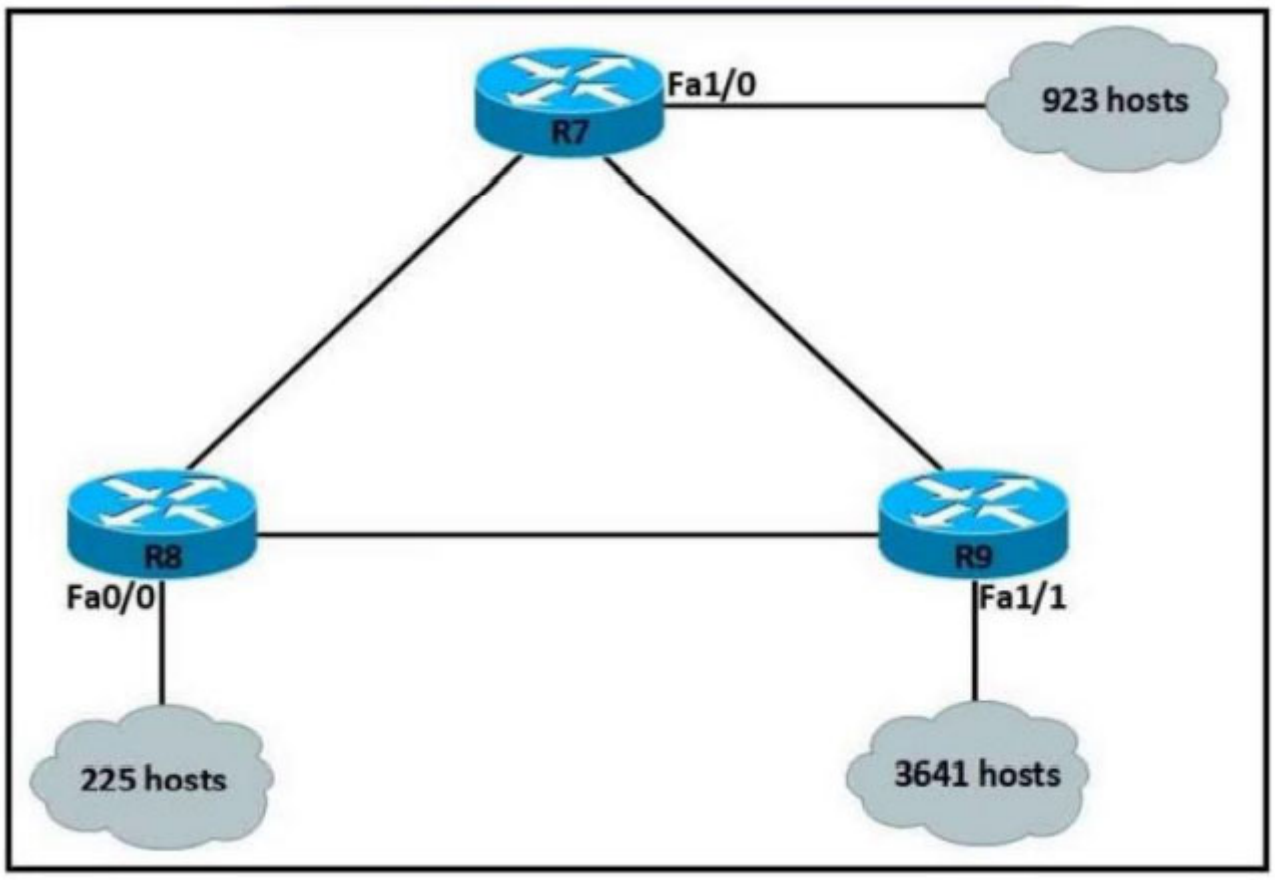
Correct Answer:



sol_ls95 Highly Voted 7 months, 4 weeks ago

correct answer

upvoted 5 times



Refer to the exhibit. An IP subnet must be configured on each router that provides enough addresses for the number of assigned hosts and anticipates no more than 10% growth for new hosts. Which configuration script must be used?

A.

```
R7#
configure terminal
interface Fa1/0
ip address 10.1.56.1 255.255.192.0
no shutdown
R8#
configure terminal
interface Fa0/0
ip address 10.9.32.1 255.255.224.0
no shutdown
R9#
configure terminal
interface Fa1/1
ip address 10.23.96.1 255.255.128.0
no shutdown
```

B.

```
R7#
configure terminal
interface Fa1/0
ip address 10.1.56.1 255.255.240.0
no shutdown
R8#
configure terminal
interface Fa0/0
ip address 10.9.32.1 255.255.224.0
no shutdown
R9#
configure terminal
interface Fa1/1
ip address 10.23.96.1 255.255.192.0
no shutdown
```

C.

```
R7#
configure terminal
interface Fa1/0
ip address 10.1.56.1 255.255.252.0
no shutdown
R8#
configure terminal
interface Fa0/0
ip address 10.9.32.1 255.255.255.0
no shutdown
R9#
configure terminal
interface Fa1/1
ip address 10.23.96.1 255.255.240.0
no shutdown
```

D.

```
R7#
configure terminal
interface Fa1/0
ip address 10.1.56.1 255.255.192.0
no shutdown
R8#
configure terminal
interface Fa0/0
ip address 10.9.32.1 255.255.224.0
no shutdown
R9#
configure terminal
interface Fa1/1
ip address 10.23.96.1 255.255.128.0
no shutdown
```

Correct Answer: *C*

BieLey Highly Voted 11 months, 3 weeks ago

Can pinpoint this easily by only looking at R8:
255.255.255.0 is enough = Answer is C

upvoted 24 times

Rydaz 4 months, 1 week ago

by luck I looked at R8 first lol

upvoted 2 times

[Removed] 3 months, 1 week ago

Same, i picked the smallest one

upvoted 1 times

iMo7ed Most Recent 7 months, 1 week ago

C is Correct

upvoted 2 times

sol_ls95 7 months, 4 weeks ago

select the router with the lowest number of hosts, wich is r8, for 225 hosts it would be a minimun of 256 hosts wich is /24 wich is the only answer that has 255.255.255.0

upvoted 3 times

Question #157 *Topic 1*

Which action is taken by a switch port enabled for PoE power classification override?

A. As power usage on a PoE switch port is checked data flow to the connected device is temporarily paused

B. When a powered device begins drawing power from a PoE switch port, a syslog message is generated

C. If a switch determines that a device is using less than the minimum configured power, it assumes the device has failed and disconnects it

D. Should a monitored port exceed the maximum administrative value for power, the port is shut down and err-disabled

Correct Answer: *D*

VarDav Highly Voted 11 months, 2 weeks ago

D
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/power_over_ethernet.html
upvoted 8 times

Question #158 *Topic 1*

What is a function spine-and-leaf architecture?

A. Offers predictable latency of the traffic path between end devices.

B. Exclusively sends multicast traffic between servers that are directly connected to the spine.

C. Mitigates oversubscription by adding a layer of leaf switches.

D. Limits payload size of traffic within the leaf layer.

Correct Answer: *A*
With a spine-and-leaf architecture, no matter which leaf switch to which a server is connected, its traffic always has to cross the same number of devices to get to another server (unless the other server is located on the same leaf). This approach keeps latency at a predictable level because a payload only has to hop to a spine switch and another leaf switch to reach its destination.
Reference:
https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/white-paper-c11-737022.html

Community vote distribution

A (100%)

ricky1802 Highly Voted 7 months, 1 week ago

Selected Answer: A
With a spine-and-leaf architecture, no matter which leaf switch to which a server is connected, its traffic always has to cross the same number of devices to get to another server (unless the other server is located on the same leaf). This approach keeps latency at a predictable level because a payload only has to hop to a spine switch and another leaf switch to reach its destination.
upvoted 6 times

lamm Most Recent 2 months ago

Selected Answer: A
best answer
upvoted 1 times

Question #159 *Topic 1*

Which action is taken by the data plane within a network device?

A. Constructs a routing table based on a routing protocol.

B. Forwards traffic to the next hop.

C. Looks up an egress interface in the forwarding information base.

D. Provides CLI access to the network device.

Correct Answer: *B*

Community vote distribution

B (86%) 14%

Yinxs 4 weeks ago

Selected Answer: B

B and C are all correct.

upvoted 1 times

lamm 2 months ago

Selected Answer: C

believe better answer

upvoted 1 times

lamm 2 months ago

i believe correct answer is C. Looks up an egress interface in the forwarding information base. Question mentioned "data plane", not control plane, so control plane determine first: Next hop then output interface, so "data plane must only get to the egress interface (and there is no need for going to another network it will happens if the network device relates to the same segment). Makes more sense for me.

upvoted 1 times

no_blink404 3 months, 1 week ago

Selected Answer: B

Poorly written question, but B would be the answer

upvoted 1 times

FALARASTA 5 months ago

B is correct

upvoted 1 times

ricky1802 7 months, 2 weeks ago

Selected Answer: B

The data plane forwards traffic flows. The data plane is the forwarding plane, which is responsible for the switching of packets through the router.

upvoted 4 times

Bankultimate 9 months ago

B is correct.

upvoted 2 times

Question #160 *Topic 1*

What is the function of the control plane?

A. It exchanges routing table information.

B. It provides CLI access to the network device.

C. It looks up an egress interface in the forwarding information base.

D. It forwards traffic to the next hop.

Correct Answer: *A*

Community vote distribution

A (100%)

mrgreat Highly Voted 1 year ago

A is correct

The control plane is the part of a network that controls how data packets are forwarded — meaning how data is sent from one place to another. The process of creating a routing table, for example, is considered part of the control plane. Routers use various protocols to identify network paths, and they store these paths in routing tables.

upvoted 10 times

dearc Most Recent 5 months, 2 weeks ago

Selected Answer: A

The answer to the question "What is the function of the control plane?" is: A. It exchanges routing table information.

The control plane is responsible for exchange of routing table information between routers . The control plane sets up and maintains the routing tables that the data plane uses to forward packets. It provides a way for routers to learn about the networks they are directly connected to, as well as about other networks that are reachable through other routers.

upvoted 2 times

Question #161 *Topic 1*

Which two cable types must be used to connect an access point to the WLC when 2.5-Gbps and 5-Gbps upload speeds are required? (Choose two.)

A. 10GBASE-T

B. 1000BASE-LX/LH

C. Cat 5e

D. Cat 5

E. Cat 3

Correct Answer: *AC*

Community vote distribution

AC (67%) C (33%)

Netcmd Highly Voted 10 months, 1 week ago

cat5e cant go more than 1GBps

upvoted 12 times

Anas_Ahmad Highly Voted 9 months, 1 week ago

CAT5e and CAT6 can handle speeds of up to 1000 Mbps, or a Gigabit per second.

upvoted 5 times

Yinxs Most Recent 4 weeks ago

Selected Answer: AC

C. Cat 5e - Cat 5e cabling can support up to 1 Gbps (Gigabit Ethernet) over distances of up to 100 meters. However, with specific hardware and shorter distances, it can also support 2.5 Gbps speeds under the NBASE-T standard.

upvoted 1 times

vnn777 1 month, 4 weeks ago

Selected Answer: C

No correct answer is possible with presented options.
2.5 Gigabit requires Cat 5e cable, 5 Gigabit requires Cat 6 cable.
Correct answer could be:
Cat 5e, Cat 6
10GBASE-T and 1000BASE-LX/LH are not cable types.

upvoted 1 times

lolungos 3 months ago

Selected Answer: AC

A more viable option is to upgrade your Cat5e cable without ever touching a wall. This is the approach that Cisco and the NBASE-T Alliance have taken to give us an immediate and cost effective solution. Thanks to their work, there is now a solution where you can get 2.5 and even 5 Gbps across existing Cat5e cable.

https://www.mercadoit.com/blog/noticias-it/como-cisco-catalyst-multigigabit-puede-aumentar-las-velocidades-de-red/

upvoted 1 times

harkindeylee 6 months, 2 weeks ago

cat 5e and base-T

upvoted 1 times

[Removed] 7 months, 1 week ago

Why not AB??

upvoted 4 times

lamm 2 months ago

i believed it is because it is for long haul, not like WLC will be set.

upvoted 1 times

Shansab 7 months, 3 weeks ago

With the inclusion of the IEEE 802.3bz standard you can even get more performance with your existing Cat5e cables. Under the standard of IEEE 802.3bz you can achieve up to 2.5GBase-T and 5GBase-T up to 328 Feet (100 meters). It's able to achieve this by having the layer of transmissions be based on 10GBase-T but perform at a lower signal rate. When lowering the signal rate it reduces the cabling requirements giving you the ability to perform this on Cat5e. While this is certainly obtainable it's not a guarantee. For Cat5e we can look to the baseline performance of 1Gb up to 328 Feet as the standard performance you can achieve and 2.5 or 5GBase-T being the performance under ideal environments including capable hardware.

https://infinity-cable-products.com/blogs/performance/what-is-the-cat5e-max-speed
So, Cat 5e could be the theoretically correct answer.

upvoted 4 times

Mahfuj_01 9 months, 4 weeks ago

The use of proper cable types will directly affect the performance of the Catalyst 9136I (A cisco AP). Since this AP has 5-Gbps ports, the recommendation is to use either CAT6 or CAT 6a cable, which support speeds of up to 10 Gbps. CAT 5e cables can still be used; however, there may be an effect on the AP's performance.
Since there is no option for Cat6 or Cat6e so answer should be 10G and Cat5e.

upvoted 2 times

Question #162 *Topic 1*

What is a benefit for external users who consume public cloud resources?

A. Implemented over a dedicated WAN

B. All hosted on physical servers

C. Accessed over the Internet

D. Located in the same data center as the users

Correct Answer: *C*

Community vote distribution

C (100%)

TKHZRD Highly Voted 8 months, 2 weeks ago

The question is formulated in a weird way... Or is it me?

upvoted 11 times

NICE_ANSWERS 3 months, 3 weeks ago

yes it is

upvoted 1 times

Silencer 7 months, 1 week ago

I also noticed.

upvoted 1 times

lamm Most Recent 2 months ago

Selected Answer: C

better answer

upvoted 1 times

wondaah 6 months, 2 weeks ago

terrible question this is

upvoted 2 times

Question #163 *Topic 1*

An engineer must update the configuration on two PCs in two different subnets to communicate locally with each other. One PC is configured with IP address
192.168.25.128/25 and the other with 192.168.25.100/25. Which network mask must the engineer configure on both PCs to enable the communication?

A. 255.255.255.248

B. 255.255.255.224

C. 255.255.255.0

D. 255.255.255.252

Correct Answer: *C*

Community vote distribution

C (100%)

Customexit Highly Voted 10 months, 3 weeks ago

Just to add more info here:
A, .248 has a group size of 8. At a glance that's too small to include both .100 and .128.
.252 has a group size of 4. Same as above.
.224 seems large enough with a 32 group size, but if you subnet you'll find that .128 is a network address.

That leaves us with 255.255.255.0. Which gives us the first usable at .25.1 and the last usable at .25.254.

upvoted 15 times

[Removed] Highly Voted 7 months, 1 week ago

I hate this kind of question because I know the answer is C but to be confirmed and confident with your answer you need to calculate the other answer too hence wasting the time.

upvoted 8 times

Da_Costa Most Recent 1 month, 4 weeks ago

Selected Answer: C

Use default class C mask

upvoted 1 times

Iamm 2 months ago

Selected Answer: C

only answer could be

upvoted 1 times

MelbourneJin 2 months, 3 weeks ago

It makes me so confused. IP address .128 is a network IP, not assignable to a PC.

upvoted 1 times

MelbourneJin 2 months, 3 weeks ago

To enable communication between the two PCs in different subnets, the engineer needs to configure both PCs with the same network mask. In this case, the PCs have IP addresses 192.168.25.128/25 and 192.168.25.100/25, indicating that they are using a subnet mask of 255.255.255.128.

Therefore, the engineer must configure both PCs with the subnet mask 255.255.255.128 to ensure they are in the same subnet and can communicate with each other locally.

upvoted 1 times

AbiZ17 8 months, 2 weeks ago

I wonder how 192.168.25.128 is configured to the host coz in a /25 prefix length it is the network. address

upvoted 1 times

soRwatches 6 months, 1 week ago

same thought.

upvoted 1 times

THEKYPTONIAN 12 months ago

The subnet must include addresses 100 and 128 so /24 is correct

upvoted 2 times

g_h_97 1 year ago

192.168.25.128/25 is the network address, I guess they meant 192.168.25.129/25

upvoted 4 times

Trdelnik 12 months ago

i think the implication was the initial config wouldn't work, so what should it be instead...? i thought the same thing myself until i saw that /24 in the answers

upvoted 2 times

everchosen13 11 months, 3 weeks ago

I agree, another one of those silly question where it is not quite clear what the question is asking you are just supposed to assume

upvoted 2 times

Question #164 *Topic 1*

Which key function is provided by the data plane?

A. Originating packets

B. Exchanging routing table data

C. Making routing decisions

D. Forwarding traffic to the next hop

Correct Answer: *D*

Community vote distribution

D (100%)

efstratios39 4 weeks, 1 day ago

I remember it by saying " Hop on a (data) plane lol

upvoted 1 times

lamm 2 months ago

Selected Answer: D

only answer could be, all other answer relates to control plane

upvoted 1 times

dearc 5 months, 2 weeks ago

The answer to the question "Which key function is provided by the data plane?" is: D. Forwarding traffic to the next hop

The data plane , also known as the forwarding plane, is responsible for the actual forwarding of data packets through a network. It consists of the hardware and software components in a network device that perform packet forwarding, routing, and switching. The data plane makes decisions about where packets should be forwarded to next and determines the appropriate ports to send them out. Therefore, the key function that is provided by the data plane is forwarding traffic to the next hop.

upvoted 4 times

harkindeylee 6 months, 2 weeks ago

forwarding packets

upvoted 3 times

Question #165 *Topic 1*

When should an engineer implement a collapsed-core architecture?

A. Only when using VSS technology

B. For small networks with minimal need for growth

C. For large networks that are connected to multiple remote sites

D. The access and distribution layers must be on the same device

Correct Answer: *B*

Community vote distribution

B (100%)

learnNcurve 6 months, 2 weeks ago

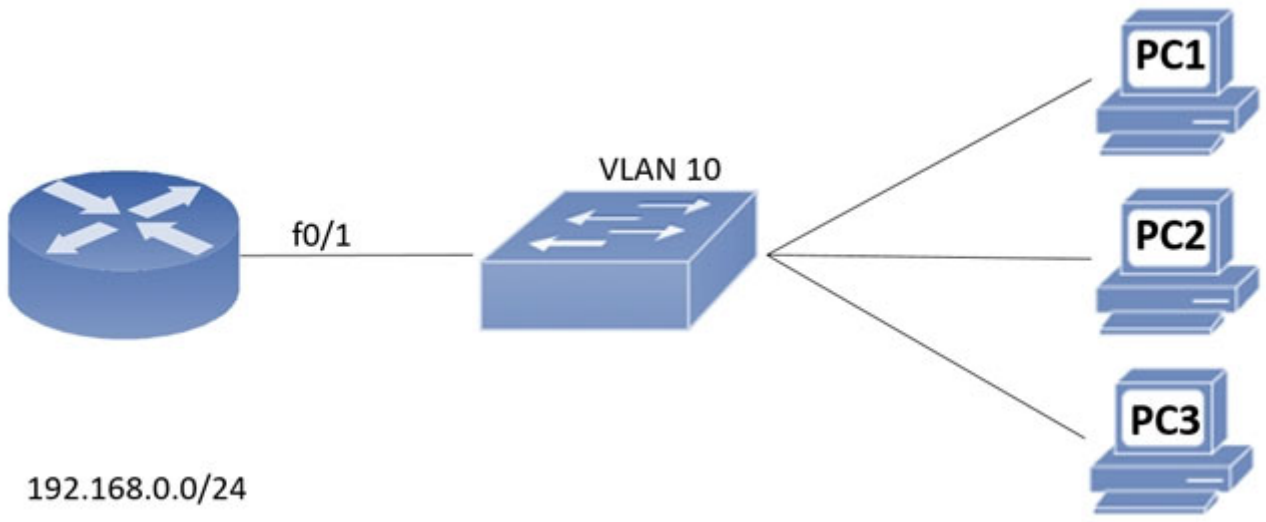
Selected Answer: B

B is the Answer.

A collapsed core architecture is typically implemented in small networks, wheres as a three tier architecture is deployed into larger networks where scalabily will be a factor

upvoted 2 times

Question #166 *Topic 1*



Refer to the exhibit. An engineer assigns IP addressing to the current VLAN with three PCs. The configuration must also account for the expansion of 30 additional
VLANS using the same Class C subnet for subnetting and host count. Which command set fulfills the request while reserving address space for the expected growth?

A. Switch(config)#interface vlan 10 Switch(config-if)#ip address 192.168.0.1 265 255.255.252

B. Switch(config)#interface vlan 10 Switch(config-if)#ip address 192.168.0.1 255 255.255.248

C. Switch(config)#interface vlan 10 Switch(config-if)#ip address 192.168.0.1 255 255.255.0

D. Switch(config)#interface vlan 10 Switch(config-if)#ip address 192.168.0.1 255.255.255.128

Correct Answer: *B*

Community vote distribution

B (78%) A (22%)

vladals Highly Voted 1 year ago

I think that the answer is good. we are looking at 31 VLANs (a sin 31 Subnets) and each one will have 3 hosts. So /29 will give us 32 subnets each with 8 hosts (6 usable). /29 means 248 mask, so B is correct.

upvoted 23 times

dendentester Highly Voted 11 months, 1 week ago

30 ADDITIONAL SUBNETS , IT MUST BE 32 = 5 BITS
CLASS C /24+5BITS = /29 = 225.255.255.248

upvoted 8 times

Coachof2 Most Recent 1 month, 1 week ago

A is wrong. Mask # can not be 265 only goes to 255

upvoted 1 times

lamm 2 months ago

Selected Answer: B

couldn't be /30 because you only could configure one PC and the subinterface router's, you can't grow up, and instead of 30 plus networks you achieved 126 so exceeds the actual requirement

upvoted 1 times

Bhrino 4 months, 1 week ago

Selected Answer: B

Because we are looking at 31 vlans we 31 different subnets each with at least 3 host address the closet one to that would be /29 or .248 giving us 8 total per subnet and 6 available for use in each one making the answer b

upvoted 2 times

omid8719 4 months, 3 weeks ago

Selected Answer: B

need 31 Subnet

upvoted 3 times

dearc 5 months, 2 weeks ago

Selected Answer: B

The correct command set that fulfills the given request while reserving address space for the expected growth is: B. Switch(config)#interface vlan 10 Switch(config-if)#ip address 192.168.0.1 255.255.255.248

The scenario mentions that a Class C subnet needs to be used, which means we have a default subnet mask of 255.255.255.0. With the requirement to implement 30 additional VLANs, we need a subnet mask that will provide enough IP addresses for all these VLANs with the same Class C network . By allocating a /29 subnet to each VLAN, it will provide 6 bit host addresses (2^6 - 2, where 2 is subtracted for the network address and broadcast address) and will provide enough IP addresses for all 30 additional VLANs.

upvoted 3 times

thomson_johnson 6 months ago

Selected Answer: B

you need /29 for 3 hosts, /30 is only for 2 and would be used in point-to-point connection

upvoted 1 times

jdcassin 6 months, 1 week ago

Selected Answer: B

With .248 you get 8-2= 6 hosts to receive IPs per subnet
With .252 you get 4-2=2 hosts to rececive IPs per subnet. As you need 3 hosts for addressing, Answer B is the correct

upvoted 2 times

iMo7ed 7 months ago

Selected Answer: B

B is correct

upvoted 2 times

shubhambala 1 year ago

Selected Answer: A

255 255.255.248 allows for 32 subnets while 255.255.255.252 allows for 64 subnets. Since we need 33 subnets(3 PCs and 30 additional vlans) I think A is answer. Correct me if I am wrong.

upvoted 4 times

everchosen13 11 months, 3 weeks ago

You need a total of 31 subnets not 33. With 255.255.255.252 subnet you will only have two useable host addresses. You need three usable host addresses.

upvoted 8 times

Question #167 *Topic 1*

A client experiences slow throughput from a server that is directly connected to the core switch in a data center. A network engineer finds minimal latency on connections to the server, but data transfers are unreliable, and the output of the show interfaces counters errors command shows a high FCS-Err count on the interface that is connected to the server. What is the cause of the throughput issue?

A. a physical cable fault

B. a speed mismatch

C. high bandwidth usage

D. a cable that is too long

Correct Answer: *A*

Community vote distribution

A (92%) 8%

cormorant Highly Voted 10 months, 2 weeks ago

questions like this have convinced me that to pass the CCNA it is necessary to bone up on dumps

upvoted 29 times

GhostWolf 10 months, 1 week ago

Exactly, the way CISCO sets their exams you can't just do it from reading a textbook.

upvoted 12 times

[Removed] 4 months, 2 weeks ago

Any idea for a reliable dump please? I cannot find a decent source.

upvoted 1 times

daddydagoth 6 months, 3 weeks ago

Absolutely agree! And they have the audacity to frown upon dumps when they themselves make the exams impossible to pass just by studying "fairly".

upvoted 7 times

DPAD 9 months ago

just like Microsoft exams

upvoted 4 times

dearc Highly Voted 5 months, 2 weeks ago

Selected Answer: A

The cause of the throughput issue described in the scenario is a physical cable fault.

The scenario mentions that the network engineer found minimal latency on connections to the server, but data transfers are unreliable, and the output of the "show interfaces counters errors" command shows a high FCS-Err count on the interface that is connected to the server. FCS-Err (Frame Check Sequence error) indicates that there is a physical issue with the cable, such as noise or interference, that is causing the data transfer errors.

A speed mismatch or high bandwidth usage may cause slow throughput or delays, but it would not cause FCS-Err errors. Similarly, a cable that is too long may cause signal attenuation, but it would not cause FCS-Err errors.

Therefore, the answer to the question "What is the cause of the throughput issue?" is A. a physical cable fault.

upvoted 10 times

lamm Most Recent 2 months ago

Selected Answer: C

believe correct answer is C: high bandwidth usage. Cable faulty will cut off communication, question relates to slow connection. Latency is ok, so it means cable long is ok, speed o duplex mismatch will cut off comunication as well, so better answer will be C.

upvoted 1 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: A

The cause of the throughput issue is most likely a physical cable fault. The high FCS-Err count on the interface indicates that there are frame check sequence errors occurring on the link between the switch and the server. These errors are typically caused by a physical problem with the cable or the network interface card (NIC) on either end of the link.

upvoted 1 times

RougePotatoe 10 months, 2 weeks ago

Anyone know why is it not D? Is it because we don't know anything about the cable; IE too specific without justification?

upvoted 3 times

cuenca73 7 months, 1 week ago

I guessed that it was not D because in the case of having a too long cable, the incremented counter would be also "Late collisions"

upvoted 3 times

diudiuQIdama 9 months ago

long cable=high latency

upvoted 1 times

RougePotatoe 7 months, 3 weeks ago

It clearly said MINIMAL latency

upvoted 2 times

Question #168 *Topic 1*

What is the difference between 1000BASE-LX/LH and 1000BASE-ZX interfaces?

A. 1000BASE-LX/LH interoperates with multimode and single-mode fiber, and 1000BASE-ZX needs a conditioning patch cable with multimode.

B. 1000BASE-ZX interoperates with dual-rate 100M/1G 10Km SFP over multimode fiber, and 1000BASE-LX/LH supports only single-rate

C. 1000BASE-ZX is supported on links up to 1000km, and 1000BASE-LX/LH operates over links up to 70 km

D. 1000BASE- LX/LH is supported on links up to 10km, and 1000Base-ZX operates over links up to 70 km

Correct Answer: *D*

Community vote distribution

D (100%)

ccna_goat Highly Voted 11 months, 3 weeks ago

another question not related with CCNA. love it. they got brazen recently, im waiting for CCIE questions on CCNA exam.

upvoted 25 times

AshenOne_31 Highly Voted 11 months ago

such a ridiculous question for the CCNA

upvoted 10 times

efstratios39 Most Recent 1 month ago

im gonna go out on a limb and say this wont be on the exam lol

upvoted 1 times

xbololi 2 months, 3 weeks ago

next stop is some cisso cert exam question (:

upvoted 1 times

[Removed] 7 months, 1 week ago

I think this is not in CCNA 200-301 exam topic

upvoted 5 times

in2it 7 months, 2 weeks ago

Wow, some conflicting info out there. This is from Cisco site. D is correct.

1000BaseSX multi-mode fiber to 550 m.
1000BaseLX/LH multi-mode fiber to 550 m. Single-mode fiber to 10 km.
1000BaseZX single mode fiber to 70 km.

https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/datasheet-c78-366584.html?dtid=osscdc000283

upvoted 5 times

jo966 7 months, 2 weeks ago

starting to hate my company. what is this? It's not i don't understand the stuff.... just the frustration gets unbearable. and that stresses ultimately

upvoted 4 times

sassasasasdccadsca 8 months, 1 week ago

In the CCNA - WAN Concepts chapter, there is only the 1000Base-ZX standard which supports cable lengths up to 70 km and the 1000BASE-LX standard which supports fiber optic cable lengths of 5 km. There is no 1000BASE-LX/LH ...

upvoted 1 times

mrgreat 1 year ago

Selected Answer: D

D is correct.
https://www.cables-solutions.com/are-there-any-differences-between-lx-lh-and-lxlh.html

upvoted 4 times

Question #169 *Topic 1*

What are two reasons to implement IPv4 private addressing on a network? (Choose two.)

A. To enable internal applications to treat the private IPv4 addresses as unique

B. To facilitate renumbering when merging networks

C. To expand the routing table on the router

D. To provide protection from external denial-of-service attacks

E. To conserve global unique IPv4 addresses

Correct Answer: *DE*

Community vote distribution

AE (66%) DE (25%) 9%

RougePotatoe Highly Voted 10 months, 3 weeks ago

Selected Answer: AE

Private IPv4 addresses weren't created to be a form of protection. It's primary purpose was to enable internal networks to communicate while conserving public IPv4 addresses.

A fits this narrative as multiple businesses could share the same private IP addresses and their application would still be able to communicate without interfering with other businesses thus it's unique to their internal applications.
E for obvious reasons.

D doesn't work because if you have servers that need to be reached from the outside you would have it port forwarded and thus having it exposed to the internet and DoS. Even if you don't have internal services advertised to the internet, attackers can still DoS your gateway because it has a public IP address.

upvoted 13 times

oatmealturkey 7 months, 1 week ago

But using public IPv4 address would serve the same purpose. The internal applications would still be able to treat them as unique. So A is wrong.

THE purpose of private IPv4 addresses is to conserve public IPv4 addresses, this means that any other reason to have private IPv4 addresses is just an additional reason, not what they were intended to be used for. So D is correct just because it's the only other accurate choice. Even though it obviously doesn't prevent DoS attacks, it still provides some level of protection which is the wording used in D.

upvoted 5 times

Dutch012 6 months, 4 weeks ago

Sorry man I wrote the comment in a hurry, I meant D & E

upvoted 1 times

Dutch012 7 months ago

it says "external DDOS attack", so I believe D & A are correctt

upvoted 1 times

DoBronx 10 months, 3 weeks ago

Yea i picked A E as well

upvoted 3 times

splashy Highly Voted 8 months ago

Selected Answer: DE

"To enable internal applications to treat the private IPv4 addresses as unique"
This describes layer 2 functionality, mac address, arp tables. So i think it's wrong.

upvoted 6 times

Hanagaki_Shinjiro Most Recent 21 hours, 11 minutes ago

I don't think A&E are correct

upvoted 1 times

kyleptt 2 weeks ago

Selected Answer: AE

These two are the best

upvoted 1 times

PlsLetMePass 1 month ago

Selected Answer: BE

The two reasons to implement IPv4 private addressing on a network are B & E:

To facilitate renumbering when merging networks. When two networks are merged, it can be difficult to renumber all of the devices on the networks to use the same public IPv4 address space. Using private IPv4 addresses on the two networks before the merge makes it easier to renumber the devices after the merge.

The other options are not reasons to implement IPv4 private addressing on a network.

Option A: Internal applications will treat the private IPv4 addresses as unique regardless of whether or not they are implemented on the network.
Option B: Renumbering when merging networks can be facilitated by using private IPv4 addresses, but it is not the main reason to implement private IPv4 addressing.
Option C: Private IPv4 addresses do not expand the routing table on the router.
Option D: Private IPv4 addresses do not provide protection from external denial-of-service attacks.

upvoted 1 times

rick2461 1 month, 1 week ago

Selected Answer: BE

B and E, according to AI

upvoted 1 times

vnn777 1 month, 4 weeks ago

Selected Answer: DE

DE is correct

upvoted 1 times

xbololi 2 months, 3 weeks ago

Selected Answer: AE

not for protection, to preserve public ip and easier internal network communication.

upvoted 1 times

VanessaR05 3 months ago

Selected Answer: AE

A. To enable internal applications to treat the private IPv4 addresses as unique: Private addressing allows organizations to use non-routable IP addresses internally, which are not globally unique. This enables internal applications, services, and devices to communicate with each other using unique addresses within the private network without conflicting with globally routable IP addresses.

E. To conserve global unique IPv4 addresses: The availability of globally unique IPv4 addresses is limited. By implementing private addressing, organizations can conserve the limited pool of global unique IPv4 addresses. Private addresses are not publicly routable on the Internet, so they can be reused within different private networks without consuming additional global address space.

Options B, C, and D are not reasons to implement private addressing on a network:

upvoted 1 times

omid8719 4 months, 3 weeks ago

Selected Answer: BE

allows organizations to merge networks or change service providers without having to renumber all the IP addresses within the network

upvoted 1 times

nthatu 3 months, 2 weeks ago

correct..
To facilitate renumbering when merging networks: Private addressing allows for easier network renumbering when merging networks or making significant changes to the network infrastructure. With private IP addresses, the internal addressing scheme can be modified without impacting the external routing or requiring changes to public IP addresses.

To conserve global unique IPv4 addresses: The pool of globally unique IPv4 addresses is limited, and private addressing helps conserve these addresses. By using private IP addresses within an internal network, organizations can allocate unique addresses without consuming globally routable IP addresses. This is especially important as IPv4 addresses become increasingly scarce.

upvoted 1 times

jonathan126 4 months, 3 weeks ago

Selected Answer: AE

E is definitely correct, so it is between A and D.
A is correct if we assume the network does not have extra public addresses. Without private/public addresses, the nodes cannot route in layer 3. So private address comes into rescue.
For D, although private IP addresses have some sort of protection by not being reachable by the internet, DoS can also happen if NAT is used. DoS is also not the major role of private IP addresses but firewalls. So the answer should be A and E.

upvoted 2 times

FALARASTA 5 months ago

I select AE. For D, what is the essence of protection while through the gateway and after translation there will still be attacks?

upvoted 2 times

dearc 5 months, 2 weeks ago

Selected Answer: AE

the answers to the question are A. To enable internal applications to treat the private IPv4 addresses as unique , and E. To conserve global unique IPv4 addresses. Private IPv4 addressing allows an organization to use private IP addresses within its internal network to conserve global unique IPv4

addresses . This means that even though multiple networks may exist with the same private IP addresses, nodes within those networks can still uniquely identify each other using these private IP addresses.

Additionally, private addressing enables internal applications to treat private IP addresses as unique by ensuring that packets containing these IP addresses are not routed to the public internet. This increases security by keeping private network traffic isolated from the public internet.

upvoted 1 times

elixirwell 5 months, 3 weeks ago

ChatGPT says:
The two reasons to implement IPv4 private addressing on a network are:

E. To conserve global unique IPv4 addresses: Private addressing allows organizations to use non-routable IP addresses within their internal networks, which conserves globally unique IP addresses. This is especially important as the pool of available IPv4 addresses is exhausted.

A. To enable internal applications to treat the private IPv4 addresses as unique: Private addressing allows organizations to use the same IP address ranges internally without having to worry about conflicting with IP addresses used by other organizations on the public Internet. This simplifies network design and reduces the risk of IP address conflicts.

upvoted 3 times

elixirwell 5 months, 3 weeks ago

Selected Answer: AE

The two reasons to implement IPv4 private addressing on a network are:

E. To conserve global unique IPv4 addresses: Private addressing allows organizations to use non-routable IP addresses within their internal networks, which conserves globally unique IP addresses. This is especially important as the pool of available IPv4 addresses is exhausted.

A. To enable internal applications to treat the private IPv4 addresses as unique: Private addressing allows organizations to use the same IP address ranges internally without having to worry about conflicting with IP addresses used by other organizations on the public Internet. This simplifies network design and reduces the risk of IP address conflicts.

upvoted 1 times

binjalala 7 months ago

Selected Answer: DE

the answer is de

upvoted 1 times

[Removed] 7 months, 1 week ago

I choose DE

upvoted 1 times

Question #170 *Topic 1*

Which concern is addressed with the use of private IPv4 addressing?

A. Lack of routing protocol support for CIDR and VLSM

B. Lack of security protocols at the network perimeter

C. Lack of available TCP/UDP ports per IPv5 address

D. Lack of available publicly routable unique IPv4 address

Correct Answer: *D*

Community vote distribution

D (100%)

mark9999 2 months ago

Selected Answer: D

How many times, and different ways can they ask this same question? The answer does seem correct in this instance.

upvoted 1 times

Hanagaki_Shinjiro 21 hours, 9 minutes ago

Could you explain for me about the answer ?

upvoted 1 times

Question #171 *Topic 1*

What is the path for traffic sent from one user workstation to another workstation on a separate switch in a three-tier architecture model?

A. access â€" core â€" access

B. access â€" distribution â€" distribution â€" access

C. access â€" core â€" distribution â€" access

D. access â€" distribution â€" core â€" distribution â€" access

Correct Answer: *D*

Community vote distribution

D (80%) B (20%)

Dutch012 Highly Voted 6 months, 4 weeks ago

Selected Answer: D

Distribution doesn't connect to another Distribution layer directly, it needs to go through core firsrt

upvoted 16 times

RougePotatoe Highly Voted 10 months, 3 weeks ago

Selected Answer: B

This question sucks. Realistically you can configure inter vlan routing on either distribution or the core layer provided that you have layer 3 switches. I have been told the core layer should only handle traffic intended to go outside your network thus according to that logic it should be configured on distribution layer. Also see this post.

https://community.cisco.com/t5/switching/ccnp-studies-svi-intervlan-routing-disagree-w-answer/td-p/2300859

upvoted 7 times

dropspablo 1 month, 3 weeks ago

However, the question informs separate switches that "could" be separated by the core, because if we look at the tree-tier architecture we notice that connecting in other parts of the company would be in other switches separated by the core, such as other sectors (commercial to engineering), in this case it would be forced to go through the core to access switches separated from other parts, which I believe is the answer. See an example of the design that the distribution switch does not reach all the access switches, in these cases it would need the core: https://www.leviton.com/en/solutions/industries/data-centers/architectures/threetier-network-architecture

upvoted 2 times

Hanagaki_Shinjiro Most Recent 21 hours, 5 minutes ago

Selected Answer: D

3-tire architecture: access, distribution/aggregation, core

upvoted 1 times

kyleptt 2 weeks ago

Selected Answer: D

In this instance D because it is 3 tier

upvoted 1 times

Kerrera 1 month ago

Selected Answer: D

I think B is not three tier. D is three tier

upvoted 1 times

Dunedrifter 2 months, 2 weeks ago

Selected Answer: D

D is correct.

upvoted 1 times

VanessaR05 3 months ago

Selected Answer: B

In a three-tier architecture model, the most common path for traffic sent from one user workstation to another workstation on a separate switch is:

B. access - distribution - distribution - access.

In a three-tier architecture model, the network is typically divided into three layers: access layer, distribution layer, and core layer.

upvoted 1 times

Hope_12 4 months, 1 week ago

Selected Answer: D

Core switches connect distribution switches.
D is the answer.
upvoted 1 times

omid8719 4 months, 3 weeks ago

Selected Answer: D

bcz when you want to expand the network and add some other D switches they should connect to the core SW
upvoted 1 times

FALARASTA 5 months ago

Selected Answer: D

Choice B lacks the full architectural formation. In a three tier there is no complete connection from one access device to another access device without going through the core layer because two access layers are not connected neither does the distribution layer interconnect without the core layer. The correct choice is D
upvoted 1 times

ASHLEY_27 5 months, 2 weeks ago

B is wrong coz a question clearly states that for three-tier network. On a three-tier there's access, distribution and core.
upvoted 2 times

elixirwell 5 months, 3 weeks ago

In a three-tier architecture model, the path for traffic sent from one user workstation to another workstation on a separate switch is:

C. access - core - distribution - access

This model has three layers: access layer, distribution layer, and core layer.

The access layer connects end-user devices such as workstations, laptops, and servers to the network.

The distribution layer aggregates traffic from the access layer and connects to the core layer and distributes traffic between different access layer switches.

The core layer is the backbone of the network and provides high-speed connectivity between different distribution layer switches.

Therefore, traffic from one user workstation to another workstation on a separate switch in a three-tier architecture model would travel from the access layer switch to the core layer switch and then to the distribution layer switch that connects to the destination access layer switch before reaching the destination workstation.
upvoted 2 times

jayasssshhhh 3 months ago

no access layer cannot directly connect with core layer,it has to pass to distribution before core
upvoted 2 times

Rydaz 4 months, 1 week ago

no direction connection from device to core brother, C is wrong, it's either B or D
upvoted 2 times

Njavwa 5 months, 3 weeks ago

Selected Answer: D

three tie, not collapsed, user to access from access to distribution from distribution to core complete three tier, from core its back to distribution, then to access.... if we remove core due to it handling traffic leaving the network, meaning we will just have access distribution back to access because no distribution to distribution connection
upvoted 1 times

daddydagoth 6 months, 3 weeks ago

Man I agree with criticism on some of the questions but how have 45% of people voted for question B when it lacks the core layer of a three tier design? What the hell people
upvoted 2 times

[Removed] 7 months, 1 week ago

I think D because the concept is Leaf Switch don't connect with Leaf Switch and Spine Switch don't connect with Spine Switch
upvoted 1 times

rijstraket 7 months, 3 weeks ago

Selected Answer: D

Distribution switches normally don't have connections to other distribution layer switches, they only connect to access layer switches and core layer switches. If you're still in doubt, search Google images for "Cisco three tier architecture".
upvoted 4 times

freeknowledge123 8 months ago

D is correct, if it were access - distribution - access b would have been correct
upvoted 2 times

Question #172 *Topic 1*

What is the difference between IPv6 unicast and anycast addressing?

A. An individual IPv6 unicast address is supported on a single interface on one node, but an IPv6 anycast address is assigned to a group of interfaces on multiple nodes.

B. IPv6 anycast nodes must be explicitly configured to recognize the anycast address, but IPv6 unicast nodes require no special configuration.

C. IPv6 unicast nodes must be explicitly configured to recognize the unicast address, but IPv6 anycast nodes require no special configuration.

D. Unlike an IPv6 anycast address, an IPv6 unicast address is assigned to a group of interfaces on multiple nodes.

Correct Answer: *A*

Community vote distribution

A (100%)

Naghini Highly Voted 8 months, 1 week ago

Aren't both A and B correct?

upvoted 5 times

kyleptt Most Recent 1 day, 11 hours ago

Selected Answer: A

A makes most sense

upvoted 1 times

mda2h 2 months, 3 weeks ago

Any one can explain why A is better than B?

upvoted 1 times

Bingchengchen236 3 months ago

Why B is not correct ?

upvoted 1 times

Ciscoman021 5 months, 1 week ago

Selected Answer: A

A is correct.

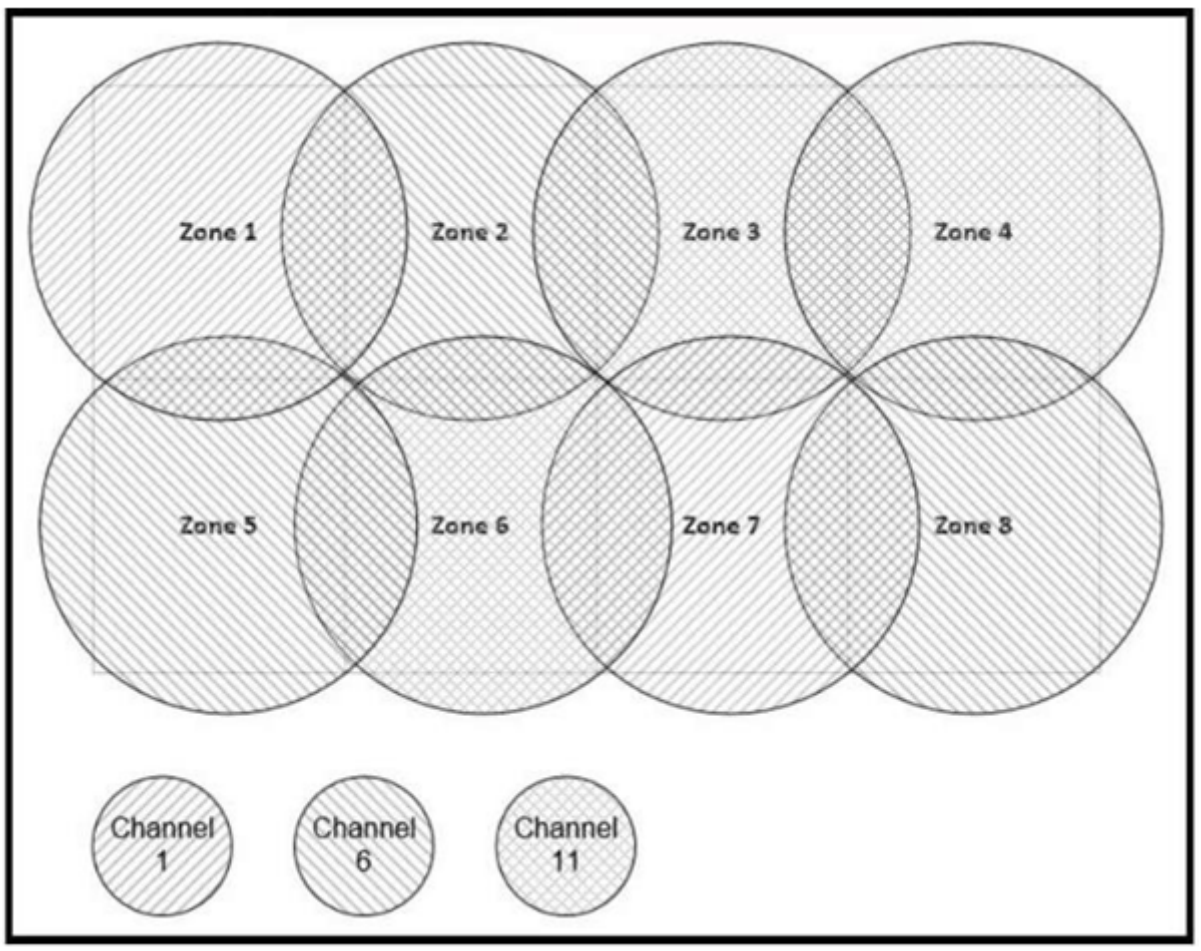
upvoted 2 times

Ceruzka 6 months, 3 weeks ago

A and B are correct. What's wrong with B?

upvoted 1 times

Question #173 *Topic 1*



Refer to the exhibit. Between which zones do wireless users expect to experience intermittent connectivity?

A. between zones 1 and 2

B. between zones 2 and 5

C. between zones 3 and 4

D. between zones 3 and 6

Correct Answer: *C*

Community vote distribution

C (100%)

rx78_2 Highly Voted 6 months, 2 weeks ago

looks like it is a vision test instead of a network exam

upvoted 18 times

soRwatches Highly Voted 6 months, 1 week ago

dafuq is this type of question?

upvoted 8 times

MelbourneJin Most Recent 2 months, 3 weeks ago

Where is the channel 11?

upvoted 1 times

xbololi 2 months, 3 weeks ago

i got a seizure thanks to this question.

upvoted 1 times

VanessaR05 3 months ago

Selected Answer: C

C is correct. Zone 3 and Zone 4 is same channel 11.

upvoted 3 times

StingVN 4 months, 2 weeks ago

Selected Answer: C

C is correct. Zone 3 and Zone 4 is same channel 11.

upvoted 2 times

daddydagoth 6 months, 3 weeks ago

Zone 3 and 4 overlap while using the same channel so answer C is correct.
The visibility of the picture is awful though

upvoted 3 times

Anas_Ahmad 8 months, 2 weeks ago

Selected Answer: C

Zones 3 and 4 both have Channel 11 and overlapped

upvoted 4 times

Anas_Ahmad 8 months, 3 weeks ago

Selected Answer: C

Zones 3 and 4 both have Channel 11 that is overlapped.
Zones 3 and 6 do not overlap at all.

upvoted 2 times

Yunus_Empire 9 months, 1 week ago

in this question: 1 is ///// and 6 is \\\\\\\\ and 11 is ####

upvoted 3 times

Yunus_Empire 9 months, 1 week ago

1 is ///// and 6 is \\\\\\\\ and 11 is ####

upvoted 2 times

ErnestoAAA 11 months ago

why is 3 and 4 zone the answer

upvoted 2 times

insulated 10 months, 4 weeks ago

I think because zone 3 and 4 both is use ch 11

upvoted 3 times

RougePotatoe 10 months, 3 weeks ago

Correct. Only 3/4 over lap with channel 11 while the other presented options do not have overlapping channels. While in real life you might not experience intermittent connection you will suffer some degradation of performance as you essential have to take turns on the channel.

upvoted 4 times

MelbourneJin 2 months, 3 weeks ago

I have no idea. Can you explain why A is not answer? For me, A and C are the same.

upvoted 1 times

mark9999 2 months ago

Look at the pattern inside the little circles at the bottom for 1, 6 and 11. The patterns are different. In answer A for zones 1 and 2 it's channels 1 and 6 which are overlapping. But zones 3 and 4 both have the channel 11 pattern. Utterly stupid framed question, if you miss the patterns you don't know what the hell's going on.

upvoted 1 times

Question #174 *Topic 1*

Which WAN topology provides a combination of simplicity quality, and availability?

A. partial mesh

B. full mesh

C. point-to-point

D. hub-and-spoke

Correct Answer: *C*

Community vote distribution

C (42%) A (38%) D (21%)

Alan100 Highly Voted 8 months ago

C is actually correct. Its P2P. According to Cisco Press, P2P (i.e Leased lines) have those exact advantages:
https://www.ciscopress.com/articles/article.asp?p=2832405&seqNum=5
upvoted 15 times

StingVN 4 months, 2 weeks ago

LOL this is Cisco test anyway. so we must follow Cisco rule.
upvoted 5 times

EliasM Highly Voted 11 months, 4 weeks ago

P2P? Shouldnt it be partial mesh? Since combines simplicity and availability, and is more available than hub and spoke.
upvoted 6 times

ccna_goat 11 months, 3 weeks ago

so-called broken question. yes, it should be partial mesh.
upvoted 5 times

Fervidales Most Recent 16 hours, 5 minutes ago

Cisco say that C is correct:
"Simplicity: Point-to-point communication links require minimal expertise to install and maintain.
Quality: Point-to-point communication links usually offer high service quality, if they have adequate bandwidth. The dedicated capacity removes latency or jitter between the endpoints.
Availability: Constant availability is essential for some applications, such as e-commerce. Point-to-point communication links provide permanent, dedicated capacity, which is required for VoIP or Video over IP."
upvoted 1 times

kyleptt 2 weeks ago

Selected Answer: C

Point to Point is simple but not to sure about reliable but C is the best answer
upvoted 1 times

MauroC19 4 weeks, 1 day ago

Selected Answer: A

IMO, answer A is correct, PARTIAL MESH. Please refer to CCNA Oficial Student Learning Guide page 217
upvoted 1 times

Cynthia2023 1 month ago

Here's why "partial mesh" might not be the preferred option:

Complexity: Partial mesh networks can become complex as the number of connections increases. Managing and maintaining the network can become challenging.

Availability: While partial mesh can provide a degree of redundancy, it might not offer the same level of availability as some other topologies. If a link between critical sites fails, there might not be alternative routes.

Quality: The quality of the connections might vary based on the specific links established in the partial mesh. Some connections might have higher latency or lower bandwidth than others.
upvoted 1 times

Cynthia2023 1 month ago

The main reason "point-to-point" might not have been selected as the answer in this case could be due to the phrasing of the question and the possible comparison with the other options provided. "Point-to-point" is often considered simple and straightforward, but in terms of availability, it might lack redundancy compared to a "hub-and-spoke" topology where multiple remote sites connect to a central hub, which can provide better failover options.
upvoted 1 times

BarkingSpider 1 month, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

zFlyingLotusz 1 month, 3 weeks ago

In the context of the CCNA (Cisco Certified Network Associate) certification, redundancy and availability are related concepts, but they are not exactly the same thing.

Redundancy refers to the use of duplicate components or backup systems to ensure continued operation in case of a failure. Redundancy is often implemented to minimize downtime and increase fault tolerance. For example, in a redundant network design, there might be multiple switches or routers providing backup paths in case the primary ones fail.

Availability, on the other hand, is a measure of how accessible and reliable a network or system is to users. It indicates the percentage of time a network or system is operational and accessible to users. High availability means that the network or system is up and running most of the time, with minimal downtime.

upvoted 1 times

dropspablo 1 month, 3 weeks ago

Selected Answer: C

I agree with splashy "Full mesh and even more so partial mesh from an enterprise perspective is anything but simple. Simplicity is the keyword as it is something a SOHO for example would prefer. A dedicated point-to-point connection is still more available than a normal broadband connection (consumer) which most people and companies use (broadband) with VPN." and with alan100 link that shows advantages of "Simplicity: Point-to-point communication links require minimal expertise to install and maintain.", "Quality: Point-to-point communication links usually offer high service quality" and "Availability: Point-to-point communication links provide permanent, dedicated capacity, which is required for VoIP or Video over IP.
https://www.ciscopress.com/articles/article.asp?p=2832405&seqNum=5#:~:text=of%20Leased%20Lines-,Advantages,-Disadvantages

upvoted 1 times

[Removed] 3 months, 1 week ago

Selected Answer: C

C is correct
Simplicity : Point-to-point communication links require minimal expertise to install and maintain.

Quality : Point-to-point communication links usually offer high quality service, if they have adequate bandwidth. The dedicated capacity removes latency or jitter between the endpoints.

Availability : Constant availability is essential for some applications, such as e-commerce. Point-to-point communication links provide permanent, dedicated capacity which is required for VoIP or Video over IP.

upvoted 1 times

Jorro99404 3 months, 2 weeks ago

Selected Answer: C

I bet on P2P

upvoted 1 times

Isuzu 4 months, 1 week ago

Selected Answer: D

The WAN topology that provides a combination of simplicity, quality, and availability is the hub-and-spoke topology.

In a hub-and-spoke topology, all traffic flows through a central hub, which simplifies the network design and makes it easier to manage. This topology also provides high availability, as failure of any one spoke does not impact the entire network.

Additionally, the hub-and-spoke topology can provide high quality of service (QoS) by allowing for centralized management and control of bandwidth allocation and traffic prioritization.

Partial mesh and full mesh topologies can provide more redundancy and fault tolerance, but they can be more complex to design and manage. Point-to-point topologies are simple, but they lack redundancy and are less fault tolerant than other topologies.

upvoted 1 times

omid8719 4 months, 3 weeks ago

Selected Answer: D

the advantage of hub and spoke

upvoted 1 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: D

D. Hub-and-spoke topology provides a combination of simplicity, quality, and availability in WAN (Wide Area Network) connectivity.

In a hub-and-spoke topology, all traffic flows between remote sites and a central hub. The hub acts as a central point of management and serves as a gateway for all communication between remote sites. This topology offers simplicity because it is easy to manage and maintain. It provides quality by providing a dedicated connection between the hub and remote sites. It also offers high availability because if one remote site goes down, it does not affect the connectivity of other sites.

Partial mesh and full mesh topologies provide higher redundancy but are more complex and expensive to implement. Point-to-point topology only provides connectivity between two endpoints, so it does not offer the same level of flexibility and scalability as hub-and-spoke topology.

upvoted 1 times

elixirwell 5 months, 3 weeks ago

Selected Answer: C

D. Hub-and-spoke topology provides a combination of simplicity, quality, and availability.

In a hub-and-spoke topology, all traffic flows through a central hub, which simplifies network design and management. The hub can be a router, switch, or any other network device that provides connectivity to the spokes. The spokes are the remote sites that are connected to the hub.

The hub-and-spoke topology provides high-quality connections because each spoke has a dedicated connection to the hub. This dedicated connection ensures that there is no contention for bandwidth between different spokes, which can cause packet loss and delay.

Moreover, the hub-and-spoke topology provides high availability because if one spoke fails, the other spokes can continue to communicate with each other through the hub. Additionally, if the hub fails, the spokes can still communicate with each other using backup links or alternate routes.

Therefore, the hub-and-spoke topology is a popular choice for WAN deployments because it provides a good balance between simplicity, quality, and availability.

upvoted 2 times

deluxeccna 5 months ago

thanks, ChatGPT

upvoted 4 times

checkoboy88 6 months, 2 weeks ago

Selected Answer: C

guys... i think the keyword here is "WAN".. this question is related to WAN connections topic.. What Alan100 says is correct.. go and read the article he pasted:

https://www.ciscopress.com/articles/article.asp?p=2832405&seqNum=5

ctrl + F and point-to-point

search for advantages and disadvantages... P2P simplicity and availability

upvoted 3 times

Dutch012 6 months, 4 weeks ago

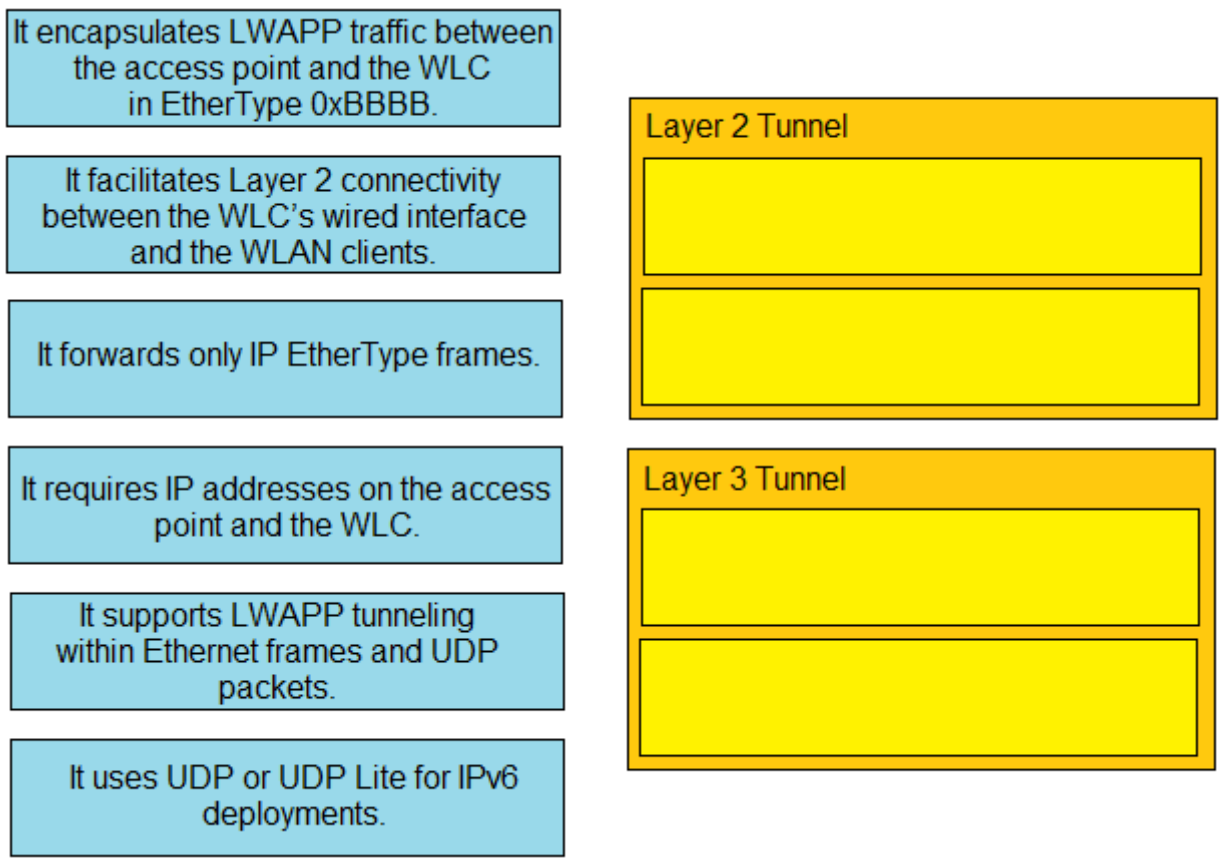
in the hub-and-spoke topology, if the hub goes down or a link from a hub to a PC or switch goes down, the subnet will lose the connection, I think A is the correct one.

upvoted 1 times

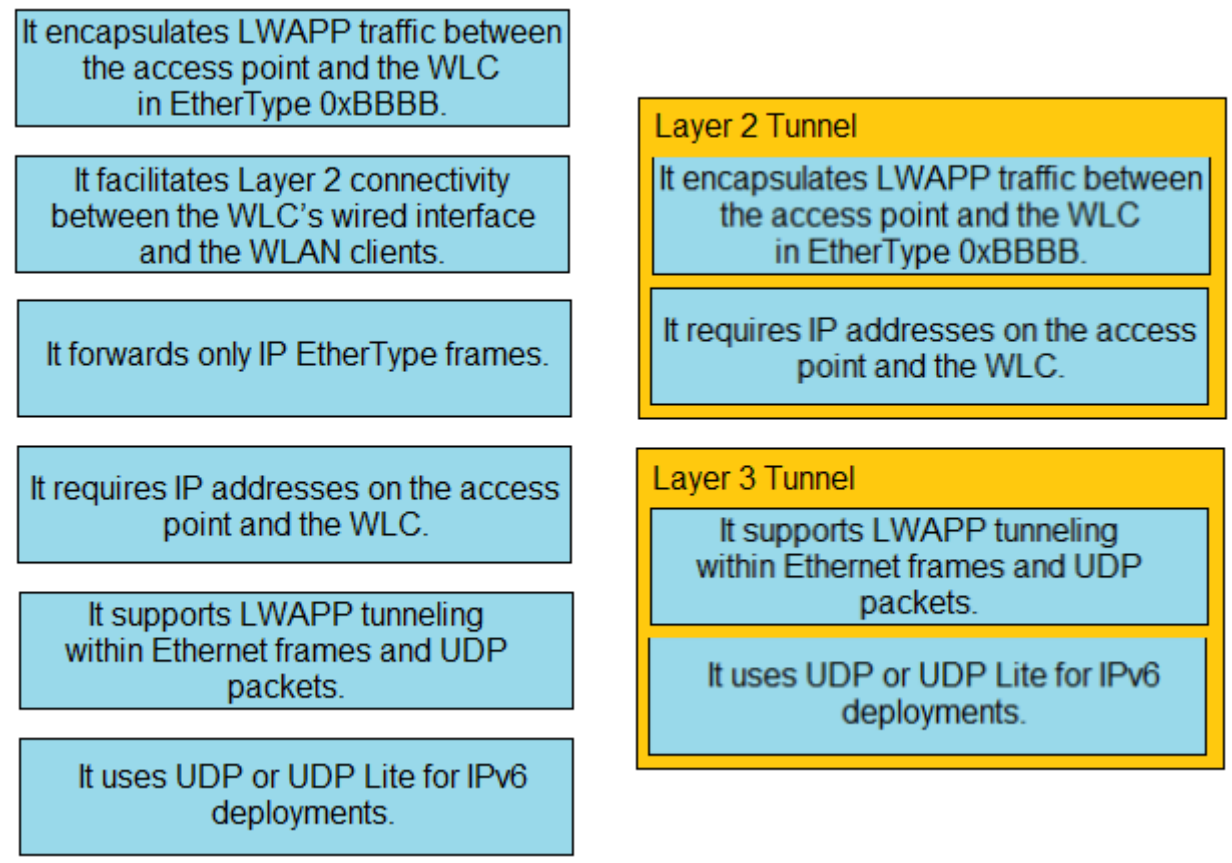
DRAG DROP -

Drag and drop the statements about wireless architectures from the left onto the architectures on the right.

Select and Place:



Correct Answer:



RougePotatoe Highly Voted 10 months, 1 week ago

Does anyone have any insights to this question? Couldn't find anything mentioning anything related to the answers in the cert guide.

upvoted 6 times

Yasyas86 10 months ago

Answers giving are correct

https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/TechArch.pdf

upvoted 12 times

PlsLetMePass Most Recent 1 month ago

The correct answer is:

Layer 2 Tunnel:
Facilitates Layer 2 connectivity between the WLC's wired interface and the WLAN clients.
Encapsulates LWAPP traffic between the access point and the WLC in Ethernet 0xBBBB.

Layer 3 Tunnel:
Requires IP addresses on the access point and the WLC.
Uses UDP or UDP Lite for IPv6 deployments.

The reason why "It forwards only IP EtherType frames" and "It supports LWAPP tunneling within Ethernet frames and UDP packets." are wrong because the CCNA exam is testing your knowledge of the different wireless architectures. These two points do not describe any specific wireless architecture. They simply describe the general features of a Layer 2 tunnel.

The correct answer for the CCNA question describes the specific features of the two wireless architectures: Layer 2 Tunnel and Layer 3 Tunnel. This is the information that the CCNA exam is testing you on.

upvoted 2 times

daddydagoth 6 months, 3 weeks ago

Not related to CCNA 200-301...

upvoted 3 times

[Removed] 7 months ago

I think this kind of question is not in CCNA 200-301 exam topic

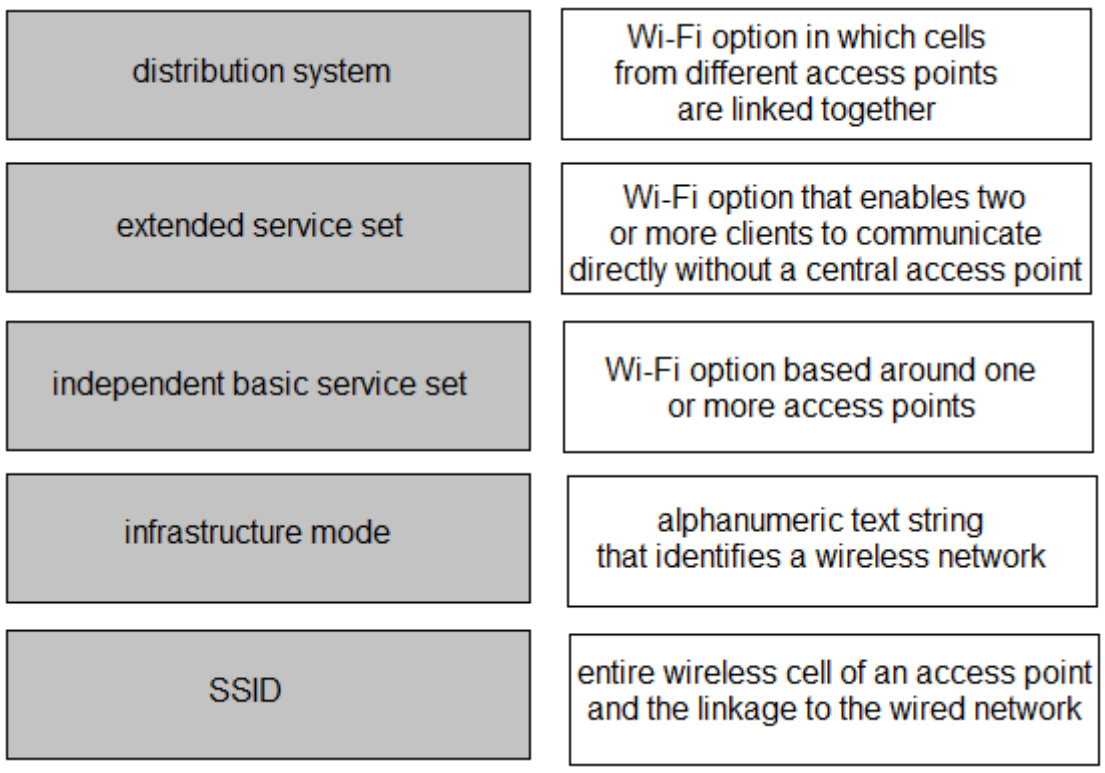
upvoted 4 times

Question #176 *Topic 1*

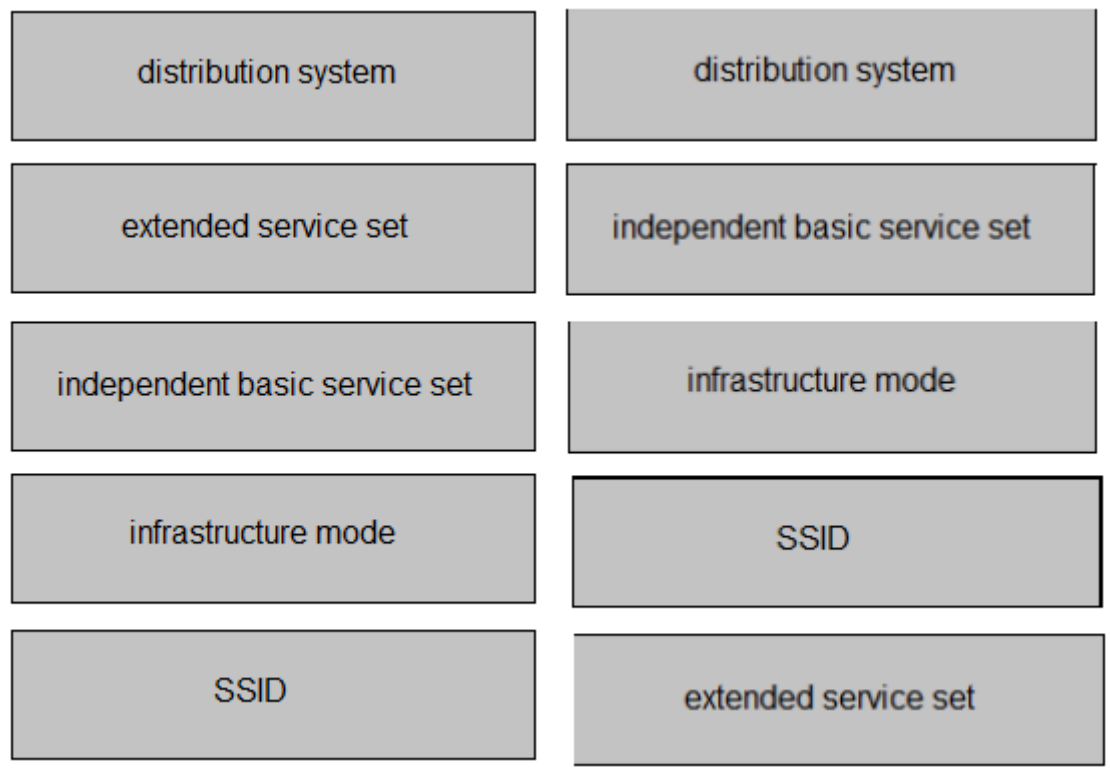
DRAG DROP -

Drag and drop the Wi-Fi terms from the left onto the descriptions on the right.

Select and Place:



Correct Answer:



splashy Highly Voted 1 year ago

I think it should be

Extended service set
Independant basic service set
Infrastructure mode
SSID
Distribution system

https://networklessons.com/cisco/ccna-200-301/wireless-lan-802-11-service-sets

upvoted 44 times

Mewkzz 12 months ago

I concur same order based on the URL shared.

upvoted 1 times

Msandie Most Recent 2 months, 2 weeks ago

Extended service set
IBSS
Infrastructure mode
SSID
Distribution

upvoted 1 times

dropspablo 4 months, 2 weeks ago

According to ChatGPT, the Distribution system and Extended service set are reversed, as follows:

Distribution system: Entire wireless cell of an access point and the linkage to the wired network.

Extended service set: Wi-Fi option in which cells from different access points are linked together.

Independent basic service set: Wi-Fi option that enables two or more clients to communicate directly without a central access point.

Infrastructure mode: Wi-Fi option based around one or more access points.

SSID: Alphanumeric text string that identifies a wireless network.

upvoted 1 times

dropspablo 4 months, 2 weeks ago

Also according to the textbooks, the Distribution System is the wired link that connects the switche to the APs - this I had already studied. So I see that it is inverted with ESS.

upvoted 1 times

dearc 5 months, 2 weeks ago

AI said:
The matches are:

distribution system: entire wireless cell of an access point and the linkage to the wired network
extended service set: Wi-Fi option in which cells from different access points are linked together
independent basic service set: Wi-Fi option that enables two or more clients to communicate directly without a central access point
infrastructure mode: Wi-Fi option based around one or more access points
SSID: alphanumeric text string that identifies a wireless network

upvoted 3 times

Njavwa 5 months, 3 weeks ago

the answers are correct check your Netacad notes
WLAN CONCEPTS
CHAPTER 12

upvoted 2 times

oatmealturkey 6 months, 3 weeks ago

Based on the OCG, I believe that this is correct:

Wi-Fi option based around one or more access points: Infrastructure mode
Wi-Fi option in which cells from different access points are linked together: Extended service set
Alphanumeric text string that identifies a wireless network: SSID
Wi-Fi option that enables two or more clients to communicate directly without a central access point: Independent basic service set
Entire wireless cell of an access point and the linkage to the wired network: Distribution system

upvoted 2 times

freeknowledge123 8 months, 2 weeks ago

again with the voodo question: think it through
ESS: relates to how WAPs are connected together: wifi option in which cells from different link are linked together
independant basic service set: it 's ad hoc devices connect to each other not through a wap: wifi option enabling communication directly without a wap
infrastructure mode: clients connecting to a wap: entire wireless cell and the linkage to the wired entwork (most logical)
SSID: a string of alphanumerical letters
distribution system: last option, havent heard of it
questions like these is why sites like exam topic are valuable

upvoted 1 times

jibon_22 9 months, 1 week ago

The Correct answer is:
> Distribution System
> IBSS
> ESS
> SSID
>Infrastructure Mode

upvoted 2 times

jibon_22 9 months, 1 week ago

Correction:
> ESS
> IBSS
> Distribution System
> SSID
> Infrastructure Mode

upvoted 2 times

everchosen13 11 months, 3 weeks ago

I think it is Infrastructure mode and Extended Service set that need to be switched

upvoted 2 times

everchosen13 11 months, 3 weeks ago

https://www.lifewire.com/infrastructure-mode-in-wireless-networking-816539

upvoted 1 times

nick9898 11 months, 3 weeks ago

this is a great article on this.
some spelling errors but otherwise a good read.
https://ipcisco.com/lesson/wireless-principles/

upvoted 2 times

PiotrMar 1 year ago

I think that in the answer: infrastructure mode and extended service set should be swapped.

upvoted 4 times

g_mindset 1 year ago

On the answer you need to swap the extended service set and distribution system

upvoted 3 times

Question #177 *Topic 1*

How are the switches in a spine-and-leaf topology interconnected?

A. Each leaf switch is connected to one of the spine switches

B. Each leaf switch is connected to each spine switch.

C. Each leaf switch is connected to two spine switches, making a loop.

D. Each leaf switch is connected to a central leaf switch, then uplinked to a core spine switch.

Correct Answer: *B*

Community vote distribution

B (85%) C (15%)

Vlad_Is_Love_ua Highly Voted 1 year ago

Selected Answer: B

In spine-leaf two-tier architecture, every lower-tier switch (leaf layer) is connected to each of the top-tier switches (spine layer) in a full-mesh topology. The leaf layer consists of access switches that connect to devices such as servers. The spine layer is the backbone of the network and is responsible for interconnecting all leaf switches. Every leaf switch connects to every spine switch. Typically a Layer 3 network is established between leaves and spines, so all the links can be used simultaneously.

upvoted 6 times

Hanagaki_Shinjiro Most Recent 20 hours, 59 minutes ago

Selected Answer: B

B is correct

upvoted 1 times

VanessaR05 3 months ago

Selected Answer: B

https://community.cisco.com/t5/blogs-routing-y-switching/caracter%C3%ADsticas-avanzadas-de-spanningtree-portfast-bpdu-guard-y/ba-p/3104851

PortFast permite que el puerto entre en un estado de Forwarding inmediatamente, pasando por alto los estados Listening y Learning.

upvoted 1 times

Isuzu 4 months, 1 week ago

Selected Answer: B

In a spine-and-leaf topology, each leaf switch is connected to every spine switch, which is option B. This design provides high bandwidth, redundancy, and low latency between the end hosts connected to the leaf switches and enables east-west traffic to traverse the network fabric in a non-blocking manner. The spine switches act as a high-speed backplane, while the leaf switches provide access ports to end hosts.

upvoted 1 times

Ciscoman021 5 months, 1 week ago

Selected Answer: B

In a spine-and-leaf topology, each leaf switch is typically connected to each spine switch, making answer B the correct choice. This provides multiple paths between any pair of devices, allowing for high bandwidth and redundancy in the network. The spine switches act as a central point of connectivity, while the leaf switches connect end devices such as servers, storage devices, or access switches. This architecture is commonly used in data center networks because it is scalable, flexible, and resilient.

upvoted 1 times

iMo7ed 7 months ago

Selected Answer: B

B is correct

upvoted 1 times

binrayelias 8 months ago

B since each leaf is needed to connect to each spine and not connect to any leaf switch

upvoted 1 times

DixieNormus 1 year ago

Answer B is correct.
https://community.fs.com/blog/leaf-spine-with-fs-com-switches.html
Each leaf switch connects to all spine switches, which creates a large non-blocking fabric, increasing the level of redundancy and reducing traffic bottlenecks.

upvoted 1 times

mrgreat 1 year ago

Selected Answer: C

Answer C is correct
https://community.fs.com/blog/leaf-spine-with-fs-com-switches.html

upvoted 2 times

Request7108 8 months, 4 weeks ago

It is not C because every leaf must connect to every spine, not just two and it's not a loop.

upvoted 4 times

Question #178 *Topic 1*

What is the primary effect of the spanning-tree portfast command?

A. It immediately enables the port in the listening state.

B. It immediately puts the port into the forwarding state when the switch is reloaded.

C. It enables BPDU messages.

D. It minimizes spanning-tree convergence time.

Correct Answer: *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_55_se/configuration/guide/3560_scg/swstpopt.html

Community vote distribution
D (58%) B (42%)

Tidestar Highly Voted 3 years, 2 months ago
I believe D is the right answer. When you enable PortFast on the switch, spanning tree places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states. If answer B did not say " when the switch is reloaded" then it would have been the correct answer.
upvoted 48 times

Tag Highly Voted 3 years, 3 months ago
guys, note, the question asks, what is the "primary" effect. Which would be D
upvoted 21 times

JWMcInSC 3 years, 3 months ago
Agreed: Because the purpose of Port Fast is to minimize the time interfaces must wait for spanning-tree to converge, it is effective only when used on interfaces connected to end stations.
upvoted 4 times

Salem2020s 2 years, 3 months ago
as long as Portfast is used for ports connected to end stations, then there is no point to ask about the effects of spanning-tree procces, i think its a tricky qusetion
upvoted 3 times

kyleptt Most Recent 2 weeks ago
No need to reload the switch once you set port Fast the port will forward immediately.
upvoted 1 times

Cynthia2023 1 month ago
Selected Answer: B
The "spanning-tree portfast" command is used to configure a port as an edge port, typically for end-user devices like computers or IP phones. When this command is applied to a port, it bypasses the normal Spanning Tree Protocol (STP) listening and learning states and immediately transitions the port to the forwarding state as soon as it's activated or the switch is reloaded.

This helps to minimize the time it takes for devices to gain network connectivity after they are powered on or connected to the network. The primary effect of the "spanning-tree portfast" command is to quickly enable the port and put it into the forwarding state to allow network traffic to flow without the delay introduced by the STP convergence process.

(D) While portfast can contribute to minimizing spanning-tree convergence time by immediately transitioning ports, the primary effect is not about overall convergence time.
upvoted 1 times

Cynthia2023 1 month ago
The "spanning-tree portfast" command is used to configure a port as an edge port, typically for devices that do not participate in Spanning Tree Protocol (STP) such as end-user devices like computers or IP phones.
upvoted 1 times

nzieno 1 month ago
D is the correct answer. B is slightly correct however a switch does not need to be reloaded for it to work.
upvoted 1 times

Paul889 2 months ago
D is the best answer however, really unfair set of choices
upvoted 1 times

davidmdlp85 2 months ago

Sound like B is also an answer

Port Fast immediately brings an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. You can use Port Fast on interfaces connected to a single workstation or server, as shown in Figure 18-1, to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge.

Interfaces connected to a single workstation or server should not receive bridge protocol data units (BPDUs). An interface with Port Fast enabled goes through the normal cycle of spanning-tree status changes when the switch is restarted.

upvoted 1 times

Danishh 2 months, 1 week ago

Selected Answer: D

PortFast is a feature can be used to speed up convergence on ports which are connected to a workstation on a server(which will not cause layer 2 loops)
enable
#configure terminal
#interface fa0/1 -15
#switchport mode access
#spanning-tree portfast
#exit

TO CHECK SPANNING TREE PORTFAST enabled ports
Sw#show running-config

upvoted 1 times

ccna_exam 2 months, 3 weeks ago

Selected Answer: B

The spanning-tree portfast command immediately puts the port into the forwarding state when the switch is reloaded. So the answer is B.

The listening and learning states are bypassed when the spanning-tree portfast command is used. This minimizes the spanning-tree convergence time, which is the time it takes for a switch to detect a topology change and converge to a new spanning-tree topology.

BPDU messages are used by the Spanning Tree Protocol (STP) to communicate between switches. The spanning-tree portfast command does not affect BPDU messages.

Therefore, the primary effect of the spanning-tree portfast command is to minimize spanning-tree convergence time by immediately putting the port into the forwarding state.

upvoted 1 times

xbololi 2 months, 3 weeks ago

It asks for effect...

upvoted 1 times

Danishh 2 months, 3 weeks ago

Portfast feature causes a switch port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states.

upvoted 1 times

VanessaR05 3 months ago

Selected Answer: B

https://community.cisco.com/t5/blogs-routing-y-switching/caracter%C3%ADsticas-avanzadas-de-spanningtree-portfast-bpdu-guard-y/ba-p/3104851

PortFast permite que el puerto entre en un estado de Forwarding inmediatamente, pasando por alto los estados Listening y Learning.

upvoted 1 times

Isuzu 4 months, 1 week ago

Selected Answer: B

The primary effect of the "spanning-tree portfast" command is to immediately transition a port from the blocking state to the forwarding state when the switch port is enabled. This is useful for ports that are connected to end devices, such as PCs or servers, which do not participate in the Spanning Tree Protocol (STP) and do not need to wait for the full STP convergence process. Portfast can reduce the time it takes for end devices to get network connectivity and minimize the risk of connectivity issues caused by spanning tree loop avoidance mechanisms. Therefore, option B is the correct answer. Option A is not accurate because the "listening" state is a transient state during the STP convergence process and Portfast does not skip it. Option C is incorrect because Portfast is not related to enabling or disabling BPDU messages. Option D is partially correct, as Portfast can minimize the STP convergence time for the specific ports where it is enabled, but it does not affect the overall STP convergence time.

upvoted 2 times

hamish88 5 months ago

When a switch is reloaded means when the STP process kicks in. It is not said we need to reload the switch to have the portfast feature work. The convergence time for STP is 40-50 seconds and for RSTP is 5-10 seconds. Portfast doesn't make them any faster. Finally, we all enable portfast to have a port up and running immediately without having it go through listening, learning, etc states. Don't care if the switch is reloaded, or unplugged, there is a power outage, water damage, earthquake, etc.

upvoted 1 times

freeknowledge123 8 months, 2 weeks ago

Selected Answer: D

switch doesn't need to reload for portfast to take effect

upvoted 2 times

jibon_22 9 months, 1 week ago

Look at the words "primary effect". Correct answer is:
> B

upvoted 1 times

AppleShredder011 11 months, 4 weeks ago

The answer is D. Portfast puts interface FROM blocking TO forwarding and not FROM a device restart. B is for Uplinkfast which puts the interface to forwarding right after reloading or a restart.

upvoted 1 times

Question #179 *Topic 1*

What occurs when PortFast is enabled on an interface that is connected to another switch?

A. Root port choice and spanning-tree recalculation are accelerated when a switch link goes down.

B. After spanning-tree converges, PortFast shuts down any port that receives BPDUs.

C. VTP is allowed to propagate VLAN configuration information from switch to switch automatically.

D. Spanning-tree fails to detect a switching loop increasing the likelihood of broadcast storms.

Correct Answer: *D*
Enabling the PortFast feature causes a switch or a trunk port to enter the STP forwarding-state immediately or upon a linkup event, thus bypassing the listening and learning states.
Note: To enable portfast on a trunk port you need the trunk keyword ƛ€spanning-tree portfast trunkƛ€

Community vote distribution
D (100%)

ratu68 Highly Voted 1 year, 2 months ago

Selected Answer: D

There was no mention of BPDU Guard so answer is D !
upvoted 5 times

medyka Most Recent 3 days, 17 hours ago

Because the purpose of PortFast is to minimize the time that ports must wait for spanning tree to converge, you should use it only on ports that no other switch is connected to, like access ports for connecting user equipment and servers or on trunk ports when connecting to a router in a router on a stick configuration. If you enable PortFast on a port that is connecting to another switch, you risk creating a spanning tree loop, or with the BPDU guard feature enabled the port will transition in errdisable.
upvoted 1 times

kyleptt 2 weeks ago

Selected Answer: D

If BPDU Guard is off yes
upvoted 1 times

R4mzes 3 months ago

B is correct.
When PortFast is enabled on an interface that is connected to another switch, the primary effect is that PortFast shuts down any port that receives Bridge Protocol Data Units (BPDUs). BPDUs are messages exchanged between switches to establish and maintain a loop-free topology using the Spanning Tree Protocol (STP).
upvoted 1 times

kyleptt 2 months, 4 weeks ago

Only when BPDU Guard is configured so D would be correct
upvoted 2 times

ZUMY 1 year, 3 months ago

D is correct!
upvoted 2 times

kijken 1 year, 7 months ago

I think this is B. The port will go in error disbaled state when receiving PBDU messages
upvoted 3 times

kijken 1 year, 7 months ago

1 day later and a little wiser then yesterday I can tell that I was wrong. BPDU Guard needs to be enabled for that, which is not te case. So answer D is correct
upvoted 27 times

Question #180 *Topic 1*

Which QoS Profile is selected in the GUI when configuring a voice over WLAN deployment?

A. Platinum

B. Bronze

C. Gold

D. Silver

Correct Answer: *A*
Cisco Unified Wireless Network solution WLANs support four levels of QoS: Platinum/Voice, Gold/Video, Silver/Best Effort (default), and Bronze/Background.
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01010111.html

Ettmoh Highly Voted 3 years ago
WLAN Quality of Service (QoS) list:
• Platinum (voice)
• Gold (video)
• Silver (best effort) is the default value.
• Bronze (background)
upvoted 33 times

Belinda 1 year, 6 months ago
Thanks
upvoted 2 times

Samitha Highly Voted 3 years, 2 months ago
Bronze---->FTP
Gold-------->Video
Platinum--->Voice
upvoted 7 times

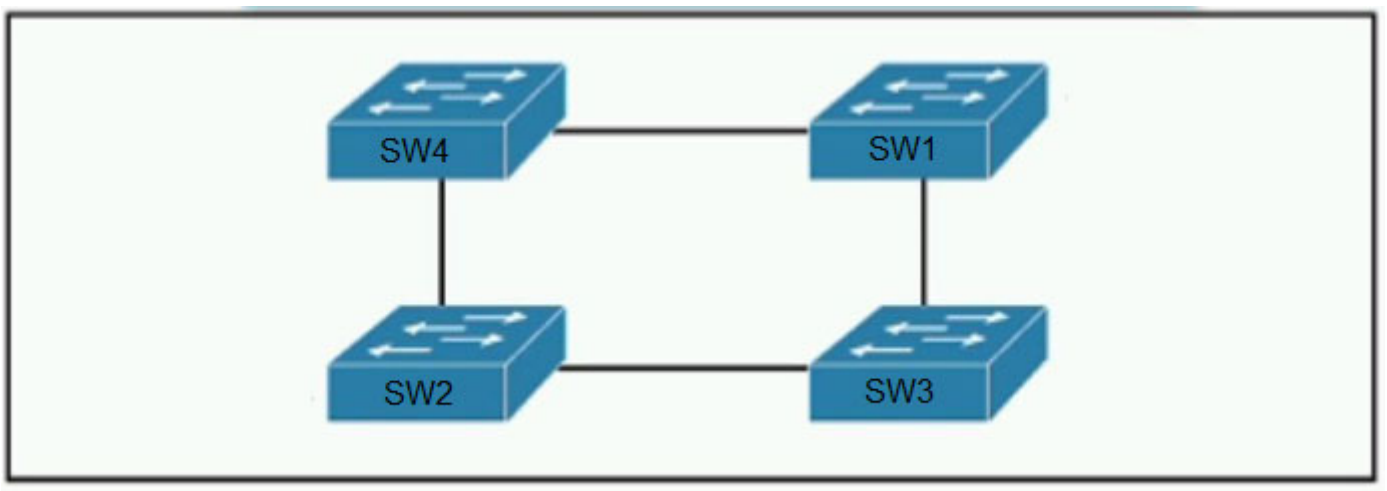
Franklin82 Most Recent 10 months, 2 weeks ago
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/81831-qos-wlc-lap.html Platinum voice
upvoted 1 times

BlankNothing1 1 year, 3 months ago
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/quality_of_service.html#ID1593
upvoted 2 times

SScott 2 years, 3 months ago
Yes Platinum is correct.
upvoted 1 times

JWMcInSC 3 years, 3 months ago
Agreed: Platinum/Voice—Ensures a high quality of service for voice over wireless.
upvoted 2 times

Question #181 *Topic 1*



Refer to the exhibit. Which switch in this configuration will be elected as the root bridge?

SW1: 0C:E0:38:41:86:07 -

SW2: 0C:0E:15:22:05:97 -

SW3: 0C:0E:15:1A:3C:9D -

SW4: 0C:E0:18:A1:B3:19 -

A. SW1

B. SW2

C. SW3

D. SW4

Correct Answer: *C*

Community vote distribution

C (100%)

Ali526 Highly Voted 2 years, 8 months ago

C is correct. '0C:0E:15:1A' is the smallest MAC. It is assumed that priority is the same for all 4 switches.

upvoted 18 times

GreatDane Highly Voted 1 year, 3 months ago

Root bridge > switch with lowest BID. The BID (bridge ID) is composed by the switch priority and by its MAC address. Since the question doesn't mention any priority, just focus on the MAC addresses and compare them "hex value- to-hex value", starting from left to right:

Switch 1 – 0C:E0:38:41:86:07
Switch 2 – 0C:0E:15:22:05:97
Switch 3 – 0C:0E:15:1A:3C:9D
Switch 4 – 0C:E0:18:A1:B3:19

The first two values are equal for all MAC addresses. Starting from the 3rd value, Switch 2 and Switch 3 have a MAC address which is lower than Switch 1 and Switch 4. Starting from the 7th value, you can see that Switch 3 is lower than Switch 4.
Answer C is correct.

upvoted 7 times

MauroC19 Most Recent 4 weeks, 1 day ago

Selected Answer: C

Answer is C. Useful link (in spanish) to enforce the concept: https://learningnetwork.cisco.com/s/article/practica-eleccion-de-roles-y-estados-de-puertos-protocolo-rapid-pvst

upvoted 1 times

[Removed] 3 months, 1 week ago

Selected Answer: C

C - It has the lowest MAC address.

upvoted 1 times

dearc 5 months, 2 weeks ago

Selected Answer: C

the decimal equivalent of the hexadecimal number 1A is 26.
the decimal equivalent of the hexadecimal number 22 is 34.

upvoted 1 times

Njavwa 5 months, 3 weeks ago

not sure why i was thinking 0(zero) is latter O

upvoted 1 times

Antol15 4 months, 3 weeks ago

Letter O doesn't exist in the hexadecimal system. It goes from 0(zero) to 9 and from A to F.
So that must be the number 0 (zero).

upvoted 2 times

DUMPledore 9 months, 1 week ago

Selected Answer: C

C correct answer

upvoted 2 times

BlankNothing1 1 year, 3 months ago

Place all the MAC addresses in Excel then sort them from smallest to largest (A-Z). You will find the answer and how to sort in Excel. You will also notice in the OCGs the numbers are listed first in the glossary and index. C is the answer.

upvoted 1 times

WowA 1 year, 3 months ago

I think your idea is great for work, but I don't think we can use exel for the exam.

upvoted 6 times

Cyberops 1 year, 4 months ago

the Switch which has the lowewst Mac address which is SW3
correct answer is C

upvoted 2 times

bmatthee01 1 year, 6 months ago

D is the answer - SW4 will become root bridge
Assuming bridge priorities are equal, tie breaker will be the lower mac address wins

SW1 and SW2 are eliminated due to high value of MAC address
SW1: 0C:E0:38:41:86:07 -
SW2: 0C:0E:15:22:05:97 -

Comparing SW3 and SW4's mac addresses, they are fairly similar until the 5th and 6th quartet , 3C=15 is higher than B3=14 and 9D=22 is higher than 19, so SW4 becomes the root bridge
SW3: 0C:0E:15:1A:3C:9D -
SW4: 0C:E0:18:A1:B3:19 -

we need to consider checking the entire mac address not just half

upvoted 1 times

Lovens 2 years, 2 months ago

C is the Answer.
1A= $(1 \times 16^1) + (10 \times 16^0) = 26$ < A1 = $(10 \times 16^1) + (1 \times 16^0) = 161$

upvoted 4 times

davletovan 2 years, 2 months ago

maybe correct answer - B?
1a = 26

upvoted 2 times

Matalongo 6 months ago

but 22 in hexadecimal is 34 in decimal

upvoted 1 times

AWSFastLearner 2 years ago

yes, $1A=26=1x16^1+10x16^0$. but $22=2x16^1+2x16^0=34$.
so 1A<22. correct answer is C.

upvoted 5 times

ZUMY 2 years, 4 months ago

C is correct
Least MAC value is selected incase of all the interface - RootBridge priorities are same

upvoted 3 times

oooMooo 2 years, 4 months ago

C is correct

Assuming Bridge Priority is the same, the lowest MAC will be elected as the root bridge.
0 is lower than E which equals 14. Eliminating SW1 and SW4.

1 is lower than 2 which equals 10. Eliminating SW2.

SW3 will be elected as the Root Bridge.

Chart: https://ptgmedia.pearsoncmg.com/images/chap7_9780136633662/elementLinks/07fig05_alt.jpg

upvoted 4 times

hippyjm 2 years, 6 months ago

i understand that the smallest mac but what would be lower 29 or 2a?
cant find a clear answer of this. how does the address increase

upvoted 2 times

Robin999 2 years, 6 months ago

2 and 2 are the same and 9 is lower then a = 29 is the lower one

upvoted 3 times

Tharwat 2 years, 6 months ago

D is the correct answer

upvoted 2 times

lordnano 2 years, 6 months ago

Without a statement why you would choose an other answer, your comment can't help anybody

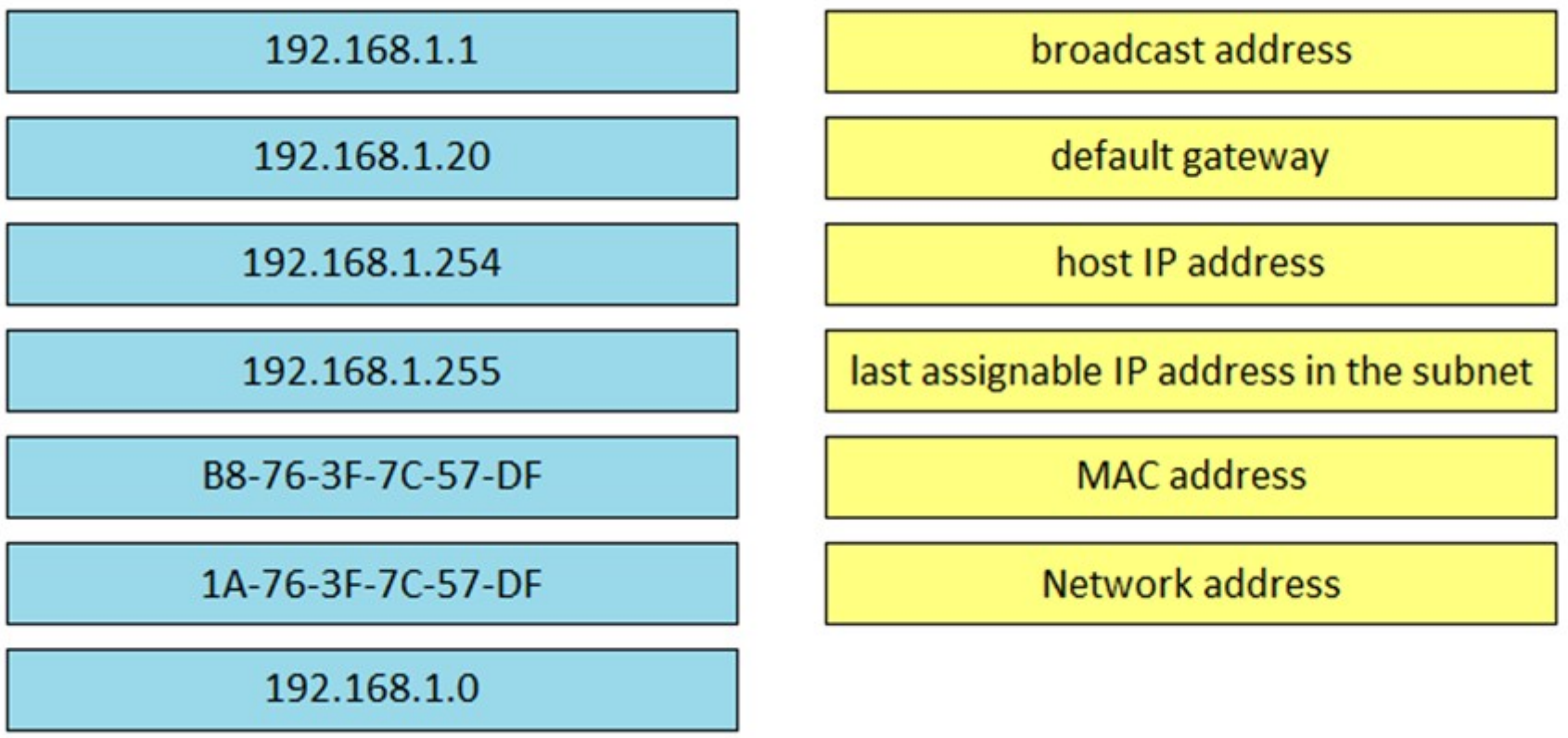
upvoted 9 times

DRAG DROP -

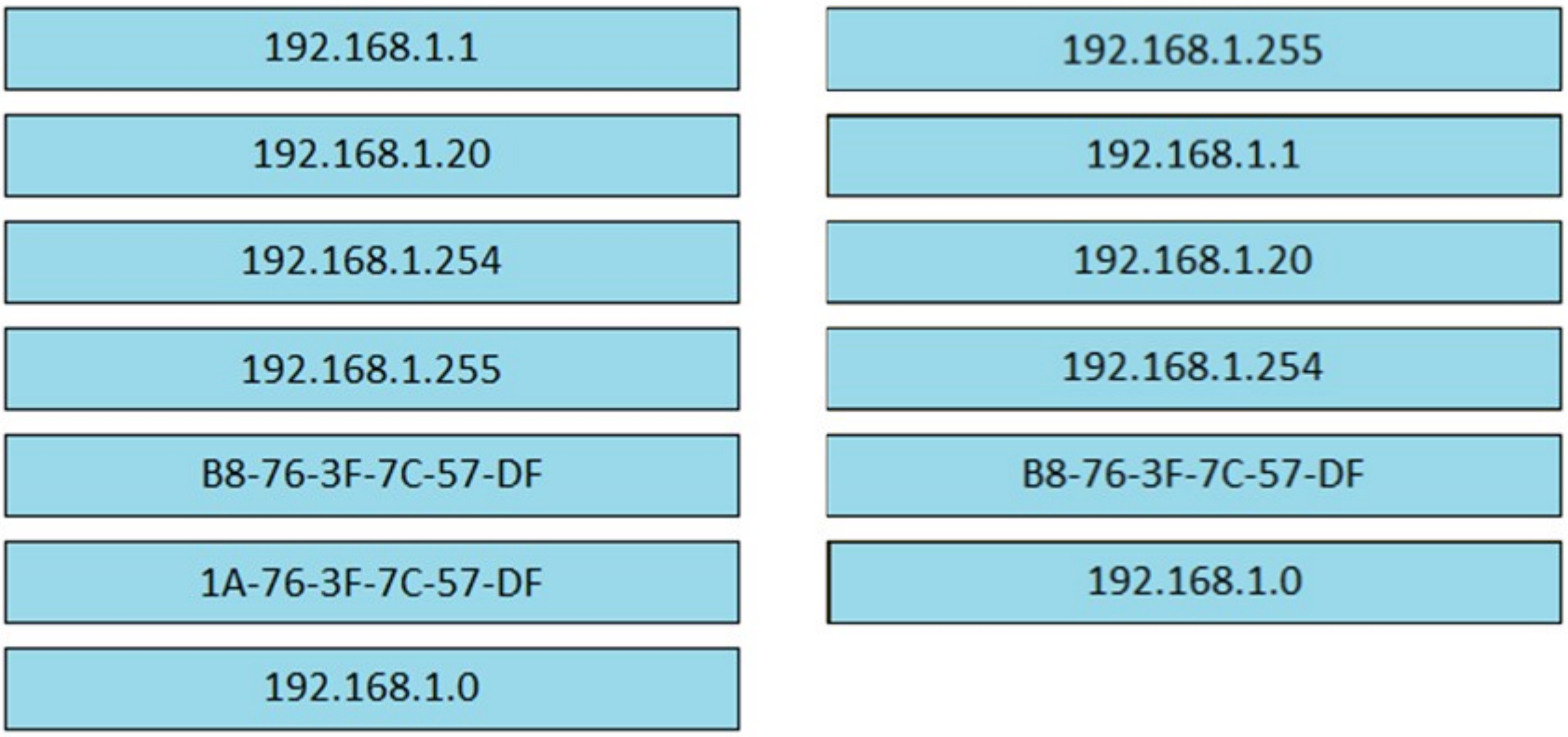
```
C:\>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Inspiron15
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 1A-76-3F-7C-57-DF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Dell Wireless 1703 802.11b/g/n <2.4GHz>
   Physical Address. . . . . . . . . : B8-76-3F-7C-57-DF
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e09f:9839:6e86:f755%12<Preferred>
                   . . . . . . . . . : 192.168.1.20<Preferred>
                   . . . . . . . . . : 255.255.255.0
                   . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 263747135
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-18-E6-32-43-B8-76-3F-7C-57-DF

                 . . . . . . . . . . : 192.168.1.15
                                       192.168.1.16
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Refer to the exhibit. An engineer is required to verify that the network parameters are valid for the users' wireless LAN connectivity on a /24 subnet. Drag and drop the values from the left onto the network parameters on the right. Not all values are used.

Select and Place:



Correct Answer:



johnnd Highly Voted 1 year, 7 months ago

Response with connection arrows:
https://i.imgur.com/qC7SZaH.png

upvoted 8 times

Adewal Highly Voted 1 year, 7 months ago

The answer is very straight forward with a good understanding of IP/subnetting.

upvoted 5 times

justy897 Most Recent 1 month, 1 week ago

wrong mac it is the mac of the AP

upvoted 2 times

Isuzu 4 months, 1 week ago

Same as Q153

upvoted 2 times

ZUMY 1 year, 3 months ago

Given answers are correct!

upvoted 4 times

Question #183 *Topic 1*

An engineer needs to configure LLDP to send the port description type length value (TLV). Which command sequence must be implemented?

A. switch(config-if)#lldp port-description

B. switch#lldp port-description

C. switch(config-line)#lldp port-description

D. switch(config)#lldp port-description

Correct Answer: *D*

Joe_Q Highly Voted 2 years, 5 months ago
The command should be:
SW(config)#lldp tlv-select port-description
upvoted 27 times

IxlJustinlxl Highly Voted 2 years, 4 months ago
Yeah... the command sucks in this question. luckily to answer this one you don't even need to look at the command. LLDP is configured from global configuration mode and only one prompt is in that mode - regardless of the command, any LLDP configuration needs to be done from global config mode.
upvoted 19 times

ajiron 1 year, 8 months ago
How about lldp transmit and lldp receive int-config commands?
upvoted 8 times

R4mzes Most Recent 3 months ago
A. switch(config-if)#lldp port-description
upvoted 1 times

[Removed] 7 months ago
I think this question will not be on ccna 200-301 exam topic.
upvoted 5 times

Anas_Ahmad 8 months, 3 weeks ago
Switch(config)#lldp tlv-select port-description
this command exist
upvoted 2 times

guisam 9 months, 1 week ago
R1(config)#lldp ?
holdtime Specify the holdtime (in sec) to be sent in packets
reinit Delay (in sec) for LLDP initialization on any interface
run Enable LLDP
timer Specify the rate at which LLDP packets are sent (in sec)
tlv-select Selection of LLDP TLVs to send

R1(config)#lldp tlv-select ?
mac-phy-cfg IEEE 802.3 MAC/Phy Configuration/status TLV
management-address Management Address TLV
port-description Port Description TLV
port-vlan Port VLAN ID TLV
power-management IEEE 802.3 DTE Power via MDI TLV
system-capabilities System Capabilities TLV
system-description System Description TLV
system-name System Name TLV
upvoted 2 times

TA77 1 year, 3 months ago
The default configured TLV is to send and receive all TLVs. To specify the port-description TLV, the following command should be used in the global configuration mode:

switch(config)#lldp tlv-select port-description
upvoted 1 times

ZUMY 1 year, 3 months ago
Going with D
The command should be:
SW(config)#lldp tlv-select port-description
upvoted 1 times

dave1992 1 year, 9 months ago

if you were configuring a port description, wouldnt you need to be at the (config-if) level?

upvoted 6 times

onikafei 1 year, 7 months ago

Tested the code multiple times in training. Renaming is just done with the config command. I almost put it in the catagory of message of the day

upvoted 1 times

kokoyul 1 year, 11 months ago

La más lógica y correcta es la letra D, debido al modo de configuración que se encuentra el prompt (global configuration).

upvoted 1 times

LordScorpius 1 year, 4 months ago

Me parece que nos estén intentando a decir lo mismo porque el comando no es correcto.

upvoted 1 times

Raymond9 2 years, 9 months ago

badly written: TLV should written as Type, Length, Value, or Type-Length-Value, since there are three different columns!

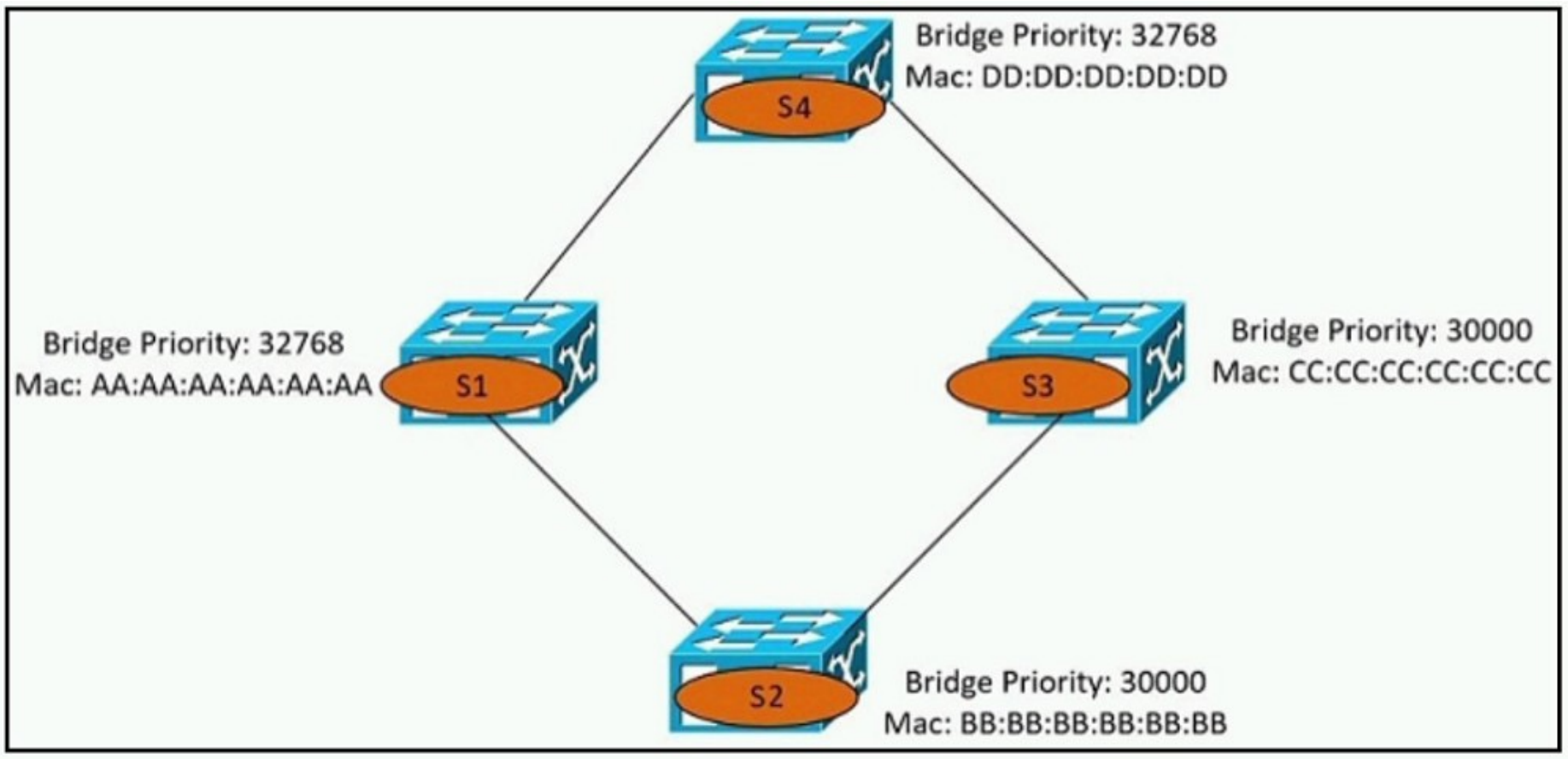
upvoted 4 times

Ali526 2 years, 8 months ago

Many of the questions are.

upvoted 3 times

Question #184 *Topic 1*



Refer to the exhibit. Which switch becomes the root bridge?

A. S1

B. S2

C. S3

D. S4

Correct Answer: *B*

Community vote distribution

A (50%) B (50%)

Ali526 Highly Voted 2 years, 8 months ago

B is correct. The lowest value of priority + MAC.

upvoted 20 times

pianetaperez 2 years, 6 months ago

If all switches in a single spanning tree have the same bridge priority, the switch with the lowest MAC address will become the root bridge.

upvoted 14 times

WeaGLe Highly Voted 1 year, 11 months ago

It Should be A.
Bridge Priority must be in increments of 4096.
Allowed values are:
0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440
A priority of 30000 is invalid.

upvoted 13 times

[Removed] 4 months, 1 week ago

How can the priority be 32768? With default VLAN 1 it should be 32769!

upvoted 1 times

kyleptt 2 months, 1 week ago

Agreed but... I assume they meant say that the invalid priorities are valid (Not sure) I am thinking we should use the valid priorities numbers .....

upvoted 1 times

MISS4 1 year, 11 months ago

" When the switch is in PVST+ mode without MAC address reduction enabled, you can enter a bridge priority value between 0-65,535. The VLAN bridge ID priority becomes that value.

When the switch is in PVST+ mode with MAC address reduction enabled, you can enter one of 16 bridge priority values: 0, 4096, 8192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, or 61,440. "

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/spantree.html

Since no mode is specified in the quesion, 30000 seems valid.

upvoted 10 times

bryanyepez92 Most Recent 3 weeks, 6 days ago

Selected Answer: A

Allowed values are:
0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440

upvoted 1 times

melmiosis 10 months, 3 weeks ago

so the priority is looked at first right... so its between S3 and S2.
then the lower MAC is chosen which is S3 cz all Cs rather than Bs.

What im i missing?

upvoted 2 times

Sutokuto 9 months ago

C is more than B

upvoted 2 times

ZUMY 1 year, 3 months ago

B is the answer
Lowest values are selected (Priority + MAC)

upvoted 1 times

onikafei 1 year, 7 months ago

Bridge priority is in the least value:

30000 narrows it down to 2 ports
Bb or cc

Bb is lowest

upvoted 1 times

Samir_123 1 year, 7 months ago

Selected Answer: B

correct

upvoted 1 times

Hodicek 1 year, 10 months ago

LOWEST PRISORITY IS THE SAME 30000 BETWEEN 2 ROUTERS, SO IT WILL CHOOSE THE LOWEST MAC ADDR. WHICH IS B

upvoted 2 times

Question #185 *Topic 1*

Which configuration ensures that the switch is always the root for VLAN 750?

A. Switch(config)#spanning-tree vlan 750 priority 38418607

B. Switch(config)#spanning-tree vlan 750 priority 0

C. Switch(config)#spanning-tree vlan 750 root primary

D. Switch(config)#spanning-tree vlan 750 priority 614440

Correct Answer: *C*

Community vote distribution

B (76%) C (24%)

Hemn1990 Highly Voted 2 years, 11 months ago

B i correct, note alwayes

upvoted 38 times

Gifu Highly Voted 2 years, 9 months ago

Although the spanning-tree vlan 750 root primary command will ensure a switch will have a bridge priority value lower than other bridges introduced to the network, the spanning-tree vlan 750 priority 0 command ensures the bridge priority takes precedence over all other priorities.

upvoted 29 times

ian77ex 1 year, 7 months ago

What about if there's other SW in the network with priority 0 as well? Maybe that other SW has a lower MAC and becomes the root switch. So the only way to be absolutely sure is by using the root primary command. The SW will check the priorities of the rest and set the lower possible on itself.

upvoted 11 times

dipanjana1990 1 year, 5 months ago

No, even if two switches have priority 0, and you run command --- spanning-tree vlan id root primary, yet root bridge among those two switches with priority 0 will selected based on MAC address, not based on this command ---spanning-tree vlan id root primary. So the correct answer would be B not C.

upvoted 3 times

picho707 Most Recent 2 weeks, 2 days ago

The answer is "Switch(config)#spanning-tree vlan 750 priority 0"
You can also use the spanning-tree vlan 750 root primary command to ensure that your switch is always the root bridge for VLAN 750. However, this command will only work if there are no other switches in the network with a lower bridge priority. If there are other switches with a lower bridge priority, the spanning-tree vlan 750 root primary command will not be effective.

upvoted 1 times

SonicVoyage 4 weeks, 1 day ago

Selected Answer: B

Tested on Cisco Catalyst 2950 and 3750. First I entered the command "spanning-tree vlan 750 priority 0" on the first switch and "spanning-tree vlan 750 root primary" on the other. The second command didn't take an effect - there was an error:
% Failed to make the bridge root for vlan 750
% It may be possible to make the bridge root by setting the priority
% for some (or all) of these instances to zero.
Then I did it vice versa (I entered the command "spanning-tree vlan 750 root primary" on the first switch and "spanning-tree vlan 750 priority 0" on the other). Even though there wasn't any error, the first command didn't take an affect - the second switch became the root bridge with priority 0 and the first one's priority was 24576 so option B is correct.

upvoted 1 times

MauroC19 4 weeks, 1 day ago

Selected Answer: B

I'm going with answer B. Seems to be a stronger method to manually set the priority to 0
https://community.cisco.com/t5/switching/root-primary-or-setting-switch-priority-to-0/m-p/4606938#M523471

upvoted 1 times

TEO1221768548956 1 month, 4 weeks ago

Selected Answer: B

I googled the answer on ITExams.net and it says the answer is B,
"Explanation: Although the spanning-tree vlan 10 root primary command will ensure a switch will have a bridge priority value lower than other bridges introduced to the network, the spanning-tree vlan 10 priority 0 command ensures the bridge priority takes precedence over all other priorities."
https://itexamanswers.net/question/which-configuration-ensures-that-the-switch-is-always-the-root-for-vlan-750#google_vignette

upvoted 1 times

Natalie89 1 month, 4 weeks ago

C is correct.

Option B (Switch(config)#spanning-tree vlan 750 priority 0) sets the priority to 0, which is the lowest value. However, it does not explicitly declare the switch as the root bridge. It relies on the default tie-breaker mechanism to determine the root bridge, which may not always result in the switch being chosen as the root.

upvoted 1 times

lamm 2 months ago

Selected Answer: C

whith this command it looks for actively being the root on this vlan.

upvoted 1 times

Jorro99404 3 months, 2 weeks ago

Selected Answer: B

Who votes for C? And why?
'root primary' command will set the bridge priority to 24576

upvoted 1 times

Shun5566 3 months, 3 weeks ago

Selected Answer: B

B is always correct

upvoted 2 times

Ioannis_Vos 4 months, 1 week ago

If a new switch is added to the network and has priority 0 and lower MAC than the root bridge then this will be elected as the root bridge. I believe the right answer is C.

upvoted 2 times

FALARASTA 5 months ago

Selected Answer: B

To prevent having a suboptimal network, we need to manually choose a root bridge within the network. By doing that, we need to manually configure a value of the root bridge or manually assign it as a root bridge by using the 'root primary' command. This will set the bridge priority to 24576, which is lower than the default priority.

What if the primary root bridge fails? To optimize further, we need to assign the other core switch as the secondary root bridge in case the primary root bridge is not operational. To do that, we enter the 'root secondary' command. This will set the bridge priority to 28672, which is lower than the default priority but higher than the root primary. When the primary switch fails, the switches will elect a new root bridge. It will then failover to the secondary switch, and it will be elected as the new root bridge.

So the priority value set for primary root command is higher than 0. The answer is B

https://study-ccna.com/spanning-tree-priority-root-primary-secondary/

upvoted 1 times

FALARASTA 5 months ago

From ChaGPT

Option C is the correct configuration to ensure that the switch is always the root for VLAN 750.

The "root primary" command configures the switch to actively try to become the root bridge for the specified VLAN. This command will automatically set the switch's priority to the lowest possible value (i.e. 0), making it the root bridge for that VLAN.

Option A sets a specific priority for the switch for VLAN 750, but there's no guarantee that this priority will be lower than the priorities of other switches in the network. Option B sets the priority to 0, which is the lowest possible value, but this configuration will not actively make the switch the root bridge. Option D sets a specific priority for the switch, but again, there's no guarantee that this priority will be lower than the priorities of other switches in the network.

upvoted 1 times

FALARASTA 5 months ago

I wonder which books I've been reading because, when the prority is set to 0, that switch automatically becomes the root. And in this case it is administratively configured. I still think the answer is B

upvoted 1 times

elixirwell 5 months, 3 weeks ago

Selected Answer: B

The correct configuration to ensure that the switch is always the root for VLAN 750 is option B, Switch(config)#spanning-tree vlan 750 priority 0.

Explanation:

In a Spanning Tree Protocol (STP) network, the switch with the lowest bridge priority value is elected as the root bridge for a particular VLAN. The lower the bridge priority value, the higher the priority of the switch in the network. Option B sets the bridge priority value to 0, which ensures that the switch is always the root for VLAN 750, regardless of the other switches' bridge priority values.
Option A sets the bridge priority value to 38418607, which is a lower value than the default but may not necessarily guarantee that the switch will always be the root bridge for VLAN 750.
Option C uses the root primary command, which makes the switch a primary root bridge for all VLANs, not just VLAN 750.

Option D sets the bridge priority value to 614440, which is higher than the default value and would make the switch less likely to be elected as the root bridge.

upvoted 2 times

linuxlife 6 months ago

B is the correct answer.
spanning-tree vlan 750 priority 0
result: spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 750 priority 0

Switch(config)#spanning-tree vlan 750 priority 0
result: spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 750 priority 24576

upvoted 1 times

linuxlife 6 months ago

B is the correct answer.
Switch(config)#spanning-tree vlan 750 priority 0
result: spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 750 priority 0

Switch(config)#spanning-tree vlan 750 priority 0
result: spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 750 priority 24576

upvoted 1 times

cpinac 6 months, 1 week ago

Selected Answer: B

https://www.ciscopress.com/articles/article.asp?p=2995351&seqNum=2

Key topic: The best way to prevent erroneous devices from taking over the STP root role is to set the priority to 0 for the primary root switch and to 4096 for the secondary root switch.

upvoted 2 times

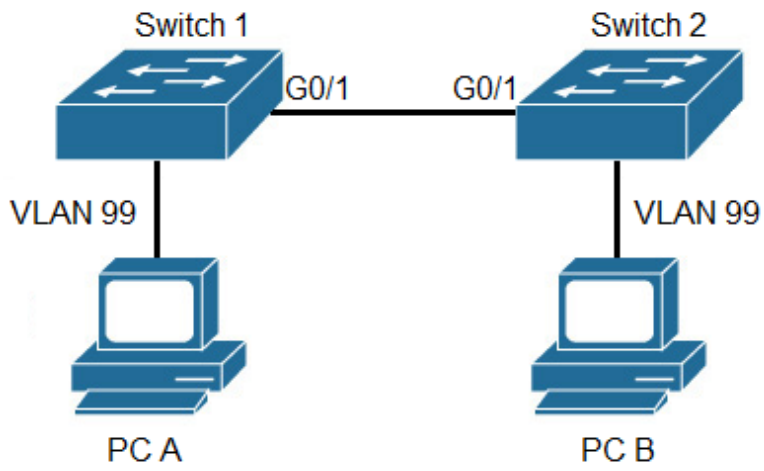
iMo7ed 7 months ago

Selected Answer: B

It's B

upvoted 1 times

Question #186 *Topic 1*



Switch 1:

```
Name: Gi0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
[output omitted]
Trunking VLANs Enabled: 50-100
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Switch 2:

```
Name: Gi0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
[output omitted]
Trunking VLANs Enabled: 50-100
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Refer to the exhibit. After the switch configuration, the ping test fails between PC A and PC B. Based on the output for switch 1, which error must be corrected?

A. The PCs are in the incorrect VLAN.

B. All VLANs are not enabled on the trunk.

C. Access mode is configured on the switch ports.

D. There is a native VLAN mismatch.

Correct Answer: *D*

Community vote distribution

D (100%)

Kane4555 Highly Voted 1 year, 8 months ago

Selected Answer: D

Don't overthink it, this is the CCNA, the CCNA says that native VLAN mismatches are bad, and there's a native VLAN mismatch. D.

upvoted 9 times

dipanjana1990 1 year, 1 month ago

can't anybody see that Native Vlan Tagging is enabled on both the switches, so native vlan traffic will go tagged on the trunk port. But allowed vlans on the trunk port is 50-100 whereas the both PC-A and PC-B belongs to vlan A so their traffic won't be allowed on the trunk port. So the correct answer should be B.

upvoted 2 times

freezeladmsflmaldfs 2 months, 2 weeks ago

Hi, wanted to input that this makes absolutely no sense at all.

upvoted 1 times

FALARASTA Most Recent 5 months ago

Selected Answer: D

There is VLAN Mismatch. Remember there is no any intervlan routing on the two sitches thus minimising the chance of communication.

Answer is D

https://www.youtube.com/watch?v=klqpX6U-_JY

upvoted 1 times

elixirwell 5 months, 3 weeks ago

Selected Answer: D

ChatGPT says,
Based on the output for switch 1, the error that must be corrected in order for the ping test to be successful between PC A and PC B is option D, "There is a native VLAN mismatch."

Explanation:

The output of the show interfaces trunk command on Switch 1 shows that the trunk link between Switch 1 and Switch 2 is configured with a native VLAN of 10 on Switch 1 and a native VLAN of 20 on Switch 2. This is a native VLAN mismatch, which can cause issues with VLAN traffic crossing the trunk link.

In this scenario, PC A is in VLAN 10 and PC B is in VLAN 20. When the switch receives traffic from PC A, it tags the traffic with VLAN 10, but when the traffic crosses the trunk link to Switch 2, the traffic is sent on the native VLAN 20, which Switch 2 is expecting to receive traffic on. As a result, the traffic from PC A is dropped and the ping test fails.

To correct this error, the native VLAN on the trunk link between Switch 1 and Switch 2 should be the same on both switches. Either the native VLAN should be changed to 10 on both switches or it should be changed to 20 on both switches.

upvoted 1 times

dipanjana1990 1 year, 1 month ago

can't anybody see that Native Vlan Tagging is enabled on both the switches, so native vlan traffic will go tagged on the trunk port. But allowed vlans on the trunk port is 50-100 whereas the both PC-A and PC-B belongs to vlan A so their traffic won't be allowed on the trunk port. So the correct answer should be B.

upvoted 1 times

DixieNormus 1 year ago

can't anybody see that Native Vlan Tagging is enabled on both the switches, so native vlan traffic will go tagged on the trunk port. But allowed vlans on the trunk port is 50-100 whereas the both PC-A and PC-B belongs to vlan 99 so their traffic will be allowed on the trunk port. So the correct answer should be D.

upvoted 7 times

Mauro_Babarram 1 year, 2 months ago

D IS CORRECT

upvoted 2 times

dipanjana1990 1 year, 1 month ago

can't anybody see that Native Vlan Tagging is enabled on both the switches, so native vlan traffic will go tagged on the trunk port. But allowed vlans on the trunk port is 50-100 whereas the both PC-A and PC-B belongs to vlan A so their traffic won't be allowed on the trunk port. So the correct answer should be B.

upvoted 1 times

bruno0147 10 months, 3 weeks ago

B is incorrect

upvoted 1 times

ZUMY 1 year, 3 months ago

D is correct

upvoted 2 times

dipanjana1990 1 year, 1 month ago

can't anybody see that Native Vlan Tagging is enabled on both the switches, so native vlan traffic will go tagged on the trunk port. But allowed vlans on the trunk port is 50-100 whereas the both PC-A and PC-B belongs to vlan A so their traffic won't be allowed on the trunk port. So the correct answer should be B.

upvoted 1 times

rictorres333 1 year, 4 months ago

The real problem is that: Sw2 has Vlan 99 as native vlan, this way send untagged traffic. If we put another vlan as native, there is not problem for pinging...

upvoted 1 times

dipanjana1990 1 year, 1 month ago

can't anybody see that Native Vlan Tagging is enabled on both the switches, so native vlan traffic will go tagged on the trunk port. But allowed vlans on the trunk port is 50-100 whereas the both PC-A and PC-B belongs to vlan A so their traffic won't be allowed on the trunk port. So the correct answer should be B.

upvoted 1 times

Nalle72 1 year, 5 months ago

Packet from PC A to PC B will reach its destination but return packet will not be encapsulated (native vlan 99) in Switch 2, and will be interpreted as vlan 1 in switch 1, thus it will not be forwarded to PC A.

upvoted 2 times

PoBratsky 1 year, 9 months ago

Correct answer is A. In this case, ping will only fail if the PC is on native VLAN. But in VLAN 99, the ping will be successful. Tested on Cisco Packet Tracer.

upvoted 1 times

PoBratsky 1 year, 9 months ago

I'm so sorry. Answer is D. Because PC B in native VLAN. So ping will be failure.

upvoted 1 times

dipanjana1990 1 year, 1 month ago

can't anybody see that Native Vlan Tagging is enabled on both the switches, so native vlan traffic will go tagged on the trunk port. But allowed vlans on the trunk port is 50-100 whereas the both PC-A and PC-B belongs to vlan A so their traffic won't be allowed on the trunk port. So the correct answer should be B.

upvoted 1 times

dave1992 1 year, 9 months ago

i think the answer is A because you would configure the link between a pc and switch as an access port, and links between switches as trunks. the only thing im thinking is if the VLANs are different, then the switch will not forward the frame to the correct vlan.

upvoted 2 times

onikafei 1 year, 7 months ago

Vlans in the chart are different from the code below. And it shows the vlans are mismatched so answer would be D

upvoted 1 times

dipanjana1990 1 year, 1 month ago

can't anybody see that Native Vlan Tagging is enabled on both the switches, so native vlan traffic will go tagged on the trunk port. But allowed vlans on the trunk port is 50-100 whereas the both PC-A and PC-B belongs to vlan A so their traffic won't be allowed on the trunk port. So the correct answer should be B.

upvoted 1 times

Micah7 2 years, 3 months ago

Native vlan traffic will still go through from one switch to another despite Native Vlan mismatch. It will just create a larger broadcast domain between the 2 switches. However, in this question for the "tagged" vlan traffic there is a disruption- the 2 PCs will not be able to communicate.

upvoted 2 times

oooMooo 2 years, 4 months ago

When an untagged frame enters a switch port, the native VLAN is tagged on the frame. So if Switch 1 were to send a frame to Switch 2, it would be sent untagged, and Switch 2 would tag it as VLAN 99. If Switch 2 were to send the frame, Switch 1 would tag it as VLAN 1.

upvoted 4 times

sim5710 2 years, 6 months ago

how is there a native vlan
mismatch ?

upvoted 2 times

NerdyNerdy 2 years, 6 months ago

Trunking native vlan on Sw1 is 1, while native vlan on Sw2 is 99

upvoted 6 times

dipanjana1990 1 year, 1 month ago

can't anybody see that Native Vlan Tagging is enabled on both the switches, so native vlan traffic will go tagged on the trunk port. But allowed vlans on the trunk port is 50-100 whereas the both PC-A and PC-B belongs to vlan A so their traffic won't be allowed on the trunk port. So the correct answer should be B.

upvoted 1 times

SUKABLED 2 years, 7 months ago

True, cause native vlans should also match in order for untagged traffic to get automatically tagged with it, If there are different native VLANs, then packet mismatch will happen, thus no ping

upvoted 2 times

amrith501 2 years, 8 months ago

any Explanation to this ?

upvoted 2 times

DRAG DROP -

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

Select and Place:

Answer Area

access point	device that manages access points
virtual interface	device that provides Wi-Fi devices with a connection to a wired network
dynamic interface	used for out of band management of a WLC
service port	used to support mobility management of the WLC
wireless LAN controller	applied to the WLAN for wireless client communication

Correct Answer:

Answer Area

access point	wireless LAN controller
virtual interface	access point
dynamic interface	service port
service port	virtual interface
wireless LAN controller	dynamic interface

The service port can be used management purposes, primarily for out-of-band management. However, AP management traffic is not possible across the service port. In most cases, the service port is used as a â€last resortâ€ means of accessing the controller GUI for management purposes. For example, in the case where the system distribution ports on the controller are down or their communication to the wired network is otherwise degraded.

A dynamic interface with the Dynamic AP Management option enabled is used as the tunnel source for packets from the controller to the access point and as the destination for CAPWAP packets from the access point to the controller.

The virtual interface is used to support mobility management, Dynamic Host Configuration Protocol (DHCP) relay, and embedded Layer 3 security such as guest web authentication. It also maintains the DNS gateway host name used by Layer 3 security and mobility managers to verify the source of certificates when Layer 3 web authorization is enabled.

Reference:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/ports_and_interfaces.html

cortib Highly Voted 1 year, 11 months ago

access point = proved wireless device with connection to the wired network
WLC = Manage access point
Service port = out of band management of WLC
virtual interface = mobility management WLC
Dynamic interface = Aplied to the WLAN for wireless client communication

upvoted 18 times

DUMPledore Highly Voted 9 months, 1 week ago

I think given answers are correct
upvoted 7 times

paolino555 Most Recent 2 months, 2 weeks ago
is in CCNA 200-301?
upvoted 1 times

lucky1559 2 years ago
From the WLC point of view, client is an AP, therefore Dynamic Int is correct to the last one. However from AP point of view, client is the end device, and thus the Virtual Interface fits in here.

So no clear answer to the last one (WLAN wireless client communication)
upvoted 1 times

kunyo99 2 years, 4 months ago
All the answers are correct
upvoted 4 times

SScott 2 years, 1 month ago
Yes and here are some articles to reference

https://www.ccexpert.us/network-design/wlan-controllers.html

http://www.firewall.cx/cisco-technical-knowledgebase/cisco-wireless/1077-cisco-wireless-controllers-interfaces-ports-functionality.html
upvoted 2 times

Question #188 *Topic 1*

Which unified access point mode continues to serve wireless clients after losing connectivity to the Cisco Wireless LAN Controller?

A. local

B. mesh

C. flexconnect

D. sniffer

Correct Answer: *C*
In previous releases, whenever a FlexConnect access point disassociates from a controller, it moves to the standalone mode. The clients that are centrally switched are disassociated. However, the FlexConnect access point continues to serve locally switched clients. When the FlexConnect access point rejoins the controller (or a standby controller), all clients are disconnected and are authenticated again. This functionality has been enhanced and the connection between the clients and the FlexConnect access points are maintained intact and the clients experience seamless connectivity. When both the access point and the controller have the same configuration, the connection between the clients and APs is maintained.
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010001101.html

Community vote distribution

C (100%)

poovnair Highly Voted 2 years, 12 months ago
When a FlexConnect access point can reach the controller (referred to as the connected mode), the controller assists in client authentication. When a FlexConnect access point cannot access the controller, the access point enters the standalone mode and authenticates clients by itself.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html
upvoted 10 times

MauroC19 Most Recent 4 weeks, 1 day ago
Selected Answer: C
FlexConnect is the correct answer. Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/config-guide/b_wl_17_11_cg/flexconnect.html#:~:text=Proxy%20ARP-,Information%20About%20FlexConnect,a%20controller%20in%20each%20office.
upvoted 1 times

Mauro_Babarram 1 year, 2 months ago
CORRECT IS C
upvoted 4 times

ZUMY 1 year, 3 months ago
C is correct!
upvoted 3 times

```
Router#
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S -Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID     Local Interface  Holdtime  Capability  Platform  Port ID
10.1.1.2      Gig 37/3         176         R I       CPT 600   Gig 36/41
10.1.1.2      Gig 37/1         174         R I       CPT 600   Gig 36/43
10.1.1.2      Gig 36/41        134         R I       CPT 600   Gig 37/3
10.1.1.2      Gig 36/43        134         R I       CPT 600   Gig 37/1
10.1.1.2      Ten 3/2          132         R I       CPT 600   Ten 4/2
10.1.1.2      Ten 4/2          174         R I       CPT 600   Ten 3/2
```

Refer to the exhibit. Which command provides this output?

A. show ip route

B. show cdp neighbor

C. show ip interface

D. show interface

Correct Answer: *B*

NZIAKOU Highly Voted 2 years, 11 months ago

B is correct

upvoted 7 times

SScott 2 years, 1 month ago

show cdp neighbors
https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/show_cdp_neighbors.htm#:~:text=Router%23-,show%20cdp%20neighbors,-Capability%20Codes%3A%20R

upvoted 5 times

tinsta Highly Voted 2 years, 2 months ago

B is Correct

upvoted 5 times

mt05 Most Recent 6 months, 1 week ago

why not D?

upvoted 1 times

xbobdan 7 months, 2 weeks ago

why all the neighbors have the same ID? can this be right?

upvoted 1 times

ZUMY 1 year, 3 months ago

B is correct!

upvoted 5 times

Question #190 *Topic 1*

Which mode must be used to configure EtherChannel between two switches without using a negotiation protocol?

A. active

B. on

C. auto

D. desirable

Correct Answer: *B*
The Static Persistence (or ג€onג€ mode) bundles the links unconditionally and no negotiation protocol is used. In this mode, neither PAgP nor LACP packets are sent or received.

John248 Highly Voted 3 years, 2 months ago
on

Mode that forces the LAN port to channel unconditionally. In the on mode, a usable EtherChannel exists only when a LAN port group in the on mode is connected to another LAN port group in the on mode. Because ports configured in the on mode do not negotiate, there is no negotiation traffic between the ports. You cannot configure the on mode with an EtherChannel protocol. If one end uses the on mode, the other end must also.

auto

PAgP mode that places a LAN port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP negotiation. (Default)

desirable

PAgP mode that places a LAN port into an active negotiating state, in which the port initiates negotiations with other LAN ports by sending PAgP packets.

passive

LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. (Default)

active

LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.
upvoted 29 times

CJ32 Highly Voted 3 years, 2 months ago
What helped me on this one was to think about what the other device would have to be configured to. For active, auto, and desirable, the other device would have to negotiate. However, with the "on" mode. There's no negotiation.
upvoted 20 times

Sonieta 1 year, 11 months ago
Very good explanation to remember, thanks!!
upvoted 1 times

linuxlife Most Recent 6 months ago
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0111110.pdf

EtherChannel Modes
You can configure an EtherChannel in one of these modes: Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or On. Configure both ends of the EtherChannel in the same mode:
• When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. If the remote port cannot negotiate an EtherChannel, the local port is put into an independent state and continues to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.
• When you configure an EtherChannel in the on mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the on mode; otherwise, packet loss can occur.
upvoted 1 times

GreatDane 1 year, 3 months ago
Ref: Cisco IOS Software Configuration Guide, Release 12.2(33)SXH and Later Releases

“CHAPTER 15
Configuring EtherChannels

...
EtherChannel Configuration Overview
..
Table 15-1 EtherChannel Modes

On Mode that forces the LAN port to channel unconditionally. In the on mode, a usable EtherChannel exists only when a LAN port group in the on mode is connected to another LAN port group in the on mode. Because ports configured in the on mode do not negotiate, there is no negotiation traffic between the ports. You cannot configure the on mode with an EtherChannel protocol. If one end uses the on mode, the other end must also.
..."

A. active

Wrong answer.

B. on

Correct answer.

C. auto

Wrong answer.

D. desirable

Wrong answer.

upvoted 2 times

ZUMY 1 year, 3 months ago

B is correct!

upvoted 1 times

ZUMY 1 year, 3 months ago

B is correct

upvoted 1 times

Hodicek 1 year, 10 months ago

NO negotiation mode= ON
NO = ON

upvoted 4 times

Bach999 2 years, 9 months ago

Ref: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/3-1-1SG/configuration/guide/config/channel.html

upvoted 2 times

karemAbdullah 2 years, 11 months ago

PAgP
Cisco Proprietary protocol
LACP Open Standard used by most of Vendors
ON Forced to form Etherchannel without using negotiation protocol

upvoted 4 times

Question #191 *Topic 1*

Which mode allows access points to be managed by Cisco Wireless LAN Controllers?

A. bridge

B. lightweight

C. mobility express

D. autonomous

Correct Answer: *B*
A Lightweight Access Point (LAP) is an AP that is designed to be connected to a wireless LAN (WLAN) controller (WLC). APs are ɹ€lightweight,ɹ€ which means that they cannot act independently of a wireless LAN controller (WLC). The WLC manages the AP configurations and firmware. The APs are ɹ€zero touchɹ€ deployed, and individual configuration of APs is not necessary.

syed5 Highly Voted 3 years, 2 months ago
Cisco Lightweight Access Point (LAP)

The Cisco LAP is part of the Cisco Unified Wireless Network architecture. A LAP is an AP that is designed to be connected to a wireless LAN (WLAN) controller (WLC). The LAP provides dual band support for IEEE 802.11a, 802.11b, and 802.11g and simultaneous air monitoring for dynamic, real-time radio frequency (RF) management. In addition, Cisco LAPs handle time-sensitive functions, such as Layer 2 encryption, that enable Cisco WLANs to securely support voice, video, and data applications.

APs are “lightweight,” which means that they cannot act independently of a wireless LAN controller (WLC). The WLC manages the AP configurations and firmware. The APs are “zero touch” deployed, and individual configuration of APs is not necessary. The APs are also lightweight in the sense that they handle only real-time MAC functionality. The APs leave all the non-real-time MAC functionality to be processed by the WLC. This architecture is referred to as the “split MAC” architecture.

Reference:

https://www.cisco.com/c/en/us/support/docs/wireless/aironet-1200-series/70278-lap-faq.html
upvoted 7 times

karemAbdullah Highly Voted 2 years, 11 months ago
lightweight AP cannot normally operate on its own; it is very dependent on a WLC somewhere in the network
upvoted 6 times

ZUMY Most Recent 1 year, 3 months ago
B is correct
upvoted 3 times

Question #192 *Topic 1*

Which two values or settings must be entered when configuring a new WLAN in the Cisco Wireless LAN Controller GUI? (Choose two.)

A. QoS settings

B. IP address of one or more access points

C. SSID

D. profile name

E. management interface settings

Correct Answer: *CD*

DonnerKomet Highly Voted 2 years ago

Click Add New WLAN. The Add New WLAN window appears.
In the General tab, perform the following:
a) The WLAN Id is automatically selected but you can change it.
b) Enter the Profile Name for the WLAN. (*) must be set
c) Enter the SSID. (*) must be set
d) Choose Admin State for the WLAN from the drop-down list. The default Admin State is Enabled.
e) Choose Radio Policy from the drop-down list. The default Radio Policy is ALL.

upvoted 21 times

DannySprings Highly Voted 3 years, 1 month ago

correct

upvoted 5 times

GreatDane Most Recent 1 year, 3 months ago

Ref: WLAN Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

"Using the Web Graphical User Interface
...
Configuring the Controller Web GUI
...
Step 11

In the WLANs page, enter the following WLAN configuration parameters, and click Next.

• WLAN identifier in the WLAN ID text box.
• SSID of the WLAN that the client is associated with in the SSID text box.
• Name of the WLAN used by the client in the Profile Name text box.
..."

A. QoS settings

Wrong answer.

B. IP address of one or more access points

Wrong answer.

C. SSID

Correct answer.

D. profile name

Correct answer.

E. management interface settings

Wrong answer.

upvoted 2 times

ZUMY 1 year, 3 months ago

C & D are correct

upvoted 4 times

Shamwedge 1 year, 9 months ago

Answers make sense. SSID and Profile Name would be used for identification and would be important when creating a new WLAN

upvoted 1 times

ManKilla 2 years ago

The answer are correct
Editing WLAN SSID or Profile Name for WLANs (GUI)
Procedure

Step 1
Choose WLANs to open the WLANs page.
This page lists all of the WLANs currently configured on the controller. For each WLAN, you can see its WLAN ID, profile name, type, SSID, status, and security policies.
The total number of WLANs appears in the upper right-hand corner of the page. If the list of WLANs spans multiple pages, you can access these pages by clicking the page number links.
Step 2
To edit the a WLAN profile or SSID, click the WLAN ID link in the WLANs > Edit page.
In the Profile Name field, edit the WLAN profile name.
In the WLAN SSID field, edit the WLAN SSID.
Step 3
Click Apply to commit your changes.
Step 4
Click Save Configuration to save your changes.

upvoted 1 times

Texter 2 years, 5 months ago

who's doing their CCNA this month coming? April.

upvoted 4 times

Joe_Q 2 years, 5 months ago

May 13th.

upvoted 4 times

Ray12345 2 years, 4 months ago

May 17th

upvoted 3 times

Shehan 2 years, 1 month ago

Did you pass? were the questions same ?

upvoted 4 times

KAT 2 years, 6 months ago

kindly, any explanation

upvoted 2 times

Jacob_Davis18 2 years, 6 months ago

Connect a WLC on packet tracer and you will see. They are the first two variables you must set.

upvoted 6 times

NetY2K 2 years, 9 months ago

So one help me out here. What is the profile name?

upvoted 4 times

SumonHossain 2 years, 12 months ago

correct ans

upvoted 4 times

Question #193 *Topic 1*

Which command is used to specify the delay time in seconds for LLDP to initialize on any interface?

A. lldp timer

B. lldp tlv-select

C. lldp reinit

D. lldp holdtime

Correct Answer: *C*
ɹ€¢ lldp holdtime seconds: Specify the amount of time a receiving device should hold the information from your device before discarding it
ɹ€¢ lldp reinit delay: Specify the delay time in seconds for LLDP to initialize on an interface
ɹ€¢ lldp timer rate: Set the sending frequency of LLDP updates in seconds
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_55_se/configuration/guide/3560_scg/swlldp.html

Ettmoh Highly Voted 3 years ago
(config)#lldp ?
holdtime Specify the holdtime (in sec) to be sent in packets
reinit Delay (in sec) for LLDP initialization on any interface
run Enable LLDP
timer Specify the rate at which LLDP packets are sent (in sec)
tlv-select Selection of LLDP TLVs to send
upvoted 18 times

karemAbdullah Highly Voted 2 years, 11 months ago
lldp reinit

Specifies the delay time in seconds for LLDP to initialize on any interface.
The range is 1 to 10 seconds; the default is 2 seconds.
upvoted 13 times

ZUMY Most Recent 1 year, 3 months ago
C is correct
upvoted 4 times

Question #194 *Topic 1*

```
SW2
vtp domain cisco
vtp mode transparent
vtp password ciscotest
interface fastethernet0/1
   description connection to sw1
   switchport mode trunk
   switchport trunk encapsulation dot1q
```

Refer to the exhibit. How does SW2 interact with other switches in this VTP domain?

A. It transmits and processes VTP updates from any VTP clients on the network on its trunk ports.

B. It processes VTP updates from any VTP clients on the network on its access ports.

C. It receives updates from all VTP servers and forwards all locally configured VLANs out all trunk ports.

D. It forwards only the VTP advertisements that it receives on its trunk ports.

Correct Answer: *D*

The VTP mode of SW2 is transparent so it only forwards the VTP updates it receives to its trunk links without processing them.

Reference:

https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html

Community vote distribution

D (100%)

JWMcInSC Highly Voted 3 years, 3 months ago

Transparent—VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements, but transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP Version 2.

upvoted 20 times

Gelo29 Highly Voted 3 years ago

Is VTP still in 200-301 exam? I'm confused.

upvoted 11 times

Aie_7 7 months, 4 weeks ago

It's only mentioned, but i never read "vtp mode transparent" in Network Academy in 2023

upvoted 2 times

KonstantinosM Most Recent 2 months, 1 week ago

Selected Answer: D

Found an excellent explanation of all 3 modes here: https://www.firewall.cx/networking-topics/vlan-networks/virtual-trunk-protocol/223-vtp-introduction.html

upvoted 1 times

ZUMY 1 year, 3 months ago

D is correct

upvoted 2 times

netlol 1 year, 8 months ago

Sorry, why not C?

upvoted 4 times

guisam 9 months ago

...all locally configured VLANs...
locally

upvoted 1 times

Keif 1 year, 11 months ago

Just took exam 200-301 I can confirm very similar question was on the exam

upvoted 6 times

[Removed] 1 year, 11 months ago

DId u pass your test?

upvoted 6 times

tweesgger 1 year, 11 months ago

Just because a topic was removed does not mean they will refrain from including questions about them in the exams, it all depends on luck i guess.

upvoted 2 times

RougePotatoe 10 months, 3 weeks ago

That's literally what the topics are for. To know what is going to be on the test if the topics don't reflect the test then why bother posting the topics at all and the sky is the limit to what they want to test you on.

upvoted 5 times

GhostWolf 10 months, 1 week ago

Lmao exactly.

upvoted 1 times

DonnerKomet 2 years ago

Guys, but VTP is not out of scope of this 200-301 exam? The topic was removed from CCNA 200-301, isnt?

upvoted 4 times

GreatDane 2 years, 10 months ago

Answer is correct:

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-4500-series-switches/13414-103.html#vlan_trunking_protocol

upvoted 3 times

karemAbdullah 2 years, 11 months ago

Transparent—VTP transparent network devices do not participate in VTP. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent network devices do forward VTP advertisements that they receive on their trunking LAN interfaces.

upvoted 4 times

Whippy29 2 years, 11 months ago

hhahaha, yeah I'm confused as well. I have access to the latest cisco course on two platforms and in either there is no mention of VTP

upvoted 2 times

Network_Surgeon 3 years, 4 months ago

SW2 being in transparent mode shows that the switch is either acting as VTP server or VTP client. So it can definitely forward VTP packets.

upvoted 3 times

caty1234 2 years, 10 months ago

what does being in transparent mode have to do with either acting as server or client, I thought it just received the updates and forwarded them without changing its local database

upvoted 4 times

Question #195 *Topic 1*

```
SW1#sh lacp neighbor
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode      P - Device is in Passive mode

Channel group 35 neighbors

Partner's information:

              LACP port                        Admin  Oper   Port    Port
Port    Flags Priority   Dev ID          Age   key    Key    Number  State
Et1/0   SP    32768      aabb.cc80.7000   8s   0x0    0x23   0x101   0x3C
Et1/1   SP    32768      aabb.cc80.7000   8s   0x0    0x23   0x102   0x3C
```

Refer to the exhibit. Based on the LACP neighbor status, in which mode is the SW1 port channel configured?

A. mode on

B. active

C. passive

D. auto

Correct Answer: *B*

From the neighbor status, we notice the ג€Flagsג€ are SP. ג€Pג€ here means the neighbor is in Passive mode. In order to create an Etherchannel interface, the (local)

SW1 ports should be in Active mode. Moreover, the ג€Port Stateג€ in the exhibit is €0ג€x3cג€ (which equals to €³ג€00111100ג in binary format).

Bit 3 is ג€1ג€ which means the ports are synchronizing -> the ports are working so the local ports should be in Active mode.

Community vote distribution

B (71%) C (29%)

DatBroNZ Highly Voted 1 year, 11 months ago

B is correct.
With LACP, at least one side must be active. So if the SW1 neighbor is passive, SW1 must be active.

upvoted 18 times

ZUMY Highly Voted 2 years, 4 months ago

B is correct

upvoted 9 times

Giuseppe_001 2 years, 4 months ago

sure? because the flag is set in SP

upvoted 2 times

jehangt3 2 years, 3 months ago

B is the right answer, this was a tricky one... I quickly realized that both partner and local routers cannot be in the same passive mode for a link to form. The question is asking "what mode are YOU on". Well since you are able to see your partner information you would be in "active mode". Weather you partner is on "active" or "passive" doesn't matter, as long as you are active you can pull neighbors information.

upvoted 17 times

Giuseppe_001 2 years, 4 months ago

i got a mistake sorry

upvoted 6 times

jehangt3 2 years, 3 months ago

you didn't make a mistake, you were right the first time.. B is the answer

upvoted 3 times

linuxlife Most Recent 6 months ago

In configuring Dynamic EtherChannel, with PAgP, at least one of the two sides must use desirable, and with LACP, at least one of the two sides must use active. The question is showing the other device with SP code...means, its LACP is PASSIVE. Therefore, opposite device's LACP configuration must be ACTIVE.

upvoted 1 times

JamPauGalBag 1 year ago

in which mode is the SW1 port channel configured?
SP = Passive
upvoted 1 times

RoVasq3 1 year, 1 month ago

Selected Answer: B

B is the correct one
upvoted 1 times

vuhidus 1 year, 1 month ago

Selected Answer: B

BBBBB based on the neighboring status
upvoted 1 times

hp2wx 1 year, 1 month ago

They key to this question is the line that reads "Partner's Information:" from there you know that you need to interpret the flags for the operational modes from the lens of "If my neighbor's port channel is configured this way, how do I need to configure mine so that I can actively form a LAG."

B is 100% correct.
upvoted 1 times

Test90 1 year, 3 months ago

In short, SW1 will always reflect its neighbor's status (how it is configured). It is displaying SP(which means SW is Passive) for LACP communication to happen, one must be active, so this means SW1 has been configured as Active.
upvoted 1 times

france60 1 year, 3 months ago

the answer is C because the question asks for the configuration mode and not how SW1 should be configured to be in etherchannel. the question is quite obvious.
upvoted 2 times

DixieNormus 1 year ago

Going by your logic there is not enough information to answer this question, we only see the neighbor's configuration mode.
upvoted 1 times

guille_teleco 1 year, 4 months ago

B is correct , the output of the command shows the neighbor info.
The neighbor is set to passive, so de local switch(SW1) must be set to active.
upvoted 2 times

Scvrfvce 1 year, 4 months ago

Selected Answer: B

B is correct
upvoted 1 times

Halop 1 year, 4 months ago

It shows the status of neighbors.B is correct.
upvoted 1 times

JSDH 1 year, 6 months ago

Selected Answer: B

B is correct
upvoted 1 times

qasawq 1 year, 7 months ago

answer is B
upvoted 1 times

AndersonMr 1 year, 8 months ago

Selected Answer: B

SW2 is passive, so SW1 has to be active.
upvoted 1 times

Hyay 1 year, 9 months ago

Selected Answer: C

C is correct to me, the command shows states of partners. So if a port is passive then the device I'm on is configured as passive.

See an example of config here :
https://blog.michaelfmcnamara.com/2016/06/lacp-configuration-examples-part-7/
upvoted 2 times

Nebulise 1 year, 8 months ago

Sorry but you're wrong
upvoted 2 times

ScorpionNet 1 year, 4 months ago

No because Passive is used to detect the neighbor that is LACP Enabled so it's Active. Like PAgP Desirable is like Active and Auto is like Passive plz keep in mind

upvoted 1 times

schleef 1 year, 10 months ago

That one is easy, you just have to look at the flags of the neighbor. B is correct

upvoted 2 times

Question #196 *Topic 1*

Two switches are connected and using Cisco Dynamic Trunking Protocol. SW1 is set to Dynamic Auto and SW2 is set to Dynamic Desirable. What is the result of this configuration?

A. The link becomes an access port.

B. The link is in an error disabled state.

C. The link is in a down state.

D. The link becomes a trunk port.

Correct Answer: *D*

Community vote distribution

D (100%)

ayd33n Highly Voted 3 years, 1 month ago

Dynamic Auto — Makes the Ethernet port willing to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to trunk or dynamic desirable mode. This is the default mode for some switchports.

Dynamic Desirable — Makes the port actively attempt to convert the link to a trunk link. The port becomes a trunk port if the neighboring Ethernet port is set to trunk, dynamic desirable or dynamic auto mode.

upvoted 29 times

KonstantinosM Most Recent 2 months, 1 week ago

Found an excellent explanation of all 3 modes here: https://www.firewall.cx/networking-topics/vlan-networks/virtual-trunk-protocol/223-vtp-introduction.html

upvoted 1 times

linuxlife 6 months ago

Dynamic Desirable - initiate negotiation messages and respond to negotiation messages to dynamically choose whether to start using TRUNK.

Dynamic Auto - passively waits to receive TRUNK negotiation messages at which point the switch will respond and negotiate whether to use TRUNKING.

upvoted 3 times

linuxlife 6 months ago

And yes, D is the right answer

upvoted 1 times

icecool2019 11 months, 2 weeks ago

According to the DTP matrix:
Dynamic Auto | Dynamic Desirable | Trunk | Access
Dynamic Auto | Access | Trunk | Trunk | Access
Dyn Desirable | Trunk | Trunk | Trunk | Access
Trunk | Trunk | Trunk | Trunk | Limited Connectivity (LC)
Access | Access | Access | LC | Access

upvoted 1 times

lock12333 1 year, 3 months ago

Selected Answer: D

ddddddddddddd

upvoted 2 times

ZUMY 2 years, 4 months ago

D is correct

upvoted 4 times

Nhan 2 years, 6 months ago

A trunk link is formed

upvoted 4 times

Question #197 *Topic 1*

A Cisco IP phone receives untagged data traffic from an attached PC. Which action is taken by the phone?

A. It drops the traffic.

B. It allows the traffic to pass through unchanged.

C. It tags the traffic with the native VLAN.

D. It tags the traffic with the default VLAN.

Correct Answer: *B*
Untagged traffic from the device attached to the Cisco IP Phone passes through the phone unchanged, regardless of the trust state of the access port on the phone.
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swvoip.pdf

Community vote distribution

B (100%)

GreatDane Highly Voted 2 years, 10 months ago
"31 Days Before Your 200-301 CCNA Exam"

Page 85, right under figure 26-1.
upvoted 11 times

ayd33n Highly Voted 3 years, 1 month ago
"Untagged traffic from the device attached to the Cisco IP Phone passes through the phone unchanged, regardless of the trust state of the access port on the phone"
upvoted 8 times

Isuzu Most Recent 4 months, 1 week ago
Selected Answer: B
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/vlan/configuration_guide/b_vlan_152ex_2960-x_cg/b_vlan_152ex_2960-x_cg_chapter_0110.pdf
upvoted 1 times

Dataset 2 years, 2 months ago
B is correct
upvoted 3 times

ZUMY 2 years, 4 months ago
B is correct
upvoted 4 times

Question #198 *Topic 1*

Which design element is a best practice when deploying an 802.11b wireless infrastructure?

A. allocating nonoverlapping channels to access points that are in close physical proximity to one another

B. disabling TCP so that access points can negotiate signal levels with their attached wireless devices

C. configuring access points to provide clients with a maximum of 5 Mbps

D. setting the maximum data rate to 54 Mbps on the Cisco Wireless LAN Controller

Correct Answer: *A*

Community vote distribution

A (100%)

ZUMY Highly Voted 2 years, 4 months ago

A is correct

upvoted 8 times

karemAbdullah Highly Voted 2 years, 11 months ago

Selecting the proper WiFi channel can significantly improve your WiFi coverage and performance. In the 2.4 GHz band, 1, 6, and 11 are the only non-overlapping channels. Selecting one or more of these channels is an important part of setting up your network correctly.

upvoted 6 times

DUMPledore Most Recent 9 months, 1 week ago

Selected Answer: A

Given answer is correct

upvoted 2 times

hasbulla01 10 months, 1 week ago

Selected Answer: A

A is correct only for discart

upvoted 1 times

Shamwedge 1 year, 10 months ago

Wouldn't it be A for any 801.11 Wi-Fi infrastructure?

upvoted 2 times

Nicocisco 1 year, 6 months ago

No, because for the 801.11a for example, we are talking about 5Ghz, which has no overlapping

upvoted 1 times

hja031 3 years, 3 months ago

answer is A

upvoted 4 times

Artengineer 3 years, 4 months ago

thecorrect answer is C

upvoted 1 times

mashiur 3 years, 3 months ago

I don't think soo..the correct answer is A

upvoted 7 times

Ali526 2 years, 8 months ago

Agreed.

upvoted 3 times

ayd33n 3 years, 1 month ago

Data rate is case-by-case. You never want overlapping channels on Access Points that are in close proximity to each other.

upvoted 2 times

Clxxcv420 2 years, 11 months ago

802.11b is support 2.4ghz on 11mbps

upvoted 1 times

SUKABLED 2 years, 7 months ago

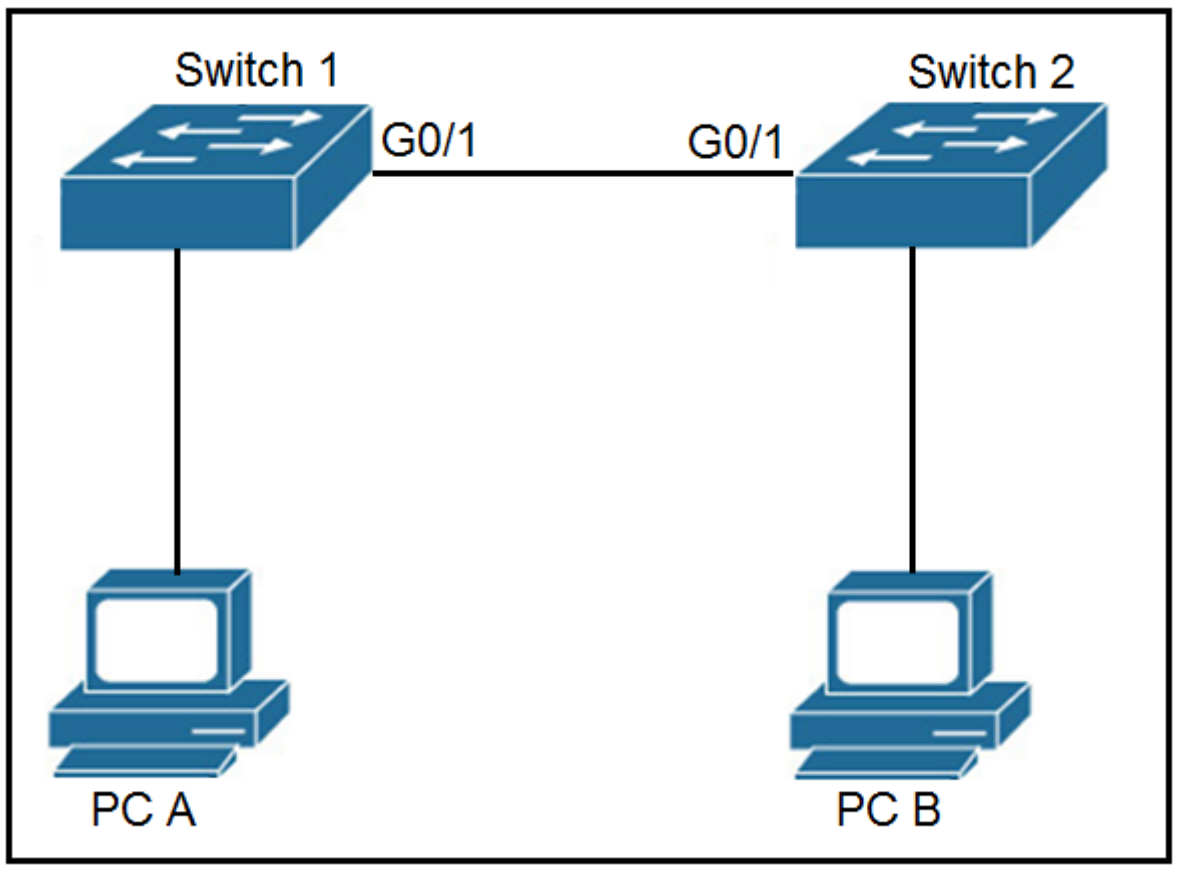
Not enough data to conclude C...for this question- definitely A!

upvoted 3 times

Question #199 *Topic 1*

Refer to the exhibit. The network administrator wants VLAN 67 traffic to be untagged between Switch 1 and Switch 2, while all other VLANs are to remain tagged.

Which command accomplishes this task?



A. switchport access vlan 67

B. switchport trunk allowed vlan 67

C. switchport private-vlan association host 67

D. switchport trunk native vlan 67

Correct Answer: *D*

Community vote distribution

D (100%)

ZUMY Highly Voted 2 years, 4 months ago

D is correct

Native VLAN: The native VLAN is the one into which untagged traffic will be put when it's received on a trunk port. This makes it possible for your VLAN to support legacy devices or devices that don't tag their traffic like some wireless access points and simply network attached devices.

upvoted 21 times

hippyjm Highly Voted 2 years, 6 months ago

https://www.summit360.com/2017/08/30/vlans-types-benefits/
D is correct

upvoted 5 times

LeonardoMeCabrio Most Recent 3 months, 2 weeks ago

Selected Answer: D

D Correct

upvoted 1 times

gc999 6 months, 1 week ago

Don't quite understand the question "wants VLAN 67 traffic to be untagged between Switch 1 and Switch 2", it should mean the original traffic is from VLAN67, when discovered it, make it untagged between SW1 and SW2.

I would 100% accept answer "D", if the question is "How to make the all untagged / VLAN unknown traffic be passing through VLAN67 between SW1 and SW2"

upvoted 1 times

couragek 8 months, 4 weeks ago

D IS CORRECT

upvoted 2 times

Yunus_Empire 9 months, 1 week ago

D is correct

upvoted 3 times

helmerpach 1 year, 8 months ago

D is correct

upvoted 2 times

Scipions 2 years, 5 months ago

Grazie a sta ceppa la nativa ha il non taggato

upvoted 4 times

echarles10 2 years, 8 months ago

D is correct

upvoted 3 times

Question #200 *Topic 1*

Which two command sequences must be configured on a switch to establish a Layer 3 EtherChannel with an open-standard protocol? (Choose two.)

A. interface GigabitEthernet0/0/1 channel-group 10 mode auto

B. interface GigabitEthernet0/0/1 channel-group 10 mode on

C. interface port-channel 10 no switchport ip address 172.16.0.1 255.255.255.0

D. interface GigabitEthernet0/0/1 channel-group 10 mode active

E. interface port-channel 10 switchport switchport mode trunk

Correct Answer: *CD*

Community vote distribution

CD (85%) Other

Dave861 Highly Voted 3 years, 2 months ago

We can answer this by discarding incorrect answers we need to use an open standard IE LACP

The option "A" is discarded: PAgP configuration
The option "B" is discarded: manual configuration ("On" mode)
The option "C" is configuration that LACP uses.
The option "D" is configuration that LACP uses.
The option "E" is discarded: It is configuration of trunk mode, not Etherchannel

C and D correct.

upvoted 60 times

Ali526 2 years, 8 months ago

Not only that; the question asks for layer3. When you put in switchport, it becomes layer 2.

upvoted 19 times

wizcas 2 years, 9 months ago

If I may correct "E": there is "switchport" twice, which is an invalid command. You actually can do access/trunk config on an EtherChannel and why wouldn't you when using VLANs.
Otherwise, good statement!

upvoted 6 times

dori Highly Voted 3 years, 3 months ago

The right answer should be C and D

upvoted 18 times

Cynthia2023 Most Recent 1 month, 1 week ago

Selected Answer: BC

The correct answers are:

B. interface GigabitEthernet0/0/1 channel-group 10 mode on

C. interface port-channel 10 no switchport ip address 172.16.0.1 255.255.255.0

To establish a Layer 3 EtherChannel, you should configure the physical interface with "channel-group 10 mode on" to enable EtherChannel and the virtual interface with an IP address using the "ip address" command. I apologize for the confusion in my previous responses.

The "mode active" command is used for LACP (Link Aggregation Control Protocol) negotiation, which is typically used for Layer 2 EtherChannel configuration. In Layer 3 EtherChannel configurations, the "mode active" command is not used.

upvoted 1 times

Cynthia2023 1 month, 1 week ago

https://networklessons.com/switching/layer-3-etherchannel-cisco-ios-switch

upvoted 1 times

elixirwell 5 months, 2 weeks ago

Selected Answer: BD

ChatGPT says,
The two command sequences that must be configured on a switch to establish a Layer 3 EtherChannel with an open-standard protocol are:

B. interface GigabitEthernet0/0/1 channel-group 10 mode on
D. interface GigabitEthernet0/0/1 channel-group 10 mode active

Option A (interface GigabitEthernet0/0/1 channel-group 10 mode auto) sets the interface to automatically negotiate the mode of the EtherChannel, which may not be desirable.

Option C (interface port-channel 10 no switchport ip address 172.16.0.1 255.255.255.0) configures a Layer 3 interface for the EtherChannel, but it does not establish the EtherChannel itself.

Option E (interface port-channel 10 switchport switchport mode trunk) configures the EtherChannel interface as a trunk, but it does not establish the EtherChannel itself.

upvoted 3 times

Amonzon 1 year, 1 month ago

C & D for sure are the correct ones.

upvoted 2 times

ptfish 1 year, 1 month ago

Selected Answer: CD

C:
interface port-channel 10
no switchport
ip address 172.16.0.1 255.255.255.0

D:
interface GigabitEthernet0/0/1
channel-group 10 mode active

upvoted 3 times

vuhidus 1 year, 1 month ago

Selected Answer: CD

Should be CD

upvoted 1 times

ZUMY 1 year, 3 months ago

C & D are Correct
why C: For Layer 3 ether channel we need to run NO SWITCHPORT command

upvoted 3 times

BlankNothing1 1 year, 3 months ago

I agree C and D are correct. The only way C would not be correct is the question asked for which "two command sequence." C has a 3 commands, interface port-channel 10 no switchport ip address 172.16.0.1 255.255.255.0. "interface port-channel 10" is one, "no switchport" is the second one, and "Ip address 172.16.0.1 255.255.255.0 is the third command in the sequence.

upvoted 1 times

ScorpionNet 1 year, 4 months ago

Yep C and D is correct because IP is Layer 3 and Trunking is Layer 2

upvoted 1 times

LordScorpius 1 year, 4 months ago

Selected Answer: CD

You need an IP address for an L3 interface and you need to use an active for LLDP, desirable for Etherchannel.

upvoted 1 times

MCsepul 1 year, 5 months ago

Selected Answer: CD

CD is correct

upvoted 1 times

ismatdmour 1 year, 6 months ago

Selected Answer: CD

E is incorrext, it makes it layer 2

upvoted 2 times

HarLikon 1 year, 7 months ago

Selected Answer: CD

Aswers are C,D

upvoted 3 times

SparkySM 1 year, 7 months ago

Selected Answer: CD

it should be c and d

upvoted 4 times

LilGhost_404 1 year, 7 months ago

A. interface GigabitEthernet0/0/1, channel-group 10 mode auto. (incorrect.. this is not open)
B. interface GigabitEthernet0/0/1, channel-group 10 mode on. (incorrect this is not open)

C. interface port-channel 10, no switchport, ip address 172.16.0.1 255.255.255.0 (correct it puts the po in L3)
D. interface GigabitEthernet0/0/1, channel-group 10 mode active. (correct, uses LACP... this is open)
E. interface port-channel 10, switchport, switchport mode trunk. (incorrect Switchport puts them in L2)
C and D are correct!

upvoted 2 times

bigbelly123 1 year, 8 months ago

A. interface GigabitEthernet0/0/1 channel-group 10 mode auto (incorrect.. this is not open)
B. interface GigabitEthernet0/0/1 channel-group 10 mode on (incorrect this is not open)
C. interface port-channel 10 no switchport ip address 172.16.0.1 255.255.255.0 (incorrect, does not need an IP, its a layer 2 protocol)
D. interface GigabitEthernet0/0/1 channel-group 10 mode active (correct, uses LACP... this is open)
E. interface port-channel 10 switchport switchport mode trunk (correct, it needs to be in trunking mode)

upvoted 1 times

Naj_Val 1 year, 8 months ago

The question states it should be an L3 Ether-Channel, not L2?

upvoted 2 times

Question #201 *Topic 1*

Refer to the exhibit. Which two commands when used together create port channel 10? (Choose two.)

Switch#show etherchannel summary
[output omitted]

Group	Port-channel	Protocol	Ports	
10	Po10(SU)	LACP	Gi0/0(P)	Gi0/1(P)
20	Po20(SU)	LACP	Gi0/2(P)	Gi0/3(P)

A. int range g0/0-1 channel-group 10 mode active

B. int range g0/0-1 channel-group 10 mode desirable

C. int range g0/0-1 channel-group 10 mode passive

D. int range g0/0-1 channel-group 10 mode auto

E. int range g0/0-1 channel-group 10 mode on

Correct Answer: *AC*

Community vote distribution

A (100%)

legitornot22 Highly Voted 2 years, 6 months ago
Desirable/Auto (PAGP)
Active/Passive (LACP)
upvoted 38 times

shakyak 1 year, 9 months ago
L-AC-P has "AC" in the middle which is easier to remember as an Active :D
upvoted 48 times

xbololi 2 months, 3 weeks ago
this guy deserves every upvote <3
upvoted 2 times

Paplewska Highly Voted 2 years, 4 months ago
I only see A as the answer because the configuration does the same on both interfaces so if they are both mode Active it will form an LACP channel; which is what is required. If both are auto it will not form, if both are desirable it will form an PAGP channel, which is not what is required, if they are both on there will be no protocol, if they are passive no LACP will form. So the only answer is A.
upvoted 11 times

uditpatel1 Most Recent 4 months, 4 weeks ago
Selected Answer: A
why question has together word?

Correct Answer is: A
upvoted 1 times

icecool2019 11 months, 2 weeks ago
LACP(vendor natural)form a Ether channel = (Active & Active) / (Active & Passive) / (Passive & Actives)
PAgP (CISCO) form a Ether channel = (Desirable & Desirable) / (Desirable & Auto) / (Auto & Desirable)
upvoted 2 times

ScorpionNet 1 year, 4 months ago
A and D is right
Easy to know if familiar to Etherchannel
upvoted 1 times

ScorpionNet 1 year, 4 months ago
I mean C sorry XD.
upvoted 1 times

ismatdmour 1 year, 6 months ago

Selected Answer: A

The command output given is only for one side of the Etherchannel on the Switch in question (we are not given the details of the other switch, do we have to assume that the other switch ends with the same interfaces and the same Channel-group?) , so option A :" mode Active" ensures that the switch will take the initiative and tries to form the channel. Surely it will result in success as the other end has one of 2 options (active or passive). Of course, assuming that the other end on the other switch is not incorrectly reconfigured using PAgP options (auto/desirable) or the no protocol option (mode on). Theses case results in that the channel is not formed.
For Choice C, it does not guarantee Ether-Channel formation as long as we don't have information about which mode the other end is being configured (if Active, channel is formed, if passive, channel is not formed).
Requiring 2 answers without having information about the other end is not correct
Also, if the 2 has to be used yogether (on the same switch) the second one will replace the first.

upvoted 2 times

Vinarino 1 year, 8 months ago

If LACP PortChannel B is Passive, then LACP PortChannel A must be Active
Or the reverse, A-to-B = Active-to-Passive. (Together, this will work).

upvoted 1 times

jerry19 2 years, 4 months ago

Answer - A & C. If you saw PAGP under protocol, in the screenshot, the answer would've been B & D.

upvoted 2 times

ZUMY 2 years, 4 months ago

PAgP- Disirable/Auto (Link formation)
LACP- Active/Active or Active/Passive (Link formation)

upvoted 2 times

Question #202 *Topic 1*

Refer to the exhibit. An administrator is tasked with configuring a voice VLAN. What is the expected outcome when a Cisco phone is connected to the
GigabitEthernet 3/1/4 port on a switch?

```
interface GigabitEthernet3/1/4
  switchport voice vlan 50
!
```

A. The phone and a workstation that is connected to the phone do not have VLAN connectivity.

B. The phone sends and receives data in VLAN 50, but a workstation connected to the phone sends and receives data in VLAN 1.

C. The phone sends and receives data in VLAN 50, but a workstation connected to the phone has no VLAN connectivity.

D. The phone and a workstation that is connected to the phone send and receive data in VLAN 50.

Correct Answer: *B*

Ibimat Highly Voted 2 years, 3 months ago

Should'nt the answer be C.
The traffic from the workstation is untagged. and there is no indication that the native vlan is vlan1

upvoted 11 times

NORLI 1 year, 5 months ago

By default all ports are in vlan1untill they are configured to be in a separate vlan

upvoted 6 times

Unemaru 2 years, 3 months ago

I think if we are talking about "tagging" we have to mention a TRUNK, tagging has no use in an isolated switched, the switch simply separates ports in different vlans, and each one with a separate MAC address table. Think about .1q tagging as a tool for giving information about an internal switch vlan to another switch.
If you don't configure explicitely a command "switchport mode access vlan x", and the port is not a trunk port, hence an Access Port (like in this example), the default data VLAN will be 1.

upvoted 12 times

SScott 2 years, 1 month ago

That's a good point. B is right. Since the native VLAN is not referenced, we can safely assume it is VLAN1 (native defaulting to the default VLAN if not configured) and the untagged data PC traffic passes through the phone unchanged. If the data traffic was tagged, we would likely have more details here such as cos value or trust with the switchport priority.

https://www.cisco.com/c/en/us/support/docs/smb/collaboration-endpoints/cisco-ip-phone-7800-series/smb5625-configure-ethernet-settings-on-a-cisco-ip-phone-7800-or-8800.html#:~:text=0%20to%204095.-,The%20default%20is%20VLAN%201,-.

https://www.youtube.com/watch?v=zW_-mf6v3fs

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvoip.html#:~:text=To%20process%20tagged%20data%20traffic%20(in%20IEEE%20802.1Q%20or%20IEEE%20802.1p%20frames)%2C%20you%20can%20configure%20the%20switch%20to%20send%20CDP%20packets%20to%20instruct%20the%20phone%20how%20to%20send%20data%20packets%20from%20the%20device%20attached%20to%20the%20access%20port%20on%20the%20Cisco%20IP%20Phone

upvoted 4 times

Dex1997 Most Recent 7 months, 4 weeks ago

shouldnt the answer be A since the command "switchport mode access" is missing?

upvoted 3 times

icecool2019 11 months, 2 weeks ago

Answer B is correct

upvoted 1 times

Ronild 1 year ago

Should the configured port have "switchport mode access" config in order for B to be the correct answer?

upvoted 3 times

michael1001 9 months ago

Yes - quite annoying and I got caught there too.

upvoted 1 times

GreatDane 1 year, 3 months ago

Ref: Voice VLAN - NetworkLessons.com

"...
The computer will be in a data VLAN, the IP phone will be in the voice VLAN.
...
Behind the scenes, we have a trunk between our switch and IP phone. The port on the IP phone that connects to the computer is an access port. The IP phone will forward all traffic from the computer to the switch untagged, traffic from the IP phone itself will be tagged. The only two VLANs that are allowed though, are the access and voice VLAN.
..."

A. The phone and a workstation that is connected to the phone do not have VLAN connectivity.

Wrong answer.

B. The phone sends and receives data in VLAN 50, but a workstation connected to the phone sends and receives data in VLAN 1.

Correct answer.

C. The phone sends and receives data in VLAN 50, but a workstation connected to the phone has no VLAN connectivity.

Wrong answer.

D. The phone and a workstation that is connected to the phone send and receive data in VLAN 50.

Wrong answer.

upvoted 2 times

mrbottomwood 10 months, 1 week ago

Bro(or Sis), I love how you normally reference your responses with a clear cut and concise statements. Thank you!

upvoted 3 times

ZUMY 1 year, 3 months ago

Going with B

upvoted 1 times

babaKazoo 1 year, 10 months ago

B because the native vlan defaults to 1 if its not changed.

upvoted 2 times

NZIAKOU 2 years, 6 months ago

Answer B.

upvoted 2 times

Question #203 *Topic 1*

Refer to the exhibit. Which action is expected from SW1 when the untagged frame is received on the GigabitEthernet0/1 interface?

```
SW1#show run int gig 0/1
interface GigabitEthernet0/1
  switchport access vlan 11
  switchport trunk allowed vlan 1-10
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 5
  switchport mode trunk
  speed 1000
  duplex full
```

A. The frame is processed in VLAN 1

B. The frame is processed in VLAN 11

C. The frame is processed in VLAN 5

D. The frame is dropped

Correct Answer: *C*

Ali526 Highly Voted 2 years, 8 months ago

Untagged and native VLAN go together, so VLAN 5. However, 'switchport mode trunk' and switchport access VALN 11', no good.

upvoted 17 times

onikafei Highly Voted 1 year, 7 months ago

Always remember native=untagged lol

upvoted 10 times

picho707 Most Recent 2 weeks, 1 day ago

I have seen in my days this type of horrible configuration. The answer is correct.

upvoted 1 times

Smaritz 1 year, 6 months ago

Trunk and Access in one?

upvoted 4 times

AlexMD 1 year, 10 months ago

C is correct answer

upvoted 1 times

ZUMY 2 years, 4 months ago

C is correct
There is an ambiguity in the question

upvoted 4 times

TEO1221768548956 1 month, 4 weeks ago

This question feels unnecessarily tricky don't you think, because an interface shouldn't be trunk interface and an access interface

upvoted 1 times

Question #204 *Topic 1*

Which command is used to enable LLDP globally on a Cisco IOS ISR?

A. lldp run

B. lldp enable

C. lldp transmit

D. cdp run

E. cdp enable

Correct Answer: *A*
Link Layer Discovery Protocol (LLDP) is an industry standard protocol that allows devices to advertise, and discover connected devices, and there capabilities
(same as CDP of Cisco). To enable it on Cisco devices, we have to use this command under global configuration mode:
Sw(config)# lldp run

ZUMY Highly Voted 2 years, 4 months ago

A is correct

#lldp run - Golably Enable
#no lldp run - Globally Disable
#lldp Recieve -To receive LLDP packets
#lldp Transmit - To transmit LLDP packets

upvoted 14 times

linuxlife Most Recent 6 months ago

For Cisco Switches & Routers, LLDP is NOT enabled by default, quick check as follow:
Switch#show lldp
% LLDP is not enabled

Switch(config)#lldp ?
run Enable LLDP

Switch#show lldp neighbors
% LLDP is not enabled
Switch#

while CDP is enabled by default:
Switch#show cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled

upvoted 1 times

linuxlife 6 months ago

so, the right answer is:
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#lldp run
Switch(config)#

upvoted 1 times

GreatDane 1 year, 3 months ago

Ref: Catalyst 2960 Switch Software Configuration Guide

"...
Disabling and Enabling LLDP Globally

LLDP is enabled by default.
...
Step 2 lldp run Enable LLDP.
..."

A. lldp run

Correct answer.

B. lldp enable

Wrong answer.

C. lldp transmit

Wrong answer.

D. cdp run

Wrong answer.

E. cdp enable

Wrong answer.
upvoted 1 times

Darrien1301 1 year, 5 months ago
But on Cisco it is cdp run and the question says ,,cisco iOS"
upvoted 3 times

jose01210 1 year, 3 months ago
I think same
upvoted 1 times

bmatthee01 1 year, 6 months ago
on cisco devices LLDP is disabled by default
"LLDP run" in global conf mode will enable it
LLDP transmit and receive must be enabled at interface level
upvoted 1 times

SScott 2 years, 1 month ago
LLDP is enabled by default so this question is a bit misleading. If disabled then lldp run will re-enable from config t

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_37_ey/configuration/guide/scg/swlldp.pdf
upvoted 2 times

shaz938 2 years ago
Can someone please clarify, isn't LLDP disabled by default on Cisco devices? It is CDP enabled by default.
upvoted 4 times

Adaya 2 years, 3 months ago
Thank for the explanation
upvoted 2 times

Question #205 *Topic 1*

Which command should you enter to configure an LLDP delay time of 5 seconds?

A. lldp timer 5000

B. lldp holdtime 5

C. lldp reinit 5000

D. lldp reinit 5

Correct Answer: *D*

☞ lldp holdtime seconds: Specify the amount of time a receiving device should hold the information from your device before discarding it

☞ lldp reinit delay: Specify the delay time in seconds for LLDP to initialize on an interface

☞ lldp timer rate: Set the sending frequency of LLDP updates in seconds

Reference:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_55_se/configuration/guide/3560_scg/swlldp.html

Community vote distribution

D (58%) B (42%)

Dutch012 Highly Voted 6 months, 4 weeks ago

Selected Answer: B

I guess the guys in the comment misunderstand the question.
if it said
Which command is used to specify the delay time of 5 seconds for LLDP to initialize on any interface? the answer would be D.
but if the question was (which is in our case)
Which command should you enter to configure an LLDP delay time of 5 seconds?
the answer would be B.

upvoted 5 times

dropspablo 1 month, 3 weeks ago

lldp hold time in 5 second? Per default is 120 second (4 lldp timer). Lldp reinit per default is 2s, can you set between 1 an 10 seconds. I believe answer is D. lldp reinit 5.

upvoted 1 times

nzieno Most Recent 1 month ago

Answer is D. reinit Delay (in sec) for LLDP initialization on any interface

upvoted 1 times

lamm 2 months ago

Selected Answer: D

Correct answer

upvoted 1 times

dearc 5 months, 2 weeks ago

Selected Answer: D

The correct answer to the question "Which command should you enter to configure an LLDP delay time of 5 seconds?" is D. lldp reinit 5.

Explanation : LLDP (Link Layer Discovery Protocol) is a network protocol used to discover network devices and their properties. The lldp reinit command is used to set the delay time for reinitializing LLDP information after an interface has gone down and come back up. By default, this delay time is set to 2 seconds. To configure it to 5 seconds, you would enter the command lldp reinit 5.

Option A, lldp timer 5000, sets the interval at which LLDP packets are sent, measured in seconds.

Option B, lldp holdtime 5, sets the amount of time a device should retain information received from its neighbors before discarding it, measured in seconds.

Option C, lldp reinit 5000, sets the delay time for reinitializing LLDP information, but the value is in milliseconds, not seconds.

Therefore, the correct answer is D, lldp reinit 5.

upvoted 4 times

iMo7ed 7 months ago

Selected Answer: D

it's D

upvoted 1 times

sol_ls95 7 months, 3 weeks ago

Selected Answer: D

d correct answer

upvoted 1 times

Question #206 *Topic 1*

In a CDP environment, what happens when the CDP interface on an adjacent device is configured without an IP address?

A. CDP becomes inoperable on that neighbor

B. CDP uses the IP address of another interface for that neighbor

C. CDP operates normally, but it cannot provide IP address information for that neighbor

D. CDP operates normally, but it cannot provide any information for that neighbor

Correct Answer: *C*

Although CDP is a Layer 2 protocol but we can check the neighbor IP address with the ג€show cdp neighbor detailג€ command. If the neighbor does not has an IP address then CDP still operates without any problem. But the IP address of that neighbor is not provided.

Community vote distribution

B (71%) C (29%)

ddban Highly Voted 2 years, 4 months ago

I tested in Packet tracer and I don't see that CDP uses an IP address of another interface for the CDP neighbor, it just leaves it empty but still works as usual. I don't see how you guys say it is B, but the simulation on PT says otherwise. I'm going with C.

upvoted 41 times

dropspablo 1 month, 3 weeks ago

According to 4aynick who tested it through GNS3 and the CISCO documentation, answer B is correct, perhaps in Packet Tracer there is indeed this limitation, but it should include the ip address of another interface in an example of a #show cdp neighbors detail command, which does not happen leaving the ip address field empty (as I tested), but in GNS3 it manages to acquire the ip address of another interface (as mentioned by 4aynick), as well as also mentions the CISCO documentation, in this case, taking this into account limitation of Packet Tracer, I agree with answer B “updates the ip address of another interface”.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html#:~:text=Restrictions%20for%20Using%20Cisco%20Discovery%20Protocol,-Cisco%20Discovery%20Protocol&text=Cisco%20Discovery%20Protocol%20is%20not,the%20non%2DIP%20address%20interface

upvoted 1 times

Bhrino 4 months ago

Packet tracer isn’t really reliable for something so in theory I believe it should be c

upvoted 3 times

Brocolee 2 months ago

Dude, I got confused with you here. You said Packet Tracer isn't reliable and therefore you disagree with his reasoning..... But then you agree with his answer. Lol wtf?

upvoted 2 times

Dunedrifter 2 months, 2 weeks ago

If B is true, cdp won't be a reliable network mapping utility. You wouldn't be able to map directly connected devices correctly if B is true.

upvoted 1 times

dropspablo 1 month, 3 weeks ago

unfortunately this is what happens, according to the cisco documentation (and GNS3 according to 4aynick), so we have to pay attention to the repeated IP addresses in the CDP "show" outputs.

upvoted 1 times

Nicocisco 1 year, 6 months ago

yeah tested in lab to, and the switch don't see other interface of my router

upvoted 5 times

Gere Highly Voted 2 years, 7 months ago

The Right answer is B. If a neighbor has no IP address on an interface enabled with Cisco Discovery Protocol, the IP address of another interface will be updated as IP address for the non-IP address interface.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html

upvoted 25 times

Aval0n1 2 years, 5 months ago

What is the another interface? The C is correct. CDP does not need IPs to works normally
https://learningnetwork.cisco.com/s/question/0D53i00000Kt3Mp/how-does-cdp-work-without-l3-addresses

upvoted 6 times

oooMooo 2 years, 4 months ago

Read his link!

"If a neighbor has no IP address on an interface enabled with Cisco Discovery Protocol, the IP address of another interface will be updated as IP address for the non-IP address interface."

B is correct, as stated by Gere.

upvoted 5 times

Nicocisco 1 year, 6 months ago

When tested in the lab, the behaviour described in the link does not occur

upvoted 7 times

berpiy1028 Most Recent 3 days, 13 hours ago

The answer is C. The question didn't mention that other interfaces have IP addresses, so we should assume that other ports are also not configured with IP addresses, unless IP addresses are automatically generated by default.

upvoted 1 times

Sant11 3 weeks, 1 day ago

Selected Answer: B

Restrictions for Using Cisco Discovery Protocol
Cisco Discovery Protocol functions only on Cisco devices.
Cisco Discovery Protocol is not supported on Frame Relay multipoint subinterfaces.
If a neighbor has no IP address on an interface enabled with Cisco Discovery Protocol, the IP address of another interface will be updated as IP address for the non-IP address interface.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html#GUID-3C4F2637-ED36-4EC0-9CD5-B73C0CF9DBEC

upvoted 1 times

Yinxs 4 weeks ago

Selected Answer: B

I tested it in GNS3. B is right. C is correct only if no ip address in any interfaces of this neighbor or the neighbor is a switching with no ipaddress.

upvoted 1 times

tubirubs 1 month, 1 week ago

It's show when do not have IP aderess in the direct interface conected

Router#show cdp neighbors detail

Device ID: Router
Entry address(es):
Platform: cisco ISR4300, Capabilities: Router
Interface: GigabitEthernet0/0/0, Port ID (outgoing port): GigabitEthernet0/0/0
Holdtime: 143

Version :
Cisco IOS Software [Everest], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.6.4,RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Sun 08-Jul-18 04:33 by mcpre

advertisement version: 2
Duplex: full

upvoted 1 times

tubirubs 1 month, 1 week ago

And this, when have IP configured

Router#show cdp neighbors detail

Device ID: Router
Entry address(es):
IP address : 10.0.0.1
Platform: cisco ISR4300, Capabilities: Router
Interface: GigabitEthernet0/0/0, Port ID (outgoing port): GigabitEthernet0/0/1
Holdtime: 166

Version :
Cisco IOS Software [Everest], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.6.4,RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Sun 08-Jul-18 04:33 by mcpre

advertisement version: 2
Duplex: full

upvoted 1 times

_mva 1 month, 3 weeks ago

B is the correct answer. Using GNS3 and assigning an IP address to any interface not connecting to a neighboring switch results in that IP address showing under Management IP in the neighbor details sh command.

upvoted 1 times

AllyK 3 months ago

I came across this issue real life. I was having an issue with being unable to ssh into a switch. I used 'cdp neighbor detail' on a switch I knew was a neighbor. The output was the same as all the others, except there was no IP address. The correct answer is C.

upvoted 2 times

funkymonksarmy 4 months ago

I cheked it and it shows ip address of another interface
B is correct

upvoted 2 times

Jorro99404 4 months ago

Selected Answer: B

"If a neighbor has no IP address on an interface enabled with Cisco Discovery Protocol, the IP address of another interface will be updated as IP address for the non-IP address interface."

upvoted 1 times

dropspablo 4 months, 2 weeks ago

Selected Answer: C

answer C is correct

upvoted 1 times

[Removed] 3 months, 1 week ago

Answer B is correct. It's in Cisco's documentation.

upvoted 1 times

dropspablo 1 month, 3 weeks ago

Thank you, yes correct answer is B.

upvoted 1 times

Kyoxi 5 months ago

Selected Answer: C

c is correct

upvoted 1 times

dearc 5 months, 2 weeks ago

Selected Answer: C

https://learningnetwork.cisco.com/s/question/0D53i00000Kt3MpCAJ/how-does-cdp-work-without-l3-addresses

upvoted 1 times

elixirwell 5 months, 2 weeks ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.htm

upvoted 2 times

linuxlife 6 months ago

Restrictions for Using Cisco Discovery Protocol

Cisco Discovery Protocol functions only on Cisco devices.

Cisco Discovery Protocol is not supported on Frame Relay multipoint subinterfaces.

If a neighbor has no IP address on an interface enabled with Cisco Discovery Protocol, the IP address of another interface will be updated as IP address for the non-IP address interface.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html

upvoted 1 times

cpinac 6 months, 1 week ago

Selected Answer: C

Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that networking applications use to learn about nearby, directly connected devices. Cisco Discovery Protocol is enabled by default. Each device configured for Cisco Discovery Protocol advertises at least one address at which the device can receive messages and sends periodic advertisements (messages) to the well-known multicast address 01:00:0C:CC:CC:CC. Devices discover each other by listening at that address. They also listen to messages to learn when interfaces on other devices are up or go down.

upvoted 2 times

daddydagoth 6 months, 3 weeks ago

Selected Answer: B

Bruh, Cisco's own documentation says it's B then it's bloody B!
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html

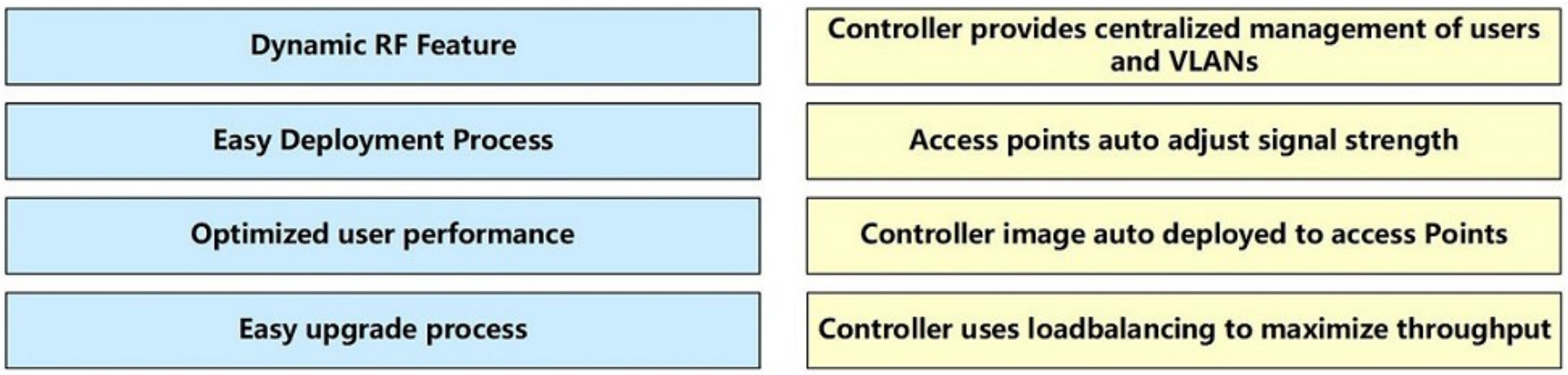
upvoted 3 times

Question #207 *Topic 1*

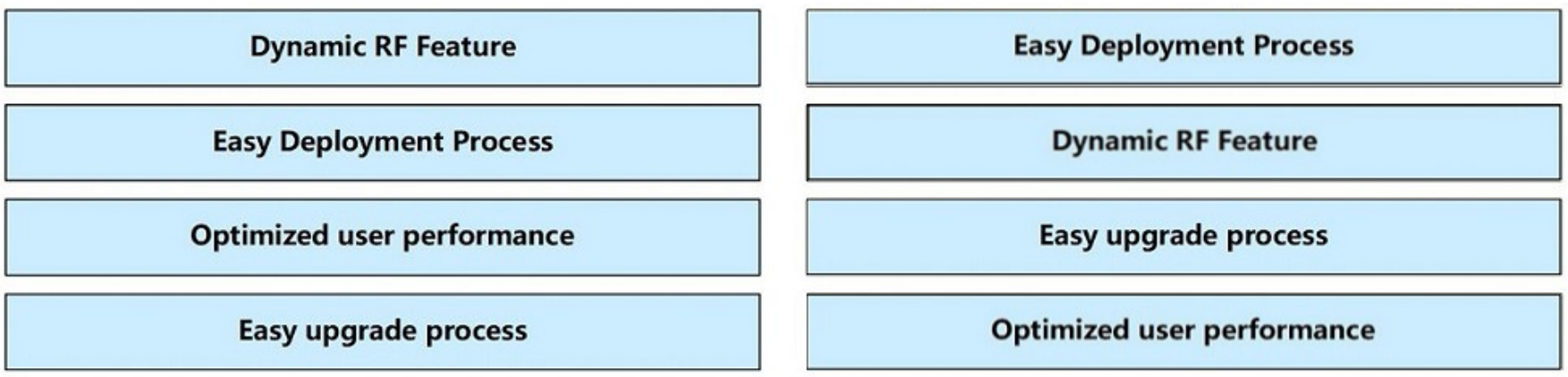
DRAG DROP -

Drag and drop the benefits of a Cisco Wireless Lan Controller from the left onto the correct examples on the right.

Select and Place:



Correct Answer:



Sten111 Highly Voted 2 years, 2 months ago

This confused me at first too, but after some research here are my thoughts;

Easy Deployment Process
Your deployment is setting up users and VLANS, WLANS etc.. The APs you purchase will have software on them already, so it will be an upgrade and not a deployment.

So easy upgrade process should be image auto deployed to access points.

The Dynamic RF Feature one is a bit tough to find decent documentation on but I think it's this;

■ Dynamic transmit power control: The Cisco WLC dynamically controls AP transmit power based on real-time WLAN conditions. In normal instances, power can be kept low to gain extra capacity and reduce interference. The Cisco WLC attempts to balance APs such that they see their neighbors at -65 dBm (a number based on best-practices experience). If a failed AP is detected, power can be automatically increased on surrounding APs to fill the gap created by the loss in coverage.

upvoted 9 times

SScott 2 years, 1 month ago

Yes Sten, that makes sense and the deployment versus upgrade is vague. Deployment pertains more to scripts and part of centralized management with users and vlans. The upgrade would generally refer to image deployment/device management, not directly effecting users nor vlans. The answers provided are correct.

https://www.cisco.com/web/AP/wireless/pdf/Benefits_of_centralizedWLan.pdf

upvoted 3 times

IxlJustinlxl Highly Voted 2 years, 3 months ago

I feel like those are backwards as well.
should be...
easy upgrade = centralized management of users/VLANs
easy deployment = image auto deployed to APs

upvoted 8 times

dropspablo Most Recent 1 month, 3 weeks ago

given answer is correctgiven answer is correct:
2-1
1-2
4-3
3-4

upvoted 2 times

no_blink404 2 months, 3 weeks ago

Dynamic RF: Access points auto adjust signal strength
Easy Deployment: Controller provides centralised management
Optimized User Performance: Controller uses load balancing
Easy upgrade process: Controller image auto deployed to access points.

Let me ask, what are you upgrading? Obviously you are upgrading the firmware on the AP. You don't upgrade users or VLANS, you would create/modify them.

upvoted 2 times

everchosen13 11 months, 3 weeks ago

I think the given answer makes sense. auto deployment of an ISO image makes it seem as if the controller is upgrading the ISO images of the access points on the network.

upvoted 6 times

splashy 11 months, 3 weeks ago

I think the answer makes sense.

you roll out upgrades -> they try to trick you the word auto deploy -> easy upgrade
you deploy vlans, users, groups... i've never heard of upgrading vlans users groups...

upvoted 5 times

johnnd 1 year, 7 months ago

answer with connected points:
https://i.imgur.com/vbuTKnI.png

upvoted 6 times

shakyak 1 year, 10 months ago

HINT: Easy-> Central
Dynamic->Auto
Upgrade->Deploy
Max ->Throughput

upvoted 4 times

shakyak 1 year, 9 months ago

Max->Optimize?

upvoted 4 times

jehangt3 2 years, 3 months ago

i's confused, "controller provides easy management of users and vlan's" how is this a "deployment" process lol

upvoted 3 times

Question #208 *Topic 1*

When configuring an EtherChannel bundle, which mode enables LACP only if a LACP device is detected?

A. Passive

B. Desirable

C. On

D. Auto

E. Active

Correct Answer: *A*
The LACP is Link Aggregation Control Protocol. LACP is an open protocol, published under the 802.3ad.
The modes of LACP are active, passive or on. The side configured as ز€passiveز€ will waiting the other side that should an Active for the Etherchannel to be established.
PAgP is Port-Aggregation Protocol. It is Cisco proprietary protocol. The mode are On, Desirable or Auto. Desirable ز€" Auto will establish an EtherChannel.
An example of how to configure an Etherchannel:

SwitchFormula1>enable -
SwitchFormula1#configure terminal
SwitchFormula1(config)# interface range f0/5 -14
SwitchFormula1(config-if-range)# channel-group 13 mode ?
active Enable LACP unconditionally
auto Enable PAgP only if a PAgP device is detected
desirable Enable PAgP unconditionally
on Enable Etherchannel only
passive Enable LACP only if a LACP device is detected

Community vote distribution

A (100%)

hokieman91 Highly Voted 2 years, 7 months ago
"A" ---- Answer given is correct. Actually a good question since this verifies the knowledge of how LACP works - remember a channel in Passive "wants" to be part of a channel but will sit and wait and only bind if the other end is "Active". I think of "Passive" as follow the leader and "active" as the "do what I say" bully config.
upvoted 17 times

bobert 2 years, 6 months ago
"Active" implies actively negotiating state.
A Passive interface will not enable LACP if the other end is also Passive (LACP) ..
So only an Active interface will enable LACP if either Active or Passive LACP interface is connected
upvoted 6 times

bobert 2 years, 6 months ago
correction ... read again and A is correct
upvoted 2 times

sdokmak 2 years, 2 months ago
I also thought same as you but yeah it is "Passive", Joe_Q's explanation was pretty good.
upvoted 2 times

Zerotime0 2 years, 7 months ago
Good clarity
upvoted 3 times

SScott 2 years, 1 month ago
Right, A is the most direct answer Passive.

https://www.ccna6rs.com/6-2-4-packet-tracer-configure-etherchannel-answers/
upvoted 1 times

ProgSnob Highly Voted 1 year, 10 months ago
The wording is a bit obfuscating. I keep rereading it and feeling like depending on how you perceive the wording, both A and E could be correct.

upvoted 5 times

Ciscoman021 8 months, 1 week ago

you are not alone. :)

upvoted 3 times

Bhrino Most Recent 4 months ago

Selected Answer: A

I think the wording of the question is weird but the reason it's passive is because the question ask which mode will only activate lacp if it dectects lacp which is passive. Passive in a way listens to what it's being told

upvoted 1 times

[Removed] 7 months ago

The question is not clear

upvoted 3 times

gc999 6 months, 1 week ago

Agree. It doesn't say which LACP device is detected. If it said "This device is detected", then answer is passive; if it said "The other device is detected", then answer is active

upvoted 1 times

ZUMY 1 year, 3 months ago

A is correct

upvoted 1 times

ismatdmour 1 year, 6 months ago

Selected Answer: A

passive Enable LACP only if a LACP device is detected. This is how the passive is described

upvoted 1 times

LKPN 1 year, 7 months ago

Selected Answer: A

From Packet Tracer
Switch(config-if-range)#channel-group 1 mode ?
active Enable LACP unconditionally
auto Enable PAgP only if a PAgP device is detected
desirable Enable PAgP unconditionally
on Enable Etherchannel only
passive Enable LACP only if a LACP device is detected

upvoted 3 times

LilGhost_404 1 year, 7 months ago

The question is not really clear.
The next question will be how a LACP device is detected? Is it because the remote device sent a LACPdu? Or the local device sent it and the remote respond it?

upvoted 2 times

johnnd 1 year, 7 months ago

LACP packets are exchanged between ports in these modes:
•Active—Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
•Passive—Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. In this mode, the port channel group attaches the interface to the bundle.

https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/gigeth.html

upvoted 1 times

dave1992 1 year, 9 months ago

lets say the other side is either active or passive. doesnt matter, but putting the opposite side as Active will always make the etherchannel. (as long as the other side is active or passive)
active is the best answer.

upvoted 3 times

Hodicek 1 year, 9 months ago

LACP ACTIVE PASSIVE, IN THE QUESTION ONE IS DETECTED SO IT IS ACTIVE SO OTHER SHOULD BE PASSIVE

upvoted 2 times

ZUMY 2 years, 4 months ago

A is correct

upvoted 4 times

asd34534 2 years, 5 months ago

Switch(config-if-range)#channel-group 1 mode ?
active Enable LACP unconditionally
auto Enable PAgP only if a PAgP device is detected
desirable Enable PAgP unconditionally
on Enable Etherchannel only

passive Enable LACP only if a LACP device is detected

the question is taken from the switch explanation above
i think the answer should me active but i will go with passive

upvoted 3 times

admin1982 2 years, 7 months ago

The correct answer should be E..."Active"

upvoted 3 times

gc999 6 months, 1 week ago

Agree. I set the mode to "Active", so it can "detected" the other end.

upvoted 1 times

Taps 2 years, 7 months ago

The word passive means the opposite: That it has found a connection and its up and ready. Active is also the opposite: It doesn't have a connection and so its not looking for one.

upvoted 3 times

Zerotime0 2 years, 7 months ago

Not clear question to me. Wouldnt it be active? Then thats how it will actively search out another lacp enabled device? If its passive its not active in search for one... can some one chime in on this ?

upvoted 3 times

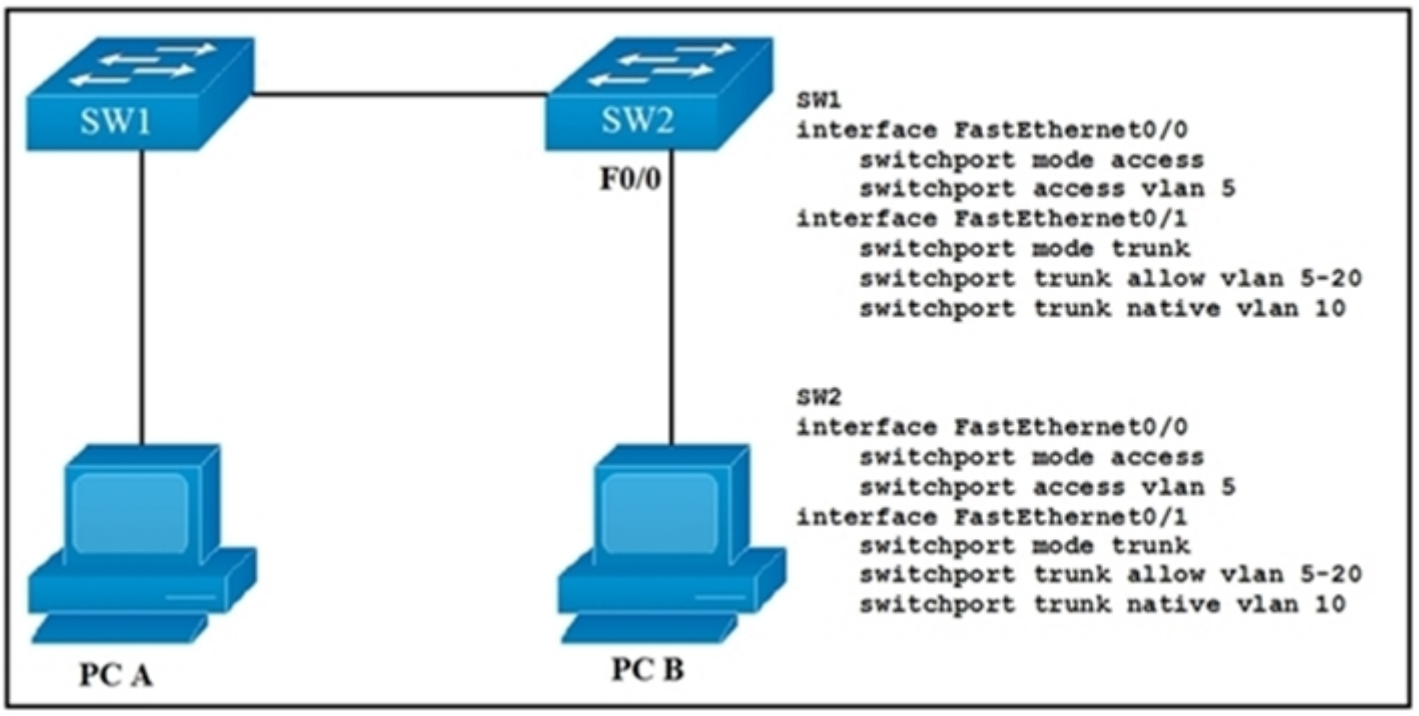
Joe_Q 2 years, 5 months ago

enables LACP only if a LACP device is detected, keyword is here is "detected". Active does not detect, it is always sending out LACP negotiation messages. Passive is always detecting, waiting for a negotiation message.

upvoted 12 times

Question #209 *Topic 1*

Refer to the exhibit. Which VLAN ID is associated with the default VLAN in the given environment?



A. VLAN 1

B. VLAN 5

C. VLAN 10

D. VLAN 20

Correct Answer: *A*

Community vote distribution

A (100%)

ZayaB Highly Voted 2 years, 7 months ago

The question is trying to trick us. Answer A is correct because Cisco switches always have VLAN 1 as the default VLAN, which is needed for many protocol communication between switches like spanning-tree protocol for instance.

You can't change or even delete the default VLAN, it is mandatory.

The native VLAN is the only VLAN which is not tagged in a trunk, in other words, native VLAN frames are transmitted unchanged.

https://community.cisco.com/t5/switching/what-is-difference-between-default-vlan-and-native-vlan/td-p/2095204

upvoted 68 times

Zerotime0 2 years, 7 months ago

Ty for clarifying.got it .a is right

upvoted 3 times

velrisan 2 years, 2 months ago

ZayaB is right, this question was made to confuse, remember the default vlan in a switch cisco is the vlan number 1, the image that you see in this question is only to make doubt.

If we see with careful, the question is given the answer, when we see the word default. That's mean that is default vlan. So

The answer is "A"

upvoted 3 times

hasbulla01 Highly Voted 10 months ago

Selected Answer: A

DEFAULT VLAN not NATIVE VLAN jeje

upvoted 5 times

Rether16 Most Recent 5 months, 1 week ago

I fell for this one and selected Vlan10. Dohh!

upvoted 1 times

GreatDane 1 year, 3 months ago

A. VLAN 1

As soon as the switches are powered on, the default VLAN is VLAN 1. Then, you execute the commands on SW1:

interface ...
switchport mode ...
switchport access ...
interface ...
switchport mode ...
switchport trunk ...
switchport trunk native vlan 10

Same happens on SW2:

interface ...
switchport mode ...
switchport access ...
interface ...
switchport mode ...
switchport trunk ...
switchport trunk native vlan 10

Now, the NATIVE VLAN on both sides of the trunk is VLAN 10. But the DEFAULT VLAN on both switches in still VLAN 1.

Correct Answer

B. VLAN 5

Wrong answer.

C. VLAN 10

Wrong answer.

D. VLAN 20

Wrong answer.

upvoted 4 times

ZUMY 1 year, 3 months ago

A is correct
Native vlan can be any #
But default vlan is always 1

upvoted 1 times

Ric4444 1 year, 3 months ago

Not sure if this is trying to trick us into maybe thinking that the answer is vlan 1 actually. The wording of the question asking "which VLAN ID is associated to the default VLAN (1) as we know all cisco switches have vlan 1 as default. But question states "Refer to the exhibit.." so why even throw that in their with a bunch of commands if not to just ask what a default vlan of a cisco switch is ?? Poor question if you ask me all around.

upvoted 3 times

DUMPledore 11 months, 2 weeks ago

exactly, it was confusing because of the "given environment" at the question

upvoted 1 times

timskis2 1 year, 3 months ago

it is vlan 10 because it states "in the given environment"

upvoted 2 times

ScorpionNet 1 year, 4 months ago

A is right because VLAN 1 is used by default.
But a poorly added exibit.

upvoted 1 times

ziok 1 year, 6 months ago

Cisco switches have a factory configuration in which default VLANs are preconfigured to support various media and protocol types. The default Ethernet VLAN is VLAN 1. It is a security best practice to configure all the ports on all switches to be associated with VLANs other than VLAN 1

upvoted 1 times

onikafei 1 year, 7 months ago

Selected Answer: A

VLAN 1 is always default

upvoted 1 times

babaKazoo 1 year, 7 months ago

VLANs 1 and 1001-1005 are default VLANs and can not be changed.

upvoted 1 times

Hodicek 1 year, 9 months ago

TRIED ON PACKET TRACER, IT CREATED VLAN 5 ONLY , SO IT DIDN'T CREATE VLAN 10 AT ALL, SO THE DEFAULT / NATIVE VLAN IS VLAN 1.
THANKS

upvoted 1 times

dave1992 1 year, 10 months ago

I hate these gotcha questions. It's so stupid to even make it a question if the default vlan is always 1. Why even ask in this way? Just ask what the default vlan is

upvoted 4 times

soRwatches 6 months, 1 week ago

exactly, this is BS.

upvoted 1 times

firstblood 2 years ago

The buzzed word is "default". Even though VLAN 10 is configured as the native VLAN.

upvoted 2 times

aleksos 2 years, 1 month ago

Tricky one...
A is correct.

upvoted 2 times

Micah7 2 years, 3 months ago

Zaya B is correct:

The question is trying to trick us. Answer A is correct because Cisco switches always have VLAN 1 as the default VLAN, which is needed for many protocol communication between switches like spanning-tree protocol for instance.

You can't change or even delete the default VLAN, it is mandatory.

The native VLAN is the only VLAN which is not tagged in a trunk, in other words, native VLAN frames are transmitted unchanged. You can and should (security precaution best practice) change the "native" vlan traffic to another vlan (10 here). HOWEVER, the "default" vlan no matter what is Vlan 1. You are just changing the "native"

upvoted 2 times

jerry19 2 years, 4 months ago

There is only one vlan associated with the default 1 vlan. And that is and always will be vlan 1. You can never delete vlan 1. The only thing you can do is move ports out of the default vlan, into 'parking lot,' or to an active vlan. Agree with Answer A.

upvoted 2 times

Question #210 *Topic 1*

Which two VLAN IDs indicate a default VLAN? (Choose two.)

A. 0

B. 1

C. 1005

D. 1006

E. 4096

Correct Answer: *BC*

VLAN 1 is a system default VLAN, you can use this VLAN but you cannot delete it. By default VLAN 1 is use for every port on the switch. Standard VLAN range from 1002-1005 it's Cisco default for FDDI and Token Ring. You cannot delete VLANs 1002-1005. Mostly we don't use VLAN in this range.

Community vote distribution

BC (100%)

ZUMY Highly Voted 2 years, 4 months ago

B & C are correct
Deafult Vlans
1
1002
1003
1004
1005

upvoted 8 times

shumps Most Recent 2 months ago

show vlan
this command will help you see the default vlans
1
1002
1003
1004
1005

upvoted 1 times

[Removed] 3 months, 1 week ago

Selected Answer: BC

1 and 1005

upvoted 1 times

linuxlife 6 months ago

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/1, Gig0/2
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

upvoted 1 times

cormorant 9 months, 3 weeks ago

default vlans:
1
1002
1003
1004
1005

just think 1,2,3,4 and 5.
then arrange this series like this:

1, 1002,1003,1004,1005
it's always 1, 1 + 002, 1+ 003, 1+ 004, 1 +005
upvoted 2 times

GreatDane 1 year, 3 months ago
Ref: LAN Switching - Configuring VLANs [Support] - Cisco Systems

"...
VLAN Ranges
...
Table 17-1 VLAN Ranges
...
1...Cisco default. You can use this VLAN but you cannot delete it.
...
1002-1005... Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002-1005.
..."

A. 0

Wrong answer.

B. 1

Correct answer.

C. 1005

Correct answer.

D. 1006

Wrong answer.

E. 4096

Wrong answer.
upvoted 2 times

ScorpionNet 1 year, 4 months ago
B and C are right
upvoted 1 times

onikafei 1 year, 7 months ago
I always see 0 as a default but I mix it up with priority. Its a bit of a trick question to watch for
upvoted 2 times

echarles10 2 years, 8 months ago
BC is correct .....VLAN 1 is a system default VLAN, you can use this VLAN but you cannot delete it. By default VLAN 1 is use for every port on the switch.
Standard VLAN range from 1002-1005 it's Cisco default for FDDI and Token Ring. You cannot delete VLANs 1002-1005. mostly we don't use VLAN in this range
upvoted 3 times

Question #211 *Topic 1*

Which two pieces of information about a Cisco device can Cisco Discovery Protocol communicate? (Choose two.)

A. the native VLAN

B. the trunking protocol

C. the VTP domain

D. the spanning-tree priority

E. the spanning-tree protocol

Correct Answer: *AC*

hokieman91 Highly Voted 2 years, 7 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html

The information contained in Cisco Discovery Protocol advertisements varies based on the type of device and the installed version of the operating system. Some of the information that Cisco Discovery Protocol can learn includes:

Cisco IOS version running on Cisco devices
Hardware platform of devices
IP addresses of interfaces on devices
Locally connected devices advertising Cisco Discovery Protocol
Interfaces active on Cisco devices, including encapsulation type
Hostname
Duplex setting
***VLAN Trunking Protocol (VTP) domain
***Native VLAN

upvoted 32 times

GreatDane Highly Voted 1 year, 3 months ago

Ref: Cisco Discovery Protocol Configuration Guide, Cisco IOS Release 15M&T

"C H A P T E R 1
Cisco Discovery Protocol Version 2
...
Cisco Discovery Protocol
...
The information contained in Cisco Discovery Protocol advertisements varies based on the type of device and the installed version of the operating system. Some of the information that Cisco Discovery Protocol can learn includes:

• Cisco IOS version running on Cisco devices
• Hardware platform of devices
• IP addresses of interfaces on devices
• Locally connected devices advertising Cisco Discovery Protocol
• Interfaces active on Cisco devices, including encapsulation type
• Hostname
• Duplex setting
• VLAN Trunking Protocol (VTP) domain
• Native VLAN
..."

A. the native VLAN

Correct answer.

B. the trunking protocol

Wrong answer.

C. the VTP domain

Correct answer.

D. the spanning-tree priority

Wrong answer.

E. the spanning-tree protocol

Wrong answer.

upvoted 5 times

ZUMY Most Recent 1 year, 3 months ago

A & C are correct

upvoted 2 times

dicksonpwc 2 years, 1 month ago

CDP Advertisement includes the following:
VTP Management Domain – 0x0009 (CDPv2)
Native VLAN – 0x000a (CDPv2)

upvoted 5 times

Question #212 *Topic 1*

After you deploy a new WLAN controller on your network, which two additional tasks should you consider? (Choose two.)

A. deploy load balancers

B. configure additional vlans

C. configure multiple VRRP groups

D. deploy POE switches

E. configure additional security policies

Correct Answer: *AE*

Community vote distribution

BE (50%) DE (25%) AE (25%)

Zerotime0 Highly Voted 2 years, 6 months ago

Found old exams from 200-225 exam and there ,poe and security are the answers....not load bal.

upvoted 25 times

Request7108 8 months, 4 weeks ago

I think you're correct on D and E because load balancers are not mentioned in the deployment guide anywhere. There are client load balancing options for the AP and LAG where load balancing is done in the links between the WLC and switch.

upvoted 1 times

Targaryen Highly Voted 2 years, 4 months ago

Remember guys: "two additional tasks should you CONSIDER?"
So it's everything working.
VLANs are must-have. Not additional.
POE are fine, but remember that everything is working in this scenario.
I go for A and E.

upvoted 21 times

Kaffi 2 years ago

yeah but then security polices seem like must haves not additional.

upvoted 5 times

gc999 6 months, 1 week ago

I agree with you IF the question is "After the WLAN controller has been deployed, what else CAN be considered?"

upvoted 1 times

battery1979 1 year, 2 months ago

How are we doing Power Over Ethernet via wireless?

upvoted 1 times

wakaish Most Recent 1 week, 3 days ago

B. Configure additional VLANs: If you are deploying multiple SSIDs or different wireless networks with different purposes (e.g., guest network, employee network, IoT network), you may need to configure additional VLANs on your network to segregate and manage traffic effectively.

E. Configure additional security policies: Wireless networks require robust security policies to protect against unauthorized access and threats. You should configure additional security policies such as WPA/WPA2 encryption, authentication methods, and access control lists to ensure the security of your WLAN.

The other options (A, C, D) may be necessary in certain network configurations, but they are not typically among the first tasks to consider when deploying a new WLAN controller.

upvoted 1 times

dropspablo 4 months, 2 weeks ago

Selected Answer: AE

The "deploy load balancers" option seems to me to be related to one of the 8 WLC activities that I studied, which would be the "Dynamic Client Load Balancing" activity, where the WLC can distribute the client load between nearby APs.
Someone correct me if I'm wrong!?

upvoted 1 times

cr0minus 4 months, 2 weeks ago

Selected Answer: DE

I think these are the correct ones

upvoted 2 times

dearc 5 months, 2 weeks ago

Selected Answer: BE

After deploying a new WLAN (Wireless Local Area Network) controller on the network , there are various tasks that need to be performed to ensure the network runs smoothly. Some of the tasks that should be considered include configuring additional VLANs to manage network traffic effectively and securely, and configuring additional security policies to protect the network from potential threats.

Option A, deploying load balancers, might not be necessary after deploying a new WLAN controller, depending on the size and complexity of the network.

Option C, configuring multiple VRRP (Virtual Router Redundancy Protocol) groups, is not directly related to WLAN deployment and might not be necessary in all cases.

Option D, deploying POE (Power over Ethernet) switches, might not be needed if the existing switches meet the power requirements of the WLAN controller and access points

upvoted 3 times

elixirwell 5 months, 2 weeks ago

Selected Answer: BE

The text you selected is a question that asks what two additional tasks should be considered after deploying a new WLAN controller on your network. The answer to this question is B. Configure additional VLANs and E. Configure additional security policies.

VLANs are used to segment network traffic and provide additional security. With a WLAN controller, you can configure multiple VLANs to separate guest traffic from corporate traffic or to separate different types of corporate traffic.

Additional security policies can be configured to ensure that only authorized users are able to access the network and that data is protected from unauthorized access.

upvoted 1 times

[Removed] 6 months, 4 weeks ago

My answer is BE. Keyword, ''after'', ''additional task''

upvoted 1 times

GreatDane 1 year, 3 months ago

Ref: Cisco 5520 Wireless LAN Controller Deployment Guide

Page 22
2nd figure on page.

A. deploy load balancers

Correct answer.

B. configure additional vlans

Wrong answer.

C. configure multiple VRRP groups

Wrong answer.

D. deploy POE switches

Wrong answer.

E. configure additional security policies

Correct answer.

upvoted 6 times

ZUMY 1 year, 3 months ago

Going with A & E

upvoted 1 times

onikafei 1 year, 7 months ago

Selected Answer: AE

It looks like a&e are correct

upvoted 1 times

Dking001 2 years, 2 months ago

B & E...
Because once a new WLAN is deployed, a network admim would want to add additional vlan for the new device different from the management vlan, from security point of view!

upvoted 4 times

Joe_Q 2 years, 5 months ago

Reference question #101
Optimized user performance - Controller uses loadbalancing to maximize throughput.

A & E are correct.

upvoted 9 times

Zerotime0 2 years, 7 months ago

Security policies and additional vlans kinda go hand in hand. And if e is right. Then b should compliment it. Not a.

upvoted 2 times

SScott 2 years ago

That's true and should be the prime objective. However, I believe this question makes the assumption initial VLANs for the new WLAN are in place ahead of deployment, so additional tasks would not be to deploy further VLANs. Addressing complaining users/VIPs will often come up as a top priority and consideration so Load Balancing is a top additional task. As we know, users will quickly test the limits of what they are not supposed to do therefore better have security policies/ACLs/ content filtering in place ahead of more POE switches or segmenting with more VLANs. We assume newly staged and/or existing POE requirements are sufficient with the new deployment; otherwise it cannot be up and running. Still see A & E as the top two.

upvoted 6 times

Techno_Head 2 years, 7 months ago

B and D for me. You want POE so you can deploy access points and vlans so you can link dynamic interfaces to VLANs. I see no logical reason for the answer other than that's what's on your to do list. I'm sticking with my logic on this one if it pops up on the exam.

upvoted 4 times

SUKABLED 2 years, 7 months ago

A lot of questions are really made up to confuse you..i see no reason to not answer B here as well...but hey i guess it is waht it is...A & D

upvoted 1 times

SUKABLED 2 years, 7 months ago

correction: A&E i mean

upvoted 2 times

Ali526 2 years, 8 months ago

May be.
D is also very important.

upvoted 4 times

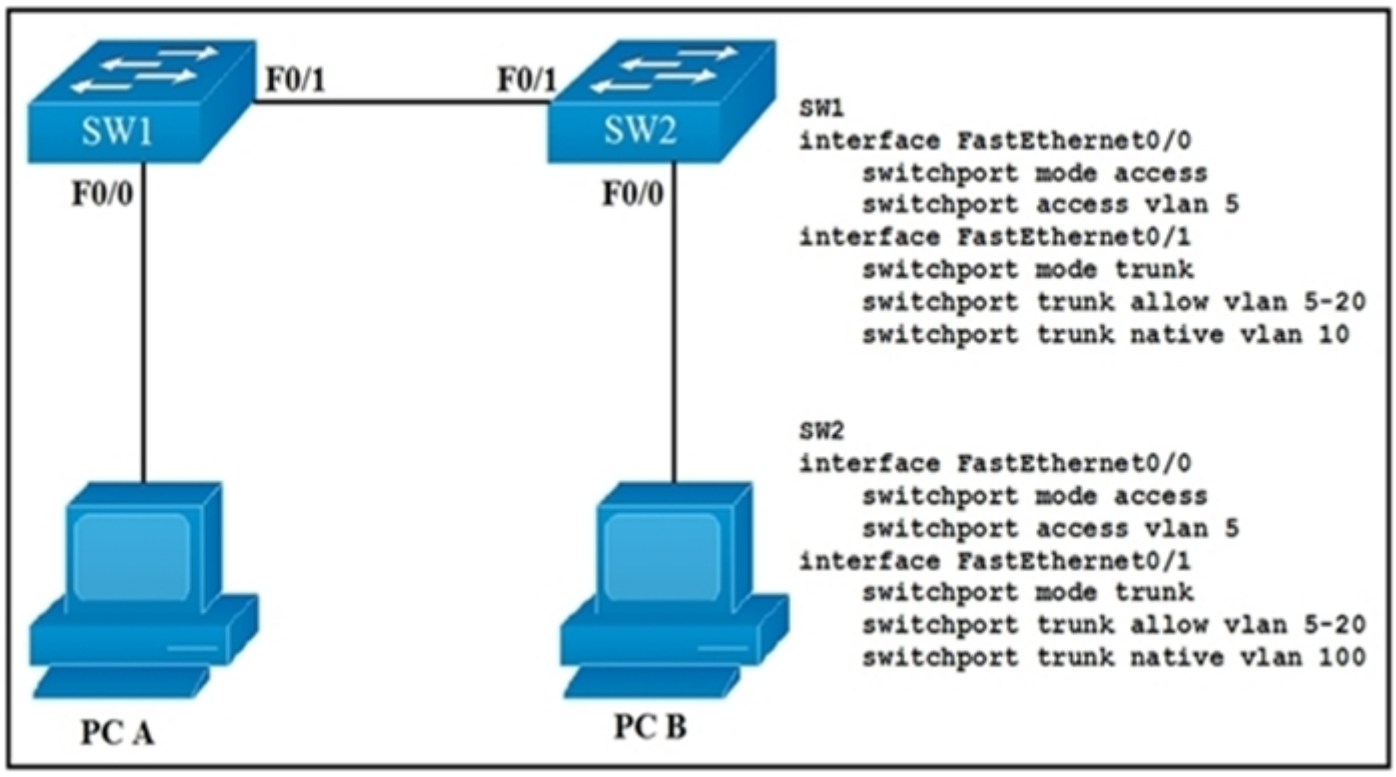
SScott 2 years, 3 months ago

Yes, A and E. In order of importance security policies and load balancing should be at the top of the list. POE would likely be third in line mainly because this would be a budgeted consideration and not necessarily an immediate post-deployment task requirement.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-6/b_Cisco_Wireless_LAN_Controller_Configuration_Best_Practices.html#concept_574CD7840A6C4DBBA7CF465C2C90304B

upvoted 2 times

Question #213 *Topic 1*

Refer to the exhibit. How will switch SW2 handle traffic from VLAN 10 on SW1?



A. It sends the traffic to VLAN 10.

B. It sends the traffic to VLAN 100.

C. It drops the traffic.

D. It sends the traffic to VLAN 1.

Correct Answer: *B*

Since SW-1 is configured native VLAN is VLAN10, so traffic coming out of VLAN-10 is untagged, & goes directly to SW-2 Native VLAN: VLAN100, due to VLAN mismatch.

Community vote distribution

B (60%) C (36%) 4%

hokieman91 Highly Voted 2 years, 7 months ago

Answer given correct - SW1 trunk native vlan 10 command will drop the tag from any Vlan 10 traffic and send it out to SW2 without a tag SW2 see's untagged traffic from SW1 and applies it to Native Vlan 100.
Earlier question on this site where the answer also states that even though switches will report a Native Vlan mismatch, they will still pass traffic and essentially merge these 2 Vlan's together (unwanted scenario and switch will continue to throw warnings).

upvoted 25 times

DARKK 1 year, 3 months ago

But VLAN 100 is not allowed (5-20), so it would get dropped if it thinks the traffic is for VLAN 100.

upvoted 3 times

dropspablo 4 months, 2 weeks ago

ChatGPT:
Native VLAN is always allowed because it is the VLAN used for device management in a VLAN network. It is not considered a regular user VLAN, but an infrastructure VLAN. This is why it is always allowed on a trunk port, regardless of the "switchport trunk native vlan" command configured on the port.

upvoted 2 times

battery1979 1 year, 2 months ago

It's a native VLAN mismatch, SW2 VLAN 100 will process the traffic from SW1 VLAN 10 because it is untagged, and untagged traffic goes into the native VLAN.

upvoted 4 times

Dpsypher Highly Voted 1 year, 1 month ago

Selected Answer: B

The fact that the community is split on this means I am going to have trouble trusting the answers from you all as a whole. The answer is B. Do not believe anything else.
If traffic is in a native VLAN it is UNTAGGED, meaning it does not have an assignment. One switch interprets untagged as VLAN 10, the other as VLAN 100, so if untagged so the identification of VLAN is based on location. It will remain untagged where ever it goes but switches will identify it as they have been told.

upvoted 16 times

DoBronx 10 months, 3 weeks ago

facts. Im a novice with a year of experience and only been studying by watching jeremy IT on youtube and i chose B
upvoted 4 times

Yeeeeeeee Most Recent 1 week ago

Selected Answer: C

https://learningnetwork.cisco.com/s/article/effects-of-mismatched-native-vlans-on-a-trunk-link
Native Vlan mismatched
upvoted 1 times

[Removed] 3 months, 1 week ago

Selected Answer: B

Answer B
upvoted 1 times

properchad 3 months, 3 weeks ago

I did this on gns3 to verify and yes it does drop the frame. I am going with answer c
If using ##sh interfaces trunk## you dont see native vlan on allowed vlan section then any untagged frame will be dropped.
I hope this will help or you guys can further verify on lab yourself and even leave reply on the thread
upvoted 1 times

ac89l 4 months ago

Selected Answer: B

answer is B
upvoted 1 times

Jorro99404 4 months ago

Selected Answer: B

Since SW-1 is configured native VLAN is VLAN10, so traffic coming out of VLAN-10 is untagged, & goes directly to SW-2 Native VLAN: VLAN100, due to VLAN mismatch.
upvoted 1 times

Isuzu 4 months, 1 week ago

Selected Answer: B

any traffic from VLAN 10 that enters switch SW2 will be untagged, and switch SW2 will forward it to the native VLAN, which is VLAN 100 in this case.

Note that if VLAN 10 was also configured on switch SW2, then the traffic would be forwarded to VLAN 10 instead of VLAN 100.
upvoted 1 times

[Removed] 4 months, 1 week ago

Answer is C. It drops the traffic because spanning-tree will block SW1 trunk port. Tested on packet tracer for proof of concept. Once I removed spanning-tree VLAN 100 on SW2 the packet went through via VLAN 100.
You will notice that cdp and spanning tree give you a warning when you have mismatched native vlans on a trunk. Spanning Tree actually puts both of the ports in a bkn (broken) state and not allow any traffic in our out. This is why you have to disable spanning tree on the ports in order to see vlan leaking as a result of mismatched native vlans.
upvoted 1 times

elixirwell 5 months, 2 weeks ago

Selected Answer: B

This is because SW1 is configured with VLAN 10 as its native VLAN. Traffic coming out of VLAN 10 is untagged and goes directly to SW2 Native VLAN which is VLAN 100
upvoted 1 times

linuxlife 6 months ago

B is correct. Simulated in Packet Tracer.
upvoted 1 times

linuxlife 6 months ago

interface GigabitEthernet0/1
switchport trunk native vlan 10
switchport mode trunk

interface GigabitEthernet0/1
switchport trunk native vlan 100
switchport mode trunk

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>

upvoted 2 times

daddydagoth 6 months, 3 weeks ago

Selected Answer: B

It's B. The swtich won't drop the traffic, it will assume that the untagged frame it recieved the native vlan. It will thus forward the traffic on Vlan 100.

upvoted 2 times

[Removed] 6 months, 4 weeks ago

My answer is B. Vlan mismatch is still working, but it has become a security issue.

upvoted 1 times

Midus 7 months, 3 weeks ago

B is correct.
For example, if switch SW1 sends a frame using native VLAN 1 on an 802.1Q trunk, SW1 does not add a VLAN header, as is normal for the native VLAN. When switch SW2 receives the frame, noticing that no 802.1Q header exists, SW2 assumes that the frame is part of SW2's configured native VLAN. If SW2 has been configured to think VLAN 2 is the native VLAN on that trunk, SW2 will try to forward the received frame into VLAN 2. (This effect of a frame being sent in one VLAN but then being believed to be in a different VLAN is called VLAN hopping.)

upvoted 1 times

sol_ls95 7 months, 3 weeks ago

Selected Answer: B

untagged traffic goes into the native VLAN from sw2

upvoted 1 times

joyboy92 7 months, 3 weeks ago

Native VLAN mismatch can cause some major issues and security implications such as:
Misdirected traffic - Frames, originating in the VLAN configured as Native, are sent untagged across the trunk. Upon receiving on the other side on the link, they are forwarded in different VLAN because trunk settings don't match on both sides.
VLAN hopping - malicious traffic can cross VLAN boundaries.
https://www.networkacademy.io/ccna/ethernet/trunk-native-vlan

upvoted 1 times

binrayelias 8 months ago

Answer is C cuz If native vlan mismatch in trunk, switch 2 will block that traffic so it will be dropped. other vlan will forwarded normally.

upvoted 1 times

Question #214 *Topic 1*

Which two commands can you use to configure an actively negotiate EtherChannel? (Choose two.)

A. channel-group 10 mode on

B. channel-group 10 mode auto

C. channel-group 10 mode passive

D. channel-group 10 mode desirable

E. channel-group 10 mode active

Correct Answer: *DE*

Community vote distribution

DE (100%)

jerry19 Highly Voted 2 years, 4 months ago

D and E, Answer D is used to 'actively negotiate' for PAGP and answer E is used to 'actively negotiate for LACP.

upvoted 13 times

GreatDane Highly Voted 1 year, 3 months ago

ACTIVE NEGOTIATION means "STARTING the negotiation process to create an EtherChannel link", and NOT waiting for someone else to start it.

There are two EtherChannel protocols: LACP (open standard) and PAgP (Cisco proprietary).

A. channel-group 10 mode on

The ON option doesn't enable negotiation (EtherChannel is always ON).
Wrong answer.

B. channel-group 10 mode auto

PAgP syntax, the AUTO option means PASSIVE negotiation (a device waits for a second device to start the negotiation).
Wrong answer.

C. channel-group 10 mode passive

LACP syntax, the PASSIVE option means PASSIVE negotiation (a device waits for a second device to start the negotiation).
Wrong answer.

D. channel-group 10 mode desirable

PAgP syntax, the DESIRABLE option means ACTIVE negotiation.
Correct answer.

E. channel-group 10 mode active

LACP syntax, the ACTIVE option means ACTIVE negotiation.
Correct answer.

upvoted 10 times

Mashj 1 year, 1 month ago

Thank you for easy explanation

upvoted 2 times

Luinus Most Recent 7 months, 4 weeks ago

this is same question in my exam but the choices only is:
active
on
passive
auto

there is no desirable in the choices

upvoted 1 times

DUMPledore 9 months, 1 week ago

Selected Answer: DE

Agree with GreatDane

upvoted 1 times

ZUMY 1 year, 3 months ago

D & E are correct
Desirable mode: Desirable mode in Port Aggregation Protocol (PAgP) initiates the negotiation and tries to form EtherChannel with other end.
Active Mode: Active Mode in Link Aggregation Control Protocol (LACP) initiates the negotiation and tries to form EtherChannel with other end.

upvoted 1 times

johnnd 1 year, 7 months ago

Switch(config-if-range)#channel-group 1 mode ?
active Enable LACP unconditionally
auto Enable PAgP only if a PAgP device is detected
desirable Enable PAgP unconditionally
on Enable Etherchannel only
passive Enable LACP only if a LACP device is detected

upvoted 1 times

AudreyLin 1 year, 9 months ago

why not c and E?

upvoted 1 times

laurvy36 1 year, 9 months ago

because it doent specify PagP or LACP

upvoted 1 times

PraygeForPass 1 year, 4 months ago

It's not C and E because the question is asking what commands will actively pursue an etherchannel. Passive from LACP and auto from PAgP do not actively pursue an etherchannel, they will only join if someone is actively pushing for one, like active or desirable.

upvoted 1 times

Pkard 1 year, 10 months ago

Shouldn't it be Active and Passive?

upvoted 1 times

dave1992 1 year, 11 months ago

for LACP you would set #channel-group 1 mode active and the other side also as active or passive
for PaGP you would set it #channel-group 1 mode Desirable and the other side of the link Desirable or Auto

upvoted 2 times

dicksonpwc 2 years, 1 month ago

PagP modes: auto | Desirable
LACP modes: active | pasive

upvoted 10 times

Ali526 2 years, 8 months ago

"negotiable" not "negotiate".
The answer is correct, though.

upvoted 2 times

Question #215 *Topic 1*

How does STP prevent forwarding loops at OSI Layer 2?

A. TTL

B. MAC address forwarding

C. Collision avoidance

D. Port blocking

Correct Answer: *D*

Community vote distribution

D (87%) 13%

mikachuu85 Highly Voted 1 year, 7 months ago

Selected Answer: D

Correct answer is D as TTL is Layer 3 which won't apply in this scenario. Thus, answer A is wrong.

upvoted 16 times

laurvy36 1 year, 7 months ago

true, that is the explenation

upvoted 1 times

dick3311 Most Recent 10 months, 3 weeks ago

Selected Answer: D

corret is D

upvoted 1 times

i_am_confused 1 year, 2 months ago

Selected Answer: D

100% D. As others have said TTL is layer 3

upvoted 1 times

ZUMY 1 year, 3 months ago

D is correct

upvoted 1 times

lohaN73 1 year, 3 months ago

TTL is a layer 3 issue,not works at Layer 2

upvoted 1 times

onikafei 1 year, 7 months ago

Selected Answer: D

Learned about looping in other training as well. Port blocking prevents traffic from getting stuck going in circles between other ports. I would have to say it's D in this case

upvoted 1 times

galgold 1 year, 7 months ago

Selected Answer: D

confirmed

upvoted 1 times

SparkySM 1 year, 7 months ago

its should be D. not A

upvoted 1 times

wpena 1 year, 9 months ago

Selected Answer: A

The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops). If BPDUs are not received on a non-designated port, and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state.

upvoted 3 times

aike92 1 year, 8 months ago

Correct Ans is D.
(if i'm not mistaken) TTL is a Layer 3 mechanism that routers decrement after a successful hop

upvoted 4 times

Tengereni 2 years, 4 months ago

explanation

upvoted 2 times

ZUMY 2 years, 4 months ago

D is correct

upvoted 4 times

Question #216 *Topic 1*

Which two statements about VTP are true? (Choose two.)

A. All switches must be configured with the same VTP domain name

B. All switches must be configured to perform trunk negotiation

C. All switches must be configured with a unique VTP domain name

D. The VTP server must have the highest revision number in the domain

E. All switches must use the same VTP version

Correct Answer: *AE*

Community vote distribution

AE (39%) AD (39%) DE (16%) 3%

[Removed] Highly Voted 2 years, 5 months ago

"All switches in a VTP domain must have the same domain name, but they do not need to run the same VTP version."https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvtp.html#wp1107364

A&D are correct

upvoted 31 times

jerry19 2 years, 4 months ago

I used your link and think the answer is A & D based off:
"Before adding a VTP client switch to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain. See the "Adding a VTP Client Switch to a VTP Domain" section for the procedure for verifying and resetting the VTP configuration revision number."

upvoted 3 times

SScott 2 years, 3 months ago

The wording is tricky in D, and the VTP Switch, not server must have the highest rev else the information can be erased from the server.... So A & D are right.

upvoted 2 times

SScott 2 years, 3 months ago

Correction to my comment above. A-- VTP Domain Name and E--All switches with same VTP version are right. The D choice referencing VTP server is the trick and wrong.

upvoted 1 times

Sten111 2 years, 2 months ago

Do you have a source to back that up because the Cisco documentation diagrees, it says that the VTP versions don't have to be the same and yes a VTP server is on a switch but it's called a VTP server by Cisco themselves.

upvoted 1 times

SScott 2 years, 1 month ago

After reviewing the documentation further, I feel the best two choices are D and E. There are three correct answers but A is third down the list since A is not a must.

upvoted 2 times

wakaish Most Recent 1 week, 3 days ago

A. All switches must be configured with the same VTP domain name: For VTP to work correctly, all switches in the same VTP domain must have the same VTP domain name. This is necessary to ensure that they exchange and synchronize VLAN information.

E. All switches must use the same VTP version: To avoid compatibility issues, all switches in the same VTP domain should use the same VTP version (VTPv1, VTPv2, or VTPv3). Using different VTP versions can lead to inconsistencies in VLAN configuration.

upvoted 1 times

Nikisan 1 month, 2 weeks ago

According to the Cisco documentation about "Configure VLAN Trunk Protocol (VTP)" it says
"VTP Configuration Guidelines
This section provides some guidelines for the configuration of VTP in the network.
All switches have the same the VTP domain name, unless the network design insists for different VTP domains.
Note: Trunk negotiation does not work across VTP domains. Refer to the Data Traffic Blocked between VTP Domains section of Troubleshooting VLAN Trunk Protocol (VTP) for more information.
All switches in a VTP domain must run the same VTP version.
All switches in a VTP domain has the same VTP password, if there is any.

All VTP Server switch(es) must have the same configuration revision number and it must also be the highest in the domain.
When you move a VTP mode of a switch from Transparent to Server, VLANs configured on the VTP Transparent switch must exist on the Server switch." this.

upvoted 2 times

dropspablo 1 month, 3 weeks ago

Selected Answer: AD

All switches in a VTP domain must have the same domain name, but they do not need to run the same VTP version.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvtp.html#:~:text=All%20switches%20in%20a%20VTP%20domain%20must%20have%20the%20same%20domain%20name%2C%20but%20they%20do%20not%20need%20to%20run%20the%20same%20VTP%20version.

upvoted 1 times

datgoonbro 2 months, 2 weeks ago

To exchange VTP messages, five requirements must be met:

1. a switch has to be configured as either a VTP server or VTP client
2. the VTP domain name has to be the same on both switches
3. if present, the VTP domain password has to be the same
4. VTP versions have to match
5. the link between the switches has to be a trunk link

Source: https://study-ccna.com/vtp-configuration/

upvoted 1 times

LeonardoMeCabrio 3 months ago

A&E
https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html

upvoted 1 times

[Removed] 3 months, 1 week ago

Selected Answer: DE

Answers D & E are correct.
- All switches in a VTP domain must run the same VTP version.
- All VTP Server switch(es) must have the same configuration revision number and it must also be the highest in the domain.
Source : https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html

upvoted 1 times

yuh 4 months, 1 week ago

Answer is D,E
-All switches in a VTP domain must run the same VTP version.
-All VTP Server switch(es) must have the same configuration revision number and it must also be the highest in the domain.
-All switches have the same the VTP domain name, unless the network design insists for different VTP domains.
In other words, different domain names are possible if there is a reason.
See the "Configure" section here
https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html

upvoted 1 times

Hope_12 4 months, 1 week ago

Selected Answer: AE

VTP domain name and version should be the same.
Having different version will cause rejection of vlan creation if one device uses VTP version 1(which does not support Extended VLAN) and the other uses VTP version 2(does
support extended VLAN)

upvoted 1 times

4aynick 4 months, 3 weeks ago

Selected Answer: AD

100000%

upvoted 1 times

dearc 5 months, 2 weeks ago

Selected Answer: AC

Option A, All switches must be configured with the same VTP domain name , is true since VTP operates within a domain, and all switches in the domain must have the same VTP domain name in order to exchange VLAN information.

Option B, All switches must be configured to perform trunk negotiation , is false, as switches can operate with VTP without being configured in trunk mode.

Option C, All switches must be configured with a unique VTP domain name , is also true since VTP domain names must be unique in order to prevent VLAN misconfigurations.

Option D, The VTP server must have the highest revision number in the domain, is false, as the VTP device with the highest configuration revision number becomes the master or server.

Option E, All switches must use the same VTP version, is false, as switches can operate with different VTP versions, although it's better to keep them

the same to avoid any possible compatibility issues.

Therefore, the correct answers are AC
upvoted 1 times

nihawk_86 5 months, 1 week ago
The wording is weird so I thought like you for a while, but I think here "unique" means that each switch get a different domain name, in opposition with option A. So A and D sounds right.
upvoted 1 times

elixirwell 5 months, 2 weeks ago
Selected Answer: AD
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvtp.html#wp1107364
upvoted 1 times

zamkljo 5 months, 3 weeks ago
for D, what happen if there is a VTP transparent with higher revision number in domain?
upvoted 1 times

linuxlife 6 months ago
VTP Configuration Guidelines

This section provides some guidelines for the configuration of VTP in the network.

All switches have the same the VTP domain name, unless the network design insists for different VTP domains.

Note: Trunk negotiation does not work across VTP domains. Refer to the Data Traffic Blocked between VTP Domains section of Troubleshooting VLAN Trunk Protocol (VTP) for more information.

All switches in a VTP domain must run the same VTP version.

All switches in a VTP domain has the same VTP password, if there is any.

All VTP Server switch(es) must have the same configuration revision number and it must also be the highest in the domain.

When you move a VTP mode of a switch from Transparent to Server, VLANs configured on the VTP Transparent switch must exist on the Server switch.
upvoted 1 times

linuxlife 6 months ago
https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html
upvoted 1 times

linuxlife 6 months ago
A, D, E are correct answers...but only two can be chosen...tricky ones
upvoted 1 times

linuxlife 6 months ago
But I will go for A and E, where the merits of correctness is the completeness of statements from the given question vs the Cisco documentations:
All VTP Server switch(es) must have the same configuration revision number and it must also be the highest in the domain.
upvoted 1 times

[Removed] 6 months, 4 weeks ago
AD for me. E is not a CCNA thing, I think.
upvoted 1 times

iMo7ed 7 months ago
Selected Answer: AE
VTP Configuration Guidelines and Restrictions:
"All network devices in a VTP domain must run the same VTP version"

Ref: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/20ewa/configuration/guide/conf/vtp.pdf
upvoted 3 times

ricky1802 7 months, 2 weeks ago
Selected Answer: AD
E definitly is not correct answer. From documentation: All switches in a VTP domain must have the same domain name, but they do not need to run the same VTP version.
upvoted 2 times

Question #217 *Topic 1*

Which type does a port become when it receives the best BPDU on a bridge?

A. The designated port

B. The backup port

C. The alternate port

D. The root port

Correct Answer: *D*

Community vote distribution

D (100%)

nenotronix Highly Voted 2 years, 6 months ago

"D" is correct

https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html#:~:text=The%20port%20that%20receives%20the,ones%20any%20other%20bridge%20sends.

upvoted 7 times

tyuipo Highly Voted 2 years, 4 months ago

" The port that receives the best BPDU on a bridge is the root port "

"D" is correct

upvoted 5 times

kyleptt Most Recent 2 months, 3 weeks ago

It "receives" mean a BPDU came from the RB thus it would be a Root Port.

upvoted 1 times

MoctarS 6 months, 1 week ago

Selected Answer: D

Di is correct answer

upvoted 2 times

cormorant 9 months ago

THE PORT THAT RECEIVES THE BEST BPDU BECOMES THE ROOT PORT. end of story

upvoted 3 times

GreatDane 1 year, 3 months ago

Ref: Understanding Rapid Spanning Tree Protocol (802.1w) – Cisco

"...

Port Roles

Root Port Roles

• The port that receives the best BPDU on a bridge is the root port.
..."

A. The designated port

Wrong answer.

B. The backup port

Wrong answer.

C. The alternate port

Wrong answer.

D. The root port

Correct answer.

upvoted 1 times

ZUMY 1 year, 3 months ago

D is correct

upvoted 1 times

onikafei 1 year, 7 months ago

The "best" is root essentially. Whats better than root?

upvoted 3 times

RichyES 1 year, 7 months ago

Selected Answer: D

D is correct

upvoted 1 times

Question #218 *Topic 1*

Which value can you modify to configure a specific interface as the preferred forwarding interface?

A. The interface number

B. The port priority

C. The VLAN priority

D. The hello time

Correct Answer: *B*

Community vote distribution

B (100%)

Claudiu1 Highly Voted 2 years, 6 months ago

This is an STP-related question

upvoted 6 times

nenotronix Highly Voted 2 years, 6 months ago

"B" is the correct answer

https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/spanning-tree-port-priority.html

upvoted 5 times

johnnd 1 year, 7 months ago

https://web.archive.org/web/20210417154626/http://www.cisco.com:80/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/spanning-tree-port-priority.html

upvoted 1 times

ZUMY Most Recent 1 year, 3 months ago

B is correct

upvoted 1 times

BlankNothing1 1 year, 3 months ago

Port priority is the answer. The following link has information on STP that mentions Spanning Tree Port Priority on page 9. It shows how to configure it on page 15. It has other topics that you'll need to know for the exam and beyond.

upvoted 1 times

ismatdmour 1 year, 6 months ago

Selected Answer: B

B: Port priority
Well, C is tricky. It says "VLAN priority". However, there is no thing called VLAN priority. The correct term is "port priority for certain VLAN/ VLANs.
You can adjust port priority without reference to any VLAN which makes it the priorityi of the port for all VLANa.
Spanning-Tree port-priority value
Else, You can adjust port priority wih reference to VLAN / VLANs which makes it the priority of the port for that specific VLAN/ VLANs
Spanning-Tree vlan value/range port-priority value

upvoted 4 times

kyleptt 2 months, 3 weeks ago

yes, this made this question tricky but spanning tree is based on VLAN so..... I guess the port in that VLAN is key lol

upvoted 1 times

youtri 2 years, 5 months ago

This example shows how to increase the probability that the spanning tree instance on access port interface 2/0 is chosen as the root bridge by changing the port priority to 32:

switch(config-if)# spanning-tree port-priority 32

upvoted 3 times

geraldinee 2 years, 6 months ago

vlan priority adjusts things only for the specified vlan, so the right answer is C. The VLAN priority.

upvoted 1 times

ismatdmour 1 year, 6 months ago

Well, C is tricky. It says "VLAN priority". However, there is no thing called VLAN priority. The correct term is "port priority for certain VLAN/ VLANs.
You can adjust port priority without reference to any VLAN which makes it the priorityi of the port for all VLANa
Else, You can adjust port priority wih reference to VLAN / VLANs which makes it the priority of the port for that specific VLAN/ VLANs

upvoted 1 times

Question #219 *Topic 1*

Which statement about Cisco Discovery Protocol is true?

A. It is a Cisco-proprietary protocol.

B. It runs on the network layer.

C. It can discover information from routers, firewalls, and switches.

D. It runs on the physical layer and the data link layer.

Correct Answer: *A*

Community vote distribution

A (100%)

paolo_brosio Highly Voted 2 years, 4 months ago

This is pure product placement

upvoted 26 times

Smaritz 1 year, 5 months ago

Agreed, although 'proprietary' is a swear word these days LOL

upvoted 2 times

Wes_60 Most Recent 5 months, 2 weeks ago

They put this one on there so no one could be totally wrong.

upvoted 2 times

[Removed] 6 months, 4 weeks ago

No need to look for other options. A is 100% correct, and the question did not ask to choose more than 1 answer. So you can save time.

upvoted 2 times

hasbulla01 10 months, 1 week ago

Selected Answer: A

all is correct less B

upvoted 1 times

ratu68 1 year, 2 months ago

Selected Answer: A

No one better get this wrong ! LOL

upvoted 3 times

ZUMY 1 year, 3 months ago

A is correct!

upvoted 1 times

raresz 1 year, 6 months ago

Selected Answer: A

It can be it's not C(which looks also correct for first view) because as far as i know there is no CDP option on Cisco firewalls. I have Cisco ASA 5505 and there is no CDP and i found information there is no CDP on Cisco firewalls for security reasons. That's why it could exclude option nr C in my opinion.

upvoted 1 times

ismatdmour 1 year, 6 months ago

Selected Answer: A

Other answers are very tricky, but this is most obvious

upvoted 1 times

Sara_Yus 1 year, 7 months ago

NOOOO WAYYYY! I would never have guessed

upvoted 2 times

Amirabbas 2 years, 4 months ago

Why not C and D?
It can collect information from switch and routers and also it is a layer 2 protocol.

upvoted 3 times

Request7108 8 months, 4 weeks ago

Remember to choose the most correct answer. C could be correct if they were all Cisco products or capable of running CDP, although that's often not the case.
D isn't correct because CDP does not operate on the physical layer.

upvoted 2 times

NetAdmin950 2 years, 4 months ago

Not C Because the option doesn't specifically say from Cisco router, switches, etc.
Not D because it does operate on the data-link layer but Not on the physical layer.

upvoted 8 times

ProgSnob 1 year, 10 months ago

It's definitely a good trick question to trip most people up. However, option A is the first thing we learn about CDP, that it's Cisco proprietary.

upvoted 3 times

Question #220 *Topic 1*

What are two reasons a network administrator would use CDP? (Choose two.)

A. to verify the type of cable interconnecting two devices

B. to determine the status of network services on a remote device

C. to obtain VLAN information from directly connected switches

D. to verify Layer 2 connectivity between two devices when Layer 3 fails

E. to obtain the IP address of a connected device in order to telnet to the device

F. to determine the status of the routing protocols between directly connected routers

Correct Answer: *DE*

Community vote distribution

DE (100%)

[Removed] Highly Voted 6 months, 4 weeks ago

Why not CE?

upvoted 8 times

wakaish Most Recent 1 week, 3 days ago

Two reasons a network administrator would use CDP (Cisco Discovery Protocol) are:

C. To obtain VLAN information from directly connected switches: CDP can provide information about the directly connected switches, including their device type, platform, and VLAN information. This can be helpful for understanding the network topology and configuration.

D. To verify Layer 2 connectivity between two devices when Layer 3 fails: CDP can be used to verify the physical and data link layer connectivity between two Cisco devices. When Layer 3 connectivity fails, CDP can help in identifying and diagnosing Layer 2 issues that may be causing the problem.

The other options (A, B, E, F) do not directly relate to the typical use cases of CDP.

upvoted 1 times

Rether16 5 months, 1 week ago

Selected Answer: DE

Never use Telnet! :-)

upvoted 3 times

Targaryen 2 years, 4 months ago

C. to obtain VLAN information from directly connected switches - You can get the Native VLAN.
D. to verify Layer 2 connectivity between two devices when Layer 3 fails - Can get information even without L3.
E. to obtain the IP address of a connected device in order to telnet to the device - You can get the Management Address of a Switch.
I guess D and E are the best options.

upvoted 4 times

SScott 2 years, 3 months ago

Yes the best two of three correct answers.

upvoted 3 times

SScott 2 years, 1 month ago

D is a primary benefit to quickly track down network errors
E would help with D and also viewing logs for native vlan mismatch errors which would precede C (once you have config terminal and log view access for the CDP info, then you can further verify task relating to C)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html
https://www.learncisco.net/courses/icnd-1/network-environment-management/neighbors-on-the-network.html
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_nx_os_cg/sm_4cdp.pdf

CDP logging message for native VLAN mismatch on access and trunk ports
https://www.cisco.com/c/en/us/support/docs/network-management/discovery-protocol-cdp/118736-technote-cdp-00.html
https://networkengineering.stackexchange.com/questions/50175/solving-native-vlan-mismatch-error
https://community.cisco.com/t5/switching/native-vlan-mismatch-detected-by/td-p/3316606
https://community.cisco.com/t5/switching/native-vlan-mismatch-error-on-access-port/td-p/1534103

upvoted 1 times

Giuseppe_001 2 years, 4 months ago

zumy aspettiamo la tua conferma

upvoted 2 times

ZUMY 1 year, 3 months ago

Going with D & E

upvoted 1 times

Question #221 *Topic 1*

What are two benefits of using VTP in a switching environment? (Choose two.)

A. It allows switches to read frame tags.

B. It allows ports to be assigned to VLANs automatically.

C. It maintains VLAN consistency across a switched network.

D. It allows frames from multiple VLANs to use a single interface.

E. It allows VLAN information to be automatically propagated throughout the switching environment.

Correct Answer: *CE*

GreatDane Highly Voted 1 year, 2 months ago

Ref: Understanding VLAN Trunk Protocol (VTP) – Cisco

"...
Introduction

VLAN Trunk Protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere.
..."

A. It allows switches to read frame tags.

Wrong answer.

B. It allows ports to be assigned to VLANs automatically.

Wrong answer.

C. It maintains VLAN consistency across a switched network.

Correct answer.

D. It allows frames from multiple VLANs to use a single interface.

Wrong answer.

E. It allows VLAN information to be automatically propagated throughout the switching environment.

Correct answer.

upvoted 10 times

Sutokuto 9 months ago

Why do you respond in this format? It's completely useless.

upvoted 13 times

siredobu 7 months, 1 week ago

Not useless, he/she is giving good explanation on the topic which is good,
rather your comment is useless.

upvoted 15 times

dicksonpwc Highly Voted 2 years, 1 month ago

VTP protocol has 3 modes Server,CLient & Transperent.There is only 1 server and all other switches in that environment are

Clients.Only server can create,modily and
delete VLAN's so in VTP environment VLAN's are consistent across the network.The changes made on the Server are automatically

propogated to all the clients
through the TRUNK links established between the switches.

upvoted 6 times

ZUMY Most Recent 1 year, 3 months ago

C & E are right.

upvoted 1 times

SScott 2 years, 3 months ago

C and E are right.

upvoted 3 times

Question #222 *Topic 1*

Which three statements are typical characteristics of VLAN arrangements? (Choose three.)

A. A new switch has no VLANs configured.

B. Connectivity between VLANs requires a Layer 3 device.

C. VLANs typically decrease the number of collision domains.

D. Each VLAN uses a separate address space.

E. A switch maintains a separate bridging table for each VLAN.

F. VLANs cannot span multiple switches.

Correct Answer: *BDE*

Community vote distribution

BDE (100%)

dicksonpwc Highly Voted 2 years, 1 month ago

To communicate between two different VLANs we need to use a Layer 3 device like router or Layer 3 switch -> B is correct.

VLANs don't affect the number of collision domains, they are the same -> C is not correct. Typically, VLANs increase the number of broadcast domains.

We must use a different network (or sub-network) for each VLAN. For example we can use 192.168.1.0/24 for VLAN 1, 192.168.2.0/24 for VLAN 2 -> D is correct.

A switch maintains a separate bridging table for each VLAN so that it can send frame to ports on the same VLAN only. For example, if a PC in VLAN 2 sends a frame then the switch look-ups its bridging table and only sends frame out of its ports which belong to VLAN 2 (it also sends this frame on trunk ports) -> E is correct.

upvoted 27 times

VanessaR05 Most Recent 2 months, 3 weeks ago

Selected Answer: BDE

B D & E are correct

upvoted 1 times

ac89l 4 months ago

Why E is Correct?

upvoted 1 times

freeknowledge123 8 months, 1 week ago

why is D correct?

upvoted 2 times

rknows 1 month, 3 weeks ago

This did not make sense to me either. I think it might be because each VLAN interface can be assigned an IP for management. Or because each vlan requires a layer three device to communicate via IP and would of necessity need it's "own" space even though you normally think of a VLAN being at layer 2.

upvoted 1 times

ZUMY 1 year, 3 months ago

B D & E are correct

upvoted 3 times

Tesfa 1 year, 9 months ago

Why is A not correct guys b/c a new switch has no vlan configuration.

upvoted 2 times

ShammaA 4 months ago

I thought the same thing, by default VLAN 1 and 1002-1005 are there so I understood the word "configured" as in newly configured VLANs.. but then I remember this is a CISCO exam

upvoted 1 times

Taku2023 6 months, 2 weeks ago

We have Vlan 1 (Default)and Vlan 1001-1005 FDDI TOKEN RING so A is out

upvoted 3 times

gvofke 1 year, 8 months ago

I think is because there is always the dafault VLAN1
upvoted 9 times

LordScorpius 1 year, 4 months ago
Right on. Actually default vlans, out of the box are '1' and 1002 -1005. None of them can be deleted
upvoted 5 times

Adaya 2 years, 2 months ago
A router is a layer 3 device which can be use to connect vlans for intervlan routing
upvoted 2 times

dave1992 1 year, 11 months ago
so is a layer 3 switch
upvoted 1 times

ScorpionNet 1 year, 4 months ago
Yes with ip routing or a router with subinterfaces configured
upvoted 1 times

bunblake 2 years, 2 months ago
Why is B correct?
upvoted 2 times

[Removed] 3 months, 1 week ago
Because you need either a router or a layer 3 switch for connectivity between VLANs
upvoted 1 times

CiscoTerminator 2 years, 1 month ago
SInce each vlan represents a subnet/ network, to route between subnets or networks you need a L3 device such as a router or a L3 switch.
upvoted 4 times

Sten111 2 years, 2 months ago
To send data from one VLAN to another you need a router or layer 3 switch. VLANs are logically seperated at layer 2.
upvoted 1 times

Question #223 *Topic 1*

On a corporate network, hosts on the same VLAN can communicate with each other, but they are unable to communicate with hosts on different VLANs. What is needed to allow communication between the VLANs?

A. a router with subinterfaces configured on the physical interface that is connected to the switch

B. a router with an IP address on the physical interface connected to the switch

C. a switch with an access link that is configured between the switches

D. a switch with a trunk link that is configured between the switches

Correct Answer: *A*

Different VLANs can't communicate with each other, they can communicate with the help of Layer3 router. Hence, it is needed to connect a router to a switch, then make the sub-interface on the router to connect to the switch, establishing Trunking links to achieve communications of devices which belong to different VLANs.

Community vote distribution

A (100%)

ZUMY Highly Voted 1 year, 3 months ago

A is correct
Router on a stick configuration

upvoted 6 times

[Removed] Most Recent 3 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

ScorpionNet 1 year, 4 months ago

A is correct because that is how Router on a Stick in implemented

upvoted 3 times

Shamwedge 1 year, 10 months ago

A and B are correct however A - Router on a stick is the method. If the answer was B, you would have to have a switch port on the the router for each VLAN. Answer A - router on a stick creates sub interfaces for each VLAN eliminating the need for a switch port for each VLAN

upvoted 3 times

shaz938 2 years ago

A is correct. In other words, have a Router On A Stick (ROAS).

Another option could be to have a Layer 3 Switch with SVIs (Switched Virtual Interfaces) and the appropriate IP addressing.

upvoted 2 times

SScott 2 years, 1 month ago

Yes A is the right answer.

https://www.practicalnetworking.net/stand-alone/routing-between-vlans/#:~:text=There%20are%20three%20options%20available%20in%20order%20to%20enable%20routing%20between%20the%20VLANs

https://www.ciscopress.com/articles/article.asp?p=2990405&seqNum=2#:~:text=The%20encapsulation%20command%2C%20and%20not%20the%20subinterface%20number%2C%20defines%20the%20VLAN%20ID%20associated%20with%20the%20subinterface

https://www.firewall.cx/networking-topics/vlan-networks/218-vlan-access-trunk-links.html#:~:text=these%20two%20VLANs%20do%20not%20exchange%20any%20traffic%20between%20each%20other%2C%20unless%20we%20are%20using%20a%20layer%203%20switch%20(or%20router)%20and%20we%20have%20explicitly%20configured%20the%20switch%20to%20route%20traffic%20between%20the%20two%20VLANs

upvoted 2 times

JammyPashmal00 2 years, 2 months ago

Yes oooMooo, but "subinterfaces" are not required. Like you said, essentially a connection to each VLAN, and IP for each connection.

upvoted 2 times

AWSFastLearner 2 years ago

Yes, like you said. I thought the answer is B...

upvoted 2 times

oooMooo 2 years, 4 months ago

A is correct.

"For inter-VLAN communication, a layer 3 device (usually a router) is needed. This layer 3 device needs to have an IP address in each subnet (VLAN) and have a connected route to each of those subnets. The hosts in each subnet can use the router's IP addresses as their default gateway."

upvoted 3 times

Question #224 *Topic 1*

Which statement about LLDP is true?

A. It is a Cisco proprietary protocol.

B. It is configured in global configuration mode.

C. The LLDP update frequency is a fixed value.

D. It runs over the transport layer.

Correct Answer: *B*

Community vote distribution

B (100%)

SScott Highly Voted 2 years, 1 month ago

B is correct, LLDP is for support with non-Cisco devices, runs on the data link layer, and lldp timer has a configurable range from 5 to 65534 sec, commands configured only from conf t

upvoted 9 times

ian77ex Highly Voted 1 year, 6 months ago

B is not correct because some LLDP parameters are configured at interface levels (transmit and receive) So it's not only configured at global configuration mode. Maybe the lack of the word "only" makes the answer correct.
C is not correct because the update timer can be modified, but anyone could understand the word "fixed" like stating that the updates are sent steadily every a certain amount of 'fixed' time.

I hate when they are not trying to measure your knowledge. Instead they're trying to trick you by using unclear questions!

upvoted 9 times

Liuka_92 1 year, 4 months ago

I totally agree.

upvoted 2 times

Stallion Most Recent 1 month, 3 weeks ago

The correct answer to the question is C. The LLDP update frequency is a fixed value. LLDP frames are sent periodically and contain information about the local device. The LLDP update frequency is a fixed value, which means that the amount of time between updates is consistent and determined by the device configuration. By default, the update frequency is 30 seconds.

Answer B is incorrect because LLDP is configured on a per-interface basis, not in global configuration mode.

upvoted 1 times

dearc 5 months, 2 weeks ago

Selected Answer: B

The answer to the question "Which statement about LLDP is true?" is: B. It is configured in global configuration mode.

This answer is supported by search results [1], [2], [3], [4], [5], [6], [7], [8], and [9], which all state that LLDP is configured in global configuration mode . The other statements listed as choices are incorrect. LLDP is not a Cisco proprietary protocol (A) - it is a vendor-neutral protocol. The LLDP update frequency is not necessarily fixed (C) - it can be configured. LLDP runs over the data link layer, not the transport layer (D)

upvoted 1 times

ZUMY 1 year, 3 months ago

B is correct

upvoted 3 times

Jbcrggddfhh 1 year, 4 months ago

B is correct, but C should have been phrased "The LLDP update frequency value can't be modified."

upvoted 1 times

JammyPashmal00 2 years, 2 months ago

Actually, two answers are correct: LLDP has a fixed timer/frequency (30 sec. by default), and it is configured at the Global command level

upvoted 1 times

DonnerKomet 2 years ago

No because, C afirms that the frecuency value is a fixed value, but is not true. It can be modified

upvoted 9 times

Question #225 *Topic 1*

What is a function of Wireless LAN Controller?

A. register with a single access point that controls traffic between wired and wireless endpoints

B. use SSIDs to distinguish between wireless clients

C. send LWAPP packets to access points

D. monitor activity on wireless and wired LANs

Correct Answer: *C*
Lightweight APs (LAPs) is devices require no initial configuration. LAPs use the Lightweight Access Point Protocol (LWAPP) to communicate with a WLAN controller (WLC), as shown in the below figure. Controller-based APs are useful in situations where many APs are required in the network. As more APs are added, each AP is automatically configured and managed by the WLC.

Community vote distribution

C (100%)

bestboy120 Highly Voted 2 years, 8 months ago

B is wrong
C. send LWAPP packets to access points

upvoted 22 times

Retxed Highly Voted 2 years, 8 months ago

Correct Answer: C
Explanation/Reference: Lightweight APs (LAPs) is devices require no initial configuration. LAPs use the Lightweight Access Point Protocol (LWAPP) to communicate with a WLAN controller (WLC), as shown in the below figure. Controller-based APs are useful in situations where many APs are required in the network. As more APs are added, each AP is automatically configured and managed by the WLC.

upvoted 8 times

[Removed] Most Recent 3 months, 1 week ago

Selected Answer: C
C is correct

upvoted 1 times

jobba111 1 year, 2 months ago

Selected Answer: C
C is correct

upvoted 1 times

GreatDane 1 year, 2 months ago

Ref: Defining LWAPP (Cisco Wireless LAN Controllers) - what-when-how.com

"...
LWAPP is a way for an AP to communicate directly with a management entity—the WLC.
..."

A. register with a single access point that controls traffic between wired and wireless endpoints

A WLC is used to configure and manage one or more APs. It doesn't control traffic between the wireless and wired part of a network, it controls APs.
Wrong answer.

B. use SSIDs to distinguish between wireless clients

On the contrary, SSIDs are used by wireless clients to distinguish among different wireless LANs and decide which one to associate with.
Wrong answer.

C. send LWAPP packets to access points

Correct answer.

D. monitor activity on wireless and wired LANs

A WLC doesn't monitor data traffic or device behaviour. A WLC is used to MANAGE one or more APs.
Wrong answer.

upvoted 1 times

ZUMY 1 year, 3 months ago

C is correct

upvoted 1 times

Jbcrggddfhh 1 year, 4 months ago

Selected Answer: C

C is correct -- WLCs communicate and manage APs by sending them LWAPP packets.

"Wireless LAN Controllers (WLC) govern a collection of Lightweight Access Points (APs)."
"Light Weight Access Point Protocol (LWAPP) defines the network protocol between the APs and WLC."

Reference: https://aristanetworks.force.com/AristaCommunity/s/article/how-to-integrate-cisco-wireless-lan-controller-with-cloudvision-wifi

upvoted 3 times

Jbcrggddfhh 1 year, 4 months ago

A sounds like it is describing a device that is a client of an AP. Definitely not a WLC.

B is wrong since SSIDs distinguish between different WLANs, not individual clients.

"SSID is short for service set identifier. In layman's terms, an SSID is the name for a Wi-Fi network."

Reference: https://www.webopedia.com/definitions/ssid/

D is incorrect because a WLC does not monitor traffic on wired LANs; it only monitors wireless activity.

"A wireless LAN controller (WLC) is a network component that manages wireless network access points and allows wireless devices to connect to the network."
"It offers central control over network elements, increases network visibility, and greatly simplifies individual component monitoring."

Reference: https://www.manageengine.com/network-monitoring/wlc-monitoring.html

upvoted 1 times

ScorpionNet 1 year, 4 months ago

I agree with everyone C is correct because LWAPP is used by WLAN Controllers to send packets to LAPs. Like how CAPWAP functions but except it's sent to WLCs

upvoted 1 times

LordScorpius 1 year, 4 months ago

Selected Answer: C

Going with C LWAPP is a protocol that allows WLC to do it's thing with LAP enabled devices.

upvoted 1 times

raresz 1 year, 6 months ago

Selected Answer: C

weird qquestion. isn't it also Standalone AP function to use SSID to distinguish between wireless clients? So if Standalone AP can do it why it would be meant about WLC?

upvoted 1 times

ismatdmour 1 year, 6 months ago

Selected Answer: C

C of course
B is meant to trick you. WLC does not use SSID to distinguish between wireless clients, it uses SSID to distinguish between wireless lans

upvoted 1 times

Nagib 1 year, 6 months ago

C. send LWAPP packets to access points

upvoted 1 times

bmatthee01 1 year, 6 months ago

In this case C is correct - LWAPP is one of the functions of a WLC, it is a means to communicate with the AP's

In this case B is not correct, because WLC does not use SSID to distinguish between wireless clients, it uses SSID to distinguish between wireless lans

just have to read the questions carefully and understand the concepts

upvoted 3 times

ian77ex 1 year, 6 months ago

Selected Answer: C

Who said B?

upvoted 1 times

Ravan 1 year, 7 months ago

Selected Answer: C

Correct Answer: C
Explanation/Reference: Lightweight APs (LAPs) is devices require no initial configuration. LAPs use the Lightweight Access Point Protocol (LWAPP) to communicate with a WLAN controller (WLC). Controller-based APs are useful in situations where many APs are required in the network. As more APs are added, each AP is automatically configured and managed by the WLC.

upvoted 1 times

AndersonMr 1 year, 8 months ago

Selected Answer: C

Explanation/Reference: Lightweight APs (LAPs) is devices require no initial configuration. LAPs use the Lightweight Access Point Protocol (LWAPP) to communicate with a WLAN

upvoted 1 times

awashenko 1 year, 8 months ago

Selected Answer: C

After digging in I think C is correct

upvoted 1 times

Question #226 *Topic 1*

Which technology is used to improve web traffic performance by proxy caching?

A. WSA

B. Firepower

C. ASA

D. FireSIGHT

Correct Answer: *A*

Community vote distribution

A (100%)

mrsiafu Highly Voted 2 years, 4 months ago

Yeah.. but what cert guide would have gave this type of info for a question like this!

upvoted 28 times

ian77ex Highly Voted 1 year, 6 months ago

This is out of scope.

upvoted 18 times

Da_Costa Most Recent 1 month, 4 weeks ago

Selected Answer: A

Web security application

upvoted 1 times

soRwatches 6 months, 1 week ago

dafuq is this sh!t?

upvoted 11 times

ZUMY 1 year, 3 months ago

A is correct

upvoted 3 times

Cyberops 1 year, 3 months ago

Selected Answer: A

A is the correct answer

upvoted 1 times

ScorpionNet 1 year, 4 months ago

A is correct because WSAs are used to detect any sites that seems fishy

upvoted 1 times

lordnano 2 years, 6 months ago

Seems to be correct. Reference:
https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/guide-c07-742373.html
"
4.1 Web proxy
Caching should be enabled in the web proxy configuration in order to save bandwidth and boost performance. This is becoming less important as the percentage of HTTPS traffic increases because the WSA does not by default cache HTTPS transactions. If the proxy is deployed to serve only explicit clients, forward mode should be specified in order to reject any traffic that isn't specifically destined for the proxy service. This reduces attack surface in the appliance and follows a good security principle: If you don't need it, turn it off.
"

upvoted 12 times

SScott 2 years, 3 months ago

https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118043-qanda-wsa-00.html

upvoted 2 times

Question #227 *Topic 1*

What criteria is used first during the root port selection process?

A. local port ID

B. lowest path cost to the toot bridge

C. lowest neighbor's bridge ID

D. lowest neighbor's port ID

Correct Answer: *B*

Community vote distribution

B (100%)

DavidFitzgerald Highly Voted 2 years, 4 months ago

lol toot bridge

upvoted 111 times

IxlJustinIxl Highly Voted 2 years, 3 months ago

Root Port selection is based on the port having lowest cost to the Root Bridge (CAT1). For PVST (Per VLAN Spanning Tree) path cost will depend on bandwidth of links and cost value is as shown below for most commonly used links.

https://mrncciew.com/2013/07/07/stp-root-port-selection/

upvoted 9 times

TaronStone Most Recent 1 month, 1 week ago

Gimme those toot privileges

upvoted 1 times

[Removed] 3 months, 1 week ago

The famous toot bridge ;-)

upvoted 1 times

tahasidd 8 months ago

toot bridge:p

upvoted 1 times

eoj8 10 months ago

toooooot

upvoted 3 times

ZUMY 1 year, 3 months ago

Selected Answer: B

B - Root bridge

upvoted 3 times

ScorpionNet 1 year, 4 months ago

Answer is B but what does toot mean a train? It supposed to be spelt root

upvoted 3 times

LordScorpius 1 year, 4 months ago

Selected Answer: B

Here comes the too too training going over the toot bridge to the toot port

upvoted 6 times

Rothus 1 year, 4 months ago

Aprendan a escribir viejos pndjos

upvoted 3 times

dave1992 1 year, 11 months ago

toot lol

upvoted 5 times

CISCO2022 2 years, 3 months ago

C is correct. question asked for the first step in electing root bridge.
STP Root Port Selection
Lowest bridge ID (Priority:MAC Address) switch becomes the Root-Bridge.
Each non-root bridge should have ONE root port (RP) which is the port having lowest path-cost to Root Bridge.

All ports in Root Bridge become Designated Ports (DP)
Each segment should have one Designated Port (DP)

upvoted 5 times

Dataset 2 years, 3 months ago

hi! the question asked "root port" , so B is correct, the root port are ports with the lowes path cost to the root bridge.
Regards!

upvoted 7 times

Ray12345 2 years, 4 months ago

STP root port election
Lowest root cost
Lowest neighbor bridge ID
Lowest neighbor port id

upvoted 5 times

kunyo99 2 years, 4 months ago

Yes Answer is correct

upvoted 3 times

Dataset 2 years, 4 months ago

B is correct

upvoted 2 times

Chun9 2 years, 7 months ago

Is it root bridge? the B answer?

upvoted 4 times

SasithCCNA 2 years, 7 months ago

yes the answer is B

upvoted 2 times

SasithCCNA 2 years, 7 months ago

its should be root bridge not toot bridge lol

upvoted 7 times

Question #228 *Topic 1*

Which statement about VLAN configuration is true?

A. The switch must be in VTP server or transparent mode before you can configure a VLAN

B. The switch must be in config-vlan mode before you configure an extended VLAN

C. Dynamic inter-VLAN routing is supported on VLAN2 through VLAN 4064

D. A switch in VTP transparent mode save the VLAN databases to the running configuration only

Correct Answer: *A*

Community vote distribution

A (75%) B (25%)

Nhan Highly Voted 2 years, 6 months ago

Correct answer is a, you can only create, add, delete edit vlan in server and transparent mode, you won't be able to create, delete vlan in client mode.

upvoted 34 times

aek994 Highly Voted 2 years, 6 months ago

Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vla
Switch(config)#vlan 20
VTP VLAN configuration not allowed when device is in CLIENT mode.

Answer is A

upvoted 24 times

aek994 2 years, 6 months ago

Also B is uncorrect. Because when vtp mode is transparent, you can create extended vlan.

Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)#vlan 1010
Switch(config-vlan)#

upvoted 3 times

SScott 2 years, 3 months ago

Right, statement A precedes B. A comes first before you can even configure an extended VLAN. A is correct.

upvoted 3 times

wakaish Most Recent 1 week, 3 days ago

C. Dynamic inter-VLAN routing is supported on VLAN2 through VLAN 4064.

This statement indicates that dynamic inter-VLAN routing (often done with a router or Layer 3 switch) typically supports VLANs numbered from 2 to 4064. VLANs outside of this range may not be supported by all devices. This range of VLAN IDs is common in networking and is consistent with industry standards.

upvoted 1 times

zFlyingLotusz 2 months ago

Uhhhhh you can configure VLANS without VTP at all, so how is A correct?

upvoted 4 times

Vikramaditya_J 4 months, 1 week ago

Selected Answer: A

Option A is a correct statement because the question doesn't ask anything about VLAN advertisement or VLAN information forwarding, so we shouldn't think deeper about VTP modes.

upvoted 1 times

linuxlife 6 months ago

Switch#show vtp status
VTP Version capable : 1 to 2
VTP version running : 1
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 00D0.FFB3.D900
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :

VTP Operating Mode : Server
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
Configuration Revision : 0
MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
0xF0 0x58 0x10 0x6C 0x9C 0x0F 0xA0 0xF7
Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 4000
VLAN_CREATE_FAIL: Failed to create VLANs 4000 : extended VLAN(s) not allowed in current VTP mode
Switch(config)#

upvoted 1 times

linuxlife 6 months ago

changing the VTP Server to Transparent Mode will allow the configurations of Extended VLANs:

Switch(config)#vtp mode transparent
Device mode already VTP TRANSPARENT.
Switch(config)#vlan 4000

Switch#show run
Building configuration...

Current configuration : 1171 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
vtp mode transparent
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan 4000

upvoted 1 times

humanbot 10 months, 1 week ago

Selected Answer: A

A is the right answer

upvoted 1 times

sasquatchshrimp 1 year, 1 month ago

Selected Answer: B

I am going B. Research how to configure an extended vlan, and you end up in config-vlan.

upvoted 1 times

rijstraket 7 months, 3 weeks ago

Correct, you end up in config-vlan, but you didn't start the configuration of the extended vlan there. That happened with the rule where you configured an extended vlan (e.g. 'vlan 1234'). Therefor answer B is incorrect.

upvoted 2 times

ZUMY 1 year, 3 months ago

A is okay

upvoted 1 times

DARKK 1 year, 3 months ago

Selected Answer: A

A is correct

upvoted 1 times

Faram 2 years, 6 months ago

A
https://study-ccna.com/vtp-modes/

upvoted 3 times

admin1982 2 years, 7 months ago

OK, so I take it back after doing some research. The correct answer could be A. This is a bit of a tricky one though.

https://community.cisco.com/t5/networking-documents/how-to-configure-extended-range-vlans-in-catalyst-6500-switch/ta-p/3122316

upvoted 2 times

admin1982 2 years, 7 months ago

wannaknow is correct, the answer is B. I did the config as well.

upvoted 1 times

wannaknow 2 years, 7 months ago

Correct answer is B, here is the explanation
Switch#
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 222
Switch(config-vlan)#name test222
Switch(config-vlan)#exit
Switch(config)#vlan 1200
VLAN_CREATE_FAIL: Failed to create VLANs 1200 : extended VLAN(s) not allowed in current VTP mode
Switch(config)#
Switch(config)#
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.
Switch(vlan)#vlan 1200
VLAN 1200 modified:
Switch(vlan)#
Switch(vlan)#
Switch#

upvoted 2 times

helkas 2 years, 7 months ago

Switch to transparent mode and try from global config again.
1

configure terminal

Enter global configuration mode.

Step 2

vtp mode transparent

Configure the switch for VTP transparent mode, disabling VTP.

Note This step is not required for VTP version 3.

Step 3

vlan vlan-id

Enter an extended-range VLAN ID and enter VLAN configuration mode. The range is 1006 to 4094.

upvoted 1 times

mariodesa 1 year, 8 months ago

You configured the extended vlan in Switch(vlan)# mode, not in Switch(config-vlan)# mode as indicated in option B. The correct answer is A. Server and transparent VTP modes can create, modify and delete vlans.

upvoted 1 times

mariodesa 1 year, 8 months ago

But VTP mode Clients cannot create, modify or delete vlans.

upvoted 1 times

SasithCCNA 2 years, 7 months ago

so what is the correct answer then?

upvoted 1 times

Techno_Head 2 years, 8 months ago

Answer D.

Explanation:

Server mode is the default VTP mode for all Catalyst switches. At least one server is required in a VTP domain to propagate VLAN information

within the VTP domain. We can create, add, or delete VLANs of a VTP domain in a Switch which is in VTP Server mode and change VLAN information in a VTP Server. The changes made in a switch in server mode are advertised to the entire VTP domain.

The VTP Transparent mode is something between a VTP Server and a VTP Client but does not participate in the VTP Domain. In Transparent mode, you are able to create, modify and delete VLANs on the local switch, without affecting any other switches regardless of the mode they might be in.

upvoted 1 times

Zerotime0 2 years, 7 months ago

You copied the explanation from another website.where answer D there is answer A here. So to be clear explanation is correct for answer A.

upvoted 5 times

Techno_Head 2 years, 7 months ago

Can I disagree with myself. The answer is B to configure vlans you need to be at this prompt. Switch(config-vlan)# Its a bad question but you don't have to be in any vtp mode to configure. Most if not all switches come with VTP disabled. I wish you could edit and delete your posts and wish you got notification when someone responds. Maybe i haven't set that up right will have a look.

upvoted 3 times

XBfoundX 2 years, 8 months ago

The explainations about VTP is right but there is a problem here, the answer said only in the running configuration but in reality vlans are not only on the running-config they are stored in te vlan.dat file into the flash. Even if it is trasparent the vlan are still also saved into the vlan.dat file into the flash memory.

Best regards

upvoted 3 times

Question #229 *Topic 1*

Refer to the exhibit. What two conclusions should be made about this configuration? (Choose two.)

```
SW1#show spanning-tree vlan 30

VLAN0030
Spanning tree enabled protocol rstp
Root ID     Priority        32798
            Address         0025.63e9.c800
            Cost            19
            Port            1 (FastEthernet 2/1)
            Hello Time      2 sec
            Max Age         30 sec
            Forward Delay   20 sec

[Output suppressed]
```

A. The root port is FastEthernet 2/1

B. The designated port is FastEthernet 2/1

C. The spanning-tree mode is PVST+

D. This is a root bridge

E. The spanning-tree mode is Rapid PVST+

Correct Answer: *AE*

Randman Highly Voted 1 year, 9 months ago

And how do we know Fe2/1 is the root port and not the designated port from this show of output?
Thank you

upvoted 10 times

ian77ex 1 year, 6 months ago

The cost to reach the root bridge is 19, meaning that the root bridge is directly connected through a 100Mbps link. That's how you know.

upvoted 12 times

DC095 6 months, 3 weeks ago

This is not quite correct. In RSTP the default cost of a 100Mbs Link is 200,000. This means that the cost of 19 would have to have been manually configured on the link.

upvoted 3 times

oatmealturkey 6 months, 3 weeks ago

Not on a Cisco switch. Cisco still uses the default settings as defined in 802.1D-1998, so you would have to manually configure the updated costs that you referred to. The cost of 19 for a 100Mbps port is indeed the default setting on a Cisco switch. I highly recommend getting the Official Certification Guide Vol. 1&2, I believe it is necessary to pass the exam.

upvoted 5 times

southcrossboss 1 year, 6 months ago

true that!

upvoted 2 times

netlol 1 year, 7 months ago

I have the same question

upvoted 1 times

Abupaa 1 year, 7 months ago

It will say "This bridge is the root" in the output

upvoted 5 times

dicksonpwc Highly Voted 2 years, 1 month ago

1. Spanning tree enabled protocol rstp(mode is Rapid PVST+)
2. Port 1(FastEthernet 2/1) = root port is FastEthernet 2/1

upvoted 6 times

icecool2019 Most Recent 11 months, 2 weeks ago

Rapid PVST+ definition: This is a Cisco enhancement of RSTP that uses PVST+ and provides a separate instance of 802.1w per VLAN. Each separate instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard. (Source: Netacad). Since there is no selection for RSTP then Rapid PVST + is the closest answer.

upvoted 2 times

ScorpionNet 1 year, 4 months ago

A and E is correct

upvoted 1 times

ZUMY 2 years, 4 months ago

A & E are Correct

upvoted 2 times

goldengodiva 2 years, 5 months ago

Why does the answer say it's using rapid pvst+ when the exhibit shows that it's using rstp?

upvoted 4 times

netlol 1 year, 7 months ago

it is pvst (per vlan spanning tree) because the show command indicates that there is a STP per vlan (in this case, showing the STP of VLAN 30). And then it's rapid because it says that "Spanning tree enabled protocol rstp", So, in conclusion it's rapid pvst (the "+" is something about Cisco but you don't have to worry about it). Hope this explanation was clear to you!

upvoted 5 times

youtri 2 years, 5 months ago

rstp: r means Rapid

upvoted 3 times

jehangt3 2 years, 3 months ago

@goldengodiva is right. Rapid STP or RSTP is IEEE standard & Rapid PVST+ is cisco proprietary so the answer does not match the question. There's a typo here

upvoted 4 times

Roberts132 2 years, 2 months ago

exact!

upvoted 2 times

echarles10 2 years, 8 months ago

AE is correct

upvoted 4 times

Question #230 *Topic 1*

A network engineer must create a diagram of a multivendor network. Which command must be configured on the Cisco devices so that the topology of the network is allowed to be mapped?

A. Device(config)#lldp run

B. Device(config)#cdp run

C. Device(config-if)#cdp enable

D. Device(config)#flow-sampler-map topology

Correct Answer: *A*

Community vote distribution

A (100%)

Jay1324 Highly Voted 1 year, 8 months ago

Key is multi-vendor--lldp. cdp is cisco only

upvoted 13 times

StingVN Most Recent 4 months, 2 weeks ago

Selected Answer: A

A. As CDP only for cisco devices. but since multi vendor then should be LLDP.

upvoted 1 times

Mohammed028 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

jose01210 1 year, 2 months ago

aprendiendo ingles a la fuerza jejeje pero vale la pena

upvoted 2 times

ZUMY 1 year, 3 months ago

A is correct

upvoted 1 times

ScorpionNet 1 year, 4 months ago

Yep its definitely the Multivendor

upvoted 1 times

dipanjana1990 1 year, 5 months ago

cdp is cisco-proprietary whereas lldp is open standard. as well as cdp is enabled by default in all cisco devices. thus A would be the correct answer.

upvoted 2 times

Smaritz 1 year, 6 months ago

CDP = Cisco only

upvoted 1 times

Question #231 *Topic 1*

How do AAA operations compare regarding user identification, user services, and access control?

A. Authorization provides access control, and authentication tracks user services

B. Authentication identifies users, and accounting tracks user services

C. Accounting tracks user services, and authentication provides access control

D. Authorization identifies users, and authentication provides access control

Correct Answer: *B*

Community vote distribution

B (100%)

Ali526 Highly Voted 2 years, 8 months ago

Authentication, Identify users
Authorization, access control
Accounting, track user services

upvoted 35 times

ZUMY Highly Voted 2 years, 4 months ago

B is correct
Authentication, Identify users
Authorization, access control
Accounting, track user services

upvoted 8 times

[Removed] Most Recent 3 months, 1 week ago

Selected Answer: B

B is correct.
Authentication identifies users
Accounting tracks user services

upvoted 1 times

ScorpionNet 1 year, 4 months ago

B is correct
Authentication = Who are you?
Authorization = Here's some things you're only allowed to do
Accounting = Hmm let's see what this person is doing

upvoted 7 times

onikafei 1 year, 7 months ago

Best way i found it is to cut out the different definitions of authentication the answers provide.

Authentication is verifying your identity, its identifying the users.
Access control is definitly not it lol, neither is tracking user services. Your not touching those without authentication lol

upvoted 1 times

ZayaB 2 years, 7 months ago

C & D are also true according to the ALI526, therefore, why answer is B?

upvoted 3 times

Zerotime0 2 years, 7 months ago

Reread.

upvoted 3 times

Question #232 *Topic 1*

What is the difference between RADIUS and TACACS+?

A. RADIUS logs all commands that are entered by the administrator, but TACACS+ logs only start, stop, and interim commands.

B. TACACS+ separates authentication and authorization, and RADIUS merges them.

C. TACACS+ encrypts only password information, and RADIUS encrypts the entire payload.

D. RADIUS is most appropriate for dial authentication, but TACACS+ can be used for multiple types of authentication.

Correct Answer: *B*

Community vote distribution

B (92%) 8%

Shamwedge Highly Voted 1 year, 6 months ago

Selected Answer: B

TACAS+ A-Authentictaion | A-Authorization (Both A's are sperated by a C) = TACAS+ seperates Authentication and Authorization.

upvoted 31 times

xbololi 2 months, 3 weeks ago

Thank you <3

upvoted 1 times

MarioE 6 months, 2 weeks ago

Haha Nice! Good way to remember this ;-)

upvoted 2 times

dipanjana1990 1 year, 5 months ago

hehe "separated by C" now m never gonna forget this.

upvoted 8 times

examcol Highly Voted 3 years, 1 month ago

B is correct answer.
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

upvoted 8 times

Ciscoman021 Most Recent 5 months, 3 weeks ago

Selected Answer: B

the correct answer is option B: TACACS+ separates authentication and authorization, while RADIUS combines them. Option A is incorrect because neither RADIUS nor TACACS+ is designed to log commands entered by administrators. Option C is incorrect because both RADIUS and TACACS+ can encrypt sensitive information. Option D is incorrect because both RADIUS and TACACS+ can be used for various types of authentication, including dial-up, wireless, and VPN.

upvoted 2 times

guisam 9 months, 2 weeks ago

https://www.geeksforgeeks.org/difference-between-tacacs-and-radius/

upvoted 1 times

miki1001 1 year, 1 month ago

Selected Answer: C

TACACS+ encrypts only password information, and RADIUS encrypts the entire payload.

upvoted 3 times

mzu_sk8 10 months, 2 weeks ago

31 days before the exam, page 179, RADIUS encrypts only the password , TACACS the entire packet

upvoted 3 times

Customexit 10 months, 3 weeks ago

TACACS is more secure. Encrypts the whole packet including username, password, and attributes.
RADIUS only encrypts the password.

upvoted 3 times

miki1001 1 year, 1 month ago

TACACS (Terminal Access Controller Access Control System) is a security protocol that provides centralized validation of users who are attempting to gain access to a router or NAS. TACACS+ provides separate authentication, authorization and accounting services
RADIUS combines authenticaiton and authorization into a single function; TACACS+ allows these services to be split between different servers.
TACACS+ encrypts only password information, and RADIUS encrypts the entire payload.

upvoted 1 times

RougePotatoe 10 months, 3 weeks ago

You got tacacs and radius encryption backwards

upvoted 1 times

schleef 1 year, 10 months ago

"RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.

TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting."

Source: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

upvoted 4 times

Benjamin8189 1 year, 11 months ago

-TACACS+ provides for separate and modular authentication, authorization, and accounting facilities
-In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information

upvoted 1 times

ZUMY 2 years, 4 months ago

B is correct
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

upvoted 3 times

Question #233 *Topic 1*

What is a difference between local AP mode and FlexConnect AP mode?

A. Local AP mode creates two CAPWAP tunnels per AP to the WLC

B. Local AP mode causes the AP to behave as if it were an autonomous AP

C. FlexConnect AP mode fails to function if the AP loses connectivity with the WLC

D. FlexConnect AP mode bridges the traffic from the AP to the WLC when local switching is configured

Correct Answer: *A*

Community vote distribution

A (100%)

dave369 Highly Voted 3 years, 3 months ago

This link supports "A" as the answer:

"In local mode, an AP creates two CAPWAP tunnels to the WLC. One is for management, the other is data traffic. This behavior is known as "centrally switched" because the data traffic is switched(bridged) from the ap to the controller where it is then routed by some routing device."

https://community.cisco.com/t5/wireless-and-mobility/what-s-the-difference-between-local-mode-and-flex-connect-mode/td-p/2532657

upvoted 42 times

SScott 2 years, 1 month ago

Good link Dave. A is the best answer.

A is an accurate statement as data traffic is tunneled back to the controller for an SSID with Local AP Mode
B should have referenced FlexConnect AP [Standalone Mode], not local ap mode [Central Switching or Connected Mode]
C is wrong as the purpose of FlexConnect is to provide local connectivity when the connection to controller is lost
D is wrong because "local" switching is referenced and it should be "central" switching

https://www.ciscolive.com/c/dam/r/ciscolive/latam/docs/2016/pdf/BRKEWN-2016.pdf

https://www.kareemccie.com/2017/08/what-is-flexconnect.html

upvoted 1 times

Ebenezer Highly Voted 2 years, 12 months ago

Actually, the right answer is A.
The FlexConnect AP can locally switch traffic between a VLAN and SSID when the CAPWAP tunnel to the WLC is down. If option D had said, "when it is down," it would have been the right answer. But here, they said, "configured."

upvoted 21 times

Raymond9 2 years, 9 months ago

save my day dude

upvoted 4 times

ZUMY Most Recent 1 year, 2 months ago

A is correct!

upvoted 3 times

ScorpionNet 1 year, 4 months ago

A is right because AP creates CAPWAP tunnels to find the WLC

upvoted 2 times

pagamar 1 year, 5 months ago

The answer is A for sure, found in a recent Exam, 100% on Topic 2 (including wireless networks).

upvoted 3 times

BreezyNet 8 months, 4 weeks ago

please share the link on which you found the exam

upvoted 1 times

shehabdawood 1 year, 8 months ago

Selected Answer: A

A is the right answer

upvoted 1 times

shehabdawood 1 year, 8 months ago

D is wrong
A correct
https://www.thenetworkdna.com/2020/10/wireless-infrastructure-analysis-local.html
upvoted 1 times

Anarckii 1 year, 9 months ago

A is the correct answer
upvoted 1 times

Ernesto_CG 1 year, 9 months ago

Selected Answer: A

A es la respuesta correcta
upvoted 2 times

mr_reyes 1 year, 9 months ago

Definitely A!
FlexConnect = Switched Locally
Local Mode = Centally Switched
upvoted 1 times

Hodicek 1 year, 9 months ago

I would say A
upvoted 1 times

PanteLa_26 1 year, 9 months ago

Selected Answer: A

Should be A. FlexConnect is only for when CAPWAP tunnel fails.
upvoted 2 times

raydel92 1 year, 9 months ago

Selected Answer: A

Answer is A.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html
upvoted 1 times

maw619 2 years ago

The question is asking for "the difference" between the two but I believe an access point creates two capwap tunnels when in flex connect mode as well. The only hard difference i see between the two is option "D"
upvoted 4 times

Taofik 2 years, 1 month ago

A is the right answer.
upvoted 2 times

diazed 2 years, 2 months ago

A is the correct one
https://community.cisco.com/t5/wireless/what-s-the-difference-between-local-mode-and-flex-connect-mode/td-p/2532657
upvoted 3 times

MMAXY 2 years, 4 months ago

so we should disregard their answer D ?
upvoted 1 times

Question #234 *Topic 1*

The SW1 interface g0/1 is in the down/down state. What are two reasons for the interface condition? (Choose two.)

A. There is a protocol mismatch

B. There is a duplex mismatch

C. The interface is shut down

D. The interface is error-disabled

E. There is a speed mismatch

Correct Answer: *DE*
The interface is shut down - ADMIN DOWN / DOWN
The interface is error-disabled - DOWN / DOWN
There is a speed mismatch - DOWN / DOWN

Community vote distribution

DE (96%) 4%

Dante_Dan Highly Voted 1 year, 8 months ago

Selected Answer: DE

A.- When there is a protocol mismatch the status is UP/DOWN
B.- When there is a duplex mismatch, the status is UP/UP
C.- When the interface is shut down the status is ADMINISTRATIVELY DOWN/DOWN

The only 2 answers where the status is DOWN/DOWN are answers C & D

upvoted 12 times

YetiPatty 2 months, 3 weeks ago

did you mean D & E? lol

upvoted 1 times

jossyda Highly Voted 1 year, 3 months ago

Selected Answer: DE

A. There is a protocol mismatch up/down
B. There is a duplex mismatch up/up
C. The interface is shut down admin down / down
D. The interface is error-disabled down/down
E. There is a speed mismatch down/down

upvoted 8 times

WowA 1 year, 1 month ago

But a duplex mismatch takes the ports to in down / down !

upvoted 1 times

RougePotatoe 10 months, 3 weeks ago

Yea I've seen a lot of people bring up the claim and a cisco source claiming it will only impact the performance but mismatched protocol will result in status: down Protocol: down in packet tracer.

upvoted 1 times

linuxlife Most Recent 6 months ago

line status/protocol status:

down/down
- No cable connected, bad cable
- neighbor device is powered off
- neighbor device is shutdown
- neighbor device is error disabled

upvoted 1 times

linuxlife 6 months ago

add-on (speed mismatch):

line status/protocol status:

down/down
- No cable connected, bad cable, speed mismatch
- neighbor device is powered off

- neighbor device is shutdown
- neighbor device is error disabled

upvoted 1 times

DB_Cooper 7 months, 3 weeks ago

Selected Answer: CD

down/ down
every else would be up/down

upvoted 1 times

Amonzon 1 year, 1 month ago

correct answers are B &D
A. There is a protocol mismatch up/down
B There is a duplex mismatch down/down
Switch(config-if)#duplex full
Switch(config-if)#
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

C. err-disable down/down

upvoted 3 times

ZUMY 1 year, 2 months ago

D & E correct

upvoted 1 times

timskis2 1 year, 4 months ago

CAN A PROTOCOL MISMATCH BE ONE AS WELL ? HDLC AND PPP ?

upvoted 1 times

ScorpionNet 1 year, 4 months ago

D and E is right because shutdown is administratively down/down when there is a speed or duplex mismatched and when error disabled down/down

upvoted 1 times

DatBroNZ 1 year, 6 months ago

Selected Answer: DE

The Down/Down combination can have two interface status:
- notconnect (no cable, bad cable, neighbor device is shutdown, speed mismatch)
- err-disabled (port security has disabled the interface)

upvoted 3 times

ismatdmour 1 year, 6 months ago

Selected Answer: DE

Correct answers are D and E
The interface will be in a down (line Status) - down (protocol status) state (not connect interface) for cases of: No cable, bad cable, wrong cable pinouts, speed mismatch and neighbouring device is (1) powered off (2)shutdown or (3) err-disabled. The interface will also be in down-down(err-disabled) because of port securirty disabling the interface

upvoted 1 times

AndersonMr 1 year, 8 months ago

Selected Answer: DE

Down/Down can be on account of phy problem: no cable attached, sw on other side shutdown, sw powered off, device speed mis match.

upvoted 3 times

awashenko 1 year, 8 months ago

If an interface is shut down it will show Admin Down. Not just down so C is wrong

upvoted 3 times

MrBadger 1 year, 5 months ago

I thought that then I guess if the other end is shutdown your end would show down/down

upvoted 1 times

awashenko 1 year, 8 months ago

Speed mismatch and error disabled are the correct answers

upvoted 2 times

Question #235 *Topic 1*

How will Link Aggregation be implemented on a Cisco Wireless LAN Controller?

A. The EtherChannel must be configured in ג€mode activeג€.

B. When enabled, the WLC bandwidth drops to 500 Mbps.

C. To pass client traffic, two or more ports must be configured.

D. One functional physical port is needed to pass client traffic.

Correct Answer: *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_010101011.html

oooMooo Highly Voted 2 years, 4 months ago
D is correct

"When you enable LAG, only one functional physical port is needed for the controller to pass client traffic."

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010100001.html#:~:text=When%20you%20enable%20LAG%2C%20only,controller%20to%20pass%20client%20traffic.&text=When%20you%20enable%20LAG%2C%20you,on%20which%20it%20received%20them.

upvoted 7 times

Dutch012 Highly Voted 6 months, 4 weeks ago
يلبعن ام اسئلتك cisco

upvoted 7 times

Drader Most Recent 5 months, 4 weeks ago
This question could be phrased better.

upvoted 3 times

ZUMY 2 years, 4 months ago
D is correct
Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller's distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the user.

LAG simplifies controller configuration because you no longer need to configure primary and secondary ports for each interface. If any of the controller ports fail, traffic is automatically migrated to one of the other ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

upvoted 5 times

Question #236 *Topic 1*

Which two conditions must be met before SSH operates normally on a Cisco IOS switch? (Choose two.)

A. IP routing must be enabled on the switch.

B. A console password must be configured on the switch.

C. Telnet must be disabled on the switch.

D. The switch must be running a k9 (crypto) IOS image.

E. The ip domain-name command must be configured on the switch.

Correct Answer: *DE*
Reference:
https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html

mazintaha Highly Voted 3 years, 2 months ago
"The Cisco IOS image used must be a k9(crypto) image in order to support SSH. "

"!--- Step 2: Configure the DNS domain of the router.

ip domain-name rtp.cisco.com"
upvoted 17 times

ZUMY Highly Voted 2 years, 4 months ago
D & E are Correct!
To use SSH in Cisco Router
01. IOS image must a k9(Crypto) image
02. Configure DNS domain for the router (eg: ip domain-name R1.Contoso.lk)
upvoted 11 times

Anas_Ahmad Most Recent 10 months, 4 weeks ago
The switch Must be running a K9 Crypto IOS image
and
The ip domain-Name command Must be configured on the Switch
upvoted 1 times

Nhan 2 years, 6 months ago
K9 crypto image support SSH version 1.99 which Is version 2
upvoted 4 times

Question #237 *Topic 1*

```
Atlanta#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Atlanta(config)#aaa new-model
Atlanta(config)#aaa authentication login default local
Atlanta(config)#line vty 0 4
Atlanta(config-line)#login authentication default
Atlanta(config-line)#exit
Atlanta(config)#username ciscoadmin password adminadmin123
Atlanta(config)#username ciscoadmin privilege 15
Atlanta(config)#enable password cisco123
Atlanta(config)#enable secret testing1234
Atlanta(config)#end
```

Refer to the exhibit. Which password must an engineer use to enter the enable mode?

A. adminadmin123

B. cisco123

C. default

D. testing1234

Correct Answer: *D*

If neither the enable password command nor the enable secret command is configured, and if there is a line password configured for the console, the console line password serves as the enable password for all VTY sessions -> The ג€enable secretג€ will be used first if available, then ג€enable passwordג€ and line password.

Community vote distribution

D (83%) A (17%)

Ray12345 Highly Voted 2 years, 4 months ago

i like this question:)

upvoted 16 times

ZUMY Highly Voted 2 years, 4 months ago

D is correct

If you set both enable password and enable secret. You will need to use the enable secret password to enter privileged mode.

upvoted 11 times

Dante_Dan 1 year, 7 months ago

Yes you are correct, but you are ignoring the "aaa new-model" and "...privilege 15" commands.

upvoted 1 times

GracieRamos 1 year, 2 months ago

I've test with Cat 2960. If you want to enable switch without enable password you need to use "privilege level 15" under line vty. please correct me if i misunderstand

upvoted 1 times

RougePotatoe 10 months, 2 weeks ago

Privilege level 15 on an interface will allow everyone to to get to user exec. If you want to limit it to per user then you want to configure username admin privilege level 15 password cisco123 in global configuration then do transport input ssh /telnet on line vty.

upvoted 1 times

RougePotatoe 10 months, 2 weeks ago

My bad I meant to say login local.

upvoted 1 times

OrwellMB Most Recent 2 months, 1 week ago

Selected Answer: D

Can be easily tested in Packet Tracer.
adminadmin123 is needed for general access, right after "Press RETURN to get started".
ciscoadmin + adminadmin123,

then "enable" and it accepts testing1234
upvoted 1 times

iMo7ed 7 months ago

Selected Answer: D

D is correct
upvoted 1 times

oatmealturkey 7 months, 1 week ago

Selected Answer: D

I tested it in PT. If you use AAA for local authentication like in the exhibit (I copied the exact lines from the exhibit), then try to Telnet in, it does not go straight to privileged EXEC mode; after logging in you will be prompted to enter the enable secret.

But then I removed AAA from the configuration so that it was just simple local authentication, without AAA, and in that case the privilege 15 password is enough to get you straight into privileged EXEC mode, no need to enter the enable secret.

So the key difference seems to be AAA.
upvoted 1 times

RougePotatoe 10 months, 2 weeks ago

Selected Answer: D

Tested it in packet tracer but I don't know why it is the right answer. The following command will allow you to get to user exec mode from line con0 with username password login "username admin privilege level 15 password cisco123 > line con 0 > login local". Based on the commands shown in the picture it seems like they were doing the same thing making the username a level 15 account but for some reason it doesn't work. Hopefully one of yall could explain the difference between (username admin privilege level 15 password cisco123) vs (username admin password cisco123 > username admin privilege level 15).
upvoted 1 times

[Removed] 1 year, 2 months ago

D secret takes precedence
upvoted 1 times

jossyda 1 year, 3 months ago

Selected Answer: D

enable secret
upvoted 3 times

ScorpionNet 1 year, 4 months ago

D is right and A is wrong because enable secret secures the Privilege Exec mode of the system
upvoted 1 times

geober 1 year, 5 months ago

D is the right answer that's it
upvoted 1 times

rlelliott 1 year, 6 months ago

Gotta love the giveme questions. If you can't answer this question correctly in less than 5 seconds, you may want to start your studying over again.
upvoted 2 times

DoBronx 10 months, 3 weeks ago

wow dude how exculpatory of you
upvoted 1 times

YaaElon 1 year, 6 months ago

The reason it is "D" is that the "adminadmin123" password gets you into USER EXEC mode. Once you enter the "enable" command it will prompt you for another password, and the "enable secret testing1234" command overrides the "enable password cisco123" forcing you to input "testing1234" to access the Privileged EXEC (enable mode).
upvoted 5 times

Shamwedge 1 year, 7 months ago

Selected Answer: D

Answer is D.
I just did this in packet tracer. The first password will adminadmin123, but the question states " to get into ENABLE mode, which is testing1234 because the secret password triumphs the unencrypted password.

So adminadmin123 will get you into the router, but testing1234 is what gets you into Enable mode.
upvoted 6 times

Dante_Dan 1 year, 7 months ago

Selected Answer: A

Very tricky question indeed.
If we remove the "login authentication default" command from VTY line, definitely the answer would be D, the one with the enable secret command. However, the "username ciscoadmin privilege 15" and "aaa new-model" commands make it a lot different.

I am at work so I couldn't look deeper into it but in such scenario, the Engineer must use the ciscoadmin credentials in order to log into the device and because of the privilege 15, they go directly into enable mode.

And because of the aaa new-model commands, no one else would be able to access to the device. so probably the answer is in fact A

Damn it!! I hate this kind of questions!!!
upvoted 2 times

cyborg7 11 months, 2 weeks ago
Yes, ciscoadmin credentials will take him to enable mode once log in. Suppose, he exit enable mode to user mode and want to enter enable mode now, which password he will use to enter enable mode ? I guess thats why testing1234 is correct.
upvoted 1 times

hector255 1 year, 7 months ago
Selected Answer: D
D is correct.
upvoted 1 times

AndersonMr 1 year, 8 months ago
Selected Answer: D
enable secret takes precidence
upvoted 1 times

Kane002 1 year, 8 months ago
Selected Answer: A
A. Login local will force username/password authentication. adminadmin123 with username ciscowhatever will be required.
upvoted 1 times

Question #238 *Topic 1*

Which state does the switch port move to when PortFast is enabled?

A. blocking

B. listening

C. learning

D. forwarding

Correct Answer: *D*

ZUMY 1 year, 2 months ago
D is correct!
upvoted 3 times

SScott 2 years, 1 month ago
D Forwarding is right

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html#:~:text=PortFast%20causes%20a%20switch%20or%20trunk%20port%20to%20enter%20the%20spanning%20tree%20forwarding%20state%20immediately%2C%20bypassing%20the%20listening%20and%20learning%20states.
upvoted 1 times

Bobrock 2 years, 1 month ago
Correct
upvoted 2 times

Question #239 *Topic 1*

Which protocol prompts the Wireless LAN Controller to generate its own local web administration SSL certificate for GUI access?

A. RADIUS

B. HTTPS

C. TACACS+

D. HTTP

Correct Answer: *B*
You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol.
When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate.
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_011.html

battery1979 1 year, 2 months ago
RADIUS and TACACS+ are not protocols, and HTTP can't utilize SSL.
upvoted 2 times

theRock2022 1 year, 5 months ago
HTTPS (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol that uses the SSL/TLS protocol for encryption and authentication.
upvoted 3 times

schleef 1 year, 10 months ago
This one is self-explaining - web(http) GUI + SSL = HTTPS
upvoted 2 times

Question #240 *Topic 1*

An engineer must configure interswitch VLAN communication between a Cisco switch and a third-party switch. Which action should be taken?

A. configure DSCP

B. configure IEEE 802.1q

C. configure ISL

D. configure IEEE 802.1p

Correct Answer: *B*

VLAN trunking offers two options, ISL and 802.1Q. ISL is Cisco proprietary while 802.1Q is standards based and supported by multiple vendors.

Timbul 8 months, 3 weeks ago

answer B and answer D look identical untill I figured out p and q difference

upvoted 2 times

ZUMY 1 year, 2 months ago

B is correct

upvoted 2 times

Ray12345 2 years, 4 months ago

B open standard

upvoted 2 times

Alsaher 2 years, 4 months ago

B is correct

upvoted 2 times

Question #241 *Topic 1*

An engineer requires a switch interface to actively attempt to establish a trunk link with a neighbor switch. What command must be configured?

A. switchport mode trunk

B. switchport mode dynamic desirable

C. switchport nonegotiate

D. switchport mode dynamic auto

Correct Answer: *B*
Reference:
https://www.ciscopress.com/articles/article.asp?
p=2181837&seqNum=8#:~:text=switchport%20mode%20dynamic%20auto%3A%20Makes,to%20trunk%20or%
.
20desirable%20mode.&text=switchport%20mode%20dynamic%20desirable%3A%20Makes,link%20to%20a%20trunk%20link

Community vote distribution

B (100%)

Nhan Highly Voted 2 years, 6 months ago

The key word here is “actively attempt” therefore only desirable is work, then the given answer is correct which is relevant to the question.

upvoted 16 times

cormorant Highly Voted 9 months, 2 weeks ago

An engineer requires a switch interface to actively attempt to establish a trunk link with a neighbor switch. What command must be configured?

actively

Actively

ACTIVELY

ACTIVELY IS EQUIVALENT TO DESIRABLE, THE SAME WAY THAT PASSIVE RELATES TO AUTO.

upvoted 7 times

[Removed] Most Recent 3 months ago

Selected Answer: B

Answer B is correct

upvoted 1 times

creaguy 11 months, 2 weeks ago

Selected Answer: B

It's B. Answer is right there in the reference ink.

upvoted 1 times

GreatDane 1 year, 2 months ago

Ref: Dynamic Trunking Protocol – Wikipedia

“...
Switch port modes
...
• Dynamic Auto — Makes the Ethernet port willing to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to trunk or dynamic desirable mode. This is the default mode for some switchports.
• Dynamic Desirable — Makes the port actively attempt to convert the link to a trunk link. The port becomes a trunk port if the neighboring Ethernet port is set to trunk, dynamic desirable or dynamic auto mode.
...”

A. switchport mode trunk

Wrong answer.

B. switchport mode dynamic desirable

Correct answer.

C. switchport nonegotiate

Wrong answer.

D. switchport mode dynamic auto

Wrong answer.

upvoted 3 times

ZUMY 1 year, 2 months ago

B is correct

upvoted 1 times

ScorpionNet 1 year, 4 months ago

B is right because Desirable actively attempts to establish a trunk port while Auto is looking for it's neighbor if it has trunk or desirable mode enabled

upvoted 1 times

YaaElon 1 year, 6 months ago

AUTO
PAgP mode places a LAN port into a PASSIVE negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP negotiation. (Default)
DESIRABLE
PAgP mode places a LAN port into an ACTIVE negotiating state, in which the port initiates negotiations with other LAN ports by sending PAgP packets.

upvoted 1 times

TA77 1 year, 2 months ago

The question is talking about trunking modes, not port aggregation modes :)

upvoted 1 times

Anarckii 1 year, 9 months ago

B is correct because its asking what configuration would have the switch "actively" form a trunk

upvoted 1 times

Hodicek 1 year, 10 months ago

B IS CORRET

upvoted 1 times

dicksonpwc 2 years, 1 month ago

Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode

upvoted 2 times

Alsaher 2 years, 4 months ago

B is correct

upvoted 2 times

YogaT 2 years, 4 months ago

The answer D "Dynamic auto" tells switch to sit there and wait on the other switch to start the negotiation. So it's wrong.

upvoted 7 times

Cisna 2 years ago

Note this statement in the question:-interface to actively attempt to establish a trunk link with a neighbor switch

upvoted 3 times

YogaT 2 years, 4 months ago

Command: switchport mode dynamic desirable, which asks the switch to both negotiate as well as to begin the negotiation process, rather than waiting on another device.
Thus B.

upvoted 5 times

Mahede 2 years, 6 months ago

A,B,D all is work

upvoted 3 times

Cisna 2 years ago

Any referal?

upvoted 1 times

Question #242 *Topic 1*

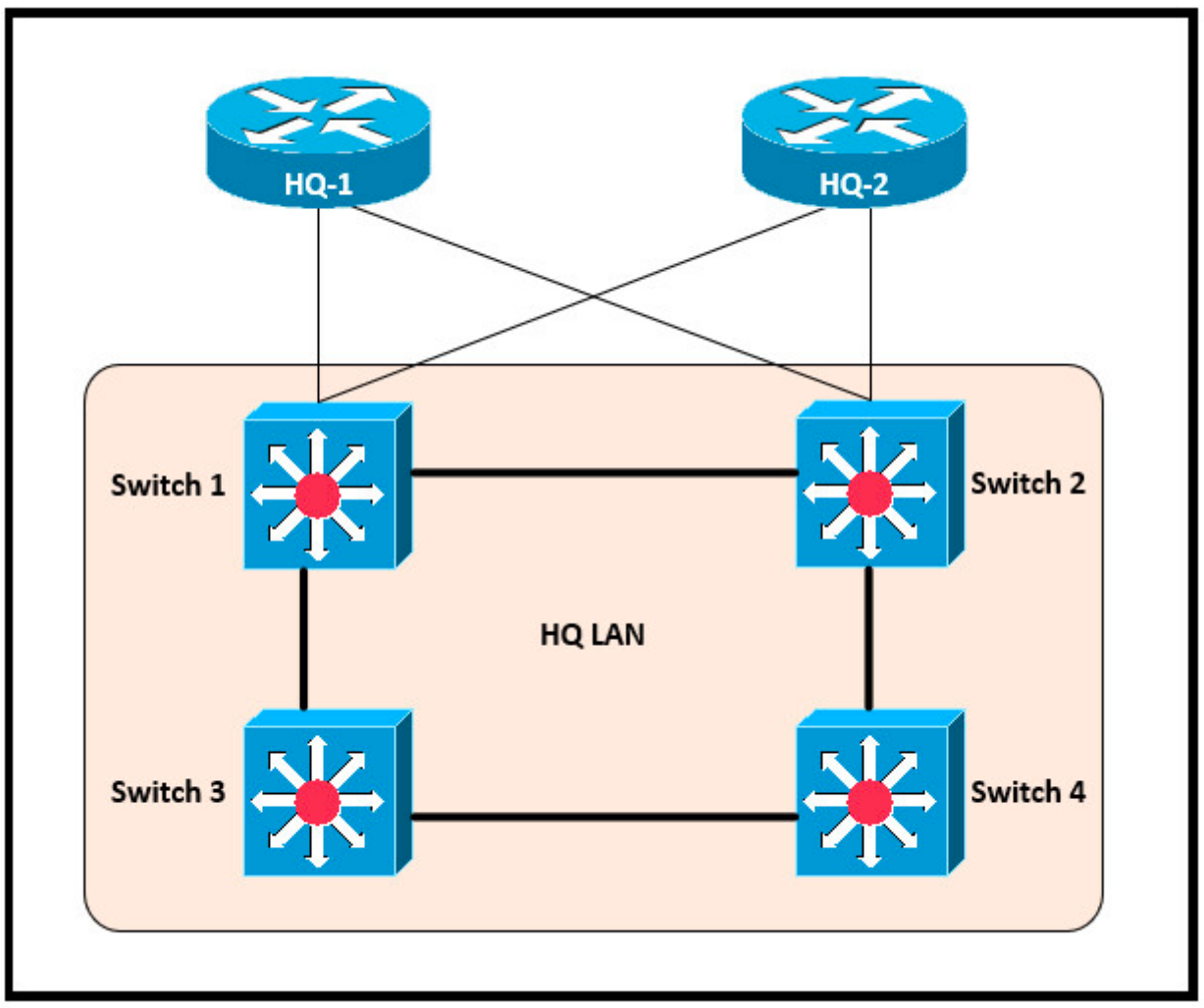
Refer to the exhibit. After the election process, what is the root bridge in the HQ LAN?

Switch 1: 0C:E0:38:81:32:58 -

Switch 2: 0C:0E:15:22:1A:61 -

Switch 3: 0C:0E:15:1D:3C:9A -

Switch 4: 0C:E0:19:A1:4D:16 -



A. Switch 1

B. Switch 2

C. Switch 3

D. Switch 4

Correct Answer: *C*

Community vote distribution

C (100%)

Anarckii Highly Voted 1 year, 9 months ago

Selected Answer: C

It's the switch with the lowest MAC address

upvoted 9 times

Lovens Highly Voted 2 years ago

C is the answer:
22hex= 2*16^1+2*16^0=32+2=32 while 1D=1*16^1+13*16^0=16+13=29

upvoted 9 times

DeadSkru11 1 year, 8 months ago

Thanks. I was furiously searching for this Ans from past 2 days

upvoted 4 times

DonnerKomet 2 years ago

wrong, 32 +2 = 34 not 32

upvoted 6 times

ZUMY Most Recent 1 year, 2 months ago

C is correct

upvoted 3 times

Question #243 *Topic 1*

An engineer must establish a trunk link between two switches. The neighboring switch is set to trunk or desirable mode. What action should be taken?

A. configure switchport nonegotiate

B. configure switchport mode dynamic desirable

C. configure switchport mode dynamic auto

D. configure switchport trunk dynamic desirable

Correct Answer: *C*

Community vote distribution

B (52%) C (48%)

Masood101 Highly Voted 2 years, 4 months ago

B and C are correct

upvoted 14 times

andiks Highly Voted 2 years, 7 months ago

Actually B is correct as well

upvoted 8 times

wakaish Most Recent 1 week, 2 days ago

B. configure switchport mode dynamic desirable

This command configures the port to operate in a dynamic desirable mode, which means it will actively attempt to form a trunk with the neighboring switch. It's a good choice when the other side is set to trunk or desirable, as it allows the two switches to negotiate and establish a trunk link.
configure switchport mode dynamic auto - This command sets the port to a dynamic auto mode, which means it will passively wait for the other side to initiate trunk negotiation. It's not ideal when the neighboring switch is set to trunk or desirable because it won't actively attempt to establish a trunk.

upvoted 1 times

_mva 1 month, 3 weeks ago

Assuming the default setting for new switches is auto (which means there is already a trunk in this case) then B is the correct answer.

upvoted 1 times

davidmdlp85 2 months ago

If there's a "must" then I'll go with Desirable (Option B)

upvoted 1 times

XuniLrve4 2 months, 2 weeks ago

Bad question, unless asking for two answers!

upvoted 1 times

xbololi 2 months, 3 weeks ago

Selected Answer: B

Both correct xD

upvoted 1 times

VanessaR05 2 months, 3 weeks ago

Selected Answer: C

C its correct

upvoted 1 times

valekky 3 months ago

C is correct - switchport mode dynamic auto: Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. The default switchport mode for newer Cisco switch Ethernet interfaces is dynamic auto. Note that if two Cisco switches are left to the common default setting of auto, a trunk will never form.

upvoted 1 times

Jorro99404 4 months ago

Selected Answer: C

B and C are correct

upvoted 2 times

Bhrino 4 months ago

Selected Answer: C

The question is kindve vague so b and c work

upvoted 1 times

EllesJ 4 months, 3 weeks ago

since the nieghboring switch is set to trunk or desirable, auto will configure the link as trunk while simultaneously preventing other links to be trunks as well. This is maybe the best option from a safety point of view, since VLAN traffic is restricted to where it needs to go

upvoted 3 times

thomson_johnson 6 months ago

https://community.cisco.com/t5/switching/why-dtp-is-used/td-p/1377495

Hall of Fame Cisco Employee Peter Paluch Hall of Fame Cisco EmployeeCisco Certified Internetwork Expert Enterprise Infrastructure (CCIE Enterprise Infrastructure)Hall of Fame Cisco Employee

"The DTP helps to automatically negotiate whether the port should be put into access or trunk mode and what trunking protocol (802.1Q or ISL) should be used. The individual DTP modes are:

dynamic auto - the port will negotiate the mode automatically, however, it prefers to be an access port
dynamic desirable - the port will negotiate the mode automatically, however, it prefers to be a trunk port"

well if the auto prefers to be an access port, i guess desirable is right.
I don't think that on the exam they would not require 2 options to be selected.

upvoted 1 times

linuxlife 6 months ago

The neighbor device was set to either TRUNK or DYNAMIC DESIRABLE.
If their is a choice to configure the local device to be TRUNK, then thats the right answer. Unfortunately, it wasnt in the choices.
So we are in between to choose:
DYNAMIC DESIRABLE or DYNAMIC AUTO.
Assuming the neighbor device is not TRUNK, instead it is DYNAMIC DESIRABLE, it means that the neighbor device initiates negotiation messages and responds to negotiation messages to dynamically choose whether to start using TRUNKING.

If this is the case, then the local device, which is our concern should have port configured with DYNAMIC AUTO which means, it will passively wait to receive TRUNK negotiation messages, at which point the switch will respond and negotiate whether to use TRUNKING.

So, assuming that the neighbor device was also set to TRUNK and the local device was set to DYNAMIC AUTO, it will still goes to TRUNK.

If both devices, neighbor and local are configured at DYNAMIC DESIRABLE, then both devices initiates negotiation messages which is not right...

upvoted 3 times

Alan100 7 months, 4 weeks ago

Selected Answer: B

auto is the default state is auto. If an action is to be made, set to dynamic desirable so the port can actively seek to become a trunk.

upvoted 3 times

DMc 8 months, 2 weeks ago

I vote B using the "Must" or force the switchport interface to take some action instead of just be "willing."
"Dynamic Auto — Makes the Ethernet port willing to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to trunk or dynamic desirable mode. This is the default mode for some switchports. Dynamic Desirable — Makes the port actively attempt to convert the link to a trunk link."

upvoted 3 times

BreezyNet 8 months, 3 weeks ago

THE CORRECT ANSWER IS B

upvoted 1 times

Question #244 *Topic 1*

Which spanning-tree enhancement avoids the learning and listening states and immediately places ports in the forwarding state?

A. BPDUfilter

B. PortFast

C. Backbonefast

D. BPDUguard

Correct Answer: *B*

Community vote distribution

B (100%)

Alsaher Highly Voted 2 years, 4 months ago

B is correct

upvoted 5 times

ricky1802 Most Recent 7 months, 1 week ago

Selected Answer: B

The correct answer is B. PortFast.

PortFast is a feature in the Spanning Tree Protocol (STP) that is used to quickly transition a port from the blocking state to the forwarding state. This feature is typically used for access ports that connect to end devices (such as PCs or servers), which do not generate Spanning Tree Protocol (BPDUs) messages. By using PortFast, the STP learning and listening states are skipped and the port is immediately placed into the forwarding state, reducing the amount of time it takes for the port to transition from a blocking to a forwarding state.

upvoted 2 times

ricky1802 7 months, 1 week ago

A. BPDUfilter: This feature disables the processing of received BPDUs on a port, but it does not change the operation of the Spanning Tree Protocol.

C. Backbonefast: This feature is used to quickly detect and recover from indirect failures in the network, but it does not change the operation of the Spanning Tree Protocol on individual ports.

D. BPDUguard: This feature helps to prevent unauthorized switches from being connected to the network by disabling a port if it receives a BPDU message. This can help to prevent unauthorized switches from affecting the operation of the Spanning Tree Protocol.

upvoted 1 times

Customexit 10 months, 3 weeks ago

PortFast: allows the port to go straight to a forwarding state because there is no danger of a loop.

BPDU Guard: If an interface with this enabled receives BPDU from another switch, the interface will be shut down to prevent a loop from forming.

Root Guard*: even if it receives a superior BPDU (lower bridge ID) on that interface, the switch will not accept the new switch as the root bridge. The interface will be disabled.

Loop Guard*: even if the interface stops receiving BPDUs, it will not start forwarding. The interface will be disabled.

* = not mentioned in objectives.

upvoted 1 times

ZUMY 1 year, 2 months ago

B is correct!

upvoted 1 times

Nebulise 1 year, 7 months ago

B is correct

upvoted 1 times

netlol 1 year, 7 months ago

Spanning Tree Portfast causes layer 2 switch interfaces to enter forwarding state immediately, bypassing the listening and learning states. It should be used on ports connected directly to end hosts like servers or workstations. Note: If portfast isn't enabled, DHCP timeouts can occur while STP converges, causing more problems.

upvoted 2 times

Pamirt 2 years, 1 month ago

B is correct

upvoted 3 times

Question #245 *Topic 1*

How does the dynamically-learned MAC address feature function?

A. The CAM table is empty until ingress traffic arrives at each port

B. Switches dynamically learn MAC addresses of each connecting CAM table.

C. The ports are restricted and learn up to a maximum of 10 dynamically-learned addresses

D. It requires a minimum number of secure MAC addresses to be filled dynamically

Correct Answer: *A*

Community vote distribution

A (100%)

Stallion 1 month, 3 weeks ago

Option B is correct because switches dynamically learn the MAC addresses of each connecting device and store them in the CAM table.

upvoted 1 times

lamm 2 months ago

Selected Answer: A

correct answer

upvoted 1 times

kyleptt 2 months, 3 weeks ago

Switches also learn MAC addresses from ARP so, thus MAC learn is also possible.

upvoted 1 times

RSA001 1 year, 7 months ago

The CAM table is empty until ingress traffic arrives at EACH port?
Is the CAM empty until then??

upvoted 1 times

Nicocisco 1 year, 6 months ago

Yes!
The mac addresse table is empty when the switch start

upvoted 1 times

VictorCisco 5 months ago

So what?? It doesn't need to receive trafic on EACH port of a switch to start to fill it. just on one port is enough !

upvoted 1 times

panagiss 1 year, 10 months ago

CAM? Is it a typo?

upvoted 2 times

kyleptt 2 months, 3 weeks ago

nope Content Addressable Memory

upvoted 1 times

laurvy36 1 year, 9 months ago

Content Addressable Memory (CAM) table is a system memory construct used by Ethernet switch logic which stores information such as MAC addresses available on physical ports

upvoted 1 times

Jbcrggddfhh 1 year, 4 months ago

It's another name for the MAC address table

upvoted 2 times

Stonetales987 1 year, 10 months ago

A is correct. https://www.cisco.com/c/en/us/td/docs/switches/metro/me2600x/config/guide/b_ME2600X-scg/b_ME2600X-scg_chapter_0110.pdf

upvoted 1 times

Question #246 *Topic 1*

When using Rapid PVST+, which command guarantees the switch is always the root bridge for VLAN 200?

A. spanning-tree vlan 200 priority 614440

B. spanning-tree vlan 200 priority 0

C. spanning-tree vlan 200 root primary

D. spanning-tree vlan 200 priority 38813258

Correct Answer: *B*

Community vote distribution

B (100%)

Asymptote Highly Voted 2 years, 1 month ago

there is the same question earlier this one,
but taht answer is D ...

upvoted 21 times

Smaritz 1 year, 5 months ago

Indeed, a bit confusing, or I'm missing something

upvoted 2 times

Taku2023 6 months, 1 week ago

The last qsn i came across was exactly the same and it says the keyword "root" should be used because there might be 2 switches with the priority of 0 on that same network

upvoted 3 times

ScorpionNet 1 year, 4 months ago

B is correct because the lowest bridge priority is the root

upvoted 1 times

sasquatchshrimp 1 year, 1 month ago

You can have two switches with 0 priority, but specifying one to be the root, will establish it as the root, and walk over priority number.

upvoted 2 times

CISCO2022 Highly Voted 2 years, 3 months ago

set as Primary dose not grantee the root stay as root always. set as zero grantees the root will always be root.

upvoted 12 times

diriba Most Recent 1 month ago

In Rapid PVST+ (Per-VLAN Spanning Tree Plus) protocol, you can use the "spanning-tree vlan 200 root primary" command to ensure that a switch becomes the root bridge for VLAN 200. This command sets the priority of the switch to the lowest value (0) for the specified VLAN, making it the root bridge.

By setting the priority to the lowest value, the switch will have the highest priority and will become the root bridge for the specified VLAN. Keep in mind that this command only affects VLAN 200 and does not impact the spanning tree topology for other VLANs.

Here's the complete command:

Copy
switch(config)# spanning-tree vlan 200 root primary
Make sure to execute this command on the desired switch to ensure it becomes the root bridge for VLAN 200 in Rapid PVST+ topology.

upvoted 2 times

Njavwa 5 months, 3 weeks ago

last question i came across with setting the priority to zero(0) was incorrect and now its correct lol... i think we need to follow our books more in as much as we need to revise

upvoted 3 times

oatmealturkey 7 months, 1 week ago

Selected Answer: B

About root primary command:
https://community.cisco.com/t5/switching/spanning-tree-vlan-root-primary/td-p/1269595
Paraphrasing from this source:
The "spanning-tree root primary" command is actually a macro and it is executed only one time. If after this somebody configures another device with a lower priority, this node cannot react to this and it will lose its root bridge role.
If you use "spanning-tree vlan 1 priority 0", only another device with pri 0 and a lower MAC address can take the role of root bridge.

upvoted 2 times

greatnickbname1 7 months, 1 week ago

C. spanning-tree vlan 200 root primary

upvoted 2 times

JonasWolfxin 1 year, 2 months ago

The spanning-tree vlan vlan_ID root command fails if the value required to be the root bridge is less than 1.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html#task_1163819

upvoted 2 times

Marcos9410 1 year, 2 months ago

Selected Answer: B

The spanning-tree vlan vlan_ID root command fails if the value required to be the root bridge is less than 1.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html

upvoted 1 times

ZUMY 1 year, 2 months ago

B is correct!

upvoted 1 times

bmatthee01 1 year, 6 months ago

Correct Answer C
technically B is relevant only if you want to change the priority of the root bridge, but to ensure the switch is always the root bridge you must explicitly configure it as the root
eg
SW4(config)#spanning-tree vlan 1 ?
priority Set the bridge priority for the spanning tree
root Configure switch as root
<cr>

https://www.omnisecu.com/cisco-certified-network-associate-ccna/how-to-configure-spanning-tree-protocol-root-primary-and-root-secondary.php

upvoted 2 times

sgashashf 1 year, 6 months ago

Execute the command "spanning-tree vlan 1 root primary" on a switch and then check the running config. All it lists is a priority 4096 lower than the lowest priority detected on the network. The primary/secondary commands don't do what you think they do.

upvoted 3 times

JackBond40 1 year, 7 months ago

The key phrase "guaranteed is always". using the primary command causes the switch to check the existing root switch priority and then lower its priority by 4096. This is only done once thus if a new switch is introduced later with an even lower priority that switch will become root bridge. The only way to guarantee a switch remains root is to set its priority to 0.

upvoted 4 times

sgashashf 1 year, 6 months ago

While you are correct, if another switch with a lower mac AND a priority of 0 is added to the network, it would then become the root bridge. I agree that B is the best answer here, but technically there is no way to "guarantee" 100%.

upvoted 4 times

hassanhhady 1 year, 9 months ago

thank you is there a new qoustions about ccna 2021 after changing exam rules

upvoted 2 times

Anarckii 1 year, 9 months ago

I looked at other resouces because I though the answer was C, but B seems to be correct

upvoted 1 times

Alibaba 1 year, 9 months ago

B true

upvoted 2 times

dthomas53 1 year, 10 months ago

Answer is C.

From Cisco Press book 31 Days Before Your CCNA Exam:

"The network administrator wants to ensure that S1 is always the root bridge (...). The following commands achieve this objective:

S1(config)# spanning-tree vlan 1 root primary

The 'primary' keyword automatically sets the priority to 24576 or to the next 4096 increment value below the lowest bridge priority detected on the network."

This suggests to me whenever a new root bridge election is held, SW1 will update its priority so as to be the lowest.

upvoted 7 times

zaguy 2 years ago

Correct Answer : spanning-tree vlan 200 priority 0

The best way to prevent erroneous devices from taking over the STP root role is to set the priority to 0 for the primary root switch and to 4096 for the secondary root switch. In addition, root guard should be used.
https://www.ciscopress.com/articles/article.asp?p=2995351&seqNum=2

upvoted 1 times

Cpynch 1 year, 7 months ago

If you have another switch with a lower MAC that is also set to priority 0, this command will not guarantee it is root bridge. Only the 'primary' command will guarantee whatever any other switch is set to, this switch will become the bridge.

upvoted 1 times

bwg 2 years, 3 months ago

What's the difference between B and C ?

upvoted 4 times

Roberts132 2 years, 2 months ago

root primary does that command reduces the the switch priority by 8192 to make it root switch (if all switch have the default priority of 32768)

upvoted 3 times

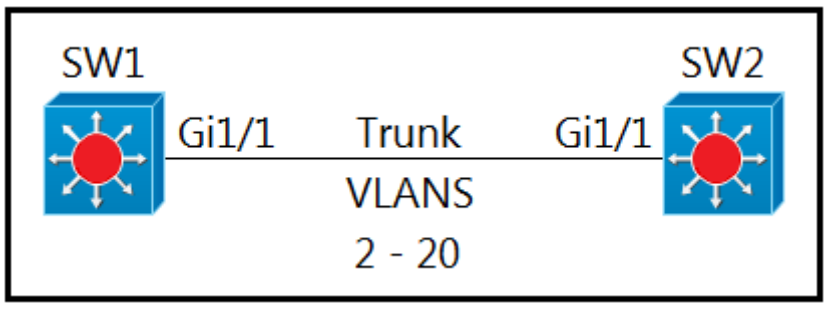
M3rc3r08 2 years, 1 month ago

When configuring root primary, the switch looks at the priority of the current root switch and chooses either (a) 24,576 or (b) 4096 less than the current root's priority (if the current root's priority is 24,576 or less) to the configuration instead.

When configuring, root secondary always results in that switch using a priority of 28,672, with the assumption that the value will be less than other switches that use the default of 32,768, and higher than any switch configured as root primary.

upvoted 2 times

Question #247 *Topic 1*



Refer to the exhibit. Which command must be executed for Gi1/1 on SW1 to passively become a trunk port if Gi1/1 on SW2 is configured in desirable or trunk mode?

A. switchport mode dynamic auto

B. switchport mode dot1-tunnel

C. switchport mode dynamic desirable

D. switchport mode trunk

Correct Answer: *A*

Community vote distribution

A (100%)

CiscoTerminator Highly Voted 2 years, 1 month ago

Key Word is "passively" - so its Auto

upvoted 13 times

xbololi Most Recent 2 months, 3 weeks ago

Selected Answer: A

"passively become"

upvoted 1 times

Ceruzka 6 months, 3 weeks ago

another bad q: " SW2 is configured in desirable or trunk mode" Saying that IF:
SW1 dynamic auto - SW2 dynamic desirable -> trunk = thats fine
BUT
SW1 dynamic auto - SW2 trunk -> will not create a trunk
I assume they expect answer "A" SW1 dynamic auto

upvoted 2 times

ZUMY 1 year, 2 months ago

A is correct

upvoted 1 times

taiyi078 1 year, 8 months ago

SW1 dynamic auto - SW2 dynamic auto -> access
SW1 dynamic auto - SW2 dynamic desirable -> trunk

upvoted 1 times

mickeil 2 years, 3 months ago

A and C are true, no ?

upvoted 3 times

Sten111 2 years, 2 months ago

Both answers will negotiate a trunk but only auto will do it passively like the question asks.

upvoted 4 times

SScott 2 years, 1 month ago

Here is a good summary

https://www.grandmetric.com/knowledge-base/design_and_configure/how-to-configure-dynamic-trunking-protocol-dtp-cisco/#:~:text=Dynamic%20auto%20%E2%80%93%20passive%20mode%2C%20allow%20to%20form%20%E2%80%9CTrunk%E2%80%9D%20state%20if%20second%20end%20is%20actively%20negotiating

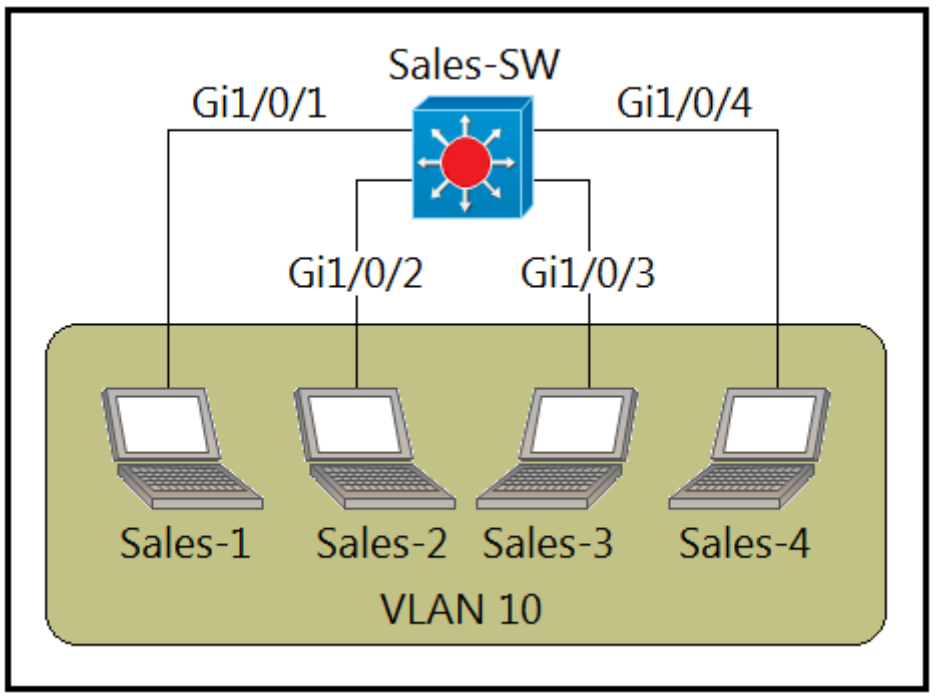
upvoted 3 times

Technique31 1 year, 11 months ago

"C" is not true because in question it says "SW1 to passively become a trunk port"
So in Dynamic Auto mode the switch port waiting passively to become Trunk

upvoted 1 times

Question #248 *Topic 1*



Refer to the exhibit. The entire contents or the MAC address table are shown. Sales-4 sends a data frame to Sales-1.

```
Sales-SW#show mac-address-table
Mac Address Table
-------------------------------------------------------------
VLAN    MAC Address       Type        Ports
10      000c.8590.bb7d    DYNAMIC     Gi1/0/1
10      3939.1170.1bb7    DYNAMIC     Gi1/0/2
10      00d0.d3b6.957c    DYNAMIC     Gi1/0/3
Sales-SW#
```

What does the switch do as it receives the frame from Sales-4?

A. Map the Layer 2 MAC address to the Layer 3 IP address and forward the frame.

B. Insert the source MAC address and port into the forwarding table and forward the frame to Sales-1.

C. Perform a lookup in the MAC address table and discard the frame due to a missing entry.

D. Flood the frame out of all ports except on the port where Sales-1 is connected.

Correct Answer: *B*

Community vote distribution

B (100%)

raul_kapone 4 weeks, 1 day ago

Selected Answer: B

The complete action performed by the switch Sales-SW is:
1) Learn the Source MAC address of the FastEthernet intefac of Sales-4
2) Associate this MAC address with the Gi1/0/4 interface of the switch (Sales-SW)
3) Finally, Sales-SW will flood a copy of the incoming frame for all their ports, except the incoming port (reaching to all hosts, including Sales-.1

However, by discarding and due to there is no an option specifing the complete action performed by Sales-SW does (one of the points specified above): The option "B" is right (but it is not the only thing what is happening!)

upvoted 1 times

achavessu 4 months, 2 weeks ago

What confuses me is the jargon, why call it Forwarding table? I mean, it is the only option that really makes sense, but the name of that data structure is clearly cam table or mac table, not forwarding table. Can anybody point me to a reference that refers to it as Forwarding table please?

upvoted 1 times

country_rooted 5 months, 2 weeks ago

D is incorrect, it says it will flood to all ports except to Sales-1, the one you're trying to reach. Switches flood to all ports except the one the frame was received (in this case Sales-4).

upvoted 2 times

Njavwa 5 months, 3 weeks ago

it cant be D,
there is no Mac addr of src in the table, but the Dst Mac is in the table so the table will be registered with Src and forward to sales-1 where its

pointing
correct answer is B
upvoted 1 times

ZUMY 1 year, 2 months ago

B is correct!
upvoted 3 times

putler2 1 year, 3 months ago

Wouldn't it be D?
Assuming Sales-4 never sent anything to Sales-1 (since there's no MAC address table entry from Sales-4 in the switch) it won't know Sales-1's MAC Address. Not knowing the MAC address, it'll use ARP and set broadcast FF:FF:FF:FF:FF:FF as the MAC Destination. When the Switch receives Sales-4s ARP request and see's the FF:FF:FF:FF:FF:FF in source MAC, it'll have no choice but to broadcast it to all ports except from where it came from.

The only way it could be B is if Sale-4 already had Sales-1's MAC address cached in it's arp table.

Am I over thinking this?
upvoted 3 times

FALARASTA 4 months, 3 weeks ago

Exactly. The switch is already aware of the address to forward the frame. What it does is to recognize the new device Mac Sales-4 and adds it Mac to its CAM and forwards the frame to the existing Mac sales-1
upvoted 2 times

battery1979 1 year, 2 months ago

The switch already knows Sale-1s address and the switch is forwarding the traffic ao it doesn't matter if Sale-4 knows where the traffic is going or not as the question is asking what the switch will do.
upvoted 4 times

johnnd 1 year, 7 months ago

Selected Answer: B

B indeed
upvoted 1 times

bhurishravas 1 year, 8 months ago

Selected Answer: B

I choose B. Not D. Because SW will flood`s only if it don`t know to whom forward the frame. In this case the SW has clear bind mac to port
upvoted 1 times

Anarckii 1 year, 9 months ago

The answer is B, because the MAC table doesnt have the MAC address or port number yet, so it is going to have to use ARP
upvoted 1 times

Hodicek 1 year, 9 months ago

B IS CORRECT AS SWITCH KNOW DST , SO IT WILL REGISTER SRC IN CAM TABLE AND PASS THE DATA TO DST AS IT IS REGISTERED ALREADY IN CAM TABLE
upvoted 4 times

FGR1987 2 years ago

it can not be answer D because switch knows the destination MAC.
upvoted 2 times

firstblood 2 years ago

It's D. Because Sale 4 MAC is missing from the CAM table.
upvoted 1 times

laurvy36 1 year, 9 months ago

the switch needs to know the destination, not the source, it already knows the destination, so it fowards the frame to the port where he learned that mac address
upvoted 2 times

PanteLa_26 1 year, 9 months ago

It's not D. Switches make forwarding decisions based on destination MAC addresses. In this case the switch knows where Sales-1 PC is, so there's no need for flooding. Sales-4 PC's MAC will be added to CAM table for future reference.
upvoted 2 times

Dante_Dan 2 years, 2 months ago

I think answer should be D.
Answer B says that adds the MAC information to the table when it’s already in.

In the exhibit you can see that laptop 4 is not in the table, so the switch needs to find where is it by flooding all ports except the one the petition came from.

D
upvoted 1 times

UmbertoReed 2 years, 1 month ago

>>> "In the exhibit you can see that laptop 4 is not in the table, so the switch needs to find where is it by flooding all ports except the one the petition came from".

This would be the case if Sales-1 were trying to frames to Sales-4, but it is the other way around, Sales-4 is sending to Sales-1.

The switch does not currently have an entry for Sales-4's MAC address, so it will add it and then send a Layer 2 unicast to Sales-1 (because it already has an entry mapped for it).

upvoted 6 times

SScott 2 years, 1 month ago

When Sales-4 sends the frame to Sales-1, the Sales-SW switch will receive the frame first and add the MAC address of Sales-4 and Gi1/0/4 to the CAM table. The switch will already have Sales-1's MAC address and port and forward the frame as requested.

upvoted 1 times

bwg 2 years, 3 months ago

B is right. Although the sentence "forward the frame to Sales-1" looks like a little strange.

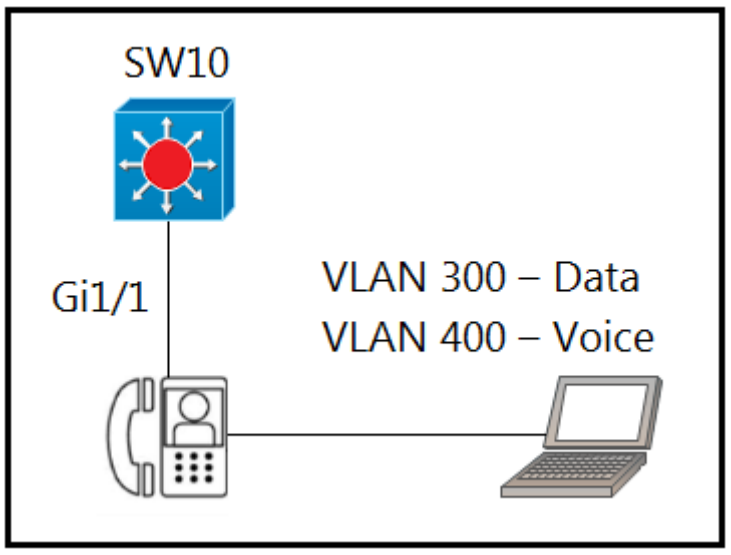
upvoted 3 times

SScott 2 years, 1 month ago

Yes, B is the best answer.
https://www.ciscopress.com/articles/article.asp?p=3089352&seqNum=6
D is incorrect because there is no reference to the frame MAC and port info being added to the table and Sales-4 is the originating machine.

upvoted 1 times

Question #249 *Topic 1*



Refer to the exhibit. An engineer must configure GigabitEthernet1/1 to accommodate voice and data traffic. Which configuration accomplishes this task?

A. interface gigabitethernet1/1 switchport mode access switchport access vlan 300 switchport voice vlan 400

B. interface gigabitethernet1/1 switchport mode trunk switchport trunk vlan 300 switchport trunk vlan 400

C. interface gigabitethernet1/1 switchport mode access switchport voice vlan 300 switchport access vlan 400

D. interface gigabitethernet1/1 switchport mode trunk switchport trunk vlan 300 switchport voice vlan 400

Correct Answer: *A*

Community vote distribution

A (88%) 13%

ZUMY 1 year, 2 months ago

A is correct

upvoted 3 times

SOAPGUY 1 year, 4 months ago

Selected Answer: A

PAGE198, VOL1;
Example 8-8 Configuring the Voice and Data VLAN on Ports Connected to Phones

upvoted 3 times

LilGhost_404 1 year, 7 months ago

Selected Answer: A

https://study-ccna.com/configuring-voice-vlans/

upvoted 2 times

Ravan 1 year, 7 months ago

A is correct

upvoted 1 times

johnnd 1 year, 7 months ago

A indeed

upvoted 1 times

AndersonMr 1 year, 8 months ago

Selected Answer: A

Voice VLANs work like this.

upvoted 1 times

yonten007 1 year, 8 months ago

Selected Answer: D

D: You need to enable protected management frame under the SSID configured

upvoted 1 times

Anarckii 1 year, 9 months ago

Selected Answer: A

For some this may be confusing and it go be the first time around untill i looked at the answer more clearly. The answer is A, because lets say you wanted to configure the port as a management port, you would want to configure that interface first before the voice vlan. Thats the only I remember from working with switching as an administrator

upvoted 1 times

vannplus11 1 year, 12 months ago

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swvoip.pdf

upvoted 1 times

etx 2 years, 2 months ago

How can this be correct? Access ports can only process one vlan per port.

upvoted 3 times

sdokmak 2 years, 2 months ago

VoIP phones work in a weird way. The access port is split into two ports, one for voice and one for data. So somehow the access access port behaves like a trunk.

upvoted 11 times

Bne_Pradhan 2 years, 3 months ago

Guys, how can a access port manage to process two different Vlans over the same interface, not convinced with the ans.

upvoted 2 times

Sten111 2 years, 2 months ago

It is a trunk but not configured as a trunk. Voice VLANS are weird.
https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/voice-vlan

upvoted 5 times

SScott 2 years, 1 month ago

While A seems to be incorrect syntax and an invalid command line, of the choices listed A is the best answer.

https://www.learncisco.net/courses/icomm-ccna-voice/cisco-uc-solution-maintenance/switch-configuration.html#:~:text=Cisco%20allows%20us%20to%20have%20two%20VLANs%20connected%20to%20one%20port%2C%20it%27s%20a%20multi-VLAN%20access%20port.%20And%20Cisco%20allows%20us%20to%20bend%20the%20rules%20if%20and%20only%20if%20one%20of%20those%20two%20VLANs%20is%20a%20voice%20VLAN

https://community.cisco.com/t5/switching/subinterface-to-access-port/td-p/3804800

https://www.reddit.com/r/networking/comments/m5ruhr/8021x_and_allowing_phones_on_voice_vlan/

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/113260-voice-vlan-00.html#:~:text=Configure%20specified%20VLANs%20for%20voice%20and%20data%20traffic

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swvoip.pdf

upvoted 2 times

SScott 2 years, 1 month ago

Some very good discussions covering answer D which illustrate this command line being invalid:

https://community.cisco.com/t5/switching/what-happens-when-voice-vlan-command-is-added-to-a-trunk-port/td-p/1570579

https://learningnetwork.cisco.com/s/question/0D53i00000Kt1GR/voice-vlan-on-a-trunk-port

upvoted 1 times

Question #250 *Topic 1*

An engineer needs to add an old switch back into a network. To prevent the switch from corrupting the VLAN database, with action must be taken?

A. Add the switch in the VTP domain with a lower revision number.

B. Add the switch in the VTP domain with a higher revision number.

C. Add the switch with DTP set to dynamic desirable.

D. Add the switch with DTP set to desirable.

Correct Answer: *A*

Community vote distribution

A (100%)

Customexit Highly Voted 10 months, 3 weeks ago

Selected Answer: A

One danger of VTP:
If you connect an old switch with a higher revision number to your network (and the VTP domain name matches), all switches in the domain will sync their VLAN database to that switch.
upvoted 6 times

[Removed] Most Recent 3 months ago

VTP is not part of CCNA 200-301
upvoted 2 times

maumorerag 2 months, 3 weeks ago

Did you already certificate?
upvoted 1 times

GreatDane 1 year, 2 months ago

Ref: VTP Client and revision numbers - Cisco Community

Post by balaji.bandi

"...
Adding a VTP Client Switch to a VTP Domain

Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number.
..."

A. Add the switch in the VTP domain with a lower revision number.

Correct answer.

B. Add the switch in the VTP domain with a higher revision number.

Wrong answer.

C. Add the switch with DTP set to dynamic desirable.

Wrong answer.

D. Add the switch with DTP set to desirable.

Wrong answer.
upvoted 3 times

ZUMY 1 year, 2 months ago

A is correct
upvoted 1 times

ScorpionNet 1 year, 4 months ago

A is right because you don't want to mess the database up
upvoted 1 times

bitree 1 year, 5 months ago

whether A or B, The switch has to have the lower revision number, not the VTP domain.
They should have used more words to make that clear. Likely the answer is A because if you're putting in a switch, you're going to do it regardless

of what the VTP domain is currently set up as. and so, the "with a lower revision number" likely refers to the switch.
upvoted 3 times

dipanjana1990 1 year, 1 month ago
exactly, that's why i got confused between "A" and "B" because of the selection of the words.
upvoted 2 times

xSora 1 year, 5 months ago
Why are people answering B?
Answer is A.
upvoted 2 times

mohdalijmc 1 year, 6 months ago
ANSWER B
I highly suggest you implement some kind of vtp configuration to prevent this in the future. Adding a switch with a higher revision can easily wipe out the vlan configuration on the remaining switches and perhaps that's exactly what happened

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_40_se/configuration/guide/scg1/swvtp.html
upvoted 2 times

CRP098274 1 year, 9 months ago
Answer is B
Please read the question carefully. The question is pertaining to the old switch from corrupting the VLAN database. It needs the highest revision number in order to prevent from corrupting the VLAN database.
upvoted 3 times

laurvy36 1 year, 8 months ago
if you put a switch with higher revision number will f...k up the database of the other switches, if you put a switch with lower revison number, it will update the database according with the other swithces
upvoted 8 times

LOST40 1 year, 6 months ago
Absolutely not! You're on drugs. Two ways to prevent network breakdown:
a). change VTP domain to an unused domain, will reset the REVISION number to ZERO.
b). Change the VTP mode to transparent in order to reset the REVISION number to ZERO.
upvoted 3 times

samuraipizza26 1 year, 12 months ago
B

Caution Before adding a VTP client switch to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number.

http://www.securecisco.com/TMCCcisco1234F12/StudyGuide/ccna3/Info/revision.number.htm
upvoted 1 times

schleef 1 year, 10 months ago
In real life you would just put a switch in transparent mode...
upvoted 4 times

UmbertoReed 1 year, 12 months ago
This source verifies that the correct answer is "A". Did you type wrong or did you misunderstand the source?
upvoted 9 times

samuraipizza26 1 year, 11 months ago
Wording error on my part. A is correct.

Thanks
upvoted 5 times

Question #251 *Topic 1*

Which technology prevents client devices from arbitrarily connecting to the network without state remediation?

A. 802.11n

B. 802.1x

C. MAC Authentication Bypass

D. IP Source Guard

Correct Answer: *B*

Community vote distribution

B (100%)

sdokmak Highly Voted 2 years, 2 months ago

B seems right.
A. is a wifi extension protocol
C. is a means of bypassing 802.1x which is the opposite of what we want.
D. is when an attacker uses the same IP as the client. But the question states client devices as a given.

upvoted 15 times

GreatDane Most Recent 1 month, 4 weeks ago

Selected Answer: B

MS Switch Access Policies (802.1X) - Cisco Meraki

"...
Access Policy Types

There are three options available for an access policy in Dashboard:

802.1X (Default)
When an 802.1X access policy is enabled on a switchport, a client that connects to that switchport will be prompted to provide their domain credentials. If the RADIUS server accepts these credentials as valid, their device will be granted access to the network and get an IP configuration. If no authentication is attempted, they will be put on a "guest" VLAN, if one is defined.
...
Other RADIUS Features
...
Failed Authentication VLAN

A client device connecting to a switchport controlled by an access-policy can be placed in the failed authentication VLAN if the RADIUS server denies its access request.
Client devices may fail RADIUS authentication because they do not comply with the network's security requirements. The failed authentication VLAN provides such clients with limited access to network for remediation purposes.
..."

upvoted 1 times

xbololi 2 months, 3 weeks ago

"arbitrarily" yeah i use this word everyday... nice one cisco...

upvoted 2 times

Alizadeh 8 months, 3 weeks ago

Selected Answer: B

802.1x is a security standard that prevents client devices from arbitrarily connecting to the network without state remediation. It provides a framework for authenticating devices that are attempting to access a LAN or WLAN.

802.1x uses a supplicant (client device) and an authenticator (network access device) to establish a secure connection. The supplicant sends an authentication request to the authenticator, which then forwards the request to an authentication server. If the authentication server approves the request, the supplicant is allowed to access the network. If the request is denied, the supplicant is not allowed to access the network.

upvoted 4 times

ZUMY 1 year, 2 months ago

B is correct!
802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. The user's identity is determined based on their credentials or certificate, which is confirmed by the RADIUS server

upvoted 4 times

BlankNothing1 1 year, 3 months ago

The source link would be in the CCNA 200-301 OCG Volume 1. Page 658, 2nd paragraph, 2nd sentence. Start with page 657, the subject "802.1x/EAP" will give more information.

upvoted 4 times

SSESSE2021 1 year, 10 months ago

Any source link for this?

upvoted 1 times

laurvy36 1 year, 9 months ago

EEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN

upvoted 5 times

Question #252 *Topic 1*

Which protocol does an access point use to draw power from a connected switch?

A. Internet Group Management Protocol

B. Cisco Discovery Protocol

C. Adaptive Wireless Path Protocol

D. Neighbor Discovery Protocol

Correct Answer: *B*

Community vote distribution

B (100%)

CISCO2022 Highly Voted 2 years, 3 months ago

PoE switches support Cisco pre-standard PD detection mechanisms, and any Standards based compliant PDs. Most Cisco made PDs, pre-standard or standard, support Cisco Discovery Protocol (CDP). Once power is applied to a port that contains a pre-standard or standard Cisco PD, CDP is used in order to determine the actual power requirement, and the system power budget is adjusted accordingly.

upvoted 10 times

GreatDane Most Recent 1 month, 4 weeks ago

Selected Answer: B

Power Over Ethernet (PoE) - Cisco

"...
Device Detection and Power Allocation

The router will detect a Cisco Pre-standard or an IEEE-compliant PD (Powered Device) when the PoE is enabled and the connected device is not being powered by an AC adapter.
After device detection, the router will determine the power requirements based on power classification class.
Depending on the available power in the power budget, the router determines if a port can be powered. The router initially allocates this power when it detects and powers the device. Power negotiation using CDP/LLDP protocols happens thereafter. Supported protocols for power negotiation are CDP for Cisco PD, and LLDP for non-Cisco PDs.
..."

upvoted 2 times

ricky1802 7 months, 1 week ago

Selected Answer: B

CDP is used in output power negotiations for POE capable devices; like IP Phones, AccessPoints etc.
https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x

upvoted 1 times

ZUMY 1 year, 2 months ago

B is correct

upvoted 3 times

jossyda 1 year, 4 months ago

Selected Answer: B

CDP is correct

upvoted 1 times

Micah7 2 years, 3 months ago

B is correct:
https://blog.router-switch.com/2012/03/faq-power-over-ethernet-poe-power-requirements/

upvoted 4 times

Question #253 *Topic 1*

An administrator must secure the WLC from receiving spoofed association requests. Which steps must be taken to configure the WLC to restrict the requests and force the user to wait 10 ms to retry an association request?

A. Enable MAC filtering and set the SA Query timeout to 10.

B. Enable 802.1x Layer 2 security and set the Comeback timer to 10.

C. Enable Security Association Teardown Protection and set the SA Query timeout to 10.

D. Enable the Protected Management Frame service and set the Comeback timer to 10.

Correct Answer: *C*

Community vote distribution

D (75%) C (25%)

MrPOW Highly Voted 2 years, 2 months ago

Has to be D based on..

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212576-configure-802-11w-management-frame-prote.html#anc8

upvoted 14 times

SScott 2 years, 1 month ago

Yes D is the best answer with 802.11w PMF with protection and validation via secure hash to verify signed frames with MIC IE from a BSSID in the network. The secure pmf command is used together with the association-comeback time to configure a portion of this setup. In addition helps more with capwap debugging for Cisco proprietary CCX/MFP messages between controller, APs, and devices. This method is supported on the newer WLCs.

https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-wireless-access-points/smb5442-frequently-asked-questions-about-management-frame-protection.html#q3

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/802-11w.html.xml

upvoted 4 times

SScott 2 years, 1 month ago

A is not as effective with hardening the controller and AP association requests at an enterprise level
https://www.portnox.com/blog/network-security/the-truth-about-mac-spoofing/

B 802.1x is secure, encrypted and effective for client authentication especially with RADIUS config. However 802.1x/802.11x are not as specifically robust as the Protected Management Frame service mechanism and processes on WLC with 802.11w.

C while Security Association is an excellent added protection with Association Comeback, this answer is wrong as the SA Query retry value is between 100 to 500 ms
SA teardown protection is a mechanism to prevent replay attacks from tearing down the session of an existing client. It consists of an Association Comeback Time and an SA-Query procedure preventing spoofed association requests from disconnecting an already connected client.
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/802-11w.html.xml

upvoted 5 times

Stevens0103 Most Recent 3 weeks, 3 days ago

Selected Answer: C

SA teardown protection is a mechanism to prevent replay attacks from tearing down the session of an existing client. It consists of an Association Comeback Time and anSA-Query procedure preventing spoofed association requests from disconnecting an already connected client.

If a client has a valid security association, and has negotiated 802.11w, the APshall reject another Association Request with status code 30. This status code stands for "Association request rejected temporarily; Try again later". The APshould not tear down or otherwise modify the state of the existing association until theSA-Query procedure determines that the original SA is invalid and shall include in the Association Response an Association Comeback Time information element, specifying a comeback time when the AP would be ready to accept an association with this client.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/config-guide/b_wl_17_11_cg/802-11w.pdf

upvoted 1 times

Stevens0103 3 weeks, 3 days ago

I mean... D.

Step 1 Choose Configuration > Tags & Profiles > WLANs.
Step 2 Click Add to create WLANs.

The Add WLAN page is displayed.
Step 3 In the Security > Layer2 tab, navigate to the Protected Management Frame section.
Step 4 Choose PMF as Disabled, Optional, or Required. By default, the PMF is disabled.
If you choose PMF as Optional or Required, you get to view the following fields:
• Association Comeback Timer—Enter a value between 1 and 10 secondsto configure 802.11w association comeback time.
• SA Query Time—Enter a value between 100 to 500 (milliseconds). Thisisrequired for clientsto negotiate 802.11w PMF protection on a WLAN.
Step 5 Click Save & Apply to Device.

upvoted 1 times

GreatDane 1 month, 4 weeks ago

Selected Answer: D

Configure 802.11w Management Frame Protection on WLC - Cisco

"...
Benefits of 802.11w Management Frame Protection
...
AP Protection
...
Included in the Association Response is an Association Comeback Time information element which specifies a comeback time when the AP is ready to accept an association with this STA. This way you can ensure that legitimate clients are not disassociated due to a spoofed association request.
..."

upvoted 1 times

[Removed] 3 months ago

Selected Answer: D

Here is what Cisco says :

"You then need to specify the comeback timer and SA query timeout. The comeback timer specifies the time that an associated client must wait before the association can be tried again..."

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212576-configure-802-11w-management-frame-prote.html

upvoted 1 times

Vikramaditya_J 4 months, 1 week ago

Selected Answer: C

Security Association (SA) Teardown Protection is a mechanism in Cisco WLC that prevents replay attacks from tearing down the session of an existing client. It consists of an Association Comeback Time and an SA-Query procedure that prevents spoofed association requests from disconnecting an already connected client. Prior to the implementation of the 802.11w standard, if an AP received either an Association or Authentication request with a spoofed source address, it would tear down the existing association with the legitimate client. With SA Teardown Protection, the AP waits for a specified time before tearing down the existing association, allowing the legitimate client to re-associate with the AP.

upvoted 1 times

jnanofrancisco 8 months ago

I am not sure but i think C is correct. D is just a part of SA teardown

https://www.hitchhikersguidetolearning.com/2017/09/17/security-association-sa-teardown-protection-part-1/

upvoted 1 times

Mahfuj_01 9 months, 3 weeks ago

Answer is C.
Reference :
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.html

upvoted 1 times

splashy 10 months, 2 weeks ago

Selected Answer: D

I checked with my netacad instructor after reading this

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.html

association-comeback—Configures the 802.11w association. The range is from 1 through 20 seconds.

saquery-retry-time ... The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.

I think the questions should say 10 seconds, 10ms does not fall into either possible range.

So 10ms should not be possible. 10 seconds? --> comeback timer

upvoted 1 times

aizudin 11 months ago

Selected Answer: C

Infrastructure protection is added by adding a Security Association (SA) tear down protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

association-comeback—Configures the 802.11w association. The range is from 1 through 20 seconds.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.html

upvoted 1 times

PiotrMar 1 year ago

it is "C"
Security Association (SA) Teardown Protection SA teardown protection is a mechanism to prevent replay attacks from tearing down the session of an existing client. It consists of an Association Comeback Time and an SA-Query procedure preventing spoofed association requests from disconnecting an already connected client.

upvoted 2 times

GreatDane 1 year, 2 months ago

Ref: Configure 802.11w Management Frame Protection on WLC – Cisco

"...
Benefits of 802.11w Management Frame Protection
...
• AP Protection
...
When you use 802.11w MFP, if the STA is associated and has negotiated Management Frame Protection, the AP rejects the Association Request with return status code 30 Association request rejected temporarily; Try again later to the client.

Included in the Association Response is an Association Comeback Time information element which specifies a comeback time when the AP would be ready to accept an association with this STA. This way you can ensure that legitimate clients are not disassociated due to a spoofed association request.
..."

A. Enable MAC filtering and set the SA Query timeout to 10.

Wrong answer.

B. Enable 802.1x Layer 2 security and set the Comeback timer to 10.

Wrong answer.

C. Enable Security Association Teardown Protection and set the SA Query timeout to 10.

Wrong answer.

D. Enable the Protected Management Frame service and set the Comeback timer to 10.

Correct answer.

upvoted 2 times

ZUMY 1 year, 2 months ago

Selected Answer: D

Going with D:

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212576-configure-802-11w-management-frame-prote.html#anc8

upvoted 1 times

jossyda 1 year, 3 months ago

Selected Answer: D

Protected Management Frames (PMF) to secure important 802.11 management frames between APs and clients, to prevent malicious activity that might spoof or tamper with a BSS's operation.

upvoted 2 times

dipanjana1990 1 year, 5 months ago

D is the correct answer.
Since Protected management Frame doesn't let spoofed clents to associate with the access point wheras Security Association Teardown Protection tears down spoofed association as original assocaition already exist in the table with WLC.
Thus, D will be the correct answer

upvoted 1 times

awashenko 1 year, 8 months ago

Selected Answer: D

I also think D is correct

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212576-configure-802-11w-management-frame-prote.html

upvoted 1 times

daanderud 1 year, 8 months ago

Selected Answer: D

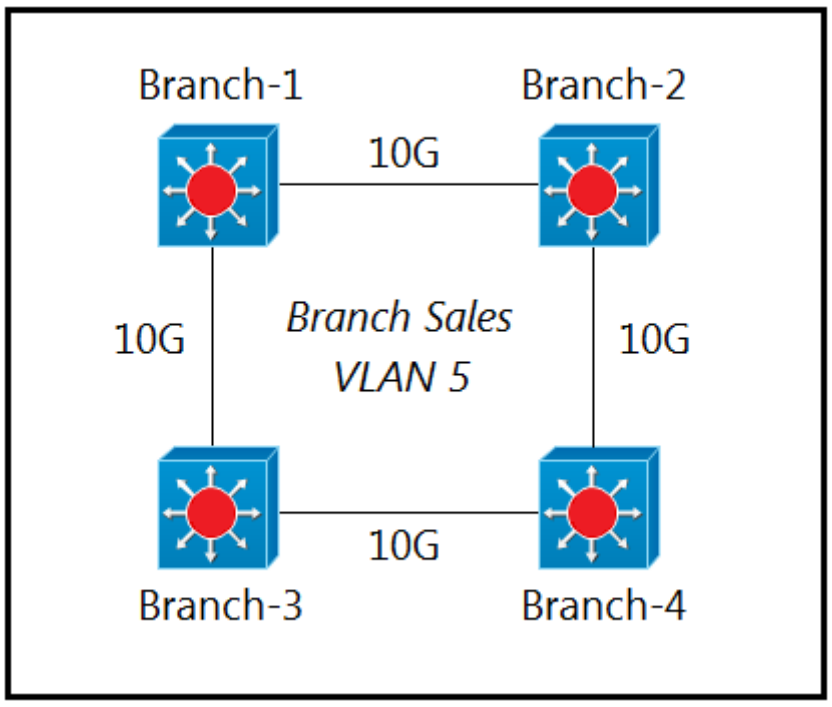
D is the correct answer

upvoted 1 times

Anarckii 1 year, 9 months ago

The answer should be D. The question ask about the association request, which involves the management of the WLC

upvoted 1 times



Refer to the exhibit. Only four switches are participating in the VLAN spanning-tree process.

Branch-1: priority 614440 -

Branch-2: priority 39391170 -

Branch-3: priority 0 -

Branch-4: root primary -

Which switch becomes the permanent root bridge for VLAN 5?

A. Branch-1

B. Branch-2

C. Branch-3

D. Branch-4

Correct Answer: *C*

Community vote distribution

C (100%)

LOST40 Highly Voted 1 year, 6 months ago

A priority 0 means that it guarantees the switch is always the root bridge of a particular VLAN. You don't need other information.

upvoted 14 times

Peter_panda Highly Voted 8 months, 2 weeks ago

I just verified with a C2960 and a C1111 - Priority 0 "beats" root primary, so the right answer is C indeed.

upvoted 7 times

mfaria Most Recent 1 month, 1 week ago

Selected Answer: C

Pri 0 beats primary

upvoted 1 times

kyleptt 1 month, 2 weeks ago

Ok I tested it the Pri 0 commands wins the race over the root primary command I was wrong but know I know

upvoted 1 times

kyleptt 1 month, 2 weeks ago

D is correct the Root Primary wins the race

upvoted 1 times

zFlyingLotusz 2 months ago

Welp, this question does not have enough context.
Root primary DOES INDEED supersede priority 0, HOWEVER, if the switch with priority 0 has a lower mac address, it will supersede Root Primary...
Poorly written question.

upvoted 1 times

GigaGremlin 11 months, 2 weeks ago

Correct answer is D, because of the manually configured Root Primary of Branch-4. As long it is well and alive Priority 0 doesn't matter. Guess in Cases like this Root Backup would be manually selected to, to prevent unexpected Root election results...

upvoted 1 times

DoBronx 10 months, 3 weeks ago

wrong. Priority 0 supersedes that

upvoted 6 times

GreatDane 1 year, 2 months ago

Ref: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

"Advanced STP Tuning
...
Root Bridge Placement

Ideally the root bridge is placed on a core switch, and a secondary root bridge is designated to minimize changes to the overall spanning tree. Root bridge placement is accomplished by lowering the system priority on the root bridge to the lowest value possible, raising the secondary root bridge to a value slightly higher than that of the root bridge, and (ideally) increasing the system priority on all other switches. This ensures consistent placement of the root bridge.
..."

A. Branch-1

Wrong answer.

B. Branch-2

Wrong answer.

C. Branch-3

Correct answer.

D. Branch-4

Wrong answer.

upvoted 2 times

ZUMY 1 year, 2 months ago

C is correct!

upvoted 1 times

ZUMY 1 year, 2 months ago

-Each switch has its own bridge ID and has a default priority value of 32768
-using the 'root primary' will set the bridge priority to 24576, which is lower than the default priority.

upvoted 3 times

bmatthee01 1 year, 6 months ago

In this case the best answer is D
To ensure the desired switch becomes the permanent root bridge for a specific vlan (in this scenario Vlan5) you must explicitly configure it as the primary
https://www.omnisecu.com/cisco-certified-network-associate-ccna/how-to-configure-spanning-tree-protocol-root-primary-and-root-secondary.php

think about it
if you configure the switch with bridge priority 0 and connect another switch with bridge priority 0 and a lower mac address the root bridge will give up its position and change the topology

wheres a switch with the primary role wont give up its position even if a switch with priority 0 and lower mac address is connected

upvoted 2 times

sgashashf 1 year, 6 months ago

But that's now how any of this works. Executing the command "spanning-tree vlan 5 root primary" doesn't place a "primary" tag into the running config, it simply checks the priorities of other switches on the networks and sets its own to 4096 lower. Kane002 is correct, without more information there is literally no way to know which of these switches would be elected root bridge.

upvoted 2 times

JackBond40 1 year, 7 months ago

I believe there is enough information. Branch 1 has lower priority then Branch 2 so it would become primary between those 2. If election was between Branch 1 and Branch 4 Branch 4 would lower value by 4096 and become primary...then Branch 3 would take primary as it has priority 0. If election was between branch 3 and Branch 1 first Branch 3 would take primary with priority 0. Since Branch 3 is already primary with a priority 0 it will not relinquish primary to Branch 4. Branch 4 will set its priority to 0 but Branch 3 will remain primary while it is active in the STP process.

upvoted 1 times

johntan1980 1 year, 8 months ago

Priority 0

upvoted 1 times

Kane002 1 year, 8 months ago

Not enough information to answer. Both root primary and priority 0 will have a priority of 0, and go down to the lowest MAC address. Root primary will also generate SNMP complaints that it can't set it's priority to negative 4096, as primary always sets to 4096 below the lowest priority. Best answer is root primary.

upvoted 2 times

SScott 2 years, 1 month ago

Yeah C

upvoted 2 times

Question #255 *Topic 1*

An engineer must configure traffic for a VLAN that is untagged by the switch as it crosses a trunk link. Which command should be used?

A. switchport trunk encapsulation dot1q

B. switchport trunk allowed vlan 10

C. switchport mode trunk

D. switchport trunk native vlan 10

Correct Answer: *D*

Community vote distribution

D (100%)

mfaria 1 month, 1 week ago

Selected Answer: D

Unttagged usualy asks for Native

upvoted 2 times

GreatDane 1 month, 3 weeks ago

Selected Answer: D

"untagged by the switch" refers to the traffic that "crosses a trunk link". And the only traffic that crosses a trunk link remaining UNTAGGED is NATIVE VLAN traffic:

Ref: VLAN Configuration Guide, Cisco IOS Release 15.2(7)Ex (Catalyst 1000 Switches) - Configuring VLAN Trunks [Support] - Cisco

"...
Configuring the Native VLAN for Untagged Traffic
...
Procedure

(steps 1 through 5)

enable
configure terminal
interface gigabitethernet 1/0/2 (or interface fastethernet 1/0/2)
switchport trunk native vlan 12
end
..."

upvoted 1 times

Bhrino 4 months ago

In most cases if the question ask for untagged data most of the time the answer is native vlan

upvoted 1 times

MoctarS 6 months, 1 week ago

Selected Answer: D

Best answer is D .

upvoted 2 times

sasquatchshrimp 1 year, 1 month ago

Cisco is getting tipsy when making these questions. What do they mean you need to configure traffic?

upvoted 4 times

ZUMY 1 year, 2 months ago

D is correct

upvoted 1 times

Rob2000 1 year, 11 months ago

D
The switchport trunk native vlan command specifies the native (untagged) VLAN for a Layer 2 interface operating in trunk mode on a Cisco IOS device. This command only takes effect for interfaces that are operating in trunk mode.

upvoted 3 times

dave1992 1 year, 11 months ago

huh?
how do you configure traffic? if youre marking traffic wouldnt you mark it with the command encap dot1q?

upvoted 1 times

lade12 1 year, 10 months ago

untagged traffic goes through the native vlan

upvoted 3 times

Question #256 *Topic 1*

What are two benefits of using the PortFast feature? (Choose two.)

A. Enabled interfaces are automatically placed in listening state.

B. Enabled interfaces wait 50 seconds before they move to the forwarding state.

C. Enabled interfaces never generate topology change notifications.

D. Enabled interfaces come up and move to the forwarding state immediately.

E. Enabled interfaces that move to the learning state generate switch topology change notifications.

Correct Answer: *AD*

Community vote distribution

CD (97%)

vannplus11 Highly Voted 1 year, 12 months ago

• Interfaces with portfast enabled that come up will go to forwarding mode immediately, the interface will skip the listening and learning state.

• A switch will never generate a topology change notification for an interface that has portfast enabled.

https://networklessons.com/switching/cisco-portfast-configuration

upvoted 25 times

checkoboy88 Highly Voted 6 months, 2 weeks ago

Selected Answer: CD

C&D are correct for sure :)

upvoted 6 times

Kene01 Most Recent 1 month, 1 week ago

Selected Answer: CD

This link explains it better
https://networklessons.com/switching/cisco-portfast-configuration#:~:text=Portfast%20does%20two%20things%20for%20us%3A%201%20,notification%20for%20an%20interface%20that%20has%20portfast%20enabled.

upvoted 1 times

mfaria 1 month, 1 week ago

Selected Answer: AD

Makes the STP process faster.

upvoted 1 times

GreatDane 1 month, 3 weeks ago

Selected Answer: CD

Cisco Learning Network > CCNA Certification Community: portfast

Post by Elvin Arias Soto

"The Portfast feature is used on access ports to bypass the listening and learning states of STP, meaning that a port shoud inmediately go to forwarding state, note that a Portfast enabled port also do not generate Topology Change Notifications (TCNs).

The reason why the port is not going to forwarding is becuase Portfast has two variants, one for access ports and one for trunks. In order to enable Portfast on trunk ports you should enter the "spanning-tree portfast trunk" command on interface mode.
..."

upvoted 1 times

Jorro99404 4 months ago

Selected Answer: CD

C and D

upvoted 2 times

Tarek70 4 months, 2 weeks ago

C and D

upvoted 2 times

Ciscoman021 8 months, 1 week ago

Selected Answer: CD

Portfast does two things for us: Interfaces with portfast enabled that come up will go to forwarding mode immediately, the interface will skip the listening and learning state. A switch will never generate a topology change notification for an interface that has portfast enabled.

https://networklessons.com/switching/cisco-portfast-configuration
upvoted 2 times

mzu_sk8 10 months, 2 weeks ago

Selected Answer: CD

"A switch will never generate a topology change notification for an interface that has portfast enabled."
upvoted 3 times

DoBronx 10 months, 3 weeks ago

this is just an obvious mistake
CD
upvoted 2 times

DUMPledore 11 months, 2 weeks ago

Selected Answer: CD

@EXAMTOPICS - pls change answer to CD
upvoted 4 times

creaguy 11 months, 2 weeks ago

Selected Answer: CD

A is wrong.

https://networklessons.com/switching/cisco-portfast-configuration#:~:text=Portfast%20does%20two,has%20portfast%20enabled.
upvoted 1 times

J1983 11 months, 3 weeks ago

"A switch will never generate a topology change notification for an interface that has portfast enabled." Source: https://networklessons.com/switching/cisco-portfast-configuration

"Another major benefit of the STP portfast feature is that the access ports bypass the earlier 802.1D STP states (learning and listening) and forward traffic immediately."
Source: https://www.ciscopress.com/articles/article.asp?p=2995351&seqNum=3
upvoted 2 times

TMT91 12 months ago

Selected Answer: CD

C&D is the correct answer
upvoted 2 times

shubhambala 1 year ago

Selected Answer: CD

CD is the anwers pals (source - Trust me please!)
upvoted 2 times

splashy 1 year ago

Selected Answer: CD

A&D contradict each other so please change the answer :)

It's C&D

You DON'T want access/edge ports LISTENING or LEARNING anything (spanning tree related) from (potentially malicious) end devices = So you enable Portfast
You can then also enable BPDU guard to detect BPDU's, which when received on an access/edge port is malicious activity or user error. BPDU guard will then put the port in err-disabled state.

Implementing these two functions is access-port hardening.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html#wp1046787
upvoted 2 times

Cracked76 1 year ago

Selected Answer: CD

Port fast = forwarding state
upvoted 1 times

Question #257 *Topic 1*

What is the benefit of configuring PortFast on an interface?

A. The frames entering the interface are marked with the higher priority and then processed faster by a switch.

B. After the cable is connected, the interface is available faster to send and receive user data.

C. Real-time voice and video frames entering the interface are processed faster.

D. After the cable is connected, the interface uses the fastest speed setting available for that cable type.

Correct Answer: *B*

Community vote distribution

B (100%)

Stonetales987 Highly Voted 1 year, 10 months ago

B is correct - Portfast causes a switch or trunk port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states.

upvoted 8 times

GreatDane Most Recent 1 month, 3 weeks ago

Selected Answer: B

Solved: When to enable Portfast? - Cisco Community

Post by bjw

"Portfast is designed for access ports where you never expect to see BPDU packets. Portfast shortens/bypasses normal STP timers to get ports up and forwarding as quickly as practical. This typically is a host PC/Workstation.
..."

upvoted 1 times

DUMPledore 11 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

ZUMY 1 year, 2 months ago

B is correct

upvoted 1 times

Nicocisco 1 year, 7 months ago

Selected Answer: B

Comme le port prend va à l'état "forwading" directement, l'interface est effectivement prête à processer de la donnée plus vite

upvoted 4 times

studying_1 4 months, 1 week ago

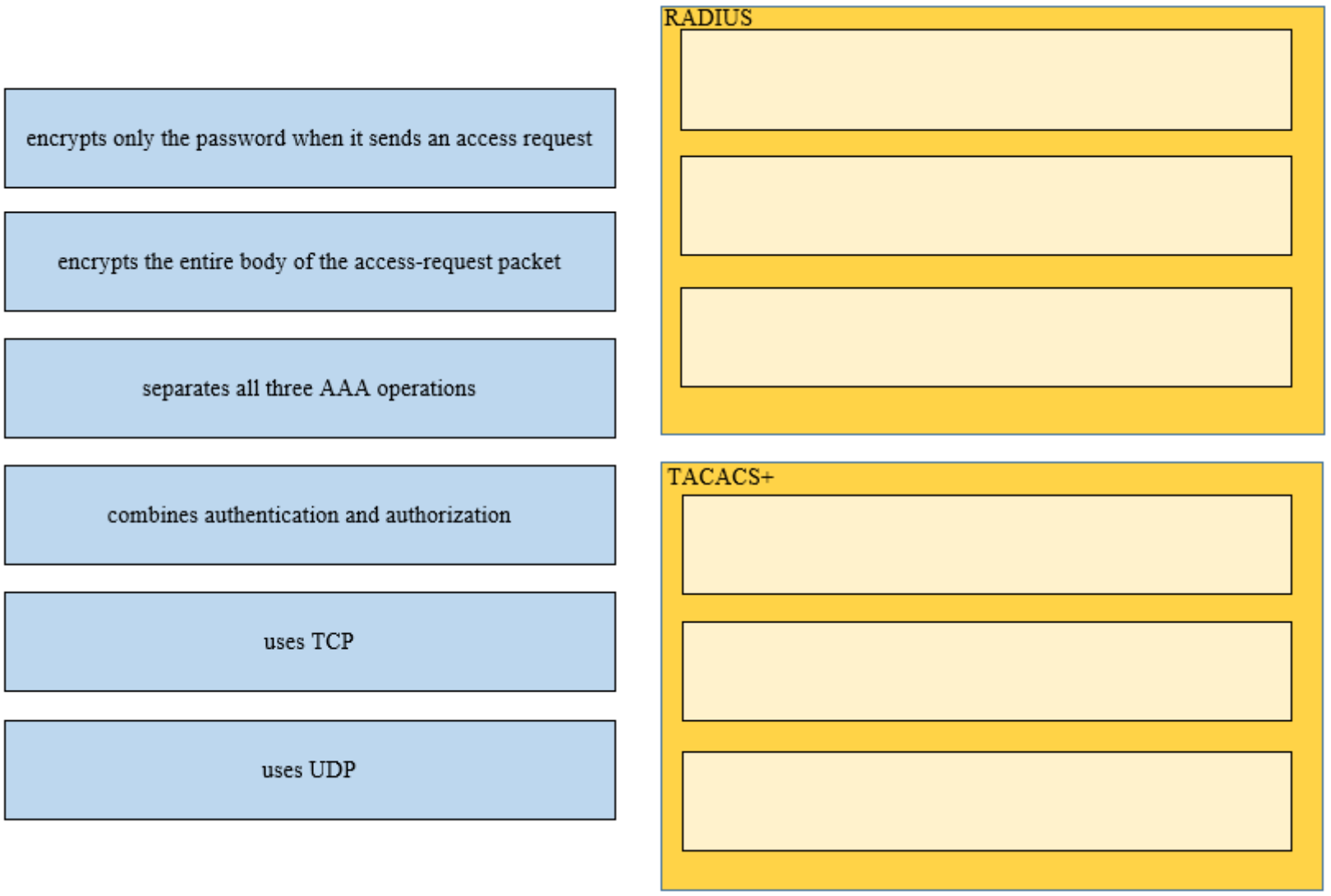
tout a fait d'accord avec toi, c'est vrai

upvoted 1 times

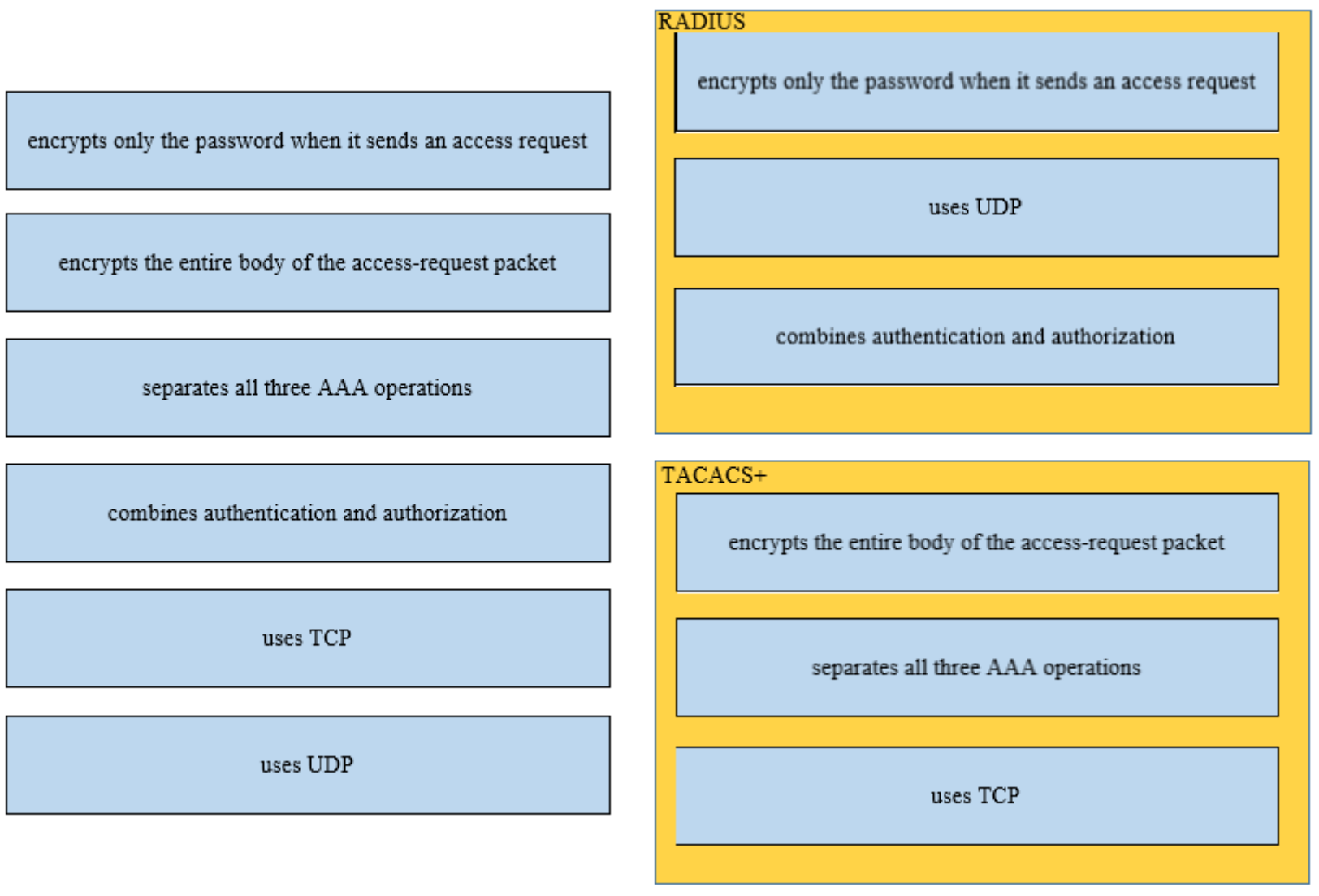
DRAG DROP -

Drag and drop the functions of AAA supporting protocols from the left onto the protocols on the right.

Select and Place:



Correct Answer:



GreatDane 1 month, 3 weeks ago

Compare TACACS + and RADIUS - Cisco

"...
Compare TACACS+ and RADIUS
These sections compare several features of TACACS+ and RADIUS.

UDP and TCP
RADIUS uses UDP while TACACS+ uses TCP.
...
Packet Encryption
RADIUS encrypts only the password in the access-request packet, from the client to the server...TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.
...
Authentication and Authorization
RADIUS combines authentication and authorization...TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting.
..."

upvoted 1 times

no_blink404 2 months, 3 weeks ago

Provided answer is correct :)

upvoted 2 times

ricky1802 7 months, 1 week ago

Answer is correct.
RADIUS uses UDP while TACACS+ uses TCP.
RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party.
TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.
RADIUS combines authentication and authorization.
TACACS+ uses the AAA architecture, which separates AAA.

upvoted 4 times

Question #259 *Topic 1*

Why does a switch flood a frame to all ports?

A. The frame has zero destination MAC addresses.

B. The destination MAC address of the frame is unknown.

C. The source MAC address of the frame is unknown

D. The source and destination MAC addresses of the frame are the same.

Correct Answer: *B*

Community vote distribution

B (94%) 4%

Fuaad Highly Voted 2 years ago

B is the correct answer
please update it
upvoted 37 times

Da_Costa Most Recent 1 month, 1 week ago

Selected Answer: B

The destination is unknown
upvoted 1 times

mfaria 1 month, 1 week ago

Selected Answer: B

Switch flooding is done to fill the CAM table and find out if the destination MAC is available.
It is sent to all ports except the source one.
upvoted 1 times

GreatDane 1 month, 3 weeks ago

Selected Answer: B

Flooding vs Broadcast - Cisco Community

Post by Kristian Alexander Brown
"...
Flooding is sometimes known as an unknown unicast. This happens when a switch receives a frame with a destination mac address it does not have in the CAM table. It will flood it out all ports except the receiving port of the frame.
..."
upvoted 1 times

perri88 3 months ago

Selected Answer: B

B is correct
upvoted 1 times

HSong 4 months, 4 weeks ago

D is the answer, if the destination MAC is unknown, the frame will be sent to all the port except the original one, but not ALL THE PORTS.
upvoted 2 times

jaypzz 9 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

R_AZZ23 1 year, 1 month ago

B is the correct answer .
upvoted 2 times

ZUMY 1 year, 2 months ago

Selected Answer: B

B is correct
upvoted 2 times

Shirona 1 year, 2 months ago

B is Correct.
upvoted 1 times

sakisg 1 year, 3 months ago

Selected Answer: B

b is correct

upvoted 1 times

Djow 1 year, 3 months ago

Selected Answer: D

D is the correct answer.
if the source MAC is know, the sw will send trafic to all ports, except the source port...

upvoted 2 times

Weezyfbaby 1 year, 3 months ago

Selected Answer: B

Because CCNA

upvoted 3 times

abual3ees 1 year, 4 months ago

Selected Answer: B

b correct

upvoted 1 times

Sajowww 1 year, 4 months ago

Selected Answer: B

Source MAC is known, only destination MAC is unknown

upvoted 1 times

battery1979 1 year, 2 months ago

Question asked what happens if both source and destination are unknown, but no clue how a switch ends up with a frame with an unknown source.

upvoted 1 times

dfvanloon 1 year, 4 months ago

B is the correct answer can you update the answer.

upvoted 2 times

ScorpionNet 1 year, 4 months ago

B is correct because it happens during an ARP request for IPv4 and ICMPv6 ND for IPv6 because the Switch doesn't know what network had the MAC Address assigned yet

upvoted 2 times

An engineer configures interface Gi1/0 on the company PE router to connect to an ISP. Neighbor discovery is disabled.

```
interface Gi1/0
description HQ_DC3992-38488
duplex full
speed 100
negotiation auto
lldp transmit
lldp receive
```

Which action is necessary to complete the configuration if the ISP uses third-party network devices?

A. Disable autonegotiation.

B. Enable LLDP globally.

C. Enable LLDP-MED on the ISP device.

D. Disable Cisco Discovery Protocol on the interface.

Correct Answer: *B*

Community vote distribution

B (100%)

mechelleh Highly Voted 1 year, 5 months ago

such a dumb question...

upvoted 17 times

CCNA_beast_69 Highly Voted 1 year, 9 months ago

It is correct. Big brain CCNA stuff right here lads.

upvoted 7 times

GreatDane Most Recent 1 month, 3 weeks ago

Selected Answer: B

Configure Link Layer Discovery Protocol (LLDP) Port Settings on a Switch through the Command Line Interface (CLI) - Cisco

"...
Disable LLDP on the Interface

LLDP is disabled globally on the switch and on all supported interfaces. You must enable LLDP globally to allow a device to send LLDP packets. Once enabled, no changes are required at the interface level.
..."

upvoted 1 times

oatmealturkey 6 months, 3 weeks ago

I am so annoyed with Odom for claiming in OCG that you can have LLDP globally disabled and just configure LLDP on an interface, and then that interface will transmit and/or receive LLDP messages while LLDP is globally disabled on the device. Did anyone else notice that?!

upvoted 3 times

Pokoyo 1 year, 2 months ago

Answer B
LLDP-MED TLV support is enabled by default if LLDP is enabled globally and locally on a supported interface. Specific TLVs, however, can be enabled and suppressed.

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/cether/configuration/15-mt/ce-15-mt-book/ce-lldp-multivend.html.xml

upvoted 2 times

asbaleha 1 year, 1 month ago

lldp transmit and lldp receive are active in the running-config thats mean the lldp is already active ? , and if its already active we need to disable cdp correct if am wrong and thx

upvoted 1 times

ZUMY 1 year, 2 months ago

B is correct
Link Layer Discovery Protocol (LLDP) is a layer 2 neighbor discovery protocol that allows devices to advertise device information to their directly connected peers/neighbors. It is best practice to enable LLDP globally to standardize network topology across all devices if you have a multi-vendor network.

upvoted 4 times

LeonardM 1 year, 5 months ago

B 100% CORRECT

upvoted 1 times

SollyMalwane 1 year, 7 months ago

Selected Answer: B

CORRECT

upvoted 1 times

reagan_donald 1 year, 7 months ago

Neither in Wendell nor on Netacad was mentioned LLDP-MED

upvoted 2 times

EDUROJAS 1 year, 7 months ago

it c
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/cether/configuration/15-mt/ce-15-mt-book/ce-lldp-multivend.html.xml

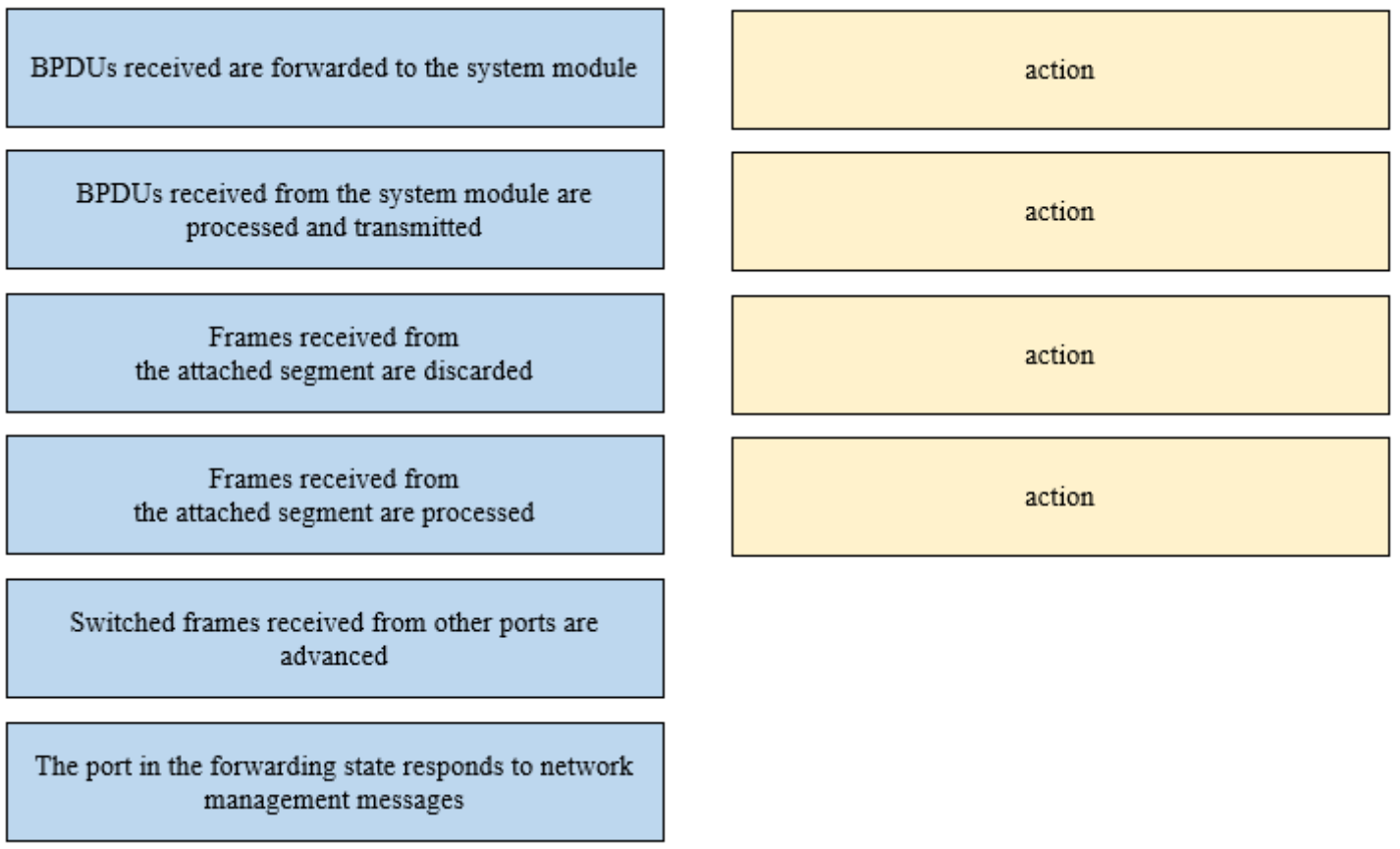
upvoted 1 times

Question #261 *Topic 1*

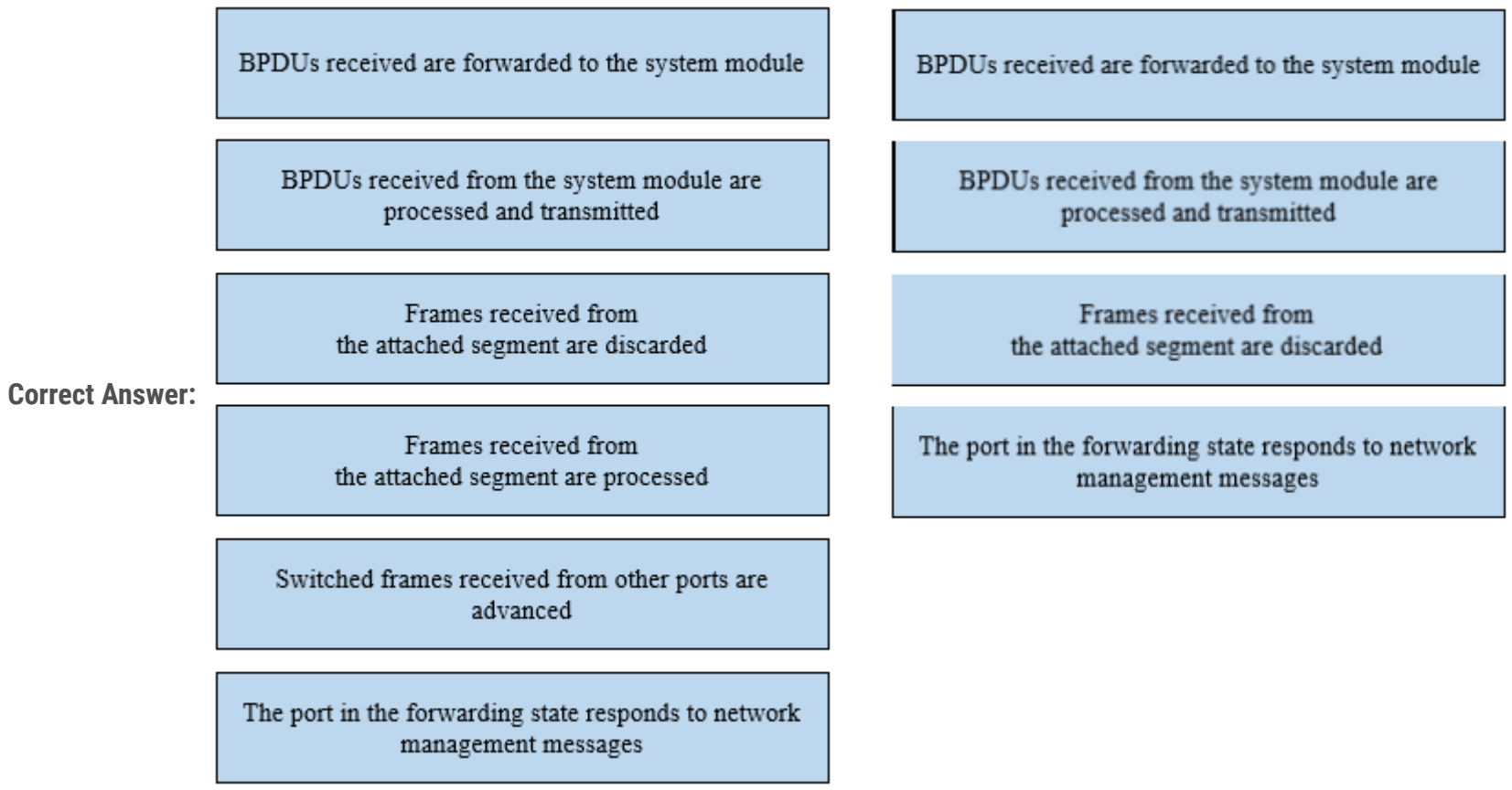
DRAG DROP -

Drag and drop the Rapid PVST+ forwarding state actions from the left to the right. Not all actions are used.

Select and Place:



Correct Answer:



ccna_goat Highly Voted 11 months, 3 weeks ago

system module, attached segment? another broken question.

upvoted 16 times

splashy Highly Voted 11 months, 3 weeks ago

BPDU'S received forwarded to system module
BPDU'S received from system module are processed and transmitted
Switched frames from other ports are advanced
The port in the forwarding state responds to netwrok management messages

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html#con_1241832

upvoted 14 times

dropspablo 1 month, 3 weeks ago

Processes BPDUs received from the system module. """But it doesn't transmit""".
Answer correct:
1- BPDUs received are forwarded to the system module.
4- Frames received from attached segment are processed.

5- Switched frames from other ports are advanced.
6- Port in the forwarding state responds to network mngmt messages.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html#con_1241832

upvoted 1 times

VictorCisco 5 months ago

Do not mess the guys studying !
there is no "Switched frames from other ports are advanced"!!

upvoted 3 times

GreatDane Most Recent 1 month, 3 weeks ago

Configuring Rapid PVST+ - Cisco

"...
Port States
...
Forwarding State

A LAN port in the forwarding state forwards frames. The LAN port enters the forwarding state from the learning state.

A LAN port in the forwarding state performs as follows:

Forwards frames received from the attached segment.
Forwards frames switched from another port for forwarding.
Incorporates the end station location information into its address database.
Receives BPDUs and directs them to the system module.
Processes BPDUs received from the system module.
Receives and responds to network management messages.
..."

upvoted 1 times

bisiyemo1 5 months, 1 week ago

A LAN port in the forwarding state performs as follows:

Forwards frames received from the attached segment.

Forwards frames switched from another port for forwarding.

Incorporates the end station location information into its address database.

Receives BPDUs and directs them to the system module.

Processes BPDUs received from the system module.

Receives and responds to network management messages.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html#con_1241832

upvoted 2 times

guisam 9 months, 1 week ago

A port in the forwarding state performs as follows:
•Forwards frames that are received from the attached segment
•Forwards frames that are switched from another port for forwarding
•Incorporates station location information into its address database
•Receives BPDUs and directs them to the system module
•Processes BPDUs that are received from the system module
•Receives and responds to network management messages

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/spantree.html#wp1174176

upvoted 5 times

binrayelias 8 months ago

Switched frames from other ports are advanced.
BPDUs received are forwarded to the sys module.
Frames received from attached segment are processed.
Port in the forwarding state responds to network mngmt messages.

upvoted 5 times

dick3311 10 months, 3 weeks ago

https://www.examtopics.com/discussions/cisco/view/61948-exam-200-301-topic-1-question-182-discussion/

upvoted 6 times

Question #262 *Topic 1*

Which access point mode relies on a centralized controller for management, roaming, and SSID configuration?

A. lightweight mode

B. autonomous mode

C. bridge mode

D. repeater mode

Correct Answer: *A*

Rether16 5 months, 1 week ago

In the words of Ronnie Coleman: Lightweight Baby!!!

upvoted 4 times

Kansen 1 year, 1 month ago

Can someone explain shortly the difference between Autonomous and Lightweight mode?

upvoted 2 times

Customexit 10 months, 3 weeks ago

Autonomous Access Points (APs) are self-contained that do not rely on a Wireless LAN Controller (WLC), they are configured individually. There is no central monitoring or management of APs,.

For Lightweight APs, the functions of an AP can be split between the AP and the WLC. Other functions are carried out by a WLC. The WLC is also sued to centrally configure the lightweight APs. Can be configured in modes such as Local or FlexConnect.

Extra info because I've seen it mentioned in other questions here:

WLC and lightweight APs use a protocol called CAPWAP (Control And Provisioning Of Wireless Access Points) to communicate. This is based of an older protocol, LWAPP (Lightweight Access Point Protocol).
Two tunnels are created between each AP and WLC: Control Tunnel (manage operations) and Data Tunnel (traffic from wireless clients is sent through this tunnel to the WLC, it does not go direct to the wired network. Traffic here is not encrypted by default).

upvoted 12 times

Godfather2022 7 months, 3 weeks ago

You completely right I have seen questions about the meaning of CAPWAP.

upvoted 1 times

ZUMY 1 year, 2 months ago

A is correct

upvoted 1 times

hassanhhady 1 year, 7 months ago

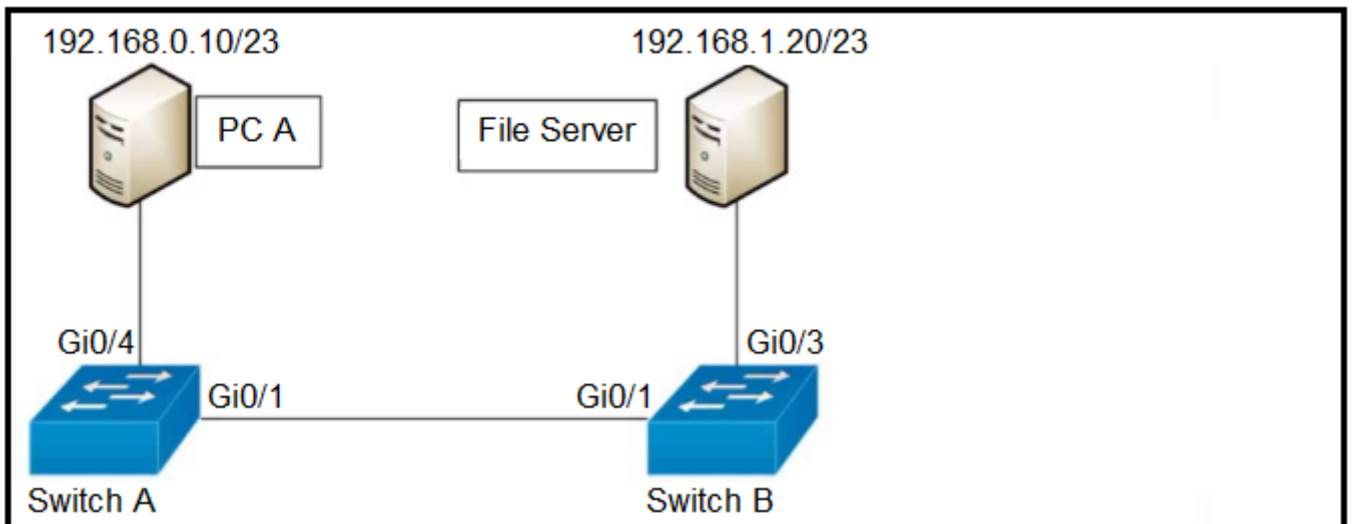
i didn't understand the question!

upvoted 2 times

PraygeForPass 1 year, 4 months ago

Lightweight AP deployment requires a centralized controller to operate, a.k.a. a WLC.
A is correct

upvoted 3 times



Switch A Vlan 10, 11, 12, 13	Switch B Vlan 10, 11, 12, 13
interface GigabitEthernet0/1 switchport mode trunk switchport trunk allowed vlan 10-12 ! interface GigabitEthernet0/4 switchport access vlan 13 switchport mode access	interface GigabitEthernet0/1 switchport mode trunk ! interface GigabitEthernet0/3 switchport access vlan 13 switchport mode access

Refer to the exhibit. A network engineer must configure communication between PC A and the File Server. To prevent interruption for any other communications, which command must be configured?

A. switchport truck allowed vlan 12

B. switchport truck allowed vlan none

C. switchport truck allowed vlan add 13

D. switchport truck allowed vlan remove 10-11

Correct Answer: *C*

Community vote distribution

C (100%)

ctoklu Highly Voted 1 year, 2 months ago

switchport TRUCK?? --> TRUNK

upvoted 11 times

Yunus_Empire 9 months, 1 week ago

Huahaha i was thinking the same what is Truck its Trunk LoL

upvoted 2 times

Aleks123 Highly Voted 1 year, 8 months ago

The switchport trunk allowed vlan command is used to specify the list of VLANs that are allowed on a trunk port. When a Layer 2 interface on a Cisco IOS device is configured to operate in trunk mode, the default setting is for the interface to carry all of the VLANs defined on the switch.

upvoted 10 times

kyleptt Most Recent 1 month, 2 weeks ago

I'm looking for the Router in this network but adding VLAN 13 on switch 1 will be the answer

upvoted 1 times

GreatDane 1 month, 2 weeks ago

Selected Answer: C

When configuring a switch interface as a trunk, unless you use the "switchport trunk allowed vlan" syntax, ALL VLANS are allowed to pass through the trunk.
And this happened on Switch B, interface Gi0/1.

On Switch A, interface Gi0/1 was configured to allow VLANs 10 to 12 through. But PC A (on Gi0/4) is inside VLAN 13. Then, you need to add VLAN 13 to allowed VLANs through interface Gi0/1.

And the syntax is:

interface GigabitEthernet0/1
switchport trunk allowed vlan add 13

upvoted 1 times

R4mzes 3 months ago

Adding Vlan 13 wont change anything as PC and Srv are in different Vlan. Correct is B, if you dissable allowed vlans. All Vlans will be allowed on the Trunk.

upvoted 2 times

perri88 3 months ago

that's not how to disable allowed vlan. to disable those vlan you have to use "no switchport trunk allowed vlan 10-12". if you use switchport allowed vlan none, means that none VLAN will be allowed. not even 13

upvoted 1 times

GigaGremlin 11 months, 2 weeks ago

If this Question really is about to add VLAN 13, you have do add it on A & B. Otherwise both devices seem to be not necessarily within VLAN 13 and maybe should just use the nativ VLAN to communicate ?!

upvoted 1 times

usamahrakib001 1 year, 1 month ago

If you need to add any more VLAN's to the already allowed list you need to use the add command otherwise you will override what is in there already.

upvoted 2 times

znabbe 1 year, 4 months ago

They can't communicate either way since they are in different subnets or am I wrong? I thought you needed a router to communicate between subnets.

upvoted 4 times

ciscodj 1 year, 3 months ago

They are on the same subnet.

upvoted 4 times

dipanjana1990 1 year, 1 month ago

they are on the same subnet.

upvoted 2 times

jiri_kurka 1 year, 5 months ago

Selected Answer: C

I'm not sure if command "switchport TRUCK allowed vlan add 13" helps.... anyway it seems be correct :-D

upvoted 3 times

bhurishravas 1 year, 8 months ago

Selected Answer: C

so just add absent vlan ID

upvoted 4 times

Cho1571 1 year, 8 months ago

Looks like Switch B is missing the Switchport trunk allowed VLAN command....lol

upvoted 1 times

```
switch(config)#interface gigabitEthernet 1/11
switch(config-if)#switchport mode access
switch(config-if)#spanning-tree portfast
switch(config-if)#spanning-tree bpduguard enable
```

Refer to the exhibit. What is the result if Gig1/11 receives an STP BPDU?

A. The port transitions to STP blocking.

B. The port immediately transitions to STP forwarding.

C. The port goes into error-disable state.

D. The port transitions to the root port.

Correct Answer: *C*

Community vote distribution

C (100%)

ZUMY Highly Voted 1 year, 2 months ago

C:
BPDU Guard feature protects the port from receiving STP BPDUs, however the port can transmit STP BPDUs. When a STP BPDU is received on a BPDU Guard enabled port, the port is shutdown and the state of the port changes to ErrDis (Error-Disable) state.

upvoted 7 times

ZUMY 1 year, 2 months ago

BPDU guard is enabled only on access ports where laptops, servers or other device are connected. If some one generate PBDU's from end devices PBDU guard will put the port in to erro-disable state

upvoted 8 times

GreatDane Most Recent 1 month, 2 weeks ago

Selected Answer: C

Ref: What is BPDU Guard and How to Configure BPDU Guard? - GeeksforGeeks

"...
BPDU Guard

BPDU Guard is a feature that defends the Layer 2 Spanning Tree Protocol (STP) topology against BPDU-related threats and is designed to protect the switching network. The BPDU guard feature must be activated on ports that should not receive BPDUs from connected devices.
...
In Global configuration mode, the BPDU Guard feature can be enabled globally, or per interface in Interface configuration mode. The port gets disabled and the port status is set to Errdisable (same as shutdown status) whenever a BPDU Guard enabled port gets a BPDU from the linked device.
...."

upvoted 1 times

binrayelias 8 months ago

hen the interface receives a BPDU, it is put in the error-disabled state

upvoted 1 times

lpham 1 year, 3 months ago

C is correct.

"Spanning tree shuts down STP ports that are in a Port Fast-operational state if any BPDU is received on those ports. In a valid configuration, Port Fast-enabled STP ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the interface in the error-disabled state."

https://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/trash/swstpopt.html#wp1095752

upvoted 2 times

amadeu 1 year, 8 months ago

C , is the correct.

upvoted 1 times

Question #265 *Topic 1*

Which access layer threat-mitigation technique provides security based on identity?

A. Dynamic ARP Inspection

B. DHCP snooping

C. 802.1x

D. using a non-default native VLAN

Correct Answer: *C*

Community vote distribution

C (100%)

GreatDane 1 month, 2 weeks ago

Selected Answer: C

Security Configuration Guide, Cisco IOS XE Amsterdam 17.1.x (Catalyst 9300 Switches) - Configuring IEEE 802.1x Port-Based Authentication [Support] – Cisco

C H A P T E R 25
Configuring IEEE 802.1x Port-Based Authentication

"...
Port-Based Authentication Process

To configure IEEE 802.1X port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

The AAA process begins with authentication. When 802.1x port-based authentication is enabled and the client supports 802.1x-compliant client software, these events occur:

- If the client identity is valid and the 802.1x authentication succeeds, the switch grants the client access to the network.
..."

upvoted 1 times

ZUMY 1 year, 2 months ago

C: answer

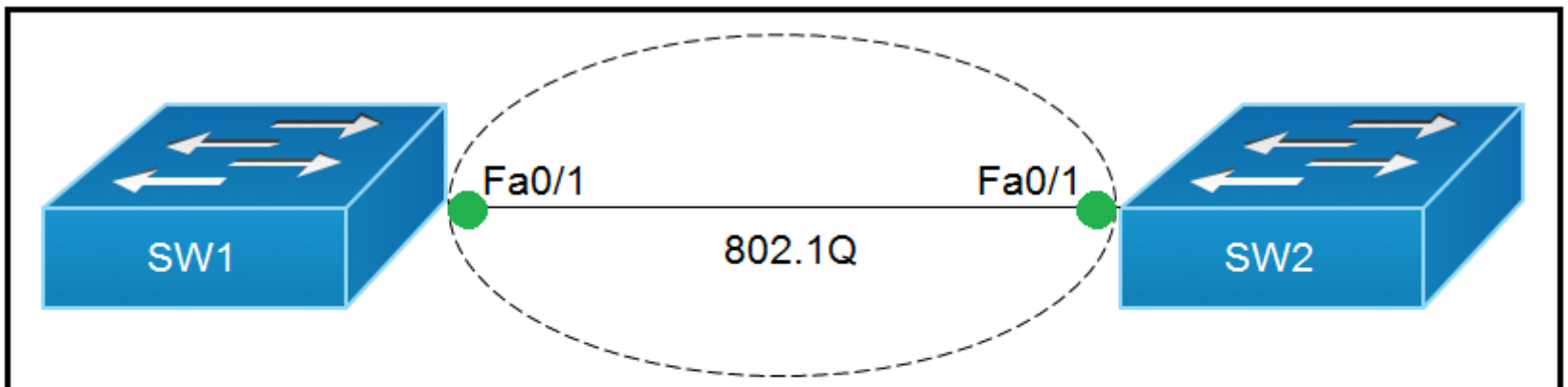
upvoted 3 times

SparkySM 1 year, 8 months ago

https://alexwilkins.dev/index.php/1-7-describe-common-access-layer-threat-mitigation-techniques/

upvoted 3 times

Question #266 *Topic 1*



SW1:
```
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
```

SW2:
```
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport mode trunk
```

Refer to the exhibit. Which action do the switches take on the trunk link?

A. The trunk does not form, and the ports go into an err-disabled status.

B. The trunk forms, but the mismatched native VLANs are merged into a single broadcast domain.

C. The trunk forms, but VLAN 99 and VLAN 999 are in a shutdown state.

D. The trunk does not form, but VLAN 99 and VLAN 999 are allowed to traverse the link.

Correct Answer: *B*

The trunk still forms with mismatched native VLANs and the traffic can actually flow between mismatched switches. But it is absolutely necessary that the native
VLANs on both ends of a trunk link match; otherwise a native VLAN mismatch occurs, causing the two VLANs to effectively merge. For example, with the above configuration, SW1 would send untagged frames for VLAN 999. SW2 receives them but would think they are for VLAN 99 so we can say these two VLANs are merged.

Community vote distribution

B (100%)

splashy Highly Voted 1 year ago

Every time i see this question... i hate it more.
B is indeed the "least incorrect/bad" option but it's just a ridiculously small part of the whole answer. Meaning this would be the end result WITHOUT spanning tree existing and putting the end of the trunk that was last configured (mismatched) in a "broken status" blocking all untagged traffic on that port.
Call me crazy but i hate questions where i need to envision a parallel reality where spanning tree does not yet exist.

upvoted 14 times

RougePotatoe 10 months, 2 weeks ago

To explain if anyone do not understand his complaint. According to Cisco STP is enabled by default on all cisco switches. Cisco documentation says STP should shut down ports when there is a native vlan mismatch. Although, I have yet to see this happen on Packet Tracer or in Lab equipment.

upvoted 9 times

GhostWolf 10 months, 1 week ago

Thanks.

upvoted 1 times

GreatDane Most Recent 1 month, 2 weeks ago

Selected Answer: B

How to Avoid and Fix VLAN Mismatch Errors - LinkedIn

" What are the common causes and solutions of VLAN mismatch errors?
...
VLAN mismatch types

There are two main types of VLAN mismatch errors: native VLAN mismatch and access VLAN mismatch. A native VLAN mismatch occurs when two switches on the same trunk link have different native VLANs configured. A native VLAN is the default VLAN that carries untagged traffic on a trunk link. A native VLAN mismatch can cause traffic to be dropped, misrouted, or broadcasted to unintended devices.
..."

upvoted 1 times

BeautifulSmile 4 months, 3 weeks ago

This particular question gets me confused all the time.

upvoted 2 times

onikafei 1 year, 7 months ago

Selected Answer: B

B is correct

upvoted 1 times

ZUMY 2 years, 4 months ago

B is correct

upvoted 3 times

nenotronix 2 years, 6 months ago

"B" is the correct answer

upvoted 3 times

SScott 2 years, 1 month ago

While B is a bit vague, this would be the general result of the native VLAN mismatch

https://www.networkacademy.io/ccna/ethernet/trunk-native-vlan#:~:text=the%20Trunk%20settings%20on%20one%20switchport%20do%20not%20have%20to%20exactly%20match%20the%20settings%20on%20the%20other%20side%20of%20the%20link

https://learningnetwork.cisco.com/s/article/effects-of-mismatched-native-vlans-on-a-trunk-link

upvoted 2 times

Question #267 *Topic 1*

A network engineer must configure two new subnets using the address block 10.70.128.0/19 to meet these requirements:
☞ The first subnet must support 24 hosts.
☞ The second subnet must support 472 hosts.
☞ Both subnets must use the longest subnet mask possible from the address block.
Which two configurations must be used to configure the new subnets and meet a requirement to use the first available address in each subnet for the router interfaces? (Choose two.)

A. interface vlan 1148 ip address 10.70.148.1 255.255.254.0

B. interface vlan 3002 ip address 10.70.147.17 255.255.255.224

C. interface vlan 4722 ip address 10.70.133.17 255.255.255.192

D. interface vlan 1234 ip address 10.70.159.1 255.255.254.0

E. interface vlan 155 ip address 10.70.155.65 255.255.255.224

Correct Answer: *DE*

Community vote distribution

AE (93%) 4%

Customexit Highly Voted 10 months, 3 weeks ago

Selected Answer: AE

Adding my answer since there is so much confusion.

Remove C because VLAN ranges are 1-1005 and 1006-4094.

!The requirement is to use the first available address in each subnet!

For A, the network address is .148.0. The first available is 148.1. 255.255.254.0 is /23, we have 512 addresses so we are good on the 472 host requirement.

For B, 10.70.147.1 is the first address. So no.

For D, (we already decided on A but we'll do this anyway) 10.70.158.1 is our first. Not 159.1.

For E, .64 is our network, .65 is our first. This works. .224 is /27 which gives us 32 total addresses, more than we need.

I highly recommend watching 'Subnetting Mastery' youtube playlist for learn how to subnet fast.

upvoted 29 times

perri88 3 months ago

are you saying D is also valid? so A and D are valid but you preferred A because it was the first option?

upvoted 1 times

perri88 3 months ago

D is incorrect because it's not using the first ip of the range. the range of D is 10.70.158.1 to 10.70.159.254

upvoted 2 times

MTrap Highly Voted 1 year, 3 months ago

It has to be A & B. The first subnet will require 24 hosts which would put in the subnet mask ending in 224 yes. However since it is the first subnet, it has to come before the second (obviously) so a since B has an IP address of 10.70.147.17 with a subnet mask of 255.255.255.224 and A has an IP address of 10.70.148.1 and a network mask of 255.255.254.0 (512 IP addresses) and it immediately follows the previous address, this should be the answer.

upvoted 10 times

TEO1221768548956 1 month, 3 weeks ago

B cannot be correct because using a /27 subnet, the first legal network address is .32 then .64, a . 16 would work for a /28 but that would not give up to 24 hosts, so the first available network we can choose from is the .64, if we choose the .64 then the first usable address will be a .65 /27

upvoted 1 times

everchosen13 11 months, 3 weeks ago

Agreed, key word here being "First"

upvoted 1 times

Deeztroyer 1 year, 2 months ago

/27 needed for 24 addresses -> magical number is 32. The router needs to be the first IP address in the range. => E is right

upvoted 5 times

MTrap 1 year, 2 months ago

Yeap, the first available IP address thing got me.

upvoted 2 times

kastorng0718 Most Recent 3 weeks, 5 days ago

Selected Answer: AE

I think there is a quicker way to do this question. First, you should be able to quickly notice that .17 is very unlikely to be the first useable address by looking at the netmask and the binary of 17. Hence, B and C is out. .1 is very likely to be the first available address to be used, so let's check if .65 is, and .65 in this case is. Then, let's look at the netmask of A, D and E. For answering this question purpose, E must be right, and because the question explicitly said the smaller subnet must be the first one, so only A is possible and D is out.

upvoted 1 times

Yinxs 3 weeks, 6 days ago

Selected Answer: AB

B is the first subnet.
A is the second bigger subnet.

upvoted 1 times

mfaria 1 month, 1 week ago

Selected Answer: AE

AE corrects.

A: Range: 10.70.148.0 ~ 10.70.149.255, Host: x.x.148.1 ~ x.x.149.254. It is the first host and the mask is /23

B: .17 is not the first Host as network is .0 and broadcast is .31. Mask is /27

C: VLAN 4722 is not available. VLAN is 1 - 1005, 1006 - 4094

D: x.x.159.1 is not the first IP. Range is x.x.158.1 ~ x.x.159.254/23

E: Range is x.x.155.64 ~ x.x.155.96. First usable x.x.155.65/27

upvoted 2 times

GreatDane 1 month, 2 weeks ago

You're given the 10.70.128.0/19 range and you need two subnets out of it.

ALWAYS start with the most populated one.

How many bits to provision 472 IP addresses? 9 bits --> 2^9 - 2 = 510 IP addresses.
4 bits for subnetting, your subnet mask will grow to /23.

How many subnets with 4 bits? 16 subnets --> 2^4 = 16.
Which are these subnets? They are 10.70.128.0 up to 10.70.158.0. Each one is a /23 and has 510 IP addresses available.

Now, choose one. Let's say the 10.70.148.0/23 one.
First available IP address 10.70.148.1, subnet mask is 255.255.254.0 (answer A).

Now, you need 24 new, available IP addresses.
How many bits to provision 24 IP addresses? 5 bits --> 2^5 - 2 = 30 IP addresses.
Another 4 bits for subnetting, your subnet mask will grow to /27.

Among the previous 16 subnets, choose another one. Let's say the 10.70.154.0/23 one.
Which are the new subnets out of it? They are 10.70.154.0 to 10.70.155.224. Each one is a /27 and has 30 IP addresses available.

Now, choose one. Let's say the 10.70.155.64/27 one.
First available IP address 10.70.155.65, subnet mask is 255.255.255.224 (answer E).

upvoted 1 times

lamm 2 months ago

Selected Answer: AE

Correct answer attending first address in each segment.

upvoted 1 times

Hari2512 2 months, 3 weeks ago

Address: 10.70.128.0
Netmask: 255.255.224.0 = 19
Network: 10.70.128.0
Broadcast: 10.70.159.255
HostMin: 10.70.128.1
HostMax: 10.70.159.254
Hosts/Net: 8190

upvoted 1 times

doribeqiraj 4 months ago

Correct answer for me is A & E
Network 10.70.128.0/19 = 10.70.128.1-10.70.159.25
D is incorrect, because is out of range. 10.70.159.1 - 10.70.160.255
upvoted 1 times

perri88 3 months ago
you are right but D is incorrect because it's not using the first ip of the range. the range of D is 10.70.158.1 to 10.70.159.254
upvoted 1 times

Bhrino 4 months ago
Why is it not b instead of e? I understand that .64 is a network address but so is .0
upvoted 1 times

Lda_cr 4 months, 3 weeks ago
Is this flsm or vlsm?
upvoted 1 times

Danielki 5 months, 1 week ago
Selected Answer: DE
Guys please read the question carefully!
Specifically
"Both subnets must use the longest subnet mask possible from the address block."

D. interface vlan 1234 ip address 10.70.159.1 255.255.254.0

This is a /23 subnet with 512 addresses, which is sufficient for 472 hosts, and it is at the end of the /19 address block (10.70.128.0/19), so it uses the longest subnet mask possible.

So, the correct configurations to meet the requirements are options D and E:

D. interface vlan 1234 ip address 10.70.159.1 255.255.254.0

For the second subnet with 472 hosts, using the longest subnet mask possible.
E. interface vlan 155 ip address 10.70.155.65 255.255.255.224

For the first subnet with 24 hosts.
upvoted 1 times

daddydagoth 6 months, 3 weeks ago
It's AE, anyone that thinks otherwise need to hold off on taking the CCNA and brush up their subnetting!
upvoted 4 times

nnfordcion 7 months, 3 weeks ago
'meet a requirement to use the first available address in each subnet for the router interfaces?'
I don't understand the meaning of this sentence at all.What is the difference between this and normal subnetting?
upvoted 1 times

Etidic 10 months, 4 weeks ago
But we need to understand that the 32hosts subnet is only guaranteed/mandatory for the first subnet that we are creating. Other subnet blocks can exist based on VLSM. So this means that we can have x.x.147.0/28 or x.x.147.8/29 already existing or for future use.
With this in mind, it allows us to have a possible first usable address of x.x.x.17 in the x.x.x.16/27 network.
And this allows us to use the first possible available subnets from the options A-E provided after ×.×.128.0/19. This would be option B
As some of us have stated and quite rightly the allowed range is between 10.70.128.1-10.70.159.254.
Making option D incorrect.
This leaves us with option A and option B fulfilling the requirements and option A closely follows after option B address.
I hope this helps!
upvoted 1 times

Etidic 10 months, 4 weeks ago
Selected Answer: AB
The instruction in the question was precise.
The FIRST SUBNET MUST = 24hosts. This implies that you have to create a subnet for 32hosts first.
After this is done, then the second subnet must be created from the remaining available range.
In order to accommodate 24hosts we would need a subnet mask of at least /27 (32hosts). We could have used /26 (x.x.x.192 = 64hosts) if we felt like, but based on the instruction, THE LONGEST SUBNET (/26) has to be used. Hence, we have to use .224. This disqualifies Answer C.
A number of us have assumed that since the subnet we are configuring for the first subnet is for 32hosts then it invalidates B. Making us settle for E.
upvoted 1 times

KoreaSpurs 11 months, 1 week ago
can anyone explain why D is not correct?
upvoted 1 times

Customexit 10 months, 3 weeks ago
From my understanding, D cannot be correct because a requirement per the question is "to use the first available address in each subnet".

If you subnet 10.70.159.1 255.255.254.0, you will see that the network address is 10.70.158.0. The 'next' network starts at 10.70.160.0. The first available would actually be 10.70.158.1. Not 10.70.159.1.

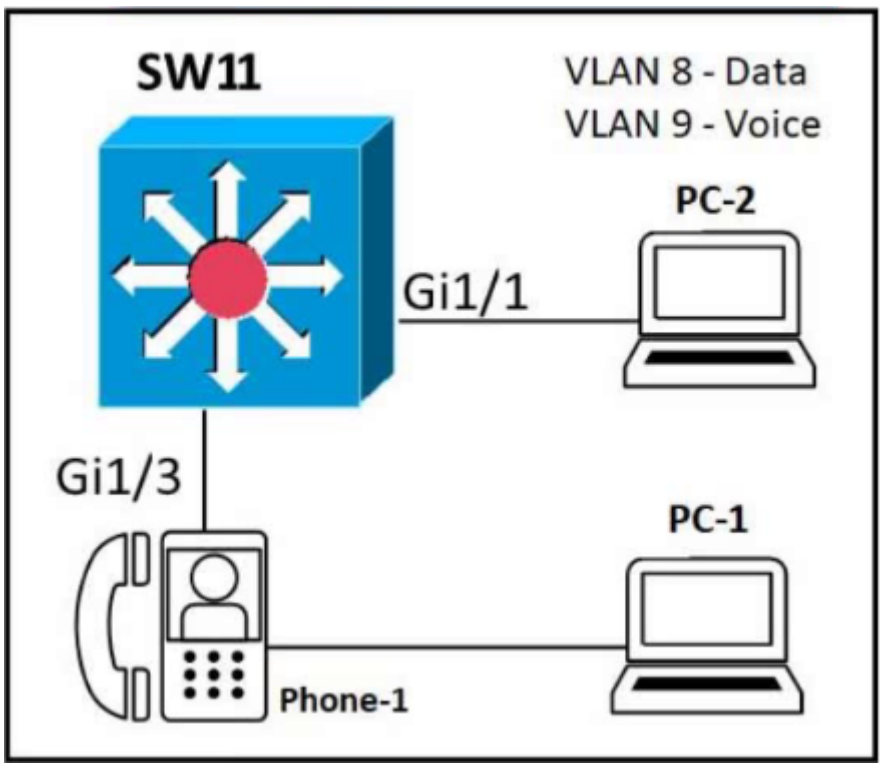
upvoted 4 times

bruno0147 10 months, 3 weeks ago

How did you get to this network if we have 0.254 1.255 with /23?

upvoted 1 times

Question #268 *Topic 1*



Refer to the exhibit. An administrator must configure interfaces Gi1/1 and Gi1/3 on switch SW11. PC-1 and PC-2 must be placed in the Data VLAN, and Phone-1 must be placed in the Voice VLAN. Which configuration meets these requirements?

A. interface gigabitethernet1/1 switchport mode access switchport access vlan 8 ! interface gigabitethernet1/3 switchport mode access switchport access vlan 8 switchport voice vlan 9

B. interface gigabitethernet1/1 switchport mode access switchport access vlan 8 ! interface gigabitethernet1/3 switchport mode trunk switchport trunk vlan 8 switchport voice vlan 9

C. interface gigabitethernet1/1 switchport mode access switchport access vlan 9 ! interface gigabitethernet1/3 switchport mode trunk switchport trunk vlan 8 switchport trunk vlan 9

D. interface gigabitethernet1/1 switchport mode access switchport access vlan 8 ! interface gigabitethernet1/3 switchport mode access switchport voice vlan 8 switchport access vlan 9

Correct Answer: *A*

Community vote distribution

A (100%)

ZUMY Highly Voted 1 year, 2 months ago

A is correct

upvoted 5 times

mfaria Most Recent 1 month, 1 week ago

Selected Answer: A

Some times identation helps

interface gigabitethernet1/1
switchport mode access
switchport access vlan 8

interface gigabitethernet1/3
switchport mode access
switchport access vlan 8
switchport voice vlan 9

upvoted 2 times

kyleptt 1 month, 2 weeks ago

A is correct

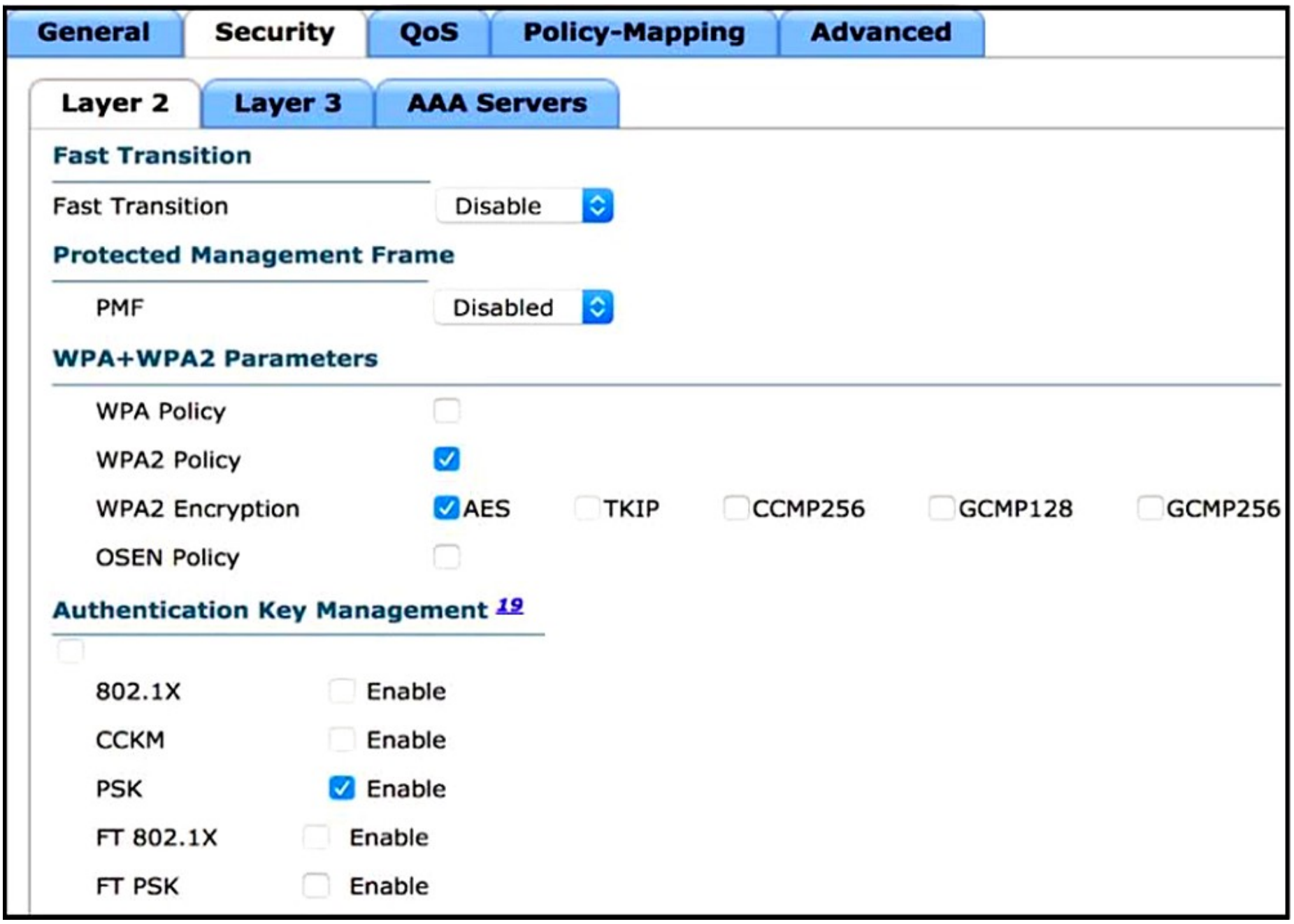
upvoted 1 times

potfur 1 year, 3 months ago

A. interface gigabitethernet1/1 switchport mode access switchport access vlan 8 ! interface gigabitethernet1/3 switchport mode access switchport access vlan 8 switchport voice vlan 9

upvoted 3 times

Question #269 *Topic 1*



Refer to the exhibit. Users need to connect to the wireless network with IEEE 802.11r-compatible devices. The connection must be maintained as users travel between floors or to other areas in the building. What must be the configuration of the connection?

A. Disable AES encryption.

B. Enable Fast Transition and select the FT 802.1x option.

C. Enable Fast Transition and select the FT PSK option.

D. Select the WPA Policy option with the CCKM option.

Correct Answer: *C*

Reference:

https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html

Community vote distribution

C (83%) B (17%)

Networknovice Highly Voted 1 year, 4 months ago

Ok, I'm going to take a swing a this...
So, the question specifically states compatible devices "Users need to connect to the wireless network with IEEE 802.11r-COMPATIBLE DEVICES."
According to the reference link, it states "If clients do not support mixed mode or 802.11r join, they can join non-802.11r WLANs. When you configure FT PSK and later define PSK, clients that can join only PSK can now join the WLAN in mixed mode."
Therefore, if you want to configure Fast Transition with COMPATIBLE DEVICES, select the FT 802.1X option. If they are non-compatible they can still join by utilizing the Pre-shared key (if selected). Consequently, I believe B is correct.

upvoted 17 times

dropspablo 1 month, 2 weeks ago

Answer is C. I believe that in the WLC GUI, generally, you cannot simultaneously enable both 802.1x and PSK authentication methods for the same WLAN, it would have to be on separate WLANs. Therefore, as the PSK method is already used, we should not change it to 802.1x/EAP, and legacy devices that do not have the 802.11r feature would just not take advantage of FT fast roaming with the initial handshake already pre-established with another AP via the 802.11r protocol, having to go through the entire reauthentication and reassociation process when roaming, creating a delay, but the devices it supports would take advantage of this feature (FT) while they roam the company's floors getting almost instantaneous associations when needs roaming.

upvoted 1 times

RougePotatoe Highly Voted 10 months, 3 weeks ago

Selected Answer: C

This question is strictly based on the configuration that is displayed here. You cannot use FT 802.1x because you don't have it configured on the the WLC; as PSK is checked not 802.1x. For you to not have to reconfigure the security setting of your network the quickest way to achieve roaming is via PSK as PSK is already configured.

upvoted 8 times

GreatDane Most Recent 1 month, 2 weeks ago

Selected Answer: C

802.11r BSS Fast Transition Deployment Guide - Cisco

"...
Configuring 802.11r Fast Transition (GUI)

Procedure
...
Step 8 Under Authentication Key Management, choose FT 802.1X or FT PSK. Check or uncheck the corresponding check boxes to enable or disable the keys. If you check the FT PSK check box, from the PSK Format drop-down list, choose ASCII or Hex and enter the key value.

Note When Fast Transition adaptive is enabled, you can use only 802.1X and PSK AKM.
..."

upvoted 2 times

Cynthia2023 1 month, 3 weeks ago

Selected Answer: C

There are two options for enabling Fast Transition:
FT 802.1x: This option is used when the wireless network employs 802.1x/EAP (Extensible Authentication Protocol) for client authentication. It allows clients to quickly transition between access points within the same ESS without reauthenticating with the RADIUS server. The clients continue using their existing 802.1x credentials as they roam.

FT PSK (Pre-Shared Key): This option is used when the wireless network uses WPA2-Personal (PSK) for client authentication. It enables fast roaming for clients that use a pre-shared key passphrase for authentication. FT PSK allows clients to roam seamlessly without reentering the PSK passphrase as they move between access points within the same ESS.
Because PSK has been checked already. so C is correct.

upvoted 4 times

HM01 2 months, 4 weeks ago

If the goal is to maintain a seamless connection for users with IEEE 802.11r-compatible devices as they move between floors or areas in a building, it is recommended to use the FT 802.1x option instead of the PSK (Pre-Shared Key) option.

The FT 802.1x option provides enhanced security and seamless authentication during the handoff process. It utilizes the IEEE 802.1x/EAP authentication method, which involves individual authentication for each user. This ensures that users are securely authenticated and their communication remains confidential.

On the other hand, the PSK option relies on a pre-shared key that is shared among all devices connecting to the network. While it provides a simpler configuration process, it may not offer the same level of security and flexibility as the FT 802.1x option.

By selecting the FT 802.1x option, you can benefit from the advanced security features and seamless authentication provided by IEEE 802.11r. This is especially important in environments where maintaining a high level of security and uninterrupted connectivity is a priority.

upvoted 1 times

lightp33 6 months, 1 week ago

https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html
In here say When Fast Transition adaptive is enabled, you can use only 802.1X and PSK AKM.. So answer is B

upvoted 1 times

freeknowledge123 8 months, 1 week ago

you cannt use FT mode without 802.1x

upvoted 1 times

ehab_alaa 9 months, 4 weeks ago

Selected Answer: B

When Fast Transition adaptive is enabled, you can use only 802.1X

upvoted 3 times

WOP_TO 1 year, 1 month ago

Selected Answer: C

PSK is enabled as a authenticatiion method, So i guess the right answer is C, because you just need to enable fast transition and FT PSK;

https://www.wiresandwi.fi/blog/configuring-fast-transition-ft-80211r-on-a-cisco-wlc

upvoted 1 times

BieLey 11 months, 3 weeks ago

PSK also supports non-compatible devices for 802.11r. Therefor it would be answer B

upvoted 1 times

ZUMY 1 year, 2 months ago

B : is correct

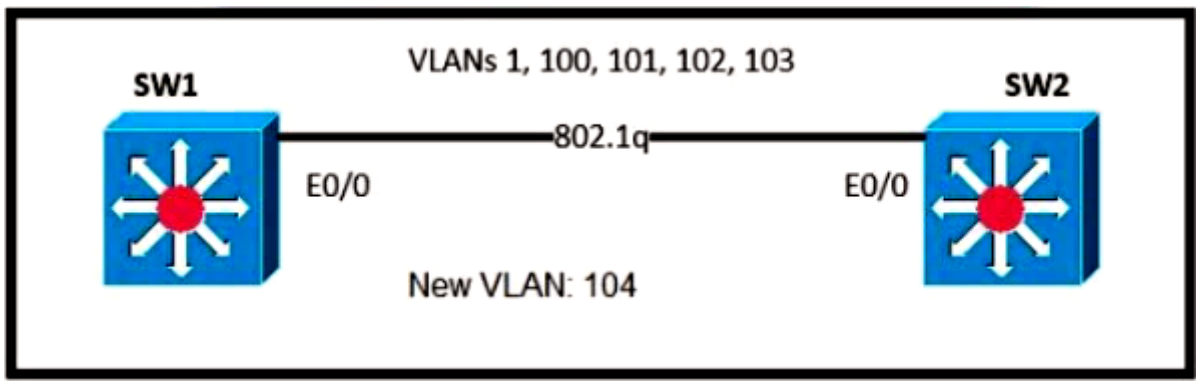
upvoted 2 times

CCNAMAN1 1 year, 4 months ago

I really dont understand why it is b, doesnt make c more sense because we want PSK?

upvoted 7 times

Question #270 *Topic 1*



Refer to the exhibit. An engineer is asked to insert the new VLAN into the existing trunk without modifying anything previously configured. Which command accomplishes this task?

A. switchport trunk allowed vlan 100-104

B. switchport trunk allowed vlan 104

C. switchport trunk allowed vlan all

D. switchport trunk allowed vlan add 104

Correct Answer: *D*

Community vote distribution

D (100%)

fabitadj 1 week ago

Switch(config-if)#switchport trunk allowed vlan ?
WORD VLAN IDs of the allowed VLANs when this port is in trunking mode
add add VLANs to the current list
all all VLANs
except all VLANs except the following
none no VLANs
remove remove VLANs from the current list

upvoted 1 times

GreatDane 1 month, 1 week ago

Selected Answer: D

How to define the VLANs allowed on a trunk link - Cisco Community

"...

2. To add a VLAN to the trunk, issue the "switchport trunk allowed vlan add <vlan-list>" command.
..."

upvoted 1 times

kyleptt 2 months, 3 weeks ago

C is also VERY valid lol

upvoted 1 times

ZUMY 1 year, 2 months ago

Selected Answer: D

D: command is correct

upvoted 4 times

Tunz 1 year, 4 months ago

Correct ans

upvoted 1 times

Question #271 *Topic 1*

Aside from discarding, which two states does the switch port transition through while using RSTP (802.1w)? (Choose two.)

A. blocking

B. speaking

C. listening

D. learning

E. forwarding

Correct Answer: *DE*
Reference:
https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html

Community vote distribution

DE (100%)

ScorpionNet Highly Voted 1 year, 4 months ago

D and E is right because
STP goes from blocked, listening, learning, and forwarding
and RSTP goes from Discarding, Learning, and Forwarding

upvoted 18 times

country_rooted Highly Voted 5 months ago

Just think Rapid. Aint got time for blocking and listening. Straight to the point

upvoted 7 times

GreatDane Most Recent 1 month, 1 week ago

Selected Answer: DE

Understand Rapid Spanning Tree Protocol (802.1w) - Cisco

"...
Port States

There are only three port states left in RSTP that correspond to the three possible operational states. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state.

STP (802.1D) Port State - Disabled -> Blocking -> Listening -> Learning -> Forwarding

RSTP (802.1w) Port State - Discarding -> Learning -> Forwarding
..."

upvoted 3 times

DUMPledore 11 months, 2 weeks ago

Selected Answer: DE

RSTP goes from Discarding, Learning, and Forwarding

upvoted 1 times

ZUMY 1 year, 2 months ago

D & E are correct

upvoted 1 times

DARKK 1 year, 3 months ago

Selected Answer: DE

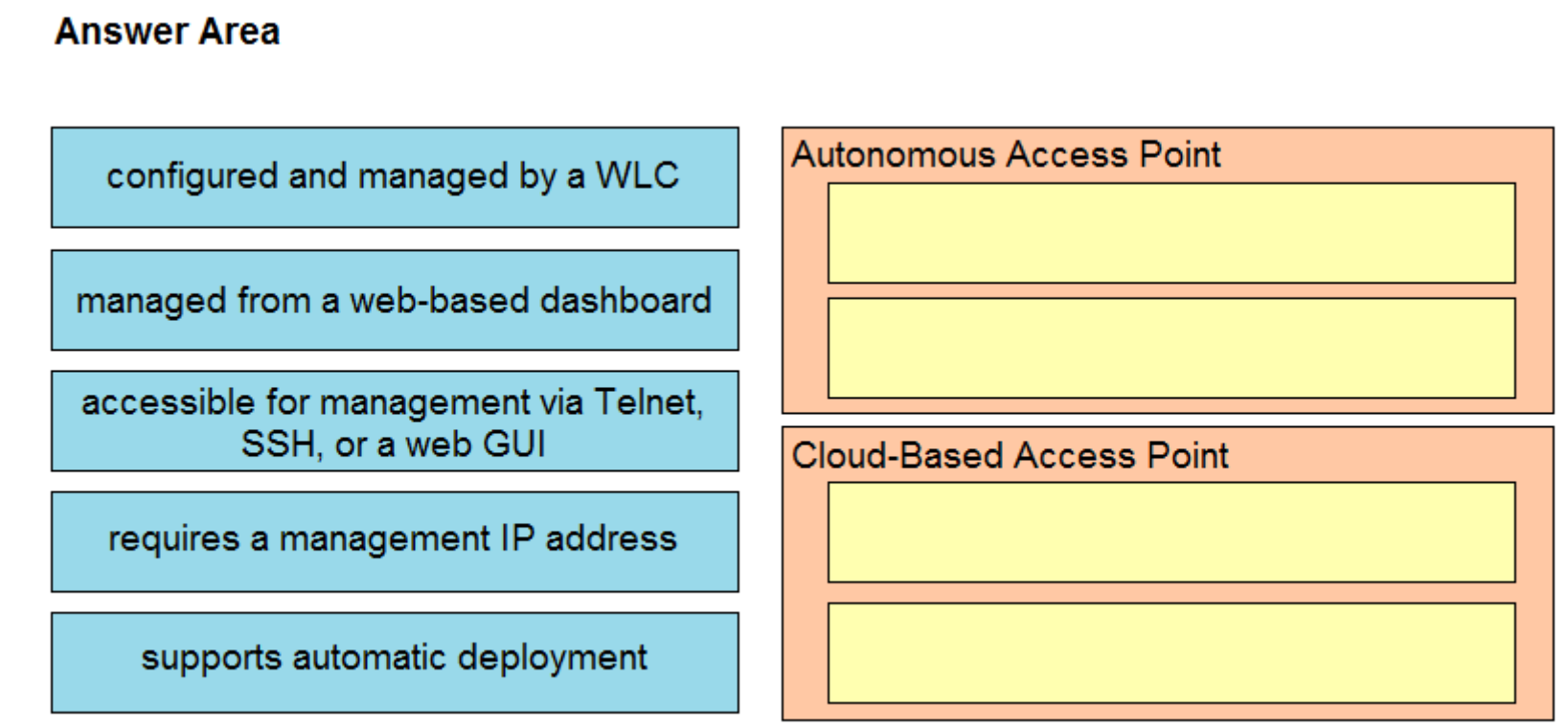
D & E Are correct. RSTP goes from Discarding to Learning, and to Forwarding.

upvoted 1 times

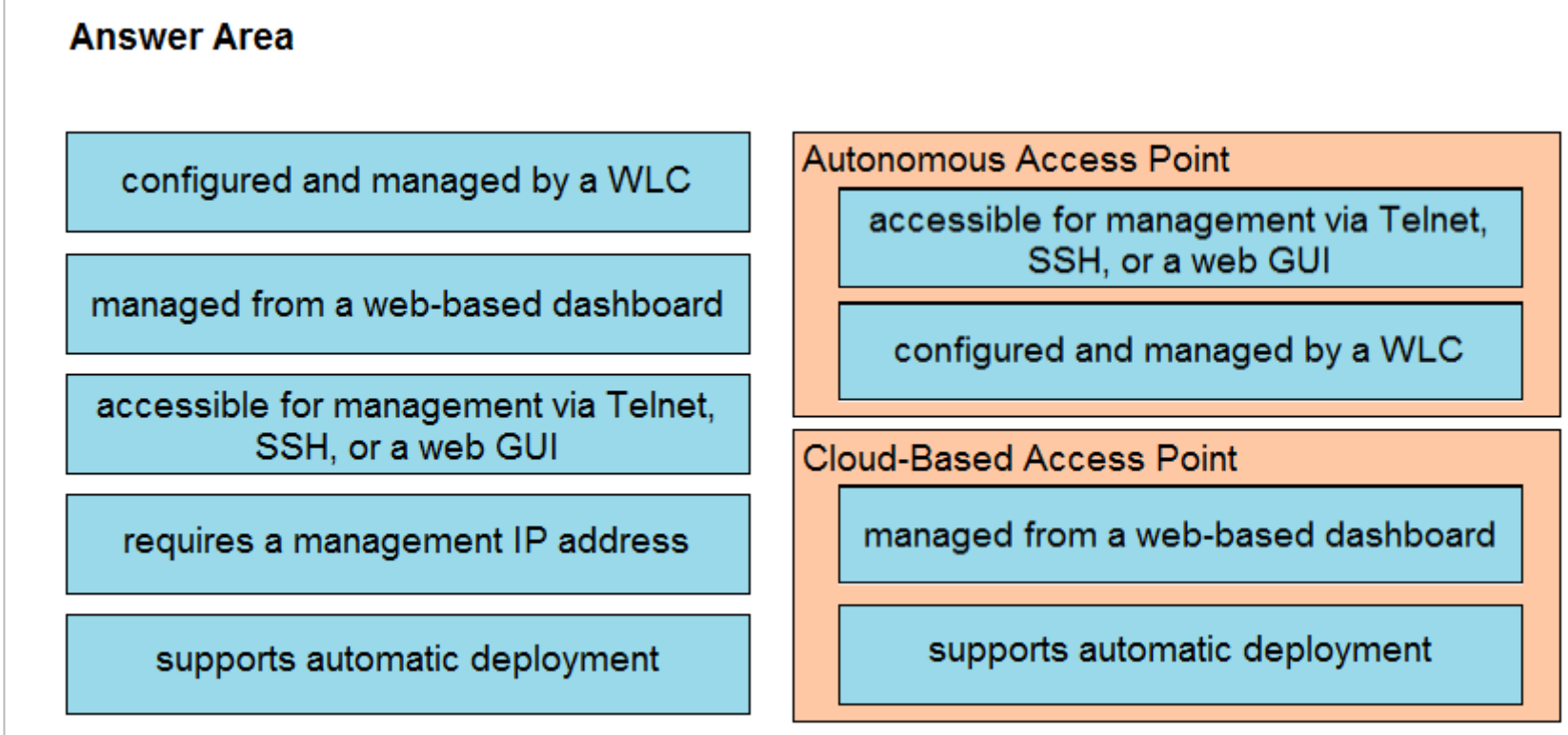
DRAG DROP -

Drag and drop the facts about wireless architectures from the left onto the types of access point on the right. Not all options are used.

Select and Place:



Correct Answer:



mrgreat Highly Voted 1 year ago

Each autonomous AP must be configured with a management IP address so that it can be remotely accessed using Telnet, SSH, or a web interface. Each AP must be individually managed and maintained unless you use a management platform such as Cisco DNA Center.

The AP management function is pushed into the Internet cloud. For example, Cisco Meraki is a cloud-based AP management service that allows you to automatically deploy Cisco Meraki APs. These APs can then be managed from the Meraki cloud web interface (dashboard).

Autonomous Access Point:
- Requires a management IP Adress
- Accessible for management via Telenet, SSH, or a web GUI

Cloud-Based Access Point:
- Supports automatic deployment
- managed from a web-based dashboard

upvoted 61 times

everchosen13 Highly Voted 11 months, 3 weeks ago

An autonomous access point does not require a WLC. The answer given is incorrect

upvoted 22 times

fabitadj Most Recent 1 week ago

Wrong answer. Should be

Autonomous Access Point:
- Requires a management IP Adress
- Accessible for management via Telenet, SSH, or a web GUI

Cloud-Based Access Point:
- Supports automatic deployment
- managed from a web-based dashboard

upvoted 1 times

raul_kapone 4 weeks, 1 day ago

The LAP is configured and managed by the WLC, not the Autonomous Access Point.
You acan see the correct answer for this question in the following link:
https://www.examtopics.com/discussions/cisco/view/77216-exam-200-301-topic-1-question-193-discussion/

upvoted 1 times

GreatDane 1 month, 1 week ago

31 Days Before your CCNA Exam: A Day-By-Day Review Guide for the CCNA 200-301 Certification Exam

AP Architectures > Wireless Concepts

"...
Autonomous AP Architecture

An autonomous AP is a self-contained device with both wired and wireless hardware so that it can bridge to the wired VLAN infrastructure wireless clients that belong to SSIDs, as shown in Figure 22-7. Each autonomous AP must be configured with a management IP address so that it can be remotely accessed using Telnet, SSH, or a web interface. Each AP must be individually managed and maintained unless you use a management platform such as Cisco DNA Center.
...
Cloud-Based AP Architecture

Cloud-based AP management is an alternative to purchasing a management platform. The AP management function is pushed into the Internet cloud. For example, Cisco Meraki is a cloud-based AP management service that allows you to automatically deploy Cisco Meraki APs. These APs can then be managed from the Meraki cloud web interface (dashboard). In Figure 22-8, the same APs shown in Figure 22-7 are now managed in the cloud.
..."

upvoted 2 times

perri88 3 months ago

Please update, the answer is incorrect, should be:
Autonomous Access Point
- acccessible for management via Tenet SSH, or a Web GUI
- requires a management IP address

upvoted 2 times

linuxlife 6 months ago

Autonomous Access Point
- acccessible for management via Tenet SSH, or a Web GUI
- requires a management IP address

upvoted 3 times

Dontguess 10 months, 2 weeks ago

Isn't "Cloud based Access Point" also configured and managed by a WLC (that in the Cloud)?

upvoted 2 times

melmiosis 10 months, 2 weeks ago

nuh, its managed with Cisco web-based dashboard aka. a software like Cisco Meraki.

upvoted 2 times

splashy 1 year ago

The given answer can only be correct in case of a HYBRID AP. It can be managed centralized with a WLC or in case of a software defined network a controller. And it can be managed like an autonomous AP: by giving it an ip address and using ssh/telnet/web to connect to it.

Autonomous Access Point:
- Requires a management IP Adress
- Accessible for management via Telenet, SSH, or a web GUI

Cloud-Based Access Point:
- Supports automatic deployment
- managed from a web-based dashboard

upvoted 10 times

Question #273 *Topic 1*

Which interface mode must be configured to connect the lightweight APs in a centralized architecture?

A. WLAN dynamic

B. trunk

C. access

D. management

Correct Answer: *C*
While the Cisco WLCs always connect to 802.1Q trunks, Cisco lightweight APs do not understand VLAN tagging and should only be connected to the access ports of the neighbor switch.
This is an example switch port configuration from the Catalyst 3750: interface GigabitEthernet1/0/22 description Access Port Connection to Cisco Lightweight AP switchport access vlan 5 switchport mode access no shutdown
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/69719-wlc-lwap-config.html

Community vote distribution

C (100%)

GreatDane 1 month, 1 week ago

Selected Answer: C
Configure Wireless LAN Controller and Lightweight Access Point Basic - Cisco

"...
Configure the Switch for the APs
...
While the Cisco WLCs always connect to 802.1Q trunks, Cisco lightweight APs do not understand VLAN tagging and must only be connected to the access ports of the neighbor switch.
..."
upvoted 1 times

rijstraket 7 months, 3 weeks ago

Lightweight Access-Points do understand VLAN tagging when in FlexConnect mode, the keyword is 'centralized' here indicating this is a "Local" deployment. Hence the use for an access port, as the user data is tunneled with CAPWAP to the WLC.
upvoted 2 times

Treasureprecious 3 weeks ago

They said CISCO access points do not. They precized
upvoted 1 times

creaguy 11 months, 3 weeks ago

"centralized architecture" why don't they call it for what it is a "switch"
upvoted 3 times

ptfish 1 year, 2 months ago

While the Cisco WLCs always connect to 802.1Q trunks, Cisco lightweight APs do not understand VLAN tagging and should only be connected to the access ports of the neighbor switch.

This is an example switch port configuration from the Catalyst 3750:

interface GigabitEthernet1/0/22
description Access Port Connection to Cisco Lightweight AP
switchport access vlan 5
switchport mode access
no shutdown
upvoted 2 times

TA77 1 year, 2 months ago

"While the Cisco WLCs always connect to 802.1Q trunks, Cisco lightweight APs do not understand VLAN tagging and should only be connected to the access ports of the neighbor switch."

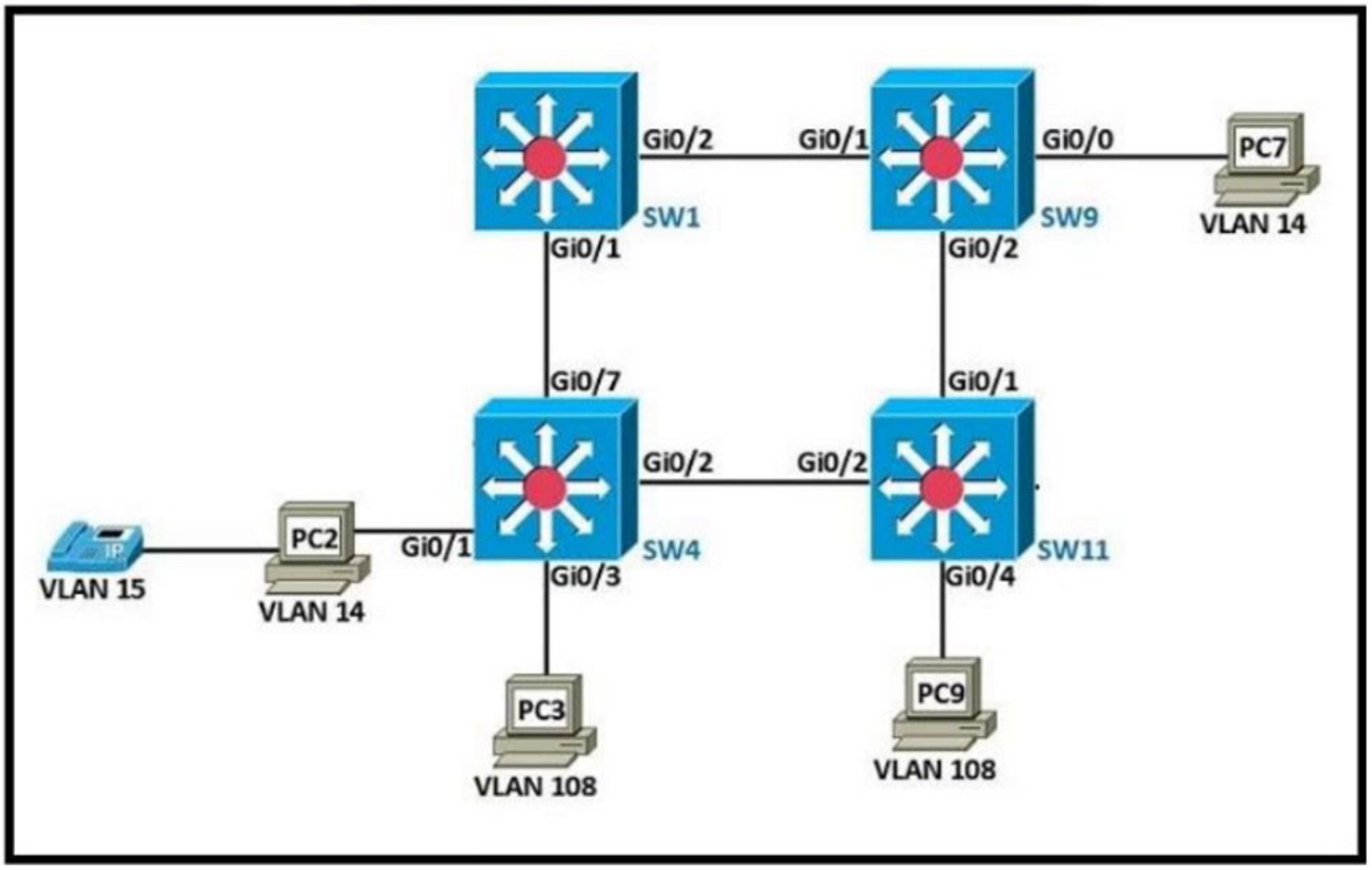
From the link provided:
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/69719-wlc-lwap-config.html
upvoted 1 times

jobba111 1 year, 2 months ago

its just asking which status its gonna be

upvoted 1 times

Question #274 *Topic 1*



Refer to the exhibit. The following must be considered:

☞ SW1 is fully configured for all traffic.

☞ The SW4 and SW9 links to SW1 have been configured.

☞ The SW4 interface Gi0/1 and Gi0/0 on SW9 have been configured.

☞ The remaining switches have had all VLANs added to their VLAN database.

Which configuration establishes a successful ping from PC2 to PC7 without interruption to traffic flow between other PCs?

A. SW4 interface Gi0/7 switchport mode trunk switchport trunk allowed vlan 108 ! interface Gi/0/2 switchport mode access switchport access vlan 14 SW11# interface Gi0/2 switchport mode trunk switchport trunk allowed vlan 14,108 ! interface Gi0/1 switchport mode trunk switchport trunk allowed vlan 14,108 SW9# interface Gi0/2 switchport mode access switchport access vlan 14

B. SW4 interface Gi0/2 switchport mode trunk switchport trunk allowed vlan 14,108 SW11# interface Gi0/2 switchport mode trunk switchport trunk allowed vlan 14,108 !! interface Gi0/1 switchport mode trunk switchport trunk allowed vlan 14,108 SW9# interface Gi0/2 switchport mode trunk switchport trunk allowed vlan 14

C. SW4 interface Gi0/2 switchport mode trunk switchport trunk allowed vlan 14 SW11# interface Gi0/1 switchport mode trunk switchport trunk allowed vlan 14 SW9# interface Gi0/2 switchport mode trunk switchport trunk allowed vlan 108

D. SW4 interface Gi/0/2 switchport mode access switchport access vlan 14 SW11# interface Gi0/2 switchport mode trunk switchport trunk allowed vlan 14 ! interface Gi0/0 switchport mode access switchport access vlan 14 ! interface Gi0/1 switchport mode trunk SW9# interface Gi0/2 switchport mode access switchport access vlan 14

Correct Answer: *C*

Community vote distribution

B (100%)

Etidic Highly Voted 10 months, 4 weeks ago

Did anyone notice that all the wrong answers have exclamation marks (!!) in the CLI?

upvoted 12 times

HMaw Highly Voted 10 months ago

C is correct. Please simulate in Cisco Package Tracer and you guys will know why it's correct. All I need to make G0/2 on SW4 to be trunk port and G0/1 on SW11 to be trunk port. I don't even have to touch SW9. Stop debating, hand on is alway the best and you will never forget. PS - preconfigured all the switches as mentioned in question. Good luck

upvoted 5 times

thomson_johnson 6 months ago

C must be wrong, because PC2 and PC7 are in VLAN 14, and the last command in C looks like that:
SW9# interface Gi0/2 switchport mode trunk switchport trunk allowed vlan 108

upvoted 3 times

linuxlife 6 months ago

C is wrong.

upvoted 2 times

binrayelias 8 months ago

It's B, based on the questions S4 gi0/2; SW11 gi0/2,gi0/1; and SW9 gi0/2 is not configured.

upvoted 1 times

raul_kapone Most Recent 4 weeks, 1 day ago

Selected Answer: B

B is correct.

SW11 is unconfigured, so their ports (Gi0/2 and Gi0/1) need to be configured as trunks to PC2 can ping PC7. Also, it needs allowing the VLAN 14 fot both interfaces (Gi0/2 and Gi0/1).

Alternative C only configures the Gi0/1 interface, not both.

upvoted 1 times

shumps 1 month, 1 week ago

B is the answer, you cannot turn one side trunk only so C is wrong

upvoted 1 times

mfaria 1 month, 1 week ago

Selected Answer: B

B is correct,

A, C and D lacks configuration of VLAN and Trunk on S4, S11 and S9

upvoted 1 times

kishan365 2 months, 1 week ago

Selected Answer: B

The key is " without interruption to traffic flow between other PCs". Thus the trunk port must be allowed for the multiple VLAN`s for the seamless traffic flow.

upvoted 4 times

dropspablo 4 months, 1 week ago

Selected Answer: B

C is wrong.
The same link between SW11 and SW9 has only VLAN 14 allowed on one side and only VLAN 108 on the other. In this case, none of them pass.
This configuration doesn't make sense:

SW11# interface Gi0/1 switchport mode trunk switchport trunk allowed vlan 14
SW9# interface Gi0/2 switchport mode trunk switchport trunk allowed vlan 108

upvoted 3 times

deluxeccna 5 months ago

Based on the exhibit and the given information, the correct configuration that establishes a successful ping from PC2 to PC7 without interruption to traffic flow between other PCs is:

B.

SW4
interface Gi0/2
switchport mode trunk
switchport trunk allowed vlan 14,108

SW11
interface Gi0/2
switchport mode trunk
switchport trunk allowed vlan 14,108
!
interface Gi0/1
switchport mode trunk
switchport trunk allowed vlan 14,108

SW9
interface Gi0/2
switchport mode trunk
switchport trunk allowed vlan 14

In this configuration, SW4 and SW11 are trunked with allowed VLANs 14 and 108, while SW9 is trunked with only VLAN 14 allowed. This allows

traffic to flow between PC2 and PC7, which belong to VLANs 14 and 108 respectively. The other VLANs will also continue to function without interruption.

upvoted 3 times

linuxlife 6 months ago

C doesnt allow all two VLANs between SW4 and SW11 which B does.

upvoted 1 times

iMo7ed 7 months ago

Selected Answer: B

It is B

upvoted 1 times

Sdiego 7 months, 4 weeks ago

Selected Answer: B

C answer is incorrect, missing configuration for Gi0/2 interface on SW11

upvoted 2 times

Anas_Ahmad 7 months, 4 weeks ago

Selected Answer: B

just look on SW 4 configuration (switchport trunk allowed vlan 14,108)

upvoted 3 times

freeknowledge123 8 months, 1 week ago

correct answer is B, don't forget to always check the discussion even if you think the answer is obvious.

upvoted 3 times

jibon_22 9 months, 1 week ago

Correct ans is: B
Because look carefully, for G0/2 of S9, allowed VLAN is 108 not 14.

upvoted 3 times

joeylam 9 months ago

at G0/2, S9 have to tag traffic from pc7 to vlan 108 and 14.
G0/2 of S9 should allowed both VLAN 108 and 14.

upvoted 2 times

everchosen13 11 months, 3 weeks ago

I believe the Answer would actually be B

upvoted 3 times

TMT91 11 months, 4 weeks ago

Selected Answer: B

I think B is the right answer

upvoted 3 times

ShadyAbdekmalek 12 months ago

However B seems most accurate among all other choices , I still think there should be a typo . VL 108 should not be allowed between SW11 and and SW9. the trunk configuration must be the same at both sides

upvoted 2 times

Question #275 *Topic 1*

```
Cat9K-1# show lldp entry Cat9K-2

Local Intf: Gi1/0/21
Chassis id: 308b.b2b3.2880
Port id: Gil/0/21
Port Description: GigabitEthernet1/0/21
System Name: Cat9K-2

Management Addresses:
   IP: 10.5.110.2
```

Refer to the exhibit. The network administrator must prevent the switch Cat9K-2 IP address from being visible in LLDP without disabling the protocol. Which action must be taken to complete the task?

A. Configure the no lldp mac-phy-cfg command globally on Cat9K-2.

B. Configure the no lldp receive command on interface G1/0/21 on Cat9K-1.

C. Configure the no lldp transmit command on interface G1/0/21 on Cat9K-1.

D. Configure the no lldp tlv-select management-address command globally on Cat9K-2.

Correct Answer: *C*

Community vote distribution

D (100%)

[Removed] Highly Voted 3 months ago

Again, this is NOT CCNA 200-301

upvoted 6 times

Shanku97 3 weeks, 1 day ago

Do they ask this kind of question in the exam ?

upvoted 1 times

chian 3 weeks ago

I wrote about this topic last week.....

upvoted 1 times

guisam Highly Voted 9 months, 1 week ago

R2#sh lldp entry R1.guisam.lan | se Mana
Management Addresses:
IP: 10.1.1.1

R1(config)#no lldp tlv-select management-address
R1(config)#no lldp run
R1(config)#lldp run

R2#sh lldp entry R1.guisam.lan | se Mana
Management Addresses - not advertised

upvoted 6 times

juneq888 Most Recent 1 week, 3 days ago

So it says here that the answer is C. But the vote says D. So what are we going to answer in the actual exam? Is it the answer on this dump (C) or is it the correct answer (D)?

upvoted 1 times

GreatDane 1 month ago

Selected Answer: D

Configuring LLDP - Cisco

"...
Configuring Optional LLDP Parameters

You can configure the frequency of LLDP updates, the amount of time for a receiving device to hold the information before discarding it, and the initialization delay time. You can also select the TLVs to include in LLDP packets.

Procedure
...
Step 6 - (Optional) [no] lldp tlv-select <tlv>

Specifies the TLVs to send and receive in LLDP packets. The available TLVs are

management-address
port-description
port-vlan
system-capabilities,
system-description
system-name

All available TLVs are enabled by default.
..."
upvoted 2 times

linuxlife 6 months ago

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_37_ey/configuration/guide/scg/swlldp.pdf

D is the correct way to answer this question
upvoted 3 times

diudiuQIdama 8 months, 4 weeks ago

Selected Answer: D

You don't want sw2's ip to be seen, you should do something on sw2 not sw1, otherwise sw34567 still can see sw's ip. a is about layer 2 address, wrong. So D
upvoted 2 times

Yunus_Empire 9 months, 2 weeks ago

Selected Answer: D

D is Correct

https://vceguide.com/which-action-must-be-taken-must-be-taken-to-complete-the-task/
upvoted 1 times

mzu_sk8 10 months, 2 weeks ago

Selected Answer: D

from another source
upvoted 1 times

Equiano 11 months, 3 weeks ago

Selected Answer: D

Option C disables the switch from transmitting LLDP. The task is to disable the switch from sending its IP address only, hence D is a better option.
upvoted 1 times

ShadyAbdekmalek 12 months ago

Selected Answer: D

This example shows how to enable LLDP to send or receive IPv4 management address TLVs:
switch# configure terminal
switch(config)# lldp tlv-select management-address v4

Source:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/layer2/602_U1_1/b_Cisco_n3k_Layer_2_Switching_Config_602_u1_1/b_Cisco_n3k_Layer_2_Switching_Config_602_u1_1_chapter_01001.pdf

So we must negate the command as per option D
upvoted 1 times

Nodirbek 1 year ago

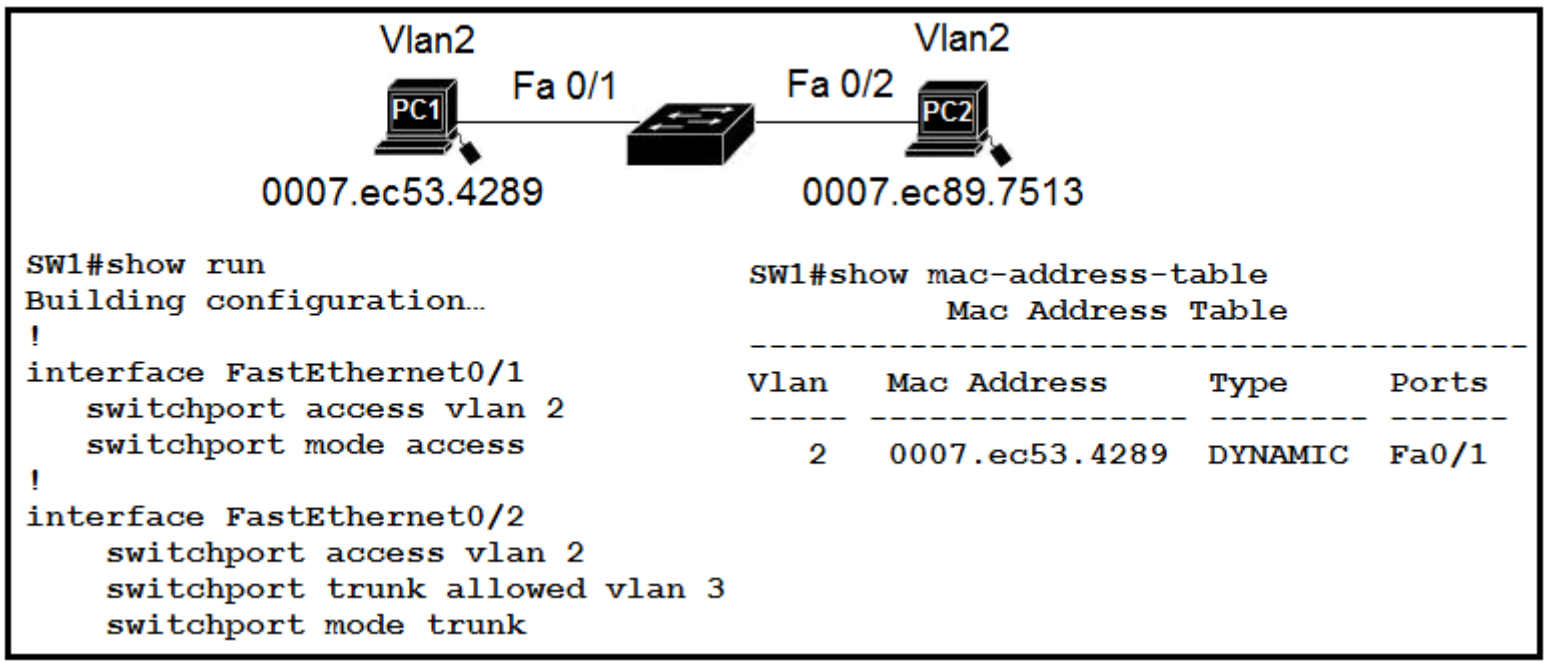
Selected Answer: D

i know this is the exact and right answer
upvoted 1 times

foreach 1 year ago

Selected Answer: D

D seems a better answer to me.
With C, you disable transmitting LLDP infos on Cat9K-1 interface, not on Cat9K-2. And the question is asking about Cat9K-2. And with B, you won't receive any LLDP infos on Cat9K-1 interface, which is overkill.
So D seems a better choice. With it, you're only disabling sending/receiving mgmt address on Cat9K-2.
upvoted 3 times



Refer to the exhibit. An engineer has started to configure replacement switch SW1. To verify part of the configuration, the engineer issued the commands as shown and noticed that the entry for PC2 is missing. Which change must be applied to SW1 so that PC1 and PC2 communicate normally?

A. SW1(config)#interface fa0/2 SW1(config-if)#no switchport access vlan 2 SW1(config-if)#no switchport trunk allowed vlan 3 SW1(config-if)#switchport trunk allowed vlan 2

B. SW1(config)#interface fa0/2 SW1(config-if)#no switchport access vlan 2 SW1(config-if)#switchport trunk native vlan 2 SW1(config-if)#switchport trunk allowed vlan 3

C. SW1(config)#interface fa0/2 SW1(config-if)#no switchport mode trunk SW1(config-if)#no switchport trunk allowed vlan 3 SW1(config-if)#switchport mode access

D. SW1(config)#interface fa0/1 SW1(config-if)#no switchport access vlan 2 SW1(config-if)#switchport access vlan 3 SW1(config-if)#switchport trunk allowed vlan 2

Correct Answer: *C*

Community vote distribution

C (100%)

Goh0503 Highly Voted 11 months, 2 weeks ago

Answer C
access port – a port that can be assigned to a single VLAN. This type of interface is configured on switch ports that are connected to end devices such as workstations, printers, or access points.
trunk port – a port that is connected to another switch. This type of interface can carry traffic of multiple VLANs, thus enabling you to extend VLANs across your entire network. Frames are tagged by assigning a VLAN ID to each frame as they traverse between switches.
https://study-ccna.com/access-and-trunk-ports/

upvoted 6 times

ananinamia Most Recent 2 weeks, 5 days ago

But where vlan3 comes what is relation with this question?

upvoted 2 times

Bhrino 4 months ago

Selected Answer: C

C is correct there's no need to use trunk ports due the fact they are all in the same vlan and c just removes all the trunking commands and adds the last access port one

upvoted 1 times

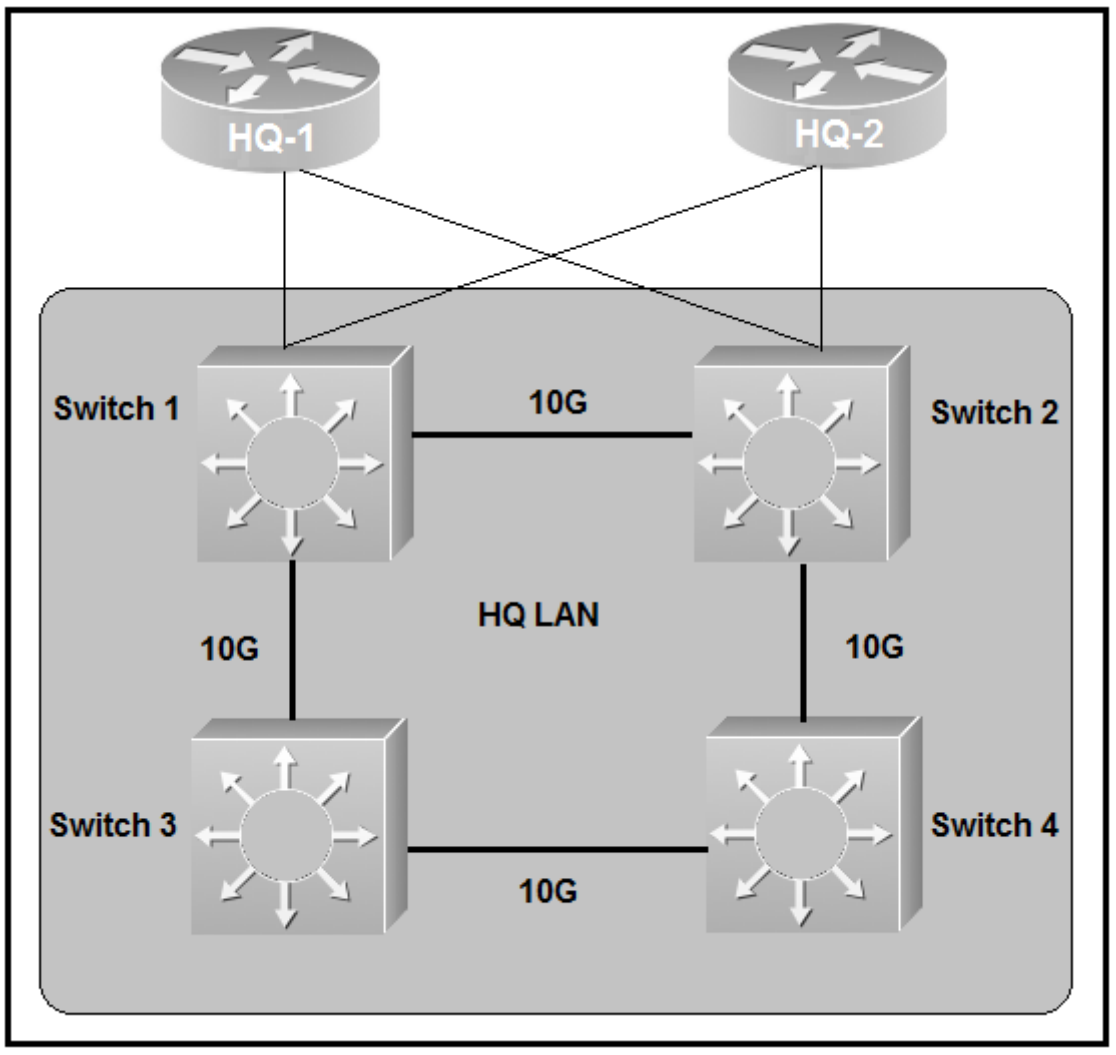
iMo7ed 7 months ago

Selected Answer: C

C is correct

upvoted 2 times

Refer to the exhibit. Which switch becomes the root of the spanning tree?



Switch 1 -

BID: 32778 0018.184e.3c00 -

Switch 2 -

BID: 24586 001a.e3ff.a680 -

Switch 3 -

BID: 28682 0022.55cf.cc00 -

Switch 4 -

BID: 64000 4e15.8403.08f -

A. Switch 1

B. Switch 2

C. Switch 3

D. Switch 4

Correct Answer: *B*

PassNow1234 Highly Voted 7 months, 2 weeks ago

Every switch taking part in spanning tree has a bridge priority. The switch with the lowest priority becomes the root bridge. If there's a tie, then the switch with the lowest bridge ID number wins

upvoted 6 times

badboyrobinson Highly Voted 9 months ago

zgzdgf

upvoted 5 times

davidmdlp85 Most Recent 2 months ago

The answer is A

upvoted 1 times

davidmdlp85 2 months ago

From Packet tracer
Switch(config)#spanning-tree vlan 1 priority 24586
% Bridge Priority must be in increments of 4096.
% Allowed values are:
0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440

upvoted 1 times

davidmdlp85 2 months ago

My question is... the priority is not supposed to be in jumps of 4096 ??? If you divide each option by 4096 only the 32768 works

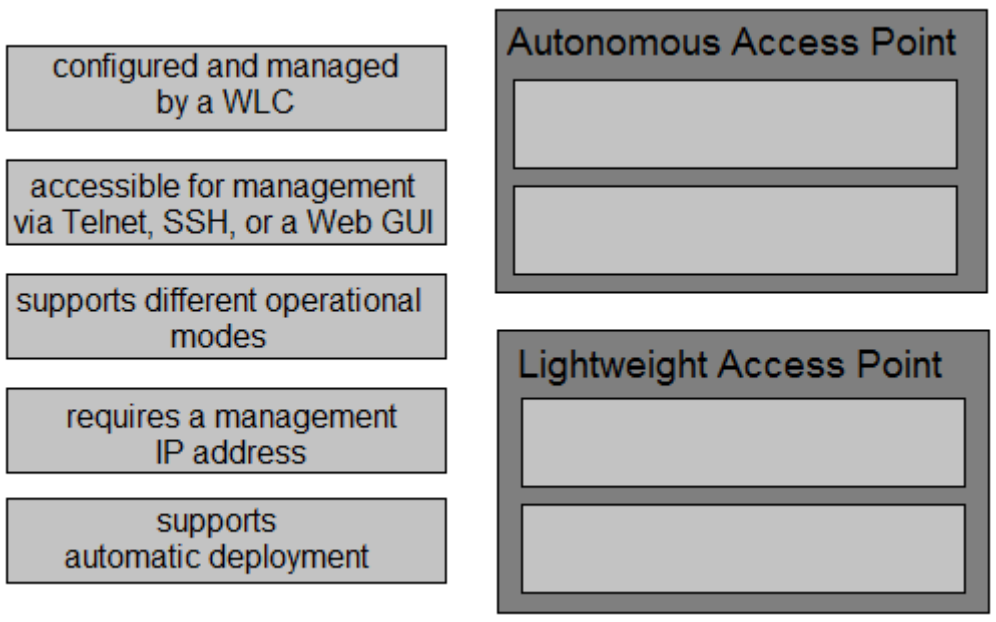
upvoted 1 times

Question #278 *Topic 1*

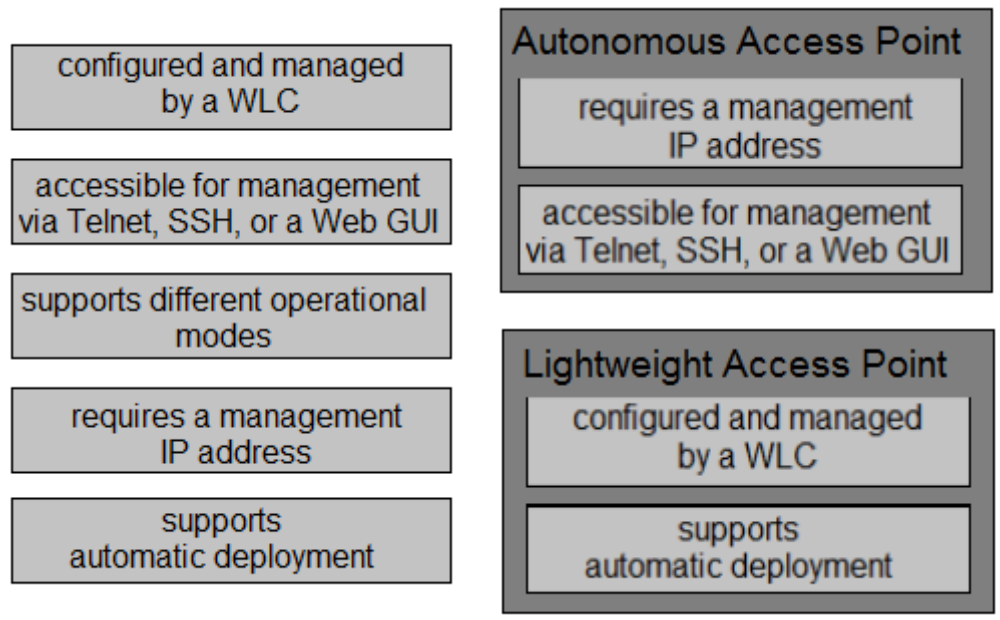
DRAG DROP -

Drag and drop the facts about wireless architectures from the left onto the types of access point on the right. Not all options are used.

Select and Place:



Correct Answer:



Bonesaw Highly Voted 11 months, 3 weeks ago

The Lightweight Access Point supports different modes, like bridge, sniffer, local, or Flexconnect.

Automatic deployments are for cloud based

upvoted 46 times

Lance789 Highly Voted 11 months, 1 week ago

i think it should be
Autonomous Access Point
- accessible for management via Telnet, SSH, or a Web GUI
-requires a management IP address

Lightweight Access Point
- configured ang managed by a WLC
- supports different operational modes

upvoted 42 times

dropspablo 1 month, 2 weeks ago

(I agree with Lance789, I'm just adding some info from the official CISCO guide.)

Cisco Meraki APs can be "deployed automatically", once you register with the Meraki cloud. Each AP will contact the cloud when it powers up and will self-configure. From that point on, you can manage the AP through the Meraki cloud dashboard. (OCG Wendell Odom V1)

Cisco AP Modes
Many Cisco APs can operate in either autonomous or lightweight mode, depending on which code image is loaded and run. From the WLC, you can also configure a lightweight AP to operate in one of the following special-purpose modes: Local:..., Monitor:..., Sniffer:..., Rogue detector:..., Bridge:..., Flex+Bridge:..., SE-Connect:... (OCG Wendell Odom V1)

upvoted 1 times

LekkiDee Most Recent 4 months ago

I have an autonomous AP I use at home to extend my Wi-Fi coverage. It has the below options if I need to configure it.

Radio0-802.11N2.4GHz
Role in Radio Network: Access Point Repeater
Root Bridge Non-Root Bridge
Workgroup Bridge Universal Workgroup Bridge Client MAC:
Scanner

This means that Autonomous APs can also support different operational modes. I wish Cisco can fix these annoying ambiguous questions.

upvoted 3 times

[Removed] 3 months ago

They won't since they want us to fail so they can make more money

upvoted 1 times

mustdoit 7 months ago

Answer is incorrect.
Autonomous:
- Accessible via telnet...
- Configured by WLC

Lightweight
- Require a management IP
- Support different operational modes

upvoted 3 times

deluxeccna 5 months ago

Autonomous is configured by WLC? That's not correct

upvoted 4 times

AlexFordly 10 months, 2 weeks ago

Autonomous Access Point
- accessible for management via Telnet, SSH, or a Web GUI
-requires a management IP address

Lightweight Access Point
- configured ang managed by a WLC
- supports different operational modes

upvoted 5 times

```
interface g2/0/0
  channel-group 1 mode active
interface g4/0/0
  channel-group 1 mode active
interface Port-channell
   ip address 203.0.113.65 255.255.255.252

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channell,
changed state to down
```

Refer to the exhibit. An engineer is configuring a Layer 3 port-channel interface with LACP. The configuration on the first device is complete, and it is verified that both interfaces have registered the neighbor device in the CDP table. Which task on the neighbor device enables the new port channel to come up without negotiating the channel?

A. Configure the IP address of the neighboring device.

B. Bring up the neighboring interfaces using the no shutdown command.

C. Change the EtherChannel mode on the neighboring interfaces to auto.

D. Modify the static EtherChannel configuration of the device to passive mode.

Correct Answer: *D*

Community vote distribution

D (50%) B (50%)

splashy Highly Voted 1 year ago

Yes... it's D

But it's also a bad answer as per cisco documentation (current netacad course)

static/manual = etherchannel ON
dynamic/negotiation = LACP PagP

So they provide an answer with a partially incorrect statement to confuse you and look at an other option with an even worse or incorrect statement... .

upvoted 12 times

Yinxs Most Recent 3 weeks, 6 days ago

Selected Answer: D

The focus of this question is how to communicate with neighbor to make a LACP l3 channel. So active <---> passive can make this goal.

upvoted 1 times

raptuz 1 month, 2 weeks ago

Selected Answer: B

Is missing some config.
For create a L3 port-channel is it necessary to no switchport for the interfaces that will be member of port-channel, this operation admin shutdown the interfaces. The question is to come up without negotiating the channel, so is it necessary to bring up the neighbors interfaces.

upvoted 1 times

FALARASTA 4 months, 3 weeks ago

But the passive mode will call for negotiation from the active mode. The answer is partially wrong but the best choice anyway

upvoted 1 times

Murphy2022 11 months, 3 weeks ago

Which task on the neighbor device enables the new port channel to come up without negotiating the channel?

As the neighboring device isn't negotiating its LACP Channel in passive mode, D is correct.
The negatiation is done by the active configuration. Passive only accepts, but doesn't negotiate.

upvoted 3 times

RougePotatoe 10 months, 2 weeks ago

Based on this cisco resource you are wrong. The right answer should be manually configure it to On as passive still participate in negotiation. Since that option is not here the closest right answer is D. "Both the active and passive LACP modes enable ports to negotiate with partner ports to an EtherChannel based on criteria such as port speed, and for Layer 2 EtherChannels, based on trunk state and VLAN numbers."
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0111110.pdf

upvoted 3 times

FALARASTA 4 months, 3 weeks ago

From that document: Both theactiveandpassiveLACPmodes enable ports to negotiatewith partnerports to an EtherChannelbasedoncriteriasuchasportspeed,andforLayer2EtherChannels,basedontrunkstateandVLANnumbers.PortscanformanEtherChannel whentheyareindifferentLACPmodesaslongasthemodesarecompatible.For example:•A port in theactivemode can form an EtherChannelwith anotherport that is in theactiveorpassivemode.•A port in thepassivemode cannotform an EtherChannelwith anotherport that is also in thepassivemode becauseneitherport starts LACP negotiation.

I support

upvoted 1 times

harsh1309 7 months ago

Yes RougePotatoe is correct, passive doesn't cause port to not negotiate, instead port wait for other switch to start negotiation and then they start negotiation.

upvoted 1 times

purenuker 10 months ago

Does "active" and "on" form an etherchannel ? I don't think so.

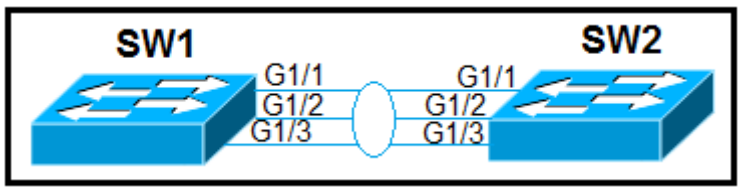
upvoted 3 times

RougePotatoe 10 months ago

Think you might be right. I've seen a chart a while back that stated it does but I've never checked it. I just did it in packet tracer and in the Active/ON configuration results in the LACP side to have po1 as connected while the ON switch has po1 as not connected. The LACP switch has 1 of the links protocol down as well.

upvoted 1 times

Question #280 *Topic 1*



Refer to the exhibit. Which configuration establishes a Layer 2 LACP EtherChannel when applied to both switches?

A. Interface range G1/1 1/3 "€λ switchport mode trunk channel-group 1 mode active no shutdown

B. Interface range G1/1 1/3 "€λ switchport mode access channel-group 1 mode passive no shutdown

C. Interface range G1/1 1/3 "€λ switchport mode trunk channel-group 1 mode desirable no shutdown

D. Interface range G1/1 1/3 "€λ switchport mode access channel-group 1 mode on no shutdown

Correct Answer: *A*

Community vote distribution

A (63%) D (38%)

freeknowledge123 Highly Voted 8 months, 1 week ago

LACP=Active PAGP=desirable Static=On

upvoted 8 times

Yinxs Most Recent 3 weeks, 6 days ago

Selected Answer: A

It's A.
Active and Active is LACP
Desirable and Desirable is PAGP

upvoted 1 times

maboud85 1 month, 3 weeks ago

for option A they choose trunk config which is not complete ,maybe the other switch its not using dot1q so the best answer is D

upvoted 1 times

[Removed] 3 months ago

Selected Answer: A

A is correct as LACP uses active and passive.

upvoted 1 times

Hope_12 4 months, 1 week ago

Selected Answer: A

LACP uses active and passive
A. Uses active(2 active interfaces do form ether channel) Correct Answer
B. Uses passive(2 passive interfaces don't form ether channel)
C. Uses desirable (This is for PAGP ether channel required is LACP)
D. Uses mode on(This is for static ether channel required is LACP)

upvoted 3 times

Jacques1982 8 months ago

Selected Answer: D

I would think answer D... because...they ask the question on both switched. If you "mode active" on both sides it won't form the etherchannel. If "mode ON" then it would establish the channel? Am I wrong?

upvoted 3 times

Mark_j_k90 2 months ago

Keep studing, you're wrong, answer is A! With LACP you can use active on both side!

upvoted 1 times

[Removed] 4 months ago

A is correct. Ether channel should be LACP hence, mode is active on both switch

upvoted 1 times

hamish88 7 months, 1 week ago

You are dead wrong. A is correct.

upvoted 5 times

joyboy92 7 months, 3 weeks ago

Wrong, in D answer you are setting the range in access; to create ethercannel we need mode trunk .... i tried to research on my netacad course. In this case i'll go A.

upvoted 9 times

Question #281 *Topic 1*

Which switching concept is used to create separate broadcast domains?

A. STP

B. VTP

C. VLAN

D. CSMA/CD

Correct Answer: *C*

Community vote distribution

C (100%)

[Removed] 3 months ago

Selected Answer: C

Answer C is correct.

upvoted 1 times

LeonardoMeCabrio 3 months, 2 weeks ago

Selected Answer: C

C Correct

upvoted 1 times

Question #282 *Topic 1*

```
Cat9300# show cdp
Global CDP information:
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
   Sending CDPv2 advertisements is enabled
```

Refer to the exhibit. Which action must be taken so that neighboring devices rapidly discover switch Cat9300?

A. Enable portfast on the ports that connect to neighboring devices.

B. Configure the cdp timer 10 command on switch Cat9300.

C. Configure the cdp holdtime 10 command on switch Cat9300

D. Configure the cdp timer 10 command on the neighbors of switch Cat9300

Correct Answer: *B*

CHCHCHC Highly Voted 7 months, 4 weeks ago
hello beautiful
upvoted 12 times

GARAAA 2 months, 3 weeks ago
hahahahahah
upvoted 1 times

RAJ_1920 4 months, 2 weeks ago
Hello chunky munkie
upvoted 2 times

NICE_ANSWERS 3 months, 2 weeks ago
hihihihihi😂😂😂😂
upvoted 2 times

Robles1979 Most Recent 1 month, 1 week ago
none of this was helpful
upvoted 2 times

Question #283 *Topic 1*

What is a requirement when configuring or removing LAG on a WLC?

A. The incoming and outgoing ports for traffic flow must be specified if LAG is enabled.

B. The management interface must be reassigned if LAG is disabled

C. The controller must be rebooted after enabling or reconfiguring LAG

D. Multiple untagged interfaces on the same port must be supported

Correct Answer: *B*

Community vote distribution

C (88%) 12%

PiotrMar Highly Voted 1 year ago

it seams like B and C might be right:
B - When you disable LAG, you must assign an AP-manager interface to each port on the controller.
C - When LAG is enabled, any change to the LAG configuration requires a controller reboot
https://community.cisco.com/t5/wireless-mobility-knowledge-base/lag-link-aggregation/ta-p/3128669#toc-hId--766763784

upvoted 6 times

splashy 11 months, 3 weeks ago

You are right after reading it again i think B might be "more correct"
because C states after enabling OR reconfiguring, which would imply you need to reboot when you enable LAG and again after configuring it, which would seem a bit strange and unpractical. Good catch Piotr.

upvoted 3 times

splashy 11 months, 3 weeks ago

I dunno C could still score some points it is just worded very weird as usual...

upvoted 1 times

dick3311 Highly Voted 10 months, 2 weeks ago

Selected Answer: C

Answer C is correct

upvoted 6 times

dropspablo Most Recent 1 month, 2 weeks ago

Selected Answer: B

B and C is correct... missing (choose two)
https://community.cisco.com/t5/wireless-mobility-knowledge-base/lag-link-aggregation/ta-p/3128669#toc-hId--766763784:~:text=for%20all%20interfaces.-,When%20you%20disable%20LAG%2C%20you%20must%20assign%20an%20AP%2Dmanager%20interface%20to%20each%20port%20on%20the%20controller.,-The%20controller%E2%80%99s%20neighbor

upvoted 1 times

dropspablo 3 weeks, 5 days ago

Correcting, B is wrong (partially correct) as we assign an AP-manager interface to each WLC port only when we disable the LAG, and answer C is more correct as we must restart the WLC either when removing the LAG or when configuring (in any change). Link: "When LAG is enabled, any change to the LAG configuration requires a controller reset."
(The question asked "configuring or removin" the LAG on the WLC, the letter "C" fits both).
https://community.cisco.com/t5/wireless-mobility-knowledge-base/lag-link-aggregation/ta-p/3128669#toc-hId--766763784:~:text=When%20LAG%20is%20enabled%2C%20any%20change%20to%20the%20LAG%20configuration%20requires%20a%20controller%20reboot.

upvoted 1 times

Tibisandres 5 months, 3 weeks ago

Selected Answer: C

When you enable LAG or make any changes to the LAG configuration, you must immediately reboot the controller.
(https://community.cisco.com/t5/wireless-mobility-knowledge-base/lag-link-aggregation/ta-p/3128669#:~:text=When%20you%20enable%20LAG%20or%20make%20any%20changes%20to%20the%20LAG%20configuration%2C%20you%20must%20immediately%20reboot%20the%20controller.)

upvoted 1 times

Ciscoman021 5 months, 4 weeks ago

Selected Answer: C

When you enable LAG or make any changes to the LAG configuration, you must immediately reboot the controller. When you enable LAG, you can configure only one AP-manager interface because only one logical port is needed. LAG removes the requirement for supporting multiple AP-manager interfaces.

upvoted 2 times

thomson_johnson 6 months ago

People here in discussion forgot that AP-manager and management interfaces are not the same.
C is correct I think
The management interface is the default interface used to access and manage the WLC. The management interface is also used by the access points to communicate with the WLC. The management interface IP address is the only ping-able IP address and is used by administrators to manage the WLC.

Administrators can log into the WLC's configuration GUI by entering the management interface IP address in a web browser and logging into the system.

nothing that relates to LAG

upvoted 3 times

linuxlife 6 months ago

https://community.cisco.com/t5/wireless-mobility-knowledge-base/lag-link-aggregation/ta-p/3128669#toc-hId--766763784

When LAG is enabled, any change to the LAG configuration requires a controller reboot.
When you enable LAG, you can configure only one AP-manager interface because only one logical port is needed.
When you disable LAG, you must assign an AP-manager interface to each port on the controller.

upvoted 1 times

DevNetAdmin 6 months, 3 weeks ago

it is C.
https://me2learn.wordpress.com/2014/05/22/wlc-link-aggregation-lag/
on part2 it is clearly written to reboot.

upvoted 1 times

Silviu11 7 months ago

It is C

upvoted 1 times

xbobdan 7 months, 2 weeks ago

Selected Answer: B

after reading some of the discussions, i agree with B

upvoted 2 times

Anas_Ahmad 7 months, 4 weeks ago

Selected Answer: C

you must immediately reboot the controller.

upvoted 4 times

Anas_Ahmad 8 months ago

Selected Answer: C

must immediately reboot the controller.

upvoted 4 times

mhdyqq 8 months, 2 weeks ago

Answer C is correct

upvoted 2 times

mrgreat 11 months, 1 week ago

Answer C is correct. When you enable LAG or change the LAG configuration, you must immediately reboot the controller.
http://what-when-how.com/deploying-and-troubleshooting-cisco-wireless-lan-controllers/lag-cisco-wireless-lan-controllers/

upvoted 3 times

splashy 1 year ago

Selected Answer: C

https://community.cisco.com/t5/wireless-mobility-knowledge-base/lag-link-aggregation/ta-p/3128669#toc-hId--766763784

Obviously C...

upvoted 3 times

splashy 11 months, 3 weeks ago

Check Piotr

upvoted 1 times

guynetwork 1 year ago

Selected Answer: C

it is c

upvoted 3 times

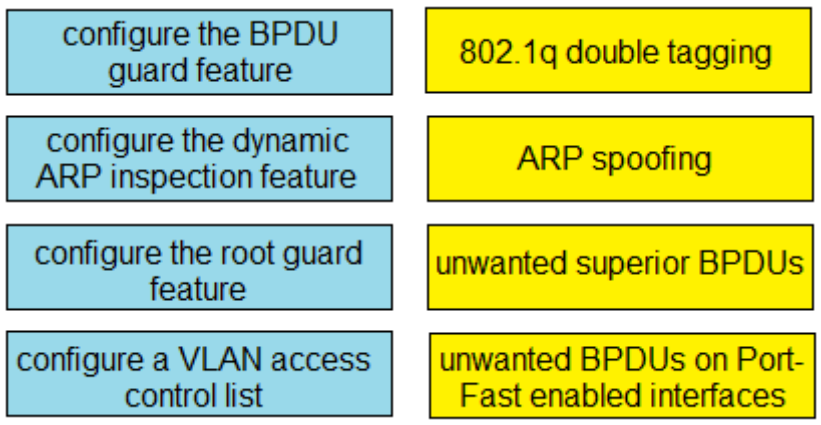
reeeda 1 year ago

C is the right answer
-When LAG is enabled, any change to the LAG configuration requires a controller reboot.
https://community.cisco.com/t5/wireless-mobility-knowledge-base/lag-link-aggregation/ta-p/3128669
upvoted 3 times

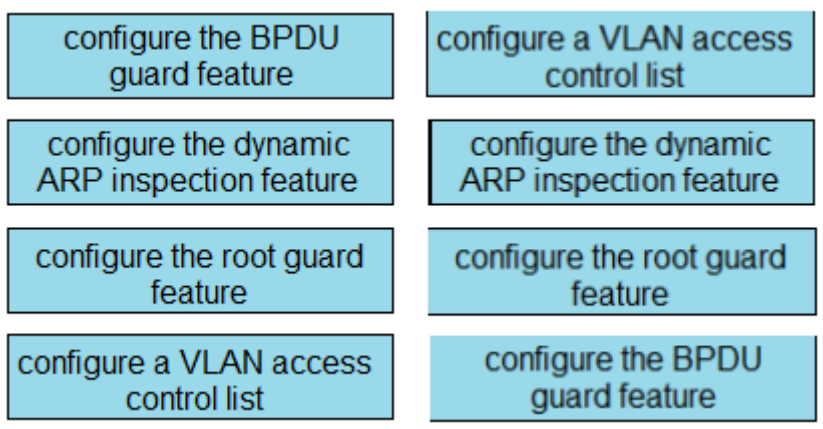
Webfat 7 months, 1 week ago
Using your link, we also have:
"When you disable LAG, you must assign an AP-manager interface to each port on the controller."
upvoted 2 times

Question #284 *Topic 1*

DRAG DROP -
Drag and drop the threat-mitigation techniques from the left onto the types of threat or attack they mitigate on the right.
Select and Place:



Correct Answer:



country_rooted Highly Voted 5 months, 2 weeks ago
The answer given is correct
upvoted 6 times

[Removed] 3 months ago
Exactly!
upvoted 1 times

no_blink404 Most Recent 2 months, 3 weeks ago
Configure the root guard feature: Unwanted superior BPDUs
Configure the dynamic ARP inspection feature: ARP spoofing
Configure the root guard feature: Unwanted superior BPDUs
Configure a VLAN access control list: 802.1q double tagging
upvoted 1 times

Question #285 *Topic 1*

Which type of port is used to connect the wired network when an autonomous AP maps two VLANs to its WLANs?

A. access

B. LAG

C. trunk

D. EtherChannel

Correct Answer: *C*

Community vote distribution

C (100%)

Da_Costa 3 weeks, 1 day ago

Selected Answer: C

The autonomous AP must be connected in trunk mode in order to carry multiple VLANs,

upvoted 1 times

MoHTimo 1 month, 1 week ago

Selected Answer: C

is correct

upvoted 1 times

everchosen13 11 months, 3 weeks ago

Answer given is correct.
https://study-ccna.com/autonomous-ap-access-point-configuration/

upvoted 3 times

Question #286 *Topic 1*

A network administrator needs to aggregate 4 ports into a single logical link which must negotiate layer 2 connectivity to ports on another switch. What must be configured when using active mode on both sides of the connection?

A. LLDP

B. LACP

C. Cisco vPC

D. 802 1q trunks

Correct Answer: *B*

country_rooted 5 months, 2 weeks ago

LACP-Active, Passive (Industry standard)
PAgP -Desirable, Auto (Cisco Proprietary)

upvoted 4 times

xbobdan 7 months ago

acronyms acronyms acronyms!

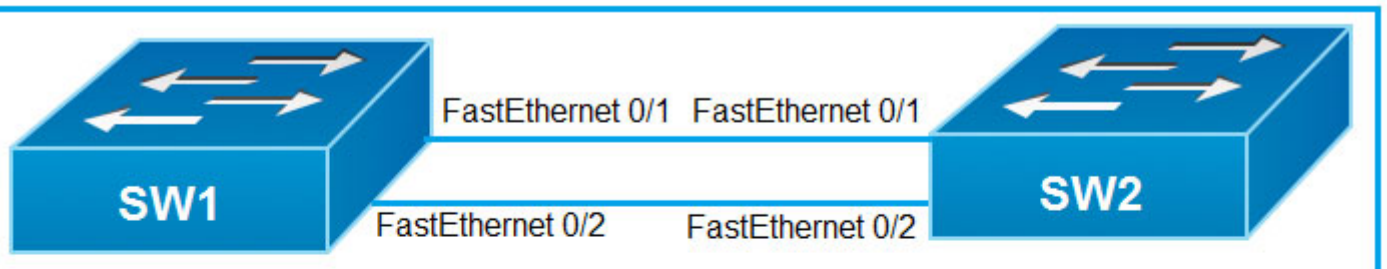
upvoted 2 times

Rether16 5 months, 1 week ago

I was just thinking that, I almost selected LLDP by accident!

upvoted 1 times

Question #287 *Topic 1*




```
SW1#show run interface fastEthernet 0/1
switchport trunk encapsulation dotlq
switchport mode trunk
switchport trunk allowed vlan 100, 200, 300
channel-group 1 mode on

SW1#show run interface fastEthernet 0/2
switchport trunk encapsulation dotlq
switchport mode trunk
switchport trunk allowed vlan 100, 200, 300
channel-group 1 mode on

SW2#show run interface fastEthernet 0/1
switchport trunk encapsulation dotlq
switchport mode trunk
switchport trunk allowed vlan 100, 200, 300
channel-group 1 mode active

SW2#show run interface fastEthernet 0/2
switchport trunk encapsulation dotlq
switchport mode trunk
switchport trunk allowed vlan 100, 200, 300
channel-group 1 mode active
```

Refer to the exhibit. An engineer built a new L2 LACP EtherChannel between SW1 and SW2 and executed these show commands to verify the work establish an
LACP port channel?

A. Change the channel-group mode on SW1 to desirable

B. Change the channel-group mode on SW1 to active or passive

C. Change the channel-group mode on SW2 to auto

D. Configure the interface port-channel 1 command on both swtiches

Correct Answer: *B*

RougePotatoe Highly Voted 10 months, 2 weeks ago
I'm literally spending more time trying to figure out what the question is asking rather than figuring out the answer...
upvoted 10 times

daddydagoth 6 months, 3 weeks ago
These are the dangers of braindumps my friend
upvoted 3 times

Yunus_Empire 9 months, 2 weeks ago
That's What Einstein Said About (Question / Answer) issue, if you know!!!
upvoted 2 times

no_blink404 Most Recent 3 months, 1 week ago
B is the correct answer. The question is checking if you know the correct combinations for establishment and the difference between LACP and PAGP
upvoted 1 times

cuenca73 7 months ago
the commands starting with "switchport" should not be inside the Po1 interface config instead inside the individual interface conforming the channel-group?

but also B is right

upvoted 1 times

Customexit 10 months, 3 weeks ago

LACP = Active/Passive
PAGP = Desirable/Auto

upvoted 3 times

everchosen13 11 months, 3 weeks ago

I think the question is not worded correctly but I believe answer given, B is correct.

upvoted 3 times

Question #288 *Topic 1*

Refer to the exhibit. For security reasons, automatic neighbor discovery must be disabled on the R5 Gi0/1 interface. These tasks must be completed:

- Disable all neighbor discovery methods on R5 interface Gi0/1
- Permit neighbor discovery on R5 interface Gi0/2.
- Verify there are no dynamically learned neighbors on R5 interface Gi0/1.
- Display the IP address of R6's interface Gi0/2

Which configuration must be used?

A. R5(config)#int Gi0/1 R5(config-if)#no cdp enable R5(config-if)#exit R5(config)#lldp run R5(config)#no cdp run R5#sh cdp neighbor detail R5#sh lldp neighbor

B. R5(config)#int Gi0/1 R5(config-if)#no cdp enable R5(config-if)#exit R5(config)#no lldp run R5(config)#cdp run R5#sh cdp neighbor R5#sh lldp neighbor

C. R5(config)#int Gi0/1 R5(config-if)#no cdp run R5(config-if)#exit R5(config)#lldp run R5(config)#cdp enable R5#sh cdp neighbor R5#sh lldp neighbor

D. R5(config)#int Gi0/1 R5(config-if)#no cdp enable R5(config-if)#exit R5(config)#no lldp run R5(config)#cdp run R5#sh cdp neighbor detail R5#sh lldp neighbor

Correct Answer: *D*

Community vote distribution

D (100%)

dropspablo Highly Voted 4 months, 1 week ago

Selected Answer: D

D. R5(config)#int Gi0/1 R5(config-if)#no cdp enable R5(config-if)#exit R5(config)#no lldp run R5(config)#cdp run R5#sh cdp neighbor detail R5#sh lldp neighbor

- Disable all neighbor discovery methods on R5 interface Gi0/1
(config-if)#no cdp enable / (config)#no lldp run

- Permit neighbor discovery on R5 interface Gi0/2.
(config)#cdp run

- Verify there are no dynamically learned neighbors on R5 interface Gi0/1.
#sh lldp neighbor (just to confirm LLDP discovery has been disabled)

- Display the IP address of R6's interface Gi0/2
#sh cdp neighbor detail ("detail" shows information such as IP address)

upvoted 5 times

SaMee69 Highly Voted 9 months, 2 weeks ago

If you don't understand why 'cdp run' command again in the end:

cdp is running by default on IOS routers and IOS switches. If you turn off cdp globally by "no cdp run", there is no cdp process running, and even if there is an interface configured with "cdp enable", the device will not send or process cdp frames. If you configure an interface with "no cdp enable" and cdp is running on the device, the device will send and process received cdp frames on any interface but the ones, where cdp is disabled.

upvoted 5 times

CHCHCHC 7 months, 4 weeks ago

what about the last command? how wil "sh lldp neighbor" work when you have already disabled it in global privilage mode? w

upvoted 5 times

FALARASTA Most Recent 4 months, 3 weeks ago

D is correct. The actions are performed for both LLDP and CDP. I was confused at first

upvoted 1 times

VictorCisco 5 months, 3 weeks ago

Why in the end show lldp neighbor? if lldp is disabled ??

upvoted 2 times

linuxlife 6 months ago

but if for specific interface only, no cdp enable is a VALID command.
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi0/1
Switch(config-if)#no cdp enable
Switch(config-if)#

upvoted 1 times

linuxlife 6 months ago

no cdp enable is an INVALID command. It must be no cdp run.

Switch(config)#no cdp enable
^
% Invalid input detected at '^' marker.

Switch(config)#no cdp run
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show cdp neigh
Switch#show cdp neighbors
% CDP is not enabled
Switch#

upvoted 1 times

country_rooted 5 months, 2 weeks ago

This command is solely to disable an interface or a range thereof as is indicated in the question. Hence, why C is wrong from the go / process of elimination because we are not trying to disble CDP globally.

upvoted 1 times

imigr 5 months, 3 weeks ago

you have to type this command under the interface Switch(config-if)#no cdp enable

upvoted 1 times

RougePotatoe 10 months, 2 weeks ago

Does anyone know why is it D? Nothing says these routers are both cisco devices?

upvoted 3 times

splashy 10 months, 2 weeks ago

I think because "Disable all neighbor discovery methods"
which means both lldp & cdp

upvoted 2 times

Question #289 *Topic 1*

Which two spanning-tree states are bypassed on an interface running PortFast? (Choose two.)

A. disabled

B. listening

C. learning

D. blocking

E. forwarding

Correct Answer: *BC*

SVN05 Highly Voted 7 months, 1 week ago

PortFast is a Spanning-Tree Protocol feature used to speed up convergence time on ports which are connected to a workstation by causing a port to enter the forwarding state instantly, bypassing the listening and learning state.

Ref:-https://www.skillset.com/questions/which-stp-feature-is-used-to-speed-up-convergence-time-on-ports-which-are-connected-to-a-workstation#:~:text=PortFast%20is%20a%20Spanning%2DTree,the%20listening%20and%20learning%20state.

upvoted 5 times

SVN05 7 months, 1 week ago

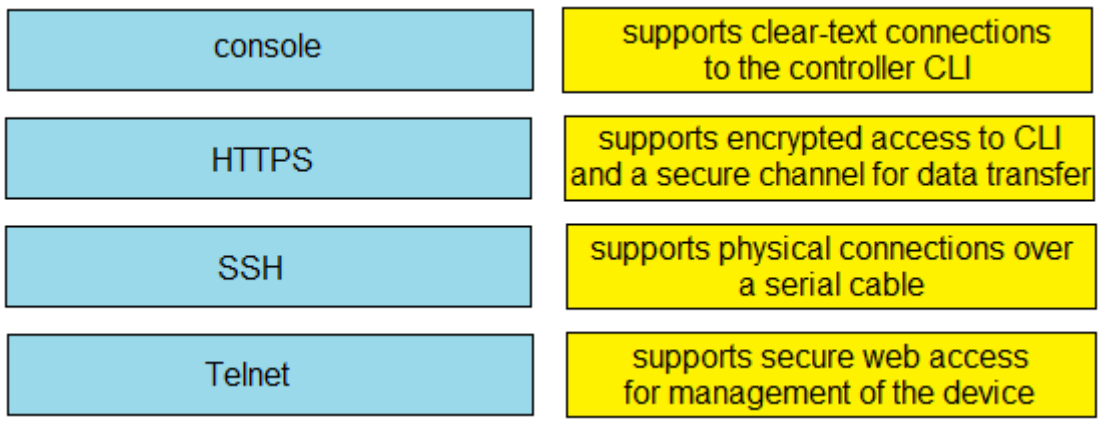
In addition, you should not confuse yourself with port states(discussed in Rapid Spanning Tree)where the states are discarding, learning and forwarding only.

upvoted 3 times

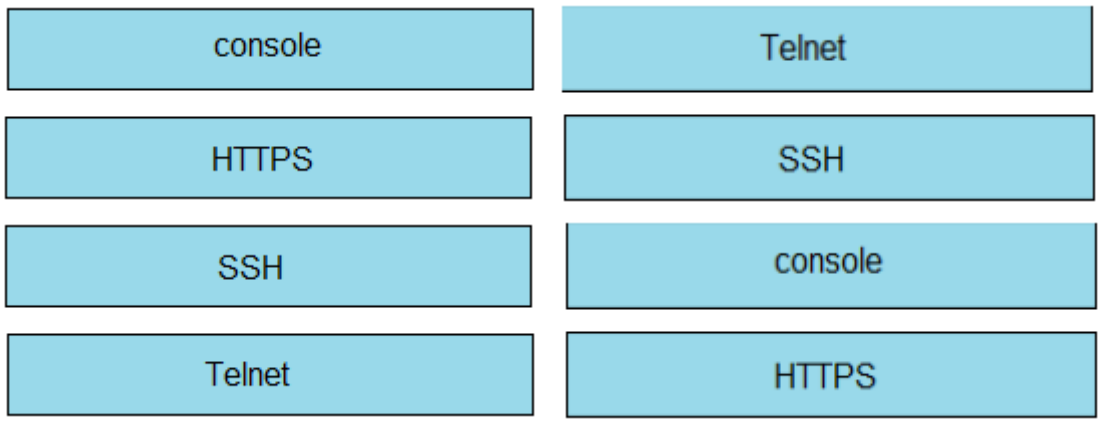
DRAG DROP -

Drag and drop the management connection types from the left onto the definitions on the right.

Select and Place:



Correct Answer:



Yunus_Empire Highly Voted 9 months, 2 weeks ago

One of The Simplest Question

upvoted 8 times

mrgreat Highly Voted 1 year ago

Answers are correct

upvoted 5 times

Question #291 *Topic 1*

An engineer is configuring data and voice services to pass through the same port. The designated switch interface fastethernet0/1 must transmit packets using the same priority for data when they are received from the access port of the IP phone. Which configuration must be used?

A. interface fastethernet0/1 switchport voice vlan dot1p

B. interface fastethernet0/1 switchport priority extend cos 7

C. interface fastethernet0/1 switchport voice vlan untagged

D. interface fastethernet0/1 switchport priority extend trust

Correct Answer: *D*

Community vote distribution

D (67%) B (33%)

Mahfuj_01 Highly Voted 9 months, 3 weeks ago

I think answer is correct.

Set the priority of data traffic received from the Cisco IP Phone access port:

•cos value—Configure the "phone" to override the priority received from the "PC or the attached device" with the specified CoS value. The value is a number from 0 to 7, with 7 as the highest priority. The default priority is cos 0.
So, If we set the value 7 here it means, port will prioritize the voice traffic over data traffic.

•trust—Configure the phone access port to trust the priority received from the "PC or the attached device".
When traffic from pc is trusted, it will consider both voice and data traffic as same priority. (Since voice traffic is prioritised over data traffic by default.)

upvoted 12 times

jibon_22 9 months, 1 week ago

you are right, D is correct.

upvoted 1 times

Johan_jelly Highly Voted 9 months, 1 week ago

Hey, I know that the answer is D, but do we have to know this type of commands for the CCNA ?

upvoted 7 times

[Removed] 3 months ago

I woud say no. This is not in Netacad official Cisco CCNA 200-301 courses.

upvoted 1 times

Aie_7 7 months, 2 weeks ago

I agree

upvoted 2 times

wakaish Most Recent 1 week, 1 day ago

switchport priority extend is used to configure the switch port to extend the priority markings of the incoming frames.

trust in this context means that the switch will trust the priority markings set by the connected device (in this case, the IP phone).

This configuration allows the switch to trust the priority markings set by the IP phone, ensuring that both voice and data packets are treated with the same priority when transmitted through the same port. This is commonly used in Quality of Service (QoS) configurations to maintain proper prioritization of traffic.

upvoted 1 times

dropspablo 4 months, 1 week ago

Selected Answer: D

D is correct, "switchport priority extend trust" in trust mode the switch transmits frames with the same marking received on its port.

Without this command, the markings would be forwarded with CoS 0, regardless of the marking received.

If the question had asked to change the marking, also with the highest possible priority, then the answer would be B, "switchport priority extend cos 7" with CoS 7 transmission for all packets, regardless of the marking received.

upvoted 2 times

mustdoit 7 months ago

Wondering why 100% said B is correct when it doesn't seem to according to below cisco source.
D is the correct answer.
Please read carefully:

"Cisco IP Phone Data Traffic
The switch can also process tagged data traffic (traffic in IEEE 802.1Q or IEEE 802.1p frame types) from the device attached to the access port on the Cisco IP Phone. You can configure Layer 2 access ports on the switch to send CDP packets that instruct the attached phone to configure the phone access port in one of these modes :
- In trusted mode , all traffic received through the access port on the Cisco IP Phone passes through the phone unchanged.
- In untrusted mode , all traffic in IEEE 802.1Q or IEEE 802.1p frames received through the access port on the Cisco IP Phone receive a configured Layer 2 CoS value . The default Layer 2 CoS value is 0. Untrusted mode is the default."

upvoted 3 times

laurvy36 7 months, 1 week ago

The switchport priority extend trust command does not configure the switch port to trust the traffic it receives from an IP phone.

upvoted 1 times

mustdoit 7 months ago

Nowhere, it's been asked to configure the switch port to trust the traffic unless I'm missing something?

upvoted 1 times

DMc 8 months, 1 week ago

B is the Answer:
Step 3 switchport priority extend {cos value | trust}
Set the priority of data traffic received from the Cisco IP Phone access port:
•cos value—Configure the phone to override the priority received from the PC or the attached device with the specified CoS value. The value is a number from 0 to 7, with 7 as the highest priority. The default priority is cos 0.
•trust—Configure the phone access port to trust the priority received from the PC or the attached device.

upvoted 3 times

Anas_Ahmad 9 months ago

Switch(config)#int g0/1
Switch(config-if)#switchport priority extend trust
^
% Invalid input detected at '^' marker

upvoted 2 times

jibon_22 9 months, 1 week ago

"D" is 100% correct.
You are not instructed to overwrite the priority received from the phone's access port. Just trust the priority received and transmit data with the same priority.
A tricky question to understand.

upvoted 3 times

Etidic 10 months, 4 weeks ago

Selected Answer: B

"switchport priority extend
{cos value | trust}

Set the priority of data traffic received from the Cisco IP Phone access port:

•cos value—Configure the phone to override the priority received from the PC or the attached device with the specified CoS value. The value is a number from 0 to 7, with 7 as the highest priority. The default priority is cos 0."

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_44_se/configuration/guide/scg/swvoip.html#wp1033848

upvoted 1 times

dick3311 11 months ago

But he ask same priority?so maybe is B

upvoted 5 times

everchosen13 11 months, 3 weeks ago

The given answer is incorrect.
C is the answer the correct Answer
https://community.cisco.com/t5/switching/switchport-priority-extend-cos-0/td-p/1638603

upvoted 1 times

EliasM 11 months, 1 week ago

This will make the IP phone send traffic with no vlan tag. But what about the CoS value?

upvoted 2 times

```
Switch1#show etherchannel summary
Flags:     D - down          P - in port-channel
           I - stand-alone   s - suspended
           H - Hot-standby (LACP only)
           R - Layer3        S - Layer2
           U - in use        f - failed to allocate aggregator
           u - unsuitable for bundling
           w - waiting to be aggregated
           d - default port

Number of channel-groups in use: 1
Number of aggregators:                 1
Group Port-channel Protocol         Ports
------+-------------+-------------+-----------------------
1          Pol (SD)          LACP       Fa0/2 (I) Fa0/1 (I)
```

```
Switch1#show run
Building configuration…
interface Port-channel1
!
interface FastEthernet0/1
   channel-group 1 mode passive
!
interface FastEthernet0/2
  channel-group 1 mode passive
```

```
Switch2#show run
Building configuration…
interface Port-channel1
!
interface FastEthernet0/1
   channel-group 1 mode passive
!
interface FastEthernet0/2
  channel-group 1 mode passive
```

Refer to the exhibit. Which change to the configuration on Switch2 allows the two switches to establish an EtherChannel?

A. Change the LACP mode to desirable

B. Change the protocol to PAgP and use auto mode

C. Change the LACP mode to active

D. Change the protocol to EtherChannel mode on

Correct Answer: *C*

Community vote distribution

C (100%)

Nikisan 1 month, 1 week ago

Selected Answer: C

LACP:-
Active + Active = Ether Channel
Active + Passive = Ether Channel
Passive + Active = Ether Channel
Passive + Passive = No

upvoted 1 times

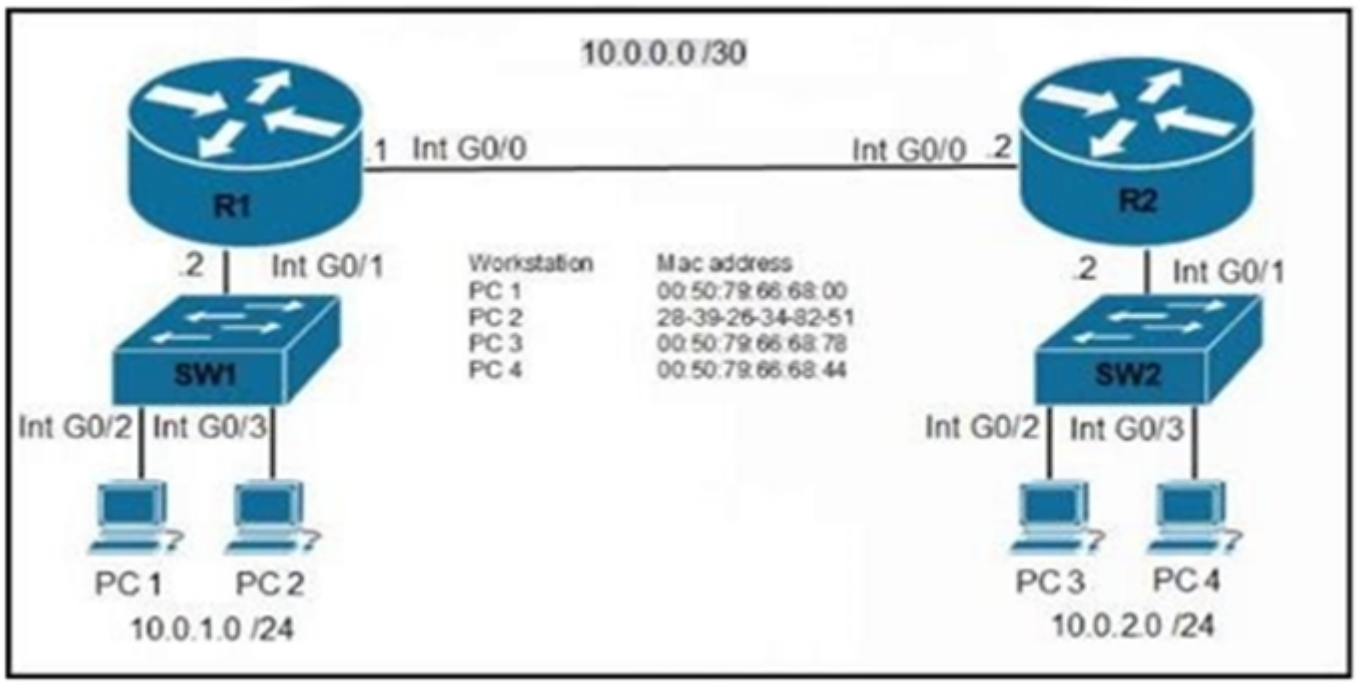
[Removed] 3 months ago

Selected Answer: C

C is correct.

upvoted 1 times

Question #293 *Topic 1*



Refer to the exhibit. An engineer must configure the interface that connects to PC1 and secure it in a way that only PC1 is allowed to use the port. No VLAN tagging can be used except for a voice VLAN. Which command sequence must be entered to configure the switch?

A. SW1(config-if)#switchport mode dynamic auto SW1(config-if)#switchport port-security SW1(config-if)#switchport port-security violation restrict

B. SW1(config-if)#switchport mode nonegotiate SW1(config-if)#switchport port-security SW1(config-if)#switchport port-security maximum 1

C. SW1(config-if)#switchport mode access SW1(config-if)#switchport port-security SW1(config-if)#switchport port-security mac-address 0050.7966.6800

D. SW1(config-if)#switchport mode dynamic desirable SW1(config-if)#switchport port-security mac-address 0050.7966.6800 SW1(config-if)#switchport port-security mac-address sticky

Correct Answer: *C*

Community vote distribution

C (100%)

everchosen13 Highly Voted 11 months, 3 weeks ago

Given answer is correct.

upvoted 6 times

anchilinq Most Recent 3 days, 19 hours ago

why is b wrong?

upvoted 1 times

[Removed] 3 months ago

Selected Answer: C

Answer C is correct

upvoted 1 times

BeautifulSmile 4 months ago

Answer is correct.

upvoted 2 times

robbydice 6 months, 2 weeks ago

The key phrase is "in a way that only PC1 is allowed to use the port" that means no VLAN tagging, no trunking. Therefore in that case the best way to configure the port with access to PC1 is to configure it with command SW1# switchport mode access ....

upvoted 3 times

Silencer 7 months ago

correct

upvoted 4 times

tyuio 9 months, 1 week ago

Given answer is correct.

upvoted 3 times

Question #294 *Topic 1*

Which protocol must be implemented to support separate authorization and authentication solutions for wireless APs?

A. RADIUS

B. TACACS+

C. 802.1X

D. Kerberos

Correct Answer: *A*

Community vote distribution

B (98%)

Ronild Highly Voted 1 year ago

Selected Answer: B

Correct: B

Authentication and Authorization
RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.

TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.

Source: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

upvoted 19 times

Isuzu 4 months, 1 week ago

but the question state "SEPARATE authorization and authentication solutions...."

upvoted 1 times

wakaish Most Recent 1 week, 1 day ago

RADIUS (Remote Authentication Dial-In User Service) is commonly used for both authentication and authorization in networking environments. It allows for separate authentication (verifying the identity of the user or device) and authorization (determining what the authenticated user or device is allowed to access) processes. This is important in scenarios like wireless networks where you want to control who can access the network and what resources they can access.

upvoted 1 times

mayra20 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

BAT47 2 months, 2 weeks ago

Selected Answer: B

correct answer: B

upvoted 1 times

[Removed] 3 months ago

Selected Answer: B

B is correct : TACACS+

upvoted 1 times

Jorro99404 4 months ago

Selected Answer: B

B. TACACS+

upvoted 1 times

Isuzu 4 months ago

Guys... referring to the below link, the correct answer might RADIUS for sure.
https://www.geeksforgeeks.org/difference-between-tacacs-and-radius/

upvoted 1 times

Jorro99404 4 months ago

Nope. Read it again
upvoted 2 times

BeautifulSmile 4 months ago
The giving answer is wrong. TACACS+ is the correct answer.
upvoted 2 times

FALARASTA 4 months, 3 weeks ago
Sometimes after vote the moderators need to change the answers to the correct ones. This is clearly B
upvoted 2 times

therandomjoke 5 months ago
Selected Answer: B
maybe Answer A its True <> the question asks ---> " to support separate Author and Authent ? so we need to implement the Radius to merge them and Support them..... them... them.... them.... or maybe not.
upvoted 2 times

elixirwell 5 months, 2 weeks ago
Selected Answer: B
TACACS+ is the correct answer.
Source: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html
upvoted 1 times

Matalongo 5 months, 3 weeks ago
B is the correct answer
upvoted 1 times

sbnpj 5 months, 4 weeks ago
Selected Answer: B
I agree B is the correct answer.
upvoted 1 times

linuxlife 6 months ago
Authentication, Authorization, and Accounting are separated in TACACS+.
Authentication and Authorization are combined in RADIUS.
upvoted 3 times

Swiz005 6 months ago
Selected Answer: B
Definitely B
upvoted 1 times

checkoboy88 6 months, 2 weeks ago
Selected Answer: B
tacacs
upvoted 1 times

checkoboy88 6 months, 3 weeks ago
Selected Answer: B
Correct: B
upvoted 1 times

Question #295 *Topic 1*

Which port type supports the spanning-tree portfast command without additional configuration?

A. trunk ports

B. Layer 3 sub interfaces

C. Layer 3 main interfaces

D. access ports

Correct Answer: *D*

Community vote distribution

D (100%)

hasbulla01 Highly Voted 10 months, 1 week ago

only access port should portfast

upvoted 8 times

xbololi Most Recent 2 months, 1 week ago

Everyone in the comments are talking about where to "use" portfast and where to not... The question is not asking you should or not... It asks which one supports "without additional configuration" .

upvoted 1 times

xbololi 2 months, 1 week ago

So answering the correct answer without knowing why won't make you knowledgeable....

upvoted 1 times

xbololi 2 months, 1 week ago

"By default, PortFast is disabled on all switch ports. You can configure PortFast as a global default, affecting all switch ports with a single command. All ports that are configured for access mode (nontrunking) will have PortFast automatically enabled."

upvoted 2 times

[Removed] 3 months ago

Selected Answer: D

Answer D is correct

upvoted 1 times

Tarek70 4 months, 1 week ago

ter the STP forwarding-state immediately or upon a linkup event, thus bypassing the listening and learning states. The PortFast feature is enabled at a port level, and this port can either be a physical or a logical port. When PortFast feature is enabled on a switch or a trunk port, the port immediately transitions to the STP forwarding state.

Though PortFast is enabled the port still participates in STP. If the port happens to be part of topology that could form a loop, the port eventually transitions into STP blocking mode

upvoted 2 times

iMo7ed 7 months ago

Selected Answer: D

Answer is D

upvoted 4 times

Murphy2022 11 months, 3 weeks ago

Accessports don't need further configuration in order to send the portfast command
Ciscologic

upvoted 3 times

MolisePan 1 year ago

who knows why?

upvoted 1 times

RougePotatoe 10 months, 3 weeks ago

That is because you should only use port fast command on access ports. If you used it on a trunk port it could cause issues with spanning tree since it skips the listening and learning stages.

upvoted 8 times

```
SW1#show spanning-tree vlan 30

VLAN0030
Spanning tree enabled protocol rstp
Root ID    Priority             32798
           Address              0025.63e9.c800
           Cost                 19
           Port                 1 (FastEthernet 2/1)
           Hello Time           2 sec
           Max Age              30 sec
           Forward Delay        20 sec

[Output suppressed]
```

Refer to the exhibit. What are two conclusions about this configuration? (Choose two.)

A. The spanning-tree mode is Rapid PVST+

B. This tea root bridge

C. The spanning-tree mode is PVST+

D. The designated port is FastEthernet 2/1

E. The root port is FastEthernet 2/1

Correct Answer: *AE*

Community vote distribution

AE (100%)

marle77 1 week, 2 days ago

There is no root cost 19 in RAPID PVST+ so it must be C & E

upvoted 1 times

Shanku97 3 weeks ago

CAN ANYONE EXPLAIN WHY IT IS A RAPID PVST+?

upvoted 1 times

ananinamia 2 weeks, 5 days ago

No idea! Maybe Vlan30?

upvoted 1 times

iMo7ed 7 months ago

Selected Answer: AE

A & E are correct

upvoted 3 times

Eminn 10 months, 3 weeks ago

AE is correct answer

upvoted 2 times

DoBronx 10 months, 3 weeks ago

why do we know it is a root port

upvoted 1 times

Etidic 10 months, 4 weeks ago

Selected Answer: AE

The answer is correct

upvoted 1 times

DoBronx 10 months, 3 weeks ago

why do we know its a root port

upvoted 1 times

skeah 10 months, 1 week ago

It's trick, this is because the cost is 19,the only way to have 19 has cost is with a 100Mb/s link

upvoted 1 times

GhostWolf 10 months, 1 week ago

I don't understand.

upvoted 1 times

cuenca73 7 months ago

Because it means that a direct link to the root bridge is trough that port. In this case, it can be deduced that the way to the root bridge is directly after this 100 Mbps link

upvoted 2 times

ananinamia 2 weeks, 5 days ago

Agree... If root bridge, it costs zero

upvoted 1 times

Question #297 *Topic 1*

A Cisco engineer must configure a single switch interface to meet these requirements:

☞ Accept untagged frames and place them in VLAN 20

Accept tagged frames in VLAN 30 when CDP detects a Cisco IP phone

▪

Which command set must the engineer apply?

A. switchport mode dynamic desirable switchport access vlan 20 switchport trunk allowed vlan 30 switchport voice vlan 30

B. switchport mode access switchport access vlan 20 switchport voice vlan 30

C. switchport mode dynamic auto switchport trunk native vlan 20 switchport trunk allowed vlan 30 switchport voice vlan 30

D. switchport mode trunk switchport access vlan 20 switchport voice vlan 30

Correct Answer: *D*

Community vote distribution

B (85%) Other

foreach Highly Voted 1 year ago

Selected Answer: B

B should be the answer.
With D, the interface operates in trunk mode. So the access configuration is not taken into account and the vlan 20 will be tagged.

upvoted 14 times

Etidic Highly Voted 10 months, 4 weeks ago

Selected Answer: B

The answer is B.
The data vlan is connected to the IP phone. Data VLANs connected to the IP phones are untagged by default.

https://www.practicalnetworking.net/stand-alone/voice-vlan-auxiliary-vlan/

https://docs.nvidia.com/networking-ethernet-software/cumulus-linux-40/Layer-2/Link-Layer-Discovery-Protocol/Voice-VLAN/

The IP phone connected to a switchport should learn its vlan using cdp. To configure this, the command is "switchport voice Vlan 30"

upvoted 7 times

Etidic 10 months, 4 weeks ago

Also from the options provided, only B is configured as an access port.
Cisco recommends using an access for for Voice VLAN configuration on a switchport. Pls note that this statement doesn't make a trunk port configuration impossible but I do you think Cisco would choose an answer that contradicts their recommendations?

"Voice VLAN Configuration Guidelines These are the voice VLAN configuration guidelines: • You should configure voice VLAN on switch access ports; voice VLAN is not supported on trunk ports. Note Voice VLAN is only supported on access ports and not on trunk ports, even though the configuration is allowed."

Cisco
https://www.cisco.com › scgPDF
Configuring Voice VLAN

upvoted 2 times

wakaish Most Recent 1 week, 1 day ago

switchport mode access switchport access vlan 20 switchport voice vlan 30

Explanation:

switchport mode access is used to set the switchport to access mode, which allows untagged frames to enter the VLAN specified by switchport access vlan 20.

switchport access vlan 20 assigns untagged frames to VLAN 20.

switchport voice vlan 30 configures the voice VLAN for Cisco IP phones. This command ensures that tagged frames detected by CDP from a Cisco IP phone will be placed in VLAN 30.

Option B meets both of the specified requirements.

upvoted 1 times

shumps 1 month, 1 week ago

please the answer is B, its a true example of a ip phone.

upvoted 1 times

xbololi 2 months, 3 weeks ago

Voice vlan works at access... No trunking for that port.

upvoted 1 times

Jorro99404 4 months ago

Selected Answer: B

They want UNTAGGED VLAN -> access port

upvoted 2 times

dropspablo 4 months, 1 week ago

BBBBBBBB

upvoted 1 times

king_oat 4 months, 2 weeks ago

wow a lot of these answers suck. cmon exam topics

upvoted 2 times

omikun 4 months, 3 weeks ago

answer B

upvoted 1 times

Webfat 6 months, 3 weeks ago

My answer was C, this was chatGTP answer when I asked why it can't be C
The command set in option C is not correct because it includes "switchport mode dynamic auto," which would cause the interface to become a trunk port if the neighboring device is set to trunk mode.

In this scenario, the requirement is to accept untagged frames in VLAN 20 and tagged frames in VLAN 30 when a Cisco IP phone is detected. Therefore, the interface should be configured as an access port in VLAN 20 and a voice VLAN should be configured for VLAN 30. The command set that meets these requirements is option B:

switchport mode access
switchport access vlan 20
switchport voice vlan 30
Option A is incorrect because it sets the interface to dynamic desirable mode, which could result in the interface becoming a trunk port if the neighboring device is set to trunk or dynamic auto mode. It also allows VLAN 30 on the access port, which is not required.

Option D is incorrect because it sets the interface to trunk mode, which is not necessary for this scenario.

upvoted 4 times

DB_Cooper 7 months, 2 weeks ago

Selected Answer: C

untagged. so native vlan 20. native vlans allow frames to pass untagged

upvoted 1 times

TechJ 3 months, 2 weeks ago

I thought it was C as well, but I guess the "allowed" is missing in the command?

upvoted 1 times

linuxlife 6 months ago

but there is no allow native vlan command from C..so its wrong

upvoted 2 times

marti28052 7 months, 3 weeks ago

I think is C, you must place the intagged frames at VLAN 20.

upvoted 2 times

marti28052 7 months, 3 weeks ago

Sorry, B is correct, the key word "native" apply to the trunk.

upvoted 2 times

jnanofrancisco 8 months ago

B is the correct one.

upvoted 1 times

EthanhuntMI6 8 months, 1 week ago

Selected Answer: D

Definitely not D.

upvoted 1 times

leooel 9 months ago

Selected Answer: B

B is correct

upvoted 2 times

everchosen13 11 months, 3 weeks ago

I believe it is B due to the fact that the ip phone is a factor here.
Remember access ports support untagged data traffic.
Don't be fooled by the native vlan in C

upvoted 2 times

creaguy 11 months, 3 weeks ago

I think C & D should work. I had to add "switchport trunk encapsulation dot1q" for d to work. So the best answer I say is C.

interface GigabitEthernet1/0/46
switchport trunk native vlan 20
switchport trunk allowed vlan 30
switchport voice vlan 30
spanning-tree portfast
!
interface GigabitEthernet1/0/47
switchport access vlan 20
switchport trunk encapsulation dot1q
switchport mode trunk
switchport voice vlan 30
spanning-tree portfast

It cannot be B. because it has to accept tagged frames and needs a trunk statement.

upvoted 1 times

Question #298 *Topic 1*

What does a switch use to build its MAC address table?

A. VTP

B. DTP

C. ingress traffic

D. egress traffic

Correct Answer: *C*

Community vote distribution

C (100%)

shumps 1 month, 1 week ago

ingress traffic simply means incoming traffic

upvoted 1 times

abdelkader163 1 month, 4 weeks ago

Selected Answer: C

The answer given is correct
The switch looks at the source address of an incoming frame before it looks at the destination address. It's the source MAC addresses that are used to build the all-important MAC address table.

upvoted 1 times

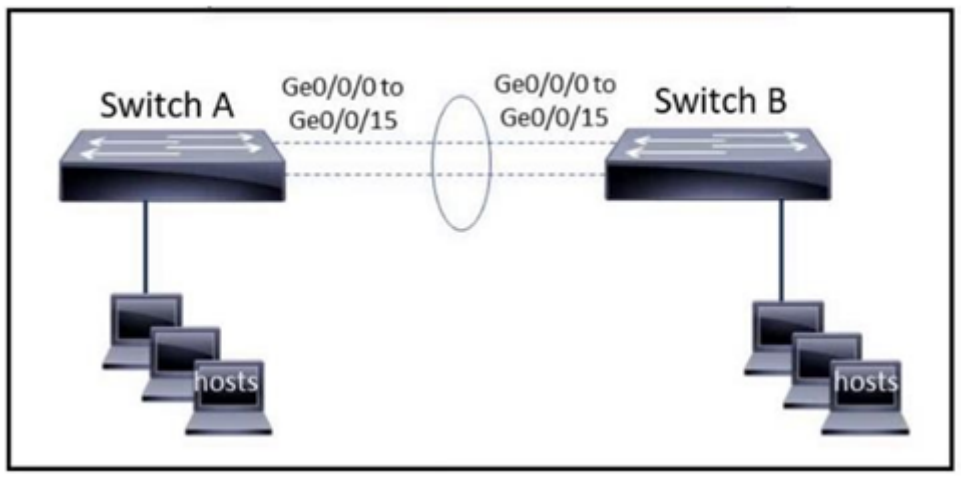
[Removed] 3 months ago

Selected Answer: C

Given answer is correct

upvoted 2 times

Question #299 *Topic 1*



Refer to the exhibit. The EtherChannel is configured with a speed of 1000 and duplex as full on both ends of channel group 1. What is the next step to configure the channel on switch A to respond to but not initiate LACP communication?

A. interface range gigabitethernet0/0/0-15 channel-group 1 mode on

B. interface range gigabitethernet0/0/0-15 channel-group 1 mode desirable

C. interface port-channel 1 channel-group 1 mode auto

D. interface port-channel 1 channel-group 1 mode passive

Correct Answer: *D*

Community vote distribution

D (72%) A (28%)

laurvy36 Highly Voted 7 months, 1 week ago

Selected Answer: D

Mode Passive:
The mode places a port into a passive negotiating state, in which the port RESPONDS to LACP packets that it receives, but DOES NOT initiate protocol negotiation.

upvoted 8 times

Yaqub009 Highly Voted 7 months, 1 week ago

Selected Answer: D

This questions say that "SW A RESPOND, BUT NOT START LACP COMMUNICATION". Ask that "WHICH LACP MODE DOESN`T START COMMUNICATION?"

LACP modes -> Active/Passive.
Active -> Start Communication
Passive -> Doesn`t start Communication.

Correct Answer is "D".

upvoted 5 times

Shanku97 Most Recent 3 weeks ago

i can understand why this is passive but what is this port channel 1?

upvoted 1 times

raul_kapone 4 weeks, 1 day ago

Selected Answer: D

Like the guys said, the correct answer is D.
In the "On mode" LACP packets are NOT EXCHANGED, so there is NO LACP COMMUNICATION. This mode forces the interface to channel without LACP.

upvoted 1 times

shumps 1 month, 1 week ago

if you can understand that LACP is Active/ passive we can move forward nicely. A is completely wrong and must not be compared with. thank you

upvoted 1 times

kyleptt 1 month, 2 weeks ago

This has to be D

upvoted 1 times

shumps 2 months ago

LACP is the give away price for D

upvoted 1 times

[Removed] 3 months ago

Selected Answer: D

Answer D

upvoted 1 times

perri88 3 months ago

All answers are wrong since:
it's not A because Static etherchannel uses "on mode".
However, the command on D should be:
interface range gigabitethernet0/0/0-15
channel-group 1 mode passive

upvoted 1 times

Hope_12 4 months, 1 week ago

Selected Answer: D

" respond to but not initiate LACP communication"
Should be passive mode interface of LACP which is just waiting for LACP communication.
Answer is D.

upvoted 1 times

Hope_12 4 months, 1 week ago

Also mode on only works with mode on.
Desirable and on/Active and on will not work.

upvoted 2 times

KeerthiPraveen 4 months, 2 weeks ago

Selected Answer: A

A is correct....D states LACP

upvoted 2 times

soRwatches 5 months, 2 weeks ago

Selected Answer: A

A is correct, Invalid command for D.

upvoted 4 times

[Removed] 4 months, 1 week ago

I think the correct answer is D as the questions mentions LACP that uses active or passive. Static etherchannel uses "on mode".
However, the command should be:
interface range gigabitethernet0/0/0-15
channel-group 1 mode passive

upvoted 5 times

linuxlife 6 months ago

MODE ON: Mode that forces the LAN port to channel unconditionally. In the on mode, a usable EtherChannel exists only when a LAN port group in the on mode is connected to another LAN port group in the on mode. Because ports configured in the on mode do not negotiate, there is no negotiation traffic between the ports. You cannot configure the on mode with an EtherChannel protocol. If one end uses the on mode, the other end must also.
MODE PASSIVE:
LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. (Default)

upvoted 3 times

Naghini 7 months, 3 weeks ago

Selected Answer: D

LACP = Active/Passive.
Answer is D.

upvoted 4 times

Sdiego 7 months, 4 weeks ago

Selected Answer: A

It does not specify LACP negotiation, but communication.
Sounds like it just want the Etherchannel set up - ON mode -

upvoted 1 times

country_rooted 5 months ago

the last couple words do mention LACP and that it simply wants a response. so the ans must be passive. ON can only work with ON

upvoted 3 times

rivera82 9 months, 1 week ago

Selected Answer: D

Passive—Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.

upvoted 3 times

dick3311 10 months, 3 weeks ago

Selected Answer: A

not initiate ==no negotiate

upvoted 2 times

dick3311 10 months, 3 weeks ago

sorry , I agree with Customexit
ans shoud be D

upvoted 3 times

Question #300 *Topic 1*

Which command entered on a switch configured with Rapid PVST+ listens and learns for a specific time period?

A. switch(config)#spanning-tree vlan 1 priority 4096

B. switch(config)#spanning-tree vlan 1 hello-time 10

C. switch(config)#spanning-tree vlan 1 max-age 6

D. switch(config)#spanning-tree vlan 1 forward-time 20

Correct Answer: *D*

Community vote distribution

D (83%) C (17%)

foreach Highly Voted 1 year ago

Strange question... In Rapid-PVST+, there's no listening state anymore

upvoted 8 times

Bonesaw 1 year ago

It says the forward delay timer has a listening and learning state here: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/layer2/503_U1_1/Cisco_n3k_layer2_config_gd_503_U1_1_chapter7.html#con_1205111

upvoted 10 times

g_mindset 1 year ago

Thank you, was getting confused already.

upvoted 2 times

mzu_sk8 10 months ago

I belive it is used for backward compatibility to a old switch that only uses STP

upvoted 3 times

xbololi Most Recent 2 months, 1 week ago

Selected Answer: D

Answer D explanation, it is a backup configuration but it still valid... "Determines how long each of the listening and learning states last before the port begins forwarding. This timer is generally not used by the protocol but is used as a backup. The default is 15 seconds, and the range is from 4 to 30 seconds."

upvoted 3 times

fmaquino 2 months, 3 weeks ago

Selected Answer: D

D seems correct

upvoted 1 times

Isuzu 4 months ago

Selected Answer: C

The maximum age timer controls the maximum time that a switch port will wait for a BPDU (Bridge Protocol Data Unit) from the root bridge before declaring the current root bridge as lost and initiating a new election process.

Option A (Wrong) configures the priority of the switch for a specific VLAN.
Option B (Wrong) configures the hello time for STP messages in the network.
Option D (Wrong) configures the forwarding delay time for STP.

upvoted 1 times

FALARASTA 4 months, 3 weeks ago

Gather here and explain to me why D and not C

upvoted 1 times

FALARASTA 4 months, 3 weeks ago

I now understand. The command "spanning-tree vlan 1 max-age 6" is used to configure the maximum age timer for the Spanning Tree Protocol (STP) on VLAN 1. The "max-age" timer controls the maximum time that a switch port will wait for a BPDU (Bridge Protocol Data Unit) from the root bridge before declaring the current root bridge as lost and initiating a new election process.

upvoted 1 times

liviuml 5 months ago

Selected Answer: D

Confirm write answer D.
Search "Rapid PVST+ Protocol Timers" in following link:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html
Regards,

upvoted 1 times

Silencer 6 months, 1 week ago

C. switch(config)#spanning-tree vlan 1 max-age 6
Explanation:
The max-age parameter controls the maximum age of STP messages in the network, which is the maximum amount of time that a switch will retain information about the network topology before discarding it. By default, the max-age is set to 20 seconds. However, in Rapid PVST+, the max-age can be set as low as 6 seconds to allow for faster convergence.

Option A sets the priority of the switch for a specific VLAN. This does not affect the listen and learn time period.

Option B sets the hello time for STP messages in the network. This does not affect the listen and learn time period.

Option D sets the forwarding delay time for STP. This does not affect the listen and learn time period.

upvoted 2 times

Dhruv3390 8 months, 1 week ago

Forward time : Determines how long each of the listening and learning states last before the port begins forwarding.

Switch(config)# [no] spanning-tree vlan vlan_ID forward-time forward_time
Configures the forward time of a VLAN. The forward_time value can be from 4 to 30 seconds.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/15-02SG/configuration/guide/config/spantree.html#56177

upvoted 1 times

Question #301 *Topic 1*

What must a network administrator consider when deciding whether to configure a new wireless network with APs in autonomous mode or APs running in cloud- based mode?

A. Autonomous mode APs are less dependent on an underlay but more complex to maintain than APs in cloud-based mode.

B. Cloud-based mode APs relay on underlays and are more complex to maintain than APs in autonomous mode.

C. Cloud-based mode APs are easy to deploy but harder to automate than APs in autonomous mode.

D. Autonomous mode APs are easy to deploy and automate than APs in cloud-based mode.

Correct Answer: *A*

freeknowledge123 Highly Voted 8 months, 1 week ago

typical voodo question of cisco: autonomous AP require a network infrastructure (underlay) to function, but not to the same degree as AP since they don't use CAPWAP, they don't rely on central controller and require more knowledge to maintain (complexity).
the other answer don't seem that incorrect to me, but option A is the more correct.

upvoted 12 times

shiv3003 Most Recent 4 months, 3 weeks ago

I go for B

upvoted 1 times

FALARASTA 4 months, 3 weeks ago

Atonomous: Having the ability to gevern itself.

upvoted 2 times

realneal92 6 months, 2 weeks ago

In autonomous mode, each AP operates independently and does not require a central controller. Configuration changes and firmware updates must be made manually on each AP. In contrast, cloud-based mode involves APs that operate under the control of a centralized controller located in the cloud. In this mode, configuration changes and firmware updates are pushed from the cloud to the APs, and the controller provides a centralized view of the network.

When deciding which mode to deploy, the network administrator must consider the dependencies of each mode. In autonomous mode, the APs are less dependent on the underlying network infrastructure but require more manual maintenance, which may be more complex for a large number of APs. In cloud-based mode, the APs rely on the underlying network infrastructure and require more complex maintenance for the centralized controller, but provide easy deployment and automation for a large number of APs.

Therefore, the correct answer to this question is option B: "Cloud-based mode APs rely on underlays and are more complex to maintain than APs in autonomous mode."

upvoted 2 times

dropspablo 1 month, 2 weeks ago

Answer is A. APs in cloud-based mode are simpler to configure, see what the Official CISCO Guide says: """"Cisco Meraki APs can be deployed automatically (deployed automatically), after registering in the Meraki cloud. Each AP on power up will contact the cloud and configure itself. From there, you can manage the AP through the Meraki cloud dashboard. (OCG Wendell Odom v1)""""

upvoted 1 times

Question #302 *Topic 1*

When a switch receives a frame for an unknown destination MAC address, how is the frame handled?

A. flooded to all ports except the origination port

B. forwarded to the first available port

C. broadcast to all ports on the switch

D. inspected and dropped by the switch

Correct Answer: *A*

freeknowledge123 8 months, 1 week ago

easy question, switch forwards frame when the dest is unknown to all other ports.

upvoted 3 times

Question #303 *Topic 1*

Which state is bypassed in Rapid PVST+ when PortFast is enabled on a port?

A. blocking

B. forwarding

C. learning

D. discarding

Correct Answer: *C*

_mva 1 month, 3 weeks ago

There is no listening in RSTP. The port moves directly to forwarding by bypassing learning.

upvoted 2 times

zezc 4 months, 2 weeks ago

Forwarding is correct

upvoted 2 times

beerbisceps1 5 months, 1 week ago

don't understand the question. in RSTP the transition states are discarding, learning and forwarding. I am not even sure if this question is brain dumped properly...

upvoted 1 times

beerbisceps1 5 months, 1 week ago

blocking and listening from STP are replaced by discarding in RSTP

upvoted 1 times

freeknowledge123 8 months, 1 week ago

weird question, when portfast is enabled two state are bypassed, discarding and learning in RSTP, i guess a port can be blocked (discarding) in RSTP but it can never be in the learning state.

upvoted 1 times

Question #304 *Topic 1*

What happens when a switch receives a frame with a destination MAC address that recently aged out?

A. The switch floods the frame to all ports in all VLANs except the port that received the frame.

B. The switch floods the frame to all ports in the VLAN except the port that received the frame.

C. The switch references the MAC address aging table for historical addresses on the port that received the frame.

D. The switch drops the frame and learns the destination MAC address again from the port that received the frame.

Correct Answer: *B*

Community vote distribution

B (73%) A (27%)

DoBronx Highly Voted 10 months, 3 weeks ago

question is trying to trick you. It's still asking about an unknown destination MAC address essentially. Answer given is correct

upvoted 8 times

Godfather2022 7 months, 2 weeks ago

You absolutely right @DoBronx.Cisco always trick people. Read the question more than once.

upvoted 2 times

Da_Costa Most Recent 1 day, 2 hours ago

Selected Answer: B

A and B are not the same but B is correct

upvoted 1 times

wakaish 1 week, 1 day ago

Once an entry ages out, the switch removes it from the table, and the frame is treated as an unknown unicast.

upvoted 1 times

raul_kapone 4 weeks ago

Selected Answer: B

A is not the same as B.
When you create a VLAN on a switch and you send a broadcast into one of them, this broadcast will reach only on the members of the respective VLAN (which this switch belongs), not on all members of all the VLANs.

Recall: Each VLAN is typically its own broadcast domain.

upvoted 1 times

Da_Costa 1 month, 3 weeks ago

Selected Answer: A

Aand B look the same

upvoted 1 times

xbololi 2 months, 3 weeks ago

"all" /"the" sadly

upvoted 1 times

Lokylax 4 months, 3 weeks ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

FALARASTA 4 months, 3 weeks ago

This is simply an unknown MAC

upvoted 1 times

Vikramaditya_J 4 months, 3 weeks ago

When the switch receives a frame for a destination MAC address which isn't listed in its CAM table, it floods the frame to all LAN ports of the "same VLAN", except the port where it received the frame. So, the option "B" is correct.

upvoted 1 times

Vikramaditya_J 4 months, 3 weeks ago

When the switch receives a frame for a MAC destination address not listed in its CAM table, it floods the frame to all LAN ports of the "same VLAN" except the port that received the frame. So, the option B is correct.

upvoted 1 times

moise_amo 7 months, 2 weeks ago

Selected Answer: B

each vlan represent it's own brodcast domain so yhe switch can't floods it in other vlan. it must be a singular vlan

upvoted 2 times

Godfather2022 7 months, 2 weeks ago

B is the correct answer.

upvoted 1 times

kobisiva 7 months, 3 weeks ago

B is not correct because when the destination mac address is not found in the mac address table the switch floods the frame to all VLANs.

upvoted 1 times

freeknowledge123 8 months, 1 week ago

goes to show that you need to read all question carefully to fully prepare for the exam.

upvoted 2 times

Anas_Ahmad 9 months ago

Selected Answer: B

the switch flood to all ports in same Vlan B is right

upvoted 1 times

battlefate 9 months, 1 week ago

Selected Answer: B

B is correct.
Switch only forward all frame to the same broadcast domain.

upvoted 2 times

hasbulla01 10 months, 1 week ago

Selected Answer: A

A and B is same

upvoted 2 times

Inceptenet 9 months ago

It's not the same. A. VLANs -- B. VLAN

upvoted 7 times

Question #305 *Topic 1*

What is a function of store-and forward switching?

A. It reduces latency by eliminating error checking within the frame

B. It produces an effective level of error-free network traffic using CRCs.

C. It buffers frames and forwards regardless of errors within the frames.

D. It forwards a frame by checking only the destination MAC address

Correct Answer: *B*

freeknowledge123 Highly Voted 8 months, 1 week ago

store and forward: checks the whole frame
frament free mode: checks the first 64 byte (no crc)
cut through: checks only the destination

upvoted 9 times

g_mindset Highly Voted 1 year ago

https://www.tutorialspoint.com/store-and-forward-packet-switching#:~:text=In%20telecommunications%2C%20store%20%E2%88%92%20and%20%E2%88%92,integrity%20of%20the%20data%20packets.

upvoted 7 times

wakaish Most Recent 1 week, 1 day ago

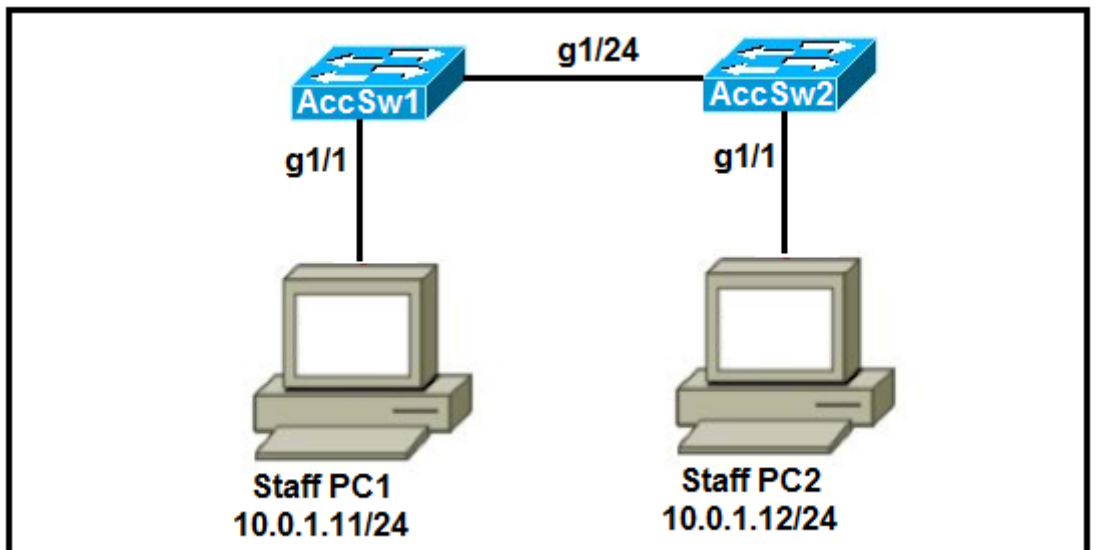
Store-and-forward switching is a switching technique used in networking where a switch receives an entire frame before it forwards it to its destination. During this process, the switch checks the frame for errors, CRC (Cyclic Redundancy Check) being one of the error-checking mechanisms. If the frame is error-free, the switch will store it temporarily in a buffer and then forward it to the appropriate port. If the frame contains errors, it will be discarded rather than forwarded.

upvoted 1 times

shiv3003 4 months, 3 weeks ago

answer is good

upvoted 1 times



AccSw1#sho vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24,
2	IT-Support	active	Fa0/1
3	Servers	active	Fa0/2
11	Staff	active	Gigi1/1
12	Guests	active	Gigi1/2

---
output suppressed

Refer to the exhibit. Switch AccSw1 has just been added to the network along with PC2. All VLANs have been implemented on AccSw2. How must the ports on
AccSw2 be configured to establish Layer 2 connectivity between PC1 and PC2?

A. interface GigabitEthernet1/2 switchport mode access switchport access vlan 2 ! interface GigabitEthernet1/24 switchport mode trunk

B. interface GigabitEthernet1/1 switchport mode access switchport access vlan 11 ! interface GigabitEthernet1/24 switchport mode trunk

C. interface GigabitEthernet1/24 switchport mode trunk switchport trunk allowed vlan 11, 12 ! interface GigabitEthernet1/1 switchport access vlan 11

D. interface GigabitEthernet1/2 switchport mode access switchport access vlan 12 ! interface GigabitEthernet1/24 switchport mode trunk switchport trunk allowed vlan 11, 12

Correct Answer: *B*

Community vote distribution

B (91%) 9%

Etidic Highly Voted 10 months, 4 weeks ago

Selected Answer: B

I imagine that the confusion is the "switchport trunk allowed VLAN 11, 12" command in option C.
Please note that this just a distraction.
As you may have learnt already when you apply the "switchport mode trunk" on an interface it allows all VLANs by default. So by using this command in option B all VLANs 1 - 4094 are allowed over the trunk.
For security reasons, during our network design we tend to remove all vlans and only allow the vlans we desire.
If we apply the command in option C "switchport trunk allowed VLAN 11, 12" it would delete all vlans and only allow VLANs 11 and 12. This means that all other devices or departments who are dependent on this trunk will be cut-off.
One of the biggest blunders sometimes made by beginners is to delete an entire VLAN by overwriting it. Always remember to use the "add" command when adding new VLANs to a trunk already configured for other VLANs.

upvoted 35 times

linuxlife 6 months ago

well explained. this is right.

upvoted 1 times

Etidic 10 months, 4 weeks ago

Reference page 5 in the Cisco document

https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_digital_building_series_switches/software/15-2_5_ex/configuration_guide/b_1525ex_consolidated_cdb_cg/b_1525ex_consolidated_cdb_cg_chapter_0110101.pdf&ved=2ahUKEwjtxrDFlO_6AhW-ADQIHZk1B6QQFnoECA8QBQ&usg=AOvVaw1HVa1ltIBL8EHVJI_H7g8b

upvoted 1 times

splashy Highly Voted 1 year ago

Selected Answer: B

A wrong interface
D wrong interface
C Traffic to/from servers won't be possible as it is tagged (vlan) and not untagged

upvoted 6 times

zFlyingLotusz Most Recent 1 month, 4 weeks ago

Why the heck would a PC use gigabit ports and not FA ports?

upvoted 1 times

BeautifulSmile 4 months ago

Take note of the two PCs. They are in the same vlan, which is Sales. hence, the correct answer is B.

upvoted 1 times

BeautifulSmile 4 months ago

I mean Staff not sales.

upvoted 1 times

binjalala 9 months, 1 week ago

the question asked "How must the ports on AccSw2 be configured?" so the correct answer should be C

upvoted 1 times

korekwsieci 10 months, 2 weeks ago

The question was: how to establish Layer 2 connectivity between PC1 and PC2. So answer C is also correct since the connecion between this two specified host will work just fine.

upvoted 2 times

g_mindset 1 year ago

Selected Answer: C

Answer is C, switchport trunk allowed VLAN 11, 12

upvoted 4 times

Taku2023 5 months, 4 weeks ago

IF you use that command only vlan 11, 12 will be allowed on the trunk. the command override the command "switchport mode trunk"

upvoted 1 times

everchosen13 11 months, 3 weeks ago

You would not need to allow vlan 12 on the trunk to support a connection between two work stations. Both pc's are in the same VLAN. I believe the answer would be B

upvoted 3 times

cyborg7 11 months, 2 weeks ago

Even two wks are not in same VLAN, switchport mode trunk will included in VLANSs

upvoted 1 times

Question #307 *Topic 1*

```
Switch2# show lldp
Global LLDP Information
   Status: ACTIVE
   LLDP advertisements are sent every 30 seconds
   LLDP hold time advertised is 120 seconds
   LLDP interface reinitialization delay is 2 seconds
```

Refer to the exhibit. A network engineer must update the configuration on Switch2 so that it sends LLDP packets every minute and the information sent via LLDP is refreshed every 3 minutes. Which configuration must the engineer apply?

A. Switch2(config)#lldp timer 60 Switch2(config)#lldp tlv-select 180

B. Switch2(config)#lldp timer 60 Switch2(config)#lldp holdtime 180

C. Switch2(config)#lldp timer 1 Switch2(config)#lldp holdtime 3

D. Switch2(config)#lldp timer 1 Switch2(config)#lldp tlv-select 3

Correct Answer: *B*

Step 2	(Optional) **[no] lldp holdtime** *seconds* **Example:** `switch(config)# lldp holdtime 200`	Specifies the amount of time in seconds that a receiving device should hold the information that is sent by your device before discarding it. The range is 10 to 255 seconds; the default is 120 seconds.
Step 4	(Optional) **[no] lldp timer** *seconds* **Example:** `switch(config)# lldp timer 50`	Specifies the transmission frequency of LLDP updates in seconds. The range is 5 to 254 seconds; the default is 30 seconds.

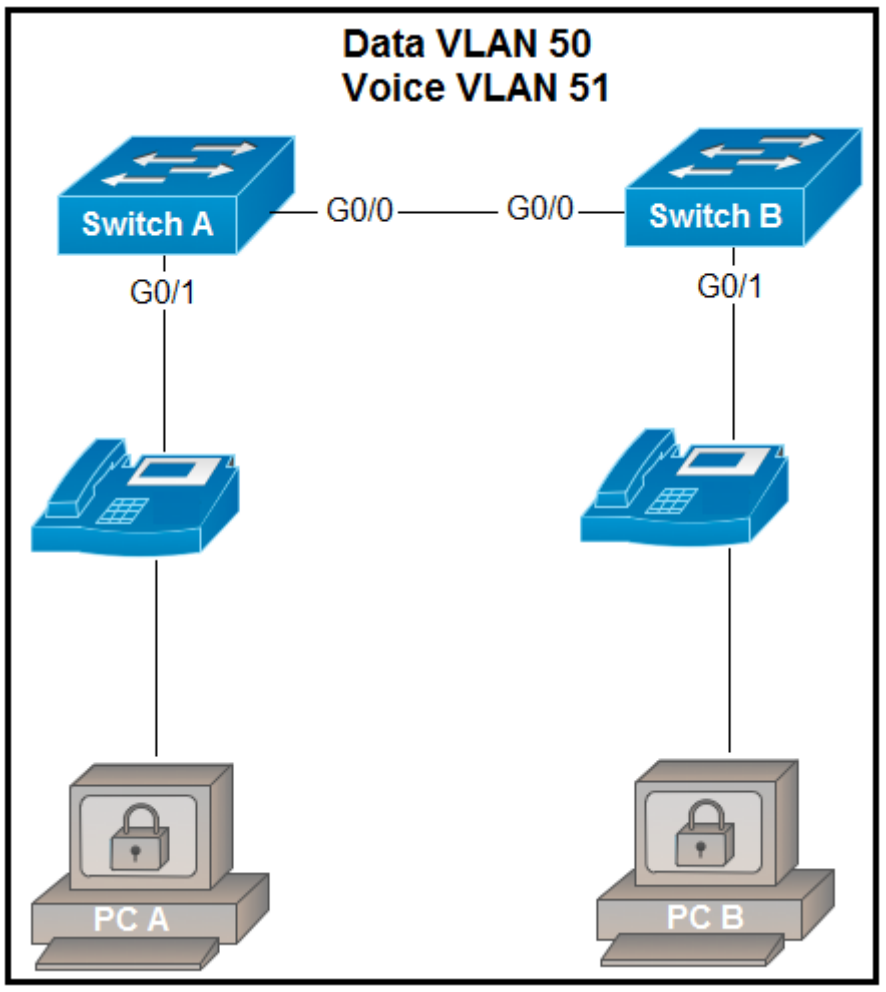
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/system_management/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide/sm_lldp.pdf

Vyncy Highly Voted 3 months, 2 weeks ago
hello beautiful
upvoted 5 times

ananinamia 3 weeks, 6 days ago
i am handsome
upvoted 1 times

ananinamia Most Recent 3 weeks, 6 days ago
hi honey
upvoted 1 times

Question #308 *Topic 1*



Refer to the exhibit. Switch A is newly configured. All VLANs are present in the VLAN database. The IP phone and PC A on Gi0/1 must be configured for the appropriate VLANs to establish connectivity between the PCs. Which command set fulfills the requirement?

A. SwitchA(config-if)#switchport mode access SwitchA(config-if)#switchport access vlan 50 SwitchA(config-if)#switchport voice vlan 51

B. SwitchA(config-if)#switchport mode trunk SwitchA(config-if)#switchport trunk allowed vlan add 50, 51 SwitchA(config-if)#switchport voice vlan dot1p

C. SwitchA(config-if)#switchport mode trunk SwitchA(config-if)#switchport trunk allowed vlan 50, 51 SwitchA(config-if)#mis qos trust cos

D. SwitchA(config-if)#switchport mode access SwitchA(config-if)#switchport access vlan 50 SwitchA(config-if)#switchport voice vlan untagged

Correct Answer: *A*

Community vote distribution

A (100%)

Goh0503 Highly Voted 12 months ago

Answer A

https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/voice-vla

First, we have to create the two VLANs:

SW1(config)#vlan 100
SW1(config-vlan)#name COMPUTER
SW1(config-vlan)#exit

SW1(config)#vlan 101
SW1(config-vlan)#name VOIP
SW1(config-vlan)#exit
Now we can configure the interface:

SW1(config)#interface GigabitEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 100
SW1(config-if)#switchport voice vlan 101
SW1(config-if)#exit
We configure the interface in access mode and use VLAN 100 for the computer. The switchport voice vlan command tells the switch to use VLAN 101 as the voice VLAN.

upvoted 14 times

FALARASTA Most Recent 4 months, 3 weeks ago

Any port configured as trunk should be eliminated first voice is configures in access ports only. The right answer is A

upvoted 1 times

iMo7ed 6 months, 4 weeks ago

Selected Answer: A

It is A

upvoted 1 times

JJY888 7 months ago

There was a question earlier where the correct answer was a truck and not access. This question clears up that confusion. Voice Vlan should be an access port.

upvoted 1 times

Shanku97 3 weeks ago

voice vlan is always access port, any option of voice vlan being trunk should get eliminated at first !!

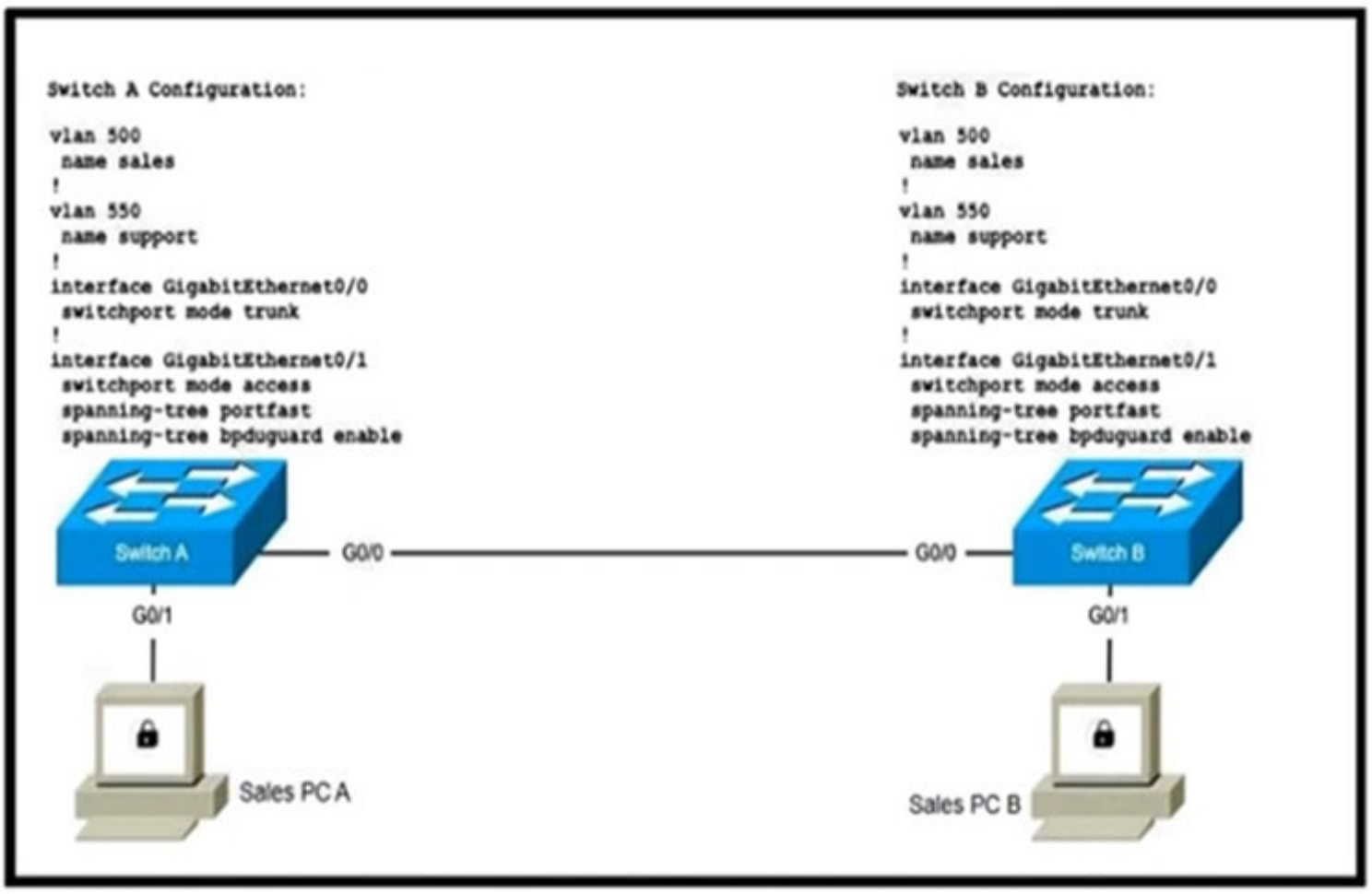
upvoted 1 times

Etidic 10 months, 4 weeks ago

Selected Answer: A

Answer A is correct

upvoted 1 times



Refer to the exhibit. Two new switches are being installed. The remote monitoring team uses the support network to monitor both switches. Which configuration is the next step to establish a Layer 2 connection between the two PCs?

A. SwitchA(config)#interface GigabitEthernet0/1 SwitchA(config-if)#switchport access vlan 500 SwitchB(config)#interface GigabitEthernet0/1 SwitchB(config-if)#switchport access vlan 500

B. SwitchA(config)#interface GigabitEthernet0/1 SwitchA(config-if)#switchport mode trunk SwitchB(config)#interface GigabitEthernet0/1 SwitchB(config-if)#switchport mode trunk

C. SwitchA(config)#interface GigabitEthernet0/0 SwitchA(config-if)#switchport trunk allowed vlan 500, 550 SwitchB(config)#interface GigabitEthernet0/0 SwitchB(config-if)#switchport trunk allowed vlan 500, 550

D. SwitchA(config)#interface GigabitEthernet0/0 SwitchA(config-if)#spanning-tree portfast SwitchA(config-if)#spanning-tree bpduguard enable SwitchB(config)#interface GigabitEthernet0/0 SwitchB(config-if)#spanning-tree portfast SwitchB(config-if)#spanning-tree bpduguard enable

Correct Answer: *A*

Community vote distribution

A (75%) C (25%)

xbololi 2 months, 3 weeks ago

you never want a sales personel get access to support/manager vlan trust me :)

upvoted 1 times

BeautifulSmile 4 months ago

Take note of the Vlan the two PCs belong to. They both belong to Sales which is the Vlan 500 and from the configurations given, you just need to add the sales vlan to established connection between the two PCs. The correct answer is A.

upvoted 1 times

HSong 4 months, 2 weeks ago

A
Please note that the PCs are all for Sales department

upvoted 4 times

Kerrera 5 months, 4 weeks ago

Selected Answer: A

L2 connectivity done : vlans allowed on trunk 1-1005. The next step is to configure the access

upvoted 1 times

Kerrera 5 months, 4 weeks ago

L2 connectivity done : vlans allowed on trunk 1-1005. The next step is to configure the access

upvoted 1 times

Italian 6 months, 1 week ago

Selected Answer: C

Support network has already been configured, for connectivity between the two PCs both vlans should be allowed on the G0/0 interface of both switch

upvoted 1 times

Goena 8 months, 2 weeks ago

Selected Answer: A

It is indeed another tricky question: the support vlan 550 is already configured. So the next step is to configure vlan 500.

upvoted 2 times

Shanku97 3 weeks ago

how is it already configured ?

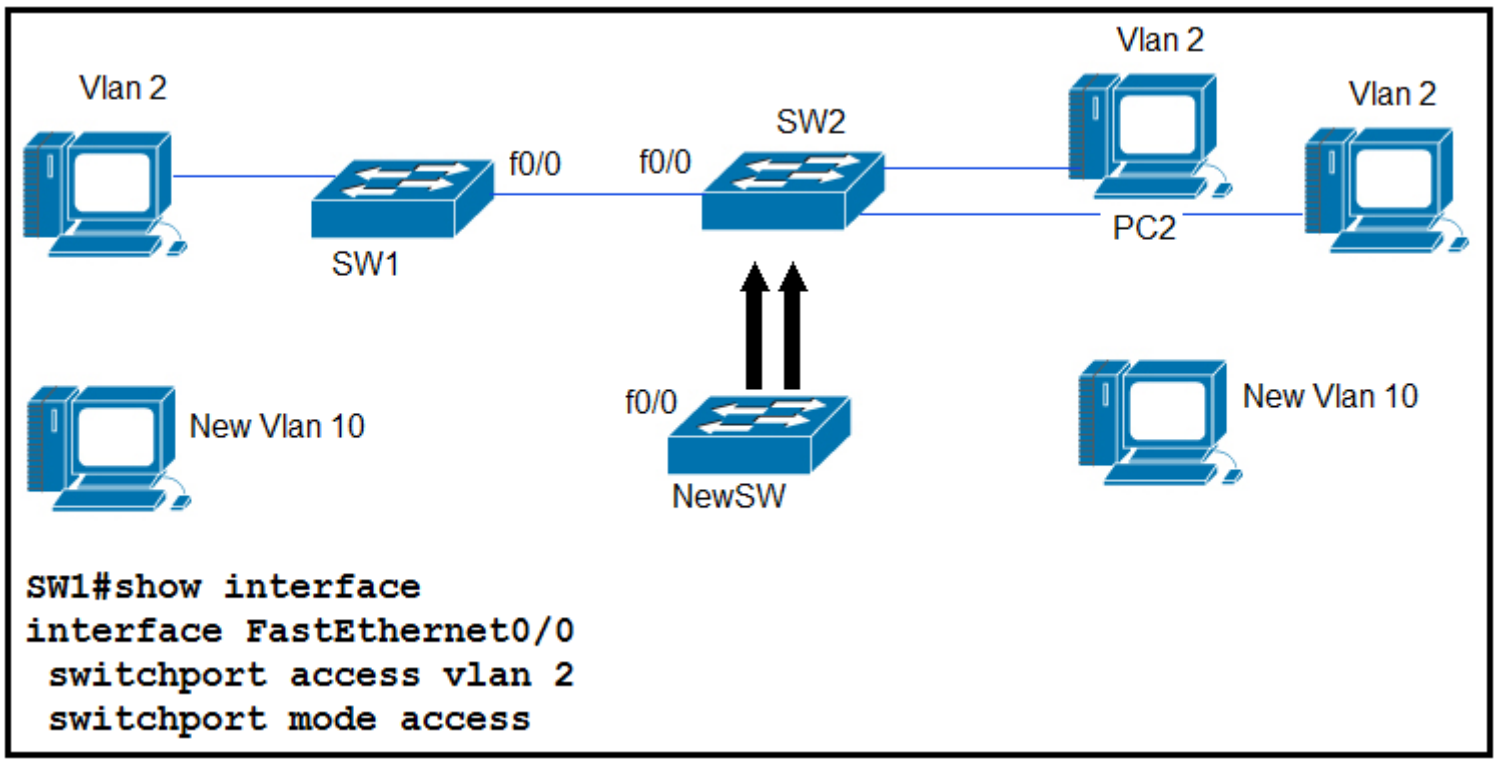
upvoted 1 times

Johan_jelly 9 months, 1 week ago

key word here is next step

upvoted 1 times

Question #310 *Topic 1*



Refer to the exhibit. An engineer is configuring a new Cisco switch, NewSW, to replace SW2. The details have been provided:

☞ Switches SW1 and SW2 are third-party devices without support for trunk ports.

☞ The existing connections must be maintained between PC1, PC2, and PC3.

☞ Allow the switch to pass traffic from future VLAN 10.

Which configuration must be applied?

A. NewSW(config)#interface f0/0 NewSW(config-if)#switchport mode trunk NewSW(config-if)#switchport trunk native vlan 10 NewSW(config-if)#switchport trunk native vlan 10

B. NewSW(config)#interface f0/0 NewSW(config-if)#switchport mode access NewSW(config-if)#switchport trunk allowed vlan 2, 10 NewSW(config-if)#switchport trunk native vlan 2

C. NewSW(config)#interface f0/0 NewSW(config-if)#switchport mode access NewSW(config-if)#switchport trunk allowed vlan 2, 10 NewSW(config-if)#switchport trunk native vlan 10

D. NewSW(config)#interface f0/0 NewSW(config-if)#switchport mode trunk NewSW(config-if)#switchport trunk allowed vlan 2, 10 NewSW(config-if)#switchport trunk native vlan 2

Correct Answer: *D*

Community vote distribution

D (70%) B (30%)

DoBronx Highly Voted 10 months, 3 weeks ago

what is this garbage question

upvoted 46 times

Godfather2022 7 months, 2 weeks ago

Have been trying to configure what is the question is asking for the past 15 minutes but I cant.

upvoted 5 times

freeknowledge123 8 months, 1 week ago

just goes to show the importance of sites like examtopic

upvoted 8 times

andresfjardim Highly Voted 7 months, 2 weeks ago

Selected Answer: D

I tested this in packet tracer, feel free to try it yourselfs, the correct answer is D!

Nothing says that the new switch doesn't allow trunking. It can´t be B, because when you configure the port in access mode it doesn´t evaluate the trunking commands, and access only permits one vlan.

If you have access on one side the vlan comes untagged, for the other side to put this untagged vlan in a native vlan the port needs to be configured as trunk. Also this imposes that in the future to have vlan 10 passing here you would need to replace SW1 to have trunk funcionality or alternatively configure another uplink to pass vlan 10 the same way to new SW.

upvoted 11 times

[Removed] 4 months, 1 week ago

SW1 is already configured in access mode.
NewSW cannot be configured in trunk mode.
In order for the ping to work both sides of the link need to have the same mode (access or trunk) and not one side trunk and the other side access.

upvoted 1 times

e072f83 Most Recent 2 weeks, 1 day ago

Selected Answer: D

Correct answer is D for sure!

upvoted 1 times

Rydaz 4 months, 1 week ago

in switchport mode access : the interface can only carry ONE VLAN on that interface, only exception is with voice

upvoted 2 times

Lokylax 4 months, 3 weeks ago

Selected Answer: D

Answer is D because of future need of vlan 10.

upvoted 2 times

Kerrera 5 months, 4 weeks ago

Selected Answer: D

The question does not talk about the need for connectivity at this time, it only talks about allowing traffic for the future... it will be necessary to install a compatible intermediate switch

upvoted 1 times

oatmealturkey 6 months, 4 weeks ago

Selected Answer: D

B is impossible. An access port can only be assigned to one vlan so the configuration would not work. One exception is that an access port can be assigned to both a data vlan and a voice vlan.

upvoted 5 times

zFlyingLotusz 2 months ago

Ummmmmmm, pretty sure "access vlan" you can enter more than one..

upvoted 1 times

kobisiva 7 months, 3 weeks ago

i'm choose B, for trunk both devices must support for trunk protocal

upvoted 1 times

freeknowledge123 8 months, 1 week ago

why is it B and not C?

upvoted 2 times

Mistwalker 8 months, 3 weeks ago

Selected Answer: B

It's B. Both A and D immediately configure a trunk port to a switch that the question clearly says doesn't support trunk ports.

upvoted 2 times

Drader 5 months, 4 weeks ago

Old switches doesn't support trunking, but the NewSwitch might.

upvoted 3 times

Sutokuto 9 months ago

Selected Answer: B

The question says the old switches don't support trunking

upvoted 2 times

sssssse 9 months, 1 week ago

Selected Answer: D

It can be D. Native VLAN2 will pass untaged traffic from VLAN2. it is a tricky question

upvoted 2 times

HMaw 10 months ago

Selected Answer: B

I tested in Package Tracer. It is B. STP will block if you turn on f0/0 to trunk port. Here is what need to be done on NewSW
#int f0/0
#sw mo acc
#sw acc vlan 2
#sw trunk allowed vlan 2

That's it

upvoted 2 times

ksl20cc0 10 months, 1 week ago

Selected Answer: B

"When two switches configure a mode of 'access' on one end and 'trunk' on the other, problems occur. Avoid this combination." (OCG vol 1 p195)

upvoted 3 times

mzu_sk8 10 months, 2 weeks ago

configure a trunk with native vlan 2, which is untaged so it can reach SW1's access Vlan 2 port, there will be no problem

upvoted 1 times

dick3311 10 months, 3 weeks ago

Selected Answer: B

It should be B
cause SW1 F0/0 is mode acess
so NewSW F0/0 should also be access

upvoted 1 times

perri88 3 months ago

it is stated and also shown in the diagram that VLAN 10 will be used in the future, how do you allow a second VLAN on an access port? B is not correct

upvoted 2 times

Etidic 10 months, 4 weeks ago

Selected Answer: D

The Answer is D.

upvoted 1 times

Question #311 *Topic 1*

Which WLC interface provides out-of-band management in the Cisco Unified Wireless Network Architecture?

A. AP-Manager

B. service port

C. dynamic

D. virtual

Correct Answer: *B*

Community vote distribution

B (100%)

mrgreat Highly Voted 1 year ago

Selected Answer: B

The service port is used for out-of-band management of the controller and system recovery and maintenance in the event of a network failure. It is important to note that the service port does not support VLAN trunking or VLAN tagging and is therefore required to connect to an access port on the switch.

It is also recommended not to connect the service port to the same VLAN as the wired clients network because by doing so, administrators will not be able to access the management interface (analysed later) of the controller.

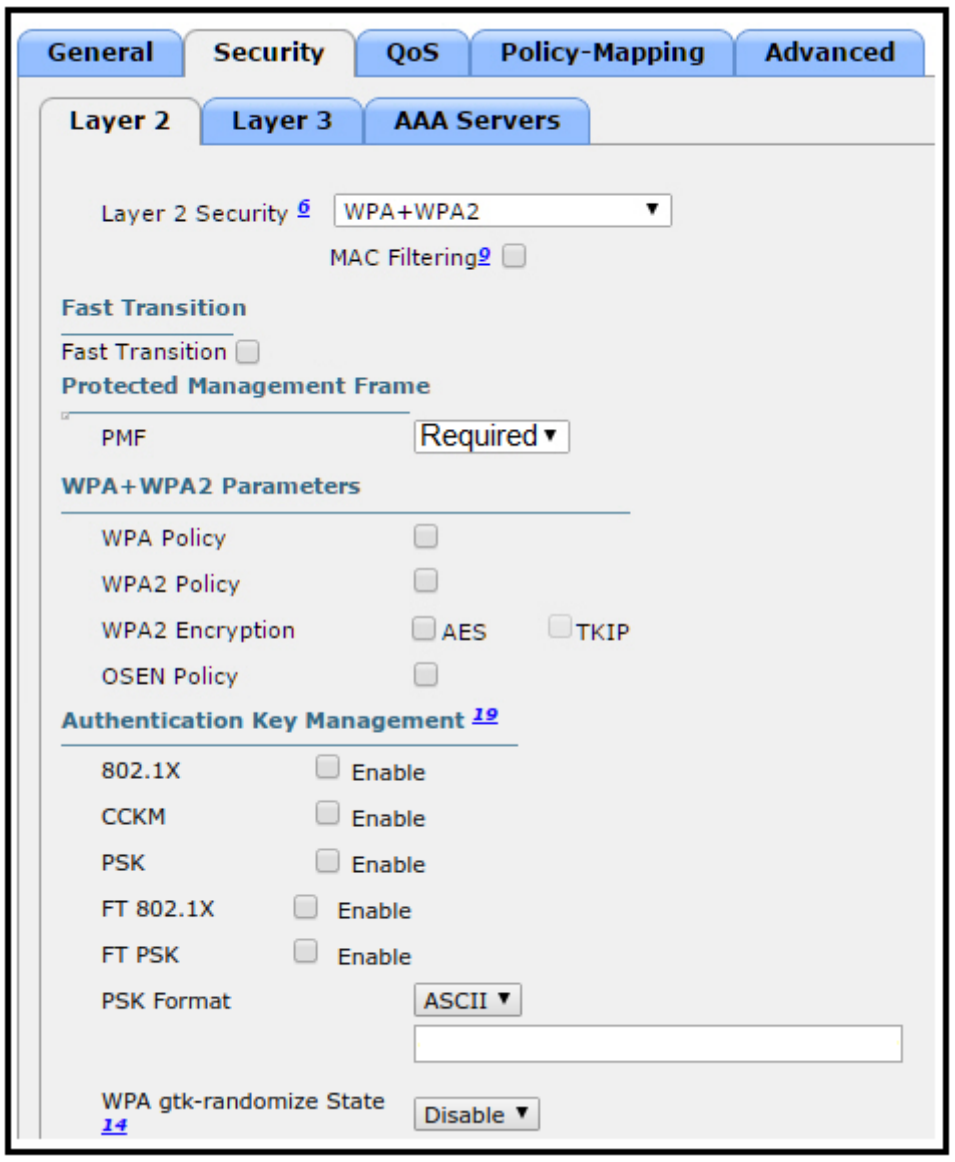
upvoted 9 times

Dhiru959 Most Recent 4 months ago

Ans : B (Service Port)

The service port is used for out-of-band management of the controller and system recovery and maintenance in the event of a network failure. It is important to note that the service port does not support VLAN trunking or VLAN tagging and is therefore required to connect to an access port on the switch.

upvoted 1 times



Refer to the exhibit. The network engineer is configuring a new WLAN and is told to use a setup password for authentication instead of the RADIUS servers.

Which additional set of tasks must the engineer perform to complete the configuration?

A. Disable PMF Enable PSK Enable 802.1x

B. Select WPA Policy Enable CCKM Enable PSK

C. Select WPA Policy Select WPA2 Policy Enable FT PSK

D. Select WPA2 Policy Disable PMF Enable PSK

Correct Answer: *D*

Community vote distribution

D (62%) B (27%) 12%

Ciscoman021 Highly Voted 5 months, 1 week ago

Selected Answer: D

The correct option for this scenario would be D. Select WPA2 Policy Disable PMF Enable PSK.

When configuring a WLAN to use a setup password for authentication instead of RADIUS servers, the following tasks must be performed:

Select WPA2 Policy: The engineer should select WPA2 (Wi-Fi Protected Access II) as the security policy for the WLAN. WPA2 is a widely used security protocol that provides strong encryption and authentication for wireless networks.

Disable PMF: PMF (Protected Management Frames) is a security feature that helps protect against certain types of attacks on wireless networks. However, it may cause compatibility issues with some client devices. Therefore, it should be disabled when using a setup password for authentication.

Enable PSK: PSK (Pre-Shared Key) is a form of authentication that uses a shared password or passphrase to authenticate clients on the wireless network. When using a setup password for authentication, the engineer should enable PSK and set the shared password or passphrase.

upvoted 6 times

oatmealturkey Highly Voted 6 months, 4 weeks ago

Selected Answer: D

It is not B, you cannot select both CCKM and PSK. Cisco is trying to throw us off with disabling PMFs, but D is the best answer.

upvoted 5 times

studying_1 4 months, 1 week ago

but PMF is a security feature of WPA3, so i guess no need to keep it enabled, since we're using WPA2, n'est ce pas? je crois que oui, please, correct me if i'm wrong

upvoted 2 times

dropspablo 1 month, 2 weeks ago

studying_1 you are correct. See what the Official Cisco Guide says:

"WPA3 includes other features that WPA and WPA2 do not have, such as SAE (Simultaneous Authentication of Equals), Forward Secrecy, and PMF (Protected Management Frames). (OCG Wendell Adom v1)".

(The correct answer is D. "need to disable PMF")
and from what I understand, when using the PMF, you would also need to enable the "PMF PSK", and not just the "PSK". I agree that this PMF (802.11w) config is meant to be misleading.

upvoted 1 times

chegurus Most Recent 13 hours, 53 minutes ago

D is the correct answer. the "Configuring WLAN Security" section in the CCNA 200-301 official cert guide has the same example.

upvoted 1 times

OrwellMB 2 months, 1 week ago

Selected Answer: B

With WPA2 enabled, you NEED to select one of the encryption options.
Therefore, B remains.

Also:
"when you configure your wireless LAN for CCKM fast secure roaming, EAP-enabled clients securely roam from one access point to another without the need to reauthenticate with the RADIUS server"

So with CCKM (only with B option) you can bypass the RADIUS server entirely.

upvoted 2 times

Dunedrifter 2 months, 2 weeks ago

Selected Answer: D

WPA2 should be used. It's more secure than WPA

upvoted 2 times

splashy 8 months ago

Selected Answer: D

A.dot1x = no
B.CCKM + PSK = no go (atleast not on the devices i've seen in netacad course + PT)
C.Possible but ONLY FT capable clients will be able to connect, non-FT will not which is very far from ideal.

D. While disabling PMF is sub-optimal, at least you will not be denying non FT-capable clients/devices to connect.

upvoted 3 times

freeknowledge123 8 months, 1 week ago

using a wpa/wpa2 mixed mode is a high security risk
https://www.speedguide.net/faq/wpa2-vs-wpa2wpa-mixed-mode-security-436#:~:text=WPA2%2FWPA%20mixed%20mode%20allows,for%20use%20by%20the%20client.
basically clients can use either wpa and wpa2 to connect, which is a big no no for security.
i think it's either B or D.
Again all options are correct but i think B is more correct because it provide the most security, CCKM works with PSK correct me if i am wrong.

upvoted 1 times

Request7108 8 months, 3 weeks ago

Selected Answer: C

This is a badly written question and answer set. I ran this on my 5520, code version 8.10.130

A) Obviously wrong because it is dot1x
B) Wrong because CCKM is not an option when using PSK. For the code version I'm running, CCKM disappears as soon as I select personal versus enterprise.
C) WPA and WPA2 is allowable but not ideal. It also needs to have the FT enabled checked and the FT PSK box checked. On my code version, this is automatically done when I set FT to enable.
D) While not ideal to disable PMF, it is possible.

Strictly speaking, this question comes down to whether or not Cisco is expecting both FT boxes to be checked or not. I hope they aren't being this neurotic so I'm choosing C, despite D being the most asinine yet accurate.

upvoted 2 times

Panda_man 9 months, 2 weeks ago

Selected Answer: B

A - Is not correct since they say RADIUS is not used and 802.1.x is to be used for authentication through RADIUS, TACACS;

C- not correct you can not have WPA Policy and WPA2 policy at the same time;

D-not correct,since it's not reccomandation to disable Pmf and especially if WPA2 is unable;

Therefore B should be correct answer.
upvoted 5 times

Request7108 8 months, 3 weeks ago
Your evaluation of C is incorrect because it is possible to have WPA and WPA2 at the same time. It is not recommended, but it is possible.
upvoted 2 times

Drader 5 months, 3 weeks ago
Isn't it possible to have WPA2 and WPA at the same time for backwards compatibility?
upvoted 1 times

fjori 9 months, 3 weeks ago
A is not the choice as 802.1x is an authentication protocol to allow access to networks with the use of a RADIUS server. C is not correct as FT PSK is used only for static configuration only . D is not correct as we shoul not disable PMF for security. So the correct answer is B
upvoted 1 times

mijhn13 10 months, 3 weeks ago
are you sure etidic? im confused
upvoted 1 times

Etidic 10 months, 4 weeks ago
Selected Answer: C
The answer is C
upvoted 1 times

chathu123 10 months, 3 weeks ago
can you explain it ?
upvoted 1 times

RougePotatoe 10 months ago
He is wrong. "802.11r FT + PMF is not recommended."
https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html
upvoted 2 times

Question #313 *Topic 1*

Which mode must be set for Aps to communicate to a Wireless LAN Controller using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol?

A. route

B. bridge

C. lightweight

D. autonomous

Correct Answer: *C*

freeknowledge123 8 months, 1 week ago
lightweight=local mode
upvoted 3 times

Trevor_VT 4 months, 2 weeks ago
Not sure what you mean by "local mode", but looks like it is exactly the opposite. Lightweight = dependent from a controller and can not run "locally". While autonomous mode runs "locally" - does not need Wireless LAN Controllers to function.
upvoted 1 times

Hope_12 4 months, 1 week ago
I think it means LAP running on one of its mode which is local. Default mode of LAP.
upvoted 1 times

Question #314 *Topic 1*

Which switch technology establishes a network connection immediately when it is plugged in?

A. PortFast

B. BPDU guard

C. UplinkFast

D. BackboneFast

Correct Answer: *A*

Community vote distribution

A (83%) C (17%)

shumps 4 weeks ago

please take not that uplink and backbone fast is used in case of interface failure and the quickly kick in RSTP. Portfast being the correct answer allows you to jump listening and learning states which take about 30mins combined to process and place the port in forwarding state immediately which is a stable state.

upvoted 1 times

Cynthia2023 1 month ago

Selected Answer: A

UplinkFast is specifically designed to provide rapid connectivity restoration when a link goes down and then comes back up. It focuses on the rapid restoration of uplink ports. On the other hand, PortFast is generally used for access ports to speed up the STP process by bypassing the listening and learning phases.

upvoted 1 times

OrwellMB 2 months, 1 week ago

Selected Answer: A

What y'all smoking with C?
"UplinkFast is a Cisco specific feature that improves the convergence time of the Spanning-Tree Protocol (STP) in the event of the failure of an uplink. "

where does this states plugging in?

Answer is A

upvoted 1 times

perri88 3 months ago

UplinkFast optimizes convergence when an uplink fails on an access layer switch. For good STP design, access layer switches should not become root or become transit switches. (A transit switch is a switch that forwards frames between other switches.) Figure 3-7 shows the actions taken when UplinkFast is enabled on a switch, and then when the Root Port fails.

https://www.ccexpert.us/routing-switching/portfast-uplinkfast-and-backbonefast.html

upvoted 1 times

perri88 3 months ago

Selected Answer: A

enable spanning-tree uplinkfast. This is a global command, you can't configure it on the interface level.
When uplinkfast is enabled a non-designated port will go to forwarding state immediately if the root port fails. Instead of 30 seconds downtime connectivity is restored immediately.

So uplink is for when a root port fails,

upvoted 2 times

jonathan126 4 months, 3 weeks ago

Selected Answer: C

The answer is D. Look carefully at the wordings: establishes a network connection immediately when "IT" is plugged in. It refers to a switch. Portfast is used for end devices not switch. The answer is C.

upvoted 1 times

jonathan126 4 months, 3 weeks ago

Sorry I mean C not D.

upvoted 2 times

Ciscoman021 5 months ago

Selected Answer: A

The switch technology that establishes a network connection immediately when it is plugged in is PortFast.

upvoted 1 times

fransCISCO 7 months, 2 weeks ago

it should be C UplinkFast. not PortFast (forwarding state only)

upvoted 2 times

checkoboy88 6 months, 3 weeks ago

Uplinkfast is mainly used in a distribution or core layer.

https://www.cisco.com/c/es_mx/support/docs/lan-switching/spanning-tree-protocol/10575-51.html

upvoted 1 times

Goh0503 12 months ago

Answer A

When you enable PortFast on a switch or trunk port, the port is immediately transitioned to the spanning tree forwarding state.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html

upvoted 3 times

Question #315 *Topic 1*

Which command on a port enters the forwarding state immediately when a PC is connected to it?

A. switch(config)#spanning-tree portfast default

B. switch(config)#spanning-tree portfast bpduguard default

C. switch(config-if)#spanning-tree portfast trunk

D. switch(config-if)#no spanning-tree portfast

Correct Answer: *A*

Community vote distribution

A (100%)

Customexit Highly Voted 10 months, 3 weeks ago

Selected Answer: A

int g0/2 spanning-tree portfast.

You can also enable portfast with the following command:
SW1(config)# spanning-tree portfast default
(this enables portfast on all access ports (not trunk ports).

upvoted 6 times

Etidic Most Recent 10 months, 4 weeks ago

Selected Answer: A

The correct answer is A.
The use of the word 'port' in the question was just a distraction.

upvoted 3 times

gorigorimmm 11 months, 3 weeks ago

I think there is no correct answer in the options.
The correct answer should be:
switch(config-if)#spanning-tree portfast

upvoted 3 times

FatimaG 11 months, 3 weeks ago

A is correct. You can enable spanning-tree portfast on the interface configuration or spanning-tree portfast default on global configuration command.

https://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/trash/swstpopt.html

upvoted 7 times

arenjenkins 11 months, 3 weeks ago

Correct anwser is C

upvoted 3 times

SABRISAEIB 11 months, 3 weeks ago

Port Fast works only with access ports

upvoted 3 times

RougePotatoe 10 months, 3 weeks ago

Incorrect. You can configure portfast on trunk links via the following command in the interface configuration mode: spanning-tree portfast trunk. It is only recommanded that you only use portfast on access ports but you can definitely configure portfast on trunk ports.

upvoted 4 times

Question #316 *Topic 1*

If a switch port receives a new frame while it is actively transmitting a previous frame, how does it process the frames?

A. The new frame is delivered first, the previous frame is dropped, and a retransmission request is sent

B. The previous frame is delivered, the new frame is dropped, and a retransmission request is sent

C. The new frame is placed in a queue for transmission after the previous frame

D. The two frames are processed and delivered at the same time

Correct Answer: *C*

Community vote distribution

C (100%)

lamm 2 months ago

is this question about duplex operation, while receiving | transmitting ... will not both be processed ... or if it is half-duplex, could be more suitable scenario to consider both tx/rx as one.

upvoted 1 times

thomson_johnson 5 months, 4 weeks ago

They are processed at the same time, but if they are supposed to be sent using the same interface, new one will be sent when it is free to go. Like blitzstorm pointed out: FIFO is default config for a queue.
Full duplex means receiving and sending is possible at the same time, but no magic will make switch send 2 frames out of the same interface simultaneously with that configuration.
plus it's a little wording puzzle, if one frame is already being transmitted, there is no possibility for the new one to be sent at exactly the same time (it still needs to be processed, so a tiny difference in time, but still a difference)

upvoted 3 times

Ceruzka 6 months, 2 weeks ago

hmmm, perhaps I have a bad English, but the port receives a frame and transmits (sends) a frame - in full duplex at the same time..so what is wrong with answer D ?

upvoted 1 times

soRwatches 6 months, 1 week ago

same thought.

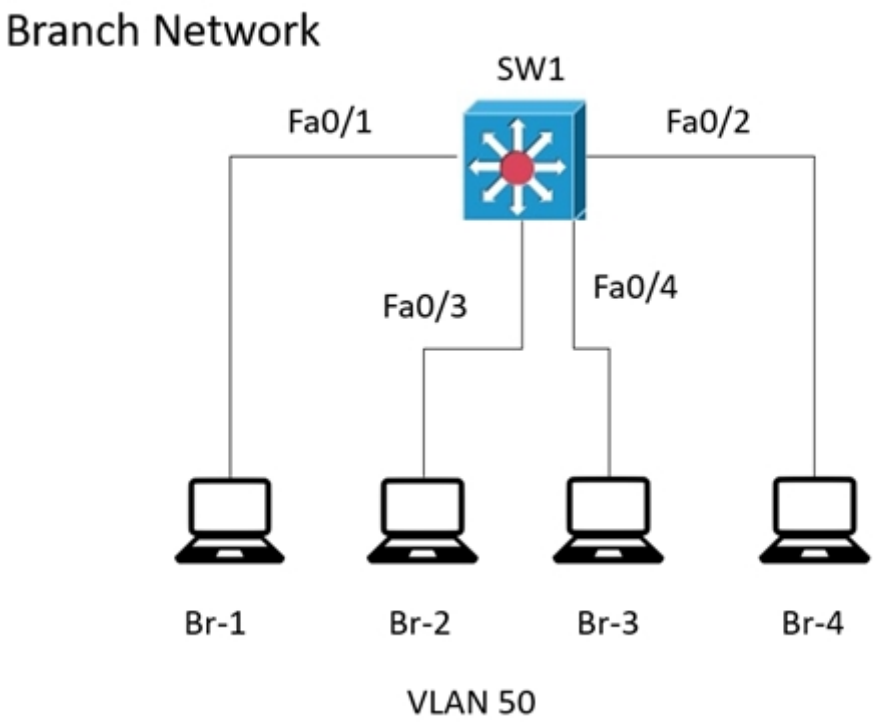
upvoted 1 times

blitzstorm 7 months, 1 week ago

Selected Answer: C

First in First out (FIFO) is default config for a queue

upvoted 2 times



Refer to the exhibit. The entire MAC address table for SW1 is shown here:

```
SW1#show mac-address-table
Mac Address Table
----------------------------------------------------------------
Vlan       Mac Address       Type        Ports
50         000c.8590.bb7d    DYNAMIC     Fa0/1
50         010a.7a17.45bc    DYNAMIC     Fa0/3
50         7aa7.4041.0525    DYNAMIC     Fa0/4
SW1#
```

What does SW1 do when Br-4 sends a frame for Br-2

A. It performs a lookup in the MAC address table for Br-4 and discards toe frame due to a missing entry.

B. It floods the frame out or all ports except on the port where Br-2 is connected.

C. It Inserts the source MAC address and port into the forwarding table and forwards the frame to Br-2.

D. It maps the Layer 2 MAC address for Fa0/3 to the Layer 3 IP address and towards the frame.

Correct Answer: *C*

Community vote distribution

C (100%)

Sdiego Highly Voted 7 months, 4 weeks ago

Tricky! Exchanging interfaces IDs with Branch numbers, b careful!

upvoted 5 times

Rydaz 4 months, 1 week ago

dirty move

upvoted 1 times

raul_kapone Most Recent 4 weeks ago

Selected Answer: C

Although the statement of alternative C doesn't explain all the process (because the switch will flood out the frame by all the ports, except by the incoming port - fa0/2), it is right, because it is somthing that happens.

Tricky question like they say.

upvoted 1 times

HSong 4 months, 2 weeks ago

the question tricks.

upvoted 2 times

Question #318 *Topic 1*

Which statement about Link Aggregation when implemented on a Cisco Wireless LAN Controller is true?

A. To pass client traffic two or more ports must be configured

B. The EtherChannel must be configured in ג€mode activeג€

C. When enabled, the WLC bandwidth drops to 500 Mbps

D. One functional physical port is needed to pass client traffic

Correct Answer: *D*

Community vote distribution

D (100%)

[Removed] 3 months ago

Selected Answer: D

Answer D is correct

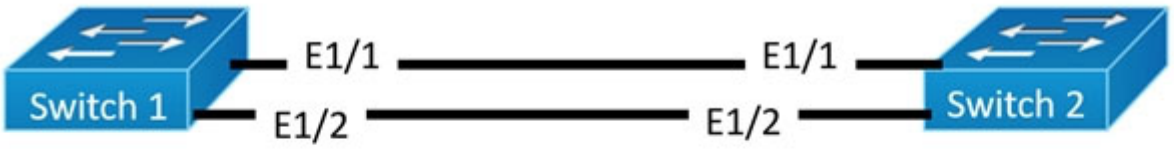
upvoted 1 times

curbstone19 6 months, 2 weeks ago

Answer: D

upvoted 4 times

Question #319 *Topic 1*



Interface Po1
switchport
switchport mode access
switchport access vlan 2

Interface E1/1 - 2
Switchport
Switchport mode access
Switchport access vlan 2

Interface Po1
switchport
switchport mode access
switchport access vlan 2

Interface E1/1 - 2
Switchport
Switchport mode access
Switchport access vlan 2

Refer to the exhibit. An engineer is configuring an EtherChannel using LACP between Switches 1 and 2.
Which configuration must be applied so that only Switch 1 sends LACP initiation packets?

A.

```
Switch1(config-if)#channel-group 1 mode on

Switch2(config-if)#channel-group 1 mode active
```

B.

```
Switch1(config-if)#channel-group 1 mode active

Switch2(config-if)#channel-group 1 mode passive
```

C.

```
Switch1(config-if)#channel-group 1 mode passive

Switch2(config-if)#channel-group 1 mode active
```

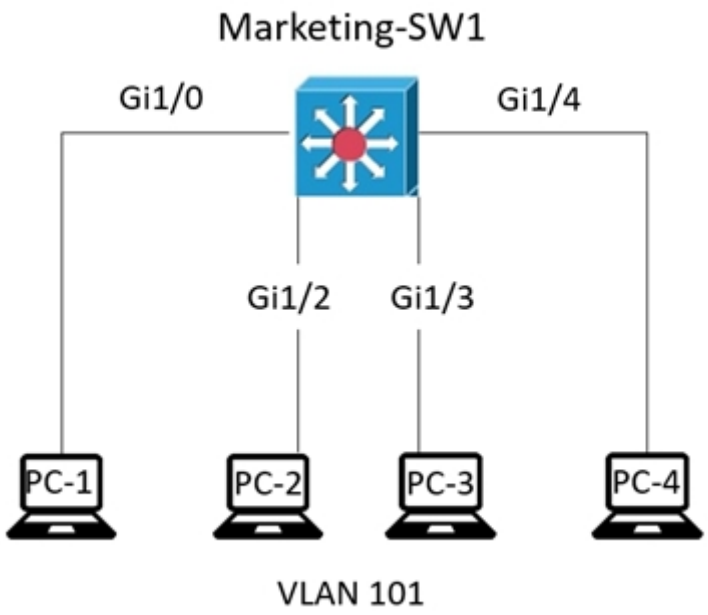
D.

```
Switch1(config-if)#channel-group 1 mode on

Switch2(config-if)#channel-group 1 mode passive
```

Correct Answer: *B*

country_rooted 5 months, 2 weeks ago
Correct
upvoted 3 times

Goena 8 months, 2 weeks ago
Switch 1 sends LACP initation packets:
Switch 1 is active.
Switch 2 is passive
upvoted 4 times




```
Marketing-SW1#show mac-address-table
Mac Address Table
-------------------------------------------
VLAN      MAC Address          Type      Ports
101       000a.000a.000a       DYNAMIC   Gi1/0
101       3986.3986.3986       DYNAMIC   Gi1/2
101       00d0.00d0.00d0       DYNAMIC   Gi1/3
```

Refer to the exhibit. The entire Marketing-SW1 MAC address table is shown here:
What does the switch do when PC-4 sends a frame to PC-1?

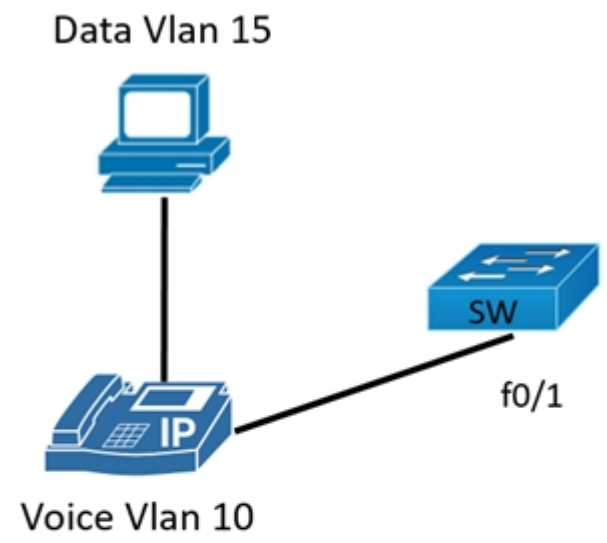
A. It performs a lookup in the MAC address table and discards the frame due to a missing entry.

B. It maps the Layer 2 MAC address to the Layer 3 IP address and forwards the frame.

C. It inserts the source MAC address and port into the table and forwards the frame to PC-1.

D. It floods the frame out of all ports except on the port where PC-1 is connected.

Correct Answer: *C*




```
SW#show run
Building configuration...
!
interface FastEthernet0/1
 switchport access vlan 15
!
 end
```

Refer to the exhibit. All VLANs are present in the VLAN database. Which command sequence must be applied to complete the configuration?

A.

```
interface FastEthernet0/1
switchport mode access
switchport voice vlan 10
```

B.

```
interface FastEthernet0/1
switchport trunk native vlan 10
switchport trunk allowed vlan 10,15
```

C.

```
Interface FastEthernet0/1
switchport trunk allowed vlan add 10
vlan 10
private-vlan isolated
```

D.

```
interface FastEthernet0/1
switchport mode trunk
switchport trunk allowed vlan 10,15
```

Correct Answer: *A*

GigaGremlin Highly Voted 11 months, 1 week ago

Answer A is fine.
Config would usually look like this:
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport voice vlan 10
Switch(config-if)#switchport access vlan 15

upvoted 11 times

Tomasek1234 Most Recent 6 months, 3 weeks ago

Answer C is correct

upvoted 1 times

Tomasek1234 6 months, 3 weeks ago

Wrong question, delete this please

upvoted 2 times

JJY888 7 months ago

There is a question earlier where a truck port is chosen as the answer regarding a VoIP phone passthrough with a PC. I believe only access ports are used for this scenario.

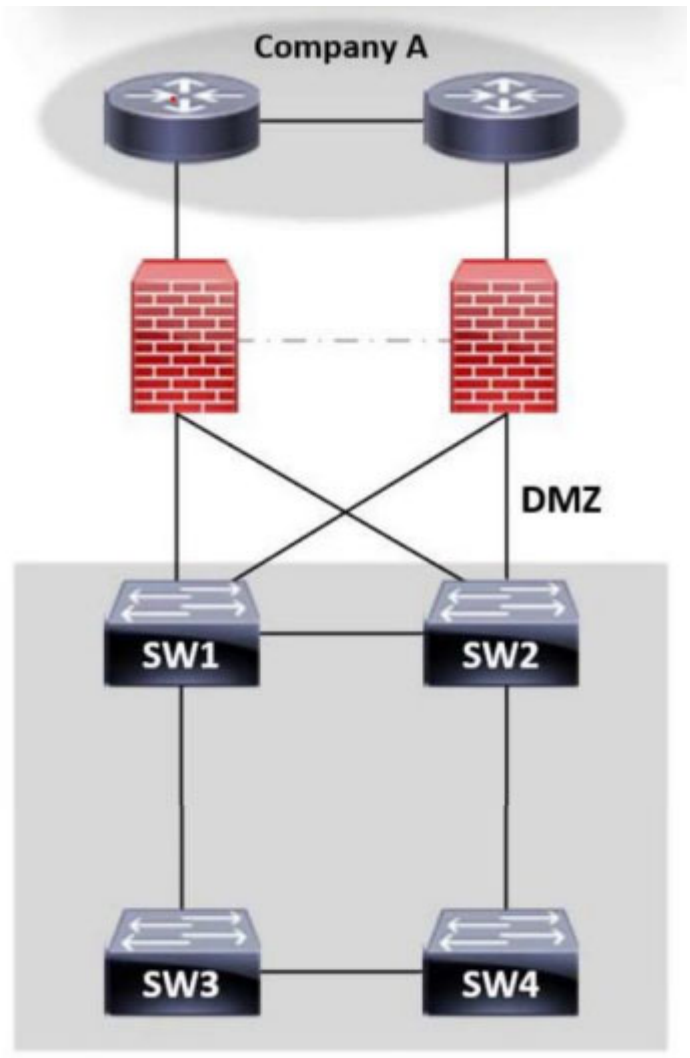
upvoted 3 times

Shanku97 2 weeks, 6 days ago

voip wont't work on trunk port, so any answer with trunk port for voice vLAN is wrong only.

upvoted 1 times

Question #322 *Topic 1*




```
SW1: VLAN10 - 32778 0018.1843.3cb0
SW2: VLAN10 - 24586 004a.13e9.3912
SW3: VLAN10 - 28682 0022.55cf.cc00
SW4: VLAN10 - 64000 0022.66ed.a29f
```

Refer to the exhibit. Which switch becomes the root of a spanning tree for VLAN 10 if the primary switch fails and all links are of equal speed?

A. SW1

B. SW2

C. SW3

D. SW4

Correct Answer: *C*

dannyode Highly Voted 11 months, 1 week ago

Selected Answer: C

Switch 2 is primary. But in this context, that is to say when it fails, the primary is chosen between SW1, SW3 and SW4. Thus, SW3 becomes the root. Answer C is correct.

upvoted 26 times

freeknowledge123 Highly Voted 8 months, 1 week ago

we need an admin here to check this bellabop, ruining answers for all users.

upvoted 23 times

FALARASTA 4 months, 3 weeks ago

The answer is correct. Which one after the first one.

upvoted 2 times

Godfather2022 7 months, 2 weeks ago

@ Bellabop please desist from confusing people. We hear to learn.

upvoted 1 times

Elle_33 8 months, 1 week ago

Let us report it

upvoted 2 times

raul_kapone Most Recent 4 weeks ago

Selected Answer: C

The answer is C.
To elect the Root Bridge:
1st criterion - Lowest Priority Value
2nd criterion - Lowest MAC Address

So, if the primary switch fails, it would be the SW1 (Lowest Priority).
Then, the second lowest priority value corresponds to SW3, so it will be become the Root Bridge.

It is not necessary to use the 2nd criterion (MAC address), because the priorities are different for each switch, so the 1st criterion prevails.

upvoted 1 times

raul_kapone 4 weeks ago

Sorry, the correction for the 5th paragraph:
*So, if the primary switch fails, it would be the SW2 (Lowest Priority).

upvoted 1 times

shumps 1 month, 1 week ago

the second is C with the lowest after sw2 is down

upvoted 1 times

lamm 2 months ago

Selected Answer: C

if you check priority values becomes clear that this is correct answer, this will be the second lowest BID.

upvoted 1 times

[Removed] 4 months ago

C is correct. The primary is SW2 and if it fails SW3 will become the primary.

upvoted 3 times

[Removed] 4 months, 1 week ago

Selected Answer: C

Increasing stat for the correct answer C.

upvoted 1 times

HSong 4 months, 4 weeks ago

SW1 should have been the primary, and it fails?

upvoted 1 times

ASHLEY_27 5 months ago

Selected Answer: C

The question says if a primary fails. According to the table primary is SW1 which has the lowest priority, followed by SW3 which has the second lowest priority making it secondary.

upvoted 1 times

Eminn 6 months, 2 weeks ago

Selected Answer: B

Correct answer is B! Because first of all selected Low Priority. If priority is default on all devices, second select is MAC

upvoted 2 times

thomson_johnson 5 months, 4 weeks ago

Question asks which switch will become the root bridge if the current one fails, so C is correct

upvoted 5 times

linuxlife 5 months, 4 weeks ago

the question if "primary failed" who will be the root switch...so its the switch with the lowest Bridge ID after Switch 2.

upvoted 3 times

Tomasek1234 6 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

[Removed] 8 months, 3 weeks ago

Selected Answer: A

Answer is C.

upvoted 2 times

[Removed] 8 months, 3 weeks ago

Selected Answer: A

Answer is C.

upvoted 2 times

[Removed] 8 months, 3 weeks ago

Selected Answer: A

Answer is C.

upvoted 2 times

[Removed] 8 months, 3 weeks ago

Selected Answer: A

Answer is C.

upvoted 1 times

[Removed] 8 months, 3 weeks ago

Selected Answer: A

Answer is C.

upvoted 1 times

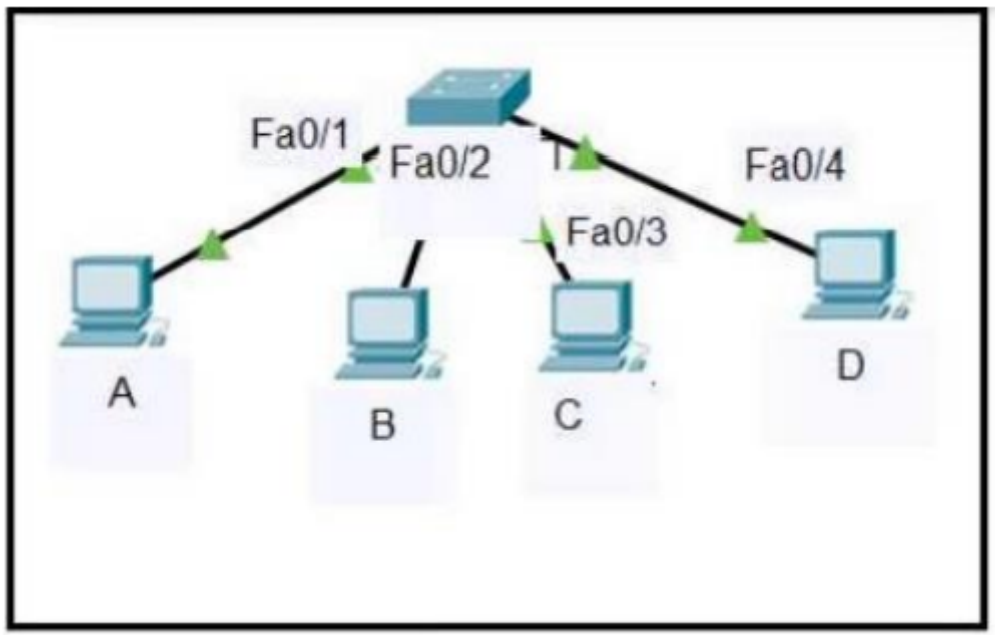
[Removed] 8 months, 3 weeks ago

Selected Answer: A

Answer is C.

upvoted 1 times

Question #323 *Topic 1*



Refer to the exhibit. Host A sent a data frame destined for host D.

```
SwitchA#show mac-address table Mac Address Table
Vlan Mac Address Type Ports
2 000c.859c.bb7b DYNAMIC Fa0/1
2 0010.11dc.3e91 DYNAMIC Fa0/2
2 0041.39d1.c469 DYNAMIC Fa0/3 Switch A#
```

What does the switch do when it receives the frame from host A?

A. It floods the frame out of all ports except port Fa0/1

B. It experiences a broadcast storm

C. It shuts down the port Fa0/1 and places it in err-disable mode

D. It drops the frame from the switch CAM table

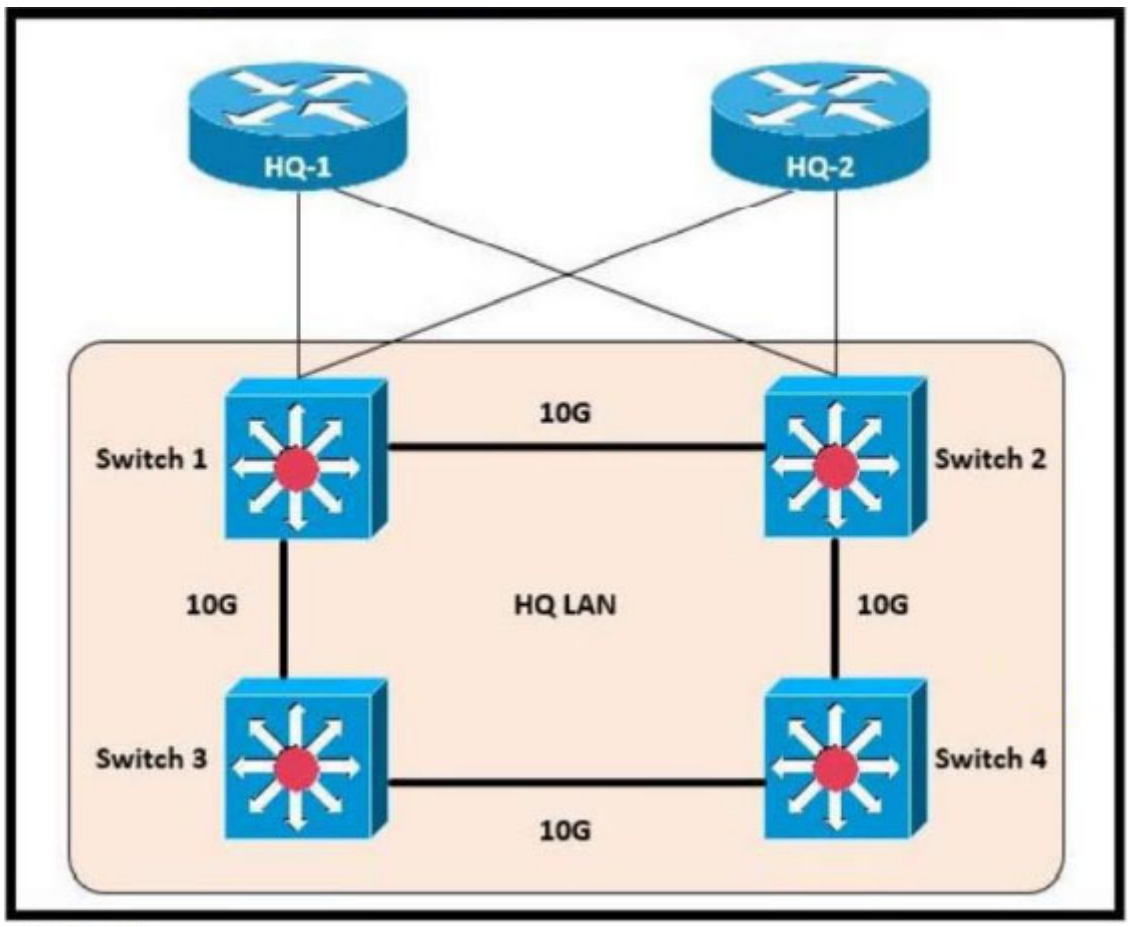
Correct Answer: *A*

holyshitbin 3 months ago

This is the definition of flooding.

upvoted 1 times

Question #324 *Topic 1*



Switch 1
BID: 32778 0018.184e.3c00
Switch 2
BID: 24586 001a.e3ff.a680
Switch 3
BID: 28682 0022.55cf.cc00
Switch 4
BID: 64000 0e41.4503.004f

Refer to the exhibit. Which switch becomes the root of the spanning tree?

A. Switch 1

B. Switch 2

C. Switch 3

D. Switch 4

Correct Answer: *B*

The root bridge is the bridge with the lowest Bridge ID. All the decisions like which ports are the root ports (the port with the best path to the root bridge) are made from the perspective of the root bridge. In case of a tie (not the case in this example) then the root bridge will be the switch with the lowest MAC address.

Shanku97 2 weeks, 6 days ago

can someone share me the steps of root port, forwarding port/designated port ?

upvoted 1 times

[Removed] 3 months ago

Selected Answer: B

Given answer is correct

upvoted 1 times

Question #325 *Topic 1*

Which channel-group mode must be configured when multiple distribution interfaces connected to a WLC are bundled?

A. Channel-group mode passive.

B. Channel-group mode on.

C. Channel-group mode desirable.

D. Channel-group mode active.

Correct Answer: *B*

creaguy 11 months, 3 weeks ago

Selected Answer: B

B is correct
https://www.firewall.cx/cisco-technical-knowledgebase/cisco-wireless/1223-how-to-configure-wlc-lag-and-port-channel-with-nexus-catalyst-switches.html#:~:text=switchport%20mode%20trunk-,channel%2Dgroup%201%20mode%20on,-!%0Ainterface%20GigabitEthernet0

upvoted 4 times

RougePotatoe 10 months, 3 weeks ago

In support of the claim above from cisco source.
"Once the EtherChannel is configured as on at both ends of the link, the Catalyst switch should not be configured for either Link Aggregation Control Protocol (LACP) or Cisco proprietary Port Aggregation Protocol (PAgP) but be set unconditionally to LAG. Because no channel negotiation is done between the controller and the switch, the controller does not answer to negotiation frames and the LAG is not formed if a dynamic form of LAG is set on the switch. Additionally, LACP and PAgP are not supported on the controller."

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010100001.html#ID1514

upvoted 10 times

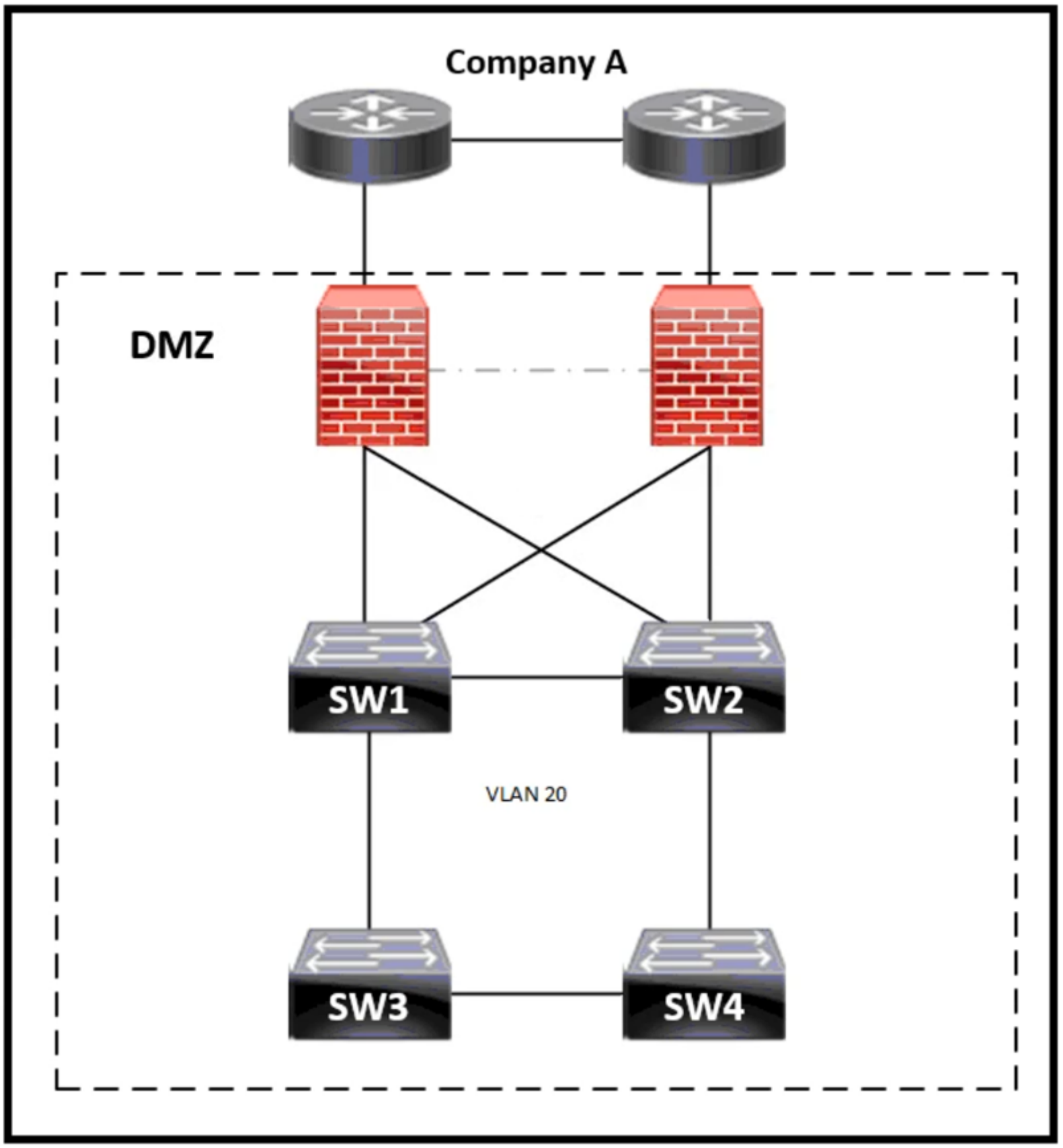
Customexit 10 months, 3 weeks ago

For anyone not wanting to search through this article, I believe the reasoning is:

"Notice that the channel-group mode is set to on which enables Etherchannel without any LACP or PAgP support. This is because the WLC doesn't support LACP or PAgP and requires a plain vanilla Etherchannel."

upvoted 15 times

Question #326 *Topic 1*




```
SW1 = 24596 0018.184e.3c00
SW2 = 28692 004a.13e9.6900
SW3 = 32788 0022.55cf.dd00
SW4 = 64000 0041.396d.690f
```

Refer to the exhibit. Which switch become the root of a spanning tree for VLAN 20 if all links are of equal speed?

A. SW1

B. SW2

C. SW3

D. SW4

Correct Answer: *A*

shiv3003 5 months ago

why not c??

upvoted 1 times

Hope_12 4 months, 1 week ago

Because SW1 has the lowest bridge ID.(lowest bridge priority)

upvoted 3 times

Goena 8 months, 2 weeks ago

Selected Answer: A

The root bridge is the bridge with the lowest Bridge ID.

upvoted 3 times

Question #327 *Topic 1*

Which Layer 2 switch function encapsulates packets for different VLANs so that the packets transverse the same port and maintain traffic separation between the
VLANs?

A. VLAN marking

B. VLAN numbering

C. VLAN DSCP

D. VLAN tagging

Correct Answer: *D*

Customexit Highly Voted 10 months, 3 weeks ago

Selected Answer: D

p.s. "marking" is for QoS stuff.

upvoted 6 times

Question #328 *Topic 1*

Which value is the unique identifier that an access point uses to establish and maintain wireless connectivity to wireless network devices?

A. VLAN ID

B. SSID

C. RFID

D. WLAN ID

Correct Answer: *B*

Kaveras 1 month ago

Selected Answer: B

B for sure

upvoted 1 times

no_blink404 3 months, 1 week ago

Since SSID is not required to be unique, the best answer is D.

upvoted 1 times

Shanku97 2 weeks, 6 days ago

WHAT IS WLAN IS, PLEASE EXPLAIN
DON'T JUST COMMENT I THINK IT'S B OR D, IT CONFUSES OTHERS, PLEASE START EXPALAINING YOUR ANSWERS AS WELL.

upvoted 1 times

thomson_johnson 5 months, 4 weeks ago

SSID doesn't have to be unique.
I'm thinking that someone who posted questions about wireless on this site doesn't know the difference between SSID and BSSID, and there are questions in which someone deleted the B or though it's useless or idk. (There are questions here that spell truck instead of trunk etc.)

upvoted 3 times

thomson_johnson 5 months, 4 weeks ago

thought* i was whining about typos and made one Xd

upvoted 1 times

Goena 8 months, 2 weeks ago

Selected Answer: B

B. SSID

upvoted 1 times

cormorant 9 months, 2 weeks ago

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or subnetwork may use the same SSIDs.

upvoted 3 times

shubhambala 1 year ago

SSID is not unique though? It seems like the most correct option.

upvoted 4 times

ccna_goat 11 months, 3 weeks ago

it should be unique, but its not mandatory. another poorly worded question.

upvoted 6 times

Question #329 *Topic 1*

An engineer must configure neighbor discovery between the company router and an ISP.

```
interface gigabitethernet0/0
description Circuit-ATT4139-84320
duplex full
speed 1000
media-type gbic
negotiation auto
lldp transmit
lldp receive
```

What is the next step to complete the configuration if the ISP uses a third-party router?

A. Enable LLDP globally.

B. Disable CDP on gi0/0.

C. Enable LLDP TLVs on the ISP router.

D. Disable auto-negotiation.

Correct Answer: *A*

Paul1111 4 weeks ago

Answer is A

Tested on packet tracer

int g0/0
duplex full
speed 1000
lldp transmit
lldp receive
do show lldp neighbors
#LLDP is not enabled
lldp run
do show lldp neighbors - shows devices

upvoted 1 times

yavuzcangiz 11 months, 1 week ago

Disabling and Enabling LLDP on an Interface – LLDP is disabled globally on all supported interfaces. You must enable LLDP globally to allow a device to send LLDP packets.
https://www.grandmetric.com/knowledge-base/design_and_configure/lldp-configuration-example-cisco/

upvoted 4 times

vladals 12 months ago

In my opinion, lldp transmit and recieve are configured on the port. We need LLDP to be configured globally in order to complete the company router configuration. Also the phrasing of the question (complete THE build) accompanied by the "snip" of the company router is against answer C as being the correct one.

upvoted 4 times

PiotrMar 1 year ago

why A when lldp transmit and recieve is already configured..? My guess was C

upvoted 3 times

[Removed] 3 months ago

Yes, lldp is already configured. Unless they mean to enable it globally on the ISP router? This question is really confusing.

upvoted 1 times

[Removed] 3 months ago

And this is from Cisco :
"Depending on the device, LLDP may be enabled by default." so in this question, we don't know if it's already globally enabled or not.

upvoted 1 times

[Removed] 3 months ago

Sorry for posting 3 messges but you can't edit. I would disable CDP on gi0/0 (answer C)
Again from Cisco : "To disable CDP on a specific interface, such as the interface facing an ISP, enter no cdp enable in the interface configuration mode."

upvoted 2 times

FALARASTA 4 months, 3 weeks ago

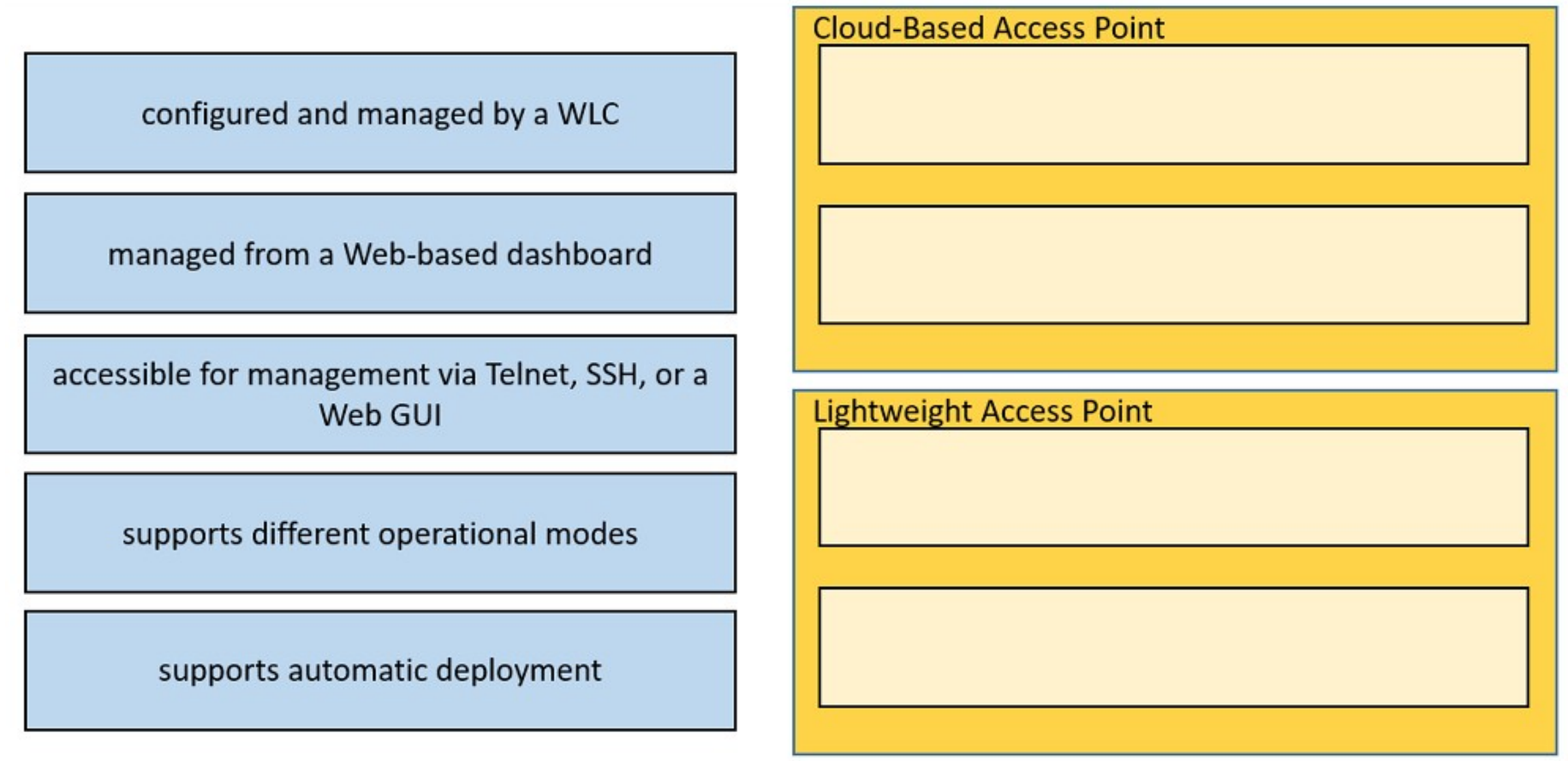
I was thinking the same.

upvoted 1 times

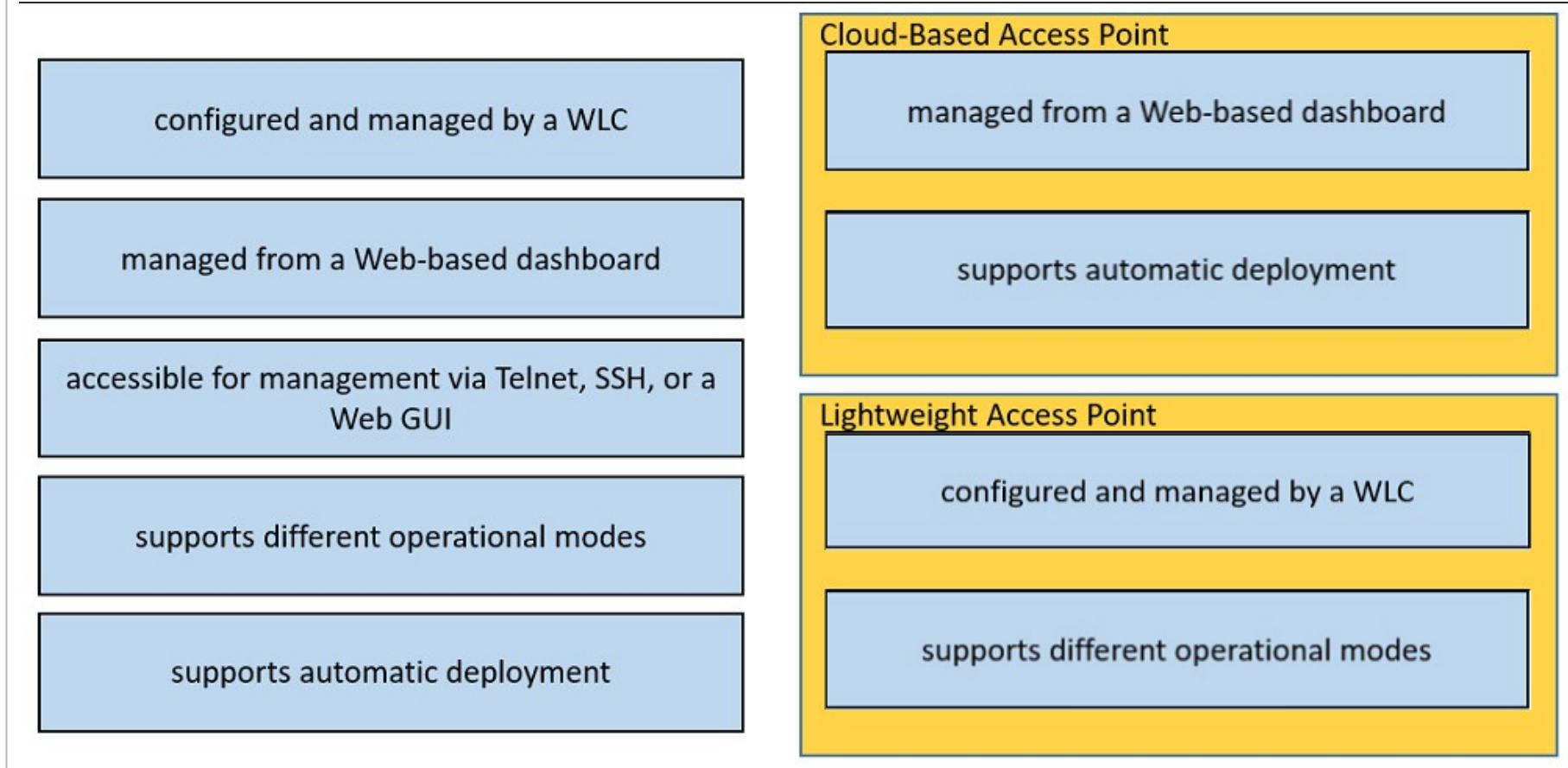
DRAG DROP -

Drag and drop the facts about wireless architectures from the left onto the types of access point on the right. Not all options are used.

Select and Place:



Correct Answer:



[Removed] 3 months ago

Very similar to #272

upvoted 1 times

huykg009 8 months ago

the answer is correct

upvoted 4 times

[Removed] 3 months ago

I don't think so because you can telnet or SSH a LWAP

upvoted 1 times

LeonardoMeCabrio 2 months, 3 weeks ago

Indeed you can telnet or SSH, but you can't manage it.
Given answers are correct.

upvoted 1 times

Question #331 *Topic 1*

What is a function of MAC learning on a switch?

A. MAC address learning is disabled by default on all VLANs.

B. Frames received for a destination MAC address not listed in the address table are dropped.

C. The MAC address table is used to populate the ARP table.

D. A static MAC address is manually added to the MAC table.

Correct Answer: *D*

HennieB Highly Voted 11 months ago

Selected Answer: C

The question specifically says LEARNING. A Static MAC is not learned

upvoted 11 times

dropspablo Highly Voted 4 months, 1 week ago

Selected Answer: D

A. Wrong - MAC address learning is generally enabled by default on switches.
B. Wrong - in this case the next step would be to replicate the original frame to the remaining ports (flood), in order to find the destination.
C. Wrong - MAC learning on a switch (MAC table) is not used to populate the ARP table. MAC learning takes place at the layer 2 level of the OSI model, while the ARP table is related to layer 3, the IP protocol. The ARP table is populated by the host's response frame from the searched IP address destination (ARP reply).
D. Correct - in MAC table learning, the addresses are learned by dynamically received frames, but it can also be learned statically, adding manually, when you want to force a destination for a specific host. Perhaps, in this case the static form can be considered a form of learning.

upvoted 5 times

4Lucky711 1 month, 2 weeks ago

ARP (Address Resolution Protocol) is a layer 2 protocol, not a layer 3 protocol. This is because ARP is used to map a network layer 3 (IP) address to a link layer 2 (MAC) address. It operates at the Data Link Layer of the OSI Model, which is the second layer. It is not considered a layer 3 protocol because it does not deal with routing or managing the flow of data at the network layer.

upvoted 1 times

4aynick 3 months, 3 weeks ago

arp is 2 layer protocol

upvoted 2 times

Sant11 Most Recent 2 weeks, 4 days ago

Selected Answer: D

A static MAC address entry is indeed manually added to the MAC address table on a switch, and this can be considered a form of MAC address learning.

upvoted 1 times

BarkingSpider 3 weeks, 6 days ago

Selected Answer: C

a static MAC is manually assigned, not learned.

upvoted 1 times

kishan365 2 months, 1 week ago

Selected Answer: D

The same question has been repeated but with different answers. The previous one had answer C but here its D.

upvoted 1 times

mda2h 2 months, 2 weeks ago

Selected Answer: C

Statically adding a MAC address is not concidered MAC learning, CISCO's words:
https://www.cisco.com/c/en/us/td/docs/optical/cpt/r_972/cpt95_configuration/cpt93_configuration_chapter_01100.pdf

upvoted 3 times

Jack67 5 months ago

Selected Answer: D

D is correct answer

upvoted 2 times

zamkljo 5 months, 2 weeks ago

D is correct!
I think MAC learning is about learning the unknown MAC Addresses, not matching the MAC addresses and IP addresses(ARP Table).

Each switch has an ARP (Address Resolution Protocol) table to store the IP addresses and MAC addresses of the network devices. The ARP table is used to determine the destination MAC addresses of the network nodes, as well as the VLANs and ports from where the nodes are reached.

upvoted 4 times

linuxlife 5 months, 4 weeks ago

A switch can learn MAC address in two ways; statically or dynamically. In the static option, we have to add the MAC addresses in the CAM table manually. In the dynamic option, the switch learns and adds the MAC addresses in the CAM table automatically. The switch stores the CAM table in the RAM. The RAM is a temporary memory. All contents stored in the RAM are wiped out automatically when we turn off the switch.

upvoted 3 times

linuxlife 5 months, 4 weeks ago

If the switch does not find an entry for the source MAC address, it creates a new entry for this MAC address. An entry contains three pieces of information; the source MAC address, the port or interface on which the frame arrived, and the time when the frame arrived.

If the switch finds an entry for the source MAC address, it updates that entry and resets the timer of that specific entry. The switch assigns a separate timer to each entry of the CAM table. This timer is used to age out old entries from the CAM table, allowing room to store new entries. This feature is known as the Aging.

Once the CAM table is full, the switch has no place to store any new addresses. Aging resolves this issue by automatically removing the old entries from the CAM table. It keeps the MAC addresses of only those devices that are constantly sending the frames.

If any device is not sending the frames, once the timer is expired, it removes the MAC address of that device from the CAM table. In this manner, only the devices that are constantly sending frames remain in the CAM table and the devices that are not sending any frames will eventually be removed from the table.

upvoted 1 times

DevNetAdmin 6 months, 3 weeks ago

A function of MAC learning on a switch is to dynamically build and maintain the MAC address table, which maps MAC addresses to the interfaces on the switch. The MAC address table is not used to populate the ARP table, which maps IP addresses to MAC addresses.

upvoted 2 times

ricky1802 7 months, 1 week ago

Selected Answer: D

Correct answer is D.
MAC table - layer 2
ARP - layer 3

upvoted 4 times

4aynick 3 months, 3 weeks ago

arp 2 layer protocol

upvoted 1 times

Naghini 8 months ago

Selected Answer: D

C - incorrect, MAC table is for layer 2 switches , ARP table - layer 3 (routers and hosts use it).
D - correct. A static entry in a MAC table is only possible if it's inserted manually.

upvoted 3 times

freeknowledge123 8 months, 1 week ago

ARP table: MAC to IP address learning, no relation to the MAC learning process.
D is the more correct choice.

upvoted 4 times

Goena 8 months, 2 weeks ago

Selected Answer: C

The answer is C.

upvoted 2 times

remoto 9 months ago

Selected Answer: C

learning, don't is static

upvoted 1 times

Sara_Yus 9 months, 2 weeks ago

Isn't it supposed to be the CAM Table?

upvoted 2 times

BakedPotato 6 months, 3 weeks ago

CAM table, MAC-address table, ARP table, forwarding table... all the same thing.

upvoted 1 times

thomson_johnson 5 months, 4 weeks ago

no, ARP table is for mapping IPs to MACs, CAM / MAC table is for mapping MACs to interfaces

upvoted 1 times

guisam 9 months, 2 weeks ago

https://medium.com/@cbitss.sheetal0303/understanding-mac-learning-in-ccna-dc3d81a4979b
upvoted 1 times

Question #332 *Topic 1*

What does a switch do when it receives a frame whose destination MAC address is missing from the MAC address table?

A. It changes the checksum of the frame to a value that indicates an invalid frame.

B. It updates the CAM table with the destination MAC address of the frame.

C. It appends the table with a static entry for the MAC and shuts down the port.

D. It floods the frame unchanged across all remaining ports in the incoming VLAN.

Correct Answer: *D*

MikD4016 Highly Voted 11 months, 3 weeks ago
If the address is in the table, the frame is forwarded out the port associated with the MAC address in the table. When the DESTINATION MAC address is not found in the MAC address table, the switch forwards the frame out of all ports (flooding) except for the ingress port of the frame
upvoted 5 times

HMaw Most Recent 10 months ago
My answer is none of them.
upvoted 3 times

yavuzcangiz 11 months, 1 week ago
In this case destination mac is missin so it will flood the frame broadcast to the vlan except incoming port
upvoted 1 times

tattybizzy 11 months, 1 week ago
D is correct
upvoted 3 times

Bibi20 12 months ago
I think the correct answer is B
https://www.ciscopress.com/articles/article.asp?p=2181835&seqNum=5#:~:text=If%20the%20address%20is%20in,ingress%20port%20of%20the%20frame.
upvoted 4 times

Question #333 *Topic 1*

By default, how long will the switch continue to know a workstation MAC address after the workstation stops sending traffic?

A. 200 seconds

B. 300 seconds

C. 600 seconds

D. 900 seconds

Correct Answer: *B*

[Removed] 3 months ago

Selected Answer: B

Given answer is correct - B

upvoted 1 times

Goh0503 12 months ago

Answer is B

DETAILED STEPS
Command or Action Purpose
Step 1 switch# configure terminal Enters configuration mode.
Specifies the time before an entry ages out and is discarded from the
MAC address table. The range is from 0 to 1000000; the default is 300
switch(config)# mac-address-table
aging-time seconds [vlan vlan_id]
Step 2
seconds. Entering the value 0 disables the MAC aging. If a VLAN is
not specified, the aging specification applies to all VLANs.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n2_1/b_Cisco_n5k_layer2_config_gd_rel_503_N2_1/b_Cisco_n5k_layer2_config_gd_rel_503_N2_1_chapter_01111.pdf

upvoted 4 times

toufa 1 year ago

300 secondes is correct

upvoted 4 times

Question #334 *Topic 1*

A project objective is to minimize the association time to the different access points as mobile devices move around the office. The ideal solution must cover numerous devices and device types, including laptops, mobile phones, tablets and wireless printers. What must be configured?

A. 802.11v BSS Max Idle Service

B. 802.11v Disassociation Imminent

C. 802.11ax BSS configure

D. 802.11k neighbor List Dual Band

Correct Answer: *B*

splashy Highly Voted 1 year ago

Selected Answer: B

I probably did... but i do not remember seeing this in the ccna course at all

802.11v
Basic Service Set (BSS) transition management - BSS transition management with Disassociation Imminent allows the network's control layer to influence client roaming behavior by providing it the load information of nearby access points. The device takes this information into account when deciding among the possible roam targets.
Directed Multicast Service (DMS) - DMS optimizes multicast traffic transmission on wireless networks. The device uses this information to enhance multicast communication and preserve device battery life.
BSS Max Idle Service - The BSS Max Idle Service helps clients and access points efficiently decide how long to remain associated when no traffic is being transmitted. The device uses this information to preserve device battery life.
Disassociation Imminent - The Disassociation Imminent option sets a flag in 11v request telling the client that it needs to roam, or it will be disassociated after a certain amount of time.

https://support.accessagility.com/hc/802.11k-802.11r-and-802.11v

upvoted 16 times

[Removed] 3 months ago

Me either. This is not in Cisco's official courses (Netacad). Not related to CCNA 200-301 to me

upvoted 1 times

splashy 8 months ago

When i purely "stick to the books" i have to say B
I don't know your wireless setup, i don't know the devices it needs to support.
I do however know (i hope lol) what is in the books.
You gave me an example of how it doesn't work as intended which is possible.
I didn't see two reasons, i also don't see any links to a knowledge base that supports/illustrates this example.
"The primary benefit of this option is to force sticky clients to roam" thats is one of the goals of this question.
"The ideal solution must cover numerous devices and device types" This also includes older devices that don't support 5Ghz
That would not make D seem like the "ideal" sollution unless every last one of your wireless devices supports both 2.4 & 5Ghz.

Don't get me wrong i'm not disagreeing with you, in real life you would most definitely also enable D.

upvoted 1 times

Request7108 8 months, 2 weeks ago

This answer is incorrect for two reasons - first from the practical standpoint of 11v disassociation imminent forcing the client to look for another access point, which requires off-channel scanning and some client devices panic, drop what they're doing, and search for another AP. I see this at work fairly often and no matter what, it does not help with minimizing association time. The primary benefit of this option is to force sticky clients to roam.

upvoted 2 times

ccna_goat 11 months, 3 weeks ago

wireless questions are the hardest ones, because they cover some topics not mentioned in OCG and even the best courses. im talking about various settings of network using GUI, there are boatload of them.

upvoted 4 times

RougePotatoe Highly Voted 10 months, 3 weeks ago

Selected Answer: D

D. 802.11k neighbor List Dual Band

"With the neighbor list information, the 11k capable client does not need to probe all of the 2.4 GHz and 5 GHz channels to find an APit can roam to. Not having to probe all of the channels reduces channel utilization on all channels, thereby increasing bandwidth on all channels. It also reduces roam time and improves the decisions made by the client."
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_010.pdf

upvoted 6 times

PlsLetMePass Most Recent 1 month ago

Selected Answer: A

Chatgpt says:
While option D (802.11k Neighbor List Dual Band) is related to improving network efficiency and assisting devices in making better decisions during roaming, it may not directly address the requirement of minimizing association time for mobile devices as they move around the office.

The 802.11k Neighbor List Dual Band feature provides information about neighboring access points, including details about their capabilities and signal strength. This information helps devices make informed decisions about when to roam and which access point to associate with. While it can contribute to better roaming decisions, it doesn't focus exclusively on minimizing the association time itself.

Given the specific requirement to minimize association time, the more relevant option would be:

A. 802.11v BSS Max Idle Service

This feature aims to improve mobility by providing information to devices about nearby access points and their capabilities, helping devices make quicker and more efficient decisions when roaming.

upvoted 1 times

Isuzu 4 months ago

802.11v BSS Max Idle Service is a feature that allows clients and access points to efficiently decide how long to remain associated when no traffic is being transmitted. This helps to preserve battery life on mobile devices.

802.11v Disassociation Imminent is a feature that allows access points to notify clients when they are about to be disassociated. This gives clients a chance to save any data that they have not yet transmitted.

802.11ax BSS configure is a feature that allows access points to be configured to support 802.11ax clients. This is not necessary for the project objective, as the project objective is to minimize the association time to the different access points as mobile devices move around the office.

802.11k neighbor List Dual Band is a feature that allows access points to maintain a list of neighboring access points on both the 2.4 GHz and 5 GHz bands. This is not necessary for the project objective, as the project objective is to minimize the association time to the different access points as mobile devices move around the office.

upvoted 1 times

dropspablo 4 months ago

Selected Answer: D

Enabling the ".11v Disassociation Imminent" setting alone does not automatically roam, it just signals the client that roaming is required, but does not provide information on the APs. To perform automatic roaming, it is activated together with the ".11v BSS Transition" option activated, which enables the Optimized Roaming resource, being able to send information about the APs, by "Disassociation Imminent" message. While we can directly enable ".11k Neighbor List Dual Band" which already provides customers with a list of neighbors from the same WLAN and roaming can be enabled automatically.

upvoted 1 times

dropspablo 4 months ago

It is recommended to use 802.11v and 802.11k together. But 802.11k is preferable for roaming as the client receives the list of neighbors in advance by management frames. And in 802.11v (with Optimized Roaming feature) the client receives information from the APs only after a "Disassociation Imminent" message.
https://support.accessagility.com/hc/802.11k-802.11r-and-802.11v

upvoted 1 times

UnbornD9 5 months ago

I feel a little disheartened... I'm searching on CCNA Official Cert Guide PDF but none of these names are reported. So. Why there is this question in the exam?

upvoted 3 times

hamish88 7 months, 2 weeks ago

As far as I understand, Disassociation Imminent option doesn't help users at all to move around.

Within a BSS Transition Management Request, the Disassociation Imminent field can be added. This function is to disassociate the client after a period of time if the client does not re-associate with another AP.

However, as we want to have the roaming option for different types of devices which are of course limited to some frequencies and channels, I go with option D.

upvoted 2 times

freeknowledge123 8 months, 1 week ago

802.11k: Radio optimization
802.11r: Roaming optimization
802.11v:Management

upvoted 1 times

Request7108 8 months, 2 weeks ago

Selected Answer: D

11k neighbor lists come from the distribution system and are a range of potential roaming targets for the client. Instead of performing the normal off-channel scanning and full sweep, the client can immediately reach out on known channels for association. Of all the answers, 11k is the most helpful in fast roaming operations if the client can handle it.

upvoted 2 times

Question #335 *Topic 1*

Which two protocols are used by an administrator for authentication and configuration on access points? (Choose two.)

A. 802.1Q

B. RADIUS

C. Kerberos

D. TACACS+

E. 802.1x

Correct Answer: *BD*

Yunus_Empire Highly Voted 9 months, 2 weeks ago

Everyone Who Like My Comment Will Get 95%+ on CCNA Exam..Inshallah

upvoted 127 times

Anas_Ahmad 8 months, 2 weeks ago

Dua Qabool na hui to Dislike ker dun ga

upvoted 2 times

Yunus_Empire Highly Voted 9 months, 2 weeks ago

Eazy Question

upvoted 5 times

wakaish Most Recent 1 week ago

Option E (802.1x) is a port-based authentication protocol commonly used for controlling access to network ports, including those on access points, but it is not typically used for configuring access points; instead, it's used to control access to the network through them.

upvoted 1 times

yousef_feras 3 weeks, 6 days ago

the correct answer is B and E

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-6/configuration-guide/b_cg76/b_cg76_chapter_01101000.pdf

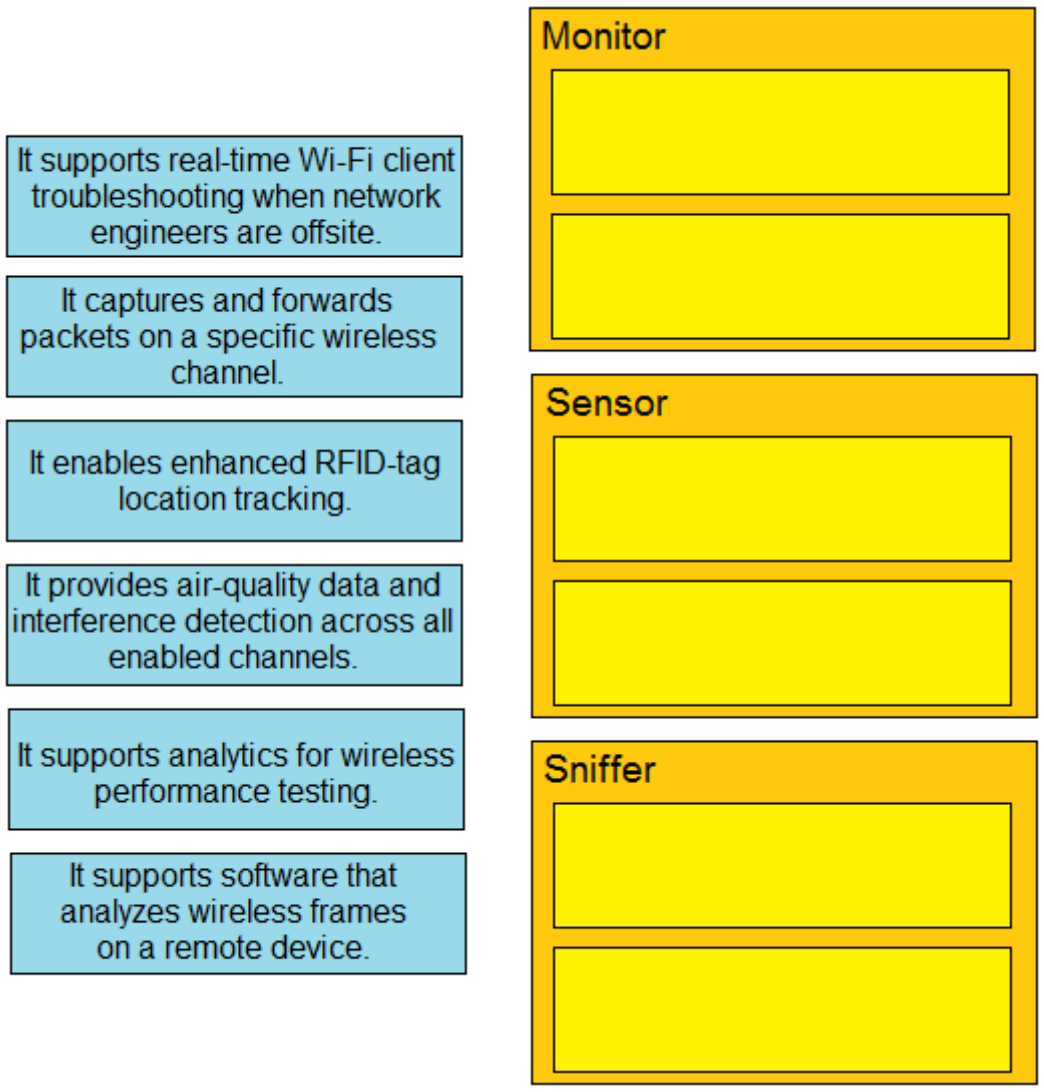
upvoted 2 times

Question #336 *Topic 1*

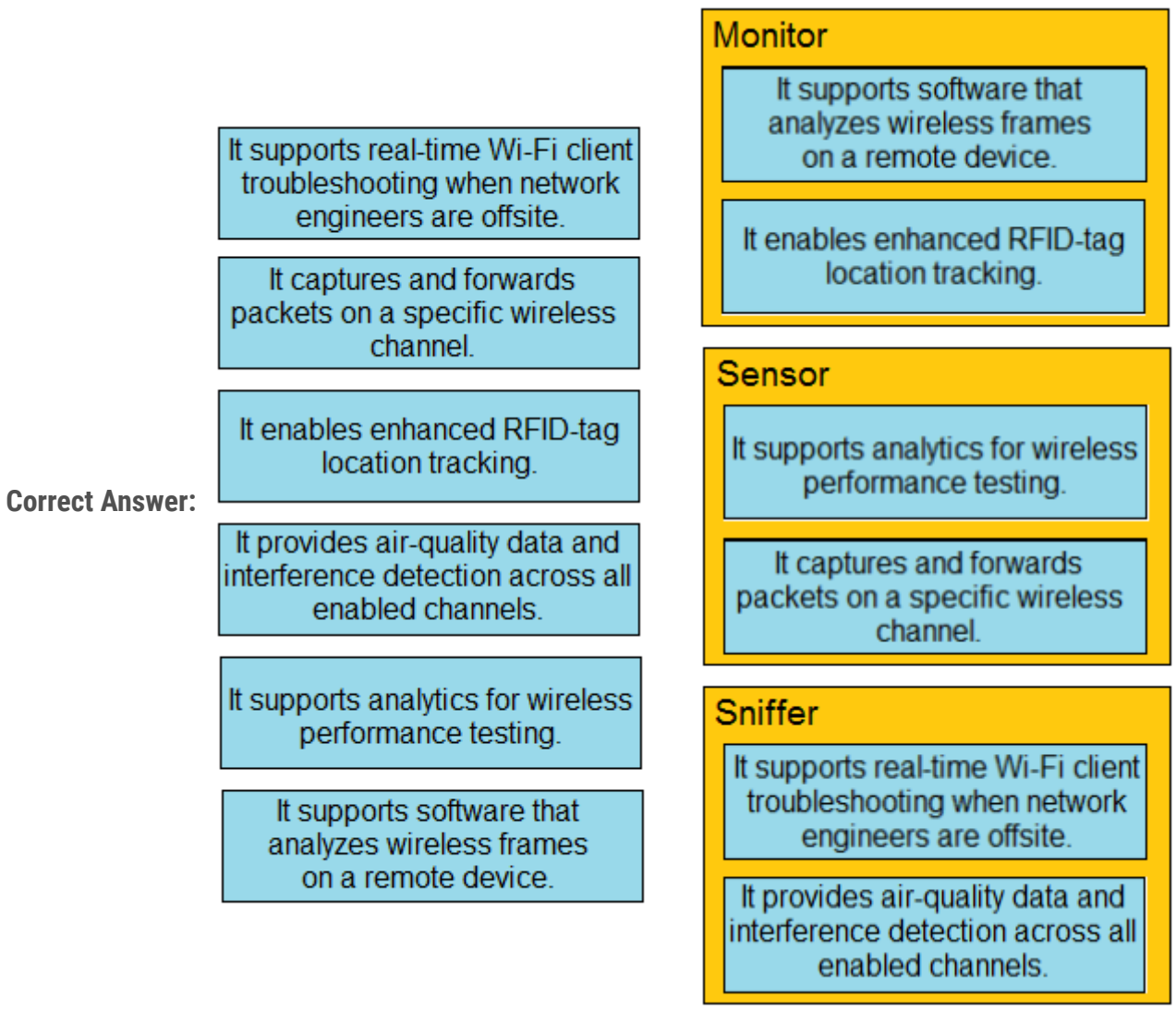
DRAG DROP -

Drag and drop the statements about access-point modes from the left onto the corresponding modes on the right.

Select and Place:



Correct Answer:



PiotrMar Highly Voted 1 year ago

not sure about the answers

upvoted 14 times

chuchuu Highly Voted 11 months ago

Monitor
It enables RFID-tag location tracking
It supports analytics for wireless performance testing

Sensor
it supports real time wifi client troubleshooting when network engineers are offline
It supports software that analyzes wireless frames on a remote device

Sniffer
it captures and forwards packets on a specific wireless channel
It enables air-quality data and interference detection across all enabled devices

monitor mode：https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/monitor-mode.pdf
sensor mode：https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/b_wl_16_10_cg_chapter_01101110.pdf
sniffer mode：https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/sniffer-mode.pdf

upvoted 8 times

chuchuu 11 months ago

sorry, I correct my answer as follows
Monitor
It enables RFID-tag location tracking
It supports software that analyzes wireless frames on a remote device

Sensor
it supports real time wifi client troubleshooting when network engineers are offline

It supports analytics for wireless performance testing

Sniffer
it captures and forwards packets on a specific wireless channel
It enables air-quality data and interference detection across all enabled devices

upvoted 2 times

dropspablo Most Recent 4 months ago

Monitor
- It enables enhanced RFID-tag location tracking.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/monitor-mode.pdf
- It provides air-quality data and interference detection across all enabled channels.
https://www.cisco.com/en/US/docs/switches/lan/catalyst3650/software/release/3se/consolidated_guide/configuration_guide/b_consolidated_3850_3se_cg_chapter_011011.html#task_8022D2989BD74F1E851BBA6C30992C2E

Sensor
- It supports real-time Wi-Fi client troubleshooting when network engineers are offsite.
- It supports analytics for wireless performance testing.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/monitor-mode.pdf

upvoted 5 times

dropspablo 1 month, 2 weeks ago

Rectifying the Sensor link:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Cisco_Aironet_Sensor_Deployment_Guide.html

upvoted 3 times

dropspablo 4 months ago

Sniffer
- It captures and forwards packets on a specific wireless channel.
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200527-Fundamentals-of-802-11-Wireless-Sniffing.html
- It supports software that analyzes wireless frames on a remote device.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-7/config-guide/b_wl_17_7_cg/m-sniffer-cg.html#:~:text=%E2%80%9Csniffer%E2%80%9D%2C%20which%20captures%20and%20forwards%20all%20the%20packets%20on%20a%20particular%20channel%20to%20a%20remote%20machine%20that%20runs%20packet%20analyzer%20software.

upvoted 4 times

freeknowledge123 8 months, 1 week ago

one of those: is the cup half empty or half full questions

upvoted 5 times

RougePotatoe 10 months ago

From Cert guide, nothing about sensor in the book.
Monitor: The AP does not transmit at all, but its receiver is enabled to act as a dedicated sensor. The AP checks for IDS events, detects rogue access points, and determines the position of stations through location-based services.

Sniffer: An AP dedicates its radios to receiving 802.11 traffic from other sources, much like a sniffer or packet capture device. The captured traffic is then forwarded to a PC running network analyzer software such as Wildpackets OmniPeek or WireShark, where it can be analyzed further.

upvoted 5 times

RougePotatoe 10 months ago

Based off the text from the cert guide I think the following fits best.
It enables enhanced RFID-tag location tracking (bit of a stretch but location services)
it provides air-quality data and interference detection across all enabled channels (detect rouge APs)

it supports analytics for wireless performance testing

it supports real-time wifi client troubleshooting when network engineers are offsite

it supports software that analyzes wireless frames on a remote device ("forwarded to a pc")
IT captures and forwards packets on a specific wireless channel (packet capture device)

upvoted 7 times

everchosen13 11 months, 2 weeks ago

Below is just one article I found. But I could not find anything about "sensor mode"
https://ipcisco.com/lesson/wireless-access-point-modes/

upvoted 1 times

splashy 12 months ago

Don't think that "sensor" is an official AP mode, but by elimination and using below sources i came to this result (please correct if wrong)

Monitor
It supports analytics for wireless performance testing

It supports software that analyzes wireless frames on a remote device

Sensor
It enables RFID-tag location tracking

It enables air-quality data and interference detection across all enabled devices

Sniffer
it supports real time wifi client troubleshooting when network engineers are offline

it captures and forwards packets on a specific wireless channel

https://community.cisco.com/t5/wireless/access-point-modes/td-p/1154701
https://study-ccnp.com/cisco-wireless-access-point-ap-modes-explained/
https://networklessons.com/cisco/ccna-200-301/cisco-wireless-ap-modes

upvoted 4 times

ShadyAbdekmalek 12 months ago

For me it would be more logic that way :

Monitor
It supports analytics for wireless performance testing

it supports real time wifi client troubleshooting when network engineers are offline

Sensor
It enables RFID-tag location tracking

It enables air-quality data and interference detection across all enabled devices

Sniffer
It supports software that analyzes wireless frames on a remote device

it captures and forwards packets on a specific wireless channel

upvoted 20 times

ac89l 4 months ago

I agree with this

upvoted 1 times

EliasM 11 months, 1 week ago

Agree with Shady. The purpose of Sniffer is to capture wireless frames and send those to a remote device (wireshark for instance) for analysis.

upvoted 1 times

splashy 11 months, 3 weeks ago

Thx for the comment,

but the description said the engineers are offsite, that made me decide to put it under sniffer.

upvoted 1 times

Question #337 *Topic 1*

A WLC sends alarms about a rogue AP, and the network administrator verifies that the alarms are caused by a legitimate autonomous AP. How must the alarms be stopped for the MAC address of the AP?

A. Remove the AP from WLC management

B. Place the AP into manual containment.

C. Manually remove the AP from Pending state.

D. Set the AP Class Type to Friendly.

Correct Answer: *B*

splashy Highly Voted 12 months ago

Keyword is "legitimate autonomous AP"

Answer is D

I think option B will kick the clients, which you probably don't want

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html#anc23

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html#anc34

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html#anc32

Also search for "Valid client on Rogue AP" in provided links

upvoted 14 times

everchosen13 11 months, 2 weeks ago

I agree basIn order to classify a rogue AP as friendly, malicious, or unclassified, navigate toMonitor > Rogue > Unclassified APs, and click the particular rogue AP name. Choose the option from the drop-down list, as shown in the image.ed on the article"
Taken from the article in the link
"

upvoted 3 times

everchosen13 11 months, 2 weeks ago

Didnt paste that in so smoothly but you get my point

upvoted 1 times

wakaish Most Recent 1 week ago

Manual containment is the appropriate action in this case. It allows you to manually identify the AP as legitimate and prevent the WLC from sending rogue AP alarms for that specific AP. This way, the WLC will stop treating it as a rogue and generating alarms while still being managed by the WLC.

upvoted 1 times

raul_kapone 4 weeks ago

Selected Answer: D

When the controller receives a rogue report from one of its managed access points, it responds as follows:
1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.

Source:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_0111010.html.xml

upvoted 1 times

raul_kapone 4 weeks ago

If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.

upvoted 1 times

lsuzu 4 months ago

Selected Answer: D

A WLC will send alarms about a rogue AP when it detects an AP that is not under its management. This can happen when a legitimate autonomous AP is installed on the network. To stop the alarms, the network administrator must set the AP Class Type to Friendly. This will tell the WLC that the AP is a legitimate AP and that it should not send alarms about it.

The other options are incorrect for the following reasons:

Removing the AP from WLC management will stop the alarms, but it will also prevent the WLC from managing the AP. This is not necessary, since the AP is a legitimate AP.
Placing the AP into manual containment will stop the alarms, but it will also prevent the AP from being used by clients. This is not necessary, since the AP is a legitimate AP.
Manually removing the AP from Pending state will not stop the alarms. The WLC will continue to send alarms about the AP until the AP Class Type is set to Friendly.

upvoted 2 times

liviuml 5 months ago

Selected Answer: D

Answer is D.

Search for "Table 1. Classification Mapping" in following link:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_0111010.html.xml
Regards,

upvoted 1 times

Ciscoman021 5 months, 2 weeks ago

Selected Answer: B

If the alarms sent by the WLC are caused by a legitimate autonomous AP, the most appropriate action to stop the alarms for the MAC address of the AP is:

B. Place the AP into manual containment.

Manual containment is a method used to block a rogue AP and prevent it from interfering with the wireless network. It is a more targeted and less disruptive method compared to removing the AP from WLC management altogether, which would result in loss of connectivity for the AP.

upvoted 1 times

linuxlife 5 months, 3 weeks ago

Rogue Classification Rules

Rogue classification rules, allow you to define a set of conditions that mark a rogue as either malicious or friendly. These rules are configured at the PI or the WLC, but they are always performed on the controller as new rogues are discovered.

upvoted 1 times

linuxlife 5 months, 3 weeks ago

Rogue Containment

Containment is a method that uses over-the-air packets to temporarily interrupt service on a rogue device until it can physically be removed. Containment works with the spoof of de-authentication packets with the spoofed source address of the rogue AP so that any clients associated are kicked off.

upvoted 1 times

linuxlife 5 months, 3 weeks ago

https://www.cisco.com/c/dam/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00-14.jpeg

upvoted 1 times

fjori 9 months, 3 weeks ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010111001.html

Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. An example is the access points in your lab network.

External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. An example is an access point that belongs to a neighboring coffee shop.

Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list.

upvoted 2 times

alejandro12 9 months, 4 weeks ago

Answer is D

upvoted 2 times

Etidic 10 months, 4 weeks ago

Selected Answer: D

The Answer is D

upvoted 4 times

Question #338 *Topic 1*

What is one reason to implement LAG on a Cisco WLC?

A. to increase security and encrypt management frames

B. to enable connected switch ports to failover and use different VLANs

C. to provide link redundancy and load balancing

D. to allow for stateful and link-state failover

Correct Answer: *C*

[Removed] 3 months ago

Selected Answer: C

Correct answer is C

upvoted 1 times

perri88 3 months ago

Selected Answer: C

C is correct

upvoted 1 times

Vyncy 3 months, 2 weeks ago

hello beautiful

upvoted 1 times

ananinamia 3 weeks, 6 days ago

HI BABY

upvoted 1 times

Question #339 *Topic 1*

When an access point is seeking to join wireless LAN controller, which message is sent to the AP-Manager interface?

A. Discovery response

B. DHCP request

C. DHCP discover

D. Discovery request

Correct Answer: *C*
The LAPs always connect to the management interface address of the controller first with a discovery request. The controller then tells the LAP the Layer 3 AP- manager interface (which can also be the management by default) IP address so the LAP can send a join request to the AP-manager interface next.
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html

perri88 3 months ago

Selected Answer: D

Can the answer be updated to D please?

upvoted 2 times

YongS0925 6 months ago

S/b join request which was not listed

upvoted 1 times

checkoboy88 6 months, 3 weeks ago

Selected Answer: D

D is the correct one

upvoted 1 times

daddydagoth 6 months, 3 weeks ago

Selected Answer: D

It's bloody D. Who the hells fact checks this answers?

upvoted 4 times

DB_Cooper 7 months, 2 weeks ago

Selected Answer: D

discovery request

upvoted 1 times

BreezyNet 8 months, 3 weeks ago

the person that post this question and put the answer as C is a fool lmao, even the site reference he put says D is the correct answer, shaking my head.

upvoted 1 times

Anas_Ahmad 9 months ago

Selected Answer: D

D is right answer

upvoted 1 times

Elidor 10 months, 1 week ago

It's D lol

upvoted 1 times

Drei0213 10 months, 3 weeks ago

I think c before send a request the need to send discover first

upvoted 2 times

Etidic 10 months, 4 weeks ago

Selected Answer: D

The answer is D

upvoted 1 times

everchosen13 11 months, 2 weeks ago

Selected Answer: D

Lol its definitely D..

upvoted 3 times

splashy 12 months ago

Selected Answer: D

The provided link and explanation literally point to D :)

upvoted 3 times

Bibi20 1 year ago

Selected Answer: D

I think the right answer is D,

upvoted 2 times

shubhambala 1 year ago

Selected Answer: D

D people

upvoted 3 times

PiotrMar 1 year ago

Selected Answer: D

its a D

upvoted 2 times

shubhambala 1 year ago

Selected Answer: D

Right answer is D https://mrncciew.com/2013/03/17/ap-registration/

upvoted 4 times

Question #340 *Topic 1*

Refer to the exhibit. A network engineer configures the Cisco WLC to authenticate local wireless clients against a RADIUS server. Which task must be performed to complete the process?

A. Change the Support for CoA to Enabled

B. Select Enable next to Management

C. Select Enable next to Network User

D. Change the Server Status to Disabled

Correct Answer: *C*

RougePotatoe Highly Voted 10 months, 3 weeks ago

Selected Answer: C

Network users is for authenticating the people connected to the wireless network.
Management is for authentication people who try to login to the WLC.
https://mrncciew.com/2013/04/21/configuring-radius-on-wlc/

upvoted 6 times

[Removed] Most Recent 3 months ago

In Netacad courses, in the part in which they talk about "Configure RADIUS Server Information" both Network User and Management are checked so this is a very tricky question.

upvoted 1 times

FALARASTA 4 months, 3 weeks ago

So the goal is wireless clients and not management.

upvoted 1 times

enzo86 5 months ago

Selected Answer: B

Check the Management box , if you want to allow the RADIUS Server to authenticate users who login to the WLC.
(I don't want to authenticate the WLC users via RADIUS)------>NETWORK USER
https://rscciew.wordpress.com/2014/01/25/configure-radius-server-on-wlc/

upvoted 2 times

Etidic 10 months, 4 weeks ago

Selected Answer: C

Network user = enabled is a must
Management is not compulsory
"If you are not authenticating management user via RADIUS then you must disable it"

upvoted 2 times

yavuzcangiz 11 months, 1 week ago

Hi @everchosen13 management is not a must according to the page you have shared

upvoted 2 times

everchosen13 11 months, 2 weeks ago

Don't both boxes need to be checked? Management and Network?
https://rscciew.wordpress.com/2014/01/25/configure-radius-server-on-wlc/

upvoted 1 times

Question #341 *Topic 1*

After installing a new Cisco ISE server which task must the engineer perform on the Cisco WLC to connect wireless clients on a specific VLAN based on their credentials?

A. Disable the LAG Mode on Next Reboot.

B. Enable the Event Driven RRM.

C. Enable the Allow AAA Override.

D. Enable the Authorize MIC APs against auth-list or AAA

Correct Answer: *C*

daddydagoth Highly Voted 6 months, 3 weeks ago

Is this even on the CCNA?

upvoted 11 times

[Removed] 3 months ago

No, not the CCNA 200-301 anyway. Maybe it was in previous CCNAs or is it CCNP? I'm not sure

upvoted 1 times

Cynthia2023 Most Recent 1 month ago

Selected Answer: C

Enabling the "allow AAA Override" option on a Cisco Wireless LAN Controller (WLC) allows the controller to forward the user authentication and authorization information to an external AAA (Authentication, Authorization, and Accounting) server, such as Cisco Identity Services Engine (ISE), for further policy enforcement.

upvoted 2 times

perri88 3 months ago

Another one that I haven't seen in any CCNA Course.

upvoted 2 times

[Removed] 3 months ago

Because this is not CCNA 200-301 related

upvoted 1 times

GigaGremlin 11 months, 1 week ago

Answer C is correct,...
In order to support centralized access control through a centralized AAA server such as the Cisco Identity Services Engine (ISE) or ACS, the IPv6 ACL can be provisioned on a per-client basis using AAA Override attributes. In order to use this feature, the IPv6 ACL must be configured on the controller and the WLAN must be configured with the AAA Override feature enabled.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-6/configuration-guide/b_cg76/b_cg76_chapter_0111001.pdf

upvoted 3 times

Goh0503 11 months, 2 weeks ago

https://rscciew.wordpress.com/2015/01/08/dynamic-vlan-assignment-with-acs-server/

upvoted 4 times

Hope_12 4 months, 1 week ago

Thanks for this link.

upvoted 2 times

Question #342 *Topic 1*

Refer to the exhibit. Router R1 is running three different routing protocols. Which route characteristic is used by the router to forward the packet that it receives for destination IP 172.16.32.1?

```
R1# show ip route
....
D       172.16.32.0/27      [90/2888597172] via 20.1.1.1
O       172.16.32.0/19      [110/292094] via 20.1.1.10
R       172.16.32.0/24      [120/2] via 20.1.1.3
```

A. longest prefix

B. administrative distance

C. cost

D. metric

Correct Answer: *A*

rlelliott Highly Voted 1 year, 6 months ago

I saw a bunch, bunch, bunch of these on the CCNA. They were all pretty easy. Find the network that the IP fits in, look at the prefix length, if you have 1 that is longer than the rest chhose that as answer. If there is more than 1 with the same longest prefix move over to AD and pick the lowest value. Once again if duplicate lowest move over to metric. Watch for the tricky non-default AD and DO NOT pick by code letter because they change ADs on some of them.

upvoted 39 times

ZUMY Highly Voted 1 year, 2 months ago

A is right
Routing preference
*Longest Prefix
*AD
*Metric

upvoted 6 times

[Removed] Most Recent 3 months ago

Selected Answer: A

A - Longest prefix

upvoted 1 times

Ciscoman021 5 months, 3 weeks ago

Selected Answer: B

The route characteristic used by the router to forward the packet for the destination IP 172.16.32.1 is:

B. administrative distance

Explanation:

From the output of the "show ip route" command, we can see that there are three different routes for the destination IP 172.16.32.1 with different routing protocols and administrative distances:

D 172.16.32.0/27[90/2888597172] via 20.1.1.1 (EIGRP)
O 172.16.32.0/19[110/292094] via 20.1.1.10 (OSPF)
R 172.16.32.0/24[120/2] via 20.1.1.3 (RIP)

The administrative distance is a measure of the trustworthiness of the source of the routing information. The lower the administrative distance, the more trustworthy the source. When there are multiple routes to the same destination, the router will choose the one with the lowest administrative distance. In this case, the route with the lowest administrative distance is the RIP route, which has an administrative distance of 120. Therefore, the router will use this route to forward packets to the destination IP 172.16.32.1.

upvoted 1 times

YongS0925 6 months, 2 weeks ago

When a router is running multiple routing protocols and has multiple routes to the same destination network, it will use the administrative distance to determine which route to use. The administrative distance is a value assigned to each routing protocol, which indicates the trustworthiness of the routing information provided by that protocol.

In general, the router will prefer the route with the lowest administrative distance, regardless of the prefix length or any other factors. If there are multiple routes with the same administrative distance, the router will then use the longest prefix match to determine the best route.
???

upvoted 2 times

DevNetAdmin 6 months, 2 weeks ago

A router uses longest prefix match when it has multiple routes to a destination with different prefix lengths. The router prefers the most specific prefix that matches the destination IP address bit-by-bit regardless of the cost or metric associated with each route.

upvoted 3 times

Etidic 10 months, 4 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

DARKK 1 year, 3 months ago

Selected Answer: A

/27 is the Highest prefix inclusive of the destination IP address therefore the router uses that route based on the Longest Prefix First rule.

upvoted 3 times

Tera_911 1 year, 4 months ago

In the given question all routes have same prefix so it would use AD .Therefore ,it should B.

upvoted 2 times

DARKK 1 year, 3 months ago

That is 100% wrong buddy. /27 is the Highest prefix inclusive of the destination IP address therefore the router uses that route.

upvoted 2 times

ismatdmour 1 year, 6 months ago

Selected Answer: A

Surely A. Answers B, C and D plays ahead in building the routing table while choice A (longest prefix match) plays later in selecting which route for a host that fits in the many target subnets in the routing table.
Remember first that the routing table shall have only one route to any one subnet (except for load balancing cases which needs more detail I like to skip here). Two subnets are not the same subnet if they differ in either subnet ID and/or Subnet mask.
Answer B, Administrative distance plays first to select which route to be inserted when we have 2 routes learned by the router using 2 different routing protocols. In this case the route with the lowest AD will be inserted.
Answer C (Cost for ospf) and answer D (metric in general) are used (lowest value) to select between 2 routes learned using the same protocol)
In the question, we have 3 routes to 3 different subnets, but if the host belongs to more then one (all of them in this case), we select the more specific subnet (the one with the longest match as our route)

upvoted 4 times

gachocop3 1 year, 6 months ago

typo - longest prefix

upvoted 2 times

gachocop3 1 year, 6 months ago

A is the correct answer
Multiple routing protocols to different destinations- longest distance.

upvoted 2 times

Stonetales987 1 year, 10 months ago

It's easier to see when you convert the Network addresses to binary. I associate the longest prefix to more specific. The /27 has 27 1 bits in the network address portion of the IP vs the 24 and 19...
/27 11111111.11111111.11111111.111 00000
/24 11111111.11111111.11111111 .00000000
/19 11111111.11111111.111 00000.00000000

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html#classless

upvoted 4 times

aliwqa777 2 years, 5 months ago

I would be glad if there is someone who can fully explain this question

upvoted 4 times

UmbertoReed 2 years, 5 months ago

The way I understand it, when you have multiple routes to reach a destination, the first criteria for choosing is which one has the longest prefix. If one of the routes has a longer prefix than the other ones, that's the only criteria considered and that route is chosen.

If the routes had the same prefix length, in that case administrative distance would come into play. But since one of the routes had a longer prefix, it didn't come down to the AD.

upvoted 14 times

SparkySM 1 year, 8 months ago

Good explanation UmbertoReed

upvoted 1 times

jerry19 2 years, 4 months ago

To caveat, if the routes had the same AD, then the metric would be the determining factor.

upvoted 3 times

SScott 2 years, 1 month ago

Right, but go back a bit before the metric and what is that primarily based on, an AD and that is calculated from the subnet mask and prefix, right? Cisco test writers are trying to determine our initial thought process with approaching and evaluating any field IP network, broadcast and routable IP issue....Choice A comes first in the perpetual flowchart.

upvoted 1 times

SScott 2 years, 1 month ago

Right do you like cider[apple]/cidr (longest prefix) or administration/ive (distance) better -- cidr subnet calculations of course! Well a silly but effective way to remember the answer :)

upvoted 4 times

FGR1987 2 years ago

Always longest prefix will be elected!

upvoted 3 times

potasio101 2 years, 2 months ago

Router Preference
*Longest Prefix
*AD
*Metric

upvoted 10 times

SScott 2 years, 1 month ago

Yes, cisco track statements are the bomb! (prefix precedes AD). Difficult config level indeed but w/out prefix consideration/calc the AD is invalid or rather irrelevant.

https://community.cisco.com/t5/switching/please-explain-how-the-longest-prefix-matching-works/td-p/2891235

https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r3-9/system_management/command/reference/yr39xr12k_chapter10.html

https://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/system_management/command/reference/yr37obj.html

A leads to B, chicken before the egg, right but of course debatable for some

upvoted 1 times

hadesmv666 2 years, 6 months ago

Correct Answer is A
View Making Forwarding Decisions on:https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html

upvoted 3 times

Nhan 2 years, 6 months ago

Correct answer is Administrarive distance which is B

upvoted 2 times

SasithCCNA 2 years, 6 months ago

No, in this case the longest prefix rule comes into play so answer A is correct.

upvoted 5 times

SScott 2 years, 1 month ago

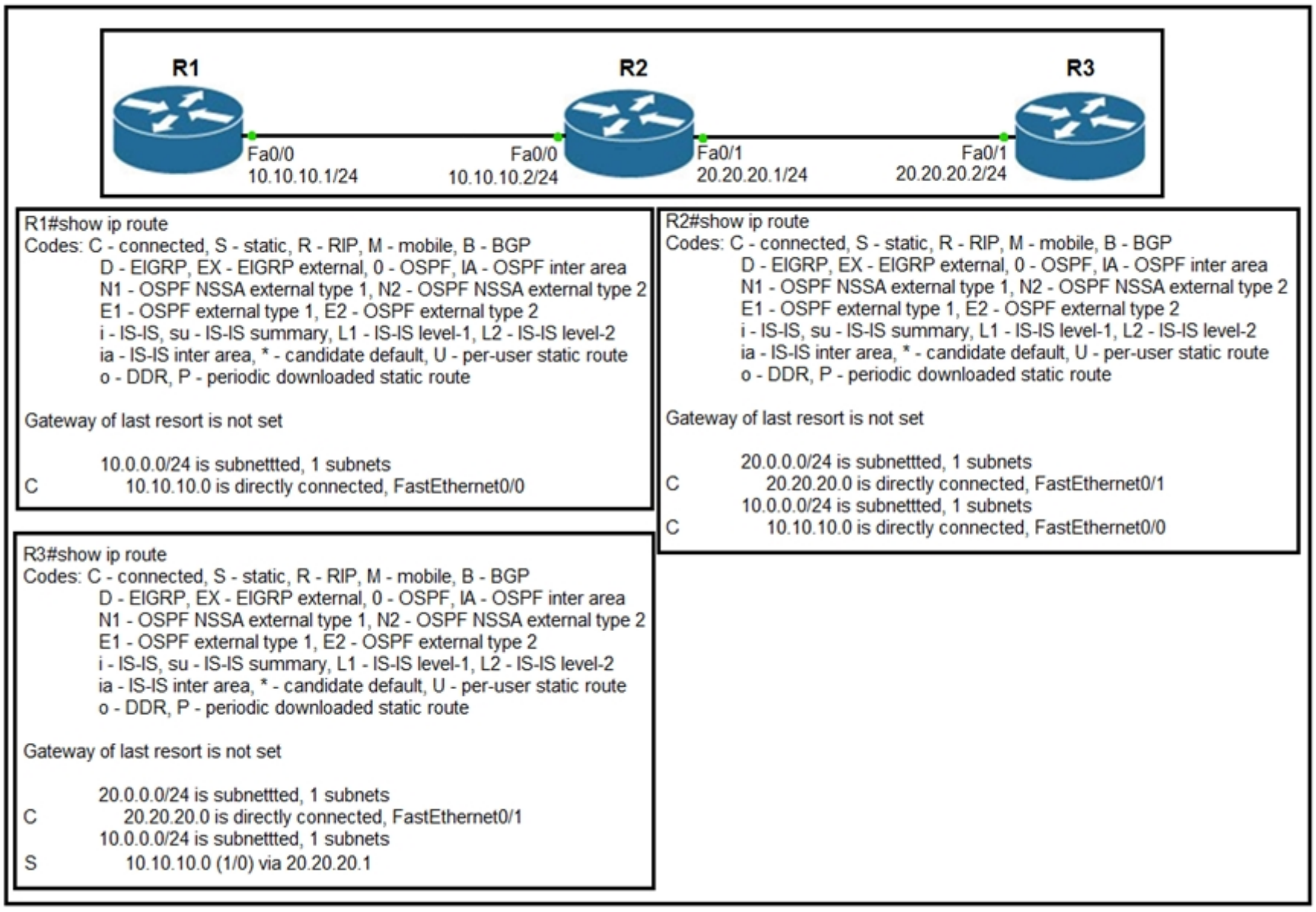
Correct, here is a good article
https://www.geeksforgeeks.org/longest-prefix-matching-in-routers/

Ouch, those people, I know.... but same networking concept. Forgive the competitor URL https://aws.amazon.com/blogs/networking-and-content-delivery/influencing-traffic-over-hybrid-networks-using-longest-prefix-match/

upvoted 1 times

Question #343 *Topic 1*

Refer to the exhibit. Router R1 Fa0/0 cannot ping router R3 Fa0/1. Which action must be taken in router R1 to help resolve the configuration issue?



A. set the default gateway as 20.20.20.2

B. configure a static route with Fa0/1 as the egress interface to reach the 20.20.2.0/24 network

C. configure a static route with 10.10.10.2 as the next hop to reach the 20.20.20.0/24 network

D. set the default network as 20.20.20.0/24

Correct Answer: *C*

vadiminski Highly Voted 2 years, 4 months ago

The given answer is correct

upvoted 6 times

SScott 2 years, 1 month ago

That's it

https://www.cisco.com/c/en/us/support/docs/dial-access/floating-static-route/118263-technote-nexthop-00.html#:~:text=A%20traceroute%20from%20the%20host%20to%20the%20Internet%20host%2010.100.1.1%20shows%20this

upvoted 2 times

ZUMY Highly Voted 1 year, 2 months ago

C is correct

upvoted 6 times

freeknowledge123 Most Recent 8 months, 1 week ago

Selected Answer: C

C is correct.

upvoted 3 times

Question #344 *Topic 1*

By default, how does EIGRP determine the metric of a route for the routing table?

A. It uses the bandwidth and delay values of the path to calculate the route metric.

B. It uses a default metric of 10 for all routes that are learned by the router.

C. It counts the number of hops between the receiving and destination routers and uses that value as the metric.

D. It uses a reference bandwidth and the actual bandwidth of the connected link to calculate the route metric.

Correct Answer: *A*

Harryjio Highly Voted 3 years, 1 month ago
A- EIGRP,
C- RIP
D-OSPF
upvoted 32 times

Hope_12 4 months, 1 week ago
B. is use for IS - IS
upvoted 1 times

SScott 2 years, 1 month ago
On point
upvoted 4 times

Heymannicerouter Highly Voted 2 years ago
EIGRP is no longer on the CCNA exam objectives btw
upvoted 6 times

[Removed] 3 months ago
Exactly!
upvoted 1 times

everchosen13 11 months, 2 weeks ago
Yes but you still might see a question on the subject just not a main focus
upvoted 2 times

[Removed] 3 months ago
This wouldn't be fair at all. It's not even on Cisco Netcad courses.
upvoted 1 times

ZUMY Most Recent 1 year, 2 months ago
A correct
upvoted 1 times

DARKK 1 year, 3 months ago
Selected Answer: A
A is correct
upvoted 1 times

examcol 3 years, 1 month ago
A is correct answer.
https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#anc6
upvoted 5 times

tyuipo 2 years, 4 months ago
tldr:
"EIGRP uses the minimum bandwidth on the path to a destination network and the total delay to compute routing metrics"
upvoted 4 times

Question #345 *Topic 1*

Router R1 must send all traffic without a matching routing-table entry to 192.168.1.1. Which configuration accomplishes this task?

A. R1#config t R1(config)#ip routing R1(config)#ip route default-route 192.168.1.1

B. R1#config t R1(config)#ip routing R1(config)#ip route 192.168.1.1 0.0.0.0 0.0.0.0

C. R1#config t R1(config)#ip routing R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1

D. R1#config t R1(config)#ip routing R1(config)#ip default-gateway 192.168.1.1

Correct Answer: *C*

FloridaMan88 Highly Voted 2 years, 7 months ago

This text appears to be from a L3 switch. On a router there is no need to turn on (config)# "ip routing" first and then the default route command.

it should be: R1# conf t R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

upvoted 13 times

Airrat 2 years, 2 months ago

It's true

upvoted 5 times

sdokmak Highly Voted 2 years, 3 months ago

This one stumped me because I figured 192.168.1.1 would be the destination address, but it should be the next hop address. So it's C

upvoted 9 times

gc999 Most Recent 6 months ago

For answer "C", just want to know if it would be shown on the routing table? If yes, then the answer should not be "C"

upvoted 1 times

Etidic 10 months, 4 weeks ago

Selected Answer: C

Answer is C

upvoted 3 times

ZUMY 1 year, 2 months ago

C is correct

upvoted 2 times

MrBadger 1 year, 5 months ago

IP default-gateway I see this as for the switch rather then data-plane traffic, might not be a strictly true but it's a good way of thinking about its function.

upvoted 1 times

Jonfernz 2 years, 4 months ago

Packets that do not match routes in the table must be sent to the default route. Hence the command to establish a default route is required here.

upvoted 4 times

Raymond9 2 years, 9 months ago

IP Default-Gateway" is usually used on switches that are not L3 switches/routers or on "hosts "IP Route 0.0.0.0" is usually used on devices that are L3 eg Layer 3 switches/routers etc

ref:https://ipwithease.com/difference-between-ip-default-gateway-and-ip-route-0-0-0-0/

upvoted 4 times

TA77 1 year, 2 months ago

Just to clarify the sentence:
"ip default-gateway" is usually used on Layer 2 switches and on hosts.
"ip route 0.0.0.0" is usually used on Layer 3 switches and on routers.

upvoted 4 times

Harryjio 3 years, 1 month ago

Need to make subnet and mask to zero

upvoted 3 times

Question #346 *Topic 1*

A packet is destined for 10.10.1.22. Which static route does the router choose to forward the packet?

A. ip route 10.10.1.0 255.255.255.240 10.10.255.1

B. ip route 10.10.1.20 255.255.255.252 10.10.255.1

C. ip route 10.10.1.16 255.255.255.252 10.10.255.1

D. ip route 10.10.1.20 255.255.255.254 10.10.255.1

Correct Answer: *B*

alexiro Highly Voted 3 years, 1 month ago

Network 10.10.1.20 /30
host range 10.10.1.21 - 10.10.1.22

upvoted 38 times

uevenasdf Highly Voted 2 years, 8 months ago

10.10.1.20 /30

20 = .000101[00] network
21 = .000101[01] host
22 = .000101[10] host
23 = .000101[11] broadcast

upvoted 25 times

cormorant Most Recent 10 months, 2 weeks ago

wouldn't the router prefer the route with the longest prefix length? whatever happened to this rule?!

upvoted 3 times

andresfjardim 7 months, 2 weeks ago

The /31 would make ip's .20 and .21 on a p2p link.

It asks for .22 so answer is correct.

upvoted 1 times

binrayelias 8 months ago

/31 can be used as p2p

upvoted 1 times

binrayelias 8 months ago

I agree so I choose D as the answer

upvoted 1 times

bruno0147 10 months, 3 weeks ago

No CCNA as perguntas são mal elaboradas dessa forma? Alguém pode nos dizer?

upvoted 1 times

Customexit 10 months, 3 weeks ago

This is B for example:

GROUP SIZE: 128 64 32 16 8 [4] 2 1
SUBNET: 128 192 224 240 248 [252] 254 255
CIDR: /25 /26 /27 /28 /29 [/30] /31 /32

10.10.1.20
Group size is 4. Start at 0 and go up by 4. 4, 8, 12, 16, 20, 24.
We land on 20 so that's the network.
Notice I continued to .24 instead of stopping at .20.

.24 is the next subnet.
.23 is the broadcast.
.22 is the last usable host.
.21 is the first usable.
.20 is the network.

upvoted 2 times

Etidic 10 months, 4 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

ZUMY 1 year, 2 months ago

B is right
Network portion|Host portion
30 | 2
Possible host
2^n=2^2=4 host
20 = .000101[00] network
21 = .000101[01] host
22 = .000101[10] host
23 = .000101[11] broadcast

upvoted 2 times

taiyi078 1 year, 9 months ago

Why is it /30? Where can I find it?

upvoted 4 times

zizo1982 2 years ago

- the destined ip address is 10.10.1.22
A- the range is 10.10.1.0 to 10.10.1.15 --> wrong range
B- the range is 10.10.1.20 to 10.10.1.23 --> right range
C- the range is 10.10.1.16 to 10.10.1.19 --> wrong range
D- the range is 10.10.1.20 to 10.10.1.21 --> wrong range
So the only correct range is answer B, so B is the correct answer
if there are more than 1 correct range, then the correct answer will be the range with the longer prefix.

upvoted 8 times

Hoklengz 2 years ago

B is correct

upvoted 3 times

CiscoTerminator 2 years ago

255.255.255.254 is a /31 which means viable routes are 10.10.1.20 and 10.10.1.21 ONLY. 10.10.1.22 is left out hence why this is the wrong answer.

upvoted 1 times

CISCO2022 2 years, 3 months ago

Router(config-if)#ip address 192.168.0.1 255.255.255.254
Bad mask /31 for address 192.168.0.1
.254 is broadcast address for /31 not valid
the longest prefix here is .252 /30

upvoted 3 times

Mardin94 2 years, 3 months ago

Can someone explain for me :(

upvoted 2 times

shanem 2 years, 2 months ago

It's using the longest match rule. IE, the longest subnet will be routed first. 255.255.255.254 is /30, which is longer than any of the other ranges that still include the target address.

upvoted 5 times

shanem 2 years, 2 months ago

Sorry I meant 255.255.255.252

upvoted 4 times

DickFrancis 2 years, 4 months ago

pretty sure 255.255.255.254 is a /31 (not /30) so B is correct

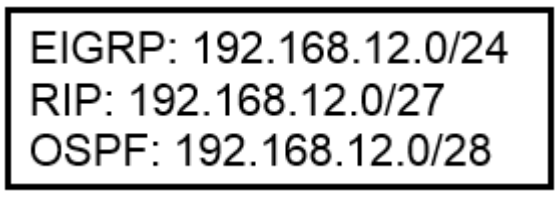
upvoted 2 times

cormorant 10 months, 2 weeks ago

but wouldn't this mean that this should be chosen as it has teh longest prefix length?

upvoted 1 times

Question #347 *Topic 1*



Refer to the exhibit. How does the router manage traffic to 192.168.12.16?

A. It chooses the EIGRP route because it has the lowest administrative distance.

B. It load-balances traffic between all three routes.

C. It chooses the OSPF route because it has the longest prefix inclusive of the destination address.

D. It selects the RIP route because it has the longest prefix inclusive of the destination address.

Correct Answer: *D*

MM_9 Highly Voted 2 years, 8 months ago

The answer is wrong. The router can't use the network OSPF because it's another network and not include the destination address (192.168.12.0/28 --> from 192.168.12.0 to 192.168.12.15). The correct answer is D because the RIP route use a /27 subnet and include the destination address (192.168.12.0/27 --> from 192.168.12.0 to 192.168.12.31).
If i wrong please correct me

upvoted 53 times

SScott 2 years, 1 month ago

D is correct. C is wrong since 192.168.12.16 is outside the host address range; therefore, a mask of 255.255.255.224 is able to route traffic properly with RIP /27

upvoted 7 times

Pkard 1 year, 11 months ago

This completely depends upon if the 192.168.12.16 in the question is a destination network or host address. If it's the destination network then 192.168.12.0/28 is correct since 192.168.12.16 is a network and not a host IP. If 192.168.12.16 is a host IP then the answer is 192.168.12.0/27. In my opinion the question isn't clear but I read it as the destination network.

upvoted 12 times

uevenasdf 2 years, 8 months ago

You're right C is wrong D is correct

upvoted 9 times

thegolden3 2 years, 5 months ago

yes, D is correct because the C addresses are 192.168.12.0-> subnet address and the last 192.168.12.15-> broadcast address

upvoted 5 times

Ali526 Highly Voted 2 years, 8 months ago

D is correct. OSPF with /28 does NOT include .16, stops at .14, .15 broadcast.

upvoted 17 times

lxlJustinlxl 2 years, 4 months ago

And even if they wanted to make this a 'trickier' question, they should have had the last one as 192.168.12.16/28. It would include the address in the range but answer would still be D since .16 would be network address. Basically, a .16 address on a /28 network can never be a host address.

upvoted 4 times

daddydagoth 6 months, 3 weeks ago

Even if it is not a host address, I am pretty sure the router will still chose the OSPF route in the case you described.

upvoted 1 times

shumps Most Recent 3 weeks, 6 days ago

Just to add on D is correct since RIP has the length of 32-2=30 which can accommodate the destination. Where as OSPF has a length of 16-2=14

upvoted 1 times

binrayelias 8 months ago

C is the answer.For IPv4, the destination address can be a host, network, subnetwork, supernetwork, or default address.
https://www.ibm.com/docs/en/zos/2.4.0?topic=panel-destination-address

upvoted 1 times

binrayelias 8 months ago

I take back C and choose D as the answer cuz since in /27 only stops at 15 so it is not inclusive in the dest address.

upvoted 1 times

atika870 8 months, 2 weeks ago

D. It selects the RIP route because it has the longest prefix inclusive of the destination address.

I've seen this question somewhere else and the answer they gave for OSPF here wasn't the same, just think they trying to trick people but I hope what I shared can help anyone here new looking for explanation to this question like me.

A router evaluates routes in the following order.
1. Prefix Length - The longest-matching route is preferred first. Prefix length trumps all other route attributes.
2. Administrative Distance - In the event there are multiple routes to a destination with the same prefix length, the route learned by the protocol with the lowest administrative distance is preferred.
3. Metric - In the event there are multiple routes learned by the same protocol with same prefix length, the route with the lowest metric is preferred. (If two or more of these routes have equal metrics, load balancing across them may occur.)

upvoted 2 times

Etidic 10 months, 4 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

everchosen13 11 months, 2 weeks ago

D is correct it would use RIP.
/28 = 0 - 15. 16 is out of the scope

upvoted 1 times

ZUMY 1 year, 2 months ago

D is correct

upvoted 1 times

DARKK 1 year, 3 months ago

Selected Answer: D

D is correct, I choses Rip because OSPF (/28) Is not inclusive of the IP address. 0-15 = 16 IPs = /28. RIP is because /27 = 32 IPs, 0-31

upvoted 1 times

dave1992 1 year, 9 months ago

Selected Answer: D

D longest prefix

upvoted 2 times

Anarckii 1 year, 9 months ago

Selected Answer: D

C is the only other "closest" subnet but the broadcast ends at .15 and the next Subnet ID would be .16 which couldn't be used as the first IP address. So D would be correct with an address range from .1-.30

upvoted 2 times

shakyak 1 year, 10 months ago

RIp is correct, 32-28 = 4, 2^4=16
usable IP range is 192.168.12.0 -192.168.12.15 so OSPF doesn't cover the network.

upvoted 3 times

kokoyul 1 year, 11 months ago

D es la correcta: https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html

upvoted 1 times

Adekoya_Oluwatobi 2 years ago

I think the correct answer is A. I believe that when a router is using different routing protocols, the protocol with the lowest administrative distance (EIGRP in this case) is used to route the packet.
EIGRP - 90
RIP - 120
OSPF -110

upvoted 2 times

RougePotatoe 10 months, 3 weeks ago

His assumption is incorrect. administrative distance only come into play when the networks are the same. /24, /27, and /28 are different networks. Thus the network with the closest match will be selected; in this case it is /27 because /28 doesn't include .16 as it is the start of a different network.

upvoted 3 times

Chenet 1 year, 12 months ago

You are Lost my friend!

upvoted 7 times

illuded03jolted 1 year, 3 months ago

1. Longest Prefix
2. Administrative distance
3. Metric

upvoted 2 times

Pamirt 2 years, 1 month ago

D is the correct answer.

upvoted 3 times

kardashian25 2 years, 1 month ago

very wrong answer .
.16 is not included to /28 network so the answer has to be RIP
please do change it. thank you

upvoted 3 times

CiscoTerminator 2 years, 1 month ago

C is definitely wrong as it does not accommodate .16 in that subnet. D is the correct answer!

upvoted 2 times

Question #348 *Topic 1*

What are two reasons for an engineer to configure a floating static route? (Choose two.)

A. to enable fallback static routing when the dynamic routing protocol fails

B. to route traffic differently based on the source IP of the packet

C. to automatically route traffic on a secondary path when the primary path goes down

D. to support load balancing via static routing

E. to control the return path of traffic that is sent from the router

Correct Answer: *AC*

dicksonpwc Highly Voted 2 years, 1 month ago

Floating static routes are static routes that have an administrative distance greater than the administrative distance of dynamic routes. Administrative distances can be configured on a static route so that the static route is less desirable than a dynamic route. In this manner, the static route is not used when the dynamic route is available. However, if the dynamic route is lost, the static route can take over, and traffic can be sent through this alternate route. If this alternate route is provided using a DDR interface, then that interface can be used as a backup mechanism.

Used when primary route is Not available.

upvoted 19 times

iGlitch Highly Voted 1 year, 4 months ago

A and C are the same thing with different wording. :)

upvoted 5 times

country_rooted Most Recent 5 months, 2 weeks ago

The answer is literally the same. Just said 2 different ways

upvoted 3 times

DoBronx 10 months, 3 weeks ago

Selected Answer: AC

A and C are literally the same

upvoted 4 times

ZUMY 1 year, 2 months ago

A & C are correct

upvoted 3 times

jackcs 1 year, 4 months ago

Selected Answer: AC

YES A and C

upvoted 3 times

Question #349 *Topic 1*

```
R1# show ip route

D       192.168.10.0/24     [90/2679326] via 192.168.1.1
R       192.168.10.0/27     [120/3] via 192.168.1.2
O       192.168.10.0/23     [110/2] via 192.168.1.3
i L1    192.168.10.0/13     [115/30] via 192.168.1.4
```

Refer to the exhibit. How does router R1 handle traffic to 192.168.10.16?

A. It selects the IS-IS route because it has the shortest prefix inclusive of the destination address

B. It selects the RIP route because it has the longest prefix inclusive of the destination address

C. It selects the OSPF route because it has the lowest cost

D. It selects the EIGRP route because it has the lowest administrative distance

Correct Answer: *B*

Stonetales987 Highly Voted 1 year, 10 months ago

B is correct.
1. Longest Prefix
2. Administrative distance
3. Metric
https://packetlife.net/blog/2010/aug/16/route-preference/

upvoted 9 times

ananinamia 3 weeks, 6 days ago

YES:
1-Longest prefix
2-Adm distance
3-Metric

upvoted 1 times

ZUMY Most Recent 1 year, 2 months ago

B is correct
Routing prefrence
Longest prefix
AD
Metric

upvoted 1 times

shaz938 2 years ago

Answer B is correct. Uses RIP route since its the longest prefix match

upvoted 1 times

Adekoya_Oluwatobi 2 years ago

The answer is D

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/15986-admin-distance.html

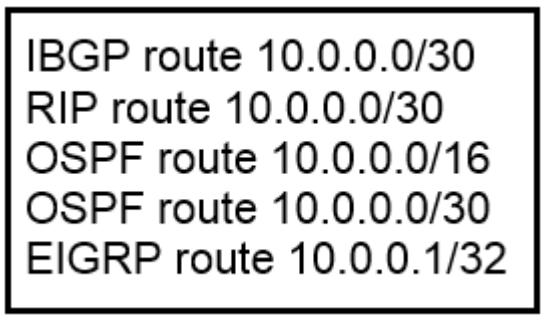
upvoted 1 times

Malojizter 2 years ago

This would be true, except the routes don't point to the same subnet, so prefix length would be used instead

upvoted 2 times

Question #350 *Topic 1*



Refer to the exhibit. A router received these five routes from different routing information sources. Which two routes does the router install in its routing table?
(Choose two.)

A. OSPF route 10.0.0.0/30

B. IBGP route 10.0.0.0/30

C. OSPF route 10.0.0.0/16

D. EIGRP route 10.0.0.1/32

E. RIP route 10.0.0.0/30

Correct Answer: *AD*

ismatdmour Highly Voted 1 year, 6 months ago

We have 3 correct answers not 2 !
One route to 10.0.0.0/30 selected from the 3 routes IBGP/OSPF and RIP (OSPF is correct option A)
One route to a host 10.0.0.1/32 (D) EIGRP
One route to 10.0.0.0/16 OSPF (C)
A D and C are correct ?

upvoted 18 times

g_mindset 1 year ago

totally agree! 3 correct answer here: A, C, & D.

upvoted 2 times

GreatDane Highly Voted 1 year, 2 months ago

Ref: Route Selection in Cisco Routers - Cisco

"...
Summary

The LONGEST PREFIX MATCH always wins among the routes actually installed in the routing table, while the routing protocol with the LOWEST ADMINISTRATIVE DISTANCE always wins when installing routes into the routing table.
..."

You have 5 routes from 4 different routing protocols. Two of these routes are from OSPF: the router must choose (between them) which one to install in the routing table, and here the longest prefix match criteria wins (router chooses OSPF route 10.0.0.0/30).
Now, you have 4 routes. 3 routes are all /30 routes (same prefix length): the router chooses on the basis of lowest administrative distance, and OSPF wins (administrative distance for these protocols is OSPF 110, which is lower than RIP 120, which is lower than BGP 200).

The last route is an EIGRP one, and this is also a host route (look at the /32 prefix). There can't be a longest prefix than a host route. Also, this route doesn't have to compete with any other route to be installed in the routing table. So, this route is the router's second choice.

Answers A and D are correct.

upvoted 14 times

DixieNormus 1 year ago

Googling your reference found me this link:
https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html

From your reference:

Let's look at another scenario to see how the router handles another common situation: varying prefix lengths. Assume, again, that a router has four routing processes running on it, and each process has received these routes:

EIGRP (internal): 192.168.32.0/26

RIP: 192.168.32.0/24

OSPF: 192.168.32.0/19

Which of these routes will be installed in the routing table? Since EIGRP internal routes have the best administrative distance, it's tempting to assume the first one will be installed. However, since each of these routes has a different prefix length (subnet mask), they're considered different destinations, and they will all be installed in the routing table.

upvoted 4 times

dropspablo Most Recent 1 month, 2 weeks ago

Answer correct:
A. Rota OSPF 10.0.0.0/30
C. Rota OSPF 10.0.0.0/16
D. Rota EIGRP 10.0.0.1/32
Next ask

upvoted 1 times

daddydagoth 6 months, 3 weeks ago

Selected Answer: AD

ADC are the correct answers. This is a missleading question that wouldn't come up like this in the actual exam.

upvoted 2 times

[Removed] 3 months ago

Hopefully because you're right, this is a misleading question.

upvoted 1 times

dick3311 10 months, 3 weeks ago

Selected Answer: CD

I think is CD cause they have different subnet mask

upvoted 2 times

DoBronx 10 months, 3 weeks ago

Selected Answer: AD

I chose ADC

upvoted 1 times

splashy 12 months ago

This question is BAF and should have three correct answers A C D
riddle me this riddle me that:
If every host route would "win" from a non host (subnet) route in the routing table, how do you think you will be able to ping other hosts in the subnets those host routes are in?

upvoted 3 times

dipanjana1990 1 year, 1 month ago

there will be three correct answers. One will be selected among the three /30 mask, other one will be /16 mask and last one will be /32 mask. among the three /30 mask routes, Ospf will be selected since Ospf has lowest AD which is 110 whereas RIP has AD value of 120 and iBGP has AD value of 200.

upvoted 5 times

nander 1 year, 1 month ago

Agree. /16 network should be added to the routing table too.

upvoted 1 times

ZUMY 1 year, 2 months ago

A & D are correct

upvoted 1 times

AWSEMA 1 year, 2 months ago

JUST ONE ROUTE IN THE ROUTING TABLE WILL APPEAR (EIGRP) !!! why they say 2 ???

upvoted 1 times

bitree 1 year, 5 months ago

source: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html

according to cisco, 3 routes will be installed, because different subnets mean different destinations. Moot question

upvoted 2 times

bitree 1 year, 5 months ago

actually 4 routes will get installed. all but the RIP route for 10.0.0.0/32 will get installed.

upvoted 1 times

i_am_confused 1 year, 3 months ago

No, the IBGP route will definitely not be installed either because IBGP has a higher AD than OSPF.

upvoted 2 times

gachocop3 1 year, 6 months ago

A&D

The longest-matching route is preferred first.

In the event, there are multiple routes to a destination with the same prefix length, the route learned by the protocol with the lowest administrative distance is preferred.

upvoted 2 times

DixieNormus 1 year ago

That is only for making forwarding decisions, not for determining what gets put on the routing table.

upvoted 1 times

dannysolisa 1 year, 7 months ago

Selected Answer: AD

A and D b/c IBGP has 200 of AD

upvoted 9 times

dannysolisa 1 year, 7 months ago

Route Source Default Distance Values
Connected interface 0
Static route 1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route 5
External Border Gateway Protocol (BGP) 20
Internal EIGRP 90
IGRP 100
OSPF 110
Intermediate System-to-Intermediate System (IS-IS) 115
Routing Information Protocol (RIP) 120
Exterior Gateway Protocol (EGP) 140
On Demand Routing (ODR) 160
External EIGRP 170
Internal BGP 200

upvoted 6 times

LilGhost_404 1 year, 7 months ago

Selected Answer: AD

First it win the longes prefix = EIGRP, after that the next longest prefix is a tie, then lowest administrative distance = OSPF

upvoted 1 times

Armoonbear 1 year, 7 months ago

Selected Answer: BD

Answer BD

Administrative distances are
IBGP - 20
EIGRP - 90
OSPF - 110
RIP - 120

IBGP and EIGRP has lowest AD (Administrative distance) leading the router to install it in it's routing table.

upvoted 1 times

Dante_Dan 1 year, 7 months ago

Actually no. The Administrative Distance of IBGP (Internal BGP) is 200.

DO NOT confuse with EBGP (External BGP) which it has and Administrative distance of 20.

upvoted 9 times

kijken 1 year, 7 months ago

Selected Answer: BD

IBGP has lower administrative distance. Should be

upvoted 2 times

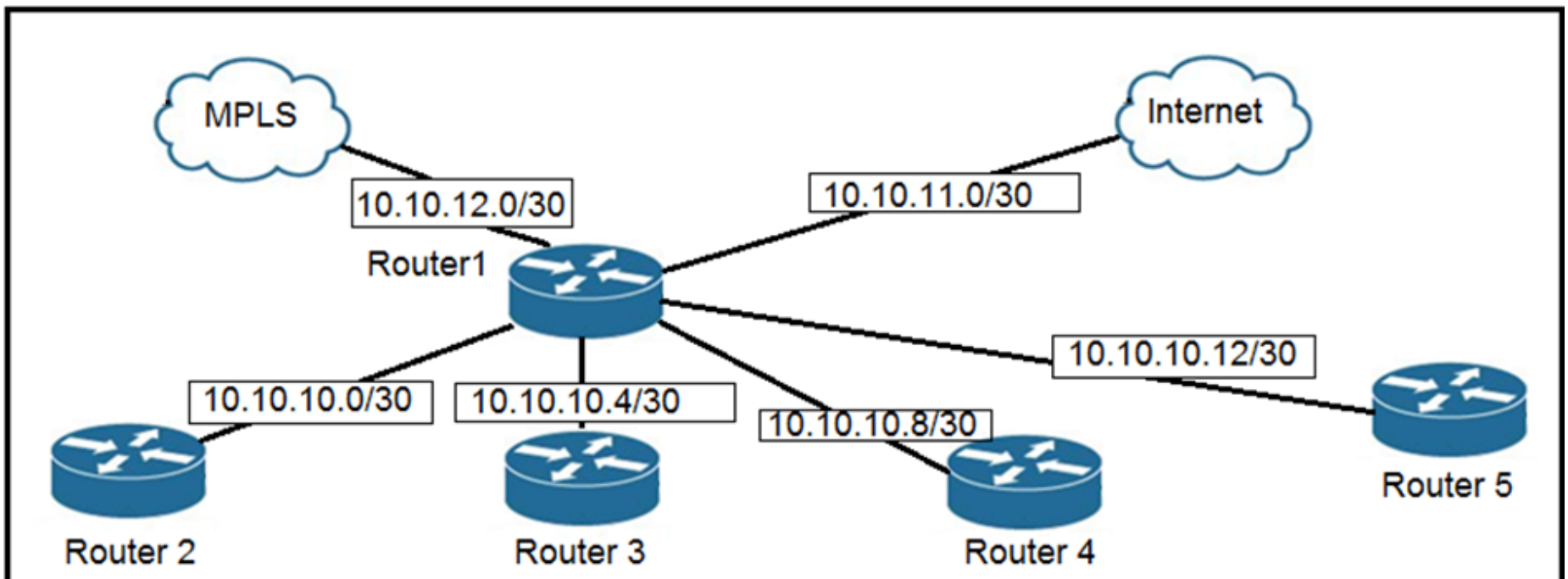
Dante_Dan 1 year, 7 months ago

Actually no. The Administrative Distance of IBGP (Internal BGP) is 200.

DO NOT confuse with EBGP (External BGP) which it has and Administrative distance of 20.

upvoted 8 times

Question #351 *Topic 1*




```
Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0
        209.165.200.0/27 is subnetted, 1 subnets
B          209.165.200.224 [20/0] via 10.10.12.2, 03:22:14
        209.165.201.0/27 is subnetted, 1 subnets
B          209.165.201.0 [20/0] via 10.10.12.2, 02:26:33
        209.165.202.0/27 is subnetted, 1 subnets
B          209.165.202.128 [20/0] via 10.10.12.2, 02:26:03
        10.0.0.0/8 is variably subnetted, 10 subnets, 4 masks
O          10.10.13.0/25 [110/2 ] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O          10.10.13.128/28 [110/2] via 10.10.10.5, 00:00:12, GigabitEthernet0/1
O          10.10.13.144/28 [110/2] via 10.10.10.9, 00:01:57, GigabitEthernet0/2
O          10.10.13.160/29 [110/2] via 10.10.10.5, 00:00:12, GigabitEthernet0/1
O          10.10.13.208/29 [110/2] via 10.10.10.13, 00:01:57, GigabitEthernet0/3
S*      0.0.0.0/0 [1/0] via 10.10.11.2
```

Refer to the exhibit. To which device does Router1 send packets that are destined to host 10.10.13.165?

A. Router2

B. Router3

C. Router4

D. Router5

Correct Answer: *B*

TheLorenz Highly Voted 1 year, 6 months ago

Here's a short subnet chart. You can write down a chart before the test starts
/32 - 1
/31 - 2
/30 - 4
/29 - 8
/28 - 16
/27 - 32
/26 - 64
/25 - 128
/24 - 256
/23 - 514

Check the routing table and look for a subnet that fits the 10.10.13.165 IP address. the only one that fits is 10.10.13.160/29. As you can see in this chart, /29 is equal to 8 total addresses and 6 total hosts (You have to subtract 2 from the total number of addresses to get the amount of hosts). 10.10.13.160 +6 = 166 which is the last usable address for 10.10.13.160/29. You pretty much do the same thing to find the router it'll send it out of.

upvoted 21 times

IFBBPROSALCEDO 1 month ago

Thank you! that helped me out so much

upvoted 2 times

BeautifulSmile 4 months ago

Perfectly explained.

upvoted 2 times

Liuka_92 1 year, 3 months ago

Great!

upvoted 2 times

Caoimhaoin 1 year, 3 months ago

/23 - 512

upvoted 6 times

DatBroNZ Highly Voted 1 year, 5 months ago

Selected Answer: B

Router 3 is the correct answer. Hard question. Need to be well versed on subnetting.

The subnet on the routing table that has 10.10.13.165 is the 10.10.13.160/29.

The 10.10.13.160/29 subnet is routed via 10.10.10.5 which is one of the usable hosts on the subnet between R1 and R3.

So the host 10.10.13.165 is reachable via R3.

upvoted 12 times

daddydagoth Most Recent 6 months, 3 weeks ago

Selected Answer: B

B is correct, refer to the explenations by TheLorenz and DatBroNZ

upvoted 1 times

HMaw 9 months, 4 weeks ago

Selected Answer: B

/28 = 248 and increment is 16
/29 = 240 and increment is 8

Destined host IP = 10.10.13.165

160 network host range for /28 is 160-175. Usable IP 161-174
160 network host range for /29 is 160-167. Usable IP 161-166

So we go with /29

O 10.10.13.160/29 [110/2] via 1010.10.5

Router 3 network is 10.10.10.4/30 increment is 4
Usable IP for 10.10.10.4/30 network is 5 and 6

Router 3 WAN IP are 10.10.10.5 and 10.10.10.6

upvoted 5 times

dosu01 11 months, 4 weeks ago

Selected Answer: B

I'ts B

upvoted 1 times

GreatDane 1 year, 2 months ago

1. Which route, inside the routing table, includes address 10.10.13.165? It's the route to subnet 10.10.13.160/29. This subnet has the following characteristics:

/29 means 3 bits in the host ID -> 2^3 – 2 = 6 IP addresses.

1st IP address = 10.10.13.161
Last IP address 10.10.13.166

2. Which is the exit interface for this route?

It's Ge0/1, which leads to IP 10.10.10.5 (the next-hop for this route).

3. Which subnet, among those shown in the exhibit, includes the next-hop's IP address? It's subnet 10.10.10.4/30. Again:

/30 means 2 bits in the host ID -> 2^2 – 2 = 2 IP addresses.

1st IP address = 10.10.10.5
Last IP address 10.10.10.6

The next-hop is inside this subnet and it's Router 3. The remaining IP address, 10.10.10.6, is Router 1's Ge0/1 IP address.

A. Router2

Wrong answer.

B. Router3

Correct answer.

C. Router4

Wrong answer.

D. Router5

Wrong answer.

upvoted 4 times

cheerios_aregreat 1 year, 6 months ago

I am trying to figure out why I cant access the Microsoft Azure 900 Fundamentals exam questions. I was on it a couple mins ago and I started getting an error and BOOM it just disappeared. Microsoft as an option has disappeared from the VIEW ALL EXAMS tab. There is no contact information for these people and when I click on CONTACT US it just sends me back to the bottom of the page? Help.

upvoted 2 times

LOST40 1 year, 6 months ago

maybe they want want you to be a contributor?

upvoted 1 times

bootloader_jack 1 year, 8 months ago

First we need to check routing table to find out which network 10.10.13.165 IP address belongs to.

If we check routing table, 10.10.13.160/29 IP address/Mask combination covers the following IP addresses: 10.10.13.160 (network address), 10.10.13.161, 10.10.13.162, 10.10.13.163, 10.10.13.164, 10.10.13.165, 10.10.13.166, 10.10.13.167 (Broadcast address). Since the address to go is 10.10.13.165, the network it is in is 10.10.13.160/29.

But, In order to go 10.10.13.160/29 network, we need to pass from 10.10.10.5 next hop address. The question asks us which router has that address. In order to find it, we need to look at question. We see many 10.10.10.X/30 networks. If we analyse 10.10.10.4/30, we see that it covers 10.10.10.4 (network address), 10.10.10.5, 10.10.10.6 and 10.10.10.7(broadcast address) addresses. So 10.10.10.5 address belongs to 10.10.10.4/30 network which is netween router1 and router3. So the answer is Router3.

upvoted 2 times

SparkySM 1 year, 8 months ago

idk why it says r3 , I think its r4

upvoted 1 times

andrewmutava 1 year, 8 months ago

can someone explain this to me please,i am lost

upvoted 2 times

Jdant 1 year, 8 months ago

The answer is B
The IP address 10.10.13.165 falls into the subnet of 10.10.13.160/29. Network address of the network is 10.10.13.160 with a broadcast address of 10.10.13.167. The route table says that anything that falls into that network is to be routed to 10.10.10.5 on interface Gei0/1. The IP address 10.10.10.5 belongs to the 10.10.10.4/30 network which connects to Router 3.

upvoted 6 times

gachocop3 1 year, 6 months ago

thank you!

upvoted 1 times

LOST40 1 year, 6 months ago

Yes, this is my understanding as well.

upvoted 1 times

hassanhhady 1 year, 8 months ago

can any one explain it tome please ?

upvoted 2 times

Question #352 *Topic 1*

R1 has learned route 10.10.10.0/24 via numerous routing protocols. Which route is installed?

A. route with the next hop that has the highest IP

B. route with the lowest cost

C. route with the lowest administrative distance

D. route with the shortest prefix length

Correct Answer: *C*

diamcle Highly Voted 2 years, 10 months ago

Route Preference:
1. Longest Prefix
2. Administrative Distance
3. Metric
In this specific question, the first option is: Administrative Distance.

upvoted 21 times

sinear 2 years, 8 months ago

Those rules u mention are for the route selection. Here the question is about route insertion. Longest Prefix does not play a role for inserting in the table, only for selecting a route.

upvoted 19 times

packitr3lgud 2 years, 6 months ago

Sinear is correct.

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html

"The longest prefix match always wins among the routes actually installed in the routing table, while the routing protocol with the lowest administrative distance always wins when installing routes into the routing table."

upvoted 16 times

oooMooo 2 years, 4 months ago

Nice quote!

upvoted 4 times

ZUMY Most Recent 1 year, 2 months ago

C is correct

upvoted 1 times

GreatDane 1 year, 2 months ago

Ref: Route Selection in Cisco Routers – Cisco

"...
Building the Routing Table
...
As each routing process receives updates and other information, it chooses the best path to any given destination and attempts to install this path into the routing table. For instance, if EIGRP learns of a path toward 10.1.1.0/24, and decides this particular path is the best EIGRP path to this destination, it tries to install the path it has learned into the routing table.

The router decides whether or not to install the routes presented by the routing processes based on the administrative distance of the route in question. If this path has the lowest administrative distance to this destination (when compared to the other routes in the table), it's installed in the routing table. If this route isn't the route with the best administrative distance, then the route is rejected.
..."

A. route with the next hop that has the highest IP

Wrong answer.

B. route with the lowest cost

Wrong answer.

C. route with the lowest administrative distance

Correct answer.

D. route with the shortest prefix length

Wrong answer.

upvoted 1 times

Anarckii 1 year, 9 months ago

Selected Answer: C

Installed and input are the same thing, don't overthink it. The reason the answer is C is because longest prefix isn't mentioned in one of the answers. So the next best thing to think of is the lowest admin distance

upvoted 1 times

Naj_Val 1 year, 8 months ago

The answer is indeed C, but I'd like to correct an inaccuracy in your reasoning. The length of the prefix is the same for all of the routes, as is stated in the question. "R1 has learned route 10.10.10.0/24 via numerous routing protocols", meaning the prefix length is the same. Therefore, the next most relevant parameter is AD.

upvoted 3 times

4guysgaming 2 years, 2 months ago

Why does the question say "lowest" admin distance instead of higher?

upvoted 1 times

Taku2023 5 months, 3 weeks ago

don't confuse longest prefix and high administrative distance

upvoted 1 times

yasyas 1 year, 10 months ago

lowest distance = higest priority

upvoted 1 times

Genshin 1 year, 11 months ago

because when the router is trying to determine which route it wants in its table, it will choose the "lowest" (the shortest path).

upvoted 2 times

Question #353 *Topic 1*

Which two minimum parameters must be configured on an active interface to enable OSPFV2 to operate? (Choose two.)

A. OSPF process ID

B. OSPF MD5 authentication key

C. OSPF stub flag

D. IPv6 address

E. OSPF area

Correct Answer: *AE*

M3rc3r08 Highly Voted 2 years, 1 month ago

Also, OSPFv2 does not advertise IPv6 addresses. That's OSPFv3.

upvoted 12 times

SScott Highly Voted 2 years ago

Answers are correct.
https://www.pearsonitcertification.com/articles/article.aspx?p=1868078#:~:text=2,area%20area-id

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3e/iro-xe-3e-book/iro-mode-ospfv2.pdf

https://www.ietf.org/rfc/rfc2328.txt#:~:text=Area%20ID%0A%20%20%20%20%20%20%20%20%20%20%20%20The%20OSPF%20area%20that%20the%20packet%20is%20being%20sent%20into

upvoted 5 times

raul_kapone Most Recent 3 weeks, 2 days ago

Selected Answer: AE

Two basics ways to enable OSPFv2 in an active interface are:

1) OSPFv2 Traditional configuration:
R1(config)# router ospf <process-id>
R1(config-router)# network <network-adddress> <wildcard-mask> area <area-number>

2) OSPv2 Interface configuration:
R1(config)# interface gigabitEthernet 0/0
R1(config-router)# ip ospf <process-if> area <area-number>

Where: R1 is the hostname of the router.

As you can see, the "process-id" and the "area-number" are necessary parameters in both configurations, including the quad-zero configuration that is similar to the "Traditional" way.

upvoted 1 times

kyleptt 2 months, 3 weeks ago

The trick is that you need the Process ID to configure OSPF but for routers to become neighbors it is not needed. IPV4 is OSPF V2

upvoted 2 times

dbcool22 1 year, 1 month ago

Selected Answer: AE

Key word is "enable", this is not pertaining to adjacency with neighbors.

upvoted 1 times

ZUMY 1 year, 2 months ago

A and E are correct

upvoted 1 times

GreatDane 1 year, 2 months ago

Ref: Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x

"...
Configuring Networks in OSPFv2
...
SUMMARY STEPS

1. configure terminal
2. interface interface-type slot/port
3. ip address ip-prefix/length
4. ip router ospf instance-tag area area-id [secondaries none]

..."

A. OSPF process ID

Correct answer.

B. OSPF MD5 authentication key

Wrong answer.

C. OSPF stub flag

Wrong answer.

D. IPv6 address

Wrong answer.

E. OSPF area

Correct answer.

upvoted 1 times

timskis2 1 year, 4 months ago

THAT IS IN CORRECT. they need an ip so they can be part of the DR/BDR process if they dont have a router id. (which is not one of the options) because "process id is only "locally" important.

upvoted 1 times

DixieNormus 1 year ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-xe-3s-book/iro-mode-ospfv2.html#GUID-C7538EF0-66B0-4F5A-896D-ED91EE5BC3CC

Enabling OSPFv2 on an Interface
SUMMARY STEPS
1. enable
2. configure terminal
3. interface type number
4. ip ospf process-id area area-id [secondaries none]
5. end
6. show ip ospf interface [type -number]

step 4 requires both a process ID and area ID

upvoted 2 times

zalogue98 1 year, 5 months ago

If there is only one area you do not have to specify there is an area 0

upvoted 1 times

Nicocisco 1 year, 6 months ago

Ip ospf <process_id> area <area_id>
A E

upvoted 1 times

NORLI 1 year, 5 months ago

The process don't need to match for ospf to come up

upvoted 3 times

Dking001 2 years, 2 months ago

No...
You don't need ipv6 address to setup ospfv2

upvoted 2 times

distortion 2 years, 2 months ago

Should'nt it also need to have an IPv6 Address before anything can happen?

upvoted 2 times

SScott 2 years ago

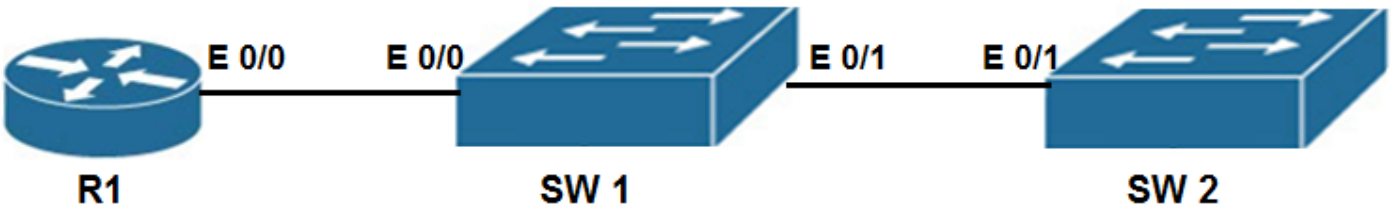
An IPv6 address will not work as OSPFv2 runs over IPv4 only.

https://www.networkworld.com/article/2298648/chapter-9--ospfv3.html#:~:text=Another%20similarity%20to%20the%20relationship%20of%20RIPng%20to%20RIPv2%20is%20that%20OSPFv3%20is%20not%20backward-compatible%20with%20OSPFv2.%20So%20if%20you%20want%20to%20use%20OSPF%20to%20route%20both%20IPv4%20and%20IPv6%2C%20you%20must%20run%20both%20OSPFv2%20and%20OSPFv3

upvoted 1 times

Question #354 *Topic 1*

Refer to the exhibit. What commands are needed to add a sub-interface to Ethernet0/0 on R1 to allow for VLAN 20, with IP address 10.20.20.1/24?



R1:

```
interface Ethernet0/0
  no ip address
!
```

SW1:

```
interface Ethernet0/0
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet0/1
  switchport trunk allowed vlan 10
  switchport trunk encapsulation dot1q
  switchport mode trunk
```

SW2:

```
interface Ethernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet0/2
  switchport access vlan 20
  switchport mode access
```

A. R1(config)#interface ethernet0/0 R1(config-if)#encapsulation dot1q 20 R1(config-if)#ip address 10.20.20.1 255.255.255.0

B. R1(config)#interface ethernet0/0.20 R1(config-if)#encapsulation dot1q 20 R1(config-if)#ip address 10.20.20.1 255.255.255.0

C. R1(config)#interface ethernet0/0.20 R1(config-if)#ip address 10.20.20.1 255.255.255.0

D. R1(config)#interface ethernet0/0 R1(config-if)#ip address 10.20.20.1 255.255.255.0

Correct Answer: *B*

ZayaB Highly Voted 2 years, 7 months ago

For a Router on a stick, you need to:
1. create a sub-interface
2. encapsulate dot1q with the VLAN ID
3. Assign an IP address

upvoted 34 times

[Removed] Most Recent 3 months ago

Selected Answer: B

B is correct :

```
R1(config)#interface ethernet0/0.20
R1(config-if)#encapsulation dot1q 20
R1(config-if)#ip address 10.20.20.1 255.255.255.0
```

upvoted 2 times

ZUMY 1 year, 2 months ago

B is correct

upvoted 1 times

MonaHamed 1 year, 7 months ago

isn't that topic cancelled in 200-301?

upvoted 4 times

Nickname53796 1 year, 3 months ago

No, Cisco wants to trick us.

upvoted 3 times

jerry19 2 years, 4 months ago

Answer B, sidenotes you must enter encap dot1q 20, in this case or you won't be able to enable 802.1q (and have vlan cross communications). The next step after you perform steps Zaya outlined would be to add your native subinterface. Which would entail "encap dot1q x native" with x being the native vlan. Native vlans are not assigned IP addresses. The physical interface is turned on and no ip is assigned to it.

upvoted 3 times

Retxed 2 years, 7 months ago

Why letter b?

upvoted 2 times

Media1993 2 years, 7 months ago

Read router ona stick and you will know why

upvoted 4 times

ScorpionNet 1 year, 4 months ago

Because the administrator is configuring Router on a Stick

upvoted 1 times

Question #355 *Topic 1*

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method  Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM   administratively down down
GigabitEthernet1/0         192.168.0.1     YES NVRAM   up                    up
GigabitEthernet2/0         10.10.1.10      YES manual  up                    up
GigabitEthernet3/0         10.10.10.20     YES manual  up                    up
GigabitEthernet4/0         unassigned      YES NVRAM   administratively down down
Loopback0                  172.16.15.10    YES manual
```

Refer to the exhibit. What does router R1 use as its OSPF router-ID?

A. 10.10.1.10

B. 10.10.10.20

C. 172.16.15.10

D. 192.168.0.1

Correct Answer: *C*

OSPF uses the following criteria to select the router ID:

1. Manual configuration of the router ID (via the ز€router-id x.x.x.xز€ command under OSPF router configuration mode).
2. Highest IP address on a loopback interface.
3. Highest IP address on a non-loopback and active (no shutdown) interface.

ZUMY 1 year, 2 months ago

C is correct

upvoted 3 times

GreatDane 1 year, 2 months ago

Ref: What is OSPF Router ID, OSPF Router ID Selection Algorithm and How to Configure OSPF Router ID - OmniSecu.com

"...
OSPF Router ID selection algorithm works as below.

o Any manually configured OSPF Router ID in OSPF Process is selected as the OSPF Router ID.

o If there is no OSPF Router ID configured, the highest IP address on any of the Routers Loopback Interfaces is selected as the OSPF Router ID.

o If there is no Loopback Interfaces configured, the highest IP address on its active interfaces is selected as the OSPF Router ID.
..."

A. 10.10.1.10

Wrong answer.

B. 10.10.10.20

Wrong answer.

C. 172.16.15.10

Correct answer.

D. 192.168.0.1

Wrong answer.

upvoted 4 times

hojusigol 1 year, 6 months ago

the highest IP address on any of the Routers Loopback Interfaces is selected as the OSPF Router ID

upvoted 1 times

dave1992 1 year, 11 months ago

anyone want to explain how 172.16.15.10 is a higher ip address than 192.168.0.1??????????????????????????????????

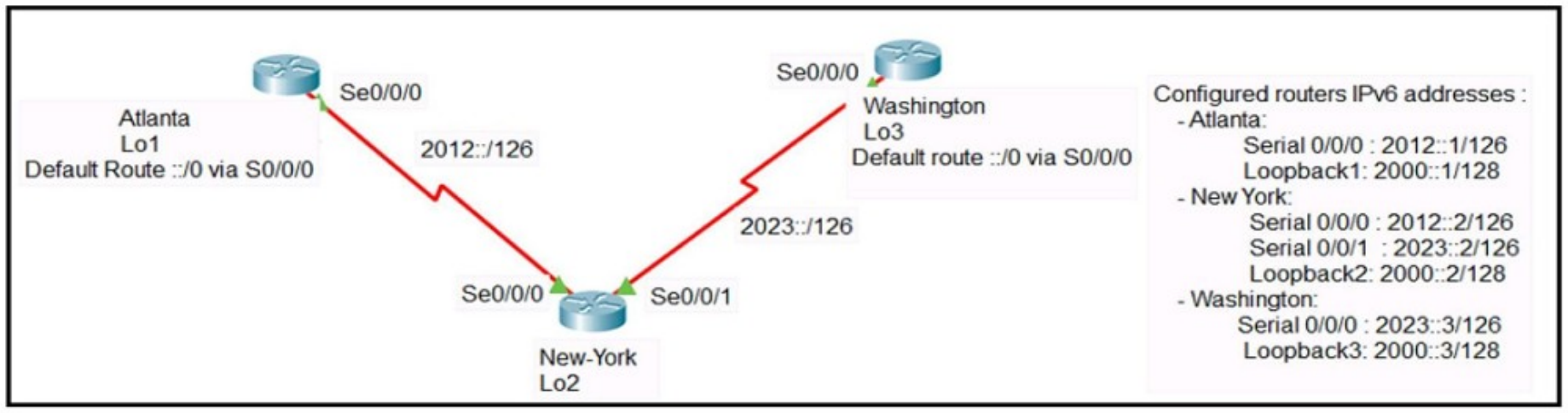
upvoted 1 times

WeaGLe 1 year, 11 months ago

Because that is the address of the loopback interface.

upvoted 11 times

Question #356 *Topic 1*



Refer to the exhibit. The loopback1 interface of the Atlanta router must reach the loopback3 interface of the Washington router. Which two static host routes must be configured on the New York router? (Choose two.)

A. ipv6 route 2000::3/128 s0/0/0

B. ipv6 route 2000::1/128 s0/0/1

C. ipv6 route 2000::1/128 2012::1

D. ipv6 route 2000::1/128 2012::2

E. ipv6 route 2000::3/128 2023::3

Correct Answer: *CE*

SOAPGUY Highly Voted 1 year, 4 months ago

Selected Answer: CE

ON NEWYORK ON NEWYORK ON NEWYORK~~~

upvoted 8 times

jerry19 Highly Voted 2 years, 4 months ago

Answer C and E, it would be much easier if the question said configure recursive route on New York router for each loopback network.

upvoted 6 times

cormorant Most Recent 9 months ago

THE NEXT HOPS ARE THE INTERFACES ON THE ATLANTA AND WASHINGTON ROUTERS.

ATLANTA: SERIAL 0/0/0 2012::1/126
WASHINGTON: SERIAL SE0/0/0 - 2023::3/126

upvoted 1 times

GreatDane 1 year, 2 months ago

To let the serial interfaces on the Atlanta and Washington routers reach other, you need to configure a static host route (on the New York router) which points to the destination IP (to the serial interface of the other router) and goes through the next-hop IP address.

For the Washington Lo3, you have to specify a static route to 2000::3/128 (destination IP) through Se0/0/0 on the Washington router (the next-hop):

ipv6 route 2000::3/128 2023::3

For the Atlanta Lo1, you have to specify a static route to 2000::1/128 (destination IP) through Se0/0/0 on the Atlanta router (the next-hop):

ipv6 route 2000::1/128 2012::1 command on the Washington router

A. ipv6 route 2000::3/128 s0/0/0

Wrong answer.

B. ipv6 route 2000::1/128 s0/0/1

Wrong answer.

C. ipv6 route 2000::1/128 2012::1

Correct answer.

D. ipv6 route 2000::1/128 2012::2

Wrong answer.

E. ipv6 route 2000::3/128 2023::3

Correct answer.
upvoted 5 times

JonasWolfxin 1 year, 2 months ago
Both static host routes must be configured on the New York router
upvoted 3 times

ludodelauz 1 year, 7 months ago
Why it's C and not D ?
upvoted 1 times

helmerpach 1 year, 8 months ago
is corresct because is static
upvoted 1 times

Anarckii 1 year, 9 months ago
the answers are correct but technically A and B are as well
upvoted 1 times

daddydagoth 6 months, 3 weeks ago
They aren't correct my friend. You might have misread the question like I did and are configuring routes on Atlanta and Washington to reach each other instead of New Yourk's router like the question asks you to!
upvoted 1 times

panagiss 1 year, 9 months ago
No, take a look at the interfaces on A & B
upvoted 2 times

Darrien1301 1 year, 5 months ago
can you explain that in more detail? Dont understand why this isnt possible
upvoted 1 times

Deeztroyer 1 year, 2 months ago
the serial interfaces are swapped around...
upvoted 1 times

Hodicek 1 year, 9 months ago
i would choose D - E
upvoted 3 times

oooMooo 2 years, 4 months ago
C and E are correct.

ipv6 [loopback network] [serial interface IP]
IPv6: /128 provides a single IPv6 address.
upvoted 3 times

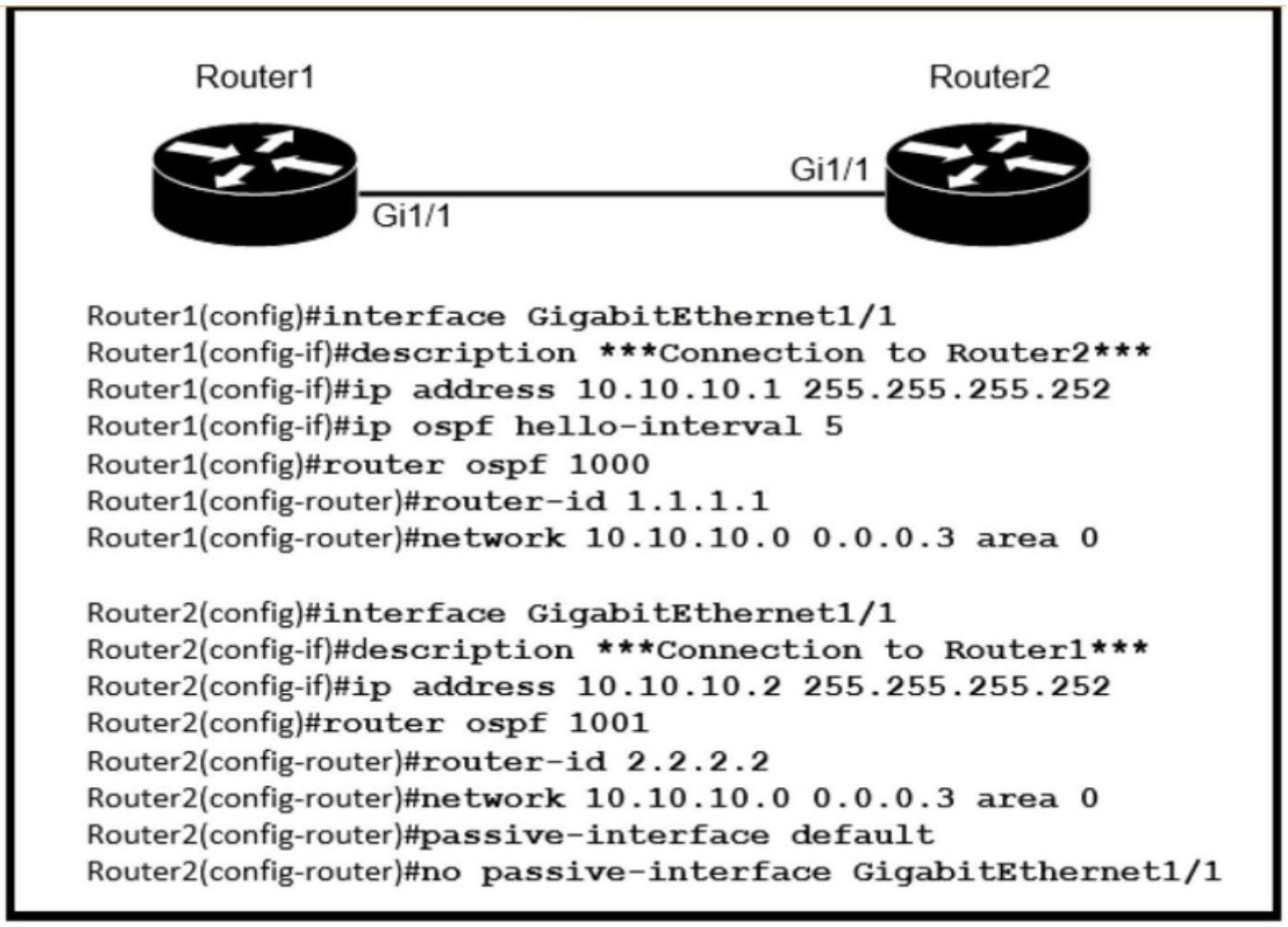
Robin999 2 years, 6 months ago
I need to correct my Statement. Given Answers are correct. They should not communicate to each other, just from one side to the other side.
upvoted 2 times

Robin999 2 years, 6 months ago
Correct answers are AB because the next Hop addresses are not matching in CD.
upvoted 4 times

ZayaB 2 years, 7 months ago
According to what I understand, you can use interface names such as s0/0/0 or g0/1 on a static route config instead of next hop IP addresses. It is not recommended but it is possible. Therefore, A and B is technically correct, isn't it?
upvoted 2 times

ZayaB 2 years, 7 months ago
Sorry, it is asking the config on NY router...C and E is correct. My bad.
upvoted 5 times

Question #357 *Topic 1*




```
Router1(config)#interface GigabitEthernet1/1
Router1(config-if)#description ***Connection to Router2***
Router1(config-if)#ip address 10.10.10.1 255.255.255.252
Router1(config-if)#ip ospf hello-interval 5
Router1(config)#router ospf 1000
Router1(config-router)#router-id 1.1.1.1
Router1(config-router)#network 10.10.10.0 0.0.0.3 area 0

Router2(config)#interface GigabitEthernet1/1
Router2(config-if)#description ***Connection to Router1***
Router2(config-if)#ip address 10.10.10.2 255.255.255.252
Router2(config)#router ospf 1001
Router2(config-router)#router-id 2.2.2.2
Router2(config-router)#network 10.10.10.0 0.0.0.3 area 0
Router2(config-router)#passive-interface default
Router2(config-router)#no passive-interface GigabitEthernet1/1
```

Refer to the exhibit. After the configuration is applied, the two routers fail to establish an OSPF neighbor relationship. What is the reason for the problem?

A. The OSPF process IDs are mismatched

B. The network statement on Router1 is misconfigured

C. Router2 is using the default hello timer

D. The OSPF router IDs are mismatched

Correct Answer: *C*

bmatthee01 Highly Voted 1 year, 6 months ago

Ospf processes can differ on each router and neighborship will form
Ospf area must be the same to form adjacency
Hello and dead timers must match to form adjacency

Ospf Default hello timer is 10 and dead timer is 40

In This case R1 hello timer was modified to 5 seconds

Timers was not changed on R2 hence using the default timers

So C is correct
upvoted 14 times

vadiminski Highly Voted 2 years, 4 months ago

The given answer is correct, the default hello time is 10 seconds which causes a mismatch
upvoted 8 times

Fuaad 2 years ago

what about the Router-ID since they are mismatching?
upvoted 2 times

kmb192006 2 years ago

router-id has to be unique on each router instead

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/23862-duplicate-router-id-ospf.html
upvoted 4 times

[Removed] Most Recent 4 months, 1 week ago

Selected Answer: C

Keith Barker's acronym for OSPF neighborship: TAN - MAT
These must match in OSPF.
Timers
Area number
Network address

MTU size
Authentication
Type (Network type: broadcast (with ethernet) or p2p)

upvoted 1 times

Etidic 10 months, 4 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

ZUMY 1 year, 2 months ago

C is correct
Hello and dead timer should much

upvoted 3 times

Mozah 1 year, 9 months ago

Router ID can not be an issue. At least if the Areas were different but are all using area "0". The given answer "C" is correct, default hello time is 10 seconds and died time its times four of hello timer. In this case, the routers are using differ hello timer which results in fail of OSPF relationship

upvoted 2 times

panagiss 1 year, 9 months ago

Process ID MUST BE Different. So the answer is correct

upvoted 1 times

ismatdmour 1 year, 6 months ago

It is not necessarily that Process IDs be Different. They can be the same or they can be different. but neither is a requirement

upvoted 2 times

dave1992 1 year, 11 months ago

process IDs are not matching. A is the correct answer.

upvoted 3 times

kokoyul 1 year, 11 months ago

Router-Id and process OSPF son de importancia local; el valor default de los hello es de 10, por lo cual la respuesta es correcta. C.

upvoted 2 times

Cisna 1 year, 12 months ago

Hey y`all how about the process ID? I think that should also be the answer

upvoted 1 times

Cisna 1 year, 12 months ago

Just confirmed, neighbors converges despite the process ID mismatch!

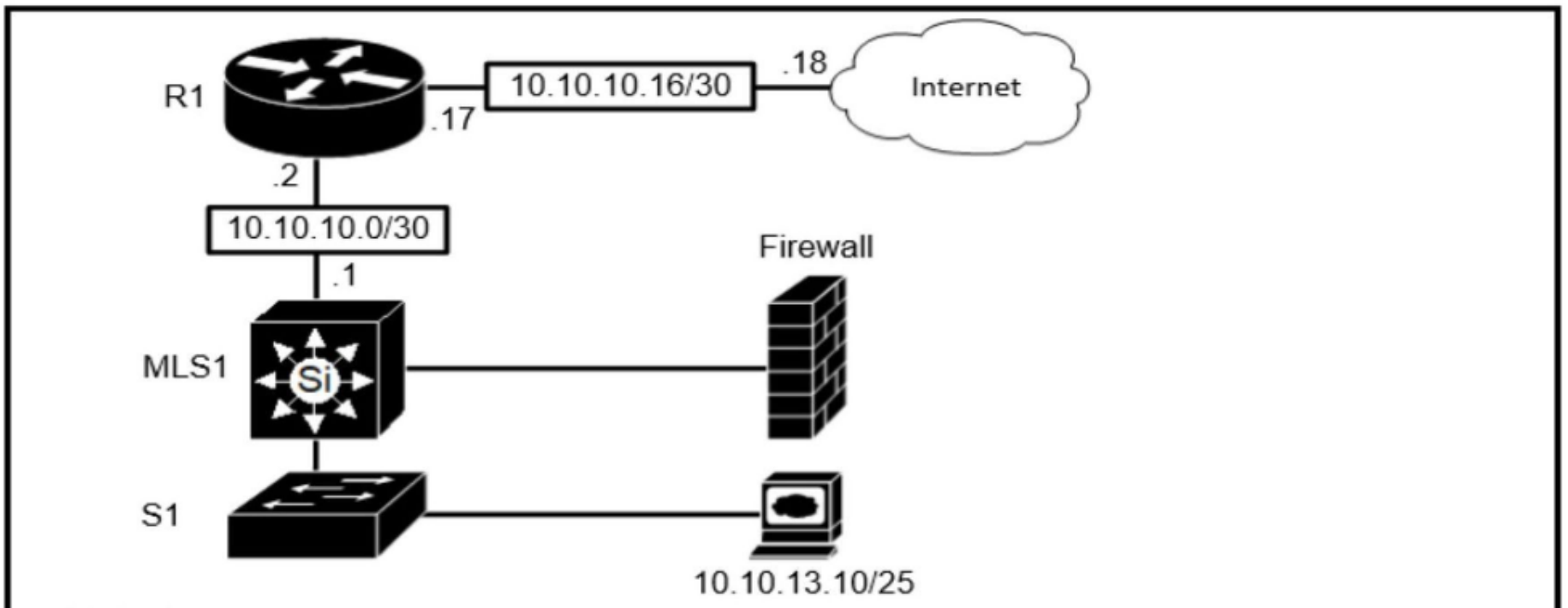
upvoted 4 times

laurvy36 1 year, 9 months ago

the process ID doesnt matter on ospf, only in eigrp has to be the same on all devices because is considered an AS

upvoted 2 times

Question #358 *Topic 1*




```
R1#sh ip ro
Gateway of last resort is 10.10.10.18 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.10.10.0/30 is directly connected, FastEthernet0/1
O       10.10.13.0/25 [110/6576] via 10.10.10.1, 06:58:21, FastEthernet0/1
C       10.10.10.16/30 is directly connected, FastEthernet0/24
O       10.10.13.144/28 [110/110] via 10.10.10.1, 06:58:21, FastEthernet0/1
B*   0.0.0.0/0 [20/0] via 10.10.10.18, 01:17:58
```

Refer to the exhibit. Which route type is configured to reach the Internet?

A. floating static route

B. host route

C. network route

D. default route

Correct Answer: *D*

TheLorenz Highly Voted 1 year, 6 months ago

D. It can reach the internet with the directly connected route but only if it's specified to go directly to 10.10.10.18. The internet itself is filled with unknown addresses, so any other unknown address will need to use the default route.

upvoted 5 times

moise_amo Most Recent 7 months, 2 weeks ago

Selected Answer: D

i hope B* is Just because the AD defined for the default route is for internal BGP

upvoted 1 times

DoBronx 10 months, 3 weeks ago

what does B* mean

upvoted 1 times

RougePotatoe 10 months, 3 weeks ago

Basically /32 address, route to a end point such as computer, phone, and what not.
https://learningnetwork.cisco.com/s/question/0D53i00000Kt1dkCAB/host-route

upvoted 2 times

ZUMY 1 year, 1 month ago

D is correct

upvoted 1 times

ScorpionNet 1 year, 4 months ago

D is right because it identifies the one network that is not in the routing table

upvoted 1 times

golddy 1 year, 6 months ago

IT S VAGUE QUESTION NO REALY CLEAR

upvoted 3 times

Mozah 1 year, 9 months ago

D. default route is correct. 0.0.0.0/0 means when there is no any match in the routing table eg for www.google.com, that traffic must use the specified next hope/path (10.10.10.18). That's the way since we don't know the destination so the next hop/router will search the destination from neighboring routers up to the tear 1 if its really available

upvoted 1 times

Networkingguy 2 years, 7 months ago

Such a vague question, the /30 which includes .17 and .18 via the connected route which is a 'network route' as they can reach the internet/next hop. As does the default route for all non specified routes that are not in the routing table.. Both are correct dumb question.

upvoted 4 times

yoyosannn 2 years, 7 months ago

Only if the PC will ask to go to 10.10.10.18 it will use the network route.
When asking to go to the internet the router will use the default gateway - the network route does not include 8.8.8.8 or any other public address
Yaki מלך Israel

upvoted 12 times

shakyak 1 year, 9 months ago

I guess we can safely say that, default route is default gateway.

upvoted 7 times

Networkingguy 2 years, 7 months ago

C The specified route, would be the route it takes out to the internet...

upvoted 4 times

sinear 2 years, 8 months ago

Why not C here ? The direct connected interface will be used to reach the internet as it matches the address .18 leading to the interface. It's not the default route that will be used here. Unless question refers to "what was configured" and not "what is used" ?

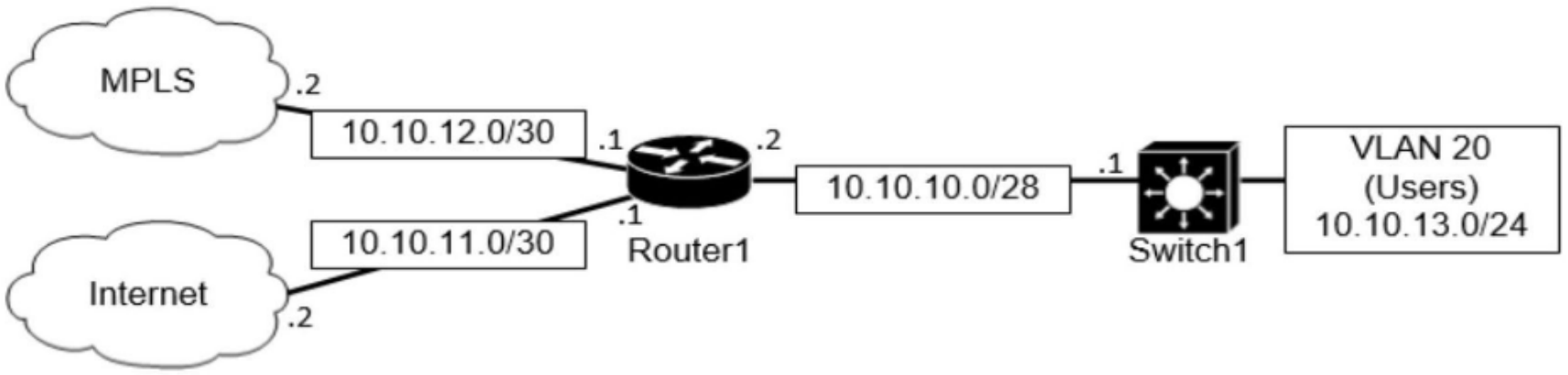
upvoted 3 times

Ongogablogian 2 years, 8 months ago

The only thing in the table that would match a packet with a public IP destination is the default route

upvoted 11 times

Question #359 *Topic 1*




```
Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0
     209.165.200.0/27 is subnetted, 1 subnets
B       209.165.200.224 [20/0] via 10.10.12.2, 00:09:57
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.10.10.0/28 is directly connected, GigabitEthernet0/0
C       10.10.11.0/30 is directly connected, FastEthernet2/0
O       10.10.13.0/24 [110/2] via 10.10.10.1, 00:08:34, GigabitEthernet0/0
C       10.10.12.0/30 is directly connected, GigabitEthernet0/1
S*   0.0.0.0/0 [1/0] via 10.10.11.2

Switch1#show ip route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.0/28 is directly connected, FastEthernet0/1
C       10.10.13.0/24 is directly connected, VLAN20
```

Refer to the exhibit. Which path is used by the router for Internet traffic?

A. 209.165.200.0/27

B. 0.0.0.0/0

C. 10.10.13.0/24

D. 10.10.10.0/28

Correct Answer: *B*

LTTAM Highly Voted 2 years, 8 months ago

For internet traffic... the destination IP's can vary. Hence in this topology, it is using the default gateway 0.0.0.0. Path selection does not meet any other criteria so it has to use gateway of last resort. Correct me if I'm wrong here folks.

upvoted 15 times

Zerotime0 2 years, 7 months ago

You right

upvoted 4 times

uevenasdf Highly Voted 2 years, 8 months ago

Why isn't 10.10.11.0/30 an option? Weird question obviously the others are wrong and the 0.0.0.0 is the only option

upvoted 7 times

sinear 2 years, 8 months ago

Indeed this is misleading... typical cisco.

upvoted 11 times

oooMooo 2 years, 4 months ago

It didn't ask which route. It asked which path. I too, was confused at first.

upvoted 3 times

ZUMY Most Recent 1 year, 1 month ago

B is correct

upvoted 1 times

promaster 2 years, 3 months ago

S* 0.0.0.0/0 is the candidate default route, and statically configured. So i am assuming that it will take presence as default route (gateway). I could be wrong, but this is my best guess.

upvoted 3 times

Nhan 2 years, 7 months ago

Default route

upvoted 4 times

Question #360 *Topic 1*

When OSPF learns multiple paths to a network, how does it select a route?

A. For each existing interface, it adds the metric from the source router to the destination to calculate the route with the lowest bandwidth.

B. It counts the number of hops between the source router and the destination to determine the route with the lowest metric.

C. It divides a reference bandwidth of 100 Mbps by the actual bandwidth of the exiting interface to calculate the route with the lowest cost.

D. It multiplies the active K values by 256 to calculate the route with the lowest metric.

Correct Answer: *C*

RebWat93 Highly Voted 2 years, 8 months ago
OSPF uses cost to make routing decisions
upvoted 8 times

suepanda Highly Voted 3 years, 2 months ago
C is correct. https://networktechstudy.com/home/learning-ospf-path-selection
upvoted 7 times

rick2461 Most Recent 1 month ago
Selected Answer: C
Isn't A specifically for the outdated IGRP? with keywords "metric from source router"?
upvoted 1 times

linuxlife 5 months, 3 weeks ago
OSPF-running routers use these criteria to select the best route to be installed in the routing table:

When there are multiple routes available to the same network with different route types, routers use this order of preference (from highest to lowest):
Intra-area routes
Inter-area routes
External Type-1 routes
External Type-2 routes
If there are multiple routes to a network with the same route type, the OSPF metric calculated as cost based on the bandwidth is used for selecting the best route. The route with the lowest value for cost is chosen as the best route.
If there are multiple routes to a network with the same route type and cost, it chooses all the routes to be installed in the routing table, and the router does equal cost load balancing across multiple paths.
upvoted 1 times

Ceruzka 6 months, 1 week ago
C says how to calculate ospf metric for a specific intf
A says how to choose the correct path to dest with the lowest cumulative metric.
A is correct answer.
upvoted 1 times

dropspablo 4 months ago
route with the lowest bandwidth???
upvoted 1 times

leooel 9 months ago
Selected Answer: C
c is correct
upvoted 3 times

dick3311 10 months, 3 weeks ago
Selected Answer: C
definitely is C
upvoted 4 times

DoBronx 10 months, 3 weeks ago
Selected Answer: C
It is C. Anyone disputing this needs to study
upvoted 7 times

hichccna 7 months, 2 weeks ago
You should rethink your answer, since the right answer is A
upvoted 2 times

Rether16 5 months, 2 weeks ago

Youre wrong. And you have made yourself looks silly by posting this.

upvoted 3 times

splashy 11 months, 3 weeks ago

Selected Answer: A

A takes every exiting interface from source to destination into account
C Only takes 1 exiting interface into account

Cumulative cost is the sum of the all costs of the outgoing OSPF interfaces in the path.
While calculating cumulative cost, OSPF consider only outgoing interfaces in path. It does not add the cost of incoming interfaces in cumulative cost.
If multiple routes exist, SPF compares the cumulative costs. Route which has the lowest cumulative cost will be chosen for routing table.

https://www.computernetworkingnotes.com/ccna-study-guide/ospf-metric-cost-calculation-formula-explained.html

upvoted 3 times

splashy 10 months, 1 week ago

metric should be cumulative cost and it should say lowest cost or highest bandwidth instead of lowest bandwidth (totally misread (past tense) it).
So C should be more correct... but it needs cumulative cost of every exiting/outgoing interface on the path from source to destination to actually be able to calculate which path is best=lowest cost. Trip up question.

upvoted 2 times

ShadyAbdekmalek 12 months ago

Selected Answer: A

I would go for A
The destination could be after several hops ,and each of those has a cost based on BW , they needed do be all added to calculate the cost to that destination

upvoted 2 times

ZUMY 1 year ago

C :
Cisco routers determine what to base the cost versus bandwidth on a 'reference bandwidth' which defaults to 100mbps. The reference bandwidth is then divided by the link bandwidth to generate the link cost

upvoted 2 times

ismatdmour 1 year, 6 months ago

In fact C is misleading. This is because cost compared is not the cost of one interface (obtained by division of ref BW/interface BW). It is rather the accumulation of all the divisions on all interfaces, e,g. if the first interface 100Mbps ==> cost=1 and the second interface is 10 Mbps==> Cost =10, the total cost is 10+1=11, which is the one compared with the total costs of other paths calculated similarly.
Hence, I would choose A as it is more descriptive of the process except for that last 2 words "lowest bandwidth" is incorrect and should be "lowest cost".

upvoted 5 times

bigbelly123 1 year, 8 months ago

to be specific, its not actual bandwidth, its the reference bandwidth :)

upvoted 1 times

Question #361 *Topic 1*

When a floating static route is configured, which action ensures that the backup route is used when the primary route fails?

A. The administrative distance must be higher on the primary route so that the backup route becomes secondary.

B. The default-information originate command must be configured for the route to be installed into the routing table.

C. The floating static route must have a lower administrative distance than the primary route so it is used as a backup.

D. The floating static route must have a higher administrative distance than the primary route so it is used as a backup

Correct Answer: *D*

alexiro Highly Voted 3 years, 1 month ago

By default, IOS considers static routes better than OSPF-learned routes. By default, IOS gives
static routes an administrative distance of 1 A floating static route floats or moves into and out of the IP routing table depending on whether the better (lower) administrative distance route learned by the routing protocol happens to exist currently.

upvoted 10 times

golddy Most Recent 2 years, 6 months ago

it could be A

upvoted 3 times

dave1992 1 year, 11 months ago

golddy, you read it wrong. the secondary route needs a higher AD, not a lower AD. Lower AD gets selected. you are mixed up.i almost agreed with you for a second.

upvoted 8 times

oooMooo 2 years, 4 months ago

It's D. A says AD should be higher on the primary route. Which is false.

upvoted 4 times

on2it 1 year, 2 months ago

that's not nice

upvoted 1 times

```
Designated Router (ID) 10.11.11.11, Interface address 10.10.10.1
Backup Designated router (ID) 10.3.3.3, Interface address 10.10.10.3
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:08
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 6
Last flood scan time is 0 msec, maximum is 1 msec
Neighbor Count is 3, Adjacent neighbor count is 3
Adjacent with neighbor 10.1.1.4
Adjacent with neighbor 10.2.2.2
Adjacent with neighbor 10.3.3.3 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

Refer to the exhibit. The show ip ospf interface command has been executed on R1. How is OSPF configured?

A. A point-to-point network type is configured.

B. The interface is not participating in OSPF.

C. The default Hello and Dead timers are in use.

D. There are six OSPF neighbors on this interface.

Correct Answer: *C*

From the output we can see there are Designated Router & Backup Designated Router for this OSPF domain so this is a broadcast network (point-to-point and point-to-multipoint networks do not elect DR & BDR).

By default, the timers on a broadcast network (Ethernet, point-to-point and point-to-multipoint) are 10 seconds hello and 40 seconds dead. The timers on a non- broadcast network are 30 seconds hello 120 seconds dead.

From the line ز€Neighbor Count is 3ز€, we learn there are four OSPF routers in this OSPF domain.

Reference:

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13689-17.html

vadiminski Highly Voted 2 years, 4 months ago

A is wrong because default and designated routers are in use
B is obviously wrong
D is wrong, the neighbour count is 3
C is correct, the default timers in broadcast networks (ethernet) are 10 seconds hello and 4*hello for the dead timer

upvoted 19 times

kunyo99 2 years, 4 months ago

Great Explanation

upvoted 6 times

freeknowledge123 Most Recent 8 months, 1 week ago

c by process of elimination

upvoted 1 times

Yunus_Empire 9 months, 2 weeks ago

Tricky Question

upvoted 1 times

ZUMY 1 year ago

C is correct

upvoted 1 times

Question #363 *Topic 1*

A user configured OSPF and advertised the Gigabit Ethernet interface in OSPF. By default, to which type of OSPF network does this interface belong?

A. point-to-multipoint

B. point-to-point

C. broadcast

D. nonbroadcast

Correct Answer: *C*
The Broadcast network type is the default for an OSPF enabled ethernet interface (while Point-to-Point is the default OSPF network type for Serial interface with
HDLC and PPP encapsulation).
Reference:
https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch08s15.html

Ahhmedd Highly Voted 3 years, 2 months ago
The Broadcast network type is the default for an OSPF enabled ethernet interface (while Point-to-Point is the default OSPF network type for Serial interface with HDLC and PPP encapsulation so the An is C
upvoted 56 times

CJ32 3 years, 2 months ago
Well worded. This is 100% correct
upvoted 4 times

Yunus_Empire Highly Voted 9 months, 2 weeks ago
Selected Answer: C
You Got This... Only 437 Questions Left.....zrezos@gmail.com
upvoted 7 times

ZUMY Most Recent 1 year ago
C is correct
upvoted 2 times

mustafa007 3 years ago
right.OSPF behaves differently on some types of interfaces based on a per-interface setting called the OSPF network type. On Ethernet links, OSPF defaults to use a network type of broadcast, which causes OSPF to elect one of the routers on the same subnet to act as the designated router (DR). The DR plays a key role in how the database exchange process works, with different rules than with point-to-point links. official Cert guide volume 2, page 456
upvoted 5 times

Jackie_Manuas12 1 year, 5 months ago
OCG Vol1 p456, not Vol2
upvoted 1 times

Abuelyoser 3 years, 2 months ago
it should be B Point to Point
upvoted 2 times

Dataset 2 years, 2 months ago
no, in serial link applies the B answer
Regards
upvoted 2 times

Alibaba 1 year, 10 months ago
c TRUE OPTION
upvoted 1 times

Question #364 *Topic 1*

Which attribute does a router use to select the best path when two or more different routes to the same destination exist from two different routing protocols?

A. dual algorithm

B. metric

C. administrative distance

D. hop count

Correct Answer: *C*
Administrative distance is the feature used by routers to select the best path when there are two or more different routes to the same destination from different routing protocols. Administrative distance defines the reliability of a routing protocol.

alexiro Highly Voted 3 years, 1 month ago
When IOS must choose between routes learned using different routing protocols, IOS uses a concept called administrative distance. Administrative distance is a number that denotes how believable an entire routing protocol is on a single router. The lower the number, the better The AD is a rating of trust when multiple routes exist to the same destination.
upvoted 11 times

SVN05 Most Recent 7 months, 1 week ago
To my understanding

If installing into routing table is AD or Metric ONLY!
If choosing a route from routing table is Longest Prefix, AD & Metric. Basically all are taken into account.

AD - When 2 or more routes to the same destination from different routing protocols
Metric - When 2 or more routes to the same destination and using the SAME ROUTING PROTOCOL
Longest Prefix(in the case when choosing a route from route table)- This will take precedence over AD and Metric

Hope everyone gets the idea on how routing questions work. Also take into account that you should also know if the subnet prefix can be used for the host that the route we are choosing.
upvoted 3 times

ZUMY 1 year ago
C is correct
-AD
upvoted 2 times

mimo1000 1 year, 9 months ago
Administrative distance is the correct answer
upvoted 2 times

lucky1559 2 years ago
When it comes to chose one route from many that ALREADY EXISTS in RIB to same destination, router uses longest prefix match rule. AD (Administrative Distance) is used when it comes to installing different paths learned through different protocols.

Hence, in my opinion the "Longest Prefix Match" answer is missing.
upvoted 4 times

Question #365 *Topic 1*

Router A learns the same route from two different neighbors; one of the neighbor routers is an OSPF neighbor, and the other is an EIGRP neighbor. What is the administrative distance of the route that will be installed in the routing table?

A. 20

B. 90

C. 110

D. 115

Correct Answer: *B*
The Administrative distance (AD) of EIGRP is 90 while the AD of OSPF is 110 so EIGRP route will be chosen to install into the routing table.

alexiro Highly Voted 3 years, 1 month ago
Admin Distance:

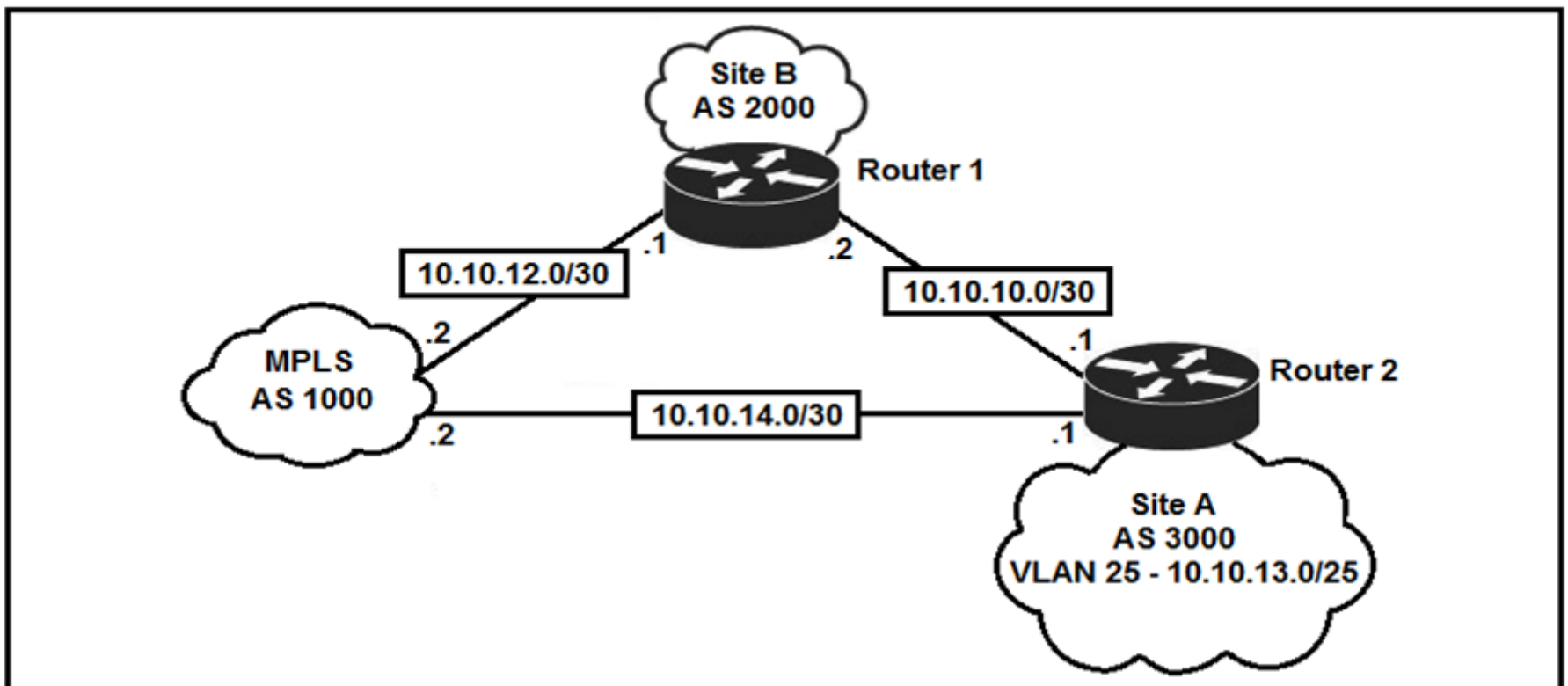
Connected.....0
Static.....1
EIGRP Summary.....5 (This occurs only on the router where the summary was generated)
eBGP.....20
Internal EIGRP.....90
OSPF.....110
IS-IS.....115
RIP.....120
External EIGRP.....170
iBGP.....200
NHRP.....250 (You'll typically only when using phase 3 DMVPN)
https://networktechstudy.com/home/learning-ospf-path-selection
upvoted 24 times

Gelo29 Highly Voted 3 years ago
Lowest AD win
upvoted 5 times

Alibaba 1 year, 9 months ago
A and B
upvoted 1 times

Customexit 10 months, 3 weeks ago
"one of the neighbor routers is an OSPF neighbor, and the other is an EIGRP neighbor."
upvoted 1 times

Question #366 *Topic 1*




```
Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0
     10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C       10.10.10.0/28 is directly connected, GigabitEthernet0/0
C       10.10.11.0/30 is directly connected, FastEthernet2/0
O       10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:17, GigabitEthernet0/0
O       10.10.13.128/28 [110/2] via 10.10.10.1, 00:33:38, GigabitEthernet0/0
O       10.10.13.144/28 [110/2] via 10.10.10.1, 00:33:38, GigabitEthernet0/0
O       10.10.13.160/29 [110/2] via 10.10.10.1, 00:33:38, GigabitEthernet0/0
O       10.10.13.208/29 [110/2] via 10.10.10.1, 00:33:39, GigabitEthernet0/0
O       10.10.13.252/30 [110/2] via 10.10.10.1, 00:33:39, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.10.11.2
```

Refer to the exhibit. An engineer is bringing up a new circuit to the MPLS provider on the Gi0/1 interface of Router 1. The new circuit uses eBGP and learns the route to VLAN25 from the BGP path.
What is the expected behavior for the traffic flow for route 10.10.13.0/25?

A. Traffic to 10.10.13.0/25 is load balanced out of multiple interfaces.

B. Traffic to 10.10.13.0/25 is asymmetrical.

C. Route 10.10.13.0/25 is updated in the routing table as being learned from interface Gi0/1.

D. Route 10.10.13.0/25 learned via the Gi0/0 interface remains in the routing table.

Correct Answer: *D*
The AD of eBGP (20) is smaller than that of OSPF (110) so the route to 10.10.13.0/25 will be updated as being learned from the new BGP path.

cybernett Highly Voted 2 years, 6 months ago
The correct answer is D
Because when new route is learned by R1 it will be added to it's routing table via Gi0/1 But the previous still stays in the routing table which is learned via Gi0/0 (ospf)
Hence we have two paths to reach 10.10.13.0/25
Cisco plays with words, read carefully.
C is wrong because they used the word updated and not added. Updated means previous route is removed
Which is not true , it stays in the table
Hence D is perfect answer
upvoted 61 times

Secsoft 3 weeks ago
The router will never allow multiple routing protocols to the same destination in its table. The correct answer is C.
upvoted 1 times

[Removed] 4 months, 1 week ago
The answer is C.
Routes That Must Win Twice | Cisco CCNA 200-301
https://www.youtube.com/watch?v=qU2qFU7NgNU
upvoted 1 times

DixieNormus 1 year ago

The correct answer is C
Because when new route is learned by R1 it will be added to it's routing table via Gi0/1 But the previous is removed from the routing table.
Hence we have one path to reach 10.10.13.0/25
Cisco plays with words, read carefully.
C is right because they used the word updated and not added. Updated means previous route is removed
Which is true , it is removed from the table
Hence C is perfect answer

upvoted 9 times

bootloader_jack 1 year, 8 months ago

I know that only the route with better administrative distance is installed in routing table. So, the ospf route will be replaced by ebgp route. Am I wrong?

upvoted 3 times

jahinchains 1 year, 4 months ago

10.10.13.0/25 is a different subnet ospf will stay on the routing table

upvoted 1 times

DixieNormus 1 year ago

How is 10.10.13.0/25 a different subnet from 10.10.13.0/25?

upvoted 7 times

cdp_neighbor Highly Voted 2 years, 8 months ago

"The AD of eBGP (20) is smaller than that of OSPF (110) so the route to 10.10.13.0/25 will be updated as being learned from the new BGP path." - which means that C is the correct answer?

upvoted 27 times

raul_kapone 3 weeks, 2 days ago

Yes man. When the router learn different routes from different sources (protocols), the Lowes Administrative Distance of each protocol says what route would be added to the routing table. Like you said:

AD of eBGP = 20 (Lowest)
AD of OSPF = 110

upvoted 2 times

sinear 2 years, 8 months ago

I think so too, though we find several answers to this in other sites.
The comment below the question seems to point to C rather than D.

upvoted 6 times

[Removed] Most Recent 3 months ago

One more question that is not CCNA 200-301 related.

upvoted 1 times

fmaquino 3 months ago

Selected Answer: C

C (AD is 20)

upvoted 1 times

gc999 6 months ago

I see the official answer here is "D", but it uses the explanation in "C". That is "so the route to 10.10.13.0/25 will be updated as being learned from the new BGP path".

upvoted 1 times

remoto 9 months ago

Selected Answer: D

The correct answer is "D"
The keys is "learned"

upvoted 2 times

arenjenkins 10 months, 3 weeks ago

beyond CCNA

upvoted 10 times

clivebarker86 11 months, 1 week ago

i just tried with PT, configured OSPF + RIP, only OSPF is added to the table, with #no router ospf command, RIP added to the table, correct answer C

upvoted 2 times

Murphy2022 11 months, 3 weeks ago

There is no Gi0/0 Interface so C must be correct.

upvoted 1 times

PiotrMar 1 year ago

Selected Answer: C

it is C
upvoted 1 times

ZUMY 1 year ago
Going with C:
upvoted 2 times

WOP_TO 1 year, 1 month ago
Selected Answer: C
C, no doubt; BGP AD 20, OSPF AD 110;

The router decides whether or not to install the routes presented by the routing processes based on the administrative distance of the route in question. If this path has the lowest administrative distance to this destination (when compared to the other routes in the table), it's installed in the routing table. If this route isn't the route with the best administrative distance, then the route is rejected.
upvoted 3 times

TA77 1 year, 2 months ago
The explaination doesn't match the selected answer. I guess the answer D was selected by mistake instead of C.
upvoted 2 times

DARKK 1 year, 3 months ago
Selected Answer: C
An OSPF(110 AD) path for VLAN 25 (10.10.13.0 /25) exits via Gi0/0, However an eBGP (20 AD) Path is being added via Gi0/1. Answer is C. Read the question carefully, and look at the image given. The eBGP path via Gi0/1 is chosen because it has a lower AD.
upvoted 3 times

ar2 1 year, 4 months ago
C.
I've just watched CBT Nuggets BGP overview, he does a demo almost identical. ie same network/mask with BGP and OSPF. The OSPF route is replaced.
upvoted 5 times

SOAPGUY 1 year, 4 months ago
Selected Answer: C
C;
https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/15986-admin-distance.html
upvoted 2 times

Nalle72 1 year, 5 months ago
D is correct. The routes OSPF learns are subnetted with longer prefixes (/28,/29, /30), but eBGP learns a route to 10.10.13.0/25. Thus, the OSPF routes need to remain. As the OSPF routes with longer prefixes do not cover the whole /25 subnet, BGP route would be added to the routing table as well.
upvoted 1 times

i_am_confused 1 year, 3 months ago
The question asks specifically about the 10.10.13.0/25 network. The more specific networks can be ignored since those are separate networks not relevant to the question. There will be two routes to 10.10.13.0/25, one through eBGP and one through OSPF. The eBGP route will be installed into the routing table and replace the OSPF route since eBGP has lower AD than OSPF. I believe the answer is C.
upvoted 4 times

Question #367 *Topic 1*

Which two actions influence the EIGRP route selection process? (Choose two.)

A. The advertised distance is calculated by a downstream neighbor to inform the local router of the bandwidth on the link.

B. The router calculates the feasible distance of all paths to the destination route.

C. The router must use the advertised distance as the metric for any given route.

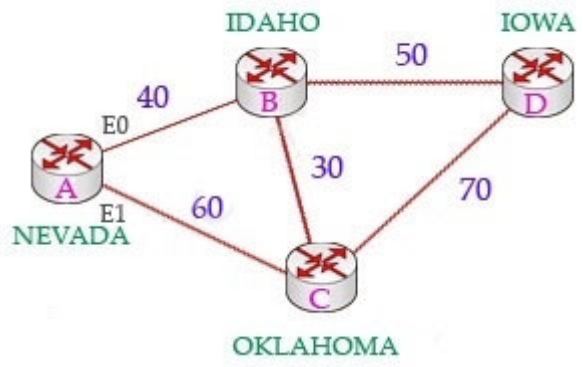
D. The router calculates the best backup path to the destination route and assigns it as the feasible successor.

E. The router calculates the reported distance by multiplying the delay on the exiting interface by 256.

Correct Answer: *BD*

The reported distance (or advertised distance) is the cost from the neighbor to the destination. It is calculated from the router advertising the route to the network.

For example in the topology below, suppose router A & B are exchanging their routing tables for the first time. Router B says ג€Hey, the best metric (cost) from me to IOWA is 50 and the metric from you to IOWA is 90ג€ and advertises it to router A. Router A considers the first metric (50) as the Advertised distance. The second metric (90), which is from NEVADA to IOWA (through IDAHO), is called the Feasible distance.



The reported distance is calculated in the same way of calculating the metric. By default (K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0), the metric is calculated as follows:

$$metric = \left[\frac{10{,}000{,}000}{\text{slowest bandwidth[in kbps]}} + \frac{\text{sum of delay[in µsec]}}{10}\right] * 256$$

Feasible successor is the backup route. To be a feasible successor, the route must have an Advertised distance (AD) less than the Feasible distance (FD) of the current successor route.

Feasible distance (FD): The sum of the AD plus the cost between the local router and the next-hop router. The router must calculate the FD of all paths to choose the best path to put into the routing table.

Note: Although the new CCNA exam does not have EIGRP topic but you should learn the basic knowledge of this routing protocol.

Shamwedge Highly Voted 1 year, 6 months ago

The two answers with feasible in it, make them feasible answers.

upvoted 24 times

anonymous1966 Highly Voted 2 years, 6 months ago

EIGRP is NOT topic of 200-301.

upvoted 9 times

oooMooo 2 years, 4 months ago

Yes, it's on the exam. You must know how it calculates the best path and it's AD cost. That's about it.

upvoted 6 times

[Removed] 3 months ago

It's not part of CCNA 200-301 or it shouldn't be. Cisco CCNA courses on Netacad don't even talk about EIGRP and then they would ask you questions about it? If so, that's a total scam and they want you to fail just to make more money.

upvoted 1 times

ddban 2 years, 4 months ago

it's on there

upvoted 5 times

[Removed] 3 months ago

It shouldn't be on there since it's NOT part of CCNA 200-301.

upvoted 1 times

DoBronx Most Recent 10 months, 3 weeks ago

I thought it was bandwith and delay
upvoted 3 times

RougePotatoe 10 months, 3 weeks ago
Read more about the operation of EIGRP and how it selects routes. Yes it uses bandwidth and delay but that's only the default parameters that it uses for the calculation.
upvoted 2 times

timskis2 1 year, 4 months ago
WHY WOULD IT NOT BE "A" LEARNING FROM THE DOWN STREAM ?
upvoted 2 times

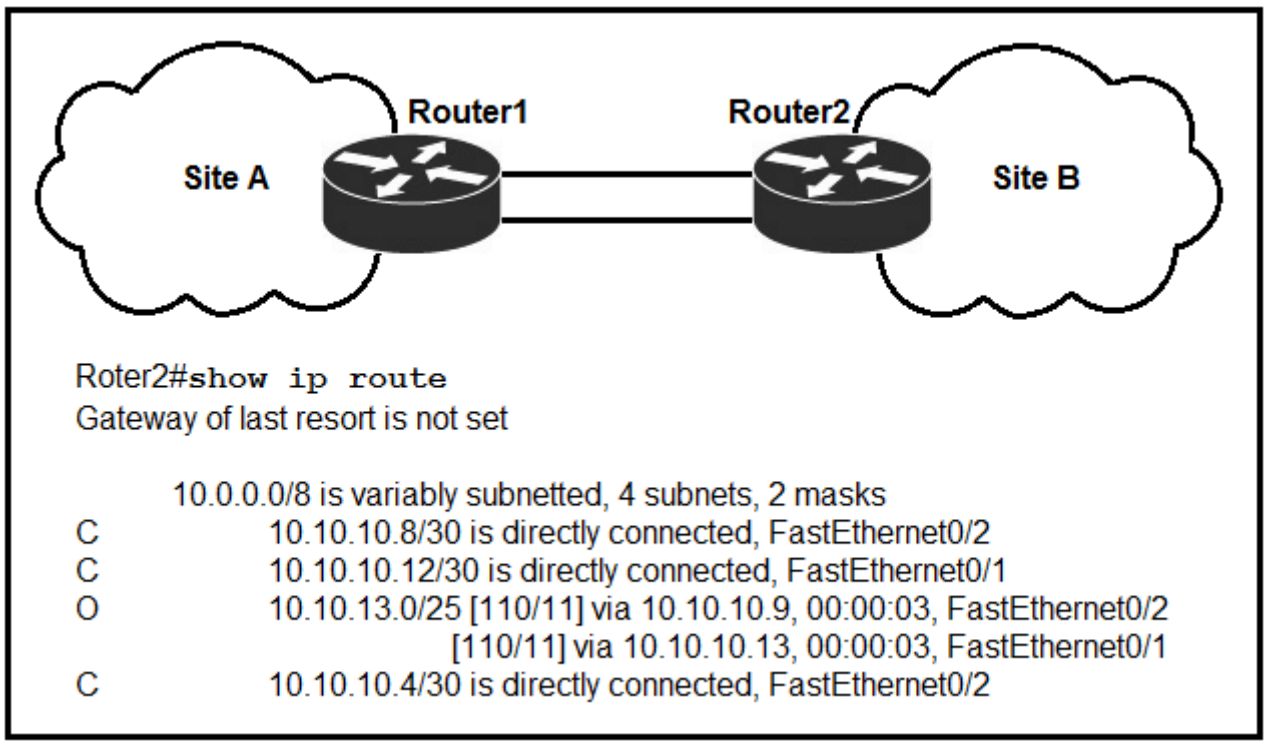
RougePotatoe 10 months, 3 weeks ago
Not A because advertised distance is not a report of the bandwidth on the link. Sure it uses bandwidth and delay to calculate a metric but don't confuse the metric with the bandwidth they are not interchangeable.
The Advertised Distance (AD) is the distance from a given neighbor to the destination router.
https://www.pluralsight.com/blog/it-ops/eigrp-overview
https://networklessons.com/eigrp/introduction-to-eigrp#:~:text=You%20have%20now%20learned%20two,to%20get%20to%20the%20destination.
upvoted 2 times

hassanhhady 1 year, 9 months ago
i didnt understand the answer yet or why
upvoted 6 times

promaster 2 years, 3 months ago
Network topology updates are sent using eigrp, therefore the answer is C, because there was a circuit update by the engineer that has lower AD than the previous route from int0/0.
upvoted 1 times

Acai 2 years, 4 months ago
Yeah you should definitely learn this as well as the AD of other routing protocols.
upvoted 2 times

Question #368 *Topic 1*



Refer to the exhibit. If OSPF is running on this network, how does Router2 handle traffic from Site B to 10.10.13.128/25 at Site A?

A. It sends packets out of interface Fa0/1 only.

B. It sends packets out of interface Fa0/2 only.

C. It load-balances traffic out of Fa0/1 and Fa0/2.

D. It cannot send packets to 10.10.13.128/25.

Correct Answer: *D*

Router2 does not have an entry for the subnet 10.10.13.128/25. It only has an entry for 10.10.13.0/25, which ranges from 10.10.13.0 to 10.10.13.127.

admin1982 Highly Voted 2 years, 7 months ago

@ Texter: Router 2 does not have an entry for the subnet 10.10.13.128/25. It only has an entry for 10.10.13.0/25, which ranges from 10.10.13.0 to 10.10.13.127. You're welcome - Je vous en prie

upvoted 19 times

mrsiafu Highly Voted 2 years, 4 months ago

Usuable range 10.10.13.1 to 10.10.13.126 for this /25

upvoted 11 times

Msandie Most Recent 1 month, 3 weeks ago

I didnt think about subnetting at all

upvoted 1 times

ZUMY 1 year ago

D is okay

upvoted 1 times

WOP_TO 1 year, 1 month ago

What a ridiculus question;
Shame on cisco;

upvoted 7 times

DoBronx 10 months, 3 weeks ago

always subnet

upvoted 1 times

MK_Engr 1 year, 2 months ago

It was Subnet mask related question, NOT routing related, lol

upvoted 4 times

tweesgger 1 year, 10 months ago

10.10.13.0/25 subnet does not include 10.10.13.128 because it is the subnet network address of the next subnet block for the /25 prefix, since it is not even a usable address to begin with, such scenario can only be hypothetical and no such situation can be found in an up and working network.

upvoted 2 times

CISCO2022 2 years, 3 months ago

X.X.X.0 /25 = Bit 25 is 128 increment = first net ID .0 Broadcast 127 IPs 0-126
2nd Net ID 128 Broadcast 255 IPs 129-254
10.10.13.128 is a Network ID

upvoted 6 times

Texter 2 years, 7 months ago

Could someone help explain how the IP Address range(s) are generated.
Thank you - Merci beacoup.

upvoted 2 times

kyleptt 2 months, 3 weeks ago

essentially .128 is none useable IP address

upvoted 1 times

Question #369 *Topic 1*

Which two outcomes are predictable behaviors for HSRP? (Choose two.)

A. The two routers negotiate one router as the active router and the other as the standby router.

B. The two routers share the same interface IP address, and default gateway traffic is load-balanced between them.

C. The two routers synchronize configurations to provide consistent packet forwarding.

D. Each router has a different IP address, both routers act as the default gateway on the LAN, and traffic is load-balanced between them.

E. The two routers share a virtual IP address that is used as the default gateway for devices on the LAN.

Correct Answer: *AE*

alexiro Highly Voted 3 years, 1 month ago

Hot Standby Router Protocol (HSRP) A Cisco proprietary protocol that allows two (or more) routers to share the duties of being the default router on a subnet, with an active/standby model, with one router acting as the default router and the other sitting by waiting to take over that role if the first router fails
HSRP

Protocol Cisco proprietary

"Number of groups" 16 groups maximum

Active/Standby "1 active, 1 standby and multiple candidates."

"Virtual IPAddress" "Different from real IP addresses on interfaces"

Multicast address 224.0.0.2

Tracking Interfaces or Objects

HSRP virtual Mac address will start with 0000.0c07.acXX

07.ac is the hexadecimal conversion of the HSRP group Id.

XX is Group number

virtual Mac for hsrp group 2 = 0000.0c07.ac02

virtual Mac for hsrp group12 = 0000.0c07.ac0C
upvoted 43 times

Ali526 2 years, 8 months ago

You have written a very long story. How about answers?
BTW, AE is correct. HSRP does not do load-balancing, unless you have multiple network subnets; that's another long story.
upvoted 8 times

Taku2023 5 months, 3 weeks ago

Yeah true GLBP, gateway load balancing protocols does load balance between active virtual router gateway and active virtual forwarding.
upvoted 1 times

DoBronx 10 months, 3 weeks ago

You always tell people they write long stories
upvoted 1 times

sinear 2 years, 8 months ago

AE are correct indeed.
upvoted 3 times

Genshin 1 year, 11 months ago

some people just want things spoon fed to them.
this guy is giving incredible information on why the answer is correct. if people just took a little time to LEARN
upvoted 9 times

[Removed] Most Recent 3 months ago

Selected Answer: AE

A and E are correct. There's one active router and one standby router and the two routers share a virtual IP address that is used as the default gateway for devices on the LAN.
upvoted 1 times

ZUMY 1 year ago

A&E are correct

upvoted 2 times

admin1982 2 years, 7 months ago

@ alexiro: what's the point with this dumb long explanation and no answer? such idiotic behavior.

upvoted 2 times

hassanhhady 1 year, 9 months ago

i think Alexiro write the best answer and explaining for this qustion
and i think you comment is the dumbest words in all these comments

upvoted 7 times

DoBronx 10 months, 3 weeks ago

Ladies calm down.

upvoted 2 times

Nebulise 1 year, 7 months ago

stop fighting-errrrr

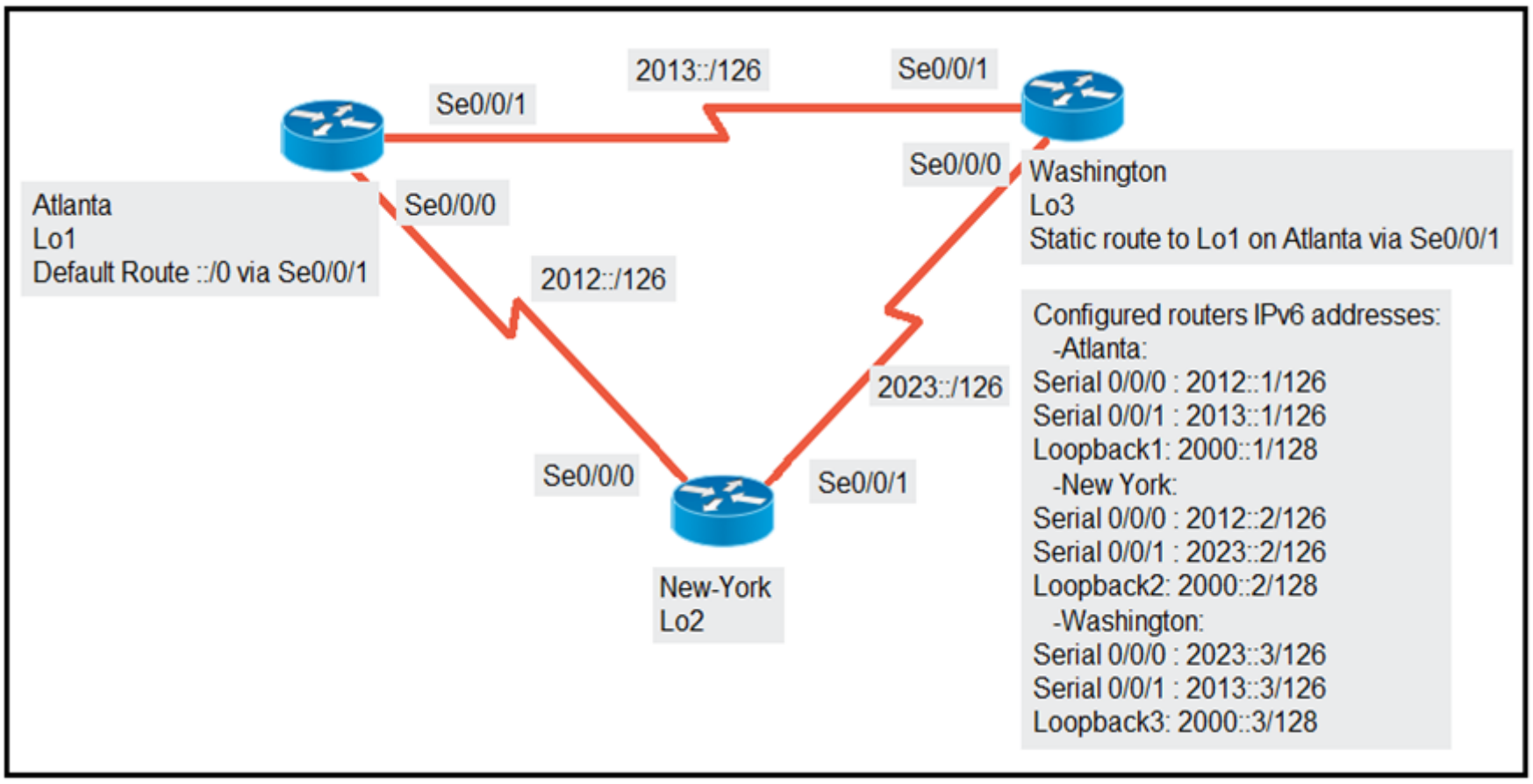
upvoted 2 times

LingLingW 1 year, 8 months ago

if you understand the long explanation you wouldn't came out with this idiotic statement

upvoted 6 times

Question #370 *Topic 1*



Refer to the exhibit. An engineer is configuring the New York router to reach the Lo1 interface of the Atlanta router using interface Se0/0/0 as the primary path.
Which two commands must be configured on the New York router so that it reaches the Lo1 interface of the Atlanta router via Washington when the link between
New York and Atlanta goes down? (Choose two.)

A. Ipv6 route 2000::1/128 2012::1

B. Ipv6 route 2000::1/128 2012::1 5

C. Ipv6 route 2000::1/128 2012::2

D. Ipv6 route 2000::1/128 2023::2 5

E. Ipv6 route 2000::1/128 2023::3 5

Correct Answer: *AE*
Floating static routes are static routes that have an administrative distance greater than the administrative distance (AD) of another static route or dynamic routes.
By default a static route has an AD of 1 then floating static route must have the AD greater than 1. Floating static route has a manually configured administrative distance greater than that of the primary route and therefore would not be in the routing table until the primary route fails.

ZayaB Highly Voted 2 years, 7 months ago
I agree with Jeff, the question is not correctly worded. I also assumed that primary path is already configured and we are just configuring the floating route. :(
upvoted 14 times

GA24 Highly Voted 2 years, 7 months ago
How come option A is also correct where in the question it clearly states that the link between New York and Atlanta is down, Which also means that network 2012::/128 is down?
upvoted 12 times

sdokmak 2 years, 3 months ago
A is correct because it's asking for WHEN the link goes down. So you still need to configure the primary link.
upvoted 19 times

perri88 Most Recent 3 months ago
I also assumed that primary path is already configured, not correctly worded. so it's asking to configure the network for when the link is up and when it's down
upvoted 1 times

DoBronx 10 months, 3 weeks ago
W Question

upvoted 2 times

ZUMY 1 year ago

A & E are correct

upvoted 2 times

aaronquiamco 1 year, 2 months ago

What does the 5 at the end mean?

upvoted 2 times

hp2wx 1 year, 1 month ago

The 5 is manually configuring the administrative distance for the static route. You should definitely review some routing concepts before you take your exam as this is a very important concept.

upvoted 2 times

JonCCNA12 1 year, 3 months ago

I hate how this is worded

upvoted 3 times

jahinchains 1 year, 4 months ago

Selected Answer: AE

the question is MUST CONFIGURE do you really configure two floating static route which is basically the same?

upvoted 1 times

ismatdmour 1 year, 6 months ago

(4)I may disappoint you more. It looks that they are the only routers in the city. The show command about each of them says that each of them are DRs and there exist no BDR (Backup designated router). Unfortunately, now, ficing the timers lead to they become 2-way at first, but they will proceed to negotiate DR/BDR roles, and finally they will agree on one of them as DR and the other as BDR. Sadly, this will bring A again (fixing timers) to false. But this leaves us with all incorrect answers. Ooops.
If you will ask me what to choose, I think A (fixing timers) is the one (correct in the examiner's mind, remeber no other action can bring relation whatsoever unless you act and fix timers first). Again, I hate it when the question is not well studied and expecting the examiners to make assumptions which might be not assumed by the one who made the question..... hmmmmmmmm

upvoted 3 times

Vinarino 1 year, 8 months ago

A) Ipv6 route 2000::1/128 2012::1 = washington to atlanta (always up hence, default AD)
Email, VoIP, etc., via an OC3 link is OK.

E) E. Ipv6 route 2000::1/128 2023::3 5 = NY to washington (backup route hence AD = 5)
Seems this BACKUP-route via NY to washington is the only link requireing setup in real life - to answer the Q.
A) is already up!

upvoted 3 times

gaber 1 year, 11 months ago

D&E. The question is pretty clear.

upvoted 1 times

AlvinNg 2 years ago

what is the 5 means ? on the answer E. Sorry I am still new in networking.. need some guide and explanation on this question..

upvoted 2 times

paulotiago 1 year, 12 months ago

AD - Administrative distance

upvoted 3 times

maximk33 2 years, 1 month ago

that it reaches the Lo1 interface of the Atlanta router** via Washington** when the link between.
how answer A correct?!
New York and Atlanta goes down?

upvoted 1 times

Coffeezw 1 year, 10 months ago

A is correct coz the question says WHEN, not IS down

upvoted 1 times

IxlJustinlxl 2 years, 4 months ago

should only be E since router should be smart enough to figure out the other part itself (which interface to exit from); however, I guess doing the config in D would be best practice so no assumptions are being made.
ANSWER = DE

upvoted 2 times

DixieNormus 1 year ago

A router can't the see loopback interfaces of its neighbors, only the IPs of the interfaces it is connected to.

upvoted 2 times

mrsiafu 2 years, 4 months ago

Only possible answers are D & E based on the question.
upvoted 3 times

jeff 2 years, 7 months ago
I believe A was an answer because the question stated the router is being configured to connect to Atlanta with a primary path "then" a back up route if the primary goes down
.....just badly/Cisco worded.
upvoted 9 times

FloridaMan88 2 years, 7 months ago
This shouldn't be a multiple choice question...there is only one real answer.

D as an answer doesn't work in reality - it is not a next hop....its the routers interface, it would need to be written as s0/0/1 5

E is the only possible answer as the question is written as GA24 states about A as an answer in their comment:
"GA24:
How come option A is also correct where in the question it clearly states that the link between New York and Atlanta is down, Which also means that network 2012::/128 is down?"
upvoted 1 times

Question #371 *Topic 1*

How does HSRP provide first hop redundancy?

A. It load-balances Layer 2 traffic along the path by flooding traffic out all interfaces configured with the same VLAN.

B. It uses a shared virtual MAC and a virtual IP address to a group of routers that serve as the default gateway for hosts on a LAN.

C. It forwards multiple packets to the same destination over different routed links in the data path.

D. It load-balances traffic by assigning the same metric value to more than one route to the same destination in the IP routing table.

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-16/fhp-xe-16-book/fhp-hsrp-mgo.html

alexiro Highly Voted 3 years, 1 month ago
This virtual IP address is in the same subnet as the interface IP address, but it is a different IP address. The router then automatically creates the virtual MAC address. All the cooperating HSRP routers know these virtual addresses, but only the HSRP active router uses these addresses at any one point in time.

The virtual router is responsible for host communications such as an ARP
request for the host's default gateway. Technically, this is served by the active router since it is hosting the virtual router. However, it is the virtual router's IP address and MAC address that are used for outgoing packets.
upvoted 12 times

[Removed] Most Recent 3 months ago
Selected Answer: B
Answer B is correct
upvoted 1 times

ZUMY 1 year ago
B is correct
upvoted 2 times

ismatdmour 1 year, 6 months ago
(2) The answer to this can be "Neighboring interfaces with MTU mismatch"; i.e to change MTU value of one router to be different that the one which belongs to the other router.
But as this option is not there, and I rejected D based on above (B and C, process ID and priority are irrelevant and are also rejected). This leaves for us A; i.e. to modify hello interval. However, before we discuss the impact of this, please read the question again to find that whatever we do, we need to act the status quo in which the two routers even have no intent to become neighbors, they send hello's but each one find a different hello timers in the hello messages and therefore refuse to proceed more. Hence, whatever other option we chose (e.g. D or if MTU is there), we have to first fix Timers (combined with the other option of your choice). Hence, I believe the answer given is the one that is on the mind of the examiner who designed this question.
upvoted 1 times

Question #372 *Topic 1*

Refer to the exhibit. Which action establishes the OSPF neighbor relationship without forming an adjacency?

```
R1# sh ip ospf int gig0/0
Gig0/0 is up, line protocol is up
        Internet Address 10.201.24.8/28, Area 1, Attached via Network Statement
        Process ID 100, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
        Topology-MTID        Cost            Disabled        Shutdown      Topology Name
                0                1               no              no              Base
        Transmit Delay is 1 sec, State DR, Priority 1
        Designated Router (ID) 192.168.1.1, Interface address 10.201.24.8
        No backup designated router on this network
        Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
                oob-resync timeout 40
                Hello due in 00:00:07

R2#sh ip ospf int gig0/0
gig0/0 is up, line protocol is up
        Internet Address 10.201.24.1/28, Area 1
        Process ID 100, Router ID 172.16.1.1, Network Type BROADCAST, Cost: 1
        Transmit Delay is 1 sec, State DR, Priority 1
        Designated Router (ID) 172.16.1.1, Interface address 10.201.24.1
        No backup designated router on this network
        Timer intervals configured, Hello 20, Dead 80, Wait 80, Retransmit 5
```

A. modify hello interval

B. modify process ID

C. modify priority

D. modify network type

Correct Answer: *A*

nebolala1 Highly Voted 1 year, 9 months ago

I hate this

upvoted 34 times

ismatdmour 1 year, 6 months ago

Agree. Missing information and improper wording. See my other comment

upvoted 6 times

anonymous1966 Highly Voted 2 years, 6 months ago

Correct is D
Pay attention to the statement: "establishes the OSPF neighbor relationship without forming an adjacency"
This two conditions (1) NO Neighbor Missing AND (2) no adjacency occurs only in two situations:
1) Neighboring interfaces with MTU mismatch.
2) Neighboring interfaces with OSPF network type mismatch
https://learning.oreilly.com/library/view/ccna-200-301-official/9780136755562/vol1_ch21.xhtml

upvoted 13 times

iGlitch 1 year, 4 months ago

According to OCG Volume 1 Chapter 21 page 515 :
"Interestingly, if you
misconfigure network type settings such that one router uses broadcast, and the other uses point-to-point, the following occurs:
■ The two routers become fully adjacent neighbors (that is, they reach a full state).
■ They exchange their LSDBs.
■ They do not add IP routes to the IP routing table.
The reason for not adding the routes has to do with the details of LSAs and how the use of a DR (or not) changes those LSAs. Basically, the two routers expect different details in the LSAs, and the SPF algorithm notices those differences and cannot trust the LSAs because of those differences."

So D cannot be the correct answer.

upvoted 11 times

[Removed] Most Recent 4 months, 1 week ago

Selected Answer: A

Question's Answer: Choosing answer A (modify hello interval) will cause R1 and R2 to successfully get to the 2-WAY OSPF neighbor relationship state but R1 and R2 will not become adjacent neighbors. Because R4 and R3 have the highest and second highest OSPF Router-IDs (192.168.1.4 and 192.168.1.3), they will become the DR and BDR. R1 will form full adjacencies with both the DR and BDR.

https://learningnetwork.cisco.com/s/question/0D56e0000CfMTBnCQO/which-action-establishes-the-ospf-neighbor-relationship-without-forming-an-adjacency?t=1683708512442

upvoted 2 times

liviuml 5 months ago

NOT possible - NO right answered if we get all request conditions.

First of all, "B. modify process ID" has nothing to do with relationship between devices, is internal.
To establishes the OSPF neighbor relationship we need to change timers to be the same. No matter if routers are in Broadcast or P2P, they cannot become neighbors if timers are not the same (even the Hello packets are transmitted, they will be ignored).

With presented settings if we adjust timers the routers will form ADJACENCY (again no matter if network types are Broadcast or P2P).

The only way to force routers to not form adjacency is to change PRIORITY to 0. In this way the routers will not become DR/BDR and will remain both DROTHERs (Neighbor Count is 1, Adjacent neighbor count is 0).
They will continue to send Hello messages, will be neighbors, but never achieve adjacency.

So, regarding the question there are 2 necessary actions to take to fulfill the request: changing timers to be the same & priority 0.
With only one action is impossible.

Tested all variants in PT.

Regards to the person who invented this impossible question/situation,

upvoted 3 times

oatmealturkey 6 months, 2 weeks ago

Selected Answer: A

I've gone back and forth on this question, but I have to finally go with A. If you change the network type, the Hello and Dead Interval timers still will not match, so a neighbor relationship still will not form. So A is the only possible answer (assuming that if you change the Hello timer, IOS automatically makes the Dead Interval timer 4 times that of the Hello timer, can anyone confirm that?).

I don't really know WHY it's A, because why then would they not reach full adjacency? I wonder if it has something to do with the fact that one router interface does not display any "attached" statement ("Attached via network statement", "Attached via interface enable")? I have no idea....

upvoted 1 times

networkin 9 months, 1 week ago

Ok. I'll take a swing at this. The question should have been "Which TWO actions establish..". Then it would have made perfect sense! A & D.

upvoted 1 times

Murphy2022 11 months, 2 weeks ago

Selected Answer: A

I have rebuild this on real switches and A is the correct answer.
When you modify the hello timer on R2 to 10 the output is:
Neighbour Count is 1, Adjacent neighbour count is 0

upvoted 4 times

RougePotatoe 10 months, 3 weeks ago

That's funny I did mismatched network types and one side is Neighbor 1 Adjacent 1 while the other is Neighbor 1 Adjacent 0. When I configured mis-matched timers it didn't event list any neighbors.

upvoted 1 times

Sal34 1 year, 3 months ago

Answer is D.

From the perspective of OSPF, there are a couple of things that must match for an OSPF neighborship to establish; these include:

1. The devices must be in the same area.
2. The devices must have the same authentication configuration.
3. The devices must be on the same subnet.
4. The devices hello and dead intervals must match.
5. The devices must have matching stub flags.

But the question is asking about OSPF neighborship without forming adjacencies. The OSPF point-to-point and point-to-multipoint nonbroadcast networks require statically defined neighbor statements without forming DR/BDR adjacencies.

upvoted 1 times

ar2 1 year, 4 months ago

A

https://community.cisco.com/t5/switching/ospf-neighbor-v-ospf-adjacency/td-p/1576785#:~:text=An%20OSPF%20adjacency%20is%20formed,routing%20updates%20from%20the%20DR.

upvoted 1 times

jahinchains 1 year, 4 months ago

https://www.ciscopress.com/articles/article.asp?p=2294214

spend time reading this one and you will know the best answer

upvoted 1 times

jahinchains 1 year, 4 months ago

Selected Answer: A

even you modify network type they will never become neighbor if it has hello interval mismatch

upvoted 9 times

Mark_j_k90 1 month, 2 weeks ago

Question is not "how do not become neighbor" but "how to not become adjacent". The answer is C modify the priority. If you change priority to 0 there will be no election for dr/bdr. So the router never send or receive bpdu eachother but just hello messages. In this case question dont'ask to choose 2 answer so we can assume that we cannot change the network type so the only possible answer is C!

upvoted 1 times

Mark_j_k90 1 month, 2 weeks ago

*so the router never send or receive LSA eachother...

upvoted 1 times

Ghost47 1 year, 6 months ago

Selected Answer: A

A is correct because the question ask "Which action establishes the OSPF neighbor relationship (without) forming an adjacency. This question is Cisco use their word games on the question to confuse people. The question is in plain terms ask what need to be change to make the router neighbors. Below is a section from the CCNA Offical Cert guide 200-301.
"Mismatched OSPF Network Types
Earlier in this chapter you read about the OSPF broadcast network type, which uses a DR/BDR, and the OSPF point-to-point network type, which does not. Interestingly, if you misconfigure network type settings such that one router uses broadcast, and the other uses point-to-point, the following occurs:
■ The two routers become fully adjacent neighbors (that is, they reach a full state).
■ They exchange their LSDBs.
■ They do not add IP routes to the IP routing table."

Have matching Hello timer is one of the requirements for OSPF to neighbors to become FULL.

upvoted 2 times

JonasWolfxin 1 year, 2 months ago

what about that both 2 routers use point-to-point type? The answer should be D

upvoted 2 times

ismatdmour 1 year, 6 months ago

(3) Let us next discuss whether this can be the correct answer or not. I say that this can be a correct. Remember that in a broadcast network where we have 4 routers or more, one of them will be Dr, another will be BDR, and all remaining routers will be DROTH (Not a DR nor a BDR). DR/BDR proceed to fully adjacent relation with all DROTHers while any 2 DROTH ers will form a 2 way (not adjacent) and each one of them will have the other as 2-way/DROTH. Wow... this our target, hence A, fixing timers can lead in such cases to neighbor relation (but not full). I believe this is what was on the examiner mind. However, the information about existence or no-existence of more than 4 routers are not there. Moreover,

upvoted 2 times

ismatdmour 1 year, 6 months ago

(1) I can say that this is a kind of question has some missing information and improper wording.
D cannot be fully correct because the question asks that no adjacency (the two routers become fully adjacent) be formed. Network mismatch will ensure that neighbor relation is formed, however, it will proceed to be fully adjacent and routers will exchange LSA and update LSDBs. The only impact on ospf process is that the SPF algorithm when digging in the LSDBs of both routers will find things which will prevent him from proceeding and it will not add routes (based on algorithm findings in ISDBs) to routing tables.

upvoted 2 times

rlelliott 1 year, 6 months ago

The easiest way to answer this question is to completely ignore the exhibit all together. Then the answer becomes quite obvious.

upvoted 1 times

rlelliott 1 year, 6 months ago

Oh by the way the answer is D

upvoted 1 times

ShaneFusco 1 year, 6 months ago

in hex?

upvoted 1 times

ksave 1 year, 7 months ago

Selected Answer: D

Answer is D.
Mismatched OSPF network types makes two routers neighbours but they do not add IP routes in the routing table.
Source: Wendell Odom, Volume 1, page 515.
whereas mismatched hello interval prevents the routers to become OSPF neighbours in the first place.

upvoted 2 times

reagan_donald 1 year, 7 months ago

Interestingly, if you misconfigure network type settings such that one router uses broadcast, and the other uses point-to-point, the following occurs:
■ The two routers become fully adjacent neighbors (that is, they reach a full state).

■ They exchange their LSDBs.
■ They do not add IP routes to the IP routing table.

Yes but it also says that it will become fully adjacent....

i think question is here interpreted wrongly
upvoted 1 times

JimmyX 1 year, 9 months ago

I believe the answer is A - modify hello interval
The default Network Type is Broadcast for Ethernet networks. Initially routers identify themselves with Hello protocol packet. Once acknowledged, this establishes the most basic relationship.

It's not until at least one of them become Designated Router or Backup Designated Router do they form the adjacency.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html
https://en.wikipedia.org/wiki/Open_Shortest_Path_First
upvoted 4 times

RSA001 1 year, 7 months ago

Among with other reasons why your point is wrong, changing ONLY hello timer will not change anything in this case
upvoted 1 times

Question #373 *Topic 1*

Which command must you enter to guarantee that an HSRP router with higher priority becomes the HSRP primary router after it is reloaded?

A. standby 10 preempt

B. standby 10 version 1

C. standby 10 priority 150

D. standby 10 version 2

Correct Answer: *A*

The ג€preemptג€ command enables the HSRP router with the highest priority to immediately become the active router.

kaus33k Highly Voted 1 year, 11 months ago

Preemption is the technology that ask a HSRP enabled router to be primary every time it comes up even though backup router is acting as Primary currently. if Preemption not enabled, when primary router reloads then backup router becomes primary and doesnot become backup even though primary router comes up.

upvoted 13 times

[Removed] Most Recent 3 months ago

Selected Answer: A

A is correct - standby 10 preempt

upvoted 1 times

ZUMY 1 year ago

A okay

upvoted 4 times

Belinda 1 year, 5 months ago

Hello! Pls this discussion part is not opening on my laptop but opens in my phone, on my laptop when u go via a question and want to check the discussion part of it, it says server error couldn't load discussion, pls what could be the issue?

upvoted 2 times

Belinda 1 year, 5 months ago

Hello! At first the discussion part was opening on my laptop out of a sudden it not , kept saying server error couldn't load discussion. But it opening on my phone that's how can even text here for help. Thanks . Waiting for anyone who can be of help.

upvoted 2 times

NICE_ANSWERS 3 months, 2 weeks ago

Check your internet connection

upvoted 1 times

Wilasky 1 year, 6 months ago

The stanby preempt command enable HSRP router with hughest priority to immediately become the active router.

upvoted 2 times

Question #374 *Topic 1*

Which command should you enter to verify the priority of a router in an HSRP group?

A. show hsrp

B. show sessions

C. show interfaces

D. show standby

Correct Answer: *D*

The following is sample output from the show standby command:

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
   2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
   Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
   Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
   Next hello sent in 1.412 secs
  Gratuitous ARP 14 sent, next in 7.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
   Tracking 2 objects, 0 up
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
Group name is "HSRP1" (cfgd)
Follow by groups:
    Et1/0.3 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs (nex
    Et1/0.4 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs (nex
  Group name is "HSRP1", advertisement interval is 34 sec
```

xsp Highly Voted 2 years, 7 months ago

on the contrary if the question is vrrp, command is:
show vrrp

upvoted 17 times

Acai 2 years, 4 months ago

and for GLBP, show glbp

upvoted 13 times

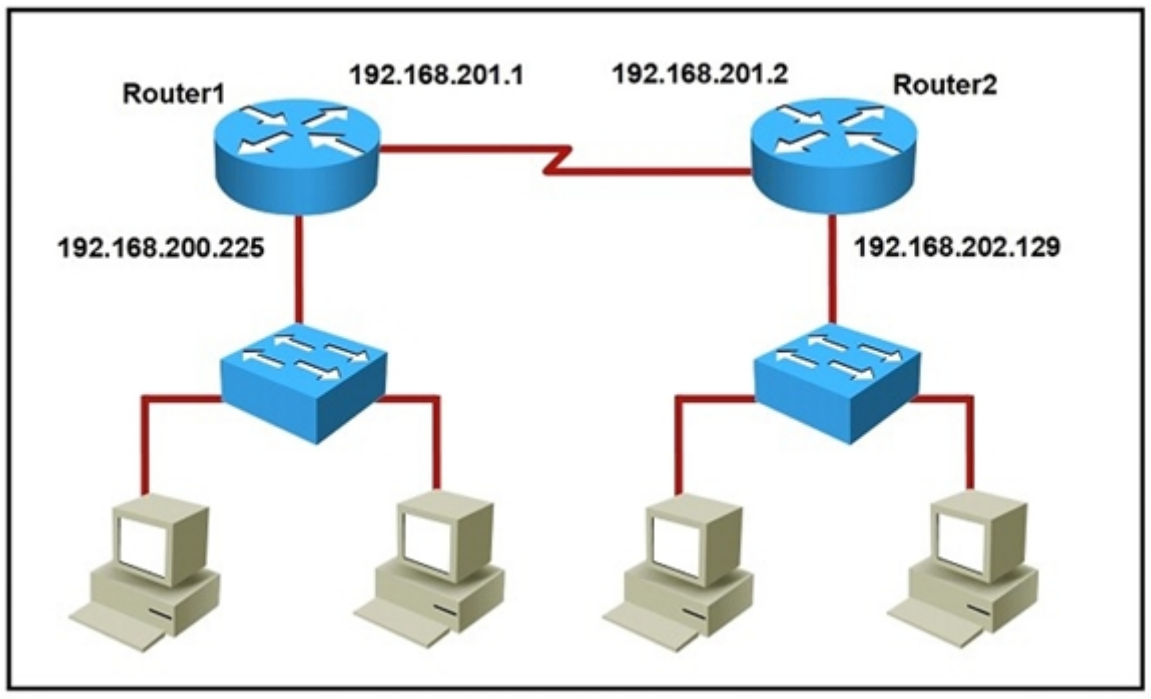
xbobdan 7 months ago

what's the point of asking these pure memorization question without any logical or sequential knowledge ground? i hate this

upvoted 6 times

Question #375 *Topic 1*

Refer to the exhibit. Which command would you use to configure a static route on Router1 to network 192.168.202.0/24 with a nondefault administrative distance?



A. router1(config)#ip route 192.168.202.0 255.255.255.0 192.168.201.2 1

B. router1(config)#ip route 192.168.202.0 255.255.255.0 192.168.201.2 5

C. router1(config)#ip route 1 192.168.201.1 255.255.255.0 192.168.201.2

D. router1(config)#ip route 5 192.168.202.0 255.255.255.0 192.168.201.2

Correct Answer: *B*

The default AD of static route is 1 so we need to configure another number for the static route.

cybernett Highly Voted 2 years, 6 months ago

Answer B is correct and not A because question asks for Non default AD therefore we use 5 as AD for static route and not 1 because Default AD for static route is 1

upvoted 13 times

Dataset Highly Voted 2 years, 3 months ago

B is correct

upvoted 5 times

checkoboy88 Most Recent 6 months, 2 weeks ago

sintax:
ip route command + subnet to be reached + submask of subnet to be reached + nexthop subnet + administrative distance (needs to be different than 1 because static route default is 1)

upvoted 3 times

msomali 1 year, 5 months ago

keyword is NON-DEFAULT AD which means FLOATING ROUTE. Static route have a default AD of 1. So looking for the static with AD higher than 1 will be correct according to the question.

upvoted 4 times

Jay1324 1 year, 8 months ago

this is a syntax question, learning the order in which the command goes and knowing the default admin distance of a static route

upvoted 4 times

Question #376 *Topic 1*

Which of the following dynamic routing protocols are Distance Vector routing protocols?

A. IS-IS

B. EIGRP

C. OSPF

D. BGP

E. RIP

Correct Answer: *BE*

Stonetales987 Highly Voted 1 year, 10 months ago

Distance Vector - RIP & EIGRP
OSPF - Link State & IS IS
BGP - Path State
https://packetlife.net/media/library/40/IOS_Interior_Routing_Protocols.pdf

upvoted 22 times

bigbux Highly Voted 2 years, 5 months ago

EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link-state protocols. For example, EIGRP doesn't send link-state packets as OSPF does; instead, it sends traditional distance-vector updates containing information about networks plus the cost of reaching them from the perspective of the advertising router. And EIGRP has link-state characteristics as well—it synchronizes routing tables between neighbors at startup and then sends specific updates only when topology changes occur. This makes EIGRP suitable for very large networks. EIGRP has a maximum hop count of 255 (the default is set to 100).

upvoted 12 times

LekkiDee Most Recent 3 months, 3 weeks ago

The keyword in the question is "are" this will indicate that they are looking for a minimum of two answers.

upvoted 2 times

SVN05 7 months, 1 week ago

Fun Tip. For Distance Vector protocols, the letters "R.I.P" are present in E"I"G"R""P" and RIP.

upvoted 9 times

Rether16 5 months, 1 week ago

I love you.

upvoted 4 times

HMaw 9 months, 4 weeks ago

Distance Vector Protocols (DVP)
Link State Protocols (LSP)

IS-IS = LSP
EIGRP = DVP+LSP
OSPF = LSP
BGP = Path-Vector Routing Protocol
RIP = DVP

upvoted 3 times

everchosen13 11 months, 2 weeks ago

I would say only E because technically is a EIGRP is not a true distance vector but a hybrid. If asked to select multiple I would have chose both EIGRP and RIP

upvoted 1 times

Murphy2022 11 months, 3 weeks ago

EIGRP is a enhanced distance vector protocol
RIP is a distance vector protocol
Question states to not choose more than 2 so I would say that only E is correct.

upvoted 2 times

bitree 1 year, 5 months ago

https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=9
cisco says RIP and EIGRP

upvoted 1 times

Nvoid 1 year, 8 months ago

Can you mark the question as taking two answers, really great person that created this site!? Thx in advance!!

upvoted 6 times

django1001 2 years ago
Should be B and D
upvoted 1 times

Alibaba 1 year, 9 months ago
are you sure about it
upvoted 1 times

Alibaba 1 year, 9 months ago
B and E dude
upvoted 1 times

paulotiago 1 year, 12 months ago
BGP is a path vector routing protocol.
upvoted 4 times

Question #377 *Topic 1*

You have configured a router with an OSPF router ID, but its IP address still reflects the physical interface.
Which action can you take to correct the problem in the least disruptive way?

A. Reload the OSPF process

B. Specify a loopback address

C. Reboot the router

D. Save the router configuration

Correct Answer: *A*
Once an OSPF Router ID selection is done, it remains there even if you remove it or configure another OSPF Router ID. So the least disruptive way is to correct it using the command ג€clear ip ospf processג€.

CISCO2022 Highly Voted 2 years, 3 months ago
Adding loopback ip still need to reload ospf process to take effect.
upvoted 15 times

Webfat 6 months, 3 weeks ago
It can be loopback because the rules to select the router ID
1. Manual configuration of the router ID (via the router-id x.x.x.x command under OSPF router configuration mode).
2. Highest IP address on a loopback interface.
3. Highest IP address on a non-loopback and active (no shutdown) interface.
In this question we already have a manual router ID, so even if you configure a loopback, manual router ID still will be the priority
upvoted 1 times

anonymous1966 Highly Voted 2 years, 6 months ago
Correct is B
in my opinion this is the "least disruptive way".
upvoted 13 times

Panda_man Most Recent 9 months, 3 weeks ago
Selected Answer: A
A is correct
upvoted 1 times

Nalle72 1 year, 5 months ago
Router id is not an IP address, the question confuses the two. (It can be the same as the IP address, for sure. But in the end, it is just an independent 32-bit id, and the only criteria, from OSPF point of view, is that it needs to be unique). Just nitpicking.
upvoted 1 times

jerry19 2 years, 4 months ago
I'm leaning towards the answer given A. If the explanation is accurate, it shouldn't be B (especially if you configured router-id x.x.x.x as indicated in problem statement). Clear ip ospf process temporarily restarts the neighbor relationships and there is disruption but my understanding it is only temporary. OSPF is self-healing with the hello packets so the OSPF routers should reconverge.
upvoted 9 times

Question #378 *Topic 1*

Which command should you enter to view the error log in an EIGRP for IPv6 environment?

A. show ipv6 eigrp neighbors

B. show ipv6 eigrp topology

C. show ipv6 eigrp traffic

D. show ipv6 eigrp events

Correct Answer: *D*

Rockrl Highly Voted 1 year, 9 months ago

A lot of EIGRP question when it is not listed in the topics to cover

upvoted 14 times

Jackie_Manuas12 1 year, 5 months ago

These must be questions from the previous CCNA exams before the update to 200-301. Rather than edit them out, admin here decided to just add to the question bank. I'm not sure if that's a good or bad decision...

upvoted 15 times

[Removed] 3 months ago

Yes they just added new questions from the old CCNA to the new one. In my opinion it's a bad decision because we need to focus on the CCNA 200-301 since it's the current one therefore the one people are preparing for and EIGRP isn't part of it.

upvoted 2 times

mrsiafu Highly Voted 2 years, 4 months ago

show ip eigrp events
To display the Enhanced Interior Gateway Routing Protocol (EIGRP) event log, use the show ip eigrp events command in user EXEC or privileged EXEC mode.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/command/ire-cr-book/ire-s1.html#wp3095206170

upvoted 8 times

Ciscoman021 Most Recent 5 months, 3 weeks ago

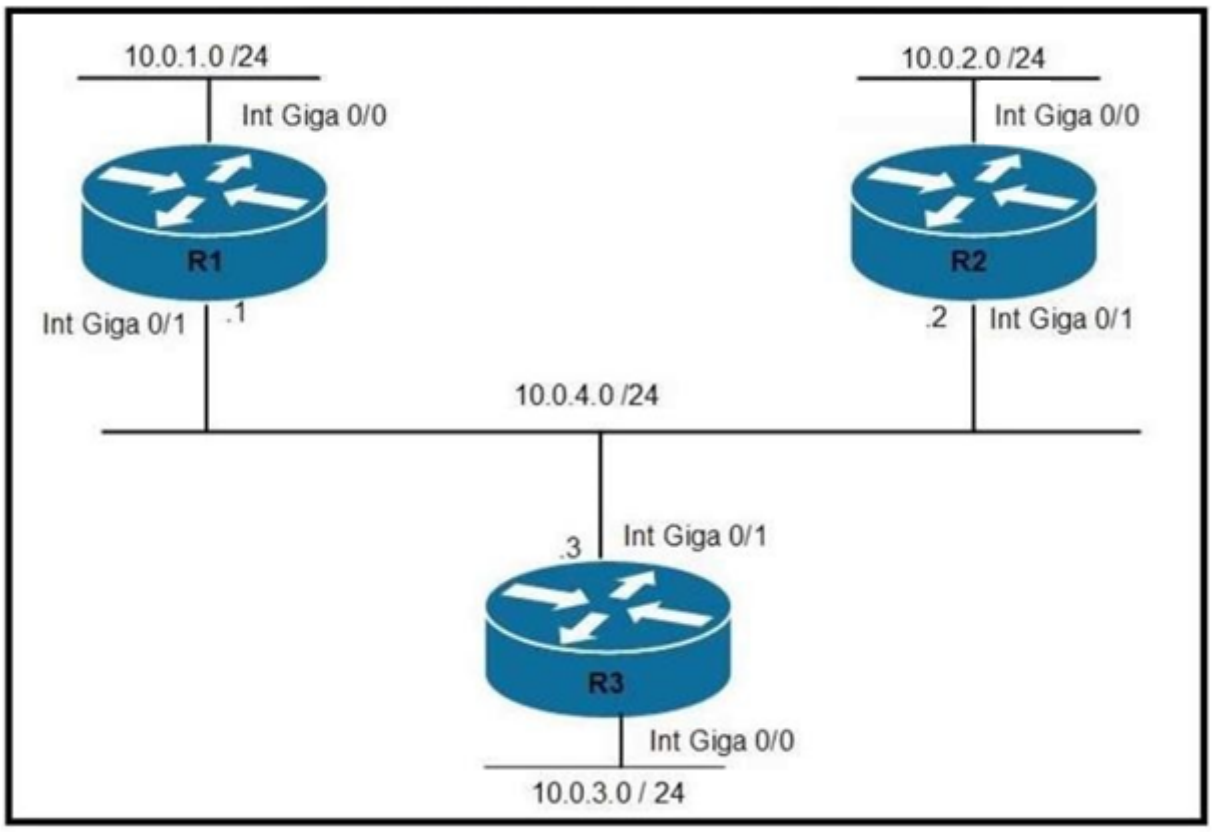
Selected Answer: D

The "show ipv6 eigrp events" command displays the recent EIGRP for IPv6 events and provides information about the error messages, notifications, and warnings generated by EIGRP for IPv6. This command is useful for troubleshooting EIGRP for IPv6 issues.

upvoted 1 times

Question #379 *Topic 1*

Refer to the exhibit. Which two statements about the network environment of router R1 must be true? (Choose two.)



Refer to the exhibit. Router R1 must be configured to reach the 10.0.3.0/24 network from the 10.0.1.0/24 segment. Which command must be used to configure the route?

A. route add 10.0.3.0 0.255.255.255 10.0.4.2

B. ip route 10.0.3.0 0.255.255.255 10.0.4.2

C. route add 10.0.3.0 mask 255.255.255.0 10.0.4.3

D. ip route 10.0.3.0 255.255.255.0 10.0.4.3

Correct Answer: *D*

Request7108 8 months, 2 weeks ago

The prompt says choose two?

upvoted 4 times

freeknowledge123 8 months, 1 week ago

relates to the next question

upvoted 4 times

```
R1#show ip route
Gateway of last resort is 10.85.33.14 to network 0.0.0.0
D*EX  0.0.0.0/0
          [170/257024] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0.100
          [170/257024] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0.100
    10.0.0.0/8 is variably subnetted, 6692 subnets, 20 masks
B         10.0.0.0/8 [20/0] via 10.48.144.14, 1w5d
D EX      10.0.1.0/24
          [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0.100
          [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0.100
D EX      10.0.2.0/23
          [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0.100
          [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0.100
D EX      10.0.4.0/22
          [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0.100
          [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0.100
D EX      10.0.8.0/21
          [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0.100
          [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0.100
D EX      10.0.16.0/20
          [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0.100
          [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0.100
D EX      10.0.32.0/19
          [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0.100
          [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0.100
B         10.1.96.0/23 [20/0] via 10.111.33.217, 2w3d
B         10.1.96.0/24 [20/0] via 10.111.33.217, 2w3d
B         10.1.97.0/24 [20/0] via 10.111.33.217, 4w5d
D EX      10.1.255.240/28
          [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0.100
          [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0.100
D EX      10.2.0.0/16
          [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0.100
          [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0.100
B         10.2.0.0/24 [20/0] via 10.111.33.217, 4w5d
B         10.2.96.0/23 [20/0] via 10.48.144.14, 4w5d
B         10.2.96.0/24 [20/0] via 10.48.144.14, 3w1d
B         10.2.97.0/24 [20/0] via 10.48.144.14, 4w5d
D EX      10.3.0.0/16
          [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0.100
          [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0.100
B         10.5.1.0/24 [20/0] via 10.111.33.217, 1w4d
B         10.5.5.0/24 [20/0] via 10.111.33.217, 4w3d
B         10.6.0.0/24 [20/0] via 10.111.33.217, 3w3d
```

A. The EIGRP administrative distance was manually changed from 90 to 170.

B. There are 20 different network masks within the 10.0.0.0/8 network.

C. Ten routes are equally load-balanced between Te0/1/0.100 and Te0/2/0.100.

D. The 10.0.0.0/8 network was learned via external EIGRP.

E. A static default route to 10.85.33.14 was defined.

Correct Answer: *BC*

Tylosh Highly Voted 1 year ago

Where is the question ?

upvoted 24 times

Yunus_Empire 9 months, 2 weeks ago

Good Question

upvoted 14 times

andresfjardim Highly Voted 7 months, 3 weeks ago

Selected Answer: BC

Question: Refer to the exhibit. Which two statements about the network environment of router R1 must be true? (Choose two.)

upvoted 6 times

shaney67 Most Recent 23 hours, 19 minutes ago

I don think C can be correct, how can they all be load balanced if not all the routes have the same metric?

upvoted 1 times

Sdiego 7 months, 4 weeks ago

B isn't correct, there may be 20 different network paths, but not 20 different network masks...

upvoted 1 times

binrayelias 8 months ago

B and C since since D EX is external eigrp with AD of 170

upvoted 1 times

DoBronx 10 months, 3 weeks ago

what? no question? freebie!

upvoted 2 times

GigaGremlin 11 months, 1 week ago

B is Wrong, WITHIN the 10.0.0.0/8 network are only 19 Network Masks
C is correct
E is correct, 10.85.33.14 is a static default route
upvoted 2 times

mzu_sk8 10 months ago
the static route is to 0.0.0.0 using 10.85.33.14 as the next hop!! E is wrong
upvoted 2 times

splashy 11 months, 3 weeks ago
Selected Answer: BC
D EX = EIGRP external = default 170 AD
So you can eliminate A+D

10.0.0.0/8 is variably subnetted,6692 subnets, 20 masks
B is correct

C is correct just count the 170 AD load balanced routes

E is not correct because it states "to 10.85.33.14" i think... at first i thought it also was correct
it should be via 10.85.33.14 or to 0.0.0.0
upvoted 5 times

Murphy2022 11 months, 3 weeks ago
E ist not correct as it isn't a static route, thanks for the explanation of B and C!
upvoted 1 times

guynetwork 1 year ago
Selected Answer: AC
Refer to the exhibit. Which two statements about the network environment of router R1 must be true? (Choose two.)

A C
upvoted 3 times

Customexit 10 months, 3 weeks ago
but it's not EIGRP (90), it's External EIGRP hence the D EX (170). nothing was changed.
upvoted 4 times

Question #381 *Topic 1*

Which two statements about exterior routing protocols are true? (Choose two.)

A. They determine the optimal within an autonomous system.

B. They determine the optimal path between autonomous systems.

C. BGP is the current standard exterior routing protocol.

D. Most modern networking supports both EGP and BGP for external routing.

E. Most modern network routers support both EGP and EIGRP for external routing.

Correct Answer: *BC*

Clinques Highly Voted 1 year, 8 months ago

Selected Answer: BC

Exterior Gateway Protocols (EGP): Used for routing between autonomous systems. It is also referred to as inter-AS routing. Service providers and large companies may interconnect using an EGP. The Border Gateway Protocol (BGP) is the only currently viable EGP and is the official routing protocol used by the Internet.

NOTE

Because BGP is the only EGP available, the term EGP is rarely used; instead, most engineers simply refer to BGP.

https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7

upvoted 15 times

mda2h Most Recent 2 months, 2 weeks ago

Selected Answer: BC

EGP is old

upvoted 1 times

[Removed] 3 months ago

I'm really tired of all these questions that have nothing to do with CCNA 200-301

upvoted 1 times

Yunus_Empire 9 months, 2 weeks ago

Selected Answer: BC

https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7

upvoted 1 times

arenjenkins 10 months, 3 weeks ago

beyond scope

upvoted 2 times

amadeu 1 year, 8 months ago

B and C is the correct answer.

upvoted 3 times

Question #382 *Topic 1*

You have two paths for the 10.10.10.0 network - one that has a feasible distance of 3072 and the other of 6144.
What do you need to do to load balance your EIGRP routes?

A. Change the maximum paths to 2

B. Change the configuration so they both have the same feasible distance

C. Change the variance for the path that has a feasible distance of 3072 to 2

D. Change the IP addresses so both paths have the same source IP address

Correct Answer: *BC*
Every routing protocol supports equal cost path load balancing. In addition, Interior Gateway Routing Protocol (IGRP) and EIGRP also support unequal cost path load balancing. Use the variance n command in order to instruct the router to include routes with a metric of less than n times the minimum metric route for that destination. The variable n can take a value between 1 and 128. The default is 1, which means equal cost load balancing. Traffic is also distributed among the links with unequal costs, proportionately, with respect to the metric.
Reference:
https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13677-19.html#topic1

jehangt3 Highly Voted 2 years, 3 months ago
THE QUESTION DOES NOT STATE TO "CHOOSE 2 ANSWERS" !
upvoted 117 times

reagan_donald Highly Voted 1 year, 9 months ago
They were claiming that they have removed EIGRP from blueprints, as i guess they just lied out there...there are lot of deep/detailed questions about EIGRP which i have not met neither in Wendell Odom nor on Netacad.
upvoted 16 times

Ali526 1 year, 2 months ago
It is not very helpful.
upvoted 1 times

[Removed] Most Recent 3 months ago
PLEASE STOP with the no CCNA 200-301 questions! They just confuse people wanting to take the 200-301 exam!!
upvoted 3 times

Chopaka 2 months, 4 weeks ago
Sow hou are 100% sure that there is not a single question Aboutaleb EIGRP?
upvoted 3 times

Dhruv3390 8 months ago
BC are correct choice here.
B: By changing the the configuration and make feasible distance same for both, will enable ECMP (Equal Cost Multiple Path) Load-balancing. It will load balance the traffic.

C: By changing the Variance by 2 (Means allowing other feasible distance upto x 2) of 3072.
In other words, If I apply variance 2 on 3072, I'm allowing other distance by to 6144 can be Load- balance. This is called Enequal-cost load-balancing. which is only supported by EIGRP. I hope this helps.
upvoted 4 times

kyleptt 2 months, 2 weeks ago
Totally agree with this
upvoted 1 times

david124 1 year, 1 month ago
this question is not a CCNA question it is a CCNP question
upvoted 11 times

Nvoid 1 year, 8 months ago
Please fix so theres two answers, thanks!
upvoted 5 times

ProgSnob 1 year, 9 months ago
I believe the answer should be C. Variance is something used to create unequal cost load balancing. I've never read anything that just says to change the configuration so they have the same feasible distance. Using variance is practically an EIGRP staple.
upvoted 3 times

Satya927 2 years ago

From what I understood, both B and C represent the same thing, i.e., by changing variance to 2 allows value to be same(2*3072=6144) which is C & B states to change the configuration to achieve same feasible distance which is if variance 2 is given both will have the same feasible distance. So I guess the answers are correct.

upvoted 2 times

Peterpyon 2 years, 1 month ago

Folks,
Eigrp supports an unequal path metrics (cost) using Variance command. in this case, C is the correct answer.

upvoted 4 times

lordnano 2 years, 6 months ago

Can someone explain the answer?
I would assume only C is a correct solution:
B: is feasible distance not a calculated number?
“feasible distance: Best metric among all path to a network. It is calculated by adding the advertised/reported distance advertised by the neighbor and the cost calculated by that current router to reach the neighbor.”
https://www.geeksforgeeks.org/eigrp-cost-calculation/
C: Makes sense since 3072 multiplied by variance 2 is 6144
https://study-ccna.com/eigrp-authentication-load-balancing/

upvoted 3 times

Robin999 2 years, 6 months ago

I would say its only B. The Distance needs to be the same but not forced 2.
Probaly both are right but B is the better answer.
However there are just 4 answers and no "Choose two".

upvoted 2 times

LTTAM 2 years, 8 months ago

Answers are correct. Source:

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13677-19.html#topic1

upvoted 5 times

velrisan 2 years, 3 months ago

is true, from the same source of LTTAM here is the answer: Every routing protocol supports equal cost path load balancing. In addition, Interior Gateway Routing Protocol (IGRP) and EIGRP also support unequal cost path load balancing

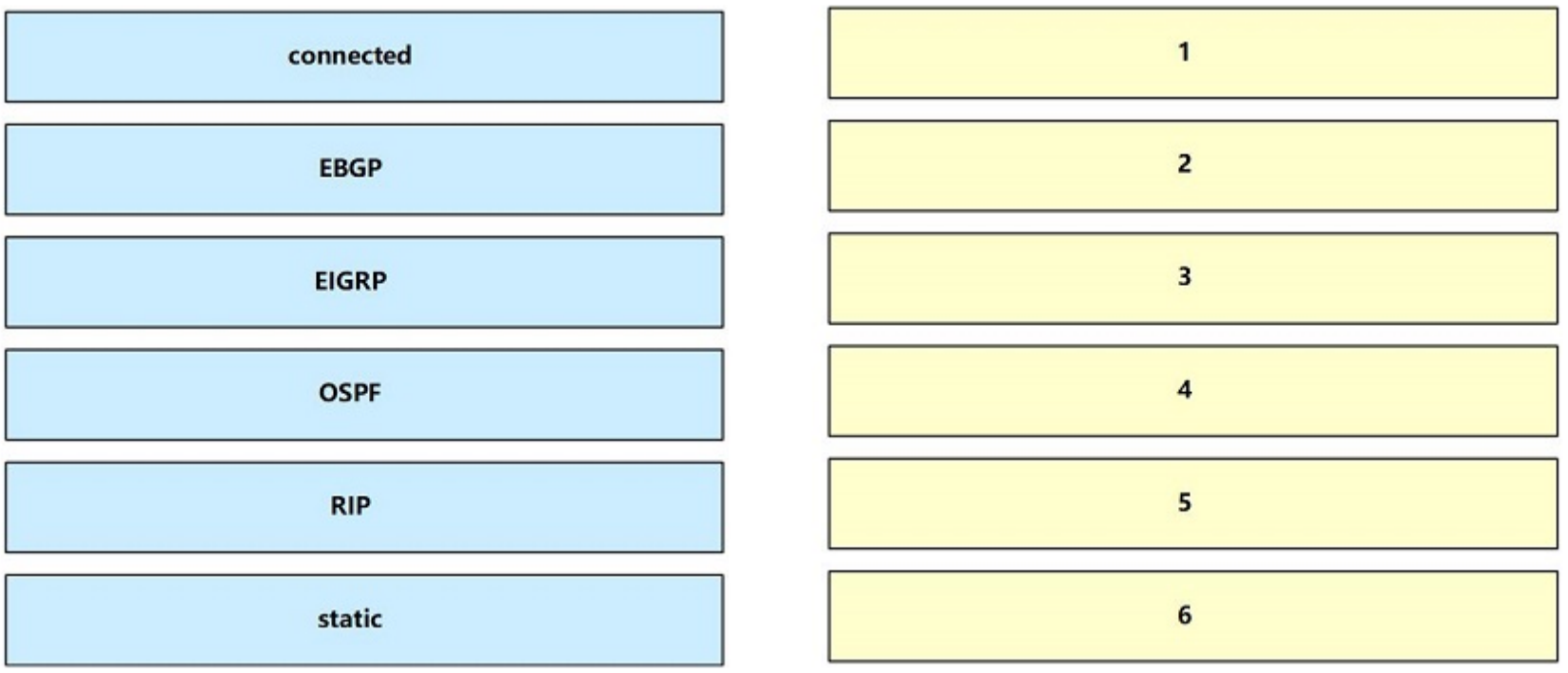
upvoted 2 times

Question #383 *Topic 1*

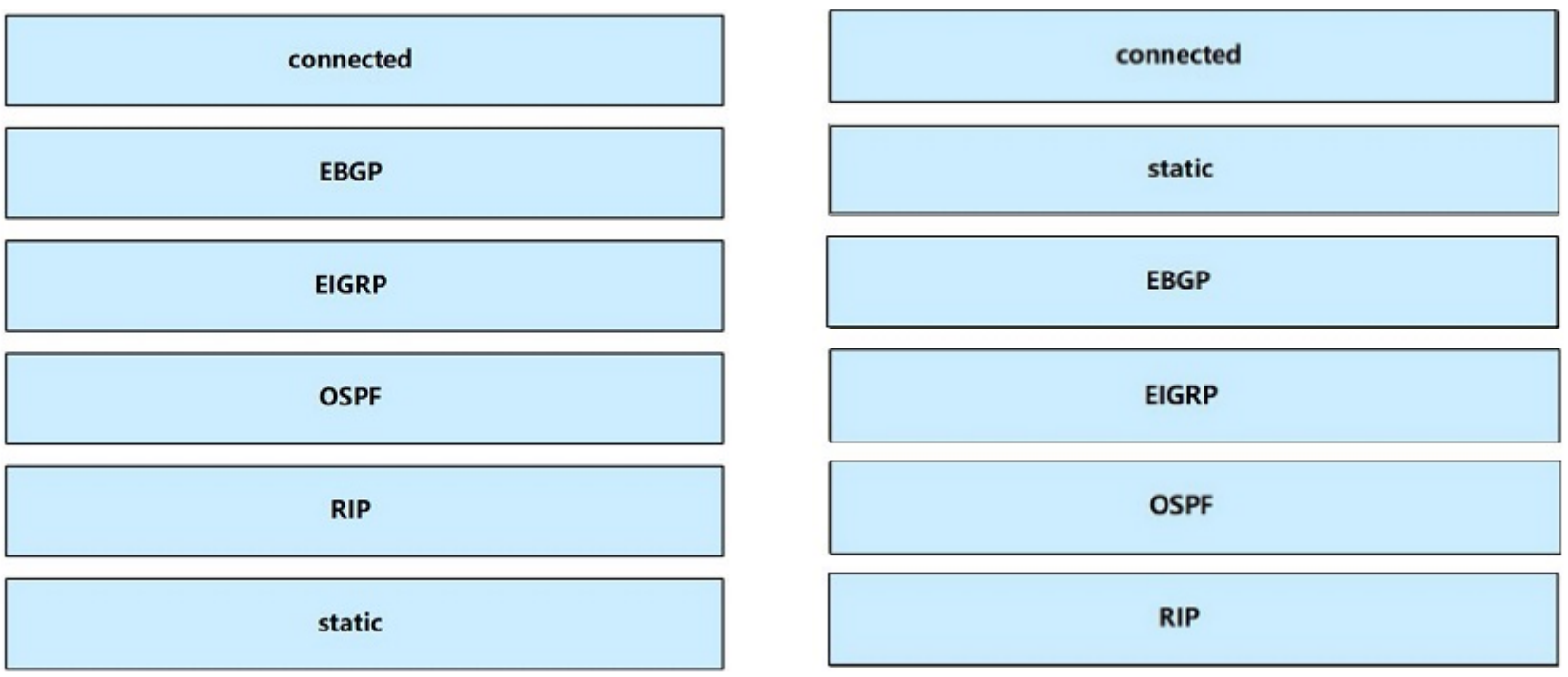
DRAG DROP -

Drag each route source from the left to the numbers on the right. Beginning with the lowest and ending with the highest administrative distance.

Select and Place:



Correct Answer:



Chocobo Highly Voted 2 years, 6 months ago

Administrative distances for these are:
Connected - 0
Static route - 1
EBGP - 20
EIGRP - 90
OSPF - 110
RIP - 120

upvoted 46 times

jerry19 2 years, 4 months ago

To caveat, IBGP is 200. Not shown here but definitely worth noting.

upvoted 19 times

BooleanPizza 2 years ago

Also worth noting, IS-IS has an AD of 115.

upvoted 16 times

msomali Highly Voted 1 year, 4 months ago

here is a list of routing protocols with default ADs

Connected = 0
Static Route = 1
eBGP (external) = 20
EIGRP (Internal) = 90

OSPF = 110
IS-IS =115
RIP =120
EIGRP (external) =170
iBGP (internal BGP) = 200
EIGRP summary route = 5

upvoted 13 times

Nevnarion Most Recent 11 months, 1 week ago

Easy way to remember these; if you can memorise that connected is first and static is second, the rest of them are in alphabetical order.

upvoted 8 times

[Removed] 3 months ago

To memorise that connected is 0 and static is 1, you can use this : c0nnected = 0 and stat1c = 1

upvoted 1 times

illuded03jolted 1 year, 3 months ago

DO – Directly connected- 0
Secure- Static- 1
Buggy- eBGP- 20
Encryption- Internal (EIGRP)- 90
On- OSPF- 110
Internet- ISIS- 115
Router- RIP- 120

upvoted 5 times

Question #384 *Topic 1*

Which two circumstances can prevent two routers from establishing an OSPF neighbor adjacency? (Choose two.)

A. mismatched autonomous system numbers

B. an ACL blocking traffic from multicast address 224.0.0.10

C. mismatched process IDs

D. mismatched hello timers and dead timers

E. use of the same router ID on both devices

Correct Answer: *DE*

dicksonpwc Highly Voted 2 years ago

Must be unique:
– OSPF process ID
– router ID
– IP address
Must match:
– netmask
– area ID
– timers
upvoted 35 times

Yinxs 3 weeks, 5 days ago

OSPF process ID doesn't need to be nuique. It is a local stuff.
upvoted 2 times

mimo1000 Highly Voted 1 year, 9 months ago

you guys confuse people here.
the giving answers are correct
upvoted 9 times

kyleptt Most Recent 2 months ago

D &E are correct
upvoted 1 times

Pamirt 11 months, 2 weeks ago

Selected Answer: DE

timers must match, router id must unique
upvoted 3 times

peshev123 1 year, 4 months ago

Selected Answer: DE

answ: C,D,E
upvoted 1 times

sdokmak 2 years, 2 months ago

D and E
upvoted 4 times

CISCO2022 2 years, 3 months ago

Area duplicate router ID
%OSPF-4-DUP_RTRID1: Detected router with duplicate
router ID 100.0.0.2 in area 0
Explanation—OSPF detected a router that has the same router ID in the area.
Recommended Action—The OSPF router ID should be unique. Make sure all routers in the area have unique router ID.
upvoted 3 times

CISCO2022 2 years, 3 months ago

b and C
OSPF uses two IP multicast addresses on broadcast and point-to-point networks: 225.0. 0.5 for all OSPF routers and 224.0. 0.6 for all DR/BDR (designated router/backup designated router) routers. Using IP multicast addresses is more efficient than using broadcast addresses.
upvoted 1 times

Nicocisco 1 year, 6 months ago

B = 224.0.0.10 so it's D & E
C = process ID is local so we dont care about that

upvoted 1 times

TA77 1 year, 2 months ago

Process ID must be unique, so C is wrong. Given answer is correct (D and E).

upvoted 1 times

DoBronx 10 months, 3 weeks ago

process ID does not have to be unique

upvoted 2 times

Cisco2021 2 years, 3 months ago

what is the correct answer?

upvoted 1 times

mkamau 2 years, 7 months ago

224.0.0.10 is used by eigrp so CD are correct

upvoted 4 times

Robin999 2 years, 6 months ago

Given Answers are correct.
C is no possibilty. Process ID doesnt needs to match, but it can - it doesnt matter for the adjacent process

upvoted 2 times

Ali526 2 years, 8 months ago

B can also be correct. Needs to be checked out.

upvoted 2 times

daynight 2 years, 8 months ago

B is wrong: The IPv4 multicast addresses used for OSPF are 224.0. 0.5 to send information to all OSPF routers and 224.0. 0.6 to send information to DR/BDR routers. The IPv6 multicast addresses are FF02::5 for all OSPFv3 routers and FF02::6 for all DR/BDR routers.

upvoted 6 times

Ali526 2 years, 8 months ago

You are 100% right. I forgot Multicast IPs of OSPF. '10' is for eigrp.

upvoted 3 times

Question #385 *Topic 1*

Which three describe the reasons large OSPF networks use a hierarchical design? (Choose three.)

A. to speed up convergence

B. to reduce routing overhead

C. to lower costs by replacing routers with distribution layer switches

D. to decrease latency by increasing bandwidth

E. to confine network instability to single areas of the network

F. to reduce the complexity of router configuration

Correct Answer: *ABE*

dicksonpwc Highly Voted 2 years ago

Hierarchical design of OSPF (basically means that you can separate the larger internetwork into smaller internetworks called areas) helps us create a network with all features listed above (decrease routing overhead, speed up convergence, confine network instability to single areas of the network).

upvoted 21 times

echarles10 Highly Voted 2 years, 8 months ago

A,B and E is correct

upvoted 6 times

splashy Most Recent 12 months ago

Selected Answer: ABE

Not D because you're not increasing bandwidth, you're decreasing ospf related multicast traffic

upvoted 4 times

ratu68 1 year, 2 months ago

OSPF uses a hierarchical design. Commonly, large OSPf uses this hierarchical design. The main reasons for using this design are the following:

To reduce the routing overhead.
For faster convergence.
To converge all the instabilities into a particular area.

https://snabaynetworking.com/what-is-ospf-area-ospf-hierarchical-network-design-and-advantages/

upvoted 1 times

qasawq 1 year, 2 months ago

Selected Answer: ABE

see @dicksonpwc's comment

upvoted 1 times

peshev123 1 year, 4 months ago

Selected Answer: ADE

it´s ok

upvoted 1 times

Robin999 2 years, 6 months ago

Could D an option too?
If you have less Overhead, because of building more areas, you can encrease the Bandtwith.

upvoted 3 times

Zerotime0 2 years, 6 months ago

In essence of what areas are for and hierarchical design ,those answers given are bestest out of maybe some others like D

upvoted 4 times

mike132 1 year, 2 months ago

No because summary routes would take care of this most of the time, making it not that much more complex.

upvoted 1 times

Refer to the exhibit. If R1 receives a packet destined to 172.16.1.1, to which IP address does it send the packet?

```
R1#show ip route
#output suppressed

Gateway of last resort is 192.168.14.4 to network 0.0.0.0

C       172.16.1.128/25 is directly connected, GigabitEthernet1/1/0
C       192.168.12.0/24 is directly connected, FastEthernet0/0
C       192.168.13.0/24 is directly connected, FastEthernet0/1
C       192.168.14.0/24 is directly connected, FastEthernet1/0
C       172.16.16.1 is directly connected, Loopback1
    192.168.10.0/24 is variably subnetted, 3 subnets, 3 masks
0       192.168.10.0/24 [110/2] via 192.168.14.4, 00:02:01, FastEthernet1/0
0       192.168.10.32/27 [110/11] via 192.168.13.3, 00:00:52, FastEthernet0/1
0       192.168.0.0/16 [110/2] via 192.168.15.5, 00:05:01, FastEthernet1/1
D       192.168.10.1/32 [90/52778] via 192.168.12.2, 00:03:44, FastEthernet0/0
0*E2    0.0.0.0/0 [110/1] via 192.168.14.4, 00:00:10, FastEthernet1/0
```

A. 192.168.14.4

B. 192.168.12.2

C. 192.168.13.3

D. 192.168.15.5

Correct Answer: *A*

jobba111 Highly Voted 1 year, 2 months ago

route is not there, goes to the default gate way instead.

upvoted 7 times

msomali Highly Voted 1 year, 4 months ago

172.16.1.1 is not in the routing table this means it is a random address.
But since a default static route of 0.0.0.0 has been configured and injected to OSPF with the next hope address of 192.168.14.4 through FastEthernet1/0, thus R1 will send the packet to 192.168.14.4.

upvoted 5 times

TA77 1 year, 2 months ago

I believe the default route was 'generated' not 'configured' as a static. But anyway, the provided answer is correct.

upvoted 2 times

Shanku97 Most Recent 2 weeks, 5 days ago

i know it will be a default gatewaybut what is that 0*E2 in the routing table ?

upvoted 1 times

[Removed] 3 months ago

Selected Answer: A

Route to 172.16.1.1 is not in the routing table so traffic will be sent to the default route (Gateway of last resort) 192.168.14.4

upvoted 1 times

MassNastty1 4 months, 1 week ago

The default gateway is specified as 192.168.14.1. Listed as “The Gateway of Last Resort” at the top of the routing table. This route is generally used to reach the internet but can route traffic to other networks as well. TA77 is correct since it would be listed in the actual routing table with the letter “S” for static route. The CLI syntax for a static route entry in the Privileged Exec Mode would would be: #R1(config): ip route 0.0.0.0 0.0.0.0 192.168.14.1. However, it is indeed specified as a generated default gateway and therefore msomali and TA77 are both correct.

upvoted 1 times

virab4 4 months, 4 weeks ago

Selected Answer: A

answer is A,192.168.15.5 also can be but answer A has lower cost,correct me if im wrong please

upvoted 1 times

UnbornD9 5 months ago

sorry but, 172.16.1.1 does not match with 172.16.0.0/16?? so, the route could be 192.168.15.5... I missed a point?

upvoted 1 times

yuh 4 months, 1 week ago

You are probably misunderstanding.
via192.168.15.5 is the route to 192.168.0.0/16. Not 172.16.0.0/16.
so,answer is A.

upvoted 2 times

Refer to the exhibit. On R1 which routing protocol is in use on the route to 192.168.10.1?

```
R1#show ip route
Codes:  C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.14.4 to network 0.0.0.0

C   192.168.12.0/24 is directly connected, FastEthernet0/0
C   192.168.13.0/24 is directly connected, FastEthernet0/1
C   192.168.14.0/24 is directly connected, FastEthernet1/0
    192.168.10.0/24 is variably subnetted, 3 subnets, 3 masks
O       192.168.10.0/24 [110/2] via 192.168.14.4, 00:02:01, FastEthernet1/0
O       192.168.10.32/27 [110/11] via 192.168.13.3, 00:00:52, FastEthernet0/1
O       192.168.0.0/16 [110/2] via 192.168.15.5, 00:05:01, FastEthernet1/1
D       192.168.10.1/32 [90/52778] via 192.168.12.2, 00:03:44, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.14.4, 00:00:10, FastEthernet1/0
```

A. RIP

B. OSPF

C. IGRP

D. EIGRP

Correct Answer: *D*

Robin999 Highly Voted 2 years, 6 months ago

no AD needed. Rule most specified Prefix you need.

upvoted 8 times

Nhan Highly Voted 2 years, 7 months ago

The AD=90

upvoted 5 times

Yunus_Empire Most Recent 9 months, 2 weeks ago

D is Symbol Used For EIGRP.....Like C Used For Connected....

upvoted 3 times

Customexit 10 months, 3 weeks ago

Not only is /32 is longest prefix, /32 is a host route. It's a route directly to the host.

upvoted 1 times

itExamDumps11 1 year, 4 months ago

D. = EIGRP. Also the default AD for it is 90. That being said, no matter what, longest prefix wins

upvoted 2 times

Scvrfvce 1 year, 4 months ago

This question needs to be looked into, if it was a host IP 192.168.10.1 the answer should be B(OSPF), and if its a network Address of 192.168.10.1, then it can be D (EIGRP), And they didn't specify which of them the IP belongs to

upvoted 2 times

Faouzi1212 1 month, 1 week ago

100% ur right

upvoted 1 times

Pkard 1 year, 9 months ago

I hate how it is often unclear if the destination is a network or a host IP. If 192.168.10.1 is a host IP address then it would use 192.1.10.0/24 (OSPF) to get there. The 192.168.10.1/32 route is only correct if it's a destination network not host.
Does anyone else see it this way and have trouble trying to figure out if they want the route to a network or host?!?

upvoted 2 times

dave1992 1 year, 9 months ago

Here's how I solved it. Look at the letter and notice the D. = EIGRP. Also the default AD for it is 90. That being said, no matter what, longest prefix wins. (Most specific path)

upvoted 3 times

Stonetales987 1 year, 10 months ago

You can also use the codes in the above table. D = EIGRP

upvoted 3 times

firstblood 2 years ago

D wins.

upvoted 4 times

dicksonpwc 2 years ago

As 192.168.10.1 /32 is Longest Prefix.

upvoted 4 times

Question #388 *Topic 1*

Refer to the exhibit. Which Command do you enter so that R1 advertises the loopback0 interface to the BGP Peers?

```
R1
interface Loopback0
    ip address 172.16.1.33 255.255.255.224

interface FastEthernet0/0
    ip address 192.168.12.1 255.255.255.0

router bgp 100
neighbor 192.168.12.2 remote-as 100
```

A. Network 172.16.1.32 mask 255.255.255.224

B. Network 172.16.1.0 0.0.0.255

C. Network 172.16.1.32 255.255.255.224

D. Network 172.16.1.33 mask 255.255.255.224

E. Network 172.16.1.32 mask 0.0.0.31

F. Network 172.16.1.32 0.0.0.31

Correct Answer: *A*

nakres64 Highly Voted 2 years, 7 months ago
BGP is out of content.
upvoted 44 times

firstblood Highly Voted 2 years ago
The way i see it, you got to be prepared for anything.
upvoted 31 times

Olebogeng_G Most Recent 3 months, 1 week ago
Well played Cisco, the mask command says it all.
upvoted 1 times

jo966 7 months, 1 week ago
never thought i could give an answer as a commend:
I exclude:
its a network command so the advertised IP can only be a network address .33 is a host
--> exclude all .33 answers
Then, so far i only used wildcard maks in ACLs so
--> exlcude the wildcards

Only A remains
upvoted 1 times

DoBronx 10 months, 3 weeks ago
well played cisco
upvoted 5 times

splashy 12 months ago
Out of scope but pretty simple to remember:
no wildcard just normal submask,
and the use of the "mask" in front of the submask which is actually syntax tautology (good way to remember)
upvoted 3 times

timskis2 1 year, 3 months ago
why is the correct answer MASK ? in the command ?
upvoted 1 times

Patrick69 1 year, 2 months ago
The correct syntax, including the keyword "mask" when you advertise the network for BGP
R1# router bgp 100
R1#neighbour 172.16.13.33 remote-as 200
R1#network 172.16.13.32 mask 255.255.255.252

upvoted 3 times

timskis2 1 year, 4 months ago

WHY WOULD IT NOT BE "C" ?

upvoted 1 times

HugoP 3 months, 1 week ago

You need to have "mask" in your command

upvoted 1 times

iGlitch 1 year, 4 months ago

BGP is out of scoop.

upvoted 3 times

Summo 1 year, 6 months ago

unlike other routing protocols like OSPF or EIGRP, we have to use subnet mask, not wildcard mask, under BGP to advertise the routes in the "network" command.

upvoted 2 times

HelloBPDU 1 year, 7 months ago

How the hell should I know how to configure BGP?

upvoted 18 times

mohamed1999 2 years ago

Correct answer is A,
D is not correct because the .33 is the first available host in the network and .32 is the network it self. Therefore A is correct.

upvoted 6 times

mrsiafu 2 years, 4 months ago

Okay a subnetting question...but if you don't know how to configure BGP, then you would get this question wrong!

upvoted 6 times

mrsiafu 2 years, 4 months ago

So BGP is part of CCNA now...?

upvoted 7 times

[Removed] 3 months ago

Absolutely not

upvoted 1 times

Acai 2 years, 4 months ago

Might be one of those ungraded questions they throw in there.

upvoted 3 times

Mozah 1 year, 9 months ago

not at all

upvoted 3 times

bobert 2 years, 6 months ago

OSPF uses wildcard mask
network ip-address wildcard-mask area area-id
should be E

upvoted 2 times

bobert 2 years, 6 months ago

nevermind ... it's BGP

upvoted 4 times

XBfoundX 2 years, 8 months ago

When BGP is configured it is not going to advertise networks is just for peering two neighbors, after that you have done your neighborship you can advertise the networks with the command suggested by Exam Topics, another important thing is that BGP needs to have the networks in the Routing table for be advertised if the networks are not in the Routing Table the networks will not be advertised.

upvoted 2 times

Zerotime0 2 years, 8 months ago

Net id 0,32,64 so D would be incorrect because its not a net id but a usable 1st ip?

upvoted 1 times

Question #389 *Topic 1*

Refer to exhibit. What Administrative distance has route to 192.168.10.1?

```
R1@show ip route
Codes:  C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.14.4 to network 0.0.0.0

C   192.168.12.0/24 is directly connected, FastEthernet0/0
C   192.168.13.0/24 is directly connected, FastEthernet0/1
C   192.168.14.0/24 is directly connected, FastEthernet1/0
    192.168.10.0/24 is variably subnetted, 3 subnets, 3 masks
O       192.168.10.0/24 [110/2] via 192.168.14.4, 00:02:01, FastEthernet1/0
O       192.168.10.32/27 [110/11] via 192.168.13.3, 00:00:52, FastEthernet0/1
O       192.168.0.0/16 [110/2] via 192.168.15.5, 00:05:01, FastEthernet1/1
D       192.168.10.1/32 [90/52778] via 192.168.12.2, 00:03:44, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.14.4, 00:00:10, FastEthernet1/0
```

A. 1

B. 90

C. 110

D. 120

Correct Answer: *B*

shumps 2 months ago

why not A because its directly connected and i don't see EIGRP in the table, why refer to the exhibit then

upvoted 1 times

ZUMY 1 year ago

B is correct
Longest pre fix elected

upvoted 3 times

Cyberops 1 year, 4 months ago

Look at the second line of the syslog from the bottom pls
D: 192.168.10.1 (here it is 90/52778) via 192.168.12..2 fa0/0

upvoted 1 times

Veasna_shadow 2 years, 6 months ago

I think 110 rather than 90... Someone help me to explain please ?

upvoted 2 times

Dataset 2 years, 3 months ago

longest prefix match, /32
EIGRP AD=90
regards

upvoted 11 times

stickerbombmaster 2 years, 5 months ago

Second route from the bottom has the longest prefix (/32, its basically host route) with AD 90

upvoted 3 times

Question #390 *Topic 1*

Which value is used to determine the active router in an HSRP default configuration?

A. Router loopback address

B. Router IP address

C. Router priority

D. Router tracking number

Correct Answer: *B*
Q. If there is no priority configured for a standby group, what determines which router is active?
A. The priority field is used to elect the active router and the standby router for the specific group. In the case of an equal priority, the router with the highest IP address for the respective group is elected as active. Furthermore, if there are more than two routers in the group, the second highest IP address determines the standby router and the other router/routers are in the listen state.

xsp Highly Voted 2 years, 7 months ago
keyword default configuration, means that priorities of both routers are the same (100).
upvoted 35 times

mrsiafu Highly Voted 2 years, 4 months ago
This was the better question...
If there is no priority configured for a standby group, what determines which router is active?
upvoted 22 times

siredobu 6 months, 4 weeks ago
That way, it is not a question, rather spoon feeding.
upvoted 1 times

[Removed] 3 months ago
No, that's still a question.
upvoted 3 times

L3nny 1 year, 10 months ago
Typical cisco, these questions are there to trick you.
upvoted 9 times

Rockrl 1 year, 8 months ago
The question stated default priority
upvoted 2 times

Yinxs Most Recent 3 weeks, 5 days ago
Selected Answer: C
Which value is used to determine the active router in an HSRP default configuration?
Answer:C
If there is no priority configured for a standby group, what determines which router is active?
ANswer:B
upvoted 1 times

shiv3003 4 months, 3 weeks ago
why not C
upvoted 1 times

Dhruv3390 8 months ago
Well played Cisco!
upvoted 3 times

everchosen13 11 months, 2 weeks ago
Highest IP by "Default"
You almost had me there cisco
upvoted 2 times

ZUMY 1 year ago
B is correct
upvoted 2 times

BlankNothing1 1 year, 3 months ago

You can go to Wendell Odom's blog which is https://blog.certskills.com/cl514-answer/ that explains why it is the IP address. If the priority is not configured (default configuration of 100) then the active router is selected by using the highest interface address (IP address).

upvoted 1 times

hassanhhady 1 year, 9 months ago

i thought HsRP take priority!!

upvoted 2 times

CCNA_beast_69 1 year, 9 months ago

B is correct

upvoted 1 times

Question #391 *Topic 1*

Refer to the exhibit. If RTR01 is configured as shown, which three addresses will be received by other routers that are running EIGRP on the network? (Choose three.)

```
RTR01 (config) #router eigrp 103
RTR01 (config-router) #network 10.4.3.0
RTR01 (config-router) #network 172.16.4.0
RTR01 (config-router) #network 192.168.2.0
RTR01 (config-router) #auto-summary
```

A. 192.168.2.0

B. 10.4.3.0

C. 10.0.0.0

D. 172.16.0.0

E. 172.16.4.0

F. 192.168.0.0

Correct Answer: *ACD*

sdokmak Highly Voted 2 years, 3 months ago

A, C and D
auto summary uses "classful boundary"
- 10.4.3.0 with mask 255.0.0.0 gives 10.0.0.0
- 172.16.4.0 with mask 255.255.0.0 gives 172.16.0.0
- 192.168.2.0 with mask 255.255.255.0 gives 192.168.2.0

upvoted 45 times

Faouzi1212 1 month, 1 week ago

thanks a lot

upvoted 2 times

hokieman91 Highly Voted 2 years, 7 months ago

Classless routing in EIGRP autosummary so
Class A 10.0.0.0 / 8
Class B 172.16.0.0 /16
Class C 192.168.x.0 /24

Gives answers A, C and D - tricky... I didn't study EIGRP as much since I thought the focus now was/is on OSPF

upvoted 19 times

[Removed] 3 months ago

And you're right. EIGRP is not part of CCNA 200-301 while OSPFv2 is.
https://learningnetwork.cisco.com/s/ccna-exam-topics
3.4 Configure and verify single area OSPFv2
3.4.a Neighbor adjacencies
3.4.b Point-to-point
3.4.c Broadcast (DR/BDR selection)
3.4.d Router ID

upvoted 1 times

hokieman91 2 years, 7 months ago

Typo - meant "classful" routing --- mask dropped

upvoted 3 times

BooleanPizza 2 years ago

Mmm, it thought it was:
A - 10.0.0.0/8
B - 172.16.0.0/12
C - 192.168.0.0/16

upvoted 7 times

Dpsypher 1 year, 2 months ago

yup, good catch.

upvoted 1 times

justajoke Most Recent 2 months, 1 week ago

I thought EIGRP wasn't on the objectives

upvoted 1 times

mda2h 2 months, 2 weeks ago

Selected Answer: ACD

Why A?

Be cause:
- Class A -> use mask 255.0.0.0
- Class B -> use mask 255.255.0.0
- Class C -> use mask 255.255.255.0

It is what it is...

upvoted 1 times

gc999 6 months ago

I think the major command here is "auto-summary", which once it is enabled, routers are summarized to the classful boundary in the routing updates.

upvoted 1 times

MEDO95 8 months ago

im sorry guys i have a guestion. if OSPF in question instead of EIGRP would answer be the same?

upvoted 1 times

kostka 11 months, 1 week ago

EIGRP is part of CCNA? I don't think so

upvoted 2 times

Augusto2332 10 months ago

Is not, not in the official topic list

upvoted 1 times

reagan_donald 1 year, 9 months ago

Probably Cisco's intentions was/is to fail as much candidates as they can, they strictly said that they have removed EIGRP from exam, even David Bombal and other guys are also saying so....it means they just lied....because seems that there are lot of EIGRP questions out there....beside that neither in Wendell Odom nor Netacad EIGRP is mentioned in details....

upvoted 9 times

justajoke 2 months, 1 week ago

Those fuckers, shit like that is why people need sites like this. I know the material I'm supposed to know. I don't know what I don't need to know. And I don't know what they're actually asking some of the time, or what the provided answers are supposed to mean.

upvoted 1 times

Hodicek 1 year, 10 months ago

TRICKY QUESTION ALTHOUGH IT IS VERY EASY ONE

upvoted 1 times

imo90s 2 years, 4 months ago

eigrp is no longer on the exam folks

upvoted 3 times

ITGirl1982 2 years, 3 months ago

Actually, EIGRP is on the exam. My bos has required my entire team to take it and everyone who has taken it so far says EIGRP is on the exam.

upvoted 11 times

mvalveal 2 years, 7 months ago

C D y F. the class are 10.0.0.0 172.16.0.0 192.168.0.0

upvoted 2 times

hokieman91 2 years, 7 months ago

Manual summarization does allow for VLSM, however, auto-summary uses "classful boundary" so Class C would still be 192.168.x.0/24
Good explanation here and demo - http://technologyordie.com/route-summarization-basics

upvoted 2 times

mekesis 2 years, 7 months ago

OK for D & C but why A and not F ? i don't understand.. Can someone help me please

upvoted 1 times

Hexa_44 2 years, 4 months ago

255.0.0.0 - Class A Subnet Mask (10.0.0.0)
255.255.0.0 - Class B Subnet Mask (172.16.0.0)
255.255.255.0 - Class C Subnet Mask (192.168.2.0)

upvoted 5 times

dave1992 1 year, 9 months ago

Based on the answers, the reason why it's A is because 192.168.2.0 is actually a network address. And because we have a 255.255.255.0 mask, that means the third octet is left alone and we move to the 4th octet. So 192.168.2.0 would be the answer and not 192.168.0.0

upvoted 1 times

TheGenoShow 2 years, 7 months ago

Can someone help me with this one if the answers are A,C,D, kinda looking over the answer why is the answer A and not F?

upvoted 6 times

Retxed 2 years, 7 months ago

Using classful, class a, b and c

upvoted 4 times

Question #392 *Topic 1*

Which configuration command can you apply to a HSRP router so that its local interface becomes active if all other routers in the group fail?

A. no additional config is required

B. standby 1 track ethernet

C. standby 1 preempt

D. standby 1 priority 250

Correct Answer: *A*

Simply because that will be the default behavior routers would follow in the event all other routers in the HSRP group fail, then it would not keep attributes such as priority or preemption. What preemption does in summary is to make sure that the configured Priority on all routers within the same HSRP group is always respected. That is, if R1 is configured on the HSRP group with a priority of 150 but he stands as active since all other routers currently subscribed to that group have a priority 150, then will router will preempt the current active router and will take over hence becoming the new active router.
With preemption disabled, the new router does not preempt the current active router, unless routers in the group have to renegotiate their roles based on each router's priority at the time of negotiation.

SollyMalwane Highly Voted 1 year, 6 months ago

Selected Answer: A

NO CONFIGURATION REQUIRED

upvoted 7 times

Yunus_Empire Most Recent 9 months, 2 weeks ago

Good Question!

upvoted 3 times

ktiwari 1 year, 7 months ago

Selected Answer: A

It is simple. No Config is required.

upvoted 2 times

Question #393 *Topic 1*

Which two statements about eBGP neighbor relationships are true? (Choose two.)

A. The two devices must reside in different autonomous systems

B. Neighbors must be specifically declared in the configuration of each device

C. They can be created dynamically after the network statement is configured

D. The two devices must reside in the same autonomous system

E. The two devices must have matching timer settings

Correct Answer: *AB*

FloridaMan88 Highly Voted 2 years, 7 months ago
This topic isn't for CCNA 200-301 exam, more likely for CCNP or CCIE level exams...just good to know for the future.
upvoted 23 times

[Removed] 3 months ago
Yes, good to know but it shouldn't be here.
upvoted 1 times

Un_Paesino_Prima_De_Genzano 2 years, 5 months ago
e c'hai ragione bro, sto albano [leggi username]
upvoted 6 times

daddydagoth 6 months, 3 weeks ago
Bella vedere i fellow network engineers italiani. Saluti a voi butei, spero che l'avete presa la CCNA
upvoted 1 times

Scipions 2 years, 5 months ago
Al castelli solo Genzano!
upvoted 5 times

ShravaniKulkarni Highly Voted 1 year, 4 months ago
We just have OSPF routing protocol in CCNA if I am not wrong.
upvoted 8 times

MDK94 Most Recent 1 year, 2 months ago
"Just like OSPF or EIGRP, BGP establishes a neighbor adjacency with other BGP routers before they exchange any routing information. Unlike other routing protocols however, BGP does not use broadcast or multicast to “discover” other BGP neighbors.

Neighbors have to be configured manually and BGP uses TCP port 179 for the connection."
Source: https://networklessons.com/bgp/bgp-neighbor-adjacency-states#:~:text=Just%20like%20OSPF%20or%20EIGRP,%E2%80%9Cdiscover%E2%80%9D%20other%20BGP%20neighbors.
upvoted 4 times

Eyan 2 years ago
its common sense type of questions, since the IGPs within autonomous systems, BGP is between autonomous systems and need to be configured manually. thats what i understood
upvoted 2 times

iGlitch 1 year, 4 months ago
What about the second choice then smart ?
upvoted 3 times

jpfulton314 2 years ago
The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

This opens the door for topics not necessarily listed in the exam objectives.
upvoted 1 times

Lucaaa 2 years, 3 months ago
Sorry, but are these questions in 200-301 exam???
upvoted 5 times

mrsiafu 2 years, 4 months ago
More BGP... SMH!

upvoted 4 times

Refer to the exhibit. How will the router handle a packet destined for 192.0.2.156?

```
router#show ip route
        Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP, D - EIGRP
        EX - EIGRP external, O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
        N2 - OSPF NSSA external type 2, E1 - OSPF external type 1, E2 - OSPF external type 2,
        E - EGP, i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default, U - per-user
        static route, o - ODR

Gateway of last resort is 192.168.4.1 to network 0.0.0.0

   10.0.0.0/24 is subnetted, 3 subnets
C           10.0.2.0 is directly connected, Ethernet1
D           10.0.3.0 [90/2195456] via 192.168.1.2, 00:03:01, Serial0
D           10.0.4.0 [90/2195456] via 192.168.3.1, 00:03:01, Serial1
C        192.168.1.0/24 is directly connected, Serial0
D        192.168.2.0/24 [90/2681856] via 192.168.1.2, 00:03:01, Serial0
                        [90/2681856] via 192.168.3.1, 00:03:01, Serial1
C        192.168.3.0/24 is directly connected, Serial1
C        192.168.4.0/24 is directly connected, Serial2
```

A. The router will forward the packet via either Serial0 or Serial1.

B. The router will return the packet to its source.

C. The router will forward the packet via Serial2.

D. The router will drop the packet.

Correct Answer: *C*

Retxed Highly Voted 2 years, 7 months ago

Explanation:
Router has pointed default router to 192.168.4.1 and this subnet is connected via serial 2 interface. Router does not have router for the 192.0.2.156. so it will use the default gateway 192.168.4.1. A default route identifies the gateway IP address to which the router sends all IP packets for which it does not have a learned or static route.

upvoted 47 times

Mozah 1 year, 9 months ago

perfect!!

upvoted 4 times

uevenasdf Highly Voted 2 years, 8 months ago

192.0.2.156 has not route so 0.0.0.0 which is connected to 192.168.4.0 (Serial 2)

upvoted 11 times

soRwatches Most Recent 6 months ago

well played Cisco!

upvoted 2 times

Sah_ 6 months, 2 weeks ago

Are there labs in ccna

upvoted 1 times

country_rooted 5 months, 2 weeks ago

Jeremy's i.t lab (Youtube) has labs that you can receive via google drive and download. (check out his ccna playlist of 121 videos. The process should be in one of the 1st 5 vids). Even if you are stuck during a lab you can follow along with his videos.

If you have the funds you can purchase boson exsim and they also have step by step guided labs that can also indicate where youve went wrong, what's been successfully completed, what's incompleted etc.

upvoted 1 times

cormorant 9 months, 1 week ago

1. look up route for 192.0.2.156. you'll see there's none
2. check gateway of last resort and see if it can route 192.0.2.156
3. you'll find out it does: it points to 0.0.0.0, which can fit any ip
4. the route pointing to 0.0.0.0 is 192.168.4.1. this is the route that you want
5. look up its subnet in the routing table and the interface connected to it. that is your answer

upvoted 4 times

Pkard 1 year, 10 months ago

My eyes have betrayed me...I kept reading 192.168.2.156...

upvoted 6 times

Aleks123 1 year, 8 months ago

They play with the numbers like that alot

upvoted 2 times

BooleanPizza 2 years ago

Are we sure that 192.0.2.156 isn't a typo and it's actually 192.168.2.156?

upvoted 2 times

Eyan 2 years ago

can't be type 156 is not even close by any sense to 0

upvoted 1 times

aike92 1 year, 8 months ago

I agree w/ BooleanPizza, this question seems off in correlation to the hundreds of others
if it was a typo &' the questions states "192.168.2.156" then the correct Ans is A (Serial 1)

but just incase it isn't a typo the others would be correct in the Answer tied to the Default gateway

upvoted 1 times

Question #395 *Topic 1*

Which statements describe the routing protocol OSPF? (Choose three.)

A. It supports VLSM.

B. It is used to route between autonomous systems.

C. It confines network instability to one area of the network.

D. It increases routing overhead on the network.

E. It allows extensive control of routing updates.

F. It is simpler to configure than RIP v2.

Correct Answer: *ACE*
The OSPF protocol is based on link-state technology, which is a departure from the Bellman-Ford vector based algorithms used in traditional Internet routing protocols such as RIP. OSPF has introduced new concepts such as authentication of routing updates, Variable Length Subnet Masks (VLSM), route summarization, and so forth.
OSPF uses flooding to exchange link-state updates between routers. Any change in routing information is flooded to all routers in the network. Areas are introduced to put a boundary on the explosion of link-state updates. Flooding and calculation of the Dijkstra algorithm on a router is limited to changes within an area.

Robin999 Highly Voted 2 years, 6 months ago
D probaly would is right too.
If you gonna use OSPF you have more Routing overhead in your network. If its already implemented you can reduce the overhead by building different areas. All in all it increases the overhead.
Answers by Question 184 proofs it
upvoted 10 times

ScorpionNet 1 year, 4 months ago
No because Dynamic Routing Protocols are used to reduce routing overhead not increase it
upvoted 2 times

Auronx92 2 years, 5 months ago
But Question 184, indicates that it reduces overhead, in this question in indicates that it increases it.
upvoted 6 times

promaster 2 years, 3 months ago
Question 184 was in the perspective of using OSPF in a hierarchical design.
upvoted 7 times

Etidic Most Recent 10 months, 3 weeks ago
Selected Answer: ACE
A C & E are correct
upvoted 4 times

ScorpionNet 1 year, 4 months ago
A C and E are correct because that's how scalable OSPF is
upvoted 1 times

Alex127 1 year, 5 months ago
i think d is incorrect
in question 222: Which three describe the reasons large OSPF networks use a hierarchical design?
answer b: to reduce routing overhead is correct
upvoted 2 times

bmatthee01 1 year, 6 months ago
A is correct
B wrong, this is related to ebgp
C correct, it confines network instability to one area of the network, eg in a multi area network if there's a problem in area 1 it will only affect area 1
D possibly correct , as the network grows it has to update its routing table and broadcast lsa, update lsdb, using more cpu and memory resource but this does not describe ospf its a symptom
E. Correct, the router will flood Lsa specifically in its own area not to other areas
F. Wrong. It's not that much easier to configure than rip v2
upvoted 3 times

ismatdmour 1 year, 6 months ago

Wow, u r great man. This word "Symptom" makes D incorrect. All others are descriptions of how ospf operates. I wonder how much those CISCO people are expected exam takers to be so strict on wording (like this)!. I doubt if I asked them the same question that they won't give 4 answers correct -D correct also- out of the six answers given. Agree?

upvoted 2 times

Chen80 2 years, 2 months ago

I think ACE are right, the only doubt is
B: It is used to route between autonomous systems
OSPF actually can operate between different AS thru the ASBR but it was born as an INTERIOR Gateway Routing Protocol, so to operate inside one AS.

upvoted 2 times

Raman1996 1 year, 7 months ago

ospf doesn't use AS, it uses area ID

upvoted 1 times

Question #396 *Topic 1*

Refer to the exhibit. After you apply the given configurations to R1 and R2 you notice that OSPFv3 fails to start.

```
R1
ipv6 unicast-routing

interface FastEthernet0/0
     no ip address
ipv6 enable
     ipv6 address 3001:DBB:13::1/64
     ipv6 ospf 1 area 0
ipv6 router ospf 1
router-id 172.16.1.1

R2
ipv6 unicast-routing

interface FastEthernet0/0
     no ip address
     ipv6 enable
     ipv6 address 2001:DBB:12::12/64
     ipv6 ospf 1 area 3
ipv6 router ospf 1
router-id 172.16.3.3
```

A. The area numbers on R1 and R2 are mismatched

B. The IPv6 network addresses on R1 and R2 are mismatched

C. The autonomous system numbers on R1 and R2 are mismatched

D. The router ids on R1 and R2 are mismatched

Correct Answer: *A*

Raulf Highly Voted 2 years, 5 months ago

Correct. Areas mismatched... however, The IPV6 global addresses are also in different subnets and there shouldn't be connectivity right?

upvoted 5 times

Nicocisco 1 year, 6 months ago

OSPFv3 use link-local address, so when R1 and R2 dont use GUA to speak
(correct me if it's wrong)

upvoted 4 times

Un_Paesino_Prima_De_Genzano 2 years, 5 months ago

sisi dije de si

upvoted 2 times

vadiminski 2 years, 4 months ago

I think the answer is correct, because "ospf fails to START" and the only must-have requirements for ist to start are matching area IDs and hello/dead timers. Correct me, if I'm wrong

upvoted 7 times

ScorpionNet Most Recent 1 year, 4 months ago

Correct because areas, timers, and wildcard masks needs to match

upvoted 3 times

YoniEth 2 years, 1 month ago

can routers on different areas can communicate??

upvoted 1 times

Petan 1 year, 11 months ago

Yes, they can but you will have to configure at least one Area Border Router to help communication between the different areas.

upvoted 5 times

Question #397 *Topic 1*

Which command is used to display the collection of OSPF link states?

A. show ip ospf link-state

B. show ip ospf lsa database

C. show ip ospf neighbors

D. show ip ospf database

Correct Answer: *D*
The "show ip ospf database" command displays the link states. Here is an example:
Here is the lsa database on R2.

R2#show ip ospf database -
OSPF Router with ID (2.2.2.2) (Process ID 1)
Router Link States (Area 0)
Link ID ADV Router Age Seq# Checksum Link count2.2.2.2 2.2.2.2 793 0x80000003 0x004F85 210.4.4.4 10.4.4.4 776 0x80000004 0x005643 1111.111.111.111
111.111.111.111 755 0x80000005 0x0059CA 2133.133.133.133 133.133.133.133 775 0x80000005 0x00B5B1 2 Net Link States (Area 0)
Link ID ADV Router Age Seq# Checksum10.1.1.1 111.111.111.111 794 0x80000001 0x001E8B10.2.2.3 133.133.133.133 812 0x80000001 0x004BA910.4.4.1
111.111.111.111 755 0x80000001 0x007F1610.4.4.3 133.133.133.133 775 0x80000001 0x00C31F

shiv3003 4 months, 3 weeks ago
B i think
upvoted 1 times

shiv3003 4 months, 3 weeks ago
No its D
upvoted 2 times

Chopaka 2 months, 4 weeks ago
Its D!
upvoted 1 times

Question #398 *Topic 1*

Refer to the exhibit. A network associate has configured OSPF with the command:
City(config-router)# network 192.168.12.64 0.0.0.63 area 0
After completing the configuration, the associate discovers that not all the interfaces are participating in OSPF. Which three of the interfaces shown in the exhibit will participate in OSPF according to this configuration statement? (Choose three.)

City#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.12.48	Yes	manual	up	up
FastEthernet0/1	192.168.12.65	Yes	manual	up	up
Serial0/0	192.168.12.121	Yes	manual	up	up
Seriak0/1	unassigned	Yes	unset	up	up
Serial0/1.102	192.168.12.125	Yes	manual	up	up
Serial0/1.103	192.168.12.129	Yes	manual	up	up
Serial0/1.104	192.168.12.133	Yes	manual	up	up

City#

A. FastEthernet0 /0

B. FastEthernet0 /1

C. Serial0/0

D. Serial0/1.102

E. Serial0/1.103

F. Serial0/1.104

Correct Answer: *BCD*
The "network 192.168.12.64 0.0.0.63 equals to network 192.168.12.64/26. This network has:
☞ Increment: 64 (/26= 1111 1111.1111 1111.1111 1111.1100 0000) + Network address:
192.168.12.64
☞ Broadcast address: 192.168.12.127
Therefore all interface in the range of this network will join OSPF.

chr Highly Voted 2 years, 4 months ago
OSPF will match IP addresses based on 192.168.12.64 0.0.0.63.
11000000.10101000.00001100.01000000 => 192.168.12.64
00000000.00000000.00000000.00111111 => 0.0.0.63
Matches will be made on the IP only for the 1's not 0's above. We can invert the bits to make it more familiar as a network mask. This becomes:
11000000.10101000.00001100.01000000 => 192.168.12.64
11111111.11111111.11111111.11000000 => /26 or 255.255.255.192

This therefore gives a match of IPs in the network 192.168.12.64 (the next network is 192.168.12.128) so broadcast is 192.168.12.127 and usable IPs are .65 to 126.

We now match IPs in this range which are:

FastEthernet0/1 (192.168.12.65) - ANSWER B
Serial0/0 (192.168.12.121) - ANSWER C
Serial0/1/102 (192.168.12.125) - ANSWER D

If you are having problems understanding this one the key to write out 0.0.0.63 in binary and then invert the bits.
upvoted 40 times

FALARASTA 4 months, 2 weeks ago
Thank you
upvoted 1 times

Carter_Milk Highly Voted 1 year, 10 months ago
Use the magic number technique. Wildcard mask minus 255 so 255 minus 63 = 192.
192 give block size of 64 (256-192)
network 0 -63
network 64 -127
network 128 - 192
upvoted 12 times

liviuml 5 months, 2 weeks ago

@Carter_Milk why you use right hand to go to the left ear?
Is more simple to add 63 (from wildcard mask) to 64 (the ip of network) an will give you 127 (the upper limit of network). Results the range x.x.x.64-127. Regards,

upvoted 1 times

dmaster42 Most Recent 11 months, 4 weeks ago

excellent explanation, chr, that the way

upvoted 2 times

aliwqa777 2 years, 4 months ago

I see that no one knows the explanation

upvoted 3 times

Jonfernz 2 years, 4 months ago

It has already been explained. The network 192.168.12.64 0.0.0.63 covers IP address ranging from .64 to .127 (it's using a /25 subnet mask).

So in this case, that's what you're looking for.

upvoted 5 times

Sayeem 2 years, 4 months ago

But why 192.168.12.64 0.0.0.63 --> IP address ranging .64 to .127 (why /25 subnet)

upvoted 1 times

BooleanPizza 2 years ago

It's /26 actually

upvoted 3 times

Jonfernz 1 year, 12 months ago

sorry. typo. i meant /26

upvoted 3 times

BooleanPizza 2 years ago

becuse it's a wildcard mask, which is the inverse of the subnet mask which in this case is 255.255.255.192

upvoted 1 times

Sayeem 2 years, 4 months ago

why network 192.168.12.64 0.0.0.63 equals to network 192.168.12.64/26? can anyone help me explain please

upvoted 2 times

jehangt3 2 years, 3 months ago

In order to identify what a wildcard mask actually represents you must subtract the amount from 255 so in this case 255-63=192. So the subnet mask is actually 255.255.255.192 which is a /26.

Use my subnet calculator below to help you master subnetting

1st OCT /1 /2 /3 /4 /5 /6 /7 /8
2nd OCT /9 /10 /11 /12 /13 /14 /15 /16
3rd OCT /17 /18 /19 /20 /21 /22 /23 /24
4th OCT /25 /26 /27 /28 /29 /30 /31 /32

HOSTS 128 64 32 16 8 4 2 1
SUBNET 1 2 4 8 16 32 64 128
PREFIX 128 192 224 240 248 252 254 255

upvoted 5 times

ttomer 2 years, 7 months ago

Why Serial 1.102 and not Serial 1.103?
192.168.12.128 is the next network, isn't it?

upvoted 1 times

hokieman91 2 years, 7 months ago

Network 192.168.12.64 0.0.0.63 covers the addresses for 192.168.12.64 to 127
192.168.12.64 - Network
192.168.12.65 to 126 - Gives 62 Usable host addresses
192.168.12.127 - Broadcast
Only Int F0/1, S0/0 and S0/1.102 fall inside this host range
S0/1.103 is in the next network

upvoted 3 times

Zerotime0 2 years, 7 months ago

So net id'$ Are 0/64/128 pick which ever fall in .64-127.

upvoted 1 times

Chun9 2 years, 7 months ago

I got it thanks.

upvoted 1 times

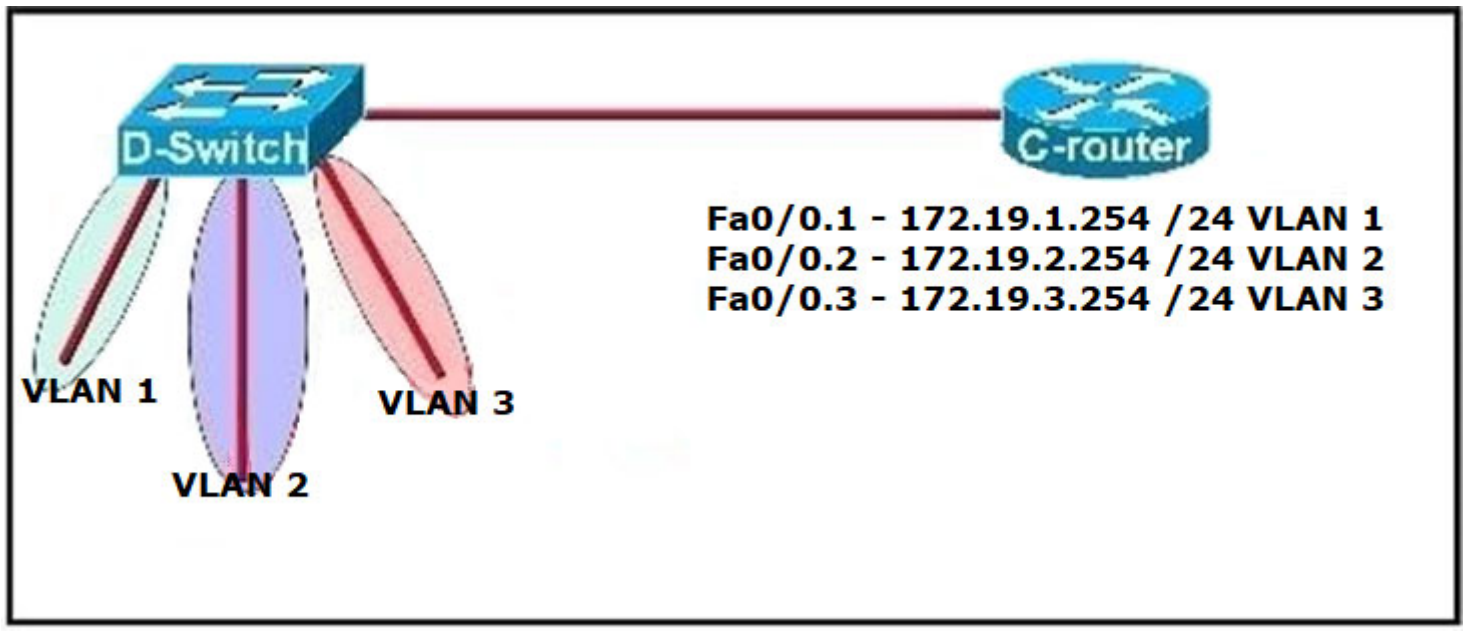
Chun9 2 years, 7 months ago

Can anyone can explain for me please? Thanks

upvoted 1 times

Question #399 *Topic 1*

Refer to the exhibit. C-router is to be used as a "router-on-a-stick" to route between the VLANs. All the interfaces have been properly configured and IP routing is operational. The hosts in the VLANs have been configured with the appropriate default gateway. What is true about this configuration?



A. These commands need to be added to the configuration: C-router(config)# router eigrp 123 C-router(config-router)# network 172.19.0.0

B. These commands need to be added to the configuration: C-router(config)# router ospf 1 C-router(config-router)# network 172.19.0.0 0.0.3.255 area 0

C. These commands need to be added to the configuration: C-router(config)# router rip C-router(config-router)# network 172.19.0.0

D. No further routing configuration is required.

Correct Answer: *D*

Since all the same router (C-router) is the default gateway for all three VLANs, all traffic destined to a different VLA will be sent to the C-router. The C-router will have knowledge of all three networks since they will appear as directly connected in the routing table. Since the C-router already knows how to get to all three networks, no routing protocols need to be configured.

LTTAM Highly Voted 2 years, 8 months ago

D is correct. However... tricky question though. They list the routing protocols to throw you off. The question is actually testing your knowledge of VLAN routing.

upvoted 13 times

Scipions Highly Voted 2 years, 4 months ago

examtopics is the new netacad

upvoted 10 times

RougePotatoe 10 months, 3 weeks ago

Netacad was literally torture here's 2 - 3 hours of reading material and we are going to constantly throw in useless cisco propaganda.

upvoted 4 times

FALARASTA Most Recent 4 months, 2 weeks ago

Always dont overthink. Trick sana

upvoted 1 times

Wes_60 5 months, 2 weeks ago

They are trying to trick you. No routing protocols are needed for router on a stick. Plus they already told you everything was properly configured and functioning.

upvoted 2 times

ScorpionNet 1 year, 4 months ago

D is right because it describes Router on a Stick so it's a VLAN topic

upvoted 1 times

Shamwedge 1 year, 7 months ago

everything is working
No information provided would indicate on which routing protocol would be the one to use
No routing protocol is needed for intervlan routing.

upvoted 1 times

Shamwedge 1 year, 7 months ago

D is my answer

upvoted 1 times

jerry19 2 years, 4 months ago

Technically, you have to configure a native subinterface or none of this will work but since that wasn't an option and we know that "all interfaces have been configured properly and all ip routing is operational," the answer is therefore D.

upvoted 4 times

kyleptt 2 months ago

I was thinking that you must configure 0/0 for this to work

upvoted 1 times

ROBZY90 2 years, 4 months ago

No routing protocols are needed for Router on a stick

upvoted 2 times

Question #400 *Topic 1*

Refer to the exhibit. Which address and mask combination represents a summary of the routes learned by EIGRP?

```
Gateway of last resort is not set

     192.168.25.0/30 is subnetted, 4 subnets
D       192.168.25.20  [90/2681856] via 192.168.15.5, 00:00:10, Serial0/1
D       192.168.25.16  [90/1823638] via 192.168.15.5, 00:00:50, Serial0/1
D       192.168.25.24  [90/3837233] via 192.168.15.5, 00:05:23, Serial0/1
D       192.168.25.28  [90/8127323] via 192.168.15.5, 00:06:45, Serial0/1
C    192.168.15.4/30 is directly connected, Serial0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

A. 192.168.25.0 255.255.255.240

B. 192.168.25.0 255.255.255.252

C. 192.168.25.16 255.255.255.240

D. 192.168.25.16 255.255.255.252

E. 192.168.25.28 255.255.255.240

F. 192.168.25.28 255.255.255.252

Correct Answer: *C*

The binary version of 20 is 10100.

The binary version of 16 is 10000.

The binary version of 24 is 11000.

The binary version of 28 is 11100.

The subnet mask is /28. The mask is 255.255.255.240.

Note:

From the output above, EIGRP learned 4 routes and we need to find out the summary of them:

☞ 192.168.25.16

192.168.25.20

▪

☞ 192.168.25.24

☞ 192.168.25.28

-> The increment should be 28 ?16 = 12 but 12 is not an exponentiation of 2; so we must choose 16 (24). Therefore the subnet mask is /28 (=1111 1111.1111

1111.1111 1111.11110000) = 255.255.255.240.

So the best answer should be 192.168.25.16 255.255.255.240.

Kareemelkh Highly Voted 2 years, 8 months ago

Ali526 check this link it will clear you confusion , I hade the same doubt
https://youtu.be/QqEcCzhlWis

upvoted 23 times

aaaaaaaaakkk 1 year, 2 months ago

this more then helpful thank you

upvoted 2 times

LLAMBRA Highly Voted 2 years, 1 month ago

```
----------------------------------------
| ====== |
192.168.25|.20 -->0001| 0100
192.168.25|.16 -->0001| 0000
192.168.25|.24 -->0001| 1000
192.168.25|.24 -->0001| 1000

128 64 32 16| 8 4 2 1
--------------------
0 0 0 1| 0 1 0 0
0 0 0 1| 0 0 0 0
0 0 0 1| 1 0 0 0
0 0 0 1| 1 0 0 0
```

192.168.25.16/28 == 255.255.255.240
==>192.168.25.16 /255.255.255.240
=== >> answer is C <<===

upvoted 16 times

kyleptt Most Recent 1 month, 2 weeks ago

https://www.youtube.com/watch?v=QqEcCzhlWis good video that helps

upvoted 1 times

bond071982 6 months ago

Is cisco 200-301 webpage down today?

upvoted 6 times

throwaway_account 6 months ago

It's hilarious that they had their "unlimited" promotion last week, then immediately removed all Cisco content. It's like they knew this was coming, but wanted a cash grab first.

upvoted 1 times

monoki 6 months ago

i can't find any cisco exams on the site, i have the same problem.

upvoted 1 times

Elsjona1 6 months ago

i have the same problem

upvoted 1 times

Channaveera 6 months ago

A. 192.168.25.0 255.255.255.240 covers (192.168.25.1 - 15 (boradcast inclusive)
B. 192.168.25.0 255.255.255.252 covers (192.168.25.1 - 3 (boradcast inclusive)
C. 192.168.25.16 255.255.255.240 covers (192.168.25.16 - 192.168.25.31 (boradcast inclusive)
D. 192.168.25.16 255.255.255.252 covers (192.168.25.16 - 192.168.25.19 (boradcast inclusive)
E. 192.168.25.28 255.255.255.240 covers (192.168.25.28 - 192.168.25.43 (broadcast inclusive)
F. 192.168.25.28 255.255.255.252 covers (192.168.25.28 - 192.168.25.31 (broadcast inclusive)
192.168.25.16 255.255.255.240 didn't cover all the range of IPs

upvoted 1 times

Freddy01 9 months, 4 weeks ago

C is the correct answer. Read the question carefully, it's saying what would be the "Summary of the route" meaning summary network address or also known as route summarisation in subnetting. Option C covers all the addresses in the range starting from .16 to .30. Broadcast address on this subnet is 192.168.25.31 which is always one address less from the next block of addresses, which in this case will be a .32 block ending at .47 as it's Broadcast and .48 as the next block. So, 192.168.25.16/28 255.255.255.240 is the summary address for those EIGRP learnt subnets in the routing table showing up in the exhibit.
Another note for those who are confusing it with /30 network: Read the question as it's asking for route summarisation address which will cover .16 to .28 addresses and your /30 prefix for 192.168.25.16 will only go up to .19(Broadcast on this subnet) and then it would be .20 block which does NOT fall in that .16 block as it's the next block of addresses. So, .16 only has .17 and .18 as two allocable host addresses with of course .19 being the broadcast address on this subnet. Hence it's incorrect.

Right answer is C

upvoted 3 times

THEKYPTONIAN 11 months, 2 weeks ago

min - max (192.168.25.16 - 192.168.25.30 = 14) so 14 = /28

upvoted 2 times

TA77 1 year, 2 months ago

The correct answer is C.

You need to find which network range covers all the EIGRP learned addresses in the routing table.

The ranges are as follows:
Answer A:
192.168.25.0 - 192.168.25.15

Answer B:
192.168.25.0 - 192.168.25.3

Answer C:
192.168.25.16 - 192.168.25.31

Answer D:
192.168.25.16 - 192.168.25.19

Answer E:
192.168.25.28 - 192.168.25.43

Answer F:
192.168.25.28 - 192.168.25.31

How to find the ranges? Well, there are different ways to find the ranges. Personally, I'm using the 'Seven Seconds Subnetting' technique by Professor Messer. You may search Youtube for that.

upvoted 3 times

AWSEMA 1 year, 2 months ago

128 64 32 16 8 4 2 1
1 0 1 0 0
1 0 0 0 0
1 1 0 0 0
1 1 1 0 0

upvoted 1 times

[Removed] 1 year, 5 months ago

How did you get the subnet mask of /28

upvoted 2 times

Darrien1301 1 year, 5 months ago

Is it possible to calculate like this: 4 Subnets = 2^4 combinations = 16 and then for the mask 256-16 = 240?

upvoted 1 times

shakyak 1 year, 9 months ago

To those of you who are confused about how the subnet is decided, all the binary that matches is considered 1, and those that don't match is considered 0. So, for the example below:

0 0 0 1| 0 1 0 0
0 0 0 1| 0 0 0 0
0 0 0 1| 1 0 0 0
0 0 0 1| 1 0 0 0

The final four digits don't match which makes the final four digital all zeros.
Hence, the final subnet would be:
11111111.11111111.11111111.11110000 = 240

upvoted 1 times

Kahowl 2 years, 1 month ago

This is stating a /30 subnet, a summary of this address should be:
B) 192.168.25.0 255.255.255.252

upvoted 2 times

Adaya 2 years, 3 months ago

I agree the answer is c

upvoted 1 times

Zerotime0 2 years, 8 months ago

In summary ,Summary encompasses 4 subnets.mask .240 fits better 4x4 =16

upvoted 2 times

Ali526 2 years, 8 months ago

I'll go with D.

upvoted 1 times

MM_9 2 years, 8 months ago

The answer C is correct because it include all network learned via EIGRP (192.168.25.16/28 ---> from 192.168.25.16 to 192.168.25.31) so it summarized all network. The D answer not include all network (192.168.25.16/30 ---> from 192.168.25.16 to 192.168.25.19) so it's wrong

upvoted 9 times

Question #401 *Topic 1*

Refer to the exhibit. Given the output for this command, if the router ID has not been manually set, what router ID will OSPF use for this router?

```
RouterD#   show ip interface brief
Interface          IP-Address     OK?   Method   Status   Protocol
FastEthernet0/0    192.168.5.3    Yes   manual     up       up
FastEthernet0/1    10.1.1.2       Yes   manual     up       up
Loopback0          172.16.5.1     Yes   NVRAM      up       up
Loopback1          10.154.154.1   Yes   NVRAM      up       up
```

A. 10.1.1.2

B. 10.154.154.1

C. 172.16.5.1

D. 192.168.5.3

Correct Answer: *C*

The highest IP address of all loopback interfaces will be chosen -> Loopback 0 will be chosen as the router ID.

Ali526 Highly Voted 2 years, 8 months ago

C is correct and so is the reasoning. If router ID is not manually setup, the highest loopback IP is selected and if there is no loopback, highest IP from the interface IPs is selected.

upvoted 18 times

SasithCCNA 2 years, 5 months ago

Accurate explanation

upvoted 4 times

Dutch012 Most Recent 6 months, 3 weeks ago

did we choose (C) because 172 > 10 (B) ?

upvoted 2 times

kyleptt 2 months, 2 weeks ago

yes that is why

upvoted 1 times

Chopaka 2 months, 4 weeks ago

Sorry maat, niemand snapt hem helaas

upvoted 1 times

SONG00992 1 year, 9 months ago

The highest IP address of any logical interface will always become a router's RID. Loopback interface is the logical interface. So answer is C.

upvoted 1 times

Scipions 2 years, 5 months ago

Grazie a sta ceppa

upvoted 1 times

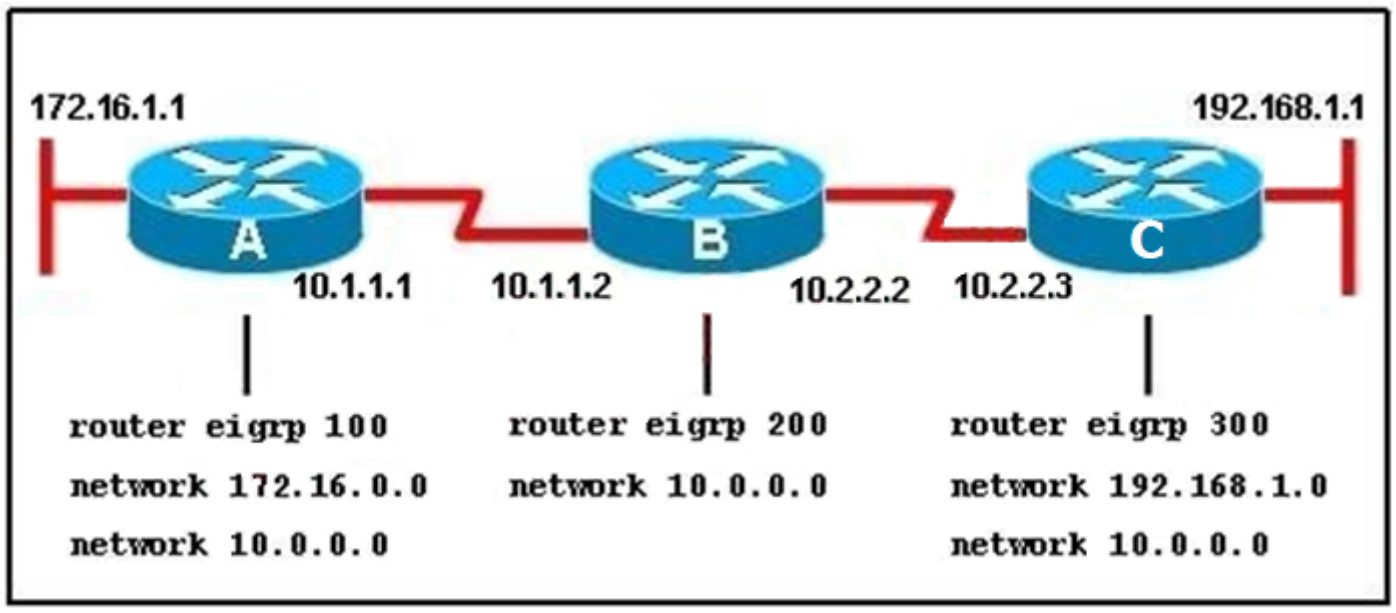
redivivo 1 year, 3 months ago

very accurate

upvoted 1 times

Question #402 *Topic 1*

Refer to the exhibit. When running EIGRP, what is required for RouterA to exchange routing updates with RouterC?



A. AS numbers must be changed to match on all the routers

B. Loopback interfaces must be configured so a DR is elected

C. The no auto-summary command is needed on Router A and Router C

D. Router B needs to have two network statements, one for each connected network

Correct Answer: *A*

This question is to examine the understanding of the interaction between EIGRP routers. The following information must be matched so as to create neighborhood. EIGRP routers to establish, must match the following information:

1. AS Number;

2. K value.

Stonetales987 Highly Voted 1 year, 10 months ago

To become neighbors, the following parameters must match on both routers:
ASN (Autonomous System Number)
subnet
K values (components of metric)

https://geek-university.com/ccna/eigrp-neighbors/

upvoted 12 times

etx Highly Voted 2 years ago

Why not d?

upvoted 6 times

shaz938 2 years ago

Because the existing 10.0.0.0 network statement (Class A address, 255.0.0.0 subnet mask or /8 prefix) already encompasses the two connected networks (10.1.1.2 and 10.2.2.2).

So Answer C is correct.

upvoted 6 times

Shanku97 Most Recent 2 weeks, 4 days ago

HERE WE GO AGAIN,

QUESTIONS AFTER QUESTION FROM EIGRP & BGP FOR CCNA

upvoted 1 times

tubirubs 1 month, 1 week ago

ANOTHER QUESTION OF EIGRP. THIS IS NOT TOPIC OF CCNA 200-301

upvoted 1 times

kishan365 2 months ago

How does router B knows about 192.168.1.0?

upvoted 1 times

gc999 6 months ago

I would choose "C", because, if auto-summary is enabled, classful route is advertised, which both Router A and C also advertise 10.0.0.0/8 which does not make sense.

upvoted 1 times

oatmealturkey 7 months, 1 week ago

Does anyone who has taken the exam remember seeing any questions about EIGRP? I ask because with the release of 200-301, EIGRP has been removed from the CCNA curriculum....

upvoted 3 times

netzwork 11 months, 1 week ago

Selected Answer: A

For EIGRP to work all AS need to be the same, otherwise they won't share the learned networks

upvoted 2 times

[Removed] 1 year, 2 months ago

Selected Answer: A

Wow.... Lesson one of eigrp. If you want neighbours to form, they need to have the same AS.....

upvoted 2 times

PoBratsky 1 year, 3 months ago

Selected Answer: A

A is correct

upvoted 1 times

PoBratsky 1 year, 3 months ago

A is correct

upvoted 1 times

Jbcrggddfhh 1 year, 4 months ago

Selected Answer: C

See shaz's comment for an explanation. Answer is definitely C.

upvoted 1 times

Jbcrggddfhh 1 year, 4 months ago

Meant to say A... mod please remove this

upvoted 1 times

DoBronx 10 months, 3 weeks ago

crazy we cant delete comments

upvoted 1 times

ScorpionNet 1 year, 4 months ago

A is right because EIGRP doesn't have a process ID like OSPF has

upvoted 1 times

Jbcrggddfhh 1 year, 4 months ago

Selected Answer: A

EIGRP routers must have the same AS number to be neighbors

upvoted 1 times

aosroyal 1 year, 5 months ago

Selected Answer: D

i dont understand what the others are saying in the comments.

seems to me like D would be the right answer. Router B needs to advertise the routes correct?

upvoted 1 times

i_am_confused 1 year, 3 months ago

Both networks connected to router B are advertised by the network 10.0.0.0 statement since auto summary is by default enabled.

upvoted 1 times

JamesDean_Youldiots 2 years, 3 months ago

no discussion on this?

upvoted 3 times

Sten111 2 years, 2 months ago

AS number is like the area ID for OSPF. They have to match to exchange routing updates.

upvoted 8 times

A network administrator is troubleshooting the OSPF configuration of routers R1 and R2. The routers cannot establish an adjacency relationship on their common
Ethernet link.

R1: Ethernet0 is up, line protocol is up
Internet address 192.168.1.2/24, Area 0
Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.31.33, Interface address 192.168.1.2
No backup designated router on this network
Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5

R2: Ethernet0 is up, line protocol is up
Internet address 192.168.1.2/24, Area 0
Process ID 2, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

The graphic shows the output of the show ip ospf interface e0 command for routers R1 and R2. Based on the information in the graphic, what is the cause of this problem?

A. The OSPF area is not configured properly.

B. The priority on R1 should be set higher.

C. The cost on R1 should be set higher.

D. The hello and dead timers are not configured properly.

E. A backup designated router needs to be added to the network.

F. The OSPF process ID numbers must match.

Correct Answer: *D*
In OSPF, the hello and dead intervals must match and here we can see the hello interval is set to 5 on R1 and 10 on R2. The dead interval is also set to 20 on R1 but it is 40 on R2.

Talloo Highly Voted 2 years, 7 months ago
By the way, the interfaces on both routers have the same IP address
upvoted 53 times

Ineng Most Recent 5 days, 21 hours ago
Not in the options but both IP of the interfaces are the same.
Plus hello and dead timer are different.
upvoted 2 times

MonsieurP 9 months, 3 weeks ago
What about IP addresses on both e0 interfaces of the 2 routers? Is it correct both be the same?
upvoted 2 times

DoBronx 10 months, 3 weeks ago
Both have same IP, both are DR, shame on cisco
upvoted 3 times

ScorpionNet 1 year, 4 months ago
D is right because the hello and dead interval needs to match in order to maintain neighbor adjacency
upvoted 1 times

dipanjana1990 1 year, 5 months ago
First of all both the routers have same IP address. As well as both belong to same area 0 yet both of them are DR. How come its possible? There are more than 1 reason for these two routers to form ospf neighborship, let alone adjacency. But since there are some parameters which are need to matched in order to form ospf neighborship and timers mismatch is one of them. Thus, option D is correct.
upvoted 1 times

Belinda 1 year, 7 months ago

The hello timer, dead and wait time differs on both routers, thereby causing the adjacency not to form

upvoted 1 times

Belinda 1 year, 7 months ago

The hello timer interval differs on both router which is the reason why the adjacency did form a relationship.

upvoted 1 times

CiscoTerminator 2 years, 1 month ago

Anyone notice that before we even talk about OSPF, the two routers have the same IP address. Definitely an error there.

upvoted 2 times

Cisna 1 year, 12 months ago

The good thing is, its not part of the multiple choices

upvoted 2 times

4guysgaming 2 years, 2 months ago

I also don't see a BDR. The output even says no backup Designated Router on this network?

upvoted 1 times

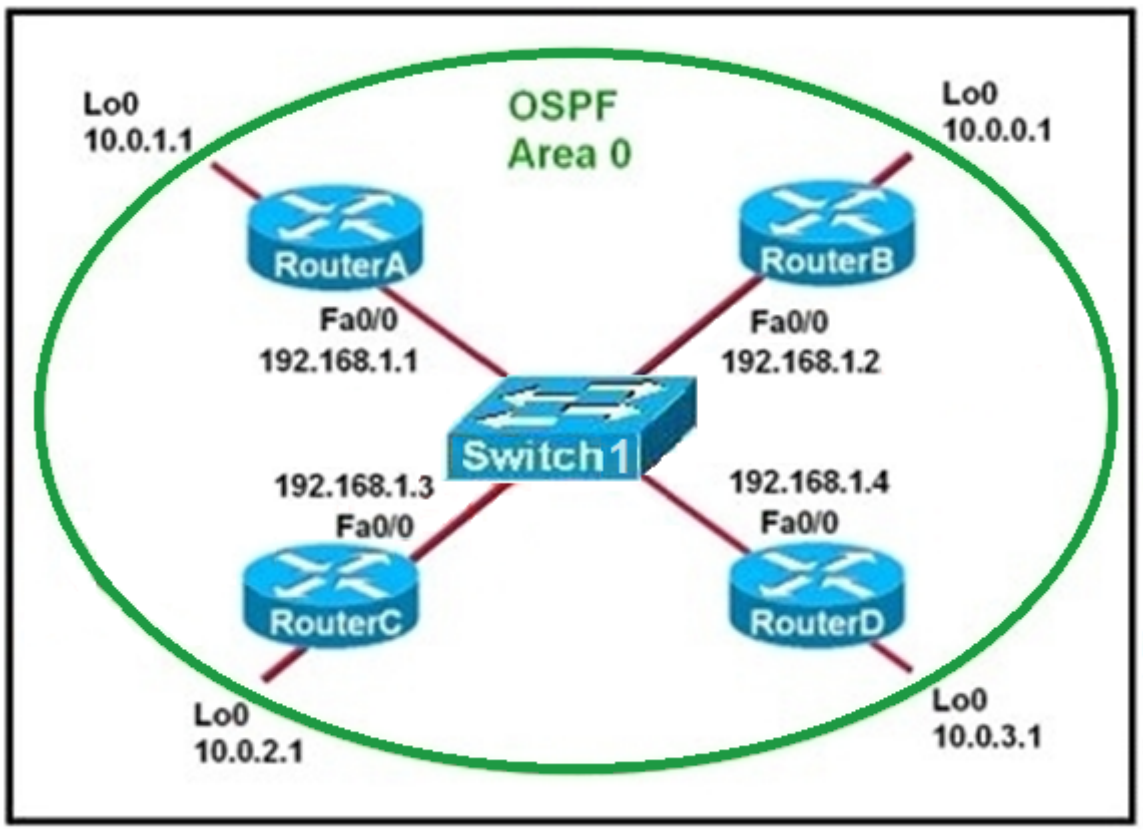
Micah7 2 years, 3 months ago

Agreed- same IP address. This was the first thing I noticed as well, but of course did not see it as an answer option so had to move on to another possibility

upvoted 4 times

Question #404 *Topic 1*

Refer to the exhibit. Which two statements are true about the loopback address that is configured on RouterB? (Choose two.)



A. It ensures that data will be forwarded by RouterB.

B. It provides stability for the OSPF process on RouterB.

C. It specifies that the router ID for RouterB should be 10.0.0.1.

D. It decreases the metric for routes that are advertised from RouterB.

E. It indicates that RouterB should be elected the DR for the LAN.

Correct Answer: *BC*

MikD4016 Highly Voted 1 year ago

A loopback interface never comes down even if the link is broken so it provides stability for the OSPF process (for example we use that loopback interface as the router-id) - B is correct.
The router-ID is chosen in the order below:
The highest IP address assigned to a loopback (logical) interface. If a loopback interface is not defined, the highest IP address of all active router's physical interfaces will be chosen. -The loopback interface will be chosen as the router ID of RouterB - C is correct.

upvoted 14 times

kyleptt Most Recent 1 month ago

Answers seem fine but a RID can be manually configured this does not mean that RID will the loopback

upvoted 1 times

murad999MV 7 months, 3 weeks ago

Selected Answer: BC

true true true

upvoted 1 times

iGlitch 1 year, 3 months ago

Can someone explain how It provides stability for the OSPF process ?

upvoted 4 times

i_am_confused 1 year, 3 months ago

I am not sure either, but if I had to guess it it because the router will have a stable router ID instead of having to pick from the highest configured interface ip address.

upvoted 3 times

hp2wx 1 year, 2 months ago

The loopback interface will provide stability for the OSPF process because the loopback interface is a virtual interface inside of the router, meaning that it is not dependent upon a physical interface being up/up. As long as the router is connected to power and OSPF is enabled, the OSPF process on the router will be active.

upvoted 9 times

kadafi 2 years, 5 months ago

The issue of DR does not apply remember that by default ospf priority is 0.
hence no need to talk about Election process.

The best answers are router id and stability.
upvoted 2 times

DonnerKomet 2 years ago
no, the deafault priority is 1, if you have 0, it means a DROTHER, a ROuter that can not become DR or DBR.
upvoted 8 times

GA24 2 years, 7 months ago
@Zerotime0 , it is the router-ID for router B only. Router-ID must be unique in every router. If the router-ID is not defined on the ospf configuration then it will choose the highest loopback address on that router, if no loopback address was configured then it will choose the highest IP address of the active interface on that router.
upvoted 4 times

Zerotime0 2 years, 7 months ago
I dont get how it specifies router id.. its not highest loopback.y.
upvoted 1 times

SasithCCNA 2 years, 7 months ago
here in the diagram only one loopback is specified so we need to assumes that only one loopback is configured on the router hence it will be used as the router id.
upvoted 2 times

Cpynch 1 year, 7 months ago
With the provided data, it's the ONLY loopback address on each router. Therefore, the router ID.
upvoted 2 times

IxlJustinlxl 2 years, 4 months ago
OSPF uses the following criteria to select the router ID:
1. Manual configuration of the router ID (via the "router-id x.x.x.x" command under OSPF router configuration mode).
2. Highest IP address on a loopback interface.
3. Highest IP address on a non-loopback and active (no shutdown) interface.

With OSPF, the loopback interface is useful because it is an interface with an IP address which never goes down (stability)

Answer = BC
upvoted 17 times

Darrien1301 1 year, 5 months ago
you forgot the priority or not
upvoted 1 times

Tharwat 2 years, 8 months ago
E. It indicates that RouterB should be elected the DR for the LAN.
upvoted 3 times

Ongogablogian 2 years, 8 months ago
Highest ID becomes the DR, not the lowest.
upvoted 5 times

Acai 2 years, 4 months ago
There's no other area in the figure beside 0, so you can't have a DR or BDR
upvoted 2 times

SVN05 1 year, 4 months ago
I was researching on this and it states, as long you have more than 2 routers(considers as Multi Access Network) will allows that area 0(for this ex.) to elect a DR and BDR no?
upvoted 1 times

Question #405 *Topic 1*

If all OSPF routers in a single area are configured with the same priority value, what value does a router use for the OSPF router ID in the absence of a loopback interface?

A. the IP address of the first Fast Ethernet interface

B. the IP address of the console management interface

C. the highest IP address among its active interfaces

D. the lowest IP address among its active interfaces

E. the priority value until a loopback interface is configured

Correct Answer: *C*

M3rc3r08 Highly Voted 2 years, 1 month ago

C is correct.
A router ID is determined in the following order:
1. using the router-id command under the OSPF process to statically configure the router ID.
2. using the highest IP address of the router's loopback interfaces.
3. using the highest IP address of the router's active physical interfaces.

upvoted 12 times

Garfieldcat Most Recent 11 months ago

Piority influent DR/BDR election only, not Router ID

upvoted 3 times

peshev123 1 year, 4 months ago

Selected Answer: C

1.priority
2.loopback
3.high IP

upvoted 1 times

hassanhhady 1 year, 9 months ago

why close dumbs from page 25 to 41 ?

upvoted 1 times

Question #406 *Topic 1*

The OSPF Hello protocol performs which of the following tasks? (Choose two.)

A. It provides dynamic neighbor discovery.

B. It detects unreachable neighbors in 90 second intervals.

C. It maintains neighbor relationships.

D. It negotiates correctness parameters between neighboring interfaces.

E. It uses timers to elect the router with the fastest links as the designated router.

F. It broadcasts hello packets throughout the internetwork to discover all routers that are running OSPF.

Correct Answer: *AC*

vadiminski Highly Voted 2 years, 4 months ago

B: wrong, by default 40 seconds
D: wrong, not only between neighbouring interfaces
E: wrong, designated router is not elected based on its hello-response time, but on its priority / router ID
F: wrong, multicast and not broadcast is used for hello packets
This leaves us with the correct answers A & B

upvoted 34 times

vadiminski 2 years, 4 months ago

Correction, the DEAD timer is 40 sec by default, the hello timer is 10 sec for ethernet networks

upvoted 9 times

Pkard 1 year, 9 months ago

Nice explanation but you must mean A & C. You already said B was wrong

upvoted 8 times

[Removed] Most Recent 1 year, 2 months ago

Selected Answer: AC

A and C is correct

upvoted 2 times

DARKK 1 year, 3 months ago

Selected Answer: AC

Given answer is correct

upvoted 3 times

SVN05 1 year, 4 months ago

B: wrong, by default 10 seconds(hello timer) & 40 seconds(dead timer) for ethernet networks.
D: wrong, not only between neighbouring interfaces
E: wrong, designated router is not elected based on its hello-response time, but on its priority / router ID
F: wrong, multicast is used for Hello packets, not Broadcasts.
This leaves us with the correct answers A & B

Credits:- vadiminski

upvoted 1 times

Question #407 *Topic 1*

What are two requirements for an HSRP group? (Choose two.)

A. exactly one active router

B. one or more standby routers

C. one or more backup virtual routers

D. exactly one standby active router

E. exactly one backup virtual router

Correct Answer: *AB*
Exactly one active router: Only one Active Router per HSRP group will be elected based on highest priority. In case of equal priority, Highest IP address will be elected as Active Router.
One or more standby routers: There can be one or more Standby Routers.

hamish88 7 months, 1 week ago

I also thought there should be only one Active router and only one standby router and the rest will remain in the listening state. However, as per the following lines, it seems we can have more than one router in a standby state:

HSRP uses an active/standby model in which one router actively assumes the role of the default gateway for devices on the subnet. One or more routers on the same subnet are then in standby mode

I also choose A and B.

upvoted 3 times

Murphy2022 11 months, 2 weeks ago

Selected Answer: AB

I think D is a weird wording for 'backup' HRSP-Router which makes no sense.
I go with A and B.

upvoted 1 times

[Removed] 1 year, 2 months ago

Selected Answer: AB

I'd go for Ab... Altough, bay they say standby active.. Maybe they are talking about the command standby?

upvoted 1 times

iGlitch 1 year, 3 months ago

Selected Answer: AD

HSRP group allows a single Active router.
HSRP group allows a single Standby router, the rest of them will be in the "Listening" state.

I think answer D is the closest one but it has "Standby active" in it, and I'll take that as a typo.

upvoted 2 times

iGlitch 1 year, 3 months ago

Or the word 'Active' in answer D means 'Operational' and Not the HSRP Active term.

upvoted 1 times

Jbcrggddfhh 1 year, 4 months ago

Selected Answer: AB

A and B are correct. The below reference shows why D must be wrong:

"HSRP allows you to configure two or more routers as standby routers and only a single router as an active router at a time. All the routers in a single HSRP group shares a single MAC address and IP address, which acts as a default gateway to the local network."

https://www.geeksforgeeks.org/hot-standby-router-protocol-hsrp/#:~:text=HSRP%20allows%20you%20to%20configure,gateway%20to%20the%20local%20network.

upvoted 2 times

eusvt 1 year, 11 months ago

Answer A&B are correct, Cisco 200-301 vol 2 pg 261 by Odom (Cisco Press)

upvoted 2 times

oscar_05 2 years, 2 months ago

I belive it's just necessary have one active router and one standby router in the same domain collition, if other router is in the same domain collition, it take the rol of "listen"

upvoted 3 times

eazy99 2 years, 3 months ago

I believe A is correct but B is not. From my understanding, HSRP can not have more than one router as standby. Any other routers will be in init state but not standby state. Not like VRRP where it doesn't matter how many router you have, you can have 1 master and all other routers become backup routers. With that being said, I believe the closest answer wil be D. Please correct me if I'm wrong.

upvoted 4 times

Sten111 2 years, 2 months ago

You make a good point, I don't think the answer is D though as there is no such thing as an 'active standby' router in HSRP.

I think the way to think of this question is not in the actual HSRP operation in which it would elect one Active and one Standby router, but to think of the HSRP group like the question asks. If you are setting up a group, you would have one router that you configure to become the active router, and one or more routers for standby use.

They are not all standby in operation, but the intended purpose is standby when you are configuring the group.

upvoted 4 times

iGlitch 1 year, 3 months ago

I think answer D has a typo.

upvoted 1 times

mickeil 2 years, 3 months ago

an HSRP group don't really need one standby router

upvoted 2 times

Question #408 *Topic 1*

Which two pieces of information can you learn by viewing the routing table? (Choose two.)

A. whether an ACL was applied inbound or outbound to an interface

B. the EIGRP or BGP autonomous system

C. whether the administrative distance was manually or dynamically configured

D. which neighbor adjacencies are established

E. the length of time that a route has been known

Correct Answer: *CE*

hokieman91 Highly Voted 2 years, 7 months ago

I also thought D and E at first - but then forgot that adjacencies are shown with (confg)# sh ip (ospf, eigrp) neighbor
Most logical is answer given (this is hoping and assuming that you would not manually input the same admin distance as an existing protocol on a route - I see myself over thinking these answers....)

upvoted 18 times

Doopfenel 1 year, 9 months ago

C is correct, because from that command you can see the AD values of the routes. If they match with the default values they have not been manually configured

upvoted 8 times

Jay1324 1 year, 8 months ago

I made the exact same mistake.

upvoted 2 times

dee17 Highly Voted 1 year, 7 months ago

Why is it E ?

upvoted 13 times

dropspablo Most Recent 1 month, 2 weeks ago

Selected Answer: CE

#show ip route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
C 10.16.0.0/30 is directly connected, GigabitEthernet0/1
L 10.16.0.1/32 is directly connected, GigabitEthernet0/1
O 10.24.0.0/30 [110/2] via 10.123.0.2, 00:11:17, GigabitEthernet0/0
S 192.168.99.0/24 [5/0] via 10.123.0.3
([5/0] - Manually configured AD.)
([110/2] - AD dynamically configured)
(00:11:17 - time the OSPF route was learned.)

upvoted 4 times

fra130186 3 months ago

C and E are correct, chat GPT also confirms it

upvoted 1 times

NICE_ANSWERS 3 months, 2 weeks ago

A quick search on google says the answers are B and E

upvoted 1 times

HugoP 3 months, 1 week ago

try it yourself you'll see that there is no AS number in a sh ip route

upvoted 2 times

Kasapin 4 months ago

Selected Answer: CD

I go with C & D. How can you view the time on show ip route?

upvoted 1 times

MadKisa 2 months, 1 week ago

How can u not? check show ip route? O 172.16.1.0 [110/11] via 1.1.1.2, 00:10:04, FastEthernet0/1

upvoted 2 times

Rydaz 4 months, 1 week ago

chat GPT and bing say its B and E

upvoted 1 times

JJY888 4 months, 2 weeks ago

Selected Answer: CD

You can tell your neighbors through directly connected routes and you can tell the AD by knowing the defaults. CD

upvoted 2 times

gc999 6 months ago

Selected Answer: BC

I choose B and C
B - By viewing the Administrative Distance, I can guess which Dynamic Routing it is used. For example, 120 is RIP, 110 is OSPF and etc.
C - We know the default AD of different dynamic routing, so if it is different from the default one, we know it was manually configured

upvoted 1 times

thomson_johnson 5 months, 4 weeks ago

autonomous system number is the one you're entering when: router eigrp 100, AS number is 100 and you don't get that from routing table.

I would go with C and D
Why E??

upvoted 1 times

alejandro12 9 months, 3 weeks ago

Answer C
You can see if the ad of a static route was changed

upvoted 1 times

agazi 1 year, 7 months ago

I think it is confusing when you look at it because D and C are more difficult to choose but due to the generalization of the question where it doesn't specify which protocol (Link state or Distance Vector) Since neighbor adjacency only to (OSPF, IS-IS..,) but administrate Distance (AD) is very common to most routing protocols so I would choose C

upvoted 2 times

q1w2e3r4t5y6 2 years, 7 months ago

i think it's D, E

upvoted 2 times

Doopfenel 1 year, 9 months ago

C is correct, because from that command you can see the AD values of the routes. If they match with the default values they have not been manually configured

upvoted 1 times

Question #409 *Topic 1*

```
      10.0.0.0/24 is subsetted, 1 subnets
C        10.0.0.0 is directly connected, FastEthernet0/1
C     172.160.0/16 is directly connected, FastEthernet0/0
D     192.168.0.0/24 [90/30720] via 172.16.0.2, 00:00:03, FastEthernet0/0
```

Refer to the exhibit. Which route type does the routing protocol Code D represent in the output?

A. statically assigned route

B. route learned through EIGRP

C. 724 route of a locally configured IP

D. internal BGP route

Correct Answer: *B*

Nhan Highly Voted 2 years, 6 months ago

Because the AD is 90

upvoted 12 times

UmbertoReed 2 years, 1 month ago

That's a good way to recognize it, but the proper answer would be: because EIGRP uses the DUAL (D) algorithm to perform its calculations.

upvoted 8 times

jerry19 Highly Voted 2 years, 4 months ago

D = EIGRP, O = OSPF, L = Local, S = Static, C = Directly Connected

upvoted 12 times

mechelleh Most Recent 1 year, 5 months ago

Oh God NOOO, NO MORE EIGRP PLS GOD NOOO

upvoted 6 times

johnnd 1 year, 7 months ago

Selected Answer: B

Route Source	Default AD	Letter
Connected Interface	0	C
Static Route	1	S
External BGP	20	B
EIGRP	90	D
OSPF	110	O
IS-IS	115	i
RIP	120	R

upvoted 5 times

Question #410 *Topic 1*

An engineer must configure an OSPF neighbor relationship between router R1 and R3. The authentication configuration has been configured and the connecting interfaces are in the same 192.168.1.0/30 subnet. What are the next two steps to complete the configuration? (Choose two.)

A. configure the interfaces as OSPF active on both sides

B. configure both interfaces with the same area ID

C. configure the hello and dead timers to match on both sides

D. configure the same process ID for the router OSPF process

E. configure the same router ID on both routing processes

Correct Answer: *BC*

klosinskil Highly Voted 2 years, 11 months ago

A and B
timers match by default
upvoted 47 times

Dante_Dan 1 year, 7 months ago

And also the interface is ISPF active by default...
Tricky question.
upvoted 8 times

Murphy2022 11 months, 2 weeks ago

Ospf isn't active on the interfaces until you configure both interfaces to be inside of area 0 which you do with the network xxxx xxxx area 0 statement inside the ospf process or by using "ip ospf area 0" inside the interface configuration
upvoted 9 times

ITstudent123 Highly Voted 2 years, 10 months ago

Timers match by default
The process ID can be the same or not
The router ID mustn't be the same

So answer is A and B
upvoted 27 times

ZayaB 2 years, 7 months ago

Agreed. For that reason A and B is correct. Tricky question
upvoted 5 times

kyleptt Most Recent 1 week, 2 days ago

Silly question imo
upvoted 1 times

tubirubs 1 month, 1 week ago

Selected Answer: AB

Hello and Dead time are the same by default 10 for hello and 40 (or 4x hello) for the dead
upvoted 1 times

[Removed] 4 months ago

AB should be correct. There's no need to manually configure the timers. Cisco IOS shall use the default timer values automatically if none was configured.
upvoted 1 times

Rydaz 4 months, 1 week ago

at least one router should be active, so if both are active it's good also, by default they are passive, so you NEED to configure them. and also SAME area ID. C is no good because you don't NEED to config hello and dead because by default they are the same value.
so answer is A and B
upvoted 1 times

linuxlife 5 months, 3 weeks ago

OSPF Neighborship Requirement

In order to become OSPF neighbor following values must be match on both routers.

Area ID
Authentication
Hello and Dead Intervals

Stub Flag
MTU Size

upvoted 1 times

Webfat 6 months, 3 weeks ago

This was ChatGPT answer for why A its incorrect and B and C are correct

Option A is not a valid configuration step for establishing an OSPF neighbor relationship. OSPF neighbors are discovered dynamically through the exchange of hello packets, so configuring the interfaces as OSPF active is not necessary.

In OSPF, two devices become neighbors when they exchange hello packets on a common subnet. In this case, since the connecting interfaces are already in the same subnet, the next steps are:

Configure both interfaces with the same area ID (Option B). OSPF routers only become neighbors and exchange information with other routers in the same OSPF area. The area ID can be configured on the interface using the ip ospf area command.
Configure the hello and dead timers to match on both sides (Option C). OSPF neighbors must agree on the interval between hello packets and the interval after which an unresponsive neighbor is considered dead. These timers can be adjusted using the ip ospf hello-interval and ip ospf dead-interval commands.

upvoted 2 times

Cynthia2023 1 month ago

This was ChatGPT answer:
You are correct, and I apologize for the confusion. In OSPF, the default hello and dead timers are 10 seconds and 40 seconds respectively, and they are often considered suitable for most network environments. Therefore, it's generally not necessary to explicitly configure these timers to match for adjacent routers, as they already match by default.

Given this information, the correct options are indeed (D) and (E):

- (D) Configure the interfaces as OSPF active on both sides. This is necessary to enable OSPF on the specific interfaces.
- (E) Configure both interfaces with the same area ID. OSPF routers in the same area must have the same area ID to become neighbors.

Thank you for pointing out the oversight, and I appreciate your understanding.

upvoted 1 times

splashy 11 months, 3 weeks ago

Selected Answer: BC

Enabling OSPF
SUMMARY STEPS
1. enable
2. configure terminal
3. router ospf process-id
4. network ip-address wildcard-mask area area-id
5. end

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html#GUID-51A06D7A-7099-453C-A9FD-34CE45080796

upvoted 1 times

splashy 11 months, 3 weeks ago

Actually... this points more towards AB, assuming the the hello & dead timers are default...

upvoted 4 times

raed6000 1 year ago

Selected Answer: BC

Look when you configure both interfaces with the same area ID and that is what you should and must do, you active OSPF on that interfaces , so answer A sh*t ,and answer B correct.
answer D&E are sh*t you know why,
leaving answer C and that OK

upvoted 2 times

Nickname53796 1 year, 3 months ago

All these questions seem to be too easy to be actual questions

upvoted 2 times

guille_teleco 1 year, 4 months ago

B and C are the correct answer, please update

upvoted 2 times

ismatdmour 1 year, 6 months ago

Selected Answer: AB

Both A and B are configured in one Network command or one ip ospf n area m command

upvoted 3 times

Nicocisco 1 year, 6 months ago

Selected Answer: AB

Yeah i think it's A and B because by default, timer are already matching

upvoted 2 times

Father 1 year, 7 months ago

Very trick, the question says authentication and connecting interfaces have already been done and these will defiantly come as setting OSPF active so I would choose B and C.

Please find ref https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html#GUID-588D1301-F63C-4DAC-BF1C-C3735EB13673

upvoted 3 times

Mozah 1 year, 9 months ago

A & B must be a correct answer. What's on "C" is always by default (Hello timer - 10sec and Dead timer - 40sec). That's my opinion

upvoted 1 times

Alibaba 1 year, 9 months ago

in my opiniop A and C, i saw in another place a and C

upvoted 1 times

Alibaba 1 year, 9 months ago

i mistake B and C right option

upvoted 1 times

Question #411 *Topic 1*

```
R1# show ip route | begin gateway
Gateway of last resort is 209.165.200.246 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.200.246, Serial0/1/0
      is directly connected, Serial0/1/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S     172.16.3.0/24 [1/0] via 209.165.200.250, Serial0/0/0
O     172.16.3.0/28 [110/1] via 209.165.200.254, 00:00:28, Serial0/0/1
      209.165.200.0/24 is variably subnetted, 6 subnets, 2 masks
C     209.165.200.244/30 is directly connected, Serial0/1/0
L     209.165.200.245/32 is directly connected, Serial0/1/0
C     209.165.200.248/30 is directly connected, Serial0/0/0
L     209.165.200.249/32 is directly connected, Serial0/0/0
C     209.165.200.252/30 is directly connected, Serial0/0/1
L     209.165.200.253/32 is directly connected, Serial0/0/1
```

Refer to the exhibit. A packet is being sent across router R1 to host 172.16.0.14. What is the destination route for the packet?

A. 209.165.200.250 via Serial0/0/0

B. 209.165.200.254 via Serial0/0/0

C. 209.165.200.254 via Serial0/0/1

D. 209.165.200.246 via Serial0/1/0

Correct Answer: *D*

The router will use the default route since there is no entry for the destination address/subnet entry in the routine table.

Nhan Highly Voted 2 years, 6 months ago

D is Right, it's use the default route since there is no entry for the destination address/subnet entry in the routine table.

upvoted 18 times

Manjil 1 year, 8 months ago

How do you know which one is the default route from the table?

upvoted 1 times

Jay1324 1 year, 8 months ago

a default route has a 0.0.0.0/0 in its address, meaning 'anything' (that doesn't match else-where in the table) also look into gateways of last resort.

upvoted 3 times

HMaw Most Recent 9 months, 3 weeks ago

It is really sad to see CCNA questions are more and more like a Microsoft exam questions now. So many gotcha Qs instead of allowing test taker to troubleshoot on simulator to fix thing on broken stuff.

upvoted 2 times

DARKK 1 year, 3 months ago

Selected Answer: D

172.16.0.14 is not on the routing table so it goes to 0.0.0.0/0 connected via - D
Pay attention to the 0, 172.16.*0.14

upvoted 1 times

israa 1 year, 5 months ago

The difference between this question & the next one is:
Here, they ask about the route, while the router doesn't learn it directly (it's not in the routing table), its route is the default route.

The next question asks about the destination, the router will route to the closet subnet, to reach distination.

upvoted 1 times

Alibaba 1 year, 9 months ago

C is rigth

upvoted 2 times

DARKK 1 year, 3 months ago

No that's wrong, 172.16.0.14 is not on the routing table so it goes to 0.0.0.0/0 connected via - D
Question #237 172.16.0.14 = D
Question #238 172.16.3.14 = C

upvoted 1 times

DARKK 1 year, 3 months ago

Correction- Question #238 172.16.3.14 = D
upvoted 1 times

taiyi078 1 year, 9 months ago
Question #237 172.16.0.14

Question #238 172.16.3.14

0 and 3 are different
upvoted 3 times

taiyi078 1 year, 9 months ago
What is the difference between Question #237 and Question #238 ???
If you follow Question #238, Question #237 is answer C.
upvoted 1 times

mohamed1999 2 years ago
C is right, because 172.16.3.14 is the last available ip in the /28 subnet.
upvoted 2 times

mohamed1999 2 years ago
nevermind i saw it wrong
upvoted 4 times

shakyak 1 year, 10 months ago
I was on opioid :D
upvoted 1 times

GangsterDady 1 year, 10 months ago
which drugs are you on mate?
upvoted 8 times

randccna 2 years, 6 months ago
Would it not go to C via serial0/0/1? 209.165.200.252/30 is an address range of 252-255 so that would include .254?
upvoted 2 times

UmbertoReed 2 years, 5 months ago
D is correct because there is no network in the routing table that includes 172.16.0.14 in its IP range, so the router needs to default to the gateway of last resort, which in this case is the serial 0/1/0 interface with the next-hop IP address 209.165.200.246.
upvoted 4 times

Retxed 2 years, 8 months ago
Default route to be used
upvoted 4 times

Cristy 2 years, 8 months ago
I think C is the correct answer
upvoted 2 times

Cristy 2 years, 8 months ago
Sorry, I was wrong. I didn't read the instruction carefully
upvoted 1 times

uevenasdf 2 years, 8 months ago
It is going to use the default route I believe it is D
upvoted 7 times

Question #412 *Topic 1*

```
R1# show ip route | begin gateway
Gateway of last resort is 209.165.200.246 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.200.246, Serial0/1/0
     is directly connected, Serial0/1/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S    172.16.3.0/24 [1/0] via 207.165.200.250, Serial0/0/0
O    172.16.3.0/28 [110/84437] via 207.165.200.254, 00:00:28, Serial0/0/1
     207.165.200.0/24 is variably subnetted, 6 subnets, 2 masks
C    207.165.200.244/30 is directly connected, Serial0/1/0
L    207.165.200.245/32 is directly connected, Serial0/1/0
C    207.165.200.248/30 is directly connected, Serial0/0/0
L    207.165.200.249/32 is directly connected, Serial0/0/0
C    207.165.200.252/30 is directly connected, Serial0/0/1
L    207.165.200.253/32 is directly connected, Serial0/0/1
```

Refer to the exhibit. A packet is being sent across router R1 to host 172.16.3.14. To which destination does the router send the packet?

A. 207.165.200.246 via Serial0/1/0

B. 207.165.200.254 via Serial0/0/0

C. 207.165.200.250 via Serial0/0/0

D. 207.165.200.254 via Serial0/0/1

Correct Answer: *D*

The longest matching route to 172.16.3.14 is the 182.16.3.0/28 route, using Serial 0/0/1 with a next hop of 207.165.200.254.

uevenasdf Highly Voted 2 years, 8 months ago

172.16.3.14 routes to ospf route 172.16.3.0-16 /28 - D is correct

upvoted 11 times

Regnalos 2 years, 7 months ago

172.16.3.0-15 /28

upvoted 2 times

cybernett Highly Voted 2 years, 7 months ago

Answer D , because it has the longest prefix compared to other route to the destination?

upvoted 7 times

HugoP Most Recent 3 months, 1 week ago

Selected Answer: D

Remember : Longest prefix match

upvoted 1 times

HugoP 3 months, 1 week ago

Remember : Longest prefix match

upvoted 1 times

msomali 1 year, 4 months ago

Although Static Route has the lower AD than OSPF But from the case study of the question The longest prefix match wins because a /28 gives us 16 possible subnets with each 14 hosts thus starts from 172.16.3.1 -- 172.16.3.14 so OSPF wins with the longest prefix match rule. and the Answer is Letter D

upvoted 2 times

MFarhankhan 2 years, 3 months ago

Hi Guys i also agree with Answer D

upvoted 1 times

mrsiafu 2 years, 4 months ago

SMH...!
172.16.3.0/28
Host range 172.16.3.1 - 172.16.3.14

upvoted 2 times

Nhan 2 years, 6 months ago

Lordnano is correct I miss that question, thank you for clearing that

upvoted 1 times

Nhan 2 years, 6 months ago

Correct answer is C, the AD is 1 which is static router.
upvoted 3 times

lordnano 2 years, 6 months ago
D should be the right answer. The prefix length is more important than the AD: https://packetlife.net/blog/2010/aug/16/route-preference/
upvoted 10 times

oooMooo 2 years, 4 months ago
Routers prefer routes with the "longest match". Meaning the smallest prefix that contains the host's IP address. /28 is a longer match than /24.

D is correct.
upvoted 7 times

```
R1#config t
R1(config)# interface gi1/1
R1(config-if)# ip address 192.168.0.1 255.255.255.0

R1(config)# router bgp 65000
R1(config-router)# neighbor 192.168.0.2 remote-as 65001
R1(config-router)# network 10.1.1.0 mask 255.255.255.0

R1(config)# router ospf 1
R1(config)# router-id 1.1.1.1
R1(config)# network 192.168.0.1 0.0.0.0 area 0
R1(config)# network 10.1.1.0 0.0.0.255 area 0

R1(config)# router eigrp 1
R1(config)# eigrp router-id 1.1.1.1
R1(config)# network 10.1.1.0 0.0.0.255
R1(config)# network 192.168.0.1 0.0.0.0

R2#config t
R2(config)# interface gi1/1
R2(config-if)# ip address 192.168.0.2 255.255.255.0

R2#config t
R2(config)# router bgp 65001
R2(config-router)# neighbor 192.168.0.1 remote-as 65000

R2(config)# router ospf 1
R2(config)# router-id 2.2.2.2
R2(config)# network 192.168.1.2 0.0.0.0 area 0

R2(config)# router eigrp 1
R2(config)# eigrp router-id 1.1.1.1
R2(config)# network 192.168.0.1 0.0.0.0

R2(config)# ip route 10.1.1.0 255.255.255.0 192.168.0.1
```

Refer to the exhibit. Router R2 is configured with multiple routes to reach network 10.1.1.0/24 from router R1. Which path is chosen by router R2 to reach the destination network 10.1.1.0/24?

A. static

B. EIGRP

C. eBGP

D. OSPF

Correct Answer: *A*

xsp Highly Voted 2 years, 7 months ago

Admin Distance:
Connected - 0
Static - 1
eBGP - 5
iEIGRP - 90
OSPF - 110
IS-IS - 115
RIP - 120
So yeah answer is correct based from AD of a statically configured route.

upvoted 14 times

oooMooo 2 years, 4 months ago

Routing Protocol Administrative distance
Directly connected interface 0[a][5]
Static route out an interface 1[b]
Static route to next-hop address 1
DMNR - Dynamic Mobile Network Routing 3
EIGRP summary route 5
External BGP 20
Internal EIGRP 90
IGRP 100
OSPF 110
IS-IS 115

Routing Information Protocol (RIP) 120
Exterior Gateway Protocol (EGP) 140
On Demand Routing (ODR) 160
External EIGRP 170
Internal BGP 200

upvoted 2 times

Gere 2 years, 7 months ago

eBGP is 20 not 5

upvoted 9 times

Stonetales987 1 year, 10 months ago

5 - Enhanced Interior Gateway Routing Protocol (EIGRP) summary route
20 - External Border Gateway Protocol (BGP)

upvoted 4 times

paolo_brosio Highly Voted 2 years, 4 months ago

Nate a riccoje e fragole

upvoted 6 times

noblackpeople Most Recent 1 year, 5 months ago

Is page 25 last free accessible page for 200-301 ?

upvoted 1 times

Jinzo03 9 months, 2 weeks ago

Yes, at some point to you need to pay to get access to the rest of the content

upvoted 1 times

RichyES 1 year, 8 months ago

The answer is A(correct)

upvoted 3 times

Hodicek 1 year, 9 months ago

check the last line in the table, static is correct

upvoted 1 times

UrMom 2 years, 8 months ago

Static route if configured Always comes First.

upvoted 3 times

uevenasdf 2 years, 8 months ago

Last line of config has static route with AD of 1. EIGRP has mis-configured router id and BGP/OSPF don't have route to 10.1.1.0/24

upvoted 3 times

lordnano 2 years, 6 months ago

I agree on AD, but why do you meen there is no route to 10.1.1.0/24 for BGP/OSPF?

upvoted 2 times

oooMooo 2 years, 4 months ago

Look at the hostnames. I overlooked them in my first pass.

upvoted 1 times

panagiss 1 year, 10 months ago

I'm not sure I get what you are saying

upvoted 1 times

Nicocisco 1 year, 6 months ago

The R1 router share BGP/OSPF network to R2

upvoted 1 times

Question #414 *Topic 1*

```
R1# show ip route
Codes:    C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
          U - per-user static route, o - ODR
Gateway of last resort is not set
C         1.0.0.0/8 is directly connected, Loopback0
          10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O              10.0.1.3/32 [110/100] via 10.0.1.3, 00:39:08, Serial0
C              10.0.1.0/24 is directly connected, Serial0
O              10.0.1.5/32 [110/5] via 10.0.1.50, 00:39:08, Serial0
O              10.0.1.4/32 [110/10] via 10.0.1.4, 00:39:08, Serial0
```

Refer to the exhibit. What is the next hop address for traffic that is destined to host 10.0.1.5?

A. Loopback 0

B. 10.0.1.4

C. 10.0.1.3

D. 10.0.1.50

Correct Answer: *D*

lmadolfo2019 Highly Voted 2 years, 5 months ago

The correct answer is line D.

upvoted 12 times

papinski Most Recent 7 months, 3 weeks ago

Selected Answer: D

Answer is D

upvoted 1 times

DoBronx 10 months, 3 weeks ago

Selected Answer: D

D is right

upvoted 1 times

i_am_confused 1 year, 3 months ago

Selected Answer: D

This is very straightforward.

upvoted 1 times

Ricci91 1 year, 4 months ago

Selected Answer: D

/32 is a host ID so answer is D

upvoted 2 times

TheLorenz 1 year, 6 months ago

Correct Answer D. Question asks what is the next hop address. Multiple routes are inserted into the router already, so now we look for the highest prefix.
A /32 prefix represents a host, and this is the highest you can get with ipv4. The next hop is 10.0.1.50 as you can see where it says 'via 10.0.1.50'.

upvoted 2 times

Samir_123 1 year, 7 months ago

Selected Answer: C

answer D is not host it is the ID

upvoted 1 times

RichyES 1 year, 7 months ago

Selected Answer: D

Anwer is D

upvoted 2 times

Mozah 1 year, 9 months ago

i cant continue from question 240.. prompting to have a Contributor Access
upvoted 3 times

panagiss 1 year, 9 months ago
Contribution access?? LOL
upvoted 1 times

Pkard 1 year, 9 months ago
the question states we are trying to get to the HOST address 10.0.1.5 so the answer should be B ...
Can anybody explain it?
upvoted 1 times

Blazeryf 1 year, 9 months ago
a /32 network is just a host.
So a 10.0.1.5 /32 (255.255.255.255 mask) adress is the only host.
upvoted 2 times

Pkard 1 year, 9 months ago
I'll be damned..you're right! Thanks!
"32 mask is used only to designate a host, not network"
upvoted 1 times

Shamwedge 1 year, 10 months ago
Selected Answer: C
I feel like the answer should be C.

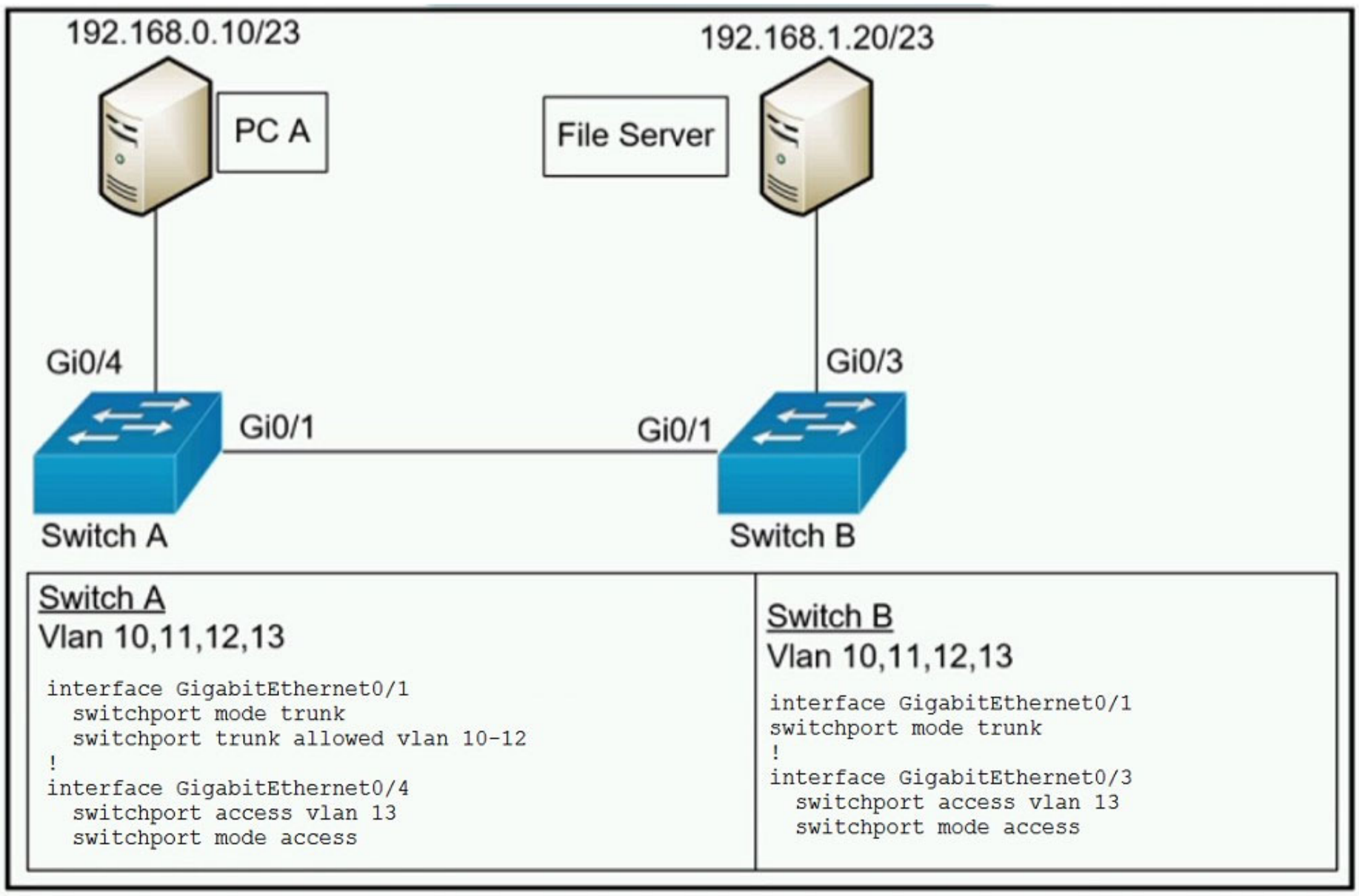
10.0.1.5/32 would that not make 10.0.1.5 the network address and not the host address?
10.0.1.4/32 would make 10.0.1.5 the host address
upvoted 1 times

Darrien1301 1 year, 5 months ago
no 255.255.255.255 is a host route
upvoted 1 times

Shamwedge 1 year, 9 months ago
I actually meant to say the answer should be B, but Blazeryf's reply makes sense
upvoted 1 times

wissmail 2 years ago
Why D??
upvoted 1 times

DonnerKomet 2 years ago
In the routing tables exist one host route learned by OSPF (.5/32) however within the answers there is a typo .50
upvoted 4 times



Refer to the exhibit. A network administrator assumes a task to complete the connectivity between PC A and the File Server. Switch A and Switch B have been partially configured with VLANs 10, 11, 12, and 13. What is the next step in the configuration?

A. Add PC A to VLAN 10 and the File Server to VLAN 11 for VLAN segmentation

B. Add VLAN 13 to the trunk links on Switch A and Switch B for VLAN propagation

C. Add a router on a stick between Switch A and Switch B allowing for Inter-VLAN routing

D. Add PC A to the same subnet as the File Server allowing for intra-VLAN communication

Correct Answer: *B*

DonnerKomet Highly Voted 2 years ago
but ALL VLANs are allowed by default in trunks. It would not be needed to add the VLAN 13 in Switch B.
upvoted 7 times

Thaier 1 month, 3 weeks ago
we choose this answer because the others are 100% wrong
upvoted 3 times

Vilsenil Highly Voted 2 years, 6 months ago
Hosts are in the same subnet /23. Answer B is correct
upvoted 5 times

Shanku97 Most Recent 2 weeks, 4 days ago
CAN ANY GOOD SIR OR MADAM EXPLAIN HOW THE PC AND FILE SERVER IS ON THE SAME SUBNET?
upvoted 1 times

DUMPledore 9 months, 1 week ago
same question with Question #263? choices just worded differently
upvoted 1 times

Garfieldcat 11 months ago
PC and Server are not in the same IP subnet. the answer should be C. A router is required for inter-VLAN route
upvoted 1 times

Customexit 10 months, 3 weeks ago
Subnet 192.168.0.10/23 and see what you get.

upvoted 9 times

Rether16 5 months, 1 week ago

...this made me laugh. ahha!

upvoted 4 times

ScorpionNet 1 year, 4 months ago

B is correct because it's in the same subnet and the Native vlans send untagged frames to others

upvoted 1 times

Mozah 1 year, 9 months ago

The interfaces between switch A and B are set to trunk mode but the VLAN in which the devices are tagged to is not allowed on the trunk. The given answer "B" is correct, simply allow the VLAN ID (VLAN 13) for them to communicate.

upvoted 3 times

KobraKai 2 years ago

switch A interface g0/4 - connected to PC is access mode with vlan13
switch B interlace g0/3 - connected to server is access mode with vlan13

The interfaces between switch A and B are set to trunk mode.
So, only thing is missing is adding vlan 13 to the trunk link
in order for PC and server to communicate.

A. wrong as switches can't do intervlan routing (vlan10 - vlan11)
B. wrong it's not required as both PC and server are in same vlan (router on a stick is for intervlan routing)
D. switches don't do intervlan routing

upvoted 1 times

Giuseppe_001 2 years, 4 months ago

zumy where are u? :-'(

upvoted 5 times

jerry19 2 years, 4 months ago

The answer is apparently B, but should be:
Switch A: switchport mode trunk allowed 10-13
Switch B: switchport mode trunk allowed vlan 10-13

Based off switch B's configs no trunks have been allowed, furthermore anytime you are configuring trunks (on router or switch), you must include native vlan as allowed and it must be identified so that non-tagged traffic is allowed. This question was written by an amateur.

upvoted 1 times

Samuelpn96 2 years ago

The question asks only to ensure communication between the PC and the Server, and just by adding the vlan 13 to the trunk links of both switches will do it.
I tested this in packet tracer.

upvoted 5 times

nenotronix 2 years, 6 months ago

Answer "C" is the correct one.

the hosts are in different subnets [layer3]. hence, a router [layer3] device is required to cater for inter-vlan routing

upvoted 4 times

asd34534 2 years, 5 months ago

here both devices are in the same vlan also same vlan can be in different subnets.
the problem here is with allowed vlans, either add vlan 13 or remove the limit

upvoted 4 times

Pkard 1 year, 9 months ago

They mention INTRA-VLAN communication, not INTER-VLAN routing

upvoted 1 times

UmbertoReed 2 years, 5 months ago

They are not on different subnets. Subnet 192.168.0.0 /23 has 2^9 = 512 hosts, which spans an IP range of 192.168.0.0 - 192.168.1.255. Addresses 192.168.0.10 and 192.168.1.20 are on the same range and their respective interfaces are on the same VLAN. The only problem here is that the trunk link on Switch A doesn't allow VLAN 13, so "B" is correct.

upvoted 11 times

Pkard 1 year, 9 months ago

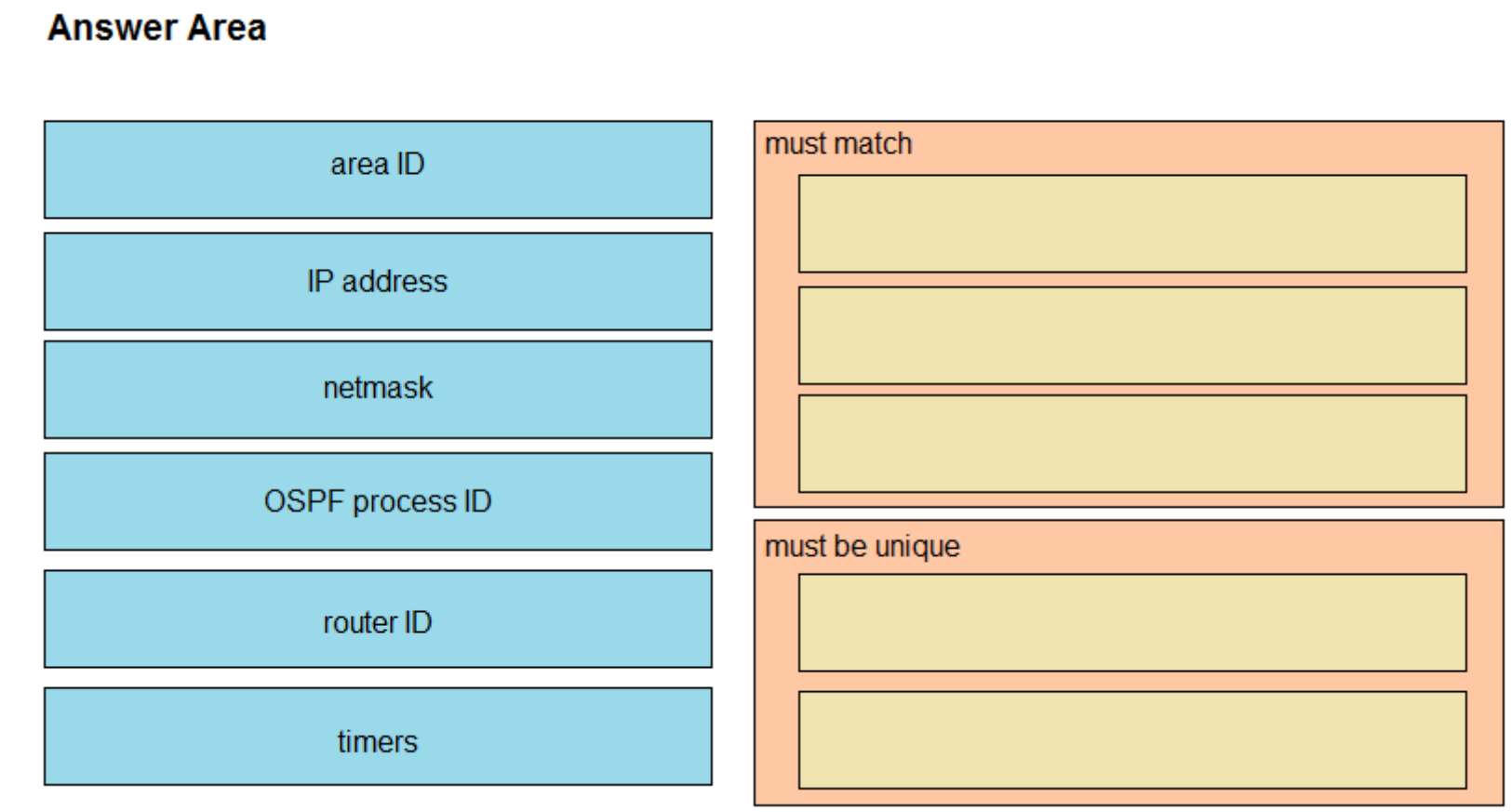
Good eye, i missed that the first time through

upvoted 1 times

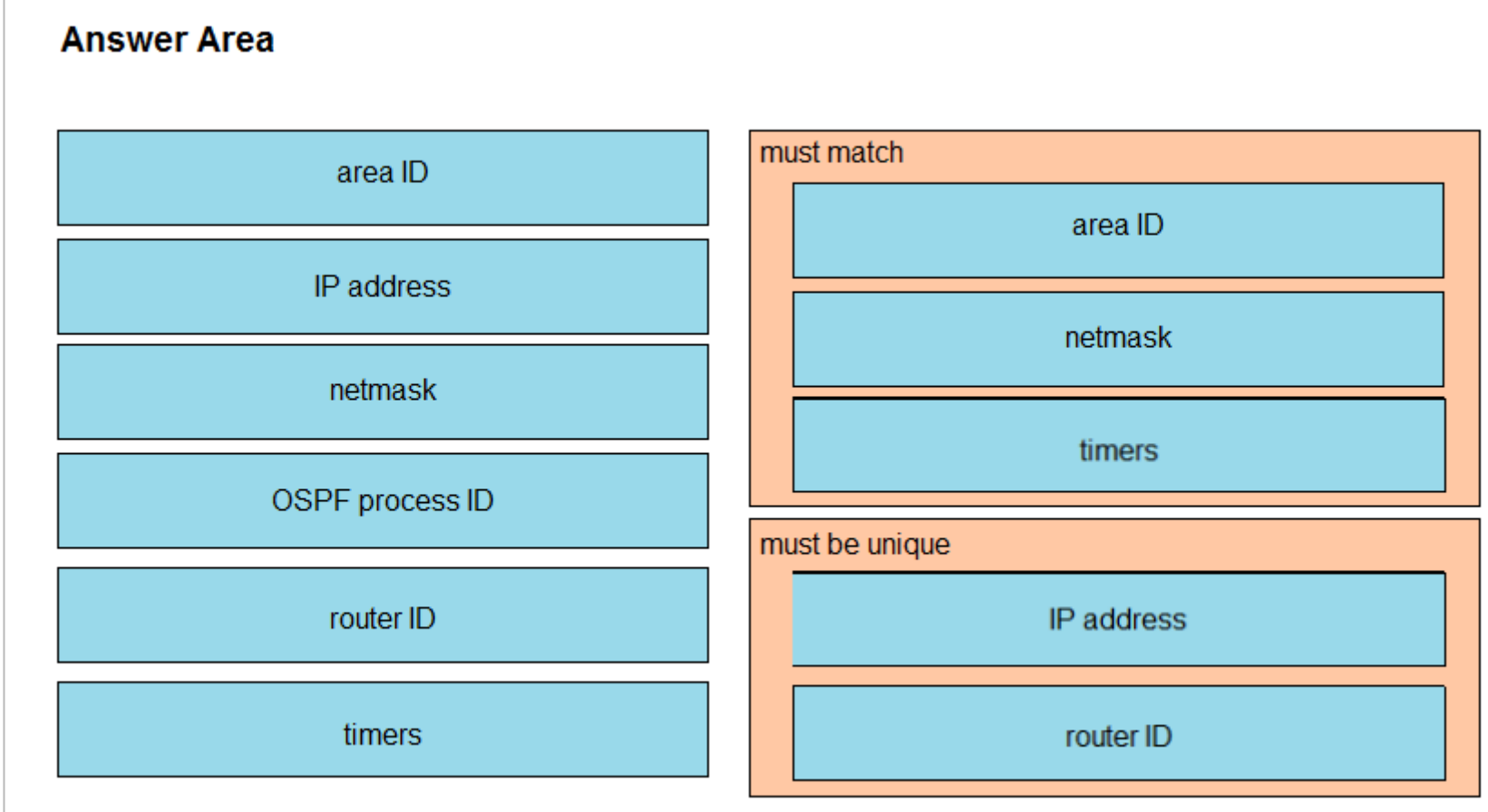
DRAG DROP -

A network engineer is configuring an OSPFv2 neighbor adjacency. Drag and drop the parameters from the left onto their required categories on the right. Not all parameters are used.

Select and Place:



Correct Answer:



ayd33n Highly Voted 3 years, 1 month ago

From the perspective of OSPF, there are a couple of things that must match for a OSPF neighborship to establish; these include:

The devices must be in the same area
The devices must have the same authentication configuration
The devices must be on the same subnet
The devices hello and dead intervals must match
The devices must have matching stub flags

https://www.expertnetworkconsultant.com/configuring/ospf-neighbor-adjacency/

So:
Must Match: Area ID, NetMask, Timers
Must have Unique: IP Address, Router ID

"The OSPF process-id is a numeric value local to the router. It does not have to match process-ids on other routers."
http://cisco2960.over-blog.com/2014/01/cisco-ospf-process-id.html

upvoted 25 times

ScorpionNet Most Recent 1 year, 4 months ago

The given is right

upvoted 4 times

Question #417 *Topic 1*

R1 has learned route 192.168.12.0/24 via IS-IS, OSPF, RIP, and Internal EIGRP. Under normal operating conditions, which routing protocol is installed in the routing table?

A. IS-IS

B. Internal EIGRP

C. RIP

D. OSPF

Correct Answer: *B*

With the same route (prefix), the router will choose the routing protocol with lowest Administrative Distance (AD) to install into the routing table. The AD of Internal

EIGRP (90) is lowest so it would be chosen. The table below lists the ADs of popular routing protocols.

Route Source	Administrative Distance
Directly Connected	0
Static	1
EIGRP	90
EIGRP Summary route	5
OSPF	110
RIP	120

Note: The AD of IS-IS is 115. The ג€EIGRPג€ in the table above is ג€Internal EIGRPג€. The AD of ג€External EIGRPג€ is 170. An EIGRP external route is a route that was redistributed into EIGRP.

Yunus_Empire 9 months, 2 weeks ago

Becz EIGRP Has Lowest AD Value

upvoted 1 times

Etidic 10 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

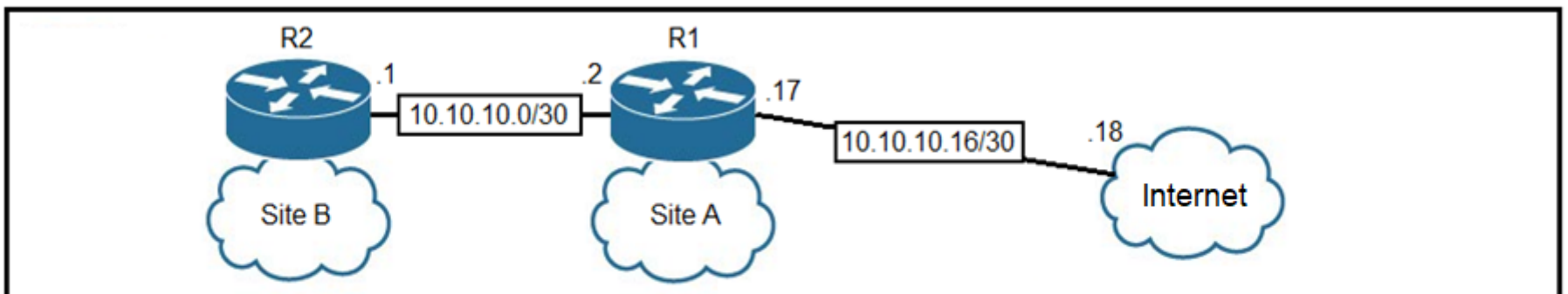
ptfish 1 year, 2 months ago

Selected Answer: B

The answer is B.

upvoted 1 times

Question #418 *Topic 1*




```
R2#sh run | b router ospf
router ospf 1
 router-id 2.2.2.2
 log-adjacency changes
 auto-cost reference-bandwidth 10000
 network 10.10.10.1 0.0.0.0 area 0
 network 10.10.13.1 0.0.0.0 area 0

R2#show ip route
Gateway of last resort is not set
   10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C       10.10.10.0/30 is directly connected
C       10.10.13.0/25 is directly connected, Vlan20
C       10.10.13.144/28 is directly connected, Vlan40
```

```
R1#show ip route
Gateway of last resort is not set
   10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.10.10.0/30 is directly connected, FastEthernet0/1
O       10.10.13.0/25 [110/6576] via 10.10.10.1, 01:37:03
C       10.10.10.16/30 is directly connected, FastEthernet0/24
O       10.10.13.144/28 [110/110] via 10.10.10.1, 01:37:03

R1#sh run | b router ospf
router ospf 1
 router-id 1.1.1.1
 log-adjacency changes
 auto-cost reference-bandwidth 10000
 network 10.10.10.2 0.0.0.0 area 0
 default-information originate
```

Refer to the exhibit. The default-information originate command is configured under the R1 OSPF configuration. After testing, workstations on VLAN 20 at Site
B cannot reach a DNS server on the Internet.
Which action corrects the configuration issue?

A. Add the default-information originate command on R2.

B. Add the always keyword to the default-information originate command on R1.

C. Configure the ip route 0.0.0.0 0.0.0.0 10.10.10.18 command on R1.

D. Configure the ip route 0.0.0.0 0.0.0.0 10.10.10.2 command on R2.

Correct Answer: *C*

Nhan Highly Voted 2 years, 6 months ago
B cannot reach a DNS server on the Intern, there for the static route of the last resort should be configure to point to the internet, therefor the given answer is correct
upvoted 9 times

Pkard 1 year, 9 months ago
That doesn't explain how it site B at Router 2 gets routed to Router 1. The DNS server IP wouldn't be on R1 so it would also need to use the default-route.
Someone please tell me how im out to lunch here, I understand routing tables
upvoted 2 times

pjvillareal 1 year, 9 months ago
"default-information originate" command results in advertising a default route. But, the router which it was configured should first have a default route.

As you can see, R1 does not have a default route. That's why the answer is correct. configuring a default route on R1 will result in R1 advertising a default route to R2. R2 nets will now have a default route pointing to R1, then to internet where DNS server resides.
upvoted 19 times

Aleks123 1 year, 8 months ago
Thank you that really helped!
upvoted 3 times

Pkard 1 year, 9 months ago
Does OSPF distribute the static route? maybe?
upvoted 2 times

kishan365 Most Recent 2 months ago
okay but why not D?

upvoted 3 times

raul_kapone 3 weeks, 1 day ago

Because there is a Connected Route in both routing tables already (of R1 and R2) for this connection. If you configure an static route between them (R1 and R2), it would be redundant, and it could replace the OSPF route because AD of the Static Route, but it doesn't meets the problem of reaching to the internet.

upvoted 1 times

yuh 4 months, 1 week ago

both A and B correct?
"default-information originate always" command, a default route can be generated and advertised even if there is no default route.
Of course, also correct to register default route static.
only choose one, answer is C?

upvoted 1 times

Dutch012 6 months, 1 week ago

R1 is already got a route to reach the internet, there is no need to add a static route.
Anyway both C and D are correct answers and this is why I hate Cisco.

upvoted 2 times

sdmejia01 7 months, 2 weeks ago

Can someone explain why not B? My understanding is that default-information originate always command would make R1 to advertise a default route even if it is not in R1's routing table. The following link explains the above. At this point, I don't see why B and C cannot be both correct answers. Thanks!

https://medium.com/network-warrior/ospf-default-route-10d8d7c251dc#:~:text=In%20OSPF%2C%20the%20%E2%80%9Cdefault%2D,route%20in%20the%20routing%20table.

upvoted 1 times

ptfish 1 year, 2 months ago

Below are the keywords.
R1#show ip route
Gateway of last resort is not set

upvoted 2 times

i_am_confused 1 year, 2 months ago

Selected Answer: C

R1/R2 needs a default route to the internet. R1 needs to have the default route statically entered. R2 will learn the static route from R1 because R1 already configured with default-information originate.

upvoted 2 times

CCNAEASY 1 year, 4 months ago

Letra correta e a (D) precisa de uma rota para o R1, R1 esta ligado diretamente ao DNS ele respondera!

upvoted 2 times

pjvillareal 1 year, 9 months ago

"default-information originate" command results in advertising a default route. But, the router which it was configured should first have a default route.

As you can see, R1 does not have a default route. That's why the answer is correct. configuring a default route on R1 will result in R1 advertising a default route to R2. R2 nets will now have a default route pointing to R1, then to internet where DNS server resides.

upvoted 2 times

shakyak 1 year, 9 months ago

R1 & R2 can communicate but the computer can't go outside of the intranet because the Router doesn't have a route to intranet so we need to add the static route to internet.

upvoted 1 times

shakyak 1 year, 9 months ago

I mean route to internet*

upvoted 2 times

Hodicek 1 year, 9 months ago

default route on r1 to the internet

upvoted 1 times

nenotronix 2 years, 6 months ago

C is correct

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/47868-ospfdb9.html

https://medium.com/network-warrior/ospf-default-route-10d8d7c251dc#:~:text=In%20OSPF%2C%20the%20%E2%80%9Cdefault%2D,route%20in%20the%20routing%20table.

upvoted 3 times

Question #419 *Topic 1*

```
R1# show ip route | begin gateway
Gateway of last resort is 209.165.200.246 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.200.246, Serial0/1/0
     is directly connected, Serial0/1/0
     172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
S    172.16.0.0/24 [1/0] via 207.165.200.250, Serial0/0/0
O    172.16.0.128/25 [110/38443] via 207.165.200.254, 00:00:23, Serial0/0/1
D    172.16.0.192/29 [90/3184439] via 207.165.200.254, 00:00:25, Serial0/0/1
     209.165.200.0/24 is variably subnetted, 4 subnets, 2 masks
C    209.165.200.248/30 is directly connected, Serial0/0/0
L    209.165.200.249/32 is directly connected, Serial0/0/0
C    209.165.200.252/30 is directly connected, Serial0/0/1
L    209.165.200.253/32 is directly connected, Serial0/0/1
```

Refer to the exhibit. With which metric was the route to host 172.16.0.202 learned?

A. 0

B. 110

C. 38443

D. 3184439

Correct Answer: *C*

Both the line ג€O 172.16.0.128/25ג€ and ג€S 172.16.0.0/24ג€ cover the host 172.16.0.202 but with the ג€longest (prefix) matchג€ rule the router will choose the first route.

uevenasdf Highly Voted 2 years, 8 months ago

I'm assuming by metric it means to ignore the 110 OSPF AD and select the cost.
A is wrong because the Static route doesn't reach 172.16.0.202
B is wrong because that is the OSPF AD not metric.
Which leaves C/D...

Host - 172.16.0.202 falls under OSPF 172.16.0.128/25
202 in binary 11001[100] .200 - .207
192 in binary 11000[000] .192 - .199

Which means the host can't reach the EIGRP route therefore the OSPF route is used and has a metric of 38443

upvoted 12 times

FloridaMan88 2 years, 7 months ago

The static route DOES reach the host ... 172.16.0.1 - 254,
BUT the keyword is "LEARNED"
a STATIC route isn't l"learned" so that leaves us with the closed network route that was learned dynamically....hence 172.16.0.128/28 (172.16.0.129 - 254 hosts) OSPF

upvoted 6 times

HugoP 3 months, 1 week ago

It's not really important here, what we have to notice is which route checks the longest prefix match algorithm. The static route doesn't match this algorithm as much as the OSPF one

upvoted 1 times

DARKK Most Recent 1 year, 3 months ago

Selected Answer: C

C. Given answer is correct. /29 is 192-200, so not inclusive, leaving /25 which has a metric of 38443

upvoted 3 times

Angpz 1 year, 5 months ago

C. 38443. Because /25 is the highest prefix to reach 172.16.0.202. So just take the metric form there.

upvoted 2 times

iGlitch 1 year, 4 months ago

but it doesn't reach 172.16.0.202, learn some subnetting

upvoted 3 times

[Removed] 2 months, 3 weeks ago

Before being rude and telling people to learn some subnetting, start with yourself.

172.16.0.128/25
Number of hosts : 126
First host : 172.16.0.129
Last host : 172.16.0.254
So...how it doesn't reach 172.16.0.202 ?

upvoted 3 times

TA77 1 year, 2 months ago

It does reach to 172.16.0.202, lol

upvoted 2 times

Yozz12 1 year, 11 months ago

isn't the number 38443 pointing towards the ospf?

upvoted 1 times

IxlJustinlxl 2 years, 4 months ago

regardless of "learned" or not.. prefix takes precedence over AD.. even if you had a static route /24 that the IP falls in and a OSPF of /25 that it also falls in, the OSPF route will be chosen due to prefix.

upvoted 2 times

Jonfernz 2 years, 4 months ago

Key word here is "metric". The answer would have been 110 if the question asked about the Administrative Distance (AD). OSPF was the preferred route in this instance because of the longest prefix match.

upvoted 4 times

sidato 2 years, 4 months ago

line D 172.16.0.192/29 doesnt it cover also the host

upvoted 1 times

Amarko 1 year, 10 months ago

because for D to be correct, it should be a different mask in routing table
172.168.0.200/29 hosts: 172.168.0.201-172.168.0.206

upvoted 1 times

theodorrrr 1 year, 11 months ago

I don't understand why is not D the correct answer

upvoted 2 times

Mozah 1 year, 9 months ago

172.16.0.128/25 has 128 addresses BUT usable hosts are only126 from to 0.129 to 0.255 which means 172.16.0.202 will be in this /25 subnet range

WHILE
172.16.0.192/29 has 8 addresses BUT only six are usable hosts which is from 0.193 to .0.199 means 172.16.0.202 is out of /29 subnet range.

upvoted 2 times

pouya1 2 years, 6 months ago

The given answer and reason are correct.

upvoted 2 times

FloridaMan88 2 years, 7 months ago

CORRECTION ;)

The static route DOES reach the host ... 172.16.0.1 - 254,
BUT the keyword is "LEARNED"
a STATIC route isn't "learned" so that leaves us with the closet network route that was learned dynamically....hence 172.16.0.128/25 (172.16.0.129 - 254 hosts) OSPF

upvoted 2 times

Question #420 *Topic 1*

A user configured OSPF in a single area between two routers. A serial interface connecting R1 and R2 is running encapsulation PPP. By default, which OSPF network type is seen on this interface when the user types show ip ospf interface on R1 or R2?

A. nonbroadcast

B. point-to-point

C. point-to-multipoint

D. broadcast

Correct Answer: *B*

ayd33n Highly Voted 3 years, 1 month ago

Broadcast default for Ethernet, Point to Point default for serial

upvoted 38 times

IxlJustinlxl Highly Voted 2 years, 4 months ago

PPP = Point-to-Point Protocol.
Kinda sums it up right there.

upvoted 14 times

nicombe Most Recent 11 months, 3 weeks ago

Selected Answer: B

No one praising 420, im disappointed

upvoted 8 times

Cyberops 1 year, 4 months ago

serial= Point to Point

upvoted 1 times

Retxed 2 years, 7 months ago

The default OSPF network type for HDLC and PPP on Serial link is point-to-point (while the default OSPF network type for Ethernet link is Broadcast).

upvoted 9 times

Question #421 *Topic 1*

Which MAC address is recognized as a VRRP virtual address?

A. 0000.5E00.010a

B. 0005.3709.8968

C. 0000.0C07.AC99

D. 0007.C070.AB01

Correct Answer: *A*

Kaygol Highly Voted 3 years, 2 months ago

Answer A - 1 VRRP over Ethernet. Over Ethernet, VRRP routers use a common MAC address of the format 00:00:5E: 00:01:XX. The first three octets are derived from the IANA's OUI. The next two octets (00:01) indicate the address block assigned to the VRRP protocol by IANA

upvoted 36 times

ismatdmour Highly Voted 1 year, 5 months ago

Selected Answer: A

0000.5E00.01xx is VRRP virtual MAC (Ans. A with xx=0A group)
0000.0c07.acxx is HSRP virtual MAC address (Ans. C with xx=99)
0007.b400.xxyy is GLBP virtual MAC (Not in the answers), xx is group and yy is AVF
I don't know what B and D are.

upvoted 16 times

BraveBadger Most Recent 1 year, 4 months ago

Any easy way to remember 0C07AC as HSRP and 5E0001 as VRRP? I confuse the two.

upvoted 3 times

paolo_brosio 2 years, 4 months ago

E' la B ma vuole la A nse sa

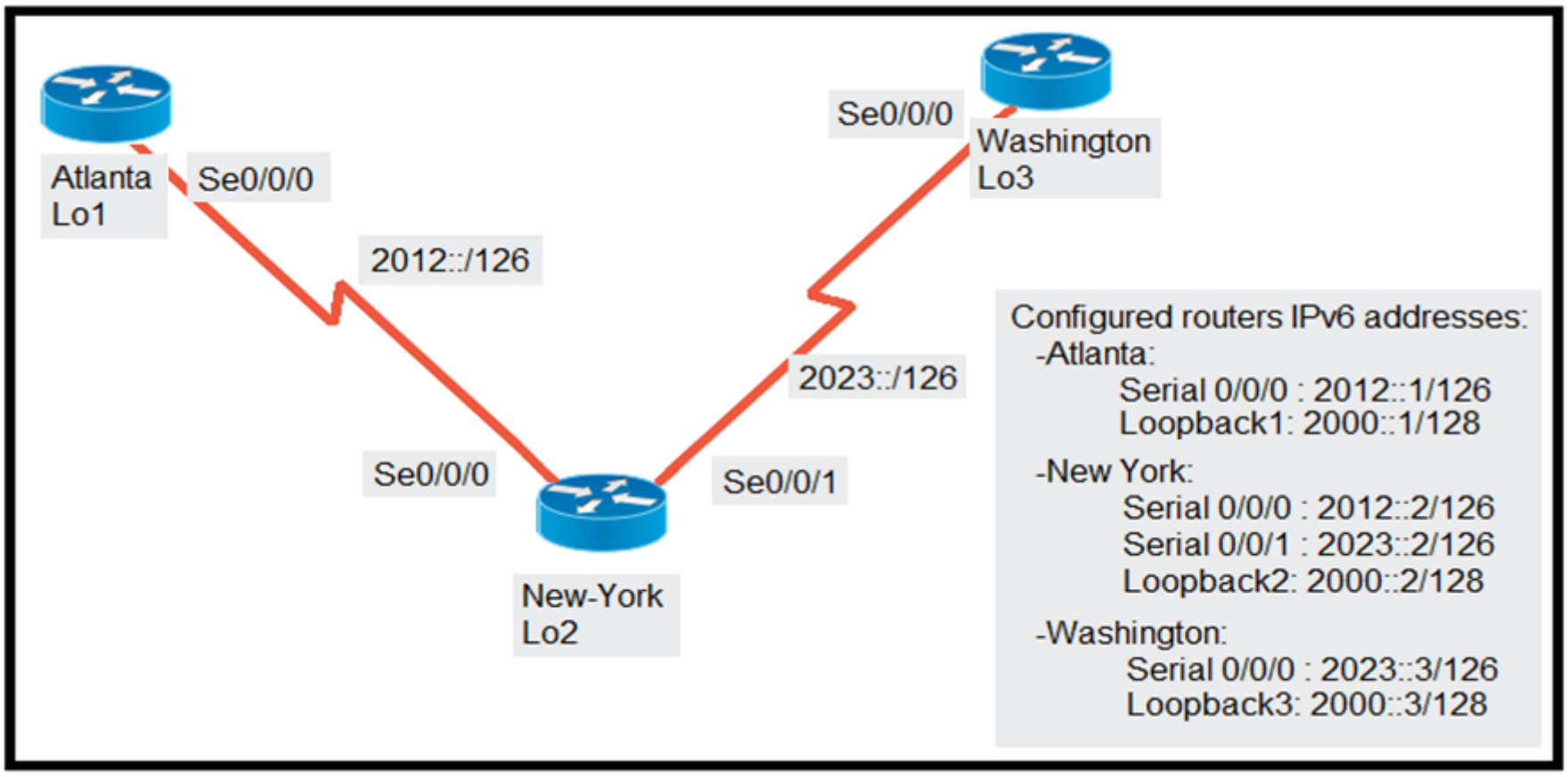
upvoted 8 times

alexiro 3 years, 1 month ago

Virtual MAC address : A virtual MAC address is automatically generated by taking the last 8 bytes as the VRRP group number in hexadecimal. In VRRP, Mac address used is 0000.5e00.01xx. Here, xx is the VRRP group number in hexadecimal.
https://www.geeksforgeeks.org/introduction-of-virtual-router-redundancy-protocol-vrrp-and-its-configuration/

upvoted 6 times

Question #422 *Topic 1*



Refer to the exhibit. The New York router is configured with static routes pointing to the Atlanta and Washington sites.
Which two tasks must be performed so that the Se0/0/0 interfaces on the Atlanta and Washington routers reach one another? (Choose two.)

A. Configure the ipv6 route 2023::/126 2012::1 command on the Atlanta router.

B. Configure the ipv6 route 2012::/126 2023::2 command on the Washington router.

C. Configure the ipv6 route 2012::/126 2023::1 command on the Washington router.

D. Configure the ipv6 route 2023::/126 2012::2 command on the Atlanta router.

E. Configure the ipv6 route 2012::/126 s0/0/0 command on the Atlanta router.

Correct Answer: *BD*

shumps 3 weeks, 2 days ago
I was vex a bit, pay close attention to the New York router ipv6 address as next hop. B & D is correct
upvoted 1 times

_mva 1 month, 3 weeks ago
Easy enough but I hate these.
upvoted 1 times

Aie_7 6 months, 2 weeks ago
Answers given are correct
upvoted 3 times

iMo7ed 6 months, 3 weeks ago
Selected Answer: BD
B and D are correct
upvoted 4 times

Question #423 *Topic 1*

A router running EIGRP has learned the same route from two different paths. Which parameter does the router use to select the best path?

A. as-path

B. administrative distance

C. metric

D. cost

Correct Answer: *D*
If a router learns two different paths for the same network from the same routing protocol, it has to decide which route is better and will be placed in the routing table. Metric is the measure used to decide which route is better (lower number is better). Each routing protocol uses its own metric.
For example, RIP uses hop counts as a metric, while OSPF uses cost.
Reference:
https://study-ccna.com/administrative-distance-metric/

Mcsonic00 Highly Voted 2 years, 10 months ago
1 routing protocol for 2 learned paths = Metric
1 learned path from 2 routing protocols = Administrative Distance
upvoted 48 times

AndrealTALIANO91 2 years, 1 month ago
are you sure about your second statement?
In many questions, when there are two routing protocols and a path, we look at the prefix length, not the AD.
For example on the page preceding question 227 in the answers an OSPF route is preferred over a static route.
upvoted 3 times

Mozah 1 year, 8 months ago
ARE WE ON THE SAME PAGE??

Question #227Topic 1
Which value is used to determine the active router in an HSRP default configuration?
upvoted 1 times

Anas_Ahmad 10 months, 4 weeks ago
The default priority is 100
upvoted 1 times

TheLorenz 1 year, 6 months ago
Prefix is dominant when the routes are already installed on the routing table (already learned). When a router is choosing which to install on the routing table, it looks at AD. When choosing multiple paths from one protocol, metric.
upvoted 1 times

TheLorenz 1 year, 6 months ago
forgot to mention the last statement I made is still when the router is trying to choose what path to install. Only look at prefix when the routes are already installed in the table.
upvoted 2 times

Vikramaditya_J Highly Voted 4 months, 3 weeks ago
Selected Answer: C
A tricky question. Let me try to explain:
According to the question, the destination is same i.e. same route, but it's learned using two different paths. Normally, router uses administrative distance as a parameter to select the best path when multiple routing protocols are used, but since both paths are running with EIGRP, so both have the same AD (=90) so it's a tie. Next the router will consider the metric value for path selection. So, C should be the correct option here.
upvoted 12 times

BJ221 Most Recent 1 month ago
Selected Answer: C
RIP - hop (both 3 letters)
OSPF - cost (both 4 letters)
EIGRP - metric (one 5 other 6... but you got the point)
upvoted 3 times

Da_Costa 3 months, 2 weeks ago
It will use metric

upvoted 1 times

omikun 4 months, 3 weeks ago

When a router running EIGRP learns the same route from multiple paths, it selects the best path based on the metric, not the administrative distance or as-path. Therefore, the correct answer is C. metric.

The EIGRP metric is calculated based on several parameters such as bandwidth, delay, reliability, and load. The router calculates the metric for each path it learns and selects the one with the lowest metric as the best path. The metric can be influenced by adjusting the weights of the individual parameters using the K values.

upvoted 2 times

DUMPledore 7 months, 3 weeks ago

Selected Answer: C

Metric EIGRP
Cost OSPF
Hop count RIP

upvoted 9 times

Sdiego 7 months, 4 weeks ago

Selected Answer: C

Metric for EIGRP

upvoted 2 times

Dhruv3390 8 months ago

Guys please dont get confused here in question we are asked Router is only running EIGRP and have multiple path to same destination, If we have multiple protocols we use Longest Prefix to get the most specific route, if multiple routs are there with multiple protocols then we use AD values to decide best route.

When it comes to only 1 protocol is running, we can't use AD, we use Metric. For every protocol we have different Metric.

1)Metric for EIGRP is Metric itself, which has been derived by using delay and bandwidth.
2)Metric for OSPF is Cost, which has been derived by using refrence bandwidth and speed of interface.
3)Metric for RIP is Hop counts.

upvoted 7 times

Surves 9 months, 2 weeks ago

Selected Answer: C

Metric EIGRP
Cost OSPF
Hop count RIP

upvoted 3 times

Netcmd 10 months ago

Selected Answer: C

Metric is used EIGRP. OSPF uses cost

upvoted 2 times

Garfieldcat 11 months ago

The question is telling us the router is running EIGRP, not OSPF. .... a generic term Metric is acceptable answer.

upvoted 1 times

Murphy2022 11 months, 2 weeks ago

Selected Answer: C

OSPF uses Combined Cost as its Metric
EIGRP uses Metric as its Metric

upvoted 1 times

creaguy 11 months, 2 weeks ago

it's right there in the explanation given. Duh !

"Metric is the measure used to decide which route is better "

upvoted 1 times

[Removed] 11 months, 3 weeks ago

I'm confused how the suggested answer is D but the explanation suggests C.

upvoted 3 times

splashy 12 months ago

Selected Answer: C

It's an Enhanced distance vector protocol so metric

https://www.ccexpert.us/subnetted-subnets/eigrp-metrics.html#:~:text=Like%20IGRP%2C%20EIGRP%20chooses%20a%20route%20based%20primarily,feasible%20distance%20to%20all%20routes%20in%20the%20network.

upvoted 1 times

Eyad_Alotaibi 1 year ago

Correct answer is C.
If a router learns two different paths for the same network from the same routing protocol, it has to decide which route is better and will be placed in the routing table. Metric is the measure used to decide which route is better (lower number is better). Each routing protocol uses its own metric. For example, RIP uses hop counts as a metric, while OSPF uses cost.

upvoted 1 times

Bl1024 1 year ago

Selected Answer: C

Answer should be c>metric not b>cost

upvoted 1 times

Question #424 *Topic 1*

An engineer configured an OSPF neighbor as a designated router. Which state verifies the designated router is in the proper mode?

A. Init

B. 2-way

C. Exchange

D. Full

Correct Answer: *D*

Demi_UY_Scuti Highly Voted 2 years, 10 months ago

D is the correct answer. A DR or a BDR router will always need to reach a full state relationship with all neighbours (DROther included!) for correct operation. A 2-way state will only be considered correct and stable between two DROther routers.

upvoted 10 times

RebWat93 Highly Voted 2 years, 9 months ago

Ans: D = Full is the state for adjacent routers that have fully synchronised databases.

upvoted 10 times

Yinxs Most Recent 3 weeks, 5 days ago

Selected Answer: D

Full state is only in adj neighbor to DR or BDR.

upvoted 1 times

divn_01 1 month, 1 week ago

Selected Answer: D

Answer is D - Full
"In this state, routers are fully adjacent with each other. All the router and network LSAs are exchanged and the routers' databases are fully synchronized."

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html#:~:text=packets%20are%20acknowledged.-,Full,state%20for%20an%20OSPF%20router.

https://itexamanswers.net/question/an-engineer-configured-an-ospf-neighbor-as-a-designated-router-which-state-verifies-the-designated-router-is-in-the-proper-mode

upvoted 1 times

dropspablo 1 month, 2 weeks ago

Selected Answer: D

The exercise asks for the adjacency status of the DR (designated router) working properly, correct answer is D. Full.
"A designated router (DR), assumes the role of pseudonode (virtual router) to reduce adjacencies avoiding overload, it obtains a FULL status with all neighbors, with BDR (FULL/BDR) and DROTHER (FULL/DROTHER). BDR receives backup information, so BDR also gets FULL status with all neighbors (FULL/DR) (FULL/DROTHER). DROTHER gets FULL status with DR (FULL/DR) and BDR (FULL/BDR) , but only with other DROTHERs (DROTHER with DROTHER) we have 2-way adjacency status (2WAY/DROTHER)."

upvoted 1 times

dropspablo 1 month, 2 weeks ago

The "2-way" state is reached when a router detects its OSPF neighbor on the network. This happens after the establishment of the "2-way" adjacency, the routers can exchange OSPF information, but still do not have complete information from the neighbor's link-state database.

upvoted 1 times

4aynick 4 months, 3 weeks ago

Selected Answer: B

drother always in 2-way state, here speach go up about DR-other routers , no dr or bdr

upvoted 2 times

ShravaniKulkarni 1 year, 3 months ago

DR and BDR gets selected in 2-way...

upvoted 1 times

Raman1996 1 year, 7 months ago

https://www.computernetworkingnotes.com/ccna-study-guide/ospf-neighbor-states-explained-with-example.html#:~:text=OSPF%20routers%20go%20through%20the,with%20other%20OSPF%20speaking%20routers.

upvoted 2 times

Raman1996 1 year, 7 months ago

Down state
Attempt/Init state
Two ways state
Exstart state
Exchange state
Loading state
Full state

remember it as DATEELF
upvoted 5 times

LTTAM 2 years, 8 months ago
D: Full is the correct answer. Source straight from Cisco below:

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html
upvoted 7 times

Dileesh 2 years, 11 months ago
Answer B
upvoted 2 times

Dileesh 2 years, 11 months ago
sorry "Full is the normal state for an OSPF router"
In this state, routers are fully adjacent with each other. All the router and network LSAs are exchanged and the routers' databases are fully synchronized.
upvoted 4 times

SALSHOUMER 2 years, 11 months ago
Correct Answer: B
upvoted 2 times

ayd33n 3 years, 1 month ago
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html
upvoted 3 times

Question #425 *Topic 1*

```
R1# show ip route

D    192.168.16.0/26 [90/2679326] via 192.168.1.1
R    192.168.16.0/24 [120/3] via 192.168.1.2
O    192.168.16.0/21 [110/2] via 192.168.1.3
i L1 192.168.16.0/27 [115/30] via 192.168.1.4
```

Refer to the exhibit. Which route does R1 select for traffic that is destined to 192.168.16.2?

A. 192.168.16.0/21

B. 192.168.16.0/24

C. 192.168.16.0/26

D. 192.168.16.0/27

Correct Answer: *D*

The destination IP addresses match all four entries in the routing table but the 192.168.16.0/27 has the longest prefix so it will be chosen. This is called the
ג€longest prefix matchג€ rule.

Chocobo Highly Voted 2 years, 6 months ago

D is correct.
Longest prefix is prioritized over lower AD.

upvoted 12 times

Yunus_Empire 9 months, 2 weeks ago

Yes.. right

upvoted 1 times

ac89l Most Recent 4 months, 2 weeks ago

what is i L1 ?

upvoted 2 times

kyleptt 1 month ago

I am thinking a loopback port

upvoted 1 times

[Removed] 4 months ago

IS-IS (AD 115)

upvoted 1 times

Question #426 *Topic 1*

```
Gateway of last resort is 10.12.0.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.12.0.1, 00:00:01, GigabitEthernet0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.0/24 is directly connected, GigabitEthernet0/0
L    10.0.0.2/32 is directly connected, GigabitEthernet0/0
C    10.13.0.0/24 is directly connected, GigabitEthernet0/1
L    10.13.0.2/32 is directly connected, GigabitEthernet0/1
```

Refer to the exhibit. If configuring a static default route on the router with the ip route 0.0.0.0 0.0.0.0 10.13.0.1 120 command, how does the router respond?

A. It starts sending traffic without a specific matching entry in the routing table to GigabitEthernet0/1.

B. It immediately replaces the existing OSPF route in the routing table with the newly configured static route.

C. It starts load-balancing traffic between the two default routes.

D. It ignores the new static route until the existing OSPF default route is removed.

Correct Answer: *D*

Our new static default route has the Administrative Distance (AD) of 120, which is bigger than the AD of OSPF External route (O*E2) so it will not be pushed into the routing table until the current OSPF External route is removed.
For your information, if you don't type the AD of 120 (using the command ג€ip route 0.0.0.0 0.0.0.0 10.13.0.1ג€) then the new static default route would replace the
OSPF default route as the default AD of static route is 1. You will see such line in the routing table:
S* 0.0.0.0/0 [1/0] via 10.13.0.1

sinear Highly Voted 2 years, 8 months ago
You really got to see the "120" here to not miss the right answer...
upvoted 12 times

mhayek 10 months, 3 weeks ago
and this is exactly what i missed
upvoted 6 times

cormorant Most Recent 10 months, 2 weeks ago
specifying te administrative distance of 120 means it's a route that will only be used when teh OSPF route is removed, since it has an administrative distance of 110 and therefore should take precedence
upvoted 1 times

i_am_confused 1 year, 3 months ago
Selected Answer: D
Floating static route with AD 120 is a backup to OSPF route. Won't be used until OSPF route goes down.
upvoted 4 times

kaifene 1 year, 4 months ago
Selected Answer: D
Because Static route as default has 1 AD but it was manually configured to 120 which is greater than 110. So, it won't be considered until former OSPF route is not removed.
upvoted 1 times

Elstak_Dennis 1 year, 6 months ago
Selected Answer: B
The best approach to answer this vague question is to eliminate the answers which are definitely wrong and these wrong answers are: A, C, E, F which leaves out B and D as the only possible anwers. Since D is a no brainer we have to focus on why B could be right. R1 which is the DR indeed won't establish an adjacency with R3. Adjacency means the that the 2 routers would be in Full state which is the state they will not reach. They will only be able to reach the 2-way state. The routers will be able to have a neighbor relationship but will not form a neighbor adjacency.
upvoted 1 times

Jonfernz 2 years, 5 months ago
the 120 AD makes it a floating static route --- which is added for redundancy in case the OSPF fails.
upvoted 4 times

Taku2023 5 months, 2 weeks ago

I think someone needs to explain to me again about floating static. OSPF already has AD of 120. if you configure a floating static isn't supposed to be 121???????????

upvoted 1 times

studying_1 4 months, 1 week ago

OSPF AD 110

upvoted 1 times

Nhan 2 years, 6 months ago

This is also the method that people setting floating route with ad higher than the default route

upvoted 4 times

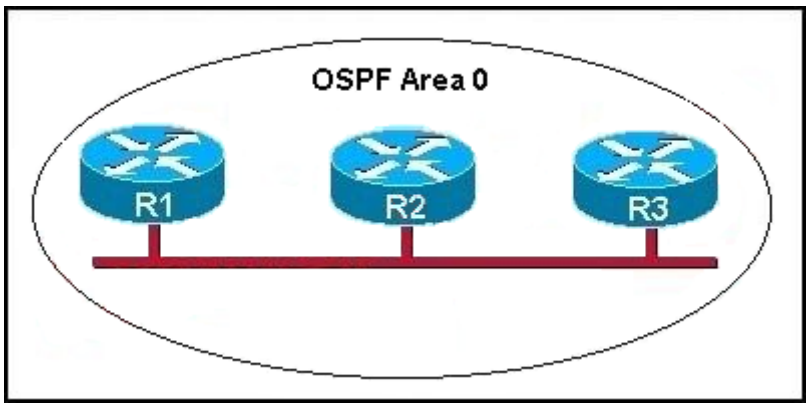
uevenasdf 2 years, 8 months ago

Tricky one can't miss the manually adding the 120 AD....

upvoted 4 times

Question #427 *Topic 1*

Refer to the graphic. R1 is unable to establish an OSPF neighbor relationship with R3. What are possible reasons for this problem? (Choose two.)



A. All of the routers need to be configured for backbone Area 1.

B. R1 and R2 are the DR and BDR, so OSPF will not establish neighbor adjacency with R3.

C. A static route has been configured from R1 to R3 and prevents the neighbor adjacency from being established.

D. The hello and dead interval timers are not set to the same values on R1 and R3.

E. EIGRP is also configured on these routers with a lower administrative distance.

F. R1 and R3 are configured in different areas.

Correct Answer: *DF*

This question is to examine the conditions for OSPF to create neighborhood. So as to make the two routers become neighbors, each router must be matched with the following items:

1. The area ID and its types
2. Hello and failure time interval timer
3. OSPF Password (Optional)

xdxp23 Highly Voted 2 years, 1 month ago

I like D and E for this. How is F possible if you can clearly see them in the same area according to the graphic? Thoughts anyone?

upvoted 19 times

DaBest 1 year, 11 months ago

i agree this should be D and E, unless they want us to answer this question baised on theory alone then yeah D and F are the answers. they must have answered that without looking at the graphic

upvoted 3 times

daddydagoth 6 months, 3 weeks ago

It can never be E as an answer. Having EIGRP configured with a lower AD (by default the AD is lower already so that's a hint that this is wrong), the only thing that happens is that The router runs both protocols and will prefer EIGRP's routes to the same destination over the OSPF routes. This will not, in any way, distrupt the OSPF adjecencies.

upvoted 5 times

Dante_Dan 1 year, 8 months ago

EIGRP will not prevent OSPF to form an adjacency with other routers. So answer E could not be correct.

upvoted 5 times

mohamed1999 2 years ago

what they mean with area is like group. so if you are now in the same group you can't see each other.

upvoted 3 times

nickname_fordiscussions Highly Voted 1 year, 5 months ago

Umm.. They're all clearly in Area 0. There's a huge circle that says Area 0. All of the routers are in the same area..

upvoted 9 times

BraveBadger 1 year, 4 months ago

Yup, but the question basically says "it's not working, what could cause it to not work" I always try to keep in mind that the graphic is solely giving a topology and not necessarily the config. So many tricks they play.

upvoted 8 times

shaney67 Most Recent 3 weeks, 2 days ago

strange question, as the graphic shows all routers are in the same area?

upvoted 2 times

shumps 3 weeks, 2 days ago

D & E. Whats the reason of the exhibit then when we can clearly see area 0 in place
upvoted 1 times

dropspablo 3 months, 3 weeks ago

Selected Answer: DF

Correct the answer. EIGRP does not prevent them from forming neighborhood adjacencies, it can only interfere with the routing table. A configuration of areas different from the proposed in the graph would prevent adjacencies.
upvoted 2 times

shiv3003 4 months, 3 weeks ago

B and D
upvoted 1 times

Rether16 5 months, 1 week ago

This comment is pure shite! Theyre clearly in the same area as theyre circled as Area 0!
upvoted 2 times

Aie_7 6 months, 2 weeks ago

Tricky question. Topology shows AREA 0
upvoted 2 times

Dutch012 7 months ago

how D & F are correct?
R3 is able to form a neighbor relationship with R2, the same thing with R1 is able to form a neighbor relationship with R2, if D & F were correct these two relations mentioned above should not be created.
upvoted 1 times

Goena 8 months, 2 weeks ago

Selected Answer: DE

I think D and E.
They're all clearly in Area 0.
Cisco doesn't mention anything about EIGRP. There is a possibility that is configured.
upvoted 2 times

Customexit 11 months ago

I can see it as, yeah it says area 0 in the picture, but perhaps F is saying it's "configured" in different areas.
upvoted 1 times

Nnandes 1 year, 4 months ago

D & F are correct.
upvoted 2 times

Aleks123 1 year, 8 months ago

The graphic is such a bait here to make the wrong mistake like the default vlan question where its 1. Noticing a trend here lol?
upvoted 1 times

sgashashf 1 year, 6 months ago

Yeah. Cisco's tests are honestly super scummy.
upvoted 8 times

Question #428 *Topic 1*

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route

Gateway of last resort is 209.165.202.131 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.202.131
      209.165.200.0/27 is subnetted, 1 subnets
S        209.165.200.224 [254/0] via 209.165.202.129
      209.165.201.0/27 is subnetted, 1 subnets
S        209.165.201.0 [1/0] via 209.165.202.130
```

Refer to the exhibit. Which command configures a floating static route to provide a backup to the primary link?

A. ip route 209.165.200.224 255.255.255.224 209.165.202.129 254

B. ip route 209.165.201.0 255.255.255.224 209.165.202.130

C. ip route 0.0.0.0 0.0.0.0 209.165.200.224

D. ip route 0.0.0.0 0.0.0.0 209.165.202.131

Correct Answer: *A*

maw619 Highly Voted 2 years ago

A is the only answer that is a static floating route.

upvoted 14 times

gaber 1 year, 8 months ago

yes, the only one with the higher AD specified

upvoted 1 times

Pkard 1 year, 11 months ago

my eyes are tired and i missed that.

upvoted 10 times

bwg Highly Voted 2 years, 3 months ago

Did no one find that the AD of primary link is also 254 ?

upvoted 6 times

Darwyn 2 years, 2 months ago

there is only one answer that has an AD that is specified in the syntax

upvoted 5 times

BooleanPizza 2 years ago

254 is the AD of the backup link aka the floating static route

upvoted 3 times

Sonieta 1 year, 11 months ago

now, I understand, thank you!!

upvoted 1 times

Dzhenkov Most Recent 4 months, 1 week ago

Selected Answer: A

highest AD

upvoted 1 times

Mafix 1 year, 2 months ago

The administrative distance is the same on both the primary link as well as the supposedly floating static route! 254 ! Should have been greater than 254 so it can be chosen as a backup, I believe !

upvoted 3 times

Nnandes 1 year, 4 months ago

A is the correct answer.

upvoted 1 times

ismatdmour 1 year, 5 months ago

Selected Answer: A

A is correct. You will only see one of 2 routes in the the table cause the floating route will be only in the table when the primary route fails and comes as alternate. The route with 254 AD should be the floating route, and the primary route has problems (not in table). I agree with yasuke, the question should have stated " which command configured the floating static route...."

upvoted 3 times

yasuke 1 year, 11 months ago

i think the question should have read " which command configured the floating static route...."

upvoted 5 times

sdokmak 2 years, 2 months ago

Literally spent hours on this one.
All the commands are already on the screen, we need to know which one is the backup and which one is the primary.

The default route is the default route so ignore that.
Leaves us with two routes, one with the lower administrative distance is the primary link:
209.165.201.0 [1/0] via 209.165.202.130
The remaining higher administrative distance is the backup link
209.165.200.224 [254/0] via 209.165.202.129

..honestly not sure.

The primary link is

upvoted 5 times

ismatdmour 1 year, 5 months ago

You will only see one of 2 routes in the the table cause the floating route will be only in the table when the primary route fails and comes as alternate.

upvoted 1 times

Micah7 2 years, 3 months ago

This was an odd question for several reasons:
- The "primary link".....at first I thought it was referring to the default route (gateway of last resort)
- Interesting to note: if there is only 1 route in the subnetted network.....no mask is displayed for the line of the subnetwork....so you have to assume the mask on the line above
- Yes, to agree with bwg: the AD is the same for the answer and the diagram's network.....I would think it needs to be a higher number. Otherwise, other factors being equal (AD).....you are just inserting what the system already has

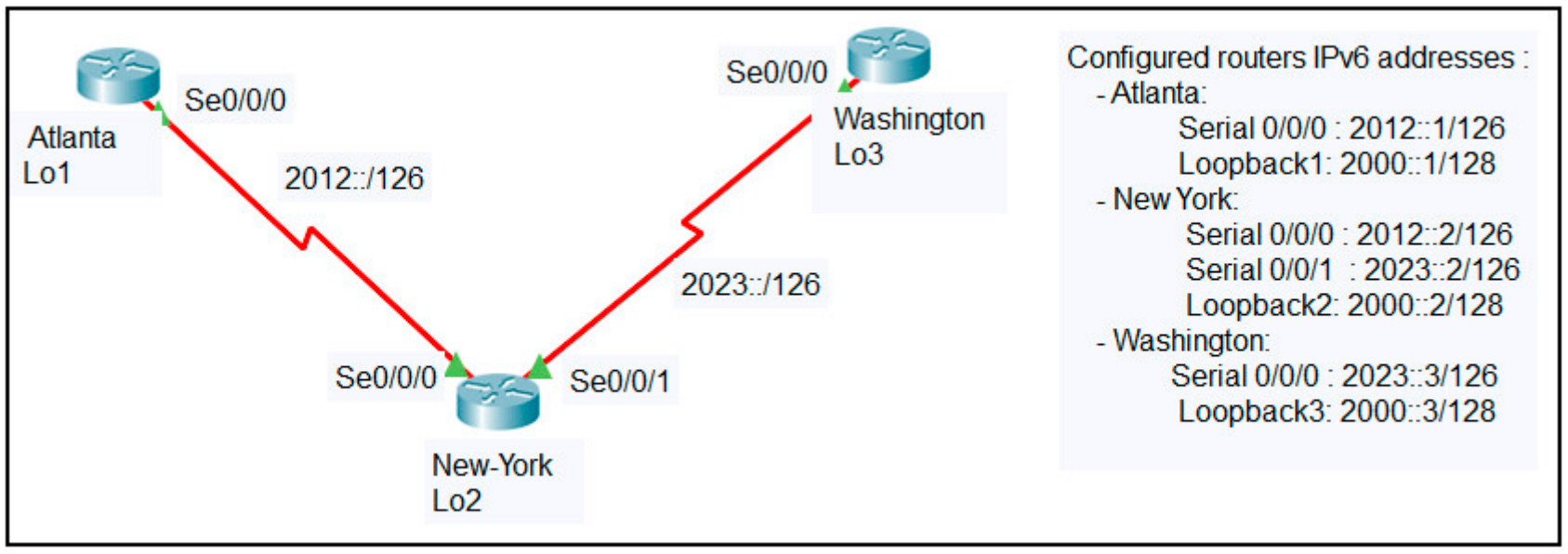
upvoted 3 times

Sten111 2 years, 2 months ago

Yeah this question is messed up. If the AD value was missing from the end of the A command that would do it because the current route in the routing table would be the floating static. If there is a correct answer here I can't see it.

upvoted 1 times

Question #429 *Topic 1*



Refer to the exhibit. An engineer configured the New York router with static routes that point to the Atlanta and Washington sites. Which command must be configured on the Atlanta and Washington routers so that both sites are able to reach the loopback2 interface on the New York router?

A. ipv6 route::/0 Serial 0/0/0

B. ipv6 route::/0 Serial 0/0/1

C. ipv6 route:0/0 Serial 0/0/0

D. ip route 0.0.0.0 0.0.0.0 Serial 0/0/0

E. ipv6 route::/0 2000::2

Correct Answer: *A*

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/xe-3s/iri-xe-3s-book/ip6-route-static-xe.html#GUID-85796C3A-3143-4DF7-B9D0-8EC87D0DB08B

kokoyul Highly Voted 1 year, 11 months ago

The static routes are:
Network + Interface (Source interface) or Next Hop (IP Address Neighbor).
So, you have 4 possibilities:
Atlanta = ipv6 route::/0 2012::2/126
or
Atlanta = ipv6 route::/0 Serial 0/0/0
_____
Washington= ipv6 route::/0 2023::2/126
or
Washington= ipv6 route::/0 Serial 0/0/0

upvoted 15 times

Pkard 1 year, 9 months ago

Agree. When you use a interface as the next hop, it is the interface of the sending router.

upvoted 3 times

redivivo 1 year, 3 months ago

when you use an interface as the next hop, it's the interface of the next router, not the sending one. As kokoyul stated :
Network (destination) + Exit interface (of the sending router)
OR
Network (destination) + Next hop (ip address of ingress interface of the neighbor router, the next one .

upvoted 2 times

Amr_001 Most Recent 1 week, 1 day ago

I believe E is the correct answer because if you set outgoing int in the ipv6 route, you need to mention the next-hop link-local address

upvoted 1 times

[Removed] 11 months, 3 weeks ago

Are you guys sure its not A (for the Atlanta route) and B (for the Washington route)?
Because i thought the next hop for Atlanta would be Serial 0/0/0 and the next hop for Washington would be Serial 0/0/1.
I may be wrong tho.

upvoted 2 times

A7med97 10 months, 3 weeks ago

s0/0/0, its exit interface for both Atlanta and Washington

upvoted 2 times

whojabagooya 1 year, 2 months ago

A is the correct answer.
The answer to this question is in the illustration of question # 209. The answer is the static default route of both routers.

upvoted 1 times

aike92 1 year, 7 months ago

IMO i would imagine the actual question stating "(Choose two)" at the end to close out the question leaving the answers to be A &' B..
But if the question is given as-is &' i could only choose One answer, E is the only choice that can apply to BOTH Atlanta &' Washington Routers.

upvoted 3 times

MEDO95 8 months ago

totally same as u. Cisco play us hard

upvoted 1 times

Shamwedge 1 year, 7 months ago

This was my logic and why I chose E

upvoted 5 times

reagan_donald 1 year, 7 months ago

First router must know how to reach the loopback interface....1 option is to use next-hop, 2nd option is to use his egress interface (exit interface)

A is correct

upvoted 4 times

Mozah 1 year, 9 months ago

ipv6 route ::/0 out interface OR ipv6 route ::/0 next hop IP address
In this case the out int for Atlanta and Washington to New york is s0/0/0 means A its correct

upvoted 2 times

ProgSnob 1 year, 9 months ago

I believe it's A. There's no ip route command that calls out the Loopback 2 address directly so we need to use ip route ::/0. The exit interface for each of the routers is Serial 0/0/0.

upvoted 2 times

Hodicek 1 year, 10 months ago

I Would say A and B , as we can't use the same command for both 2 routers

upvoted 4 times

dave1992 1 year, 11 months ago

E should be the correct answer.
a default static route of ::/0 to reach 2000::2 which is the loopback of the NY router.

trying to make sense of the answer givin is wrong. A is not the correct answer.
otherwise B would also be the correct answer.

upvoted 4 times

Nicocisco 1 year, 6 months ago

How Atlanta & Washinton know where is 2002::2?
Just New-york has been was configured

upvoted 3 times

CozTurk 1 year, 11 months ago

I am confused with how the answer is A here - Are we sure this is not a typo or a question requiring 2 answers? Can someone please elaborate?

The question is asking to enter the static routes from the perspective of the ATLANTA and WASHINTON routers hence making the next hop interfaces S0/0/1 for Washington and S0/0/0 for Atlanta. Shouldn't this mean A and B are correct?

upvoted 1 times

reagan_donald 1 year, 7 months ago

both of them is using same command, because both of them same egress interfaces, Default route is as well static route.

upvoted 1 times

Asymptote 2 years, 1 month ago

it point the ::/0 using both Alanta and Washington serial interface S0/0/0 ,

so both of them using the same command .

upvoted 4 times

Dibilili 2 years, 1 month ago

If A is correct, why B isn`t?

upvoted 3 times

CiscoTerminator 2 years, 1 month ago

S0/0/1 is not the exit interface facing New York on both routers hence its wrong.

upvoted 1 times

bwg 2 years, 3 months ago

Why E is wrong?

upvoted 3 times

CiscoTerminator 2 years, 1 month ago

E is wrong becoz its not the correct next hop IP for both routers. Qstn requires one command that works for both routers.

upvoted 1 times

Question #430 *Topic 1*

What is the effect when loopback interfaces and the configured router ID are absent during the OSPF Process configuration?

A. The lowest IP address is incremented by 1 and selected as the router ID.

B. The router ID 0.0.0.0 is selected and placed in the OSPF process.

C. No router ID is set, and the OSPF protocol does not run.

D. The highest up/up physical interface IP address is selected as the router ID.

Correct Answer: *D*

ccna_goat 11 months ago

actually correct answer is poorly worded. interface could be in state UP/DOWN and still be eligible for being router ID.

upvoted 1 times

Nnandes 1 year, 4 months ago

D: is the correct one "The highest up/up physical interface IP address is selected as the router ID."

upvoted 3 times

Question #431 *Topic 1*

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 192.168.30.10 to network 0.0.0.0
     192.168.30.0/29 is subnetted, 2 subnets
C       192.168.30.0 is directly connected, FastEthernet0/0
C       192.168.30.8 is directly connected, Serial0/0.1
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
O IA    192.168.10.32/28 [110/193] via 192.168.30.10, 00:18:49, Serial0/0.1
O IA    192.168.10.0/27 [110/192] via 192.168.30.10, 00:18:49, Serial0/0.1
     192.168.20.0/30 is subnetted, 1 subnets
O IA    192.168.20.0 [110/128] via 192.168.30.10, 00:18:49, Serial0/0.1
     192.168.50.0/32 is subnetted, 1 subnets
C       192.168.50.1 is directly connected, Loopback0
O*IA 0.0.0.0/0 [110/84] via 192.168.30.10, 00:10:36, Serial0/0.1
```

Refer to the exhibit. What is the metric of the route to the 192.168.10.33/28 subnet?

A. 84

B. 110

C. 128

D. 192

E. 193

Correct Answer: *E*

virab4 Highly Voted 4 months, 4 weeks ago

Selected Answer: E

remember my friend,be very very carefull on exam day

upvoted 11 times

creaguy Highly Voted 11 months, 3 weeks ago

192.168.10.33/28 subnet?
Is this another way they try to trick you ? or is this an actual typo ?
192.168.10.33 Is a host IP and not a subnet ID.

upvoted 6 times

kyleptt 2 months, 2 weeks ago

It should be host .33 but I think that was implied ?? not sure

upvoted 1 times

kyleptt Most Recent 2 months, 2 weeks ago

If I didn't read that correctly I would have lost some easy marks lol

upvoted 1 times

no_blink404 3 months ago

This is a good example of why we need to carefully read the question! METRIC not AD
Answer is E

upvoted 2 times

JimmiCook 1 year, 1 month ago

Why the metric is 193 ? not 110 as ospf default cost ?

upvoted 1 times

BieLey 11 months, 3 weeks ago

110 = Administrative Distance
193 = The Metric

upvoted 9 times

Nnandes 1 year, 4 months ago

The question is "What is the metric of the route to the 192.168.10.33/28 " so this belongs to network 10.32/28 and the metric of this network 193

upvoted 3 times

seecos 1 year, 4 months ago

tricky ... just cal 192.168.10.32/28 subnet and 192.168.10.33 is the host .
upvoted 2 times

Pkard 1 year, 11 months ago
Someone is going to have to explain this to me...192.168.10.33 is the first available host in the 192.168.10.32/28 network..
So there is no route in the table and it should use the gateway of last resort, right?
upvoted 1 times

Stonetales987 1 year, 10 months ago
What route would you use to send traffic to the 192.168.10.33/28 subnet. 192.168.10.33 is part of the 192.168.10.32/28 subnet and would use that OSPF route. These IPs would also use that same route (.33 - .47)/ (AD/METRIC) (110/193).
upvoted 7 times

shakyak 1 year, 10 months ago
What do you mean by gateway of last resort?
upvoted 1 times

Pkard 1 year, 10 months ago
having looked at this question again, what i meant was the O* route at the bottom. It's just a shitty question because they called it the 192.168.10.33/28 subnet not host
upvoted 4 times

gaber 1 year, 8 months ago
Agreed.
upvoted 1 times

Keif 1 year, 11 months ago
I guess the way you could look at the question is the /28 subnet that .33 belongs to. which is .32 network ID
upvoted 4 times

Question #432 *Topic 1*

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2 * - candidate
 default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C  192.168.3.5 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O       10.0.1.3/32 [110/100] via 192.168.0.40, 00:39:08, Serial0
C       10.0.1.0/24 is directly connected, Serial0
O       10.0.1.190/32 [110/5] via 192.168.0.35, 00:39:08, Serial0
O       10.0.1.0/24 [110/10] via 192.168.0.4, 00:39:08, Gigabit Ethernet 0/0
D       10.0.1.0/28 [90/10]  via 192.168.0.7, 00:39:08, Gigabit Ethernet 0/0
```

Refer to the exhibit. Traffic sourced from the loopback0 interface is trying to connect via ssh to the host at 10.0.1.15. What is the next hop to the destination address?

A. 192.168.0.7

B. 192.168.0.4

C. 192.168.0.40

D. 192.168.3.5

Correct Answer: *A*

The router will choose the route will the longest matching prefix, in this case that is 10.0.1.0.28.

dicksonpwc Highly Voted 2 years ago

Answer A is incorrect. If select 10.0.1.0/28 and subnet mask is 255.255.255.240. Then, host address range will be 10.10.1.1 to 10.10.1.14. Therefore, it coorrect answer should be B.

upvoted 52 times

cortib 1 year, 12 months ago

Agree, but this is really fucked up question, in real scenario this configuration will cause a lot of problem, should we assume that engineer mistake the configuration? I hope to not find this question in the exam.

upvoted 10 times

cortib 1 year, 12 months ago

and assuming this the correct answer is note listed, because we are missing an entry for the serial interface that will be the one used in that casa (i think)

upvoted 4 times

Dante_Dan 1 year, 9 months ago

Well, what if its sending a broadcast? 10.0.1.15 still belongs to 10.0.1.0/28 subnet.

Answer: A

upvoted 19 times

Dante_Dan 1 year, 9 months ago

Forget the comment above. The question states that is trying to connect to a host via SSH...
Sorry!!

upvoted 10 times

FALARASTA 4 months, 2 weeks ago

Because I think .15 is the broadcast for the /28 network and here its via SSH.. is that what you mean is wrong?

upvoted 2 times

Dante_Dan 1 year, 9 months ago

I think even answer B is incorrect. As there is another route in the table stating that 10.0.1.0/24 network is directly connected on Serial0. And if I understand the previous entry conrrectly, Serial0 interface has 192.168.0.40.

(Probably) Answer C

upvoted 10 times

[Removed] 4 months ago

C is 192.168.0.40 - 10.0.1.3/32 via 192.168.0.40. That is not the host, you are looking for 10.0.1.15.
upvoted 1 times

DonnerKomet 2 years ago
Well, in the question is not mentioned that the IP is a host, so then you can have .15 as the broadcast IP valid.
upvoted 5 times

DonnerKomet 2 years ago
Sorry I didnt see the word "host", you are rite, it would not be a valid IP for host. So then the rite answer is B
upvoted 3 times

bruce007 Highly Voted 2 years ago
why doesn't it use the directly connected route??
upvoted 12 times

[Removed] 4 months ago
There is no such an answer.
upvoted 1 times

daytonadave2011 1 year, 10 months ago
Agreed. It should be Serial0 IP and none of the options listed is for Serial0.
upvoted 3 times

AWSFastLearner 1 year, 11 months ago
Yes, if people not think the answer is A (192.168.0.7). With same prefix, the next hop should be chosen directly connected with AD=0.
upvoted 1 times

raul_kapone Most Recent 3 weeks, 1 day ago
If the correct answer would be "A":
I think the logic is like that:
There are two routes to reach from the Loopback0 to the host with the IP address of 10.0.1.15 into the routing table:
- 10.0.1.0/24
- 10.0.1.0/28 (with 10.0.1.15 as the broadcast of this subnet)

. If the router wants to reach to 10.0.1.15, it can use the broadcast address of 10.0.1.0/28 (thus, the ssh traffic can reach the host with IP address of 10.10.1.15)
. And since the destination IP address of the SSH traffic matchs with the IP address of the host (10.0.1.15), the connection can be established.
. So, the router will use the route with the longest prefix length: 10.0.1.0/28
. Feel free to correct me if I'm wrong.
upvoted 1 times

kobisiva 4 weeks, 1 day ago
Selected Answer: B
a wrong becouse is broad cast address
upvoted 1 times

bilatuba 1 month, 2 weeks ago
Selected Answer: A
A is the correct answer: it says "to the host at 10.0.1.15". So, the ssh is going to "some host" on that subnet, and not the broadcast per se.
upvoted 1 times

chuvash 1 month, 2 weeks ago
Selected Answer: A
The quastion says "is trying to connect". Will he succeed with that? No! Coz 10.0.1.15 is a bradcast adress of 10.0.1.0/28, nevertheless the packet to 10.0.1.15 still gonna be routed to 10.0.1.0/28 coz 10.0.1.15 is part of this subnet.
upvoted 1 times

lamm 2 months ago
Selected Answer: A
Correct answer is A, it doesnt matter if 10.0.1.15 is believed as a broadcast in this segment, it doesnt mean it is, because this is a route learn by a neighbor so may be his intend is only to reveal this part of the network, so you neighbor will route whole segment, not only host valid ip, instead 10.0.1.0 to 10.0.1.15. My opinion on this.
upvoted 4 times

Hari2512 2 months, 3 weeks ago
Address: 10.0.1.0
Netmask: 255.255.255.240 = 28
Wildcard: 0.0.0.15
Network: 10.0.1.0
Broadcast: 10.0.1.15
HostMin: 10.0.1.1
HostMax: 10.0.1.14
Hosts/Net: 14
upvoted 1 times

dropspablo 3 months, 3 weeks ago

Selected Answer: A

I tested it on Packet Tracert, it's very simple when sending a command ssh -l name 10.0.1.15 and the final destination is a broadcast (in the routing table), the router normally forwards via 10.0.1.15/28, because within the 10.0.1.0 range - 10.0.1.15 it does not differentiate network id or broadcast.

Do a ping test and you will see, only when it arrives at the destination RT the packet is discarded because it is broadcast and there is no socket for that IP and port (22 SSH), but the pings work, and are forwarded by MASK /28.

You can ping to broadcast destinations or network id, but an SSH will fail, remembering that it is only a broadcast when the destination MAC is FFFF:FFFF:FFFF, in this case the frames would not be broadcast, only the destination location.

upvoted 2 times

ac89l 4 months, 2 weeks ago

from lab
answer A is correct

#sh ip route 172.26.192.15
Routing entry for 172.26.192.0/28
Known via "bgp", distance 20, metric 10, External Route Tag: 0, best
Last update 04w1d03h ago

upvoted 1 times

MRSCARLet 4 months, 3 weeks ago

B 10.0.1.0(Network) 255.255.255.0(/24) 10.0.1.1~10.0.1.254(Usable IP address) 10.0.1.255(Broadcast)
so 10.0.1.15 is usable IP address in this subnet, can been SSH
and the next hop: 10.0.1.0/24 [110/10] via "192.168.0.4"

A. 10.0.1.0(Network) 255.255.255.240(/28) 10.0.1.1~10.0.1.14(Usable IP address) 10.0.1.15(Broadcast)
so 10.0.1.15 is the broadcast address in this subnet, cannot been SSH
C. 10.0.1.3(Network) 255.255.255.255(/32) NA(Usable IP address) 10.0.1.3(Broadcast)
so 10.0.1.15 not in this subnet, cannot been SSH
D. -_-|||

upvoted 1 times

gc999 6 months ago

Selected Answer: A

Even it is the broadcast, I still choose "A". Because it is the thumb of rule for the routing decision in the routing table.

upvoted 2 times

Webfat 6 months, 3 weeks ago

This question is a mess, before Seeing the answer, I was thinking is C because static AD > OSPF AD and broadcast bad, but the more I see people comments more I think A is correct
The route doenst care if its a SSH Packet, he is a layer 3 device, so he justs see "hummm, I have this IP, I need to see the valid longest IP addr on my table, wow look at this, I have /28 here, but this way it will be a broadcast address... Well, whatever, broadcast it will go"
The user whos trying to connect via ssh shortly after will receive a error, but the route did his job as per programmed

upvoted 2 times

Webfat 6 months, 3 weeks ago

Just a correction from my comment, I think the router instead of broadcast the traffic, it will drop him, because routers do not propragate broadcas, and he will interpret this ip addr as broadcast

upvoted 1 times

iMo7ed 6 months, 3 weeks ago

Selected Answer: B

It's B, not A

upvoted 1 times

daddydagoth 6 months, 3 weeks ago

Selected Answer: B

You can't assign a broadcast address to a HOST, if you try it, the router will return "bad mask" and it won't work. So if a HOST with the 10.0.1.15 address needs to be reached via SSH, it's not possible that the subnet will be 10.0.1.0 /28, therefore the only correct answer left is B, the /24 subnet as that would allow address 10.0.1.15 to be assigned to a host.

upvoted 5 times

siredobu 6 months, 3 weeks ago

This question is not valid question, it mentioned a single network address (10.0.1.0/24) is connected to two interface types (sSerial0 and Gigabit Ethernet 0/0), which can not exist in reality

upvoted 1 times

Ciscoman021 7 months, 2 weeks ago

Selected Answer: B

Answer A is incorrect. 10.0.1.0/28 that means 10.0.1.1 - 10.0.1.14 . total host 14 plus network ip and broadcast IP.
Answer B is correct.

upvoted 1 times

Question #433 *Topic 1*

When the active router in a VRRP group fails, which router assumes the role and forwards packets?

A. forwarding

B. standby

C. backup

D. listening

Correct Answer: *C*

DaBest Highly Voted 1 year, 11 months ago

HSRP usese Active/Standby
VRRP usese Master/Backup
these roles are for the routers in the virtual group

upvoted 74 times

jaaks 1 year, 2 months ago

On Vol. 2 p260 of the Official Certification Guide, Wendell says that VRRP uses an active/standby, NOT master/backup redundancy approach.

upvoted 4 times

siredobu 6 months, 3 weeks ago

which is wrong, DaBest's comment is correct

upvoted 4 times

DUMPledore 7 months, 3 weeks ago

VRRP uses Master/Backup

upvoted 2 times

dicksonpwc Highly Voted 2 years ago

In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backups in case the virtual router master fails

upvoted 7 times

Shanku97 Most Recent 2 weeks, 2 days ago

In a Virtual Router Redundancy Protocol (VRRP) group, when the active router (also known as the master router) fails, the router with the highest priority among the backup routers will assume the active role and start forwarding packets. VRRP is a network protocol that provides high availability by allowing multiple routers to work together as a virtual router with a single IP address and MAC address.

answer - backup

upvoted 1 times

shumps 3 weeks, 1 day ago

C backup i over rule any debate on this question.

upvoted 1 times

LeonardoMeCabrio 2 months, 1 week ago

Selected Answer: C

C correct

upvoted 1 times

[Removed] 2 months, 3 weeks ago

Selected Answer: C

C is correct :
" In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backups, in case the virtual router master fails."

upvoted 1 times

4bed5ff 2 months, 3 weeks ago

Selected Answer: C

Cisco iOS says backup:
R2(config-if)#vrrp 10 ip 10.22.0.3
R2(config-if)#
*Mar 2 06:05:31.784: %VRRP-6-STATECHANGE: Fa0/0 Grp 10 state Init -> Backup
R2(config-if)#
*Mar 2 06:05:35.396: %VRRP-6-STATECHANGE: Fa0/0 Grp 10 state Backup -> Master

upvoted 1 times

phkumara 3 months ago

When the active router in a VRRP (Virtual Router Redundancy Protocol) group fails, the standby router assumes the role and forwards packets.

The standby router is the backup router in the VRRP group, ready to take over the responsibilities of the active router in case of a failure. It constantly monitors the status of the active router and listens for the advertisement messages sent by the active router. If the standby router detects that the active router has failed or become unreachable, it assumes the active role and starts forwarding packets on behalf of the virtual router.

So, the correct answer is:
B. standby

upvoted 1 times

linuxlife 5 months, 2 weeks ago

BACKUP is the proper conventions for VRRP.
https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/addr_serv/configuration/guide/ic40crs1book_chapter10.html#con_IPAddrCG_1279291971985

upvoted 1 times

checkoboy88 6 months, 2 weeks ago

Selected Answer: C

Correc is C... the VRRP uses MASTER and BACKUP.. i´ve seen it in production, we work with HSRP and VRRP as well... HSRP uses ACTIVE and STANDBY

upvoted 2 times

gewe 7 months ago

this is right :

HSRP usese Active/Standby
VRRP usese Master/Backup

upvoted 3 times

kobisiva 7 months, 2 weeks ago

Selected Answer: C

back is correct

upvoted 1 times

Ciscoman021 8 months, 2 weeks ago

Selected Answer: B

If VRRP router fails, another VRRP standby router automatically takes over as master.

upvoted 1 times

Shansab 8 months, 4 weeks ago

Selected Answer: C

Backup

upvoted 1 times

humanbot 10 months ago

Selected Answer: C

HSRP usese Active/Standby
VRRP usese Master/Backup

upvoted 1 times

Netcmd 10 months ago

VRRP uses master and Backup
https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/addr_serv/configuration/guide/ic40crs1book_chapter10.html

upvoted 1 times

Etidic 10 months, 3 weeks ago

Selected Answer: C

The answer is C

upvoted 1 times

Question #434 *Topic 1*

Which action does the router take as it forwards a packet through the network?

A. The router encapsulates the original packet and then includes a tag that identifies the source router MAC address and transmits it transparently to the destination.

B. The router encapsulates the source and destination IP addresses with the sending router IP address as the source and the neighbor IP address as the destination.

C. The router replaces the original source and destination MAC addresses with the sending router MAC address as the source and neighbor MAC address as the destination.

D. The router replaces the source and destination labels with the sending router interface label as a source and the next hop router label as a destination.

Correct Answer: *C*
Reference:
https://www.freeccnastudyguide.com/study-guides/ccna/ch4/ip-routing/

DaBest Highly Voted 1 year, 11 months ago
C is the correct answer , only mac address gets changed when forwarding, IP address always stays the same
upvoted 22 times

Chopaka 2 months, 3 weeks ago
I thought that the mac adres never change right?
upvoted 1 times

Mark_j_k90 1 month, 3 weeks ago
You need to keep studying!
upvoted 2 times

```
R2#show ip route
C        192.168.1.0/26 is directly connected, FastEthernet0/1
```

Refer to the exhibit. Which two prefixes are included in this routing table entry? (Choose two.)

A. 192.168.1.17

B. 192.168.1.61

C. 192.168.1.64

D. 192.168.1.127

E. 192.168.1.254

Correct Answer: *AB*

netzwork Highly Voted 11 months, 1 week ago

If Cisco is wording questions like this, they should take a dive off a cliff

upvoted 14 times

bikila123 1 month, 1 week ago

😀hhhhh

upvoted 1 times

MCMH2000 Highly Voted 1 year, 4 months ago

Question should be:
"Which two IP addresses are included in this routing table entry?"

upvoted 5 times

bikila123 Most Recent 1 month, 1 week ago

C is network address
D and E are broadcast address for a given network

upvoted 1 times

bikila123 1 month, 1 week ago

A and B are correct answer

upvoted 1 times

splashy 1 year ago

Question is written by a edonkey, "prefixes" should be "hosts"

upvoted 4 times

DARKK 1 year, 3 months ago

Selected Answer: AB

192.168.0-63 because /26 = 64 IP addresses per subnet and 4 subnets (256/64), 0-63, 64-127, 128-191, 192-255. A & B are correct.

upvoted 1 times

moses23 7 months, 3 weeks ago

How does this correlate with the answers?

upvoted 2 times

Question #436 *Topic 1*

Which virtual MAC address is used by VRRP group 1?

A. 0504.0367.4921

B. 0007.c061.bc01

C. 0050.0c05.ad81

D. 0000.5E00.0101

Correct Answer: *D*

DARKK Highly Voted 1 year, 3 months ago

Selected Answer: D

VRRP = 0000.5E00.01XX (XX = GROUP ID) -Answer D.
HSRP V1 = 0000.0C07.ACXX (XX = GROUP ID)
HSRP V2 = 0000.0C9F.FXXX (XXX = GROUP ID)
GLBP = 0007.B400.XXYY (XX = GROUP ID) (YY = AVF ID)

upvoted 8 times

laurvy36 Most Recent 1 year, 8 months ago

A virtual MAC address is generated by the virtual router based on the virtual router ID. The virtual MAC address format is 00-00-5E-00-01-{VRID} (VRRP) and 00-00-5E-00-02-{VRID}

upvoted 4 times

Question #437 *Topic 1*

What is the purpose of using First Hop Redundancy Protocol on a specific subnet?

A. forwards multicast hello messages between routers

B. sends the default route to the hosts on a network

C. ensures a loop-free physical topology

D. filters traffic based on destination IP addressing

Correct Answer: *B*
The routers in the FHRP group share a virtual MAC and Virtual IP and that acts as the Default Gateway for the HOSTS. It provides redundancy is case a router fails, no need to change the default gateway information.

Dante_Dan Highly Voted 1 year, 8 months ago
Well, among the answers, A is the least incorrect, as I don't think that forwarding multicast hello messages between routers is the PURPOSE of using a First Hop Redundancy Protocol.
The other answers refer to other protocols:
Answer B refers to a DHCP server
Answer C refers to STP
Answer D refers to ACL
upvoted 13 times

TheLorenz 1 year, 6 months ago
B doesn't refer to DHCP. DHCP is responsible for providing IP addresses dynamically to hosts.
upvoted 2 times

D0nkey_h0t 1 year, 3 months ago
it does! cause along with ip adresses it provides also subnet masks, default gateways and even DNS servers
upvoted 4 times

TA77 Highly Voted 1 year, 2 months ago
I have no idea what is the benefit of twisting words to come up with complicated question, which will not serve in real life.

The purpose of FHRP is to provide redundancy for the gateway. PERIOD!

Anyway, I'm going with option A.
upvoted 13 times

sasquatchshrimp 1 year, 1 month ago
Just in case an enduser finds themselves in your switches, calls in and asks you dumb questions they know nothing about, which will eventually achieve nothing. haha
upvoted 2 times

shumps Most Recent 3 weeks, 1 day ago
Answer is B a stable routing.
upvoted 1 times

kyleptt 2 months, 2 weeks ago
Poorly worded question but HSRP sends hello packets between each other to ensure that the routers are up but this is not the reason for HSRP
upvoted 1 times

Rether16 5 months, 1 week ago
Some of these quetions by Cisco are really poor. The purpose of FHRP is simply for redundancy. I picked A but It was a lucky guess between that and B if im honest!
upvoted 3 times

daddydagoth 6 months, 3 weeks ago
Selected Answer: A
A is correct. FHRPs do not forward the default gateway to hosts.
upvoted 2 times

DUMPledore 9 months, 1 week ago
Selected Answer: A
I would go with A
upvoted 4 times

Eyad_Alotaibi 9 months, 1 week ago

FHRP forwards "Hello Messages" and "Hold Time Messages" between routers.
Hello Message : "Active Router" sends "Hello Message" every x second to "Standby Router" to verify if it is there or down.
Hold time : Standby router Wait for "Hello Message" from the "Active Router", if it does not arrive, the "Standby Router" will become "Active Router".

HSRP (cisco protocol)
Hello Message : every 3 sec
Hold Time : waiting 10 sec

VRRP (open standard protocol)
Hello Message : every 1 sec
Hold Time : waiting 3 sec

upvoted 6 times

Eyad_Alotaibi 9 months, 1 week ago

so the correct answer is A

upvoted 1 times

mzu_sk8 10 months ago

Selected Answer: A

on other sites!

upvoted 2 times

splashy 11 months, 3 weeks ago

Selected Answer: A

100% A

I thought it was more or too ospf related BUT

With HSRP, there are three types of multicast messages sent between the devices:
Hello
Resign
Coup

https://study-ccna.com/cisco-hsrp-explained/

B.Default route? Routers can haven them and share them with other routers. = wrong
If it would say default gateway the only thing (we learned) that can send that is a DHCP server. = wrong
C.STP = wrong
D.ACL = wrong

upvoted 5 times

rictorres333 1 year ago

B is posible thinking in layer 2, about host asking by mac of its configured defaul gateway IP. The protocol send de virtual mac assigned to active router. Remember reviewing output from wireshark, hosts asking fist time o each arp cache timeout for "who is this ip", FHRP answer with the virtual mac.

upvoted 1 times

iGlitch 1 year, 3 months ago

Selected Answer: B

B - It connects to HOSTS with the default gateway (VIP).
It's the most appropriate answer among other answers.

upvoted 3 times

DARKK 1 year, 3 months ago

Selected Answer: B

A just seems wrong, B is correct. The routers in the FHRP group share a virtual MAC and Virtual IP and that acts as the Default Gateway for the HOSTS. It provides redundancy is case a router fails, no need to change the default gateway information. Poorly worded Question, but it is B.

upvoted 2 times

redivivo 1 year, 3 months ago

sorry but answer B says " sends default route", not default gateway, so I don't get how can be correct. The default route is sent to routers, not hosts, and with a dynamic routing protocol through the "originate" command

upvoted 4 times

iGlitch 1 year, 3 months ago

I agree.

upvoted 1 times

mantest 1 year, 4 months ago

Ans B is correct.
A first hop redundancy protocol (FHRP) is a computer networking protocol which is designed to protect the default gateway used on a subnetwork by allowing two or more routers to provide backup for that address;[1][2] in the event of failure of an active router, the backup router will take over the address, usually within a few seconds

upvoted 2 times

markdonald 1 year, 4 months ago

Why am I restricted to the next page¿??
Pls I don't have money now for contribution access it too expensive..... someone should help on what to do? My exams is next tomorrow.

upvoted 2 times

pagamar 1 year, 5 months ago

Tumbative: the RIGHT answer is A; found in a recent Exam, Topic 3, 100% correct.

upvoted 3 times

ismatdmour 1 year, 6 months ago

I agree with the comments made before me. This is a Naive question by CISCO and is ill worded. I arrived at A as answer by execluding B (DHCP), C (STP) and D (ACLs). Option A states something correct about HSRP routers in that they exchange hello messages to get to know each other and elect the active one and who is standby as well as to inquire about the health of the Active router so that the standby router can replace him in case it becomes down. Well, this is not the "PURPOSE" of FHRP (Purpose is to provide redundancy) but rather how FHRP is doing its work.
Just wondering about those CISCO guys who put the questions, sometimes they are very strict in the question formation and the word they use are very much selected while in many other cases, such as this one, they are even naively using the incorrect word (or elsewise they mean it - to fail more people!!!!-

upvoted 3 times

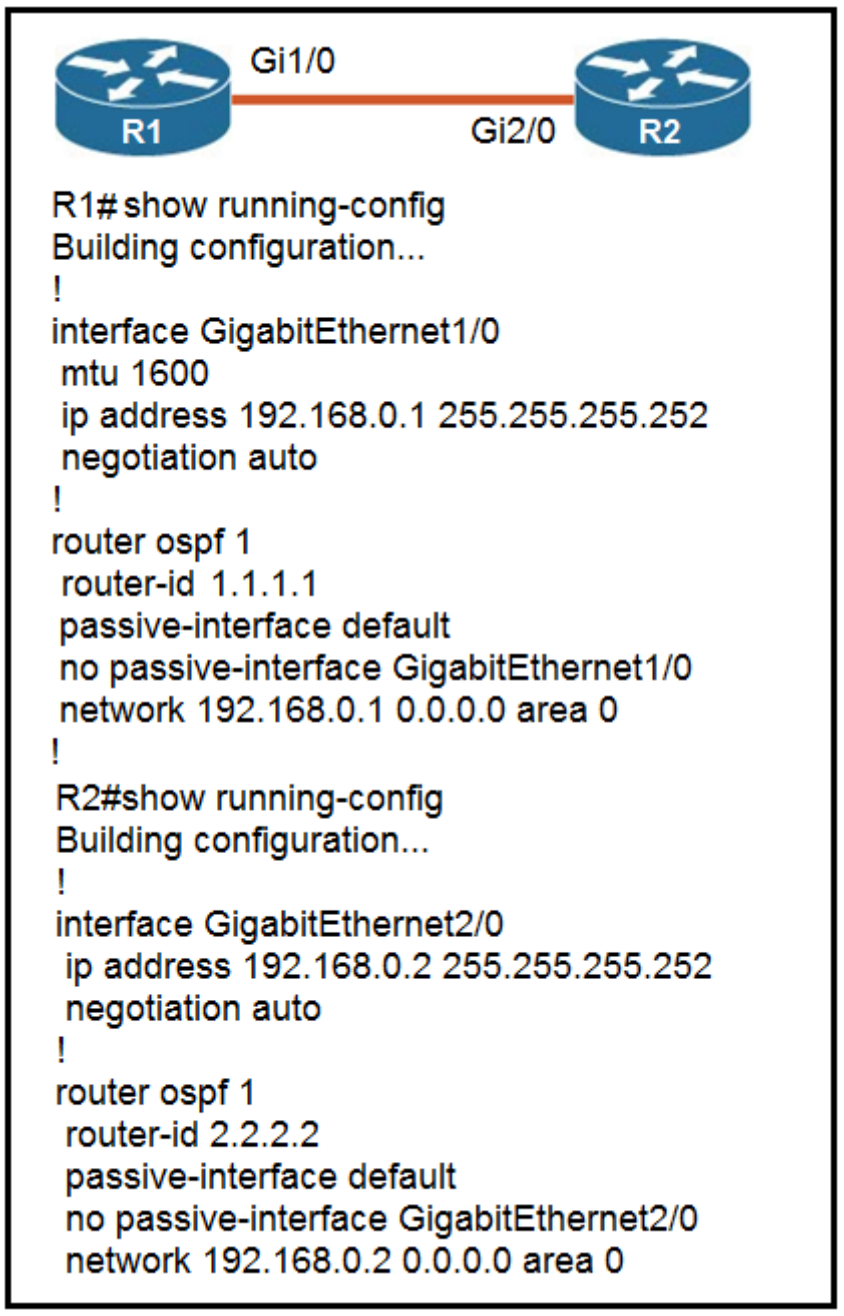
TA77 1 year, 2 months ago

That's why using dumps is essential before taking the exam, lol. If you try to take the exam without studying dumps you'll have high chances of failing. smh!

upvoted 2 times

Question #438 *Topic 1*

Refer to the exhibit. Which configuration issue is preventing the OSPF neighbor relationship from being established between the two routers?



A. R1 has an incorrect network command for interface Gi1/0.

B. R2 should have its network command in area 1.

C. R1 interface Gi1/0 has a larger MTU size.

D. R2 is using the passive-interface default command.

Correct Answer: *C*

oooMooo Highly Voted 2 years, 4 months ago

You can configure OSPF to ignore MTU size: ip ospf mtu-ignore

upvoted 15 times

SScott 2 years, 1 month ago

While true, this is very infrequently configured on business routers. Thus C MTU mismatch is correct.

upvoted 7 times

tyuipo Highly Voted 2 years, 4 months ago

The normal or default MTU size typically used is 1500 bytes.

Ans: "C" is correct

upvoted 11 times

Yinxs Most Recent 3 weeks, 5 days ago

Selected Answer: D

MTU mismatch doesn't lead to break of neighbor relationship, only can lead to abnormal work. But the passive-interface will lead the interface stop to send HELLO, than no neighbor set up.

upvoted 1 times

ODZA 1 month, 3 weeks ago

A mismatched mtu prevent ospf from forming full adjacency, not 2 way neighbor relationship so C doesnt make full sense for me though it is the better option among the provided answers

upvoted 1 times

Raman1996 1 year, 7 months ago

is the network command issued with correct network address and wildcard bits?

upvoted 2 times

vannplus11 1 year, 12 months ago

MTU mismatch between neighboring interfaces. show interface <int-type><int-num>

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13699-29.html?referring_site=bodynav#anc13

upvoted 2 times

Chocobo 2 years, 6 months ago

RFC 2328:
If the Interface MTU field in the Database Description packet indicates an IP datagram size that is larger than the router can accept on the receiving interface without fragmentation, the
Database Description packet is rejected.

upvoted 6 times

SScott 2 years, 1 month ago

C is absolutely right.
Yes, I've experienced this in the field on several occasions ..an odd issue but a definite sneak up and bang factor - your tunnel and consistent traffic be done.

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/116119-technote-ospf-mtu-00.html#:~:text=In%20this%20example%2C%20the%20routers%20have%20GigabitEthernet%20interfaces%20with%20an%20MTU%20set%20to%202000.%20The%20MTU%20of%20the%20L2%20switch%20is%20only%201500%20bytes

https://www.reddit.com/r/networking/comments/k9hr35/ospf_mtu/

upvoted 3 times

Question #439 *Topic 1*

```
R1# show ip route
Codes:  L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is 10.56.0.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 10.56.0.1
        10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C          10.56.0.0/17 is directly connected, Vlan56
L          10.56.0.19/32 is directly connected, Vlan56
C          10.56.128.0/18 is directly connected, Vlan57
L          10.56.128.19/32 is directly connected, Vlan57
```

Refer to the exhibit. When router R1 is sending traffic to IP address 10.56.192.1, which interface or next hop address does it use to route the packet?

A. 10.56.0.1

B. 0.0.0.0/0

C. Vlan57

D. 10.56.128.19

Correct Answer: *A*

kentsing Highly Voted 1 year, 4 months ago

Like other questions, barely not covered by network routes and falls to default route.
A is correct.

upvoted 6 times

john1247 Most Recent 3 months, 2 weeks ago

Be careful if you judge by looking at the prefix length. If you are not familiar with it, I recommend calculating the IP address. The calculation will give you 10.56.0.1.not a VLAN57

upvoted 2 times

RaselAhmedIT 6 months, 2 weeks ago

192.168.192.1 isn't available in the routing table that's why Router# automatically selects *Default Static Route*

upvoted 1 times

Webfat 6 months, 3 weeks ago

There is not Vlan56, but if it was a option should he be the correct answer?

upvoted 1 times

studying_1 3 months, 3 weeks ago

No, it will be sent via the default route, so you need to check the next hop, which is A, 10.56/0/0/17 doesnt cover it, 10.56.0.0 - 10.56.127.254

upvoted 1 times

niangbah 8 months, 2 weeks ago

why not Vlan 57(answer C) as the network 10.56.128.0/18 include the ip address 10.56.192.1 and look like it's the longest prefix match?

upvoted 3 times

laurvy36 7 months, 2 weeks ago

doesnt include, if you calculate is until 191.254

upvoted 4 times

ratu68 1 year, 2 months ago

Selected Answer: A

A is correct as other routes in the table doesn't cover the mentioned address

upvoted 3 times

Question #440 *Topic 1*

```
R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       El - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, Ll - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C    172.16.0.0/16 is directly connected, Loopback0
     172.16.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.16.1.3/3 [110/100] via 192.168.7.40, 00:39:08, Serial0
C       172.16.1.0/24 is directly connected, Serial0
O       172.16.1.184/29 [110/5] via 192.168.7.35, 00:39:08, Serial0
O       172.16.3.0/24 [110/10] via 192.168.7.4, 00:39:08, Gigabit Ethernet 0/0
D       172.16.1.0/28 [90/10]  via 192.168.7.7, 00:39:08, Gigabit Ethernet 0/0
```

Refer to the exhibit. Load-balanced traffic is coming in from the WAN destined to a host at 172.16.1.190. Which next-hop is used by the router to forward the request?

A. 192.168.7.4

B. 192.168.7.7

C. 192.168.7.35

D. 192.168.7.40

Correct Answer: *C*

DARKK 1 year, 3 months ago

Selected Answer: C

Simple way to look at it:
/29 = 8 IPs, 182-191, 190 is the last Assignable IP on that Subnet, so /29 is picked because it is the Longest Prefix route INCLUSIVE of the IP address. And the next hop IP for that is C. 192.168.7.35

upvoted 2 times

fl_it_guy 1 year, 2 months ago

Did you mistype above? 184-191, with 185-190 usable.
Answer: C

upvoted 4 times

SVN05 1 year, 3 months ago

Excluding all the description about load-balancing traffic, etc etc... the bottom line is what is the next hop of address 172.16.1.190? Answer is C.192.168.7.35.
How I got it?
/29 subnet(/32 minus /29 equals to 3 subnet bits)
Now take 2 to the power of 3 youll have 8 subnets and for host just minus 2 which is 6 hosts(for network & broadcast subnet ID, ITS A MUST)
So, in the network address 172.16.1.184....starting address is 172.16.1.185 all the way to 172.16.1.191 thus the 172.16.1.190 host is able to be allocated to this network ID(172.16.1.184). That's how you'll get your answer. Good Luck to all.

upvoted 2 times

Question #441 *Topic 1*

What is a benefit of VRRP?

A. It provides the default gateway redundancy on a LAN using two or more routers.

B. It provides traffic load balancing to destinations that are more than two hops from the source.

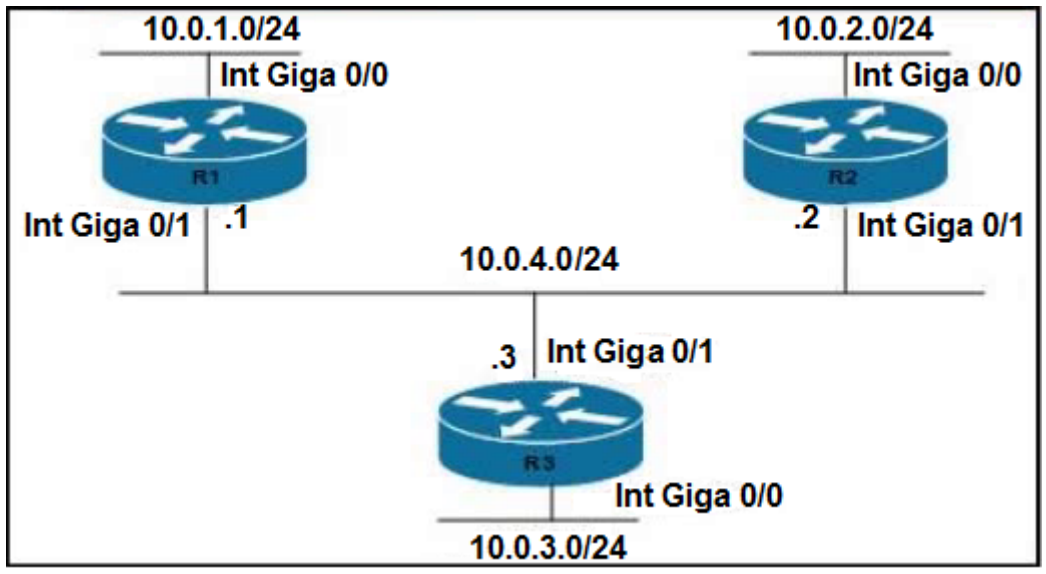
C. It prevents loops in a Layer 2 LAN by forwarding all traffic to a root bridge, which then makes the final forwarding decision.

D. It allows neighbors to share routing table information between each other.

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/addr_serv/configuration/guide/ic40crs1book_chapter10.html

Nnandes Highly Voted 1 year, 4 months ago
A is the correct
upvoted 5 times

Question #442 *Topic 1*



Refer to the exhibit. Routers R1 and R3 have the default configuration. The router R2 priority is set to 99. Which commands on R3 configure it as the DR in the
10.0.4.0/24 network?

A. R3(config)#interface Gig0/0 R3(config-if)#ip ospf priority 100

B. R3(config)#interface Gig0/0 R3(config-if)#ip ospf priority 1

C. R3(config)#interface Gig0/1 R3(config-if)#ip ospf priority 0

D. R3(config)#interface Gig0/1 R3(config-if)#ip ospf priority 100

Correct Answer: *D*
In the case of OSPF, 0 means you will never be elected as DR or BDR. Default priority is 1. Highest priority will be elected as the DR.

Mili2023 7 months, 1 week ago
answer is A.
As we need to configure the opposite interface which is G0/0
upvoted 2 times

Rick3390 2 weeks ago
are you serious? have you suffer of a recent blow of the head? you don't even understand the question, but you still comment! Answer is not A you dumb ass!!!! stop comment if you don't know shit. Answer is D!
upvoted 1 times

Shanku97 2 weeks, 2 days ago
KUCH BHI KYA ? BEHENCHOD CHECK THE N/W FOR G0/0 FIRST AND THEN REA THE QUESTION, DON'T JUST CONUSE EVERYONE BY TYPING ANYTHING RANDOM
upvoted 1 times

i_am_confused 1 year, 2 months ago
Priority is 100 by default so you actually don't have to configure anything?
upvoted 2 times

i_am_confused 1 year, 2 months ago
Sorry, default priority is 1, so you would need to configure.
upvoted 2 times

deeanaho 1 year, 3 months ago
Why not C the correct answer?
upvoted 1 times

takaman 1 year, 2 months ago
This is not spanning tree protocol where 0 becomes the highest priority.
In the case of OSPF, 0 means you will never be elected as DR or BDR. Default priority is 1.
upvoted 8 times

DARKK 1 year, 3 months ago
Selected Answer: D
Highest Priority interface becomes the DR. So it would be 100 since it is higher than 99 in this case.
upvoted 1 times

jtyphoon 1 year, 4 months ago

I would have thought setting the loopback on R3 with a higher priority of 100 would have got DR.Why choose setting the main interface with the higher priority?

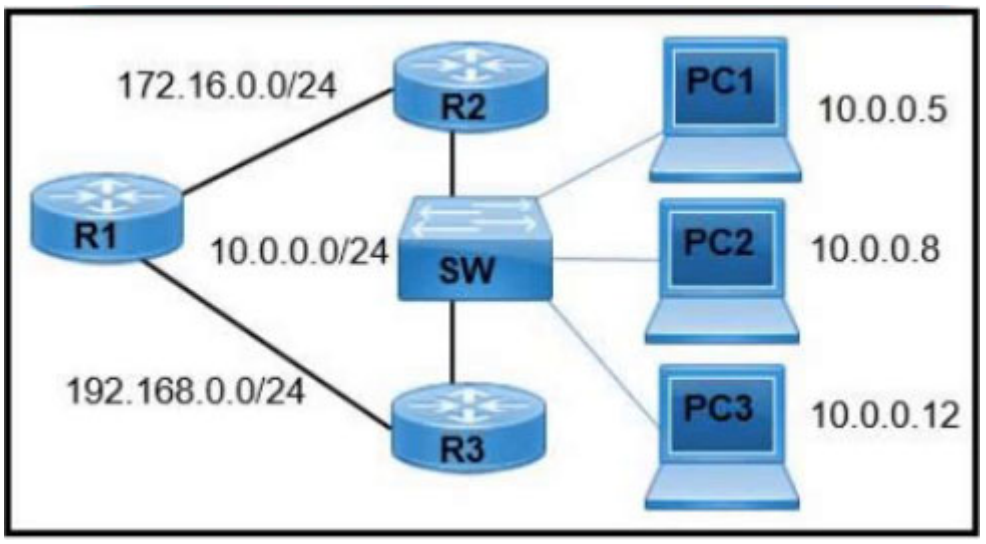
upvoted 1 times

jossyda 1 year, 4 months ago

Los routers en la red seleccionan como DR al router con la prioridad de interfaz más alta. El router con la segunda prioridad de interfaz más alta se elige como BDR.

upvoted 2 times

Question #443 *Topic 1*



Refer to the exhibit. A network engineer must configure R1 so that it sends all packets destined to the 10.0.0.0/24 network to R3, and all packets destined to PC1 to R2. Which configuration must the engineer implement?

A. R1(config)#ip route 10.0.0.0 255.255.255.0 172.16.0.2 R1(config)#ip route 10.0.0.5 255.255.255.255 192.168.0.2

B. R1(config)#ip route 10.0.0.0 255.255.0.0 172.16.0.2 R1(config)#ip route 10.0.0.5 255.255.255.255 192.168.0.2

C. R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.0.2 R1(config)#ip route 10.0.0.5 255.255.255.255 172.16.0.2

D. R1(config)#ip route 10.0.0.0 255.255.0.0 192.168.0.2 R1(config)#ip route 10.0.0.5 255.255.255.0 172.16.0.2

Correct Answer: *C*

shumps 3 weeks, 1 day ago

C is correct. Another part was left behind,
i feel like this question has to parts. the path from PC1 to router 2, though they is no static answer for it in the given answers

upvoted 1 times

StingVN 4 months ago

Selected Answer: C

Am I the only one notice that the netmask of R1(config)#ip route 10.0.0.5 255.255.255.255 172.16.0.2 should be changed to 255.255.255.0?

upvoted 1 times

studying_1 4 months ago

no, it shouldn't, it is a host root, only reach the host(pc), not a network, so it's /32

upvoted 2 times

DARKK 1 year, 3 months ago

Selected Answer: C

Given answer is Correct

upvoted 2 times

aaandyyy 1 year, 4 months ago

The question is not finished!! Please fix.
A network engineer must configure R1 so that it sends all packets destined to the 10.0.0.0/24 network to R3, and all packets destined to PC1 to R2 from R2!

upvoted 2 times

aaandyyy 1 year, 4 months ago

Sorry, delete please)
did not read carefully

upvoted 6 times

Question #444 *Topic 1*

```
CPE# show ip route
     192.168.1.0/24 is variably subnetted, 3 subnets, 3 masks
B    192.168.1.0/24 [20/1] via 192.168.12.2, 00:00:06
R    192.168.1.128/25 [120/5] via 192.168.13.3, 00:02:35, Ethernet0/1
O    192.168.1.192/26 [110/11] via 192.168.14.4, 00:02:23, Ethernet0/2
D    192.168.1.224/27 [90/1024640] via 192.168.15.5, 00:01:40, Ethernet0/3
```

Refer to the exhibit. All traffic enters the CPE router from interface Serial0/3 with an IP address of 192.168.50.1. Web traffic from the WAN is destined for a LAN network where servers are load-balanced. An IP packet with a destination address of the HTTP virtual IP of 192.168.1.250 must be forwarded. Which routing table entry does the router use?

A. 192.168.1.0/24 via 192.168.12.2

B. 192.168.1.128/25 via 192.168.13.3

C. 192.168.1.192/26 via 192.168.14.4

D. 192.168.1.224/27 via 192.168.15.5

Correct Answer: *D*

Augusto2332 Highly Voted 10 months ago

Dont get confused by reading first part of questions, basically CCNA exam creators want you to focus in the beginning of the question which has nothing to do with finding the answer. You need to keep reading until the last part of the question.

This dumps are good way to practice, thanks a lot guys

upvoted 15 times

[Removed] 2 months, 3 weeks ago

You are 100%. I got confused when i read the first part of the question then it became obvious when reading the second part. So yes, they're trying to get you confused!

upvoted 1 times

Chopaka 2 months, 3 weeks ago

Yes sirrr boss!

upvoted 2 times

phkumara 3 months ago

okay boss

upvoted 3 times

DARKK Highly Voted 1 year, 3 months ago

Selected Answer: D

D is right. Longest Prefix route inclusive of the IP Address. /27 = 32, which is inclusive in this case.

upvoted 7 times

Drians_21 1 year, 2 months ago

I agree

upvoted 1 times

Thaier Most Recent 1 month, 3 weeks ago

This question is depending on distracting you not examining you.

upvoted 2 times

RaselAhmedIT 6 months, 1 week ago

I think D (192.168.1.224/27 via 192.168.15.5) is the correct answer.

upvoted 1 times

gewe 7 months ago

beautiful question... really

upvoted 2 times

jasmineelly 9 months, 2 weeks ago

thanks for share nice article. https://newextendersetup.live/192-168-1-250

upvoted 1 times

Etidic 10 months, 3 weeks ago

Selected Answer: D

The answer is D

upvoted 1 times

ratu68 1 year, 2 months ago

Selected Answer: D

easy answer - D is correct.

upvoted 1 times

BitterOldMan 1 year, 4 months ago

D: 192.168.1.224/27 wins over 192.168.1.128/25
First IP 192.168.1.225
Last IP 192.168.1.254

upvoted 3 times

bongthu 1 year, 4 months ago

Selected Answer: B

I think its B

upvoted 1 times

Etidic 10 months, 3 weeks ago

B is wrong

upvoted 1 times

DARKK 1 year, 3 months ago

That is wrong.

upvoted 1 times

jossyda 1 year, 4 months ago

Por la regla longest preffix match. Opción D.

upvoted 1 times

Question #445 *Topic 1*

```
A# show ip ospf neighbor
Neighbor ID  Pri  State          Dead Time  Address       Interface
172.1.1.1    1    EXCHANGE/ -    00:00:36   172.16.32.1   Serial0.1
```

Refer to the exhibit. An engineer assumes a configuration task from a peer. Router A must establish an OSPF neighbor relationship with neighbor 172.1.1.1. The output displays the status of the adjacency after 2 hours. What is the next step in the configuration process for the routers to establish an adjacency?

A. Configure router A to use the same MTU size as router B.

B. Configure a point-to-point link between router A and router B.

C. Set the router B OSPF ID to the same value as its IP address.

D. Set the router B OSPF ID to a nonhost address.

Correct Answer: *A*
Reference:
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13684-12.html#neighbors

Wilasky Highly Voted 1 year, 4 months ago

In Exstart/Exchange State, when attempting to run OSPF between a Cisco router and another vendor's router. If the router with the higher MTU sends a packet larger that the MTU set on the neighboring router, the neighboring router ignores the packet.

upvoted 25 times

Dutch012 Most Recent 6 months, 3 weeks ago

I think it's A.

the interface is using serial type, and the default configuration for OSPF is broadcast network type, so we must change the network type to point-to-point since it uses a serial connection

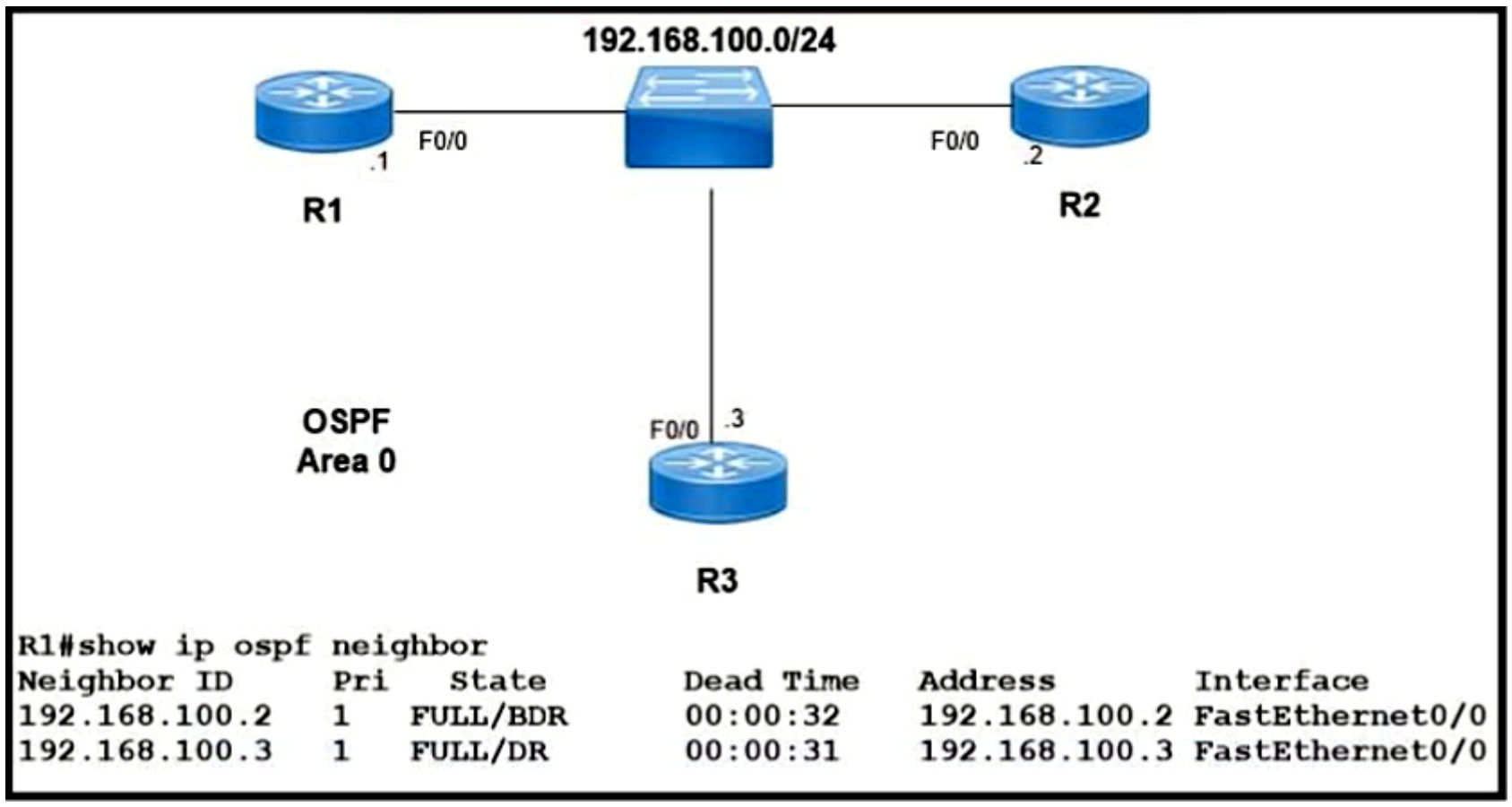
upvoted 3 times

Dutch012 6 months, 1 week ago

P-to-P is enabled by default in serials interfaces, I agree with Wilasky

upvoted 5 times

Question #446 *Topic 1*



Refer to the exhibit. Which two configurations must the engineer apply on this network so that R1 becomes the DR? (Choose two.)

A. R3(config)#interface fastethernet 0/0 R3(config-if)#ip ospf priority 0

B. R1(config)#router ospf 1 R1(config-router)#router-id 192.168.100.1

C. R1(config)#interface fastethernet 0/0 R1(config-if)#ip ospf priority 200

D. R1(config)#interface fastethernet 0/0 R1(config-if)#ip ospf priority 0

E. R3(config)#interface fastethernet 0/0 R3(config-if)#ip ospf priority 200

Correct Answer: *AC*

SVN05 Highly Voted 1 year, 3 months ago

Answer A is settings router 3 to have priority 0(0 means they are not allowed to participate in DR/BDR election)
Answer C is making R1 to have a higher priority(default is 1 but putting very high number is only for safety reasons to ensure that the R1 is elected DR)

upvoted 12 times

Shanku97 Most Recent 2 weeks, 2 days ago

C IS ALREADY SUFFICIENT , WHY WE NEED TO CHOOSE A ?

upvoted 1 times

tubirubs 1 month, 1 week ago

WTH IS THIS QUESTION??? It request the R1 become a DR. Its not necessary remove R3 of the electon... sh1t of question.

upvoted 2 times

GigaGremlin 11 months, 1 week ago

You can use the command Router(config-if)#ip ospf priority 200
to change the priority to 200 (The default value is 1) and then you use
Router# clear ip ospf process
command to enforce your changes...

upvoted 4 times

DARKK 1 year, 3 months ago

Selected Answer: AC

A & C are Correct. R1 must have the Highest priority, and thus R3 a low or lowest Priority.

upvoted 4 times

VictorCisco 5 months, 3 weeks ago

once you configured on R1 priority 200, R3 already has a lower priority. Why it is deeded to set it to 0?

upvoted 2 times

tubirubs 1 month, 1 week ago

its necessary execute the comand # clear ip ospf process to change. not necessary remove R3 of DR/BDR election

upvoted 1 times

kyleptt 1 month, 4 weeks ago

i dont think it would be needed also 200 make that router the DR

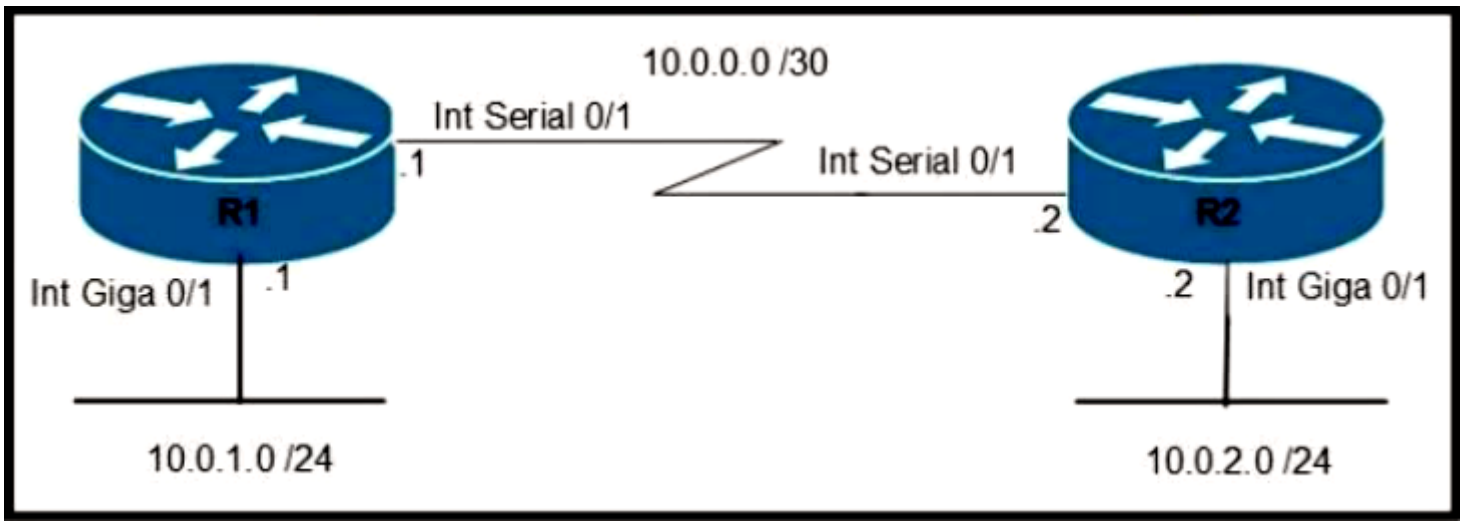
upvoted 1 times

JuanluRea 2 months, 3 weeks ago

I think so

upvoted 1 times

Question #447 *Topic 1*



Refer to the exhibit. Which command configures OSPF on the point-to-point link between routers R1 and R2?

A. router-id 10.0.0.15

B. neighbor 10.1.2.0 cost 180

C. network 10.0.0.0 0.0.0.255 area 0

D. ip ospf priority 100

Correct Answer: *C*

Sal34 Highly Voted 1 year, 3 months ago
The subnet mask seems wrong. Because the wildcard for a /30 should be 0.0.0.3, not 0.0.0.255.
upvoted 18 times

ptfish 1 year, 1 month ago
OSPF uses wildcard masks. So only the first 24bits (10.0.0) are checked.
upvoted 2 times

DoBronx 10 months, 3 weeks ago
yes but a /30 wildcard is 0.0.0.3
upvoted 9 times

Ysy Highly Voted 1 year, 2 months ago
just needs to match, not be identical
upvoted 7 times

Shanku97 Most Recent 2 weeks, 2 days ago
I GUESS IT'S A TYPO FOR SUBNET MASK OF 255.255.255.252 , WILDCARD MASK SHOULD BE 0.0.0.3
upvoted 1 times

bikila123 1 month ago
Ip wild card dont much the adjacency could not much
upvoted 1 times

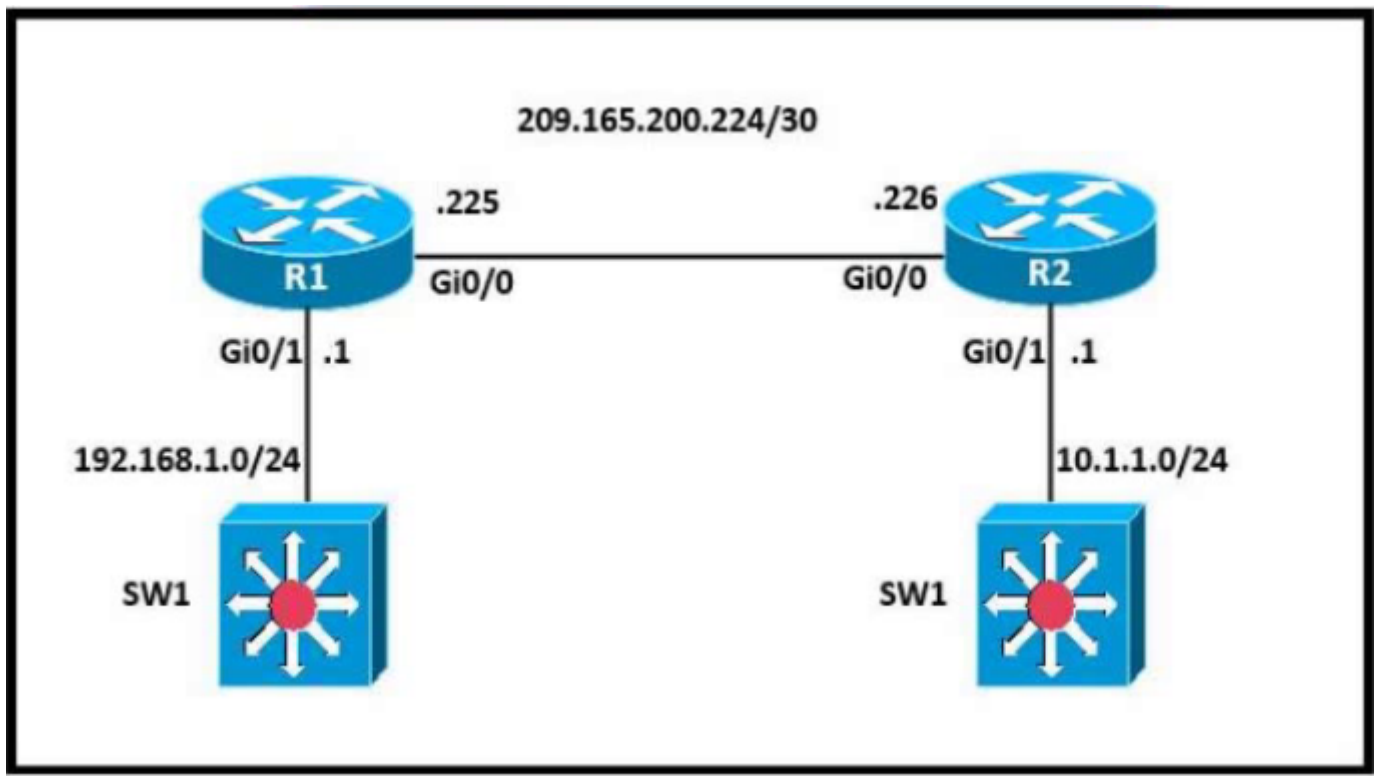
Da_Costa 3 months, 2 weeks ago
Confusing.. I thought /30 wild mask is 0.0.0.3 I don't think /24 is appropriate can someone explain better please?
upvoted 1 times

HugoP 3 months, 1 week ago
Seems like a mistake from them tbh
upvoted 2 times

cormorant 10 months, 2 weeks ago
ospf command = look for answer with wildcard
upvoted 2 times

Customexit 10 months, 3 weeks ago
Despite what the wildcard says and the other answers, the other commands won't configure an OSPF connection with each other.
upvoted 3 times

Question #448 *Topic 1*



Refer to the exhibit. A network engineer is in the process of establishing IP connectivity between two sites. Routers R1 and R2 are partially configured with IP addressing. Both routers have the ability to access devices on their respective LANs. Which command set configures the IP connectivity between devices located on both LANs in each site?

A. R1 ip route 192.168.1.1 255.255.255.0 GigabitEthernet0/1 R2 ip route 10.1.1.1 255.255.255.0 GigabitEthernet0/1

B. R1 ip route 192.168.1.0 255.255.255.0 GigabitEthernet0/0 R2 ip route 10.1.1.1 255.255.255.0 GigabitEthernet0/0

C. R1 ip route 0.0.0.0 0.0.0.0 209.165.200.225 R2 ip route 0.0.0.0 0.0.0.0 209.165.200.226

D. R1 ip route 0.0.0.0 0.0.0.0 209.165.200.226 R2 ip route 0.0.0.0 0.0.0.0 209.165.200.225

Correct Answer: *D*

SVN05 Highly Voted 1 year, 3 months ago

Answer D is correct as it is stating any route goes through next hop of 2019.165.200.226(for R1) while any route next hops to 209.165.200.225(On R2)

Answer A and B are not correct as the question states that both routers can access their respective LANs thus having a static route in each own LAN makes no sense.

upvoted 14 times

ananinamia Most Recent 1 week, 6 days ago

REMEMBER! package flows from source to destination!!! so first source then destination comes

upvoted 1 times

Shanku97 2 weeks, 2 days ago

the question already states that both route is already configured to access devices on their local lan, so a & b will be eliminated at first,

upvoted 1 times

Jorro99404 3 months, 2 weeks ago

Selected Answer: D

D is the correct

upvoted 1 times

iMo7ed 6 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

DoBronx 10 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

GigaGremlin 11 months, 1 week ago

Selected Answer: D

Answer D is correct
Router(config)#ip route 0.0.0.0 0.0.0.0 [exit-interface or IP address of the next-hop]

upvoted 1 times

ShehuUsman 1 year, 1 month ago

Selected Answer: C

D is wrong. Answer C is correct as it is stating any route goes through 209.165.200.225(for R1) while any route to 209.165.200.226(On R2)

upvoted 1 times

Sutokuto 12 months ago

No, answer D is correct because after 0.0.0.0 0.0.0.0 you put the next hop, which is router 2 on .226 You don't put the router's own interface.

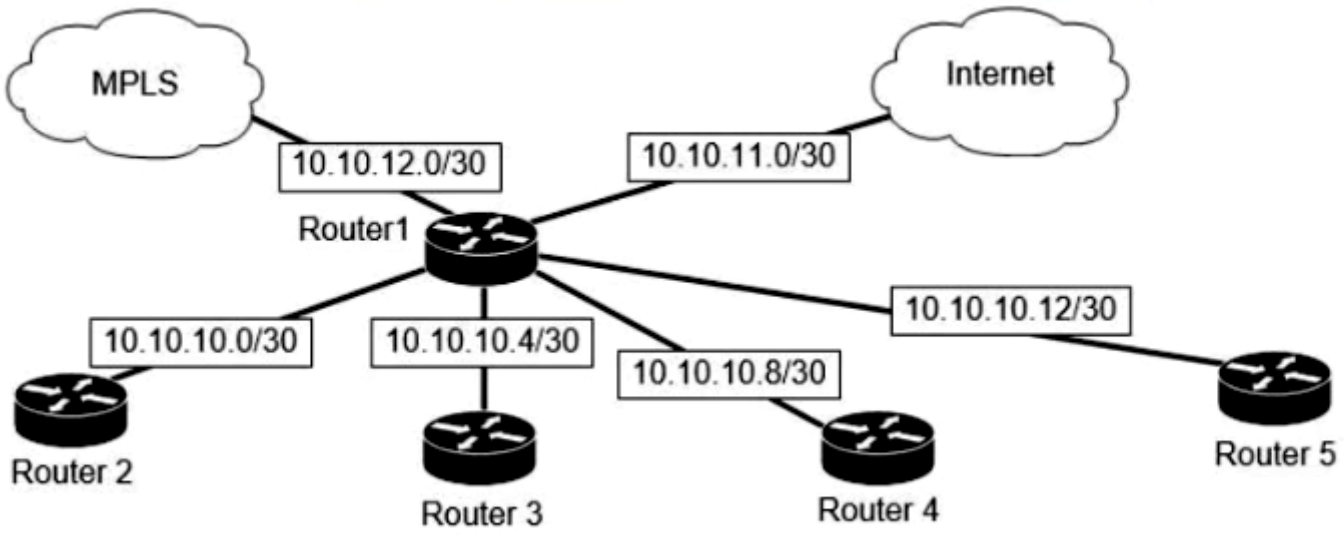
upvoted 6 times

Customexit 10 months, 3 weeks ago

IIRC, if you decided to enter the local router's interface, you would put g0/0 in this case.
But the answers use the next-hop.

upvoted 3 times

Question #449 *Topic 1*




```
Router1# show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0
     209.165.200.0/27 is subnetted, 1 subnets
B       209.165.200.224 [20/0] via 10.10.12.2, 03:22:14
     209.165.201.0/27 is subnetted, 1 subnets
B       209.165.201.0 [20/0] via 10.10.12.2, 02:26:33
     209.165.202.0/27 is subnetted, 1 subnets
B       209.165.202.128 [20/0] via 10.10.12.2, 02:26:03
     10.0.0.0/8 is variably subnetted, 10 subnets, 4 masks
O       10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O       10.10.13.128/28 [110/2] via 10.10.10.5, 00:00:12, GigabitEthernet0/1
O       10.10.13.144/28 [110/2] via 10.10.10.9, 00:01:57, GigabitEthernet0/2
O       10.10.13.160/29 [110/2] via 10.10.10.5, 00:00:12, GigabitEthernet0/1
O       10.10.13.208/29 [110/2] via 10.10.10.13, 00:01:57, GigabitEthernet0/3
S*   0.0.0.0/0 [1/0] via 10.10.11.2
```

Refer to the exhibit. Which next-hop IP address does Router1 use for packets destined to host 10.10.13.158?

A. 10.10.10.9

B. 10.10.10.5

C. 10.10.11.2

D. 10.10.12.2

Correct Answer: *A*

TechJ Highly Voted 3 months, 2 weeks ago

Selected Answer: A

I cant believe there is multiple people answer B, how is the host address 158 included in 10.10.13.160 network address????

upvoted 5 times

mda2h Most Recent 2 months, 2 weeks ago

Selected Answer: B

basic subnetting

upvoted 1 times

Brocolee 2 months ago

It is so basic and you still got it wrong. Lol.

upvoted 5 times

shumps 4 months ago

B is wrong because it starts from 160-168 so it has passed the network we want. the increment of it is 8 subtract 2.

upvoted 1 times

yuh 4 months, 1 week ago

Selected Answer: A

The correct answer is A.
144/28 145-158 (Broadcast 159)
The options below do not cover 10.10.13.158.
128/28 129-142 (Broadcast 143)
160/29 161-166 (Broadcast 167)
208/29 209-214 (Broadcast 215)

upvoted 1 times

Hope_12 4 months, 1 week ago

Selected Answer: A

10.10.13.144/28 via 10.10.10.9
inc = 16

10.10.13.144(NetAdd) - 10.10.13.159(BroadAdd)
10.10.13.168

10.10.13.145-10.10.13.158 USABLE HOSTS
packet 10.10.130.158 is in range

10.10.13.160/29 via 10.10.10.5
inc = 8

10.10.13.160(NetAdd) - 10.10.13.167(BroadAdd)
10.10.13.168

10.10.13.161-10.10.13.166 USABLE HOSTS
packet 10.10.130.158 is not in range

Answer: A. 10.10.10.9

upvoted 1 times

Hope_12 4 months, 1 week ago

packet 10.10.13.158

upvoted 1 times

bisiyemo1 4 months, 2 weeks ago

Selected Answer: B

B is the correct answer based on long prefix rule. 10.0.13.160/29 will be considered

upvoted 1 times

raul_kapone 3 weeks, 1 day ago

From:
10.10.13.160/29

Last octet in binary:
10.10.13.10100/000

Address Range:
10.10.13.10100/000 = 10.10.13.160
10.10.13.10100/001 = 10.10.13.161
10.10.13.10100/010 = 10.10.13.162
10.10.13.10100/011 = 10.10.13.163
10.10.13.10100/100 = 10.10.13.164
10.10.13.10100/101 = 10.10.13.165
10.10.13.10100/110 = 10.10.13.166
10.10.13.10100/111 = 10.10.13.167

The subnet "10.10.13.160/29" doesn't contain 10.10.13.158
So, the router cannot find a route for 10.10.13.158 in the route 10.10.13.160/29
So, B is incorrect.

upvoted 1 times

ac89l 4 months, 2 weeks ago

do you know even how to calculate subnets ?

upvoted 4 times

Channaveera 6 months ago

IP 0.10.13.158 has presence in both the networks. 10.0.13.160/29 and 10.10.13.144/28, so 10.0.13.160/29 is the longest prefix

upvoted 2 times

Myth1977 7 months, 2 weeks ago

A is correct. Longest prefix match

upvoted 2 times

shabby999 7 months, 3 weeks ago

answer is B

upvoted 3 times

nathnotnut 6 months, 2 weeks ago

it's A, how can we delete your answer here

upvoted 2 times

iMo7ed 6 months, 3 weeks ago

No, it's A (Longest prefix match)

upvoted 1 times

Nnandes 1 year, 4 months ago

A is the correct.

upvoted 4 times

Question #450 *Topic 1*

```
RIP        10.1.1.16/28[120/5]    via   F0/0
OSPF       10.1.1.0/24 [110/30]   via   F0/1
OSPF       10.1.1.0/24 [110/40]   via   F0/2
EIGRP      10.1.0.0/26 [90/20]    via   F0/3
EIGRP      10.0.0.0/8  [90/133]   via   F0/4
```

Refer to the exhibit. Packets received by the router from BGP enter via a serial interface at 209.165.201.1. Each route is present within the routing table. Which interface is used to forward traffic with a destination IP of 10.1.1.19?

A. F0/0

B. F0/1

C. F0/4

D. F0/3

Correct Answer: *A*

DUMPledore 7 months, 3 weeks ago

Selected Answer: A

this if for "forwarding traffic" so longest prefix or more specific route

upvoted 4 times

Goh0503 12 months ago

Correct Answer: A

upvoted 1 times

DANAAH 8 months, 3 weeks ago

could you explain how to solve this question in detail please?

upvoted 1 times

rijstraket 8 months ago

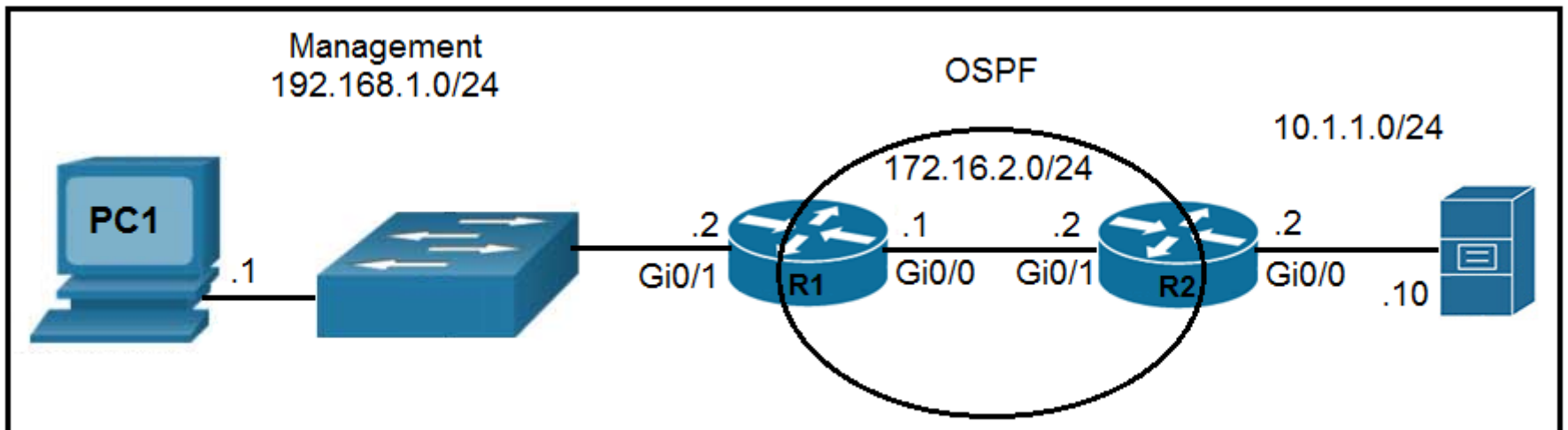
When multiple routes are present that match the destination address, always check for the "more-specific" route first. The smallest subnet (or highest/longest prefix) would be chosen.

upvoted 4 times

diudiuQIdama 8 months, 2 weeks ago

longest prefix

upvoted 2 times



During outage

```
R1#show ip route 10.1.1.10
%Network not in table
```

Normal operation

```
R1#show ip route 10.1.1.10
Routing entry for 10.1.1.0/24
Known via "ospf 1", distance 110, metric 2, type intra area
  Last update from 172.16.2.2 on GigabitEthernet0/0, 00:00:18 ago
  Routing Descriptor Blocks:
  * 172.16.2.2, from 10.1.1.10, 00:00:18 ago, via GigabitEthernet0/0
        Route metric is 2, traffic share count is 1
```

Refer to the exhibit. Which route must be configured on R1 so that OSPF routing is used when OSPF is up, but the server is still reachable when OSPF goes down?

A. ip route 10.1.1.10 255.255.255.255 gi0/0 125

B. ip route 10.1.1.0 255.255.255.0 172.16.2.2 100

C. ip route 10.1.1.0 255.255.255.0 gi0/1 125

D. ip route 10.1.1.10 255.255.255.255 172.16.2.2 100

Correct Answer: *A*
This is an example of a floating static route when the Administrative Distance must be greater than the primary route. Currently the OSPF AD for the route is 110, so if that route was to go away then this route with an AD of 125 would be used.

Netcmd Highly Voted 10 months ago

Selected Answer: A

Answer C is wrong because it uses the wrong interface id

upvoted 6 times

soRwatches 6 months ago

the interface used is the R1 exit interface. so A is correct.

upvoted 1 times

shumps Most Recent 3 weeks ago

D is also correct but interface is mostly preferred and reliable. so A is correct

upvoted 1 times

Shanku97 2 weeks, 2 days ago

A HAS A HIGHER AD THAN D

upvoted 1 times

mda2h 2 months, 2 weeks ago

Selected Answer: A

next hop can be specified in 2 ways:
- IP address: must use IP of the next hop router
- Interface: must use local interface connected to the next hop router

upvoted 1 times

vsm97 10 months ago

why is it 255.255.255.255 when the network is /24? Isnt that 255.255.255.0?

upvoted 3 times

bikila123 1 month ago

Route to one host is called host route,

upvoted 1 times

Hope_12 4 months, 1 week ago

When you are using a host route or specific route.
You can use the 255.255.255.255 /32.
You use /24 if you are pertaining to a network route.

upvoted 1 times

cormorant 10 months, 2 weeks ago

this demonic detail answers the question: gi0/0
this is teh interface towards the fateful server 1. the ip route syntax is destination + netmask + next hop. the latter can be replaced bythe interfaceif you want to reach a destination in a more direct manner

upvoted 1 times

Customexit 10 months, 3 weeks ago

Selected Answer: A

Answer is A.

At a glance, B has a lower manually set AD of 100.
C command is wrong anyway, if you want to use the interface name instead of the next hop, you use the local router's interface which is R1's g0/0. G0/1 is the next hop to R2.

D has a lower AD than 110.

A has the correct command with a static host route directly to the server, a /32 subnet (host route), the local router's exit interface of g0/0, and a higher manually set AD of 125.

upvoted 3 times

RougePotatoe 10 months, 3 weeks ago

Selected Answer: C

Answer is C because we need to configure a floating static route. Cannot use A because that will configure a static route as OSPF does not have a entry for 10.1.1.10 only the network 10.1.1.0/24. In order for a static route to become a floating static route we need the AD to be higher than the OSPF routing protocol so it will not be put into the routing table. If you configure A you will create a static route for 10.1.1.10 in your routing table which is wrong.

upvoted 2 times

splashy 10 months, 1 week ago

10.1.1.0 /24 is reachable via ospf -> known via ospf 1
Only the server needs to be reachable if ospf 1 should go down
So A

upvoted 4 times

RougePotatoe 10 months ago

By configuring a static address to a /32 address you would create an entry in the routing table. When the router tries to route to the server network it will look for the longest matching prefix which would be the /32 (statically configured route). So it would by pass OSPF because the OSPF network is /24. Although C isn't right either since the interface is incorrect.

upvoted 2 times

RHER 4 months ago

como vas a salir por la interfaz g0/0, si el proximo salto es g0/1 c es correcta

upvoted 1 times

RougePotatoe 10 months ago

I mean server not server network.

upvoted 1 times

RougePotatoe 10 months ago

Looking back while A is not the right answer it is the best answer.

upvoted 2 times

Question #452 *Topic 1*

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       p - periodic downloaded static route

Gateway of last resort is not set
     10.0.0.0/24 is subnetted, 5 subnets
D       10.1.2.0/24 [90/2170112] via 10.165.20.226, 00:01:30, Serial0/0
D       10.1.3.0/24 [90/2170112] via 10.165.20.226, 00:01:30, Serial0/0
D       10.1.2.0/25 [90/2170112] via 10.165.20.126, 00:01:30, Serial0/0
D       10.1.3.0/25 [90/2170112] via 10.165.20.146, 00:01:30, Serial0/0
D       10.1.4.0/24 [90/2170112] via 10.165.20.156, 00:01:30, Serial0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.18.10.0/24 is directly connected, GigabitEthernet0/0
       192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.18.11.0/24 is directly connected, GigabitEthernet0/1
    10.165.20.0/24 is variably subnetted, 2 subnets, 2 masks
C   10.165.20.224/24 is directly connected, Serail0/0
S       10.1.12.112/28 [1/0] via 10.165.20.166
```

Refer to the exhibit. What is the next hop for traffic entering R1 with a destination of 10.1.2.126?

A. 10.165.20.126

B. 10.165.20.146

C. 10.165.20.166

D. 10.165.20.226

Correct Answer: *A*

Liquid_May 3 weeks, 4 days ago

Selected Answer: C

The last route should be the one that is used, because it is the longest prefix that will match the ip. Therefore, C would be the answer in this case.

upvoted 2 times

bikila123 1 month ago

Answer iw C
Longest prefix match with Last usable host in /25 network

upvoted 2 times

kobisiva 4 weeks, 1 day ago

thats wrong, check ip address

upvoted 1 times

kishan365 2 months ago

Can anyone tell me why not C? As it has the highest prefix of 28 as well as the range is from 10.1.12.112--10.1.12.128. The destination(.126) ofcourse lies within this range.

upvoted 1 times

kishan365 2 months ago

sorry my bad. I misread the ip..

upvoted 1 times

yuh 4 months, 1 week ago

Selected Answer: C

I think C.
Static route for 10.1.12.112/28.
range 10.1.12.113-10.1.12.126
longestmatch and in range

upvoted 2 times

yuh 4 months, 1 week ago

sorry i misread the address...
A is right.

upvoted 2 times

fak3zito 5 months ago

D is the correct answer,the static have the longest prefix, and btw has a ad of 1.

upvoted 1 times

MRSCARLet 4 months, 1 week ago

the static is 10.1.12.112/28, /28 is the longest but the destination is 10.1.2.126.
The correct way is via 10.1.2.0/25

upvoted 1 times

Ciscoman021 5 months, 1 week ago

Selected Answer: A

A is correct.

upvoted 2 times

Yannik123 5 months, 3 weeks ago

Selected Answer: A

Longest prefix. An x.x.x.126 is the last useable address in a /25 subnet.

upvoted 4 times

lucantonelli93 6 months, 2 weeks ago

Selected Answer: A

The correct answer it's A

upvoted 1 times

iMo7ed 6 months, 3 weeks ago

Selected Answer: D

D is the correct answer

upvoted 1 times

Ciscoman021 5 months, 1 week ago

why? can you explain me please? 10.1.2.0/25 is too here. thats means 10.1.2.1 - 10.1.2.126
with next hop 10.165.20.126

upvoted 1 times

Xenon1337 6 months, 3 weeks ago

correction, its A, the route with longest prefix is chosen if multiple routes are available in this case /25

upvoted 5 times

Question #453 *Topic 1*

```
R1# show ip route | begin gateway
Gateway of last resort is not set
        172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.0/24 is directly connected, FastEthernet0/0
L       172.16.1.1/32 is directly connected, FastEthernet0/0
EX      172.16.2.0/24 [170/2] via 207.165.200.250, 00:00:25, Serial0/0/0
O       192.168.1.0/24 [110/84437] via 207.165.200.254, 00:00:17, Serial0/0/1
D       192.168.2.0/24 [90/184437] via 207.165.200.254, 00:00:15. Serial0/0/1
E1      192.168.3.0/24 [110/1851437] via 207.165.200.254, 00:00:19, Serial0/0/1
        207.165.200.0/24 is variably subnetted, 4 subnets, 2 masks
C       207.165.200.248/30 is directly connected, Serial0/0/0
L       207.165.200.249/32 is directly connected, Serial0/0/0
C       207.165.200.252/30 is directly connected, Serial0/0/1
L       207.165.200.253/32 is directly connected, Serial0/0/1
```

Refer to the exhibit. Which prefix did router R1 learn from internal EIGRP?

A. 192.168.3.0/24

B. 192.168.1.0/24

C. 172.16.1.0/24

D. 192.168.2.0/24

Correct Answer: *D*

Mili2023 7 months, 3 weeks ago

you can also get the answer as the AD for internal EIGRP is 90. and External in 170 so in the question they have asked the internal EIGRP which is only with ip address in D.
the AD for OSPF is110 so options A and B is out of question anyway!

upvoted 3 times

Panda_man 9 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 3 times

cormorant 10 months, 2 weeks ago

internal EIGRP = D

upvoted 2 times

motop9 11 months, 2 weeks ago

EX - EIGRP external
E1 - OSPF external type 1, E2 - OSPF external type 2

upvoted 3 times

razif 11 months, 2 weeks ago

should be learn from EXTERNAL EIGRP? instead of internal?

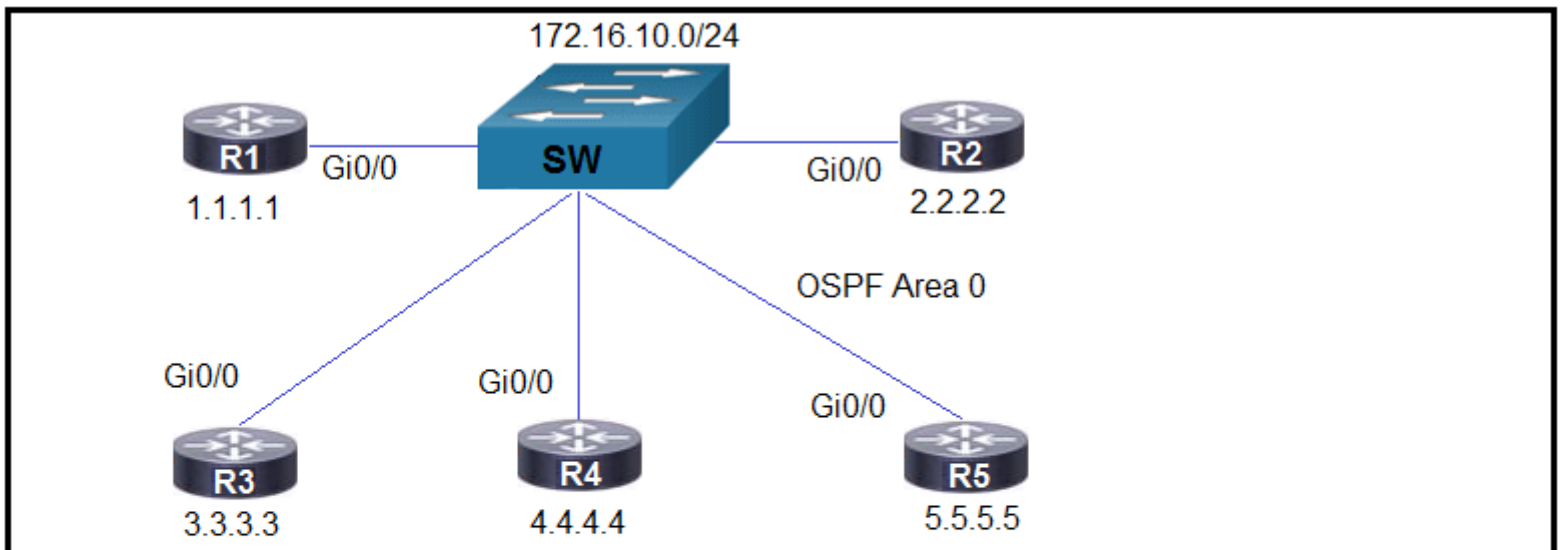
upvoted 2 times

Customexit 10 months, 3 weeks ago

The question asks for internal EIGRP. That's a code of D in the routing table.

upvoted 1 times

Question #454 *Topic 1*




```
R3# show ip ospf neighbor

Neighbor ID   Pri    State           Dead Time  Address       Interface
1.1.1.1         1    2WAY/DROTHER    00:00:32   172.16.10.1   GigabitEthernet0/0
2.2.2.2         1    2WAY/DROTHER    00:00:33   172.16.10.2   GigabitEthernet0/0
4.4.4.4         1    FULL/BDR        00:00:31   172.16.10.4   GigabitEthernet0/0
5.5.5.5         1    FULL/DR         00:00:30   172.16.10.5   GigabitEthernet0/0
```

Refer to the exhibit. R5 is the current DR on the network, and R4 is the BDR. Their interfaces are flapping, so a network engineer wants the OSPF network to elect a different DR and BDR. Which set of configurations must the engineer implement?

A. R4(config)#interface gi0/0 R4(config-if)#ip ospf priority 20 R5(config)#interface gi0/0 R5(config-if)#ip ospf priority 10

B. R5(config)#interface gi0/0 R5(config-if)#ip ospf priority 120 R4(config)#interface gi0/0 R4(config-if)#ip ospf priority 110

C. R3(config)#interface gi0/0 R3(config-if)#ip ospf priority 255 R2(config)#interface gi0/0 R2(config-if)#ip ospf priority 240

D. R2(config)#interface gi0/0 R2(config-if)#ip ospf priority 259 R3(config)#interface gi0/0 R3(config-if)#ip ospf priority 256

Correct Answer: *C*

mda2h 2 months, 2 weeks ago

Selected Answer: C

Max priority is 255 and all routers here have priority 1. DR/BDR election's based on highest priority!

upvoted 3 times

4aynick 4 months, 3 weeks ago

Selected Answer: C

highest metrik is DR.
max 255

upvoted 4 times

Swiz005 5 months, 2 weeks ago

Selected Answer: C

The answer is C - manually forcing the priority

upvoted 2 times

RougePotatoe 10 months, 3 weeks ago

Selected Answer: A

This really depends on what the question is trying to ask.
Yes option C will also achieve the same effect but you are manually forcing R3 and R2 to become DR and BDR. The question only asked for you to have OSPF elect a different DR and BDR so I think A fits best as it will leave OSPF to elect a DR and BDR instead of you basically forcing it.

upvoted 3 times

RougePotatoe 10 months, 3 weeks ago

I messed up OSPF's default priority value is 1 so A would do nothing. ANSWER IS C.

upvoted 4 times

arenjenkins 11 months, 3 weeks ago

why not D?

upvoted 1 times

EngrRex 11 months, 3 weeks ago

OSPF priority range is 0-255. D is out of range

upvoted 9 times

MikD4016 11 months, 2 weeks ago

because the value can go from 0 to 255 (default = 1): with 0 you avoid the election to DR / BDR, with higher values you can drive it at will. If all the routers on the LAN have priority = 0, OSPF will not work

upvoted 6 times

Question #455 *Topic 1*

```
R1# show ip route
    Codes:
    C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP, D -
    EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA
    external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type
    1, E2 - OSPF external type 2, E - EGP
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default,
    U - per-user static route, o - ODR
Gateway of last resort is not set
C     10.0.0.0/8 is directly connected, Loopback0
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O     10.0.1.3/32 [110/100] via 10.0.1.100, 00:39:08, Serial0
C     10.0.1.0/24 is directly connected, Serial0
O     10.0.1.5/32 [110/5] via 10.0.1.50, 00:39:08, Serial0
O     10.0.10.0/24 [110/10] via 10.0.1.4, 00:39:08, Gigabit Ethernet 0/0
D     10.0.10.0/24 [90/10] via 10.0.1.5, 00:39:08, Gigabit Ethernet 0/1
```

Refer to the exhibit. Web traffic is coming in from the WAN interface. Which route takes precedence when the router is processing traffic destined for the LAN network at 10.0.10.0/24?

A. via next-hop 10.0.1.5

B. via next-hop 10.0.1.4

C. via next-hop 10.0.1.50

D. via next-hop 10.0.1.100

Correct Answer: *A*

RougePotatoe Highly Voted 10 months, 3 weeks ago

I really need someone to explain to me how there is an OSPF and EIGRP entry for the same network in this routing table.

upvoted 8 times

RougePotatoe 9 months, 4 weeks ago

Since everyone who replied so far doesn't seem to understand my question let me clarify. IRL you should only get one routing entry per network route from the show routing table command; unless you configured load balancing. Obliviously EIGRP has lower AD than OSPF which is why only the EIGRP route should be shown in this show command. I'm asking how on earth could there be an OSPF and EIGRP entry in this show command when there should only be 1 entry for the network route as to my knowledge and google there doesn't seem to be a way you can load balance between 2 routing protocols.

upvoted 4 times

mda2h 2 months, 2 weeks ago

Let me repeat on behalf of the comment above:
"Plain and simple: This is a cooked up table. There can't be"

upvoted 1 times

networkin 9 months, 1 week ago

Plain and simple: This is a cooked up table. There can't be.

upvoted 10 times

victor520 10 months, 1 week ago

OSPF AD=110 EIGRP AD=90 ,so i think choose A

upvoted 2 times

RougePotatoe 9 months, 4 weeks ago

You didn't answer my question. IRL you wouldn't event see the OSPF route because the router would've selected the EIGRP route already due to it having a lower AD. So this show command is unrealistic.

upvoted 2 times

soRwatches 6 months ago

relax, this made just to test the knowledge. just answer the question then your good to go the next question. don't over think.

upvoted 3 times

Myth1977 Most Recent 7 months, 2 weeks ago

Longest prefix is the same for both route on 10.0.10 network. AD takes the charge to determine the route

upvoted 4 times

Question #456 *Topic 1*

```
Gateway of last resort is 172.16.2.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C     10.10.8.0/28 is directly connected, GigabitEthernet0/0/2
C     10.10.10.0/24 is directly connected, GigabitEthernet0/0/0
L     10.10.10.3.32 is directly connected, GigabitEthernet0/0/0

    172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S     172.16.1.33/32 is directly connected, GigabitEthernet0/0/1
C     172.16.2.0/23 is directly connected, GigabitEthernet0/0/1
L     172.16.2.1/32 is directly connected, GigabitEthernet0/0/1
S*  0.0.0.0/0 [1/0] via 172.16.2.2
```

Refer to the exhibit. A packet sourced from 10.10.10.1 is destined for 10.10.8.14. What is the subnet mask of the destination route?

A. 255.255.254.0

B. 255.255.255.240

C. 255.255.255.248

D. 255.255.255.252

Correct Answer: *B*

Tomasek1234 6 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 3 times

iMo7ed 6 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

daddydagoth 6 months, 3 weeks ago

Selected Answer: B

The destination is the last host of the 10.10.8.0/28 subnet. So the mask of the destination is /28 aka 255.255.255.240

upvoted 4 times

sdmejia01 7 months, 1 week ago

Correct Answer is B. 255.255.255.240, means /28. The IP 10.10.8.14 falls within the 10.10.8.0/28 range, which is: 10.10.8.0 network ID - 10.10.8.15 Broadcast IP.

upvoted 3 times

Goena 7 months, 3 weeks ago

Selected Answer: A

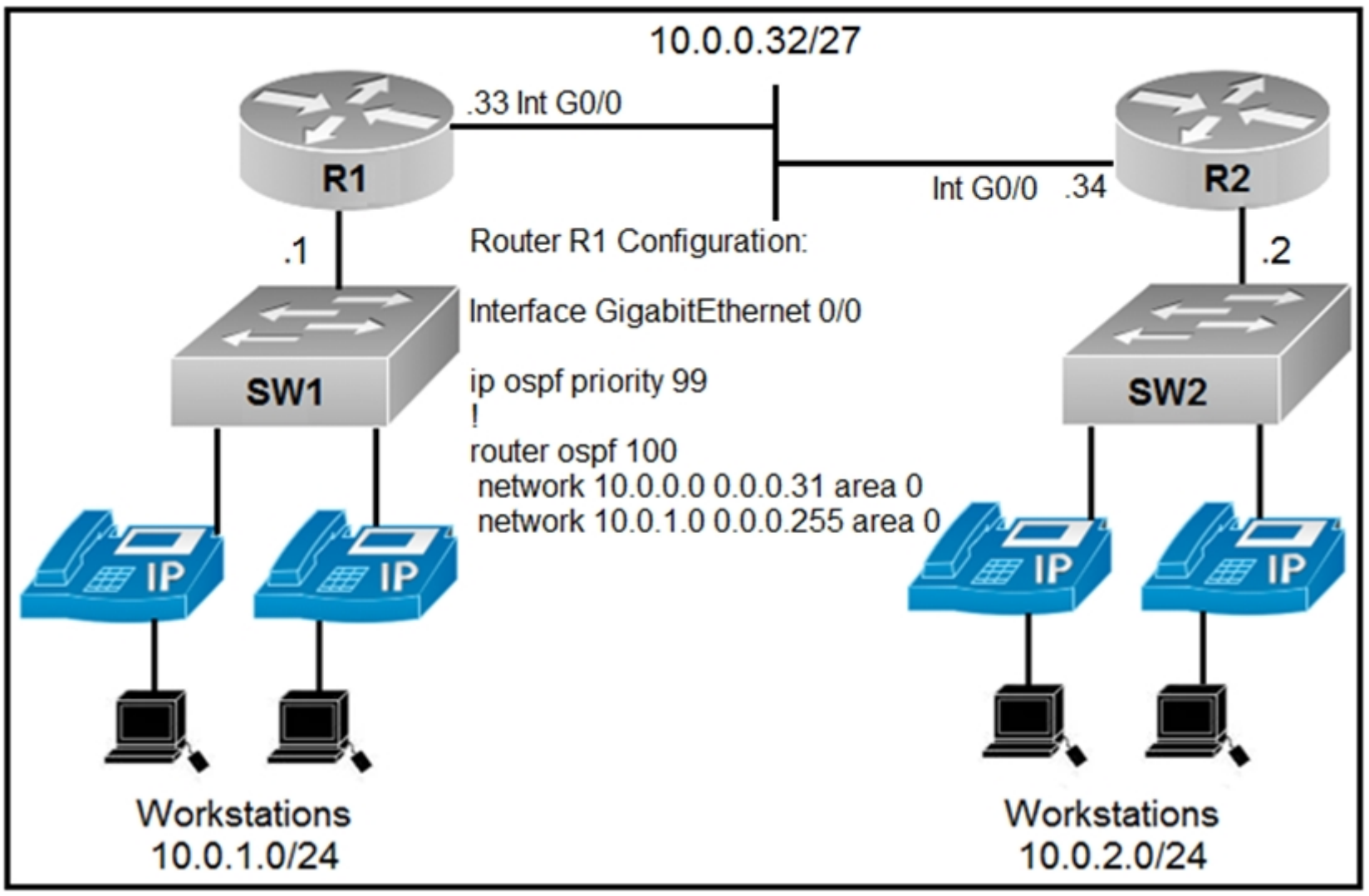
Answer is A
The destination route is default route 172.16.2.2.
172.16.2.0/23 is directly connected g0/0/1
255.255.254.0

upvoted 2 times

daddydagoth 6 months, 3 weeks ago

Wrong! The destination is the last host of the 10.10.8.0/28 subnet. So the mask of the destination is /28 aka 255.255.255.240

upvoted 3 times



Refer to the exhibit. An engineer must configure router R2 so it is elected as the DR on the WAN subnet. Which command sequence must be configured?

A. interface gigabitethernet0/0 ip address 10.0.0.34 255.255.255.248 ip ospf priority 0

B. interface gigabitethernet0/0 ip address 10.0.0.34 255.255.255.224 ip ospf priority 100

C. interface gigabitethernet0/0 ip address 10.0.1.1 255.255.255.0 ip ospf priority 255

D. interface gigabitethernet0/0 ip address 10.0.1.1 255.255.255.224 ip ospf priority 98

Correct Answer: *B*

shumps 3 weeks ago

please pay close attention to details 10.0.0.34

upvoted 1 times

molly_zheng 3 months, 4 weeks ago

why not c?

upvoted 3 times

dropspablo 3 months, 3 weeks ago

Because of the IP Address configuration, it needs to be indented from the 10.0.0.32/27 network (host 10.0.0.33 to 10.0.0.62 - Broadcast 10.0.0.63).
Prefix 27 minus 32 = 5 left over used for host (1=2 - 2=4 - 3=8 - 4=16 - 5=32), i.e. we have a range of 32 hosts available in each subnet:
Subnet 10.0.0.0 - 10.0.0.32 - 10.0.0.64 - 10.0.0.96 - 10.0.0.128 - 10.0.0.160 - 10.0.0.192 - 10.0.0.224.

upvoted 3 times

Goena 8 months, 2 weeks ago

Selected Answer: B

Answer B is correct:
Network on G0/0 is 10.0.0.32/27 ===> 10.0.0.34 255.255.255.224 with priority higher then default (1) , 100

upvoted 2 times

IFBBPROSALCEDO 2 months ago

How did you get 10.0.0.34? I can if the answer is 10.0.0.33 but not 34. Thank you for your time in advance.

upvoted 1 times

IFBBPROSALCEDO 2 months ago

Nevermind, I just saw the .34 next to R2!! I really need to pay attention to detail!

upvoted 3 times

Question #458 *Topic 1*

An engineer is configuring router R1 with an IPv6 static route for prefix 2019:C15C:0CAF:E001::/64. The next hop must be 2019:C15C:0CAF:E002::1. The route must be reachable via the R1 Gigabit 0/0 interface. Which command configures the designated route?

A. R1(config-if)#ip route 2019:C15C:0CAF:E001::/64 GigabitEthernet 0/0

B. R1(config)#ip route 2019:C15C:0CAF:E001::/64 GigabitEthernet 0/0

C. R1(config-if)#ipv6 route 2019:C15C:0CAF:E001::/64 2019:C15C:0CAF:E002::1

D. R1(config)#ipv6 route 2019:C15C:0CAF:E001::/64 2019:C15C:0CAF:E002::1

Correct Answer: *D*

Swiz005 Highly Voted 5 months, 2 weeks ago

Selected Answer: D

C is incorrect because the command is entered in the interface R1(config-if). The default route must be entered in the glocal config. Making D the correct answer.

upvoted 14 times

Philipli308 Most Recent 2 weeks, 1 day ago

C must be wrong, cause who tell you the R1(config-if) must be the interface G0/0?

upvoted 1 times

Shanku97 2 weeks, 2 days ago

WHY NOT B,

IT'S CONFIRUED IN GLOBAL CONFIG MODE, IT USED DESTINATION IP AND EXIT INTEREFACE .

PLEASE EXPLAIN SOMEONE

upvoted 1 times

ananinamia 1 week, 6 days ago

where are the source and dest?

upvoted 1 times

BettoAtzeni 1 month, 2 weeks ago

ChatGPT:
Here's how you would configure the IPv6 static route in global configuration mode:

Enter global configuration mode:

R1# configure terminal

Add the IPv6 static route using the ipv6 route command:

R1(config)# ipv6 route 2019:C15C:0CAF:E001::/64 2019:C15C:0CAF:E002::1 Gigabit0/0

Exit configuration mode and save the configuration:

R1(config)# end
R1# write memory

This will add the specified IPv6 static route to the routing table, and the router will forward packets for the destination prefix 2019:C15C:0CAF:E001::/64 to the next hop address 2019:C15C:0CAF:E002::1 via the Gigabit0/0 interface.

upvoted 1 times

BettoAtzeni 1 month, 2 weeks ago

In Packet Tracer, as with most Cisco routers, the ipv6 route command should be configured in global configuration mode. This command is used to add an IPv6 static route in the routing table of the router, so it should be applied in the global context to affect the entire router's behavior.

upvoted 1 times

paolino555 2 months ago

Selected Answer: C

it says "The route must be reachable via the R1 Gigabit 0/0 interface."

upvoted 1 times

mda2h 2 months, 2 weeks ago

Selected Answer: D

the ipv6 instead of ip got me good with this one

upvoted 1 times

Olebogeng_G 3 months, 1 week ago

Admin please input your explanation for this question. I'm finally smashing Routing but questions like these will put us off.

upvoted 1 times

loco_desk 6 months ago

Selected Answer: C

It's an ipv6 address and the Answer says this : "The route must be reachable via the R1 Gigabit 0/0 interface." Then then you need to ingres the comand on G0/0 interface or in global config but adding G0/0 . C is correct.

upvoted 3 times

ukguy 8 months, 2 weeks ago

bcz next hop address is global unicast address not link local address

upvoted 1 times

EEGentle 10 months, 3 weeks ago

shouldn't be R1(config)#ipv6 route 2019:C15C:0CAF:E001::/64 g0/1 2019:C15C:0CAF:E002::1 ?

upvoted 3 times

daddydagoth 6 months, 3 weeks ago

A fully specified route would be better, considering the formatting of the question but I suppose the one we were given is the next best, especially considering that the rest of the asnwers are blatantly wrong.

upvoted 1 times

r0m 11 months, 1 week ago

why not C?

upvoted 1 times

Customexit 11 months ago

Because C shows the command being entered on an interface (config-if).

upvoted 6 times

Peter_panda 5 months, 2 weeks ago

C is also valid. Global configuration mode commands (ipv6 route) can be given in interface configuration mode (but not the other way around). I doubt that at the exam they will ask us to choose between exactly these correct options, probably the question here is defective.

upvoted 1 times

loco_desk 6 months ago

The Answer says this "The route must be reachable via the R1 Gigabit 0/0 interface." Then then you need to ingres the comand on G0/0 interface. C is correct.

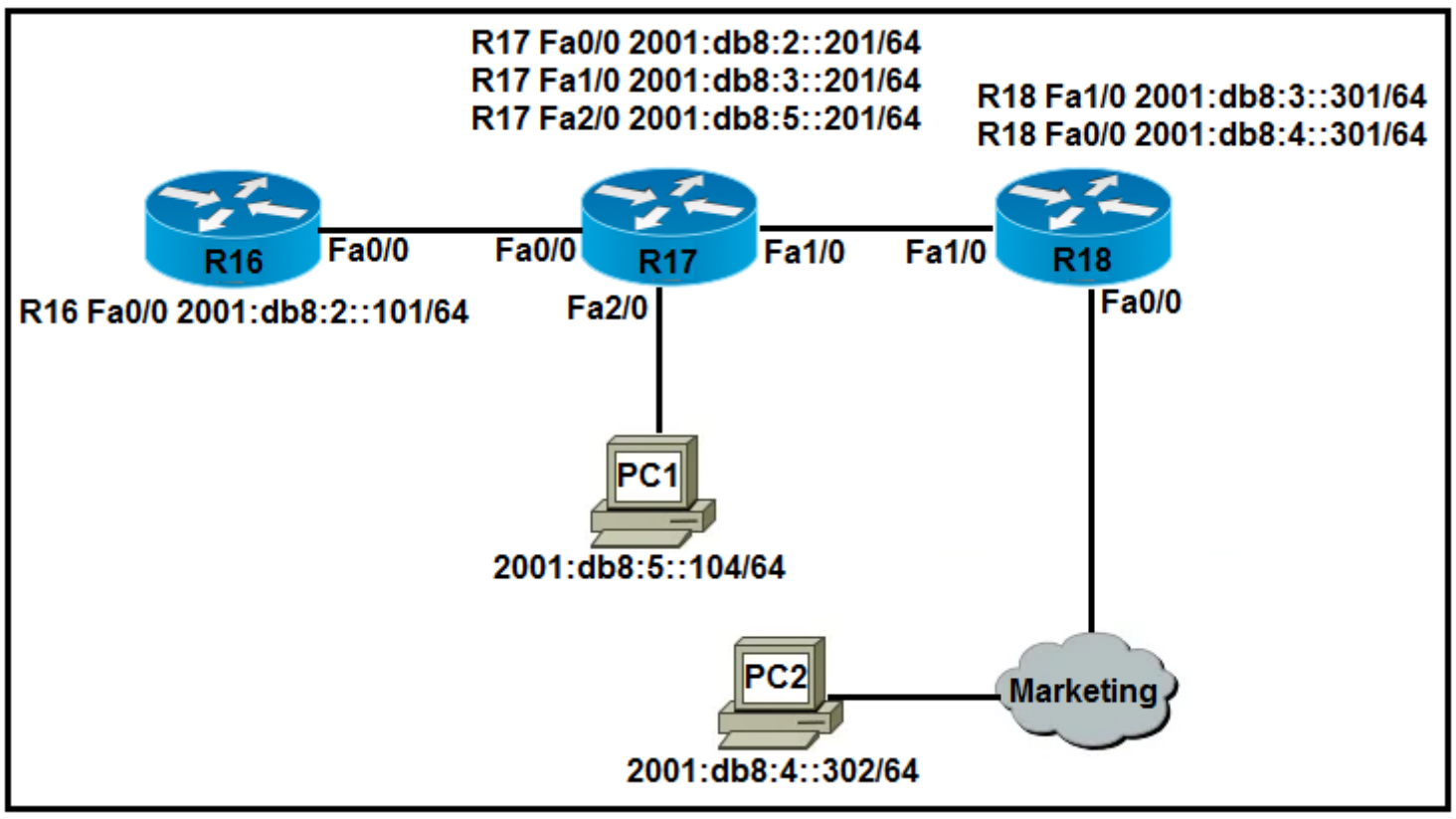
upvoted 1 times

soRwatches 6 months ago

nope, static route must be configure in global configuration mode. Answer is D which is definietly reachable by G0/0 interface.

upvoted 3 times

Question #459 *Topic 1*



Refer to the exhibit. Which IPv6 configuration is required for R17 to successfully ping the WAN interface on R18?

A. R17# ! no ip domain lookup ip cef ipv6 cef ! interface FastEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:2::201/64 ! Interface FastEthernet1/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:3::201/64 ! no cdp log mismatch duplex ipv6 route 2001:DB8:4::/64 2001:DB8:4::302

B. R17# ! no ip domain lookup ip cef ipv6 unicast-routing ! interface FastEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:2::201/64 ! Interface FastEthernet1/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:3::201/64 ! no cdp log mismatch duplex ipv6 route 2001:DB8:4::/64 2001:DB8:3::301

C. R17# ! no ip domain lookup ip cef ! interface FastEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:3::201/64 ! Interface FastEthernet1/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:2::201/64 ! no cdp log mismatch duplex ipv6 route 2001:DB8:4::/64 2001:DB8:5::101

D. R17# ! no ip domain lookup ip cef ipv6 unicast-routing ! interface FastEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:2::201/64 ! Interface FastEthernet1/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:3::201/64 ! no cdp log mismatch duplex ipv6 route 2001:DB8:4::/64 2001:DB8:2::201

Correct Answer: *B*

tui9 Highly Voted 8 months, 4 weeks ago
A whole load of useless text, check the ipv6 route command in the last bit. :)
upvoted 29 times

[Removed] 2 months, 3 weeks ago
Exactly! :)
upvoted 3 times

bisiyemo1 5 months, 3 weeks ago
Good of you man
upvoted 3 times

MEDO95 8 months ago
man u saved my life. thx!
upvoted 6 times

ananinamia 1 week, 6 days ago
How i did not get it?
upvoted 1 times

soRwatches Highly Voted 6 months ago
if you will read all the answers in the actual exam you will be waste alot of time.
upvoted 7 times

shumps Most Recent 1 week, 1 day ago
ipv6 route 2001:DB8:4::/64 2001:DB8:3::301 quickest way is to pick route command as pointed out by TUI9

upvoted 1 times

ananinamia 1 week, 6 days ago

it seems so complicated..

upvoted 1 times

lolungos 3 months ago

did anyone else notice is asking for the WAN interface tha is directly connected? Another poorly written question

upvoted 2 times

dropspablo 3 months, 3 weeks ago

Selected Answer: B

Necessary command "ipv6 unicast-routing" for IPv6 routing, with that we have already eliminated from the beginning the letter "A" and "C" that do not have. Without this command, the IPv6 Routing Table is not created.

upvoted 3 times

FALARASTA 4 months, 2 weeks ago

Stupidly worded answers...nkt!

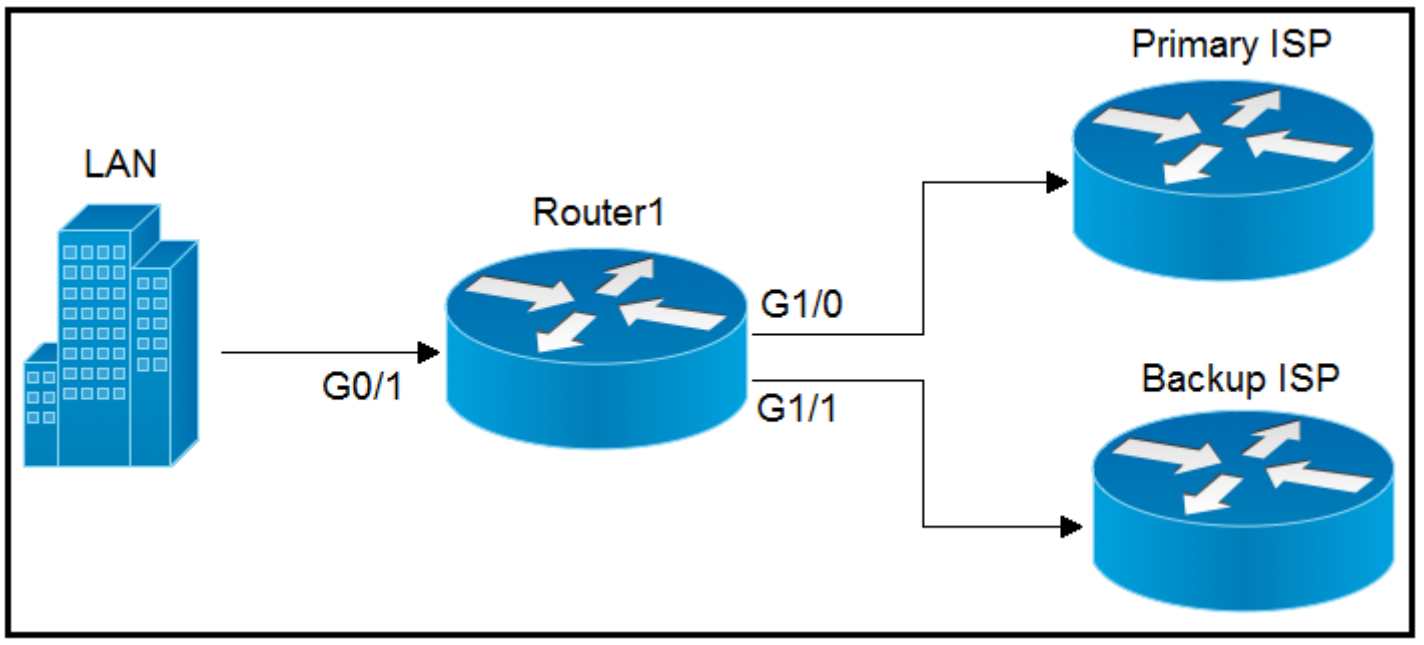
upvoted 2 times

Dutch012 6 months, 1 week ago

the answer fu.cks

upvoted 3 times

Question #460 *Topic 1*



Refer to the exhibit. A company is configuring a failover plan and must implement the default routes in such a way that a floating static route will assume traffic forwarding when the primary link goes down. Which primary route configuration must be used?

A. ip route 0.0.0.0 0.0.0.0 192.168.0.2

B. ip route 0.0.0.0 0.0.0.0 192.168.0.2 GigabitEthernet1/0

C. ip route 0.0.0.0 0.0.0.0 192.168.0.2 floating

D. ip route 0.0.0.0 0.0.0.0 192.168.0.2 tracked

Correct Answer: *A*

The primary route should use the default administrative distance, since the AD for static routes is 1.

Dutch012 Highly Voted 6 months, 3 weeks ago

Selected Answer: A

Not B, A is the answer.

a fully specified route is written like that
dest IP | interface | next-hop

upvoted 11 times

Ceruzka 6 months, 1 week ago

good point. First comes the outgoing intf than comes next hop-IP, not the other way !!

upvoted 1 times

shaney67 Most Recent 3 days, 3 hours ago

answer should be B, how do you know 192.168.0.2 is the primary router?

upvoted 1 times

learntstuff 2 months ago

Tricky. They lead with floating static route then at last second ask about primary route

upvoted 3 times

cengizcihan 2 months, 4 weeks ago

Selected Answer: B

questinon asks "which PRIMARY route configuration must be used? So, it should be B.

upvoted 1 times

TechJ 3 months, 2 weeks ago

100% A, if you really want B to be the correct answer,

it needs to be:
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1/0 192.168.0.2

not:
ip route 0.0.0.0 0.0.0.0 192.168.0.2 GigabitEthernet1/0

notice the different?

upvoted 1 times

dropspablo 3 months, 3 weeks ago

Selected Answer: A

(answer B is wrong)
Unlike IPv6, in IPv4 static routing configuration, for the next hop you either enter an IP Address of the neighboring interface or your local interface, BUT NEVER BOTH. Example:

R1(config)# ip route 192.168.20.0 255.255.255.0 10.12.0.2
Or
R1(config)# ip route 192.168.20.0 255.255.255.0 g0/0

upvoted 1 times

j1mlawton 7 months, 1 week ago

Selected Answer: B

Surely B as it askes for the primary route

upvoted 1 times

Naghini 8 months ago

Why not B?

upvoted 1 times

4aynick 8 months ago

g1/0 is primery

upvoted 1 times

Question #461 *Topic 1*

OSPF must be configured between routers R1 and R2. Which OSPF configuration must be applied to router R1 to avoid a DR'BDR election?

A. router ospf 1 network 192.168.1.1 0.0.0.0 area 0 interface e1/1 ip address 192.168.1.1 255.255.255.252 ip ospf cost 0

B. router ospf 1 network 192.168.1.1 0.0.0.0 area 0 hello interval 15 interface e1/1 ip address 192.168.1.1 255.255.255.252

C. router ospf 1 network 192.168.1.1 0.0.0.0 area 0 interface e1/1 ip address 192.168.1.1 255.255.255.252 ip ospf network broadcast

D. router ospf 1 network 192.168.1.1 0.0.0.0 area 0 interface e1/1 ip address 192.168.1.1 255.255.255.252 ip ospf network point-to-point

Correct Answer: *D*

motop9 Highly Voted 11 months, 2 weeks ago

Point-to-point has no DR/BDR election.

upvoted 13 times

ananinamia 1 week, 6 days ago

thanks

upvoted 1 times

Stichy007 Most Recent 6 months, 3 weeks ago

D is correct

upvoted 1 times

SVN05 7 months, 1 week ago

It was close between A & D. A could have been the answer but cost doesn't affect DR/BDR. If it were "ip ospf priority 0" then yes it would not join DR/BDR election.

upvoted 4 times

perri88 3 months ago

if ip ospf priority was set to 0 on R1, it would have only prevented from being the DR, but it would be the BDR instead.

upvoted 1 times

perri88 3 months ago

sorry, it also prevents the router from being a BDR, you can disregard my previous message

upvoted 1 times

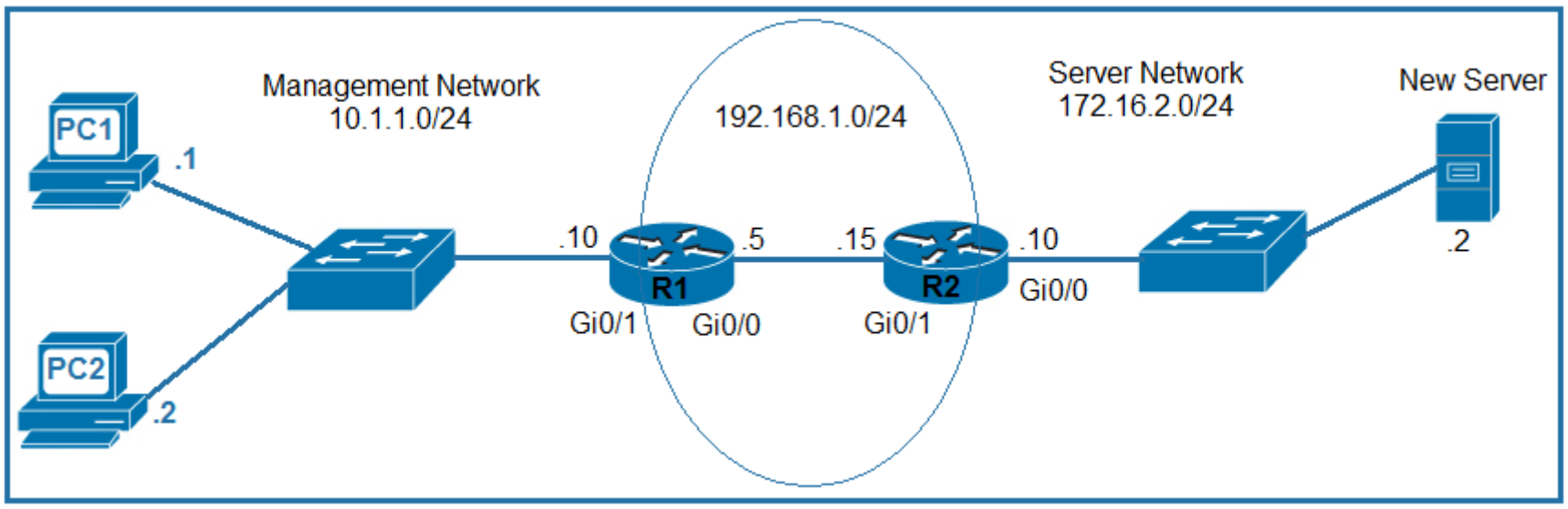
Panda_man 9 months, 3 weeks ago

Selected Answer: D

D is good

upvoted 3 times

Question #462 *Topic 1*



Refer to the exhibit. An engineer is updating the R1 configuration to connect a new server to the management network. The PCs on the management network must be blocked from pinging the default gateway of the new server. Which command must be configured on R1 to complete the task?

A. R1(config)#ip route 172.16.2.0.255.255.255.0 192.168.1.15

B. R1(config)#ip route 172.16.2.2 255.255.255.248 gi0/1

C. R1(config)#ip route 172.16.2.2 255.255.255.255 gi0/0

D. R1(config)#ip route 172.16.2.0 255.255.255.0 192.168.1.5

Correct Answer: *C*

By specifying the outgoing interface and not the next hop IP address, the Management devices will be able to ping the new server, but not the default gateway of the server.

splashy Highly Voted 8 months ago

Selected Answer: C

The fact that you specify a host route is the reason you cannot ping any other host than the server in that subnet. Not that you specified the egress interface instead of the next hop address.

I tried both scenarios in PT with a host route and they give exactly the same result, as to be expected.

upvoted 10 times

shumps Most Recent 1 week, 1 day ago

C is is a give way price, 172.16.2.2 255.255.255.255 192.168.1.15 its not on the answers but its another way to do it on PT

upvoted 1 times

diriba 1 month ago

I don't see this in the diagram: "An engineer blocking from pinging the default gateway."

upvoted 1 times

perri88 3 months ago

I don't see this in the diagram: "An engineer is updating the R1 configuration to connect a new server to the management network."

upvoted 1 times

RougePotatoe 10 months, 3 weeks ago

Selected Answer: C

While C is the right answer wouldn't the ideal configuration be ip route 172.16.2.2 255.255.255.255?

C is the right answer because it is a /32 host route so as long as the 172 number isn't advertised by OSPF or configured statically packets from R1 can not reach the 172 gateway.

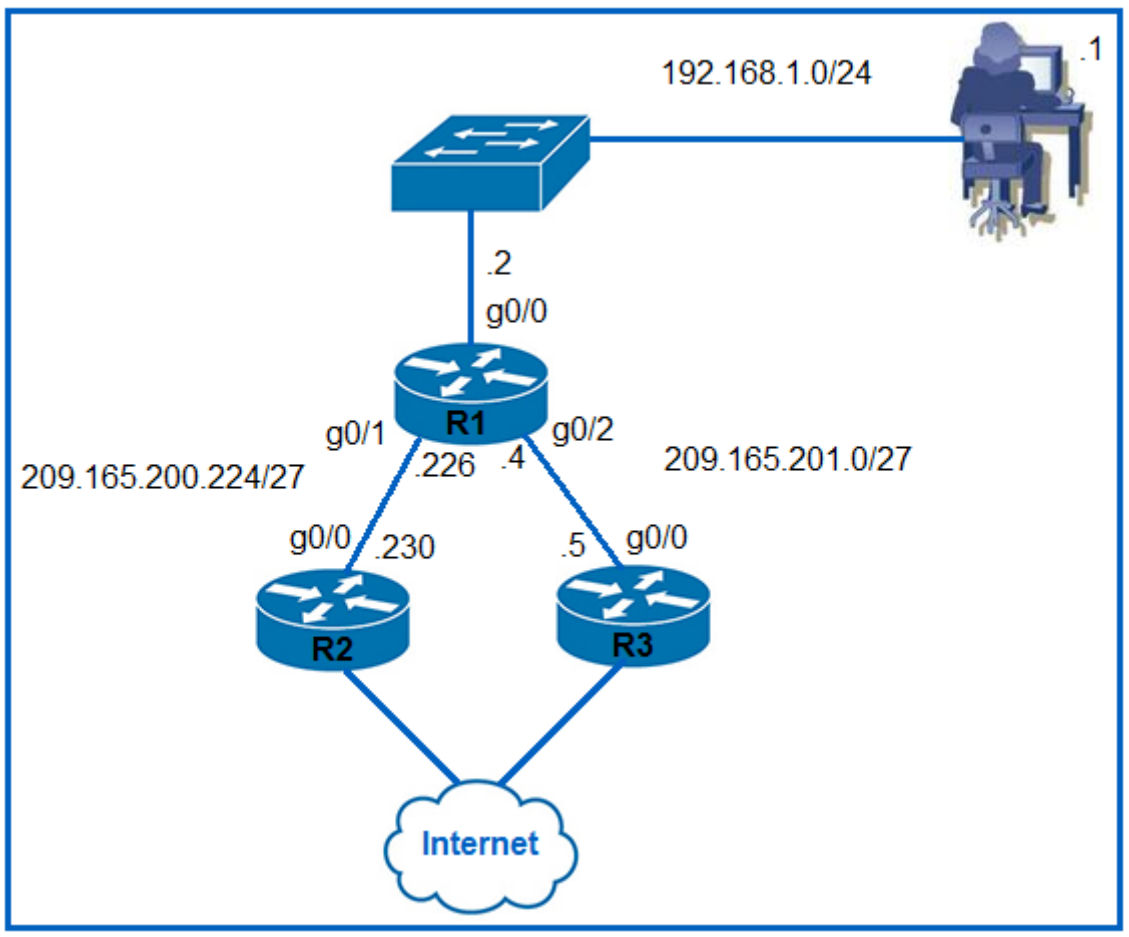
upvoted 4 times

Chopaka 2 months, 3 weeks ago

You right my friend

upvoted 1 times

Question #463 *Topic 1*



Refer to the exhibit. Router R1 currently is configured to use R3 as the primary route to the internet, and the route uses the default administrative distance settings. A network engineer must configure R1 so that it uses R2 as a backup, but only if R3 goes down. Which command must the engineer configure on R1 so that it correctly uses R2 as a backup route, without changing the administrative distance configuration on the link to R3?

A. ip route 0.0.0.0 0.0.0.0 209.165.201.5.10

B. ip route 0.0.0.0 0.0.0.0 g0/1 1

C. ip route 0.0.0.0 0.0.0.0 209.165.200.226 1

D. ip route 0.0.0.0 0.0.0.0 g0/1 6

Correct Answer: *D*

Vikramaditya_J Highly Voted 4 months, 1 week ago

Selected Answer: D

Important thing to take note of is, the syntax for creating a default static route or connected static route uses the exit interface or output interface of source device (that's the interface on which all packets are sent to the destination network). Some of us may confuse and think to use Gi0/0 interface on R3 in the command, but the interface to configure the backup route here must use the exit interface on the R1 itself i.e. Gi0/1. So command will be:
ip route 0.0.0.0 0.0.0.0 g0/1 6 ("6" here is AD that's greater than the connected route's AD i.e., 1)

upvoted 8 times

BeautifulSmile 3 months, 4 weeks ago

Thank you so much Vikramaditya_J. so educating.

upvoted 1 times

mellos Most Recent 10 months, 3 weeks ago

"D" es correcto. Porque la AD por defecto es "1". Por lo tanto quien tiene el AD mas alto es "D" en este caso es "6". De esta forma queda configurada la ruta de respaldo

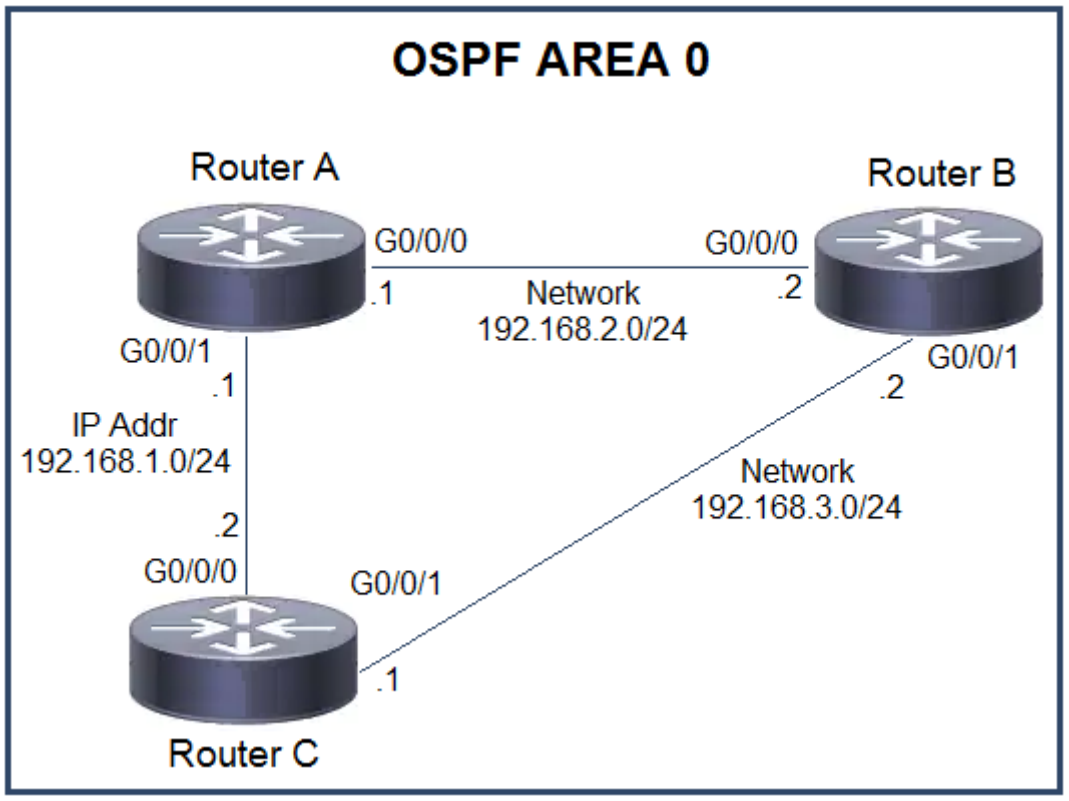
upvoted 3 times

Dutch012 6 months, 1 week ago

gracias love

upvoted 1 times

Question #464 *Topic 1*



Refer to the exhibit. Which action must be taken to ensure that router A is elected as the DR for OSPF area 0?

A. Configure the router A interfaces with the highest OSPF priority value within the area

B. Configure router B and router C as OSPF neighbors of router A

C. Configure the OSPF priority on router A with the lowest value between the three routers.

D. Configure router A with a fixed OSPF router ID

Correct Answer: *A*

no_blink404 2 months, 3 weeks ago

The answer is A. You would want to configure the priority as close to the maximum (255) to ensure election as DR.

upvoted 1 times

john1247 3 months, 2 weeks ago

Isn't C the answer? Why is A the answer?

upvoted 1 times

Rick3390 3 days, 4 hours ago

Are you serious?? The router with the highest priority becomes the DR. if the priority is equal, the router with the highest ip configured on an interface , make this router become the DR! keep study dude!

upvoted 1 times

jonathan126 4 months, 3 weeks ago

Answer is correct

upvoted 3 times

Question #465 *Topic 1*

```
EIGRP 10.10.10.0/24 [90/1441]     via F0/10
EIGRP 10.10.10.0/24 [90/144]      via F0/11
EIGRP 10.10.10.0/24 [90/1441]     via F0/12
OSPF  10.10.10.0/24 [110/20]      via F0/13
OSPF  10.10.10.0/24 [110/30]      via F0/14
```

Refer to the exhibit. Packets received by the router from BGP enter via a serial interface at 209.165.201.10. Each route is present within the routing table. Which interface is used to forward traffic with a destination IP of 10.10 10 24?

A. F0/10

B. F0/11

C. F0/12

D. F0/1

Correct Answer: *B*

raul_kapone 3 weeks ago

Selected Answer: B

BEAUTIFUL QUESTION!
Better than the Cisco tricky questions that seem made for a SAW movie.

upvoted 2 times

ccnk 2 months, 4 weeks ago

BBBBBBBB

upvoted 2 times

yousfs1212 4 months, 2 weeks ago

Selected Answer: B

Of course B because the router firt choose EIGRP Instead OSPF , then , because all prefix length is equal , router choose to lowest AD

upvoted 3 times

Stichy007 6 months, 3 weeks ago

Selected Answer: B

metric is lower than 1441

upvoted 2 times

SVN05 7 months, 1 week ago

Dear Danaah,
When installing to routing table is AD and Metric Only
When choosing a route from routing table is Longest Prefix, AD and Metric can play a role

Since the question stats based on routing table means now we have to consider 3 factors(longest prefix, AD and Metric) however all are /24 so longest prefix is out of the question. Now comes the tricky part

If there are 2 or more routes to the same destination using different protocol is AD
If there are 2 or more routes to the same destination using same protocol is Metric

In this case example, OSPF route via F0/13 and EIGRP route via F0/11 are viable options however they ask to choose 1 so in the answer sheet is EIGRP route via F0/11 available thus being the answer.

upvoted 1 times

kobisiva 7 months, 2 weeks ago

metric looks confuse A & C 1441 B 144

upvoted 2 times

Panda_man 9 months, 3 weeks ago

Selected Answer: B

lowest metric is correct

upvoted 2 times

DANAAH 8 months, 3 weeks ago

could you please explain how to solve this question in detail please?

upvoted 1 times

joseangelatm 8 months, 2 weeks ago

Its easy, first find the lowest AD then the lowest metric.

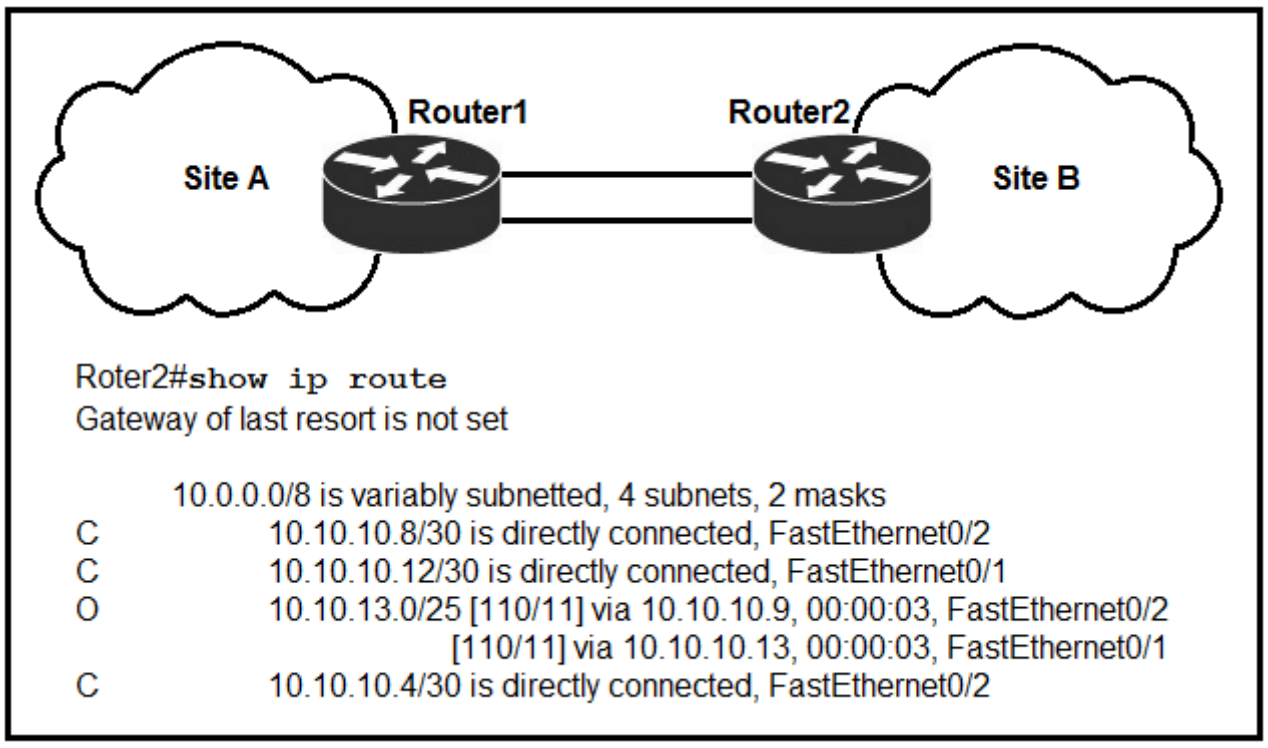
upvoted 2 times

motop9 11 months, 2 weeks ago

B. Metric is Small.

upvoted 4 times

Question #466 *Topic 1*



Refer to the exhibit. If OSPF is running on this network, how does Router2 handle traffic from Site B to 10.10.13.128/25 at Site A?

A. It sends packets out of interface Fa0/1.

B. It sends packets out of interface Fa0/2.

C. It load-balances traffic out of Fa0/1 and Fa0/2.

D. It is unreachable and discards the traffic.

Correct Answer: *D*

DoBronx Highly Voted 10 months, 3 weeks ago

Selected Answer: D

10.10.13.0/25 encompasses .1-.127 and there is no default route configured so answer given is correct

upvoted 14 times

MarioE 4 months, 2 weeks ago

Yes sir

upvoted 2 times

NICE_ANSWERS 3 months, 2 weeks ago

I think it's 0-127... Which is 128 addresses in total...usable ones are 1-126... Please correct me if i'm wrong

upvoted 1 times

Stichy007 Highly Voted 6 months, 3 weeks ago

Selected Answer: D

network 10.10.13.128/25, not contained in any of the routing table entries.

upvoted 5 times

Question #467 *Topic 1*

```
R1#show run
!
router ospf 1
auto-cost reference-bandwidth 100000
!
interface GigabitEthernet0/0
bandwidth 10000000
!
interface GigabitEthernet0/1
bandwidth 100000000
!
interface GigabitEthernet0/2
ip ospf cost 100
!
interface GigabitEthernet0/3
ip ospf cost 1000
end
```

Refer to the exhibit. Router R1 resides in OSPF Area 0. After updating the R1 configuration to influence the paths that it will use to direct traffic, an engineer verified that each of the four Gigabit interfaces has the same route to 10 10.0.0/16.
Which interface will R1 choose to send traffic to reach the route?

A. GigabitEthernet0/0

B. GigabitEthernet0/1

C. GigabitEthernet0/2

D. GigabitEthernet0/3

Correct Answer: *B*

splashy Highly Voted 11 months, 3 weeks ago

Selected Answer: B

ref BW 100000 MB

ref BW BW
G0/0
100000MB divided by 10000MB (or 10000000KB) = 10 cost

G0/1
100000MB divided by 100000MB (or 100000000KB) = 1 cost

upvoted 17 times

g_mindset Highly Voted 1 year ago

Selected Answer: A

Answer should be A.

Ref-bandwidth / bandwith = ospf cost
note that bandwidth is in kilobits per second, so you need to convert to Mbs to get the accurate cost.

upvoted 5 times

Shanku97 Most Recent 2 weeks, 1 day ago

ANSWER is b,

since the bandwidth value is altered for g0/0 & g0/1, the bw value for them are in kb.

first divided them by 1000 to get the values in MB.

second, now divide the ref bw value/ interface bw values

the cost for g0/1 would be 1, which is lowest.

upvoted 1 times

mda2h 2 months, 2 weeks ago

Selected Answer: B

bandwidth (BW) is expressed in kbps.

cost = 100 Mbps/BW

cost Ge0/0 = 1/100

cost Ge0/1 = 1/1000
cost Ge0/2 = 100
cost Ge0/3 = 1000

Answer is B: Ge0/1 has the lowest cost
upvoted 2 times

Phonon 8 months ago
This is a trick question, both G0/0 and G0/1 have a cost of 1

In OSPF if the interface has a higher bandwidth than the cost metric it will be 1.

The answer is indeterminate between A and B
upvoted 4 times

Netcmd 10 months ago
Selected Answer: B
it cannot be A as B has a higher Bandwidth
upvoted 2 times

Customexit 11 months, 3 weeks ago
to expand to what g_mindset said:
OSPF's metric is called "cost".

When you change an interface's bandwidth, it's in kilobits
#R1(config-if)#bandwidth ?
<1-10000000> Bandwidth in kilobits

It's in kilobits.

We can tell G0/0 and G0/1's bandwidth were manually altered because 'auto-cost reference bandwidth' was set to 100000 (it's different).

A router's cost reference bandwidth is default 100mbps.
This is what it looks like when you change the auto-cost reference bandwidth:
Router(config-router)#auto-cost reference-bandwidth ?
<1-4294967> The reference bandwidth in terms of Mbits per second

It's it Mbits per second.

Reference-Bandwidth(Mbps) / Interface Bandwidth(Mbps) = OSPF cost

10000000kbps / 1000(Mbps (intG0/0's)) = 10000
10000 / 1000 = 10

Interface GigabitEthernet0/0 has a cost of 10.
upvoted 3 times

Customexit 11 months ago
Disregard my answer, it is B G0/1.
I miscounted the 0's in the auto-cost reference bandwidth. Refer to splashy's comment.
upvoted 2 times

nicombe 11 months, 3 weeks ago
Selected Answer: B
B is correct because int g0/1 has a higher bandwidth configured than int g0/0 and therefore a lower cost.
upvoted 4 times

Question #468 *Topic 1*

```
R1# show ip route | begin gateway
Gateway of last resort is 209.165.200.254 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.200.254, Serial0/0/1
                            is directly connected, Serial0/0/1
   172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C     172.16.1.0/24 is directly connected, FastEthernet0/0
L     172.16.1.1/32 is directly connected, FastEthernet0/0
R     172.16.2.0/24 [120/2] via 297.165.200.250, 00:00:25, Serial0/0/0
O     192.168.1.0/24 [110/4437] via 207.165.200.254, 00:00:17, Serial0/0/1
D     192.168.2.0/24 [90/84437] via 207.165.200.254, 00:00:15, Serial0/0/1
       207.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
S      207.165.200.244/30 [1/1] via 207.165.200.254, Serial0/0/1
C     207.165.200.248/30 is directly connected, Serial0/0/0
L     207.165.200.249/32 is directly connected, Serial0/0/0
C     207.165.200.252/30 is directly connected, Serial0/0/1
L     207.165.200.253/32 is directly connected, Serial0/0/1
```

Refer to the exhibit. Which network prefix was learned via EIGRP?

A. 172.160.0/16

B. 207.165.200.0/24

C. 192.168.1.0/24

D. 192.168.2.0/24

Correct Answer: *D*

Eyad_Alotaibi Highly Voted 9 months, 1 week ago

D = EIGRP
C = connected
S = static
I = IGRP
R = RIP
B = BGP
O = OSPF
E = EGP
i = IS-IS
* = default route

upvoted 5 times

Panda_man Most Recent 9 months, 3 weeks ago

Selected Answer: D

D correct

upvoted 1 times

ShehuUsman 12 months ago

D is correct the AD of eigrp is 90

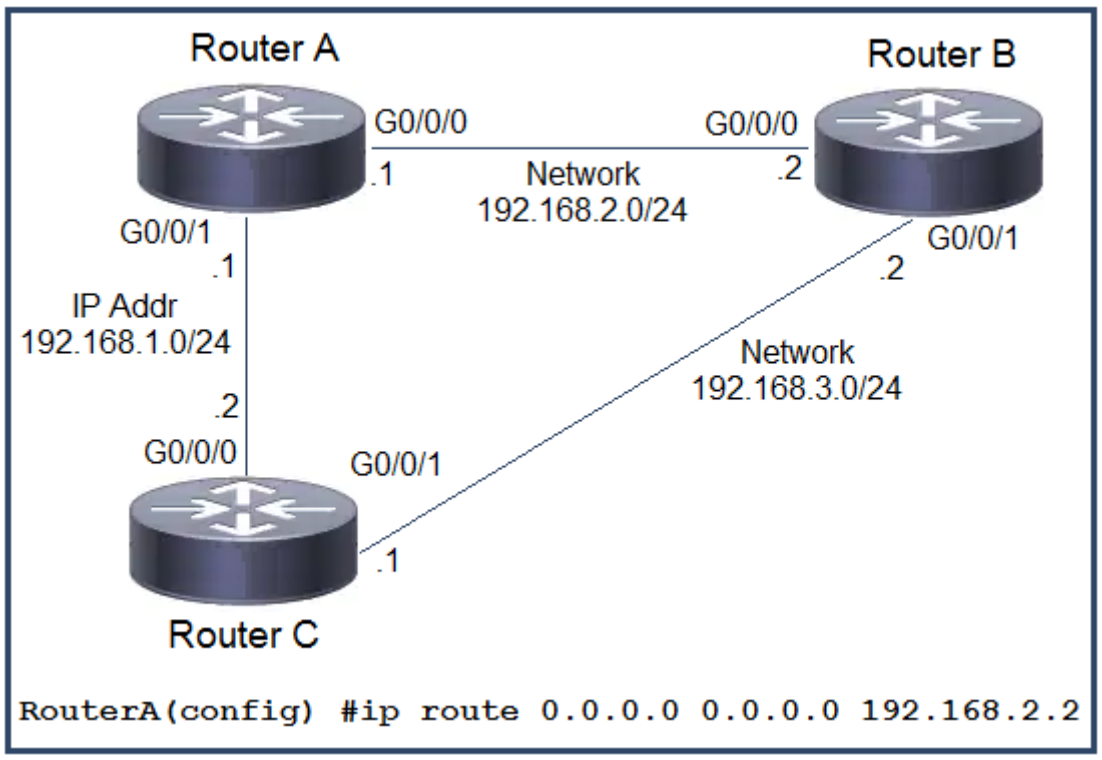
upvoted 1 times

netzwork 11 months, 1 week ago

You are right, but also on the IP Route table, you can see the "D" on the left. Dynamically learned via EIGRP

upvoted 2 times

Question #469 *Topic 1*



Refer to the exhibit. Which command must be issued to enable a floating static default route on router A?

A. ip route 0.0.0.0 0.0.0.0 192.168.1.2 10

B. ip route 0.0.0.0 0.0.0.0 192.168.1.2

C. ip default-gateway 192.168.2.1

D. ip route 0.0.0.0 0.0.0.0 192.168.2.1 10

Correct Answer: *A*

Customexit Highly Voted 11 months, 3 weeks ago

Selected Answer: A

A & D are the only answers with a configured distance metric (10).
A floating static route is meant to be a backup.

The current route has a route traveling through Router B.
So it would make sense we have our backup (floating static route) going through Router C with a metric higher than a default route (1).

upvoted 10 times

ABCenergo Highly Voted 7 months, 1 week ago

D is wrong because address is 192.168.2.2 not 2.1

upvoted 5 times

Stichy007 6 months, 3 weeks ago

brilliant observation.

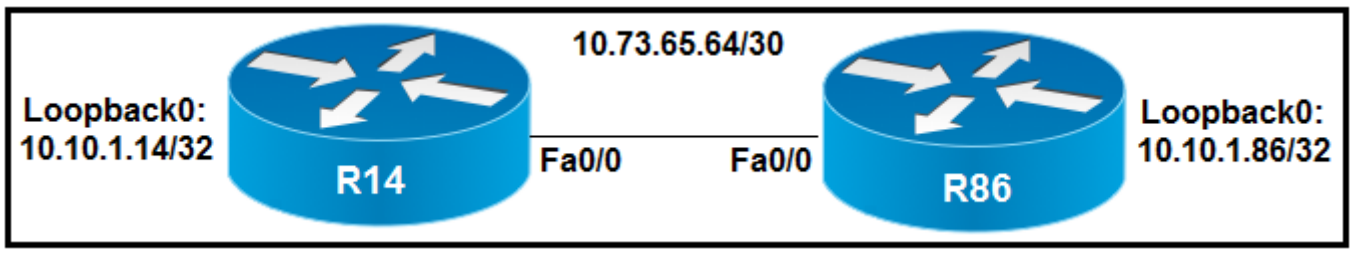
upvoted 1 times

ananinamia Most Recent 1 week, 6 days ago

i think i have to study for floating static default! What a name!!!

upvoted 1 times

Question #470 *Topic 1*



Refer to the exhibit. Which configuration allows routers R14 and R86 to form an OSPFv2 adjacency while acting as a central point for exchanging OSPF information between routers?

A. R14# interface FastEthernet0/0 ip address 10.73.65.65 255.255.255.252 ip ospf network broadcast ip ospf priority 0 ip mtu 1400 router ospf 10 router-id 10.10.1.14 network 10.10.1.14 0.0.0.0 area0 network 10.73.65.64 0.0.0.3 area0 R86# interface Loopback0 ip address 10.10.1.86 255.255.255.255 interface FastEthernet0/0 ip address 10.73.65.66 255.255.255.252 ip ospf network broadcast ip mtu 1500 router ospf 10 router-id 10.10.1.86 network 10.10.1.86 0.0.0.0 area 0 network 10.73.65.64 0.0.0.3 area 0

B. R14# interface Loopback0 ip ospf 10 area 0 interface FastEthernet0/0 ip address 10.73.65.65 255.255.255.252 ip ospf network broadcast ip ospf 10 area 0 ip mtu 1500 router ospf 10 ip ospf priority 255 router-id 10.10.1 14 R86# interface Loopback0 ip ospf 10 area 0 interface FastEthernet0/0 ip address 10.73.65.66 255.255.255.252 ip ospf network broadcast ip ospf 10 area 0 ip mtu 1500 router ospf 10 router-id 10.10.1.86

C. R14# interface FastEthernet0/0 ip address 10.73.65.65 255.255.255.252 ip ospf network broadcast ip ospf priority 255 ip mtu 1500 router ospf 10 router-id 10.10.1.14 network 10.10.1.14 0.0.0.0 area0 network 10.73.65.64 0.0.0.3 area0 R86# interface FastEthernet0/0 ip address 10.73.65.66 255.255.255.252 ip ospf network broadcast ip mtu 1500 router ospf 10 router-id 10.10.1.86 network 10.10.1.86 0.0.0.0 area 0 network 10.73.65.64 0.0.0.3 area 0

D. R14# interface FastEthernet0/0 ip address 10.73.65.65 255.255.255.252 ip ospf network broadcast ip ospf priority 255 ip mtu 1500 router ospf 10 router-id 10.10.1.14 network 10.10.1.14 0.0.0.0 area0 network 10.73.65.64 0.0.0.3 area0 R86# interface FastEthernet0/0 ip address 10.73.65.66 255.255.255.252 ip ospf network broadcast ip mtu 1400 router ospf 10 router-id 10.10.1.86 network 10.10.1.86 0.0.0.0 area 0 network 10.73.65.64 0.0.0.3 area 0

Correct Answer: *C*

Sutokuto Highly Voted 12 months ago
Anybody else just want to keep scrolling when you see answer choices like this?
upvoted 75 times

Dhruv3390 Highly Voted 8 months ago
Its C. Answer is straight forward, 1st I noticed mtu are mismatched in A and D, so we will eliminate them, in option B, Network command is missing so, C os is more appropriate.
upvoted 14 times

shumps Most Recent 1 week, 1 day ago
Quickest method is to see if the MTU match and the area, then i eliminate the wrong ones, Left with B & C, then check the syntax
upvoted 1 times

XxxYyyZzz 1 month, 1 week ago
TL;DR—
upvoted 1 times

tubirubs 1 month, 1 week ago
Selected Answer: C
B its wrong because:
B. R14# interface Loopback0 ip ospf 10 area 0 interface FastEthernet0/0 ip address 10.73.65.65 255.255.255.252 ip ospf network broadcast ip ospf 10 area 0 ip mtu 1500 "router ospf 10 ip ospf priority 255" this line. the comand exit from interface configuration and enter in OSPF global configuration and priority comando must be aplicate in the INTERFACE configuration prompt
upvoted 2 times

mda2h 2 months, 2 weeks ago
Selected Answer: C
A. and D. are wrong because MTU of miss match
B. is wrong because # ip ospf priority xx should be executed in interface mode
upvoted 1 times

PacketFapper 3 months, 2 weeks ago
How is B incorrect?

upvoted 1 times

dropspablo 3 months, 3 weeks ago

Selected Answer: C

B. R14# interface Loopback0
* ip ospf 10 area 0
* interface FastEthernet0/0
* ip address 10.73.65.65 255.255.255.252
* ip ospf network broadcast
* ip ospf 10 area 0
* ip mtu 1500
* router ospf 10
* ip ospf priority 255 (***WRONG***)
* router-id 10.10.1 14
* R86# interface Loopback0
* ip ospf 10 area 0
* interface FastEthernet0/0
* ip address 10.73.65.66 255.255.255.252
* ip ospf network broadcast
* ip ospf 10 area 0
* ip mtu 1500
* router ospf 10
* router-id 10.10.1.86

upvoted 1 times

dropspablo 3 months, 3 weeks ago

C. RESPOSTA CERTA)

C. R14# interface FastEthernet0/0
* ip address 10.73.65.65 255.255.255.252
* ip ospf network broadcast
* ip ospf priority 255
* ip mtu 1500
* router ospf 10
* router-id 10.10.1.14
* network 10.10.1.14 0.0.0.0 area0
* network 10.73.65.64 0.0.0.3 area0
* R86# interface FastEthernet0/0
* ip address 10.73.65.66 255.255.255.252
* ip ospf network broadcast
* ip mtu 1500
* router ospf 10
* router-id 10.10.1.86
* network 10.10.1.86 0.0.0.0 area 0
* network 10.73.65.64 0.0.0.3 area 0

upvoted 1 times

Drader 5 months, 3 weeks ago

i swear they could at least format this such that it's easier to read

upvoted 6 times

daddydagoth 6 months, 3 weeks ago

Holy hell, it's C but the amount of text makes me wanna bash my head into the keyboard.

upvoted 7 times

McNov14 10 months ago

To set the priority of an interface, use the command ip ospf priority value, where value is 0 to 255

upvoted 2 times

Ghugs 11 months, 2 weeks ago

Why is B incorrect?

upvoted 1 times

Ghugs 11 months, 2 weeks ago

Nvm I see it, the ip command under router ospf

upvoted 1 times

xWhosNext 9 months ago

In case someone is still confused like I was.

The command ip ospf priority should be done in interface configuration mode and not router configuration mode.

Correct me if I am wrong.

Correct me if I am wrong.

upvoted 2 times

dropspablo 1 month, 2 weeks ago

Exactly :DDD
upvoted 1 times

dropspablo 1 month, 2 weeks ago
Answer is "C"
upvoted 1 times

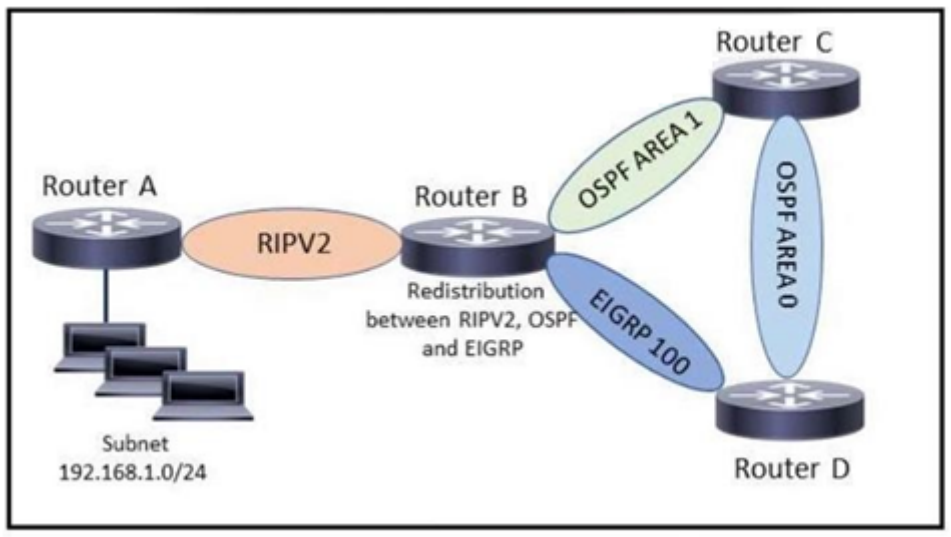
creaguy 11 months, 3 weeks ago
Why can't they put these configuration scripts in proper format? Line per line. Is it actually like this on the exam ?
upvoted 6 times

dmaster42 11 months, 3 weeks ago
Many questions like this are present in this 200-301 exam, be well prepared, if I remember correctly this was one of them.
upvoted 3 times

osuzu 1 year ago
c and d are same commands?
upvoted 1 times

MikD4016 1 year ago
The last MTU change (1400-1500)
upvoted 3 times

Question #471 *Topic 1*



Refer to the exhibit. When an administrator executes the show ip route command on router D to view its routing table, which value is displayed for the administrative distance for the route to network 192.168 1.0?

A. 110

B. 120

C. 170

D. 90

Correct Answer: *A*

EngrRex Highly Voted 11 months, 3 weeks ago

A is correct because when EIGRP is redistributed the new AD will be 170 (external EIGRP) making OSPF the lowest AD available. Redistribution topic is in CCNP

upvoted 8 times

Ceruzka 6 months, 1 week ago

I agree with EngrRex and "A" is correct and definitely it's CCNP topic.

upvoted 2 times

Shanku97 Most Recent 2 weeks, 1 day ago

SO ROUTE RE DISTRIBUION IS ALSO IN CCNA NOW, WHAT ELSE IS THERE ?

upvoted 1 times

shumps 3 weeks ago

D 90 eigrp. this is not CCNP

upvoted 1 times

dropspablo 3 months, 3 weeks ago

Selected Answer: A

Letter A is correct, it's simple:

If you test in Packet Tracer, you will see that every route redistributed from another protocol (interface X) on the router to (interface Y) OSPF, appears ON THE NEXT router as "O E2", but the administrative distance remains the same "AD 110".

Unlike EIGRP - when a router receives a redistributed route from another protocol (in this case RIPv2), it will appear as an EIGRP route with the initials "D EX", but its administrative distance will no longer be 90, in this case it will appear as "AD 170".

In the question we have both, AD 110 (O E2) or AD 170 (D EX) for the same destination network 192.168 1.0. AD 110 will be the winner and will appear in the routing table of router D... AD 170 will be a backup and will only be displayed if the first one fails.

upvoted 2 times

UDITH_ins8659 4 months ago

can you explain me correct anser and explain

upvoted 1 times

Panda_man 9 months, 3 weeks ago

Selected Answer: A

would go with A

upvoted 3 times

rictorres333 11 months, 3 weeks ago

Selected Answer: C

I tried on my virtual environment. The net 192.168.1.0 comes by RIPV2 to Router B with redistribution between routing protocols, it means that 192.168.1.0 go into EIGRP as external route and go in to Router D as D EX with AD 170.

upvoted 1 times

splashy 12 months ago

Selected Answer: D

With the knowledge of CCNA which does not include route redistribution the answer should be D

I have read for about an hour and a half about route redistribution between ripv2 & ospf and ripv2 & eigrp on Cisco. And if the redistribution is correctly configured it should also be D.

upvoted 3 times

splashy 11 months ago

Tried it in PT and the destination shows up as a D ex route with AD 170 so OSPF does win...
A

upvoted 4 times

rictorres333 1 year ago

It can be because of it comes redistributed and become a external EIGRP AD 170?

upvoted 3 times

mrgreat 11 months, 3 weeks ago

Its correct. See https://community.cisco.com/t5/switching/eigrp-ad-of-redistributed-routes/td-p/1602887. Answer is A

upvoted 2 times

guynetwork 1 year ago

Selected Answer: D

It is D

upvoted 1 times

g_mindset 1 year ago

Selected Answer: D

Someone tell me why the answer is not D here?

upvoted 1 times

Bl1024 1 year ago

Should be D, no? Eigrp AD

upvoted 1 times

melmiosis 10 months, 2 weeks ago

When redistribution is configured on EIGRP (which is the case here), we get an EXTERNAL EIGRP, which has an AD of 170 thus higher AD than OSPF

upvoted 1 times

osuzu 1 year ago

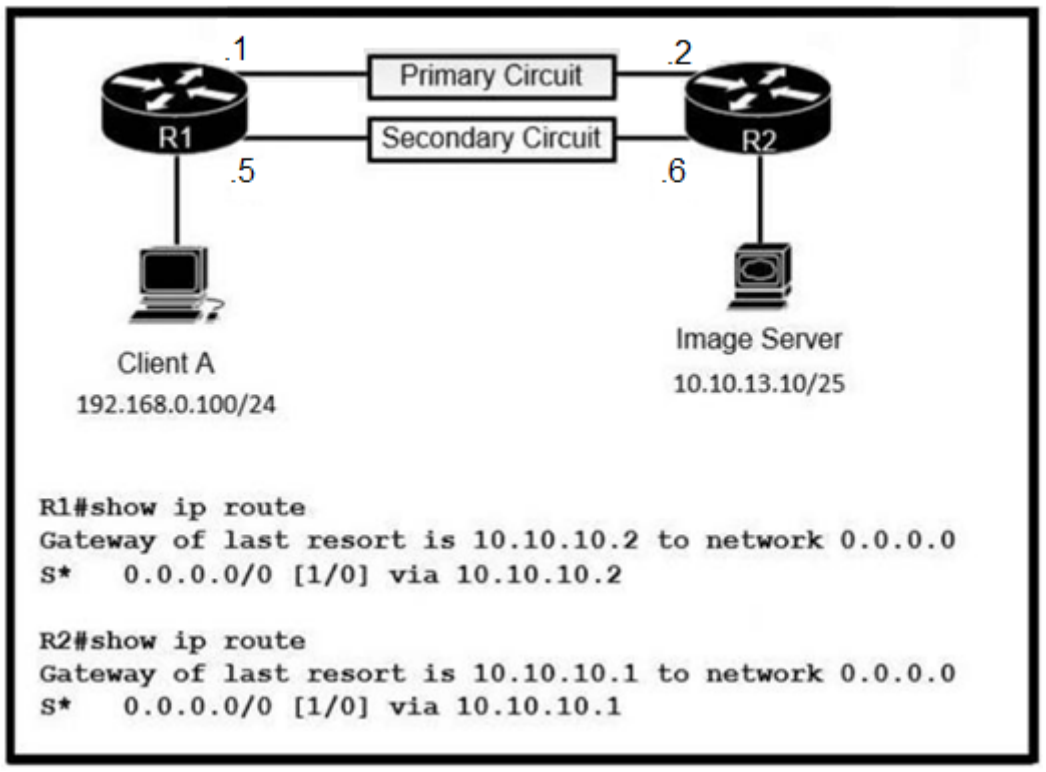
why...? OSPF?

upvoted 2 times

THEKYPTONIAN 11 months, 2 weeks ago

EIGRP with redistribute is 170

upvoted 1 times



Refer to the exhibit Routers R1 and R2 have been configured with their respective LAN interfaces. The two circuits are operational and reachable across WAN.

Which command set establishes failover redundancy if the primary circuit goes down?

A. R1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.6 R2(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.5

B. R1(config)#ip route 10.10.13.10 255.255.255.255 10.10.10.2 R2(config)#ip route 192.168.0.100 255.255.255.255 10.10.10.1

C. R1(config)#ip route 10.10.13.10 255.255.255.255 10.10.10.6 R2(config)#ip route 192.168.0.100 255.255.255.255 10.10.10.5

D. R1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.6 2 R2(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.5 2

Correct Answer: *D*

ananinamia 1 week, 6 days ago

why is ending with 2

upvoted 1 times

StreZ 7 months, 3 weeks ago

Why not C?

upvoted 1 times

Peter_panda 5 months, 2 weeks ago

Because it is not a failover route, but a permanent route (traffic will pass through this route even if the default route is functional)

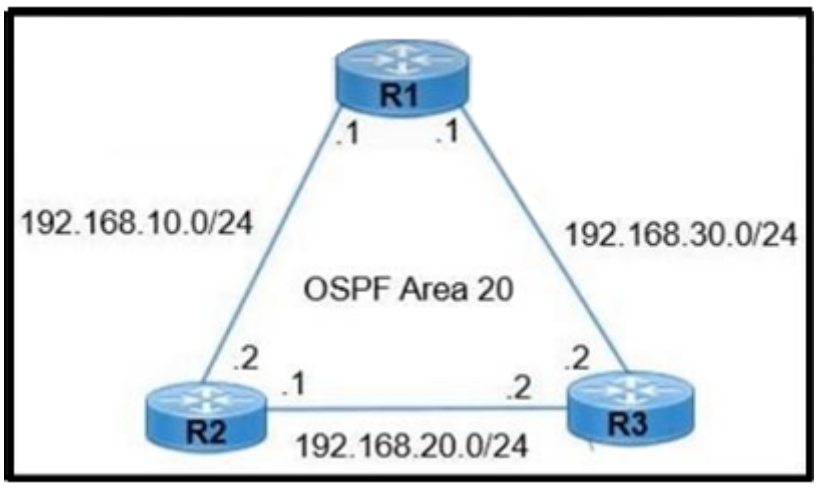
upvoted 3 times

Bugatti 7 months, 3 weeks ago

We need to configure secondary gateway of last resort. D, is the only one with modified AD value

upvoted 3 times

Question #473 *Topic 1*



Refer to the exhibit. R1 learns all routes via OSPF. Which command configures a backup static route on R1 to reach the 192.168.20 0/24 network via R3?

A. R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.2 111

B. R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.2 90

C. R1(config)#ip route 192.168.20.0 255.255.0.0 192.168.30.2

D. R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.2

Correct Answer: *A*

[Removed] 2 months, 3 weeks ago

Selected Answer: A

A is correct. We need to configure a backup static route so the OSPF administative distance needs to be higher than the default one (110) so 111 will make it.

upvoted 1 times

Bl1024 1 year ago

B is correct as well.
Why choose A and not B?

upvoted 2 times

Paullll 1 year ago

I think it's because of the "back-up static route", if everything is learned via OSPF (110), it needs a bigger AD for a back-up one, so 111. This is the way I think, at least.

upvoted 25 times

shumps 4 months ago

You spot on!!

upvoted 2 times

FALARASTA 4 months, 2 weeks ago

thats true

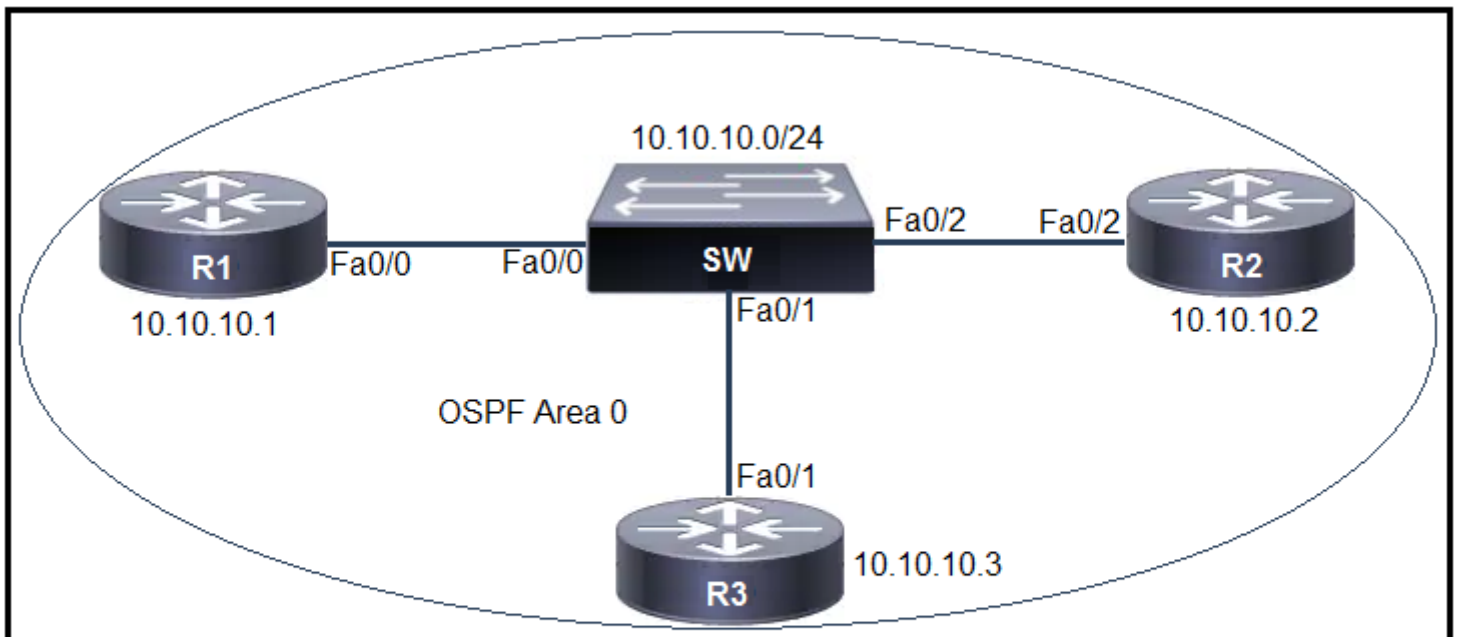
upvoted 3 times

nicombe 11 months, 3 weeks ago

This is the way

upvoted 6 times

Question #474 *Topic 1*




```
R1#show ip ospf neighbor

Neighbor ID   Pri   State      Dead Time   Address       Interface
10.10.10.2      1   FULL/BDR   00:00:37    10.10.10.2    FastEthernet0/0
10.10.10.3      1   FULL/DR    00:00:35    10.10.10.3    FastEthernet0/0
```

Refer to the exhibit. R1 has taken the DROTHER role in the OSPF DR/BDR election process. Which configuration must an engineer implement so that R1 is elected as the DR?

A. R1(config)#interface FastEthernet 0/0 R1(config-if)#ip ospf priority 1 R1#clear ip ospf process

B. R3(config)#interface FastEthernet 0/1 R3(config-if)#ip ospf priority 200 R3#clear ip ospf process

C. R2(config)#interface FastEthernet 0/2 R2(config-if)#ip ospf priority 1 R2#clear ip ospf process

D. R1(config)#interface FastEthernet 0/0 R1(config-if)#ip ospf priority 200 R1#clear ip ospf process

Correct Answer: *D*

RidzV 6 months, 4 weeks ago

We want R1 to be DR here. Considering all 3 routers are set to use default values for OSPF priority (I.e. value 1) and selection has happened on the basis of highest router ID (highest IP address of its interface), R1 is currently selected as DROTHER. To make it DR, it needs to have the highest priority. Hence correct answer is D from the given options.

Reason: On LANs, DR and BDR have to be elected. Two rules are used to elect a DR and BDR:

router with the highest OSPF priority will become a DR. By default, all routers have a priority of 1.
if there is a tie, a router with the highest router ID wins the election. The router with the second highest OSPF priority or router ID will become a BDR.

https://study-ccna.com/designated-backup-designated-router/

upvoted 3 times

jini4200 7 months ago

is it correct?? could someone explain it to me?...? why is it not B?

upvoted 1 times

FALARASTA 4 months, 2 weeks ago

The iterface used is also wrong

upvoted 1 times

soRwatches 6 months ago

D is correct, configure the R1 interface ospf priority to become DR. B is incorrect, the question is to implement the R1 as a DR.

upvoted 2 times

Question #475 *Topic 1*

Which SDN plane forwards user-generated traffic?

A. Management plane

B. Control plane

C. Policy plane

D. Data plane

Correct Answer: *D*

Danishh 2 months, 1 week ago

Selected Answer: D

Data Plane - also called forwarding plane which forwards user data/traffic from one interface to another are part of the data plane. Also de-encapsulates the original layer 2 header, and re-encapsulates with a new headser destined for the next hop's MAC address. NAT is the part of the Data Plane.

upvoted 1 times

Question #476 *Topic 1*

An application in the network is being scaled up from 300 servers to 600. Each server requires 3 network connections to support production, backup, and management traffic. Each connection resides on a different subnet. The router configuration for the production network must be configured first using a subnet in the 10.0.0.0/8 network. Which command must be configured on the interface of the router to accommodate the requirements and limit wasted IP address space?

A. ip address 10.10.10.1 255.255.254.0

B. ip address 10.10.10.1 255.255.252.0

C. ip address 10.10.10.1 255.255.240.0

D. ip address 10.10.10.1 255.255.255.240

Correct Answer: *A*

splashy Highly Voted 12 months ago

Selected Answer: B

We need to be able to put 600 hosts 3 different dedicated subnets.

So not 300 existing servers in one subnet and 300 new servers in the next subnet, belonging to production only for example. The subnets must be dedicated.

/22 is the only solution for each subnet.

upvoted 16 times

VictorCisco 5 months, 3 weeks ago

600 servers, 3 connections on EACH, so 1600 ip are needed. /22 = 1022 ip.
answer is C.

upvoted 3 times

learntstuff 2 months ago

600 x 3 = 1800

upvoted 1 times

lolungos 3 months ago

"Each connection resides on a different subnet" make sure to read the question slowly so you don't skip details like that

upvoted 2 times

Murphy2022 11 months, 2 weeks ago

10.0.0.0 /23
10.0.2.0 /23
10.0.4.0 /23
?

upvoted 2 times

RougePotatoe 10 months ago

/23 = 510 hosts
/22 = 1020 hosts
3 ip addresses, each on different vlan x 300 servers = 900 ip addresses

IMO this question makes no sense since it asks you to configure an interface on the router. Configuring a .1 will not allow routing for the requested 3 distinct vlan groups since you need a default gateway for each vlan. You would have to configure sub interfaces on this router to enable routing to the 3 distinct vlans.

upvoted 1 times

RougePotatoe 10 months ago

After some more thought A is starting to make more sense. Remember we are being asking to subnet the /8 network. /22 only provides us with 1 subnet and there is no way you can slice /22 into 3 subnets that support 300 hosts each.

This question is still worded horribly though since A only provides the ip address of only one of the vlan's gateway.

upvoted 2 times

JohnJacobJr 9 months, 3 weeks ago

/8 is a class a address

255.255.254.0 = 32768 subnets
255.255.252.0 = 16384 subnets
255.255.240.0 = 4096 subnets
255.255.255.240 = 16 subnets

We need to accommodate 3 subnets of 600, so we need 10 host bits. 255.255.252.0 gives us exactly 10 host bits so the answer is B.

upvoted 3 times

creaguy Highly Voted 11 months, 3 weeks ago

Selected Answer: A

300 additional server with 3 connections = 900 connects
each connection will have it's own subnet = 3 subnets
900 connections divided by 3 subnets = 300 connections per subnet
/24 = 254 connection/ip's
/23 = 510 connections/ip's
/23 = 255.255.254.0
So A is the correct answer

upvoted 7 times

AndreaGambera Most Recent 3 weeks, 2 days ago

Selected Answer: B

B is correct 3 x 300 = 900
255.255.252.0 /2

upvoted 1 times

Vikramaditya_J 1 month, 2 weeks ago

Selected Answer: A

It's a tricky question. Keep in mind that here we already have 300 existing servers (and we don't need new IPs for them) but we're adding 300 servers (to make the count to 600), so we need 300 new IPs for those new servers, divided in 3 subnets. Simply put, we need 3 new subnets where each subnet can accommodate 300 IP addresses. So, if we consider subnet 255.255.254 (or /23), it will give us 2^9 (=512) IP addresses i.e., 510 usable IP addresses, and 2^15 (23 – 8 = 15) subnets, which is sufficient for the given scenario. So correct answer is A.

upvoted 1 times

OrwellMB 2 months, 1 week ago

Selected Answer: A

Need 300 more servers, each 3 connections for:
PROD, bck, mgm
"The router configuration for the production network must be configured first using a subnet in the 10.0.0.0/8 network"

"For the PRODuction" -> 300 IP needed, bck and mgm are DIFFERENT subnets.

/23 -> A

upvoted 1 times

mda2h 2 months, 2 weeks ago

Selected Answer: B

Production Network had 300 servers. Now it has 600.
/23 gives 510
/22 gives 1022 = 255.255.252.0

upvoted 1 times

4bed5ff 2 months, 3 weeks ago

Selected Answer: A

We aren't considering all 3 subnets. Just one subnet, for the production network:
"Each server requires 3 network connections to support production, backup, and management traffic. Each connection resides on a different subnet. The router configuration for THE PRODUCTION NETWORK MUST BE CONFIGURED FIRST using a subnet in the 10.0.0.0/8 network ..."
Therefore we only budget for the 300 hosts in the production network.

upvoted 1 times

dropspablo 3 months, 3 weeks ago

Selected Answer: A

The question asks to add 300 hosts in three subnets, it doesn't make sense to mess with the settings of the servers that already exist (including SWs, Servers, and the whole network). In the case he asked to segment without waste (different from summarizing routes), that is, he would need to deliver to sub-interfaces (router-on-stick) or SVIs (SW L3), then the letter A 10.10.10.1 255.255.254.0 (/ 23) is correct, for the "Production Network" 10.10.10.0 - 10.10.11.255 (512-2 Hosts) would serve the additional 300 hosts. Example 10.10.12.0/23 for "Backup" and 10.10.14.0/23 for "Management"... on sub-interfaces or SVIs (SW L3).

upvoted 1 times

dropspablo 1 month, 2 weeks ago

"scaled up from 300 servers to 600" = 300 new servers. "Each server requires 3 network connections" = 3 networks. - Answer A. ip address 10.10.10.1 255.255.254.0.It would be 512-2 valid hosts per network (no waste).

upvoted 1 times

dropspablo 2 weeks ago

Stupid question! Looking again, I changed my mind. I believe it refers to the 600 servers on the production network, as we directly configured the production router (not just the new 300). In this case I stick with the letter B (prefix /22).

upvoted 1 times

Vikramaditya_J 4 months, 1 week ago

Selected Answer: B

There are already 300 servers divided in 3 subnets. The requirement here is to take up the number of servers from 300 to 600 i.e. increase it by "300" and each of those new 300 servers will need 3 different subnets. Therefore, the requirement is to have 3 new subnets and 900 (300 server x 3 subnets) IP addresses. Only /22 (255.255.252.0) fulfill this requirement by giving us 1024 IP addresses in each subnet.

upvoted 1 times

daddydagoth 6 months, 3 weeks ago

Selected Answer: B

The answers is B.

upvoted 1 times

Sdiego 7 months, 4 weeks ago

Selected Answer: B

/23 can holds 500 hosts aprox, /22 reachs 1000 hosts. B is correct

upvoted 1 times

Shansab 9 months ago

Selected Answer: B

The question is a little bit tricky. The servers increased from 300 to 600 and each server needs three connections with different subnets, so in this, if we consider /23 we will have only 510 usable IPs, so we should consider /22 (1022) to fulfill the requirement.

upvoted 2 times

tui9 8 months, 4 weeks ago

But the config is for the production subnet, so you can disregard the other 2 subnets. 300 new servers = /23 (510 hosts) to accommodate 300 server hosts. The least possible for this subnet.

upvoted 1 times

tui9 8 months, 4 weeks ago

Actually, it would be 510 per subnet. Still fine.

upvoted 1 times

Yadarsh 9 months ago

Selected Answer: B

Answer B

upvoted 1 times

RougePotatoe 10 months ago

Selected Answer: A

This question is worded horribly and makes no sense to begin with since you need multiple default gateways for each subnet. There is no way to configure 1 interface and allow routing to all the subnets you would need to create multiple sub interfaces. Remember you can't route to multiple / in-between vlans, IE subnets, without a router configured with sub interfaces or a L3 switch with SVIs because each vlan is their own network.

upvoted 2 times

RougePotatoe 10 months ago

Assuming this question is asking us to create 3 subnets that can support 300 hosts each. The only address that can do that efficiently is /23 because /22, while yielding 900 required addresses, cannot be subnetted into 3 vlans that support 300 hosts since /22 = 1022 hosts while /23 = 510 hosts. Needless to say you can only fit 510 into 1022 twice meaning only 2 vlans can be created. Answer A will give us the IP address of 1 of the sub interfaces that would need to be configured. If you are caught up on the last sentence of the question read the above paragraph.

upvoted 2 times

dropspablo 3 months, 3 weeks ago

RougePotatoe is right, even if we use a summarized route 10.0.0.0/22 it would not serve 3 subseats with 300 each later with VLSM, at most one with 510 host and two with 254 each. Or two of 510 hosts.
(I drew it below, please note without the translation so as not to lose the format.)
Example:
Summary Routes 10.0.0.0/22 (from 10.0.0.0 To 10.0.3.255 [1024-2 hosts])
VLSM
Subinterface .1 = 10.0.0.0/23 (512-2 hosts [300 ok])
Subinterface .2 = 10.0.2.0/23 (512-2 hosts [300 ok])
Subinterface .3 = 10.0.4.0/23 (WRONG - outside subnet 10.0.0.0/22)
Or 10.0.2.0/24 (256-2 hosts [not 300])
10.0.3.0/24 (256-2 hosts [not 300])

upvoted 1 times

daddydagoth 6 months, 3 weeks ago

You need to seriously brush up on how subnet calcs are done dude and stop spreading misinformation. A little helpin hint for you: to calculate the amount of subnets that can be made, do 2 to the power of borrowed host bits and you get the result. We're subnetting a /8 block, that means 14 borrowed bits in a /22 to make subnets. 2 to the power of 14 is 16384. We can make that many addresses from the /22.

upvoted 1 times

dropspablo 3 months, 3 weeks ago

daddydagoth I'm sorry but what you say doesn't make any sense, 22 - 32 = 10 bits for Hosts, that is 1024 - 2. 14 bits would be prefixed with /18 which would give about 16000 hosts, but nobody mentioned 18 or 14 bits borrowed prefix hahaha

upvoted 1 times

Etidic 10 months, 3 weeks ago

Selected Answer: B

B is the correct answer

upvoted 1 times

JohnJacobJr 11 months ago

255.255.254.0 only gives you 2 subnets, we need 3. 255.255.252.0 gives you 4 subnets with 1022 hosts each so B is correct.

upvoted 3 times

Customexit 11 months ago

Just going to plug this here as it's a good chart:
/32 1
/31 2
/30 4
/29 8
/28 16
/27 32
/26 64
/25 128
/24 256
/23 512
/22 1024
/21 2048

# of addresses on the right. -2 = # of hosts
255.255.252.0 is /22

upvoted 1 times

Question #477 *Topic 1*

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*    0.0.0.0/0 is directly connected, Null0
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.12.0/24 is directly connected, GigabitEthernet0/1
L        10.0.12.1/32 is directly connected, GigabitEthernet0/1
C        10.0.13.0/24 is directly connected, GigabitEthernet0/2
L        10.0.13.1/32 is directly connected, GigabitEthernet0/2
C        10.0.14.0/24 is directly connected, GigabitEthernet0/3
L        10.0.14.1/32 is directly connected, GigabitEthernet0/3
D     192.168.0.0/16 [90/130816] via 10.0.13.3, 00:10:09, GigabitEthernet0/2
O     192.168.0.0/23 [110/2] via 10.0.14.4, 00:00:46, GigabitEthernet0/3
S     192.168.0.0/24 [100/0] via 10.0.12.2
```

Refer to the exhibit. Which interface is chosen to forward traffic to the host at 192.168.0.55?

A. GigabitEthernet0/3

B. Null0

C. GigabitEthernet0/1

D. GigabitEthernet0/2

Correct Answer: *C*

RaselAhmedIT Highly Voted 6 months, 4 weeks ago

I think Longest Prefix (192.168.0.0/24) is connected via 10.0.12.2 (Static) & 10.0.12.0/24 is connected via G0/1.

upvoted 7 times

Danishh Most Recent 2 months, 1 week ago

192.168.0.0/24
Network Address - 192.168.0.0
Broadcast Address - 192.168.0.255
First Usable- 192.168.0.1
Last Usable - 192.168.0.254
That is why 192.168.0.55 which is the C option is correct.

upvoted 1 times

Myth1977 7 months, 2 weeks ago

Here, as far as i understand the longest prefix matches the 192.168.0.0/24 . Since, the /32 for the int g0/1 represents the hosts itself and g0/1 r with /24 masks represents the network containing the ".2" interface. The ans is g0/1.

upvoted 2 times

Freddy01 9 months, 4 weeks ago

10.0.12.1 is the IP configured on the router interface Gi0/1, whereas the next hop address is 10.0.12.2 and the route to get to subnet 192.168.0.55 is hanging off the neighbouring router. So, to get that 192.168.0.55 subnet, R1 will send traffic out of its Gi01 interface pointing to 10.0.12.2 next hop neighbouring router's interface which will pass it on to the subnet 192.168.0.55 hanging off its LAN interface. The routing table shows you 192.168.0.0/24 via 10.0.12.2 route, which clearly means the next hop address of the neighbouring router and 192.168.0.55 falls in that range of addresses. Hope this clarifies it :)

upvoted 2 times

Paullll 1 year ago

I am not sure why, can someone explain?

upvoted 1 times

Tylosh 12 months ago

I think the reason of answer C is correct is because 192.168.0.55 fit the range of /24 with the longest prefix , while it's via 10.0.12.2 , choosing the longest prefix 10.0.12.1/32. Will get the answer, hope it will help u a bit !!

upvoted 4 times

Customexit 11 months ago

While I believe C is in fact correct, I don't think it's because of the reason you give.
A /32 in the table means it's a host route. 10.0.12.1 is a end host.

10.0.12.0/24 contains 10.0.12.2 on the G0/1 interface.

Unless I'm understanding wrong

upvoted 3 times

Question #478 *Topic 1*

```
CPE# show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
       lA - LISP away, le - LISP extranet-policy, lp - LISP publications
ND  ::/0 [2/0]
     via FE80::A8BB:CCFF:FE00:200, Ethernet0/0
NDp 2001:DB8:1234:1::/64 [2/0]
     via Ethernet0/0, directly connected
L   2001:DB8:1234:1:A8BB:CCFF:FE00:100/128 [0/0]
     via Ethernet0/0, receive
C   2001:DB8:1234:2::/64 [0/0]
     via Ethernet0/1, directly connected
L   2001:DB8:1234:2:A8BB:CCFF:FE00:110/128 [0/0]
     via Ethernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Refer to the exhibit. The administrator must configure a floating static default route that points to 2001:db8:1234:2::1 and replaces the current default route only if it fails. Which command must the engineer configure on the CPE?

A. ipv6 route ::/0 2001:db8:1234:2::1 3

B. ipv6 route ::/128 2001:db8:1234:2::1 3

C. ipv6 route ::/0 2001:db8:1234:2::1 1

D. ipv6 route ::/0 2001:db8:1234:2::1 2

Correct Answer: *A*

Goena Highly Voted 7 months, 2 weeks ago

Selected Answer: A

Answer A:
- AD has to be higher then 2 so 3.
- Default route is ::/0
ipv6 route ::/0 2001:db8:1234:2::1 3

upvoted 7 times

dropspablo Most Recent 3 months, 3 weeks ago

Selected Answer: A

ND ::/0 [2/0] - means that the default route was automatically configured with the "ipv6 address autoconfig default" command (interface mode), and will always have AD 2. That's why to have a static default floating route we must include AD 3, if the first route fails, the static will assume with the initials "S ::/0 [3/0]".

Out of the question but taking advantage, we can also see the initials "NDp [2/0]" which represents a configuration of a directly connected interface, however the command "ipv6 address autoconfig" was used, in this case without default.

These are some of the uses of SLAAC and Neighbor Discovery Protocol (NDP) on the router - to configure IPv6 addresses and default route.

upvoted 2 times

virab4 4 months, 3 weeks ago

ND is our floating route with 2 ad?

upvoted 1 times

Ciscoman021 5 months, 2 weeks ago

Selected Answer: A

A is correct.

upvoted 1 times

SVN05 7 months, 1 week ago

Anybody can give a detailed explanation on why AD of default route is 2 and not 1 like it always is? Cause i cant see in the table it saying 2. Thanks.

upvoted 1 times

MRSCARLet 4 months, 3 weeks ago

I think the picture show the default route is 2
ND ::/0 [2/0]

P.S. Sry for my bad english

upvoted 1 times

country_rooted 5 months, 2 weeks ago

It was mostlikely manually configured to be that way to throw us off from choosing the correct answer. Youd automatically think that the default is 1 and choose an ans with the AD as 2.

upvoted 1 times

m4n1 8 months ago

why not a?

upvoted 1 times

ShadyAbdekmalek 11 months, 4 weeks ago

Why not D?

upvoted 1 times

EngrRex 11 months, 3 weeks ago

It is because the current default route AD is 2

upvoted 5 times

```
OldR#show ip ospf interface
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.1.2/24, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 192.168.1.1
  Backup Designated Router (ID) 192.168.1.1, Interface address 192.168.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1, flood queue length 0
  Neighbor Count is 1, Adjacent neighbor count is 2

R2#show ip ospf interface
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 192.168.1.2
  Backup Designated Router (ID) 192.168.1.1, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 2/2, flood queue length 0
   Neighbor Count is 1, Adjacent neighbor count is 2
```

Refer to the exhibit. Router OldR is replacing another router on the network with the intention of having OldR and R2 exchange routes. After the engineer applied the initial OSPF configuration, the routes were still missing on both devices. Which command sequence must be issued before the clear IP ospf process command is entered to enable the neighbor relationship?

A. OldR(config)#interface g0/0/0 OldR(config-if)#ip ospf hello-interval 15

B. OldR(config)#router ospf 1 OldR(config-router)#network 192.168.1.0 255.255.255.0 area 2

C. OldR(config)#interface g0/0/0 OldR(config-if)#ip ospf dead-interval 15

D. OldR(config)#router ospf 1 OldR(config-router)#no router-id 192.168.1.1

Correct Answer: *D*

With OSPF each router must have a unique router ID. Here we see that both routers have a router ID of 192.168.1.1. Removing the router-id command on the
OldR will force it to use one of its actual interface IP addresses as the router ID.

BieLey Highly Voted 11 months, 3 weeks ago

Selected Answer: D

Can even do this with the power elimination
Hello = matched
Dead = matched
Area = matches

Just 1 answer left!

upvoted 6 times

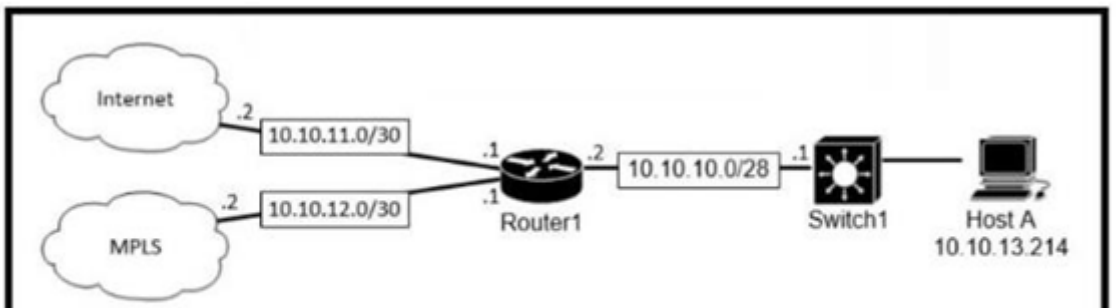
[Removed] Most Recent 2 months, 3 weeks ago

Selected Answer: D

Given answer is correct

upvoted 1 times

DRAG DROP -



Refer to the exhibit. Drag and drop the prefix lengths from the left onto the corresponding prefixes on the right. Not all prefixes are used.

Select and Place:

255.255.255.128	10.10.13.0
255.255.255.224	10.10.13.144
255.255.255.240	10.10.13.160
255.255.255.248	209.165.202.128
255.255.255.252	

Correct Answer:

255.255.255.128	255.255.255.252
255.255.255.224	255.255.255.248
255.255.255.240	255.255.255.224
255.255.255.248	255.255.255.128
255.255.255.252	

MikD4016 Highly Voted 1 year ago

Correct order:
.128
.240
.248
.224

upvoted 57 times

vladals 12 months ago

I would say the last one is .252
The reason for this is: 209.165.202.128 is reachable via 10.10.12.2 and 10.10.12.2 is part of the 10.10.12.2/30, hence 252

upvoted 25 times

PacketFapper 3 months, 2 weeks ago

By that logic, pretty much all of the other prefixes are reachable via 10.10.10.1 and the 10.10.10.0 is /28, hence all of the other selections are wrong. I think you overthunk this one, bud. Answer for last one is .224 /27

upvoted 3 times

clivebarker86 11 months, 1 week ago

i see 209.165.202.128 as a subnet of (by magic number) 209.165.202.0 - 32 - 64 - 96 - 128..... /27

upvoted 3 times

BieLey 11 months, 3 weeks ago

Agreeing with vladals here

upvoted 1 times

shubhambala 1 year ago

Agreed!

upvoted 1 times

Yasyas86 Highly Voted 10 months ago

The Correct order is :
.128
.240
.248
.224 : About this ..... it already stated that the 209.165.202.0/27 is subnetted into 1 subnet which is 209.165.202.128 the 5th available subnet for /27 they go as (first 0-31, second 32-63, third 64-95 , Fourth 96-127 AND the 5th 128-160 etc...)

upvoted 9 times

Divino Most Recent 10 months, 3 weeks ago

Correct order:
.128
.240
.248
.252

upvoted 5 times

purenuker 9 months, 1 week ago

The last one is not .252 but .224

upvoted 3 times

chathu123 11 months ago

Who is faced exam in this month and passed ?

upvoted 2 times

dmaster42 11 months ago

i am agree with MikD4016 /27 ----->32 magic number

upvoted 2 times

Question #481 *Topic 1*

```
R1# show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S* 0.0.0.0/0 is directly connected, Serial0/0/1
    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.2.0/24 is directly connected, GigabitEthernet0/0
L       172.16.2.2/32 is directly connected, GigabitEthernet0/0
C       172.16.4.0/21 is directly connected, Serial0/0/1
L       172.16.8.2/26 is directly connected, Serial0/0/1
```

Refer to the exhibit. What is the subnet mask for route 172.16.4.0?

A. 255.255.255.192

B. 255.255.254.0

C. 255.255.248.0

D. 255.255.240.0

Correct Answer: *C*

Chongste 1 month, 1 week ago

/21 is 21 bit for network address, so 21 bits = (16 + 5)bits 255.255 takes up 16bits, another 5 bits = 1111000 = 248. hence /21 = 1111 1111 . 1111 1111 . 1111 1000 . 0000 0000 = 255.255.248.0

upvoted 1 times

SAEEDOM 2 months ago

cn u explain please ?

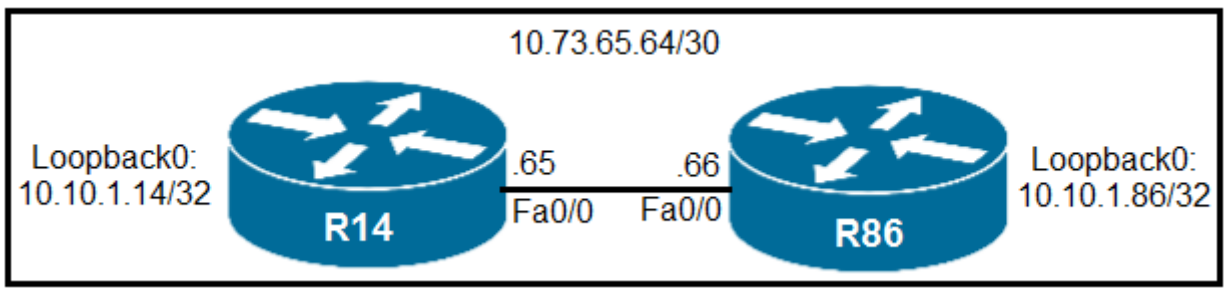
upvoted 1 times

f2killer 4 months ago

The given answer is correct

upvoted 1 times

Question #482 *Topic 1*



Refer to the exhibit. A static route must be configured on R14 to forward traffic for the 172.21.34.0/25 network that resides on R86. Which command must be used to fulfill the request?

A. ip route 172.21.34.0 255.255.255.192 10.73.65.65

B. ip route 172.21.34.0 255.255.255.128 10.73.65.66

C. ip route 172.21.34.0 255.255.255.0 10.73.65.65

D. ip route 172.21.34.0 255.255.128.0 10.73.65.64

Correct Answer: *B*

Thaier 1 month, 2 weeks ago

Selected Answer: B

The way i see it it, these routes will not work any way on R14, cause the destination network is directly connected.

upvoted 1 times

```
R1#show ip ospf interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.1.2/24, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type POINT-TO-POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 15, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)

R2#show ip ospf interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 15, Dead 45, Wait 15, Retransmit 5
    Hello due in 00:00:11
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
```

Refer to the exhibit. The network engineer is configuring router R2 as a replacement router on the network. After the initial configuration is applied, it is determined that R2 failed to show R1 as a neighbor. Which configuration must be applied to R2 to complete the OSPF configuration and enable it to establish the neighbor relationship with R1?

A. R2(config)#router ospf 1 R2(config-router)#network 192.168.1.0 255.255.255.0 area 2

B. R2(config)#interface g0/0/0 R2(config-if)#ip ospf hello-interval 10

C. R2(config)#interface g0/0/0 R2(config-if)#ip ospf dead-interval 40

D. R2(config)#router ospf 1 R2(config-router)#router-id 192.168.1.2

Correct Answer: *C*
For OSPF the hello and dead timers must match to become neighbors. R1 is configured with a dead time of 40 seconds, while R2 is set to 45 seconds.

Shanku97 2 weeks ago
is it okay to have different wait timing in two router ?
upvoted 1 times

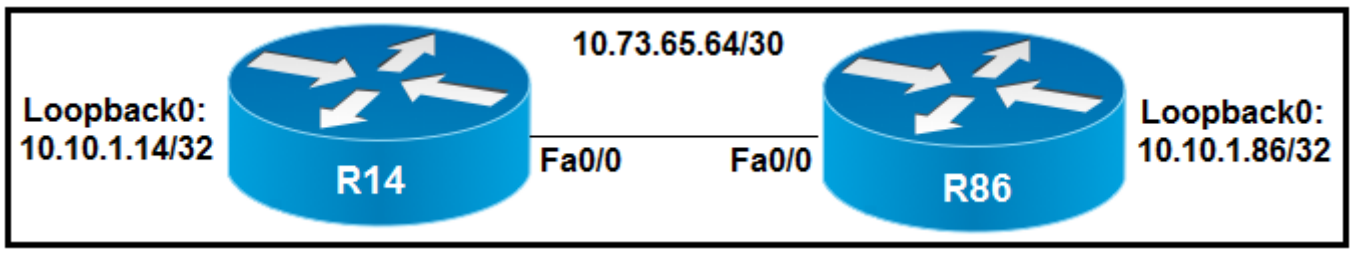
dropspablo 1 month, 2 weeks ago
Selected Answer: C
Answer is correct. Only change "ip ospf dead-interval 40" in R2
upvoted 2 times

rx78_2 5 months, 1 week ago
Selected Answer: B
B and C should both be implemented to achieve the result
upvoted 1 times

studying_1 4 months, 1 week ago
No, on R2 hello timer is 15, so we only need to change the dead timer
upvoted 1 times

studying_1 4 months, 1 week ago
sorry, i meant on R1
upvoted 1 times

Question #484 *Topic 1*



Refer to the exhibit. All interfaces are configured with duplex auto and ip ospf network broadcast. Which configuration allows routers R14 and R86 to form an
OSPFv2 adjacency and act as a central point for exchanging OSPF information between routers?

A. R14# interface FastEthernet0/0 ip address 10.73.65.65 255.255.255.252 ip ospf priority 255 ip mtu 1500 router ospf 10 router-id 10.10.1.14 network 10.10.1.14 0.0.0.0 area 0 network 10.73.65.64 0.0.0.3 area 0 R86# interface FastEthernet0/0 ip address 10.73.65.66 255.255.255.252 ip mtu 1400 router ospf 10 router-id 10.10.1.86 network 10.10.1.86 0.0.0.0 area 0 network 10.73.65.64 0.0.0.3 area 0

B. R14# interface Loopback0 ip ospf 10 area 0 interface FastEthernet0/0 ip address 10.73.65.65 255.255.255.252 ip ospf 10 area 0 ip mtu 1500 router ospf 10 ip ospf priority 255 router-id 10.10.1.14 R86# interface Loopback0 ip ospf 10 area 0 interface FastEthernet0/0 ip address 10.73.65.66 255.255.255.252 ip ospf 10 area 0 ip mtu 1500 router ospf 10 router-id 10.10.1.86

C. R14# interface FastEthernet0/0 ip address 10.73.65.65 255.255.255.252 ip ospf priority 0 ip mtu 1500 router ospf 10 router-id 10.10.1.14 network 10.10.1.14 0.0.0.0 area 0 network 10.73.65.64 0.0.0.3 area 0 R86# interface FastEthernet0/0 ip address 10.73.65.66 255.255.255.252 ip mtu 1500 router ospf 10 router-id 10.10.1.86 network 10.10.1.86 0.0.0.0 area 0 network 10.73.65.64 0.0.0.3 area 0

D. R14# interface Loopback0 ip ospf 10 area 0 interface FastEthernet0/0 ip address 10.73.65.65 255.255.255.252 ip ospf priority 255 ip ospf 10 area 0 ip mtu 1500 router ospf 10 router-id 10.10.1.14 R86# interface Loopback0 ip ospf 10 area 0 interface FastEthernet0/0 ip address 10.73.65.66 255.255.255.252 ip ospf 10 area 0 ip mtu 1500 router ospf 10 router-id 10.10.1.86

Correct Answer: *A*

joondale Highly Voted 1 year ago

Selected Answer: D

Going with D
A is wrong because ip mtu of R14 and R86 are different
B is wrong because because ip ospf priority is configured inside router-config, it should be on the interface
C is wrong because ip ospf priority is 0 on R14 and it makes R14 not participate on ospf dr/bdr election, the network type is broadcast so i assume dr/bdr should be elected otherwise the network type should be point-to-point
D is correct answer - because mtu are same for both routers, participates in dr/bdr election

upvoted 32 times

LeonardoMeCabrio 1 month, 2 weeks ago

Shouldnt there be Network commands in D. like there are in C.? Cause I dont see any.

upvoted 1 times

spazzix 3 weeks, 5 days ago

You can enable OSPF on a per-interface basis with:
ip ospf <PROCESS ID> area <AREA #>
command in an interface config

That can do the exact same thing as
network <IP> <WILDCARD MASK> area <AREA #>

The benefit of the network command is it allows you activate multiple interfaces at once
The downside of the network command is that it may unintentionally add a network into OSPF that you didn't want to. Especially if you configure another subnet or interface down the road.

upvoted 3 times

shubhambala Highly Voted 1 year ago

Selected Answer: D

A is wrong!

upvoted 6 times

tubirubs Most Recent 1 month, 1 week ago

Selected Answer: D

WTFFFFF. A have a diferente size of MTU! 1400 and 1500. its the 1st for exclude. lol this dump is very dump

upvoted 1 times

zFlyingLotusz 1 month, 3 weeks ago

I'm literally skipping these questions.
upvoted 1 times

TechJ 3 months, 2 weeks ago

Selected Answer: D

going with D,

A is clearly wrong due to MTU mismatch
For the people that think D is wrong, you need to look at the entire command line, because I got tricked at the beginning as well.
It does provide "ip ospf 10 area 0" on both the loopback and actual interface (not just loopback only)
upvoted 1 times

krzysiew 3 months, 2 weeks ago

Selected Answer: C

An OSPF priority of 0 does not prevent the router from establishing OSPF adjacencies.
upvoted 1 times

perri88 3 months ago

When you set the OSPF priority to 0, that router becomes ineligible for being the DR/BDR on that segment, which is exactly what you see when it is in DROTHER state. This is the state a OSPF neighbor is in, if it is not acting as the DR or BDR. An OSPF priority of 0 does not prevent the router from establishing OSPF adjacencies.
upvoted 1 times

dropspablo 3 months, 3 weeks ago

Selected Answer: D

Router with "priority 0" and another with "priority default (1)" formed adjacency and exchanged LSAs and LSDBs normally (I tested it in P.Trace and OSPF dynamic routing works normally), the difference is that there will not be a DR Backup in case fail (that's all). One will be DR Other (neighbor Full/DR) and one DR (neighbor Full/DROther), and BDR appears written that it does not exist, because priority 0 cannot be neither DR nor BDR. (Observation: "point-to-point type" is recommended for this type of connection.)
However, the exercise asks them to act as a central point for exchanging information, in this case "it gives the impression" that he asked us to select a "DR". Letter "D" would be the most correct because using "ip ospf priority 255" (in the interface) we define R14 as DR.
upvoted 2 times

[Removed] 4 months ago

Selected Answer: D

Tested in packet tracer.
A. OSPF neighborship was established even with mismatched MTU.
B. You cannot enter this command on R14: router ospf 10 - ip ospf priority 255
C. OSPF neighborship was established R14 will be FULL/DROTHER, R86 will be DR so it cannot be the central point for exchanging OSPF information between routers
D. OSPF neighborship was established
upvoted 2 times

MJBM 4 months ago

C is for me.
A is mtu issue
B is network issue
D is network issue
upvoted 1 times

linuxlife 4 months, 3 weeks ago

as per the standard OSPF specification defined in RFC 2328, “OSPF Version 2”. Specifically the RFC states the following:

10.6 - Database Description Packet.
If the Interface MTU field in the Database Description packet indicates an IP datagram size that is larger than the router can accept on the receiving interface without fragmentation, the Database Description packet is rejected.

Basically this means that if a router tries to negotiate an adjacency on an interface in which the remote neighbor has a larger MTU, the adjacency will be denied. The idea behind this check is two-fold. The first is to alleviate a problem in the data plane, in which a sending host transmits packets to a receiver that are too large to accept. Typically, Path MTU Discovery (PMTUD) should be implemented on the sender to prevent this case, however this process relies on ICMP messages that could possibly be filtered out in the transit path due to a security policy. The second, and most important issue, is to alleviate a problem in the control plane in which OSPF packets are exchanged.
upvoted 1 times

daddydagoth 6 months, 3 weeks ago

Selected Answer: D

It's absolutely D
upvoted 4 times

gewe 7 months ago

option A would be best if MTU match...
option D has no routes advertised...
upvoted 3 times

Netcmd 10 months ago

D is wrong because the network cmd is not configured for the networks. How can you form neighbours without it

upvoted 4 times

Ceruzka 6 months ago

IMHO correct is "C" I agree with Netcmd. @joondale comment: Priority 0 on R14 just mean that this intf will neither be DR nor BDR, but it will work. So for me "C"

upvoted 2 times

Ceruzka 6 months ago

my BAD, looks like D" is correct.

upvoted 1 times

Ceruzka 6 months ago

intf are advertised instead with cmd "ip ospf 10 area 0" so no network cmd needed in router ospf process..

upvoted 1 times

mzu_sk8 10 months ago

ip ospf 10 area 0 subinterface command, does the same , is even better , it has preemption over "network" command

upvoted 7 times

GigaGremlin 11 months, 1 week ago

Selected Answer: D

D is the correct answer

upvoted 1 times

nicombe 11 months, 3 weeks ago

I'm also going with D. While OSPF Routers can create an adjacancy having mismatched MTUs, they won't be able to exchange LSDBs and therefore won't be able to act as a central point for exchanging OSPF information between routers.

upvoted 1 times

g_mindset 1 year ago

Selected Answer: A

A is correct. The IP OSPF priority is key here. The two routers are set as the highest priority making them DR and BDR.

upvoted 1 times

arenjenkins 11 months, 2 weeks ago

but they have different mtu configured

upvoted 10 times

[Removed] 2 months, 3 weeks ago

True so it can't be A

upvoted 1 times

Question #485 *Topic 1*

A packet from a company's branch office is destined to host 172.31.0.1 at headquarters. The sending router has three possible matches in its routing table for the packet: prefixes 172.31.0.0/16, 172.31.0.0/24, and 172.31.0.0/25. How does the router handle the packet?

A. It sends the traffic via prefix 172.31.0.0/24.

B. It sends the traffic via prefix 172.31.0.0/16.

C. It sends the traffic via prefix 172.31.0.0/25.

D. It sends the traffic via the default gateway 0.0.0.0/0.

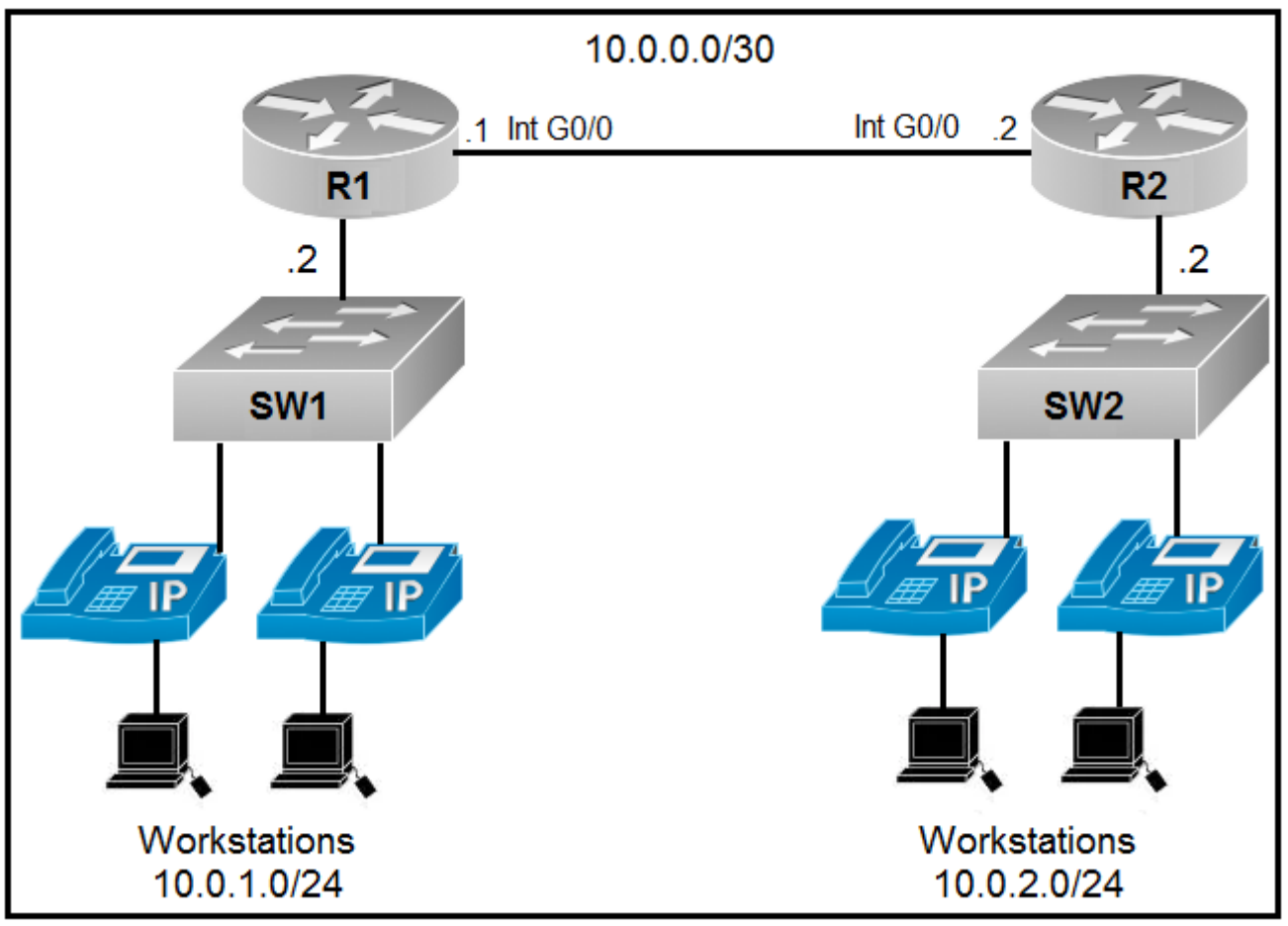
Correct Answer: *C*

Goh0503 Highly Voted 10 months, 3 weeks ago

Answer: C
how a router makes a forwarding decision by
a Longest match >>b Administrative distance >>c Routing protocol metric, in this order

upvoted 7 times

Question #486 *Topic 1*



Refer to the exhibit. An engineer is asked to configure router R1 so that it forms an OSPF single-area neighbor relationship with R2. Which command sequence must be implemented to configure the router?

A. router ospf 100 network 10.0.0.0 0.0.0.252 area0 network 10.0.1.0 0.0.0.255 area0

B. router ospf 100 network 10.0.0.0 0.0.0.3 area0 network 10.0.2.0 255.255.255.0 area0

C. router ospf 10 network 10.0.0.0 0.0.0.3 area0 network 10.0.1.0 0.0.0.255 area0

D. router ospf 10 network 10.0.0.0 0.0.0.3 area0 network 10.0.2.0 0.0.0.255 area0

Correct Answer: *C*

Sdiego Highly Voted 7 months, 3 weeks ago

Selected Answer: C

Forget about that comment, R1 advertises his networks, so C is correct.

upvoted 5 times

FALARASTA 4 months, 2 weeks ago

I understand now about the second part. Thanks

upvoted 2 times

Goena Most Recent 7 months, 2 weeks ago

Selected Answer: C

Answer C:
Configure route to 10.0.0.0/30 with wildcard 0.0.0.3
Confugure route to 10.0.1.0/24 with wildcard 0.0.0.255
router ospf 10 network 10.0.0.0 0.0.0.3 area0 network 10.0.1.0 0.0.0.255 area0

upvoted 2 times

Sdiego 7 months, 3 weeks ago

Selected Answer: D

R1 has to reach 10.0.2.0 network, 10.0.1.0 is directly connected

upvoted 1 times

Sdiego 7 months, 3 weeks ago

Forget about that comment, R1 advertises his networks, so C is correct.

upvoted 1 times

EthanhuntMI6 8 months, 3 weeks ago

Why not D?

upvoted 4 times

laurvy36 7 months, 2 weeks ago

Because you need to advertise 10.0.1.0, on R1, no 10.0.2.0, that is on R2.

upvoted 1 times

alejandro12 9 months, 4 weeks ago

Should be a, same format
router ospf 100 network 10.0.0.0 0.0.0.252 area0 network 10.0.1.0 0.0.0.255 area0

upvoted 1 times

andresfjardim 9 months, 2 weeks ago

No, C is correct because wildcard mask for 10.0.0.0/30 is 0.0.0.3

upvoted 5 times

MEDO95 8 months ago

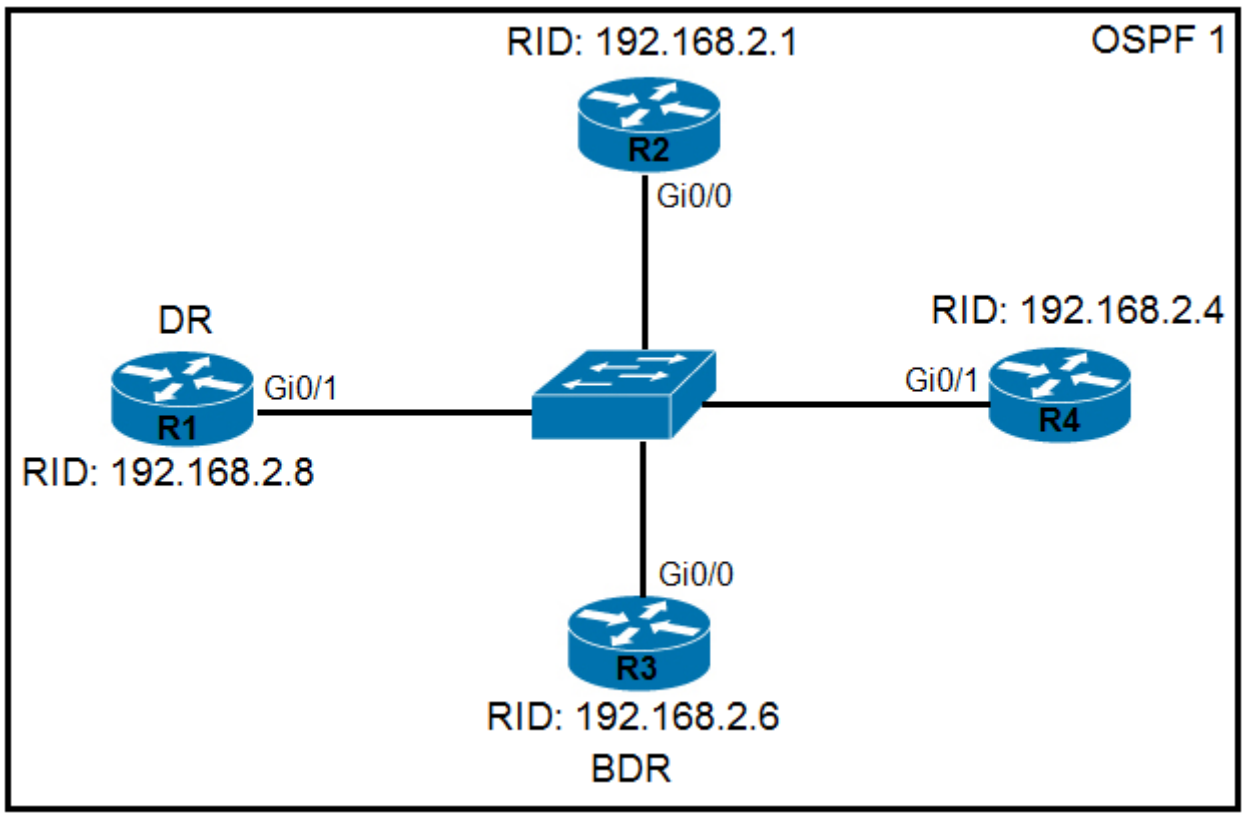
i think d has the same wildcard. why we didnt choose it

upvoted 1 times

laurvy36 7 months, 2 weeks ago

Because you need to advertise 10.0.1.0, on R1, no 10.0.2.0, that is on R2.

upvoted 2 times



Refer to the exhibit. All routers in the network are configured. R2 must be the DR. After the engineer connected the devices, R1 was elected as the DR. Which command sequence must be configured on R2 to be elected as the DR in the network?

A. R2(config)#intergface gi0/0 R2(config-if)#ip ospf priority 100

B. R2(config)#router ospf 1 R2(config-router)#router-id 192.168.2.7

C. R2(config)#router ospf 1 R2(config-router)#router-id 10.100.100.100

D. R2(config)#intergface gi0/0 R2(config-if)#ip ospf priority 1

Correct Answer: *A*

all4one 3 months, 2 weeks ago

Selected Answer: A

R1 was initially elected as the DR because they would have the same priority by default (1). The next step in the election process would be the highest IP address which R1 has over R2. Thus, setting the priority of R2 to 100 would elect it as DR. The highest priority wins for DR once it is within scope.

upvoted 1 times

[Removed] 4 months ago

Selected Answer: A

B. R2's new router ID 192.168.2.7 is still lower than R1's 192.168.2.8
C. R2's new router ID 10.100.100.100 is still lower than R1's 192.168.2.8
D. The OPSF priority is 1 by default, all routers have the same.

upvoted 1 times

VictorCisco 5 months, 3 weeks ago

R1 is elected because the highest ID, so if change ID on R2 on higher it will be elected as DR.
so C is correct. Moreover there is a spelling mistake in A.

upvoted 1 times

Elidor 9 months, 3 weeks ago

intergface

upvoted 2 times

cormorant 10 months, 2 weeks ago

simple. you must specify a priority that is higher (thus lower) than the default 90 of OSPF; then you use priority 100

upvoted 2 times

purenuker 9 months, 1 week ago

You are making a mistake , my friend. AD has nothing to do with priority.

upvoted 6 times

Sara_Yus 9 months, 2 weeks ago

do you mean the administrative distance? the ad of ospf is 110. eigrp is 90.
the port of ospf is 89, but i dont think that is considered in the answer

upvoted 2 times

DoBronx 10 months, 3 weeks ago

intergface

upvoted 2 times

Customexit 11 months ago

intergface

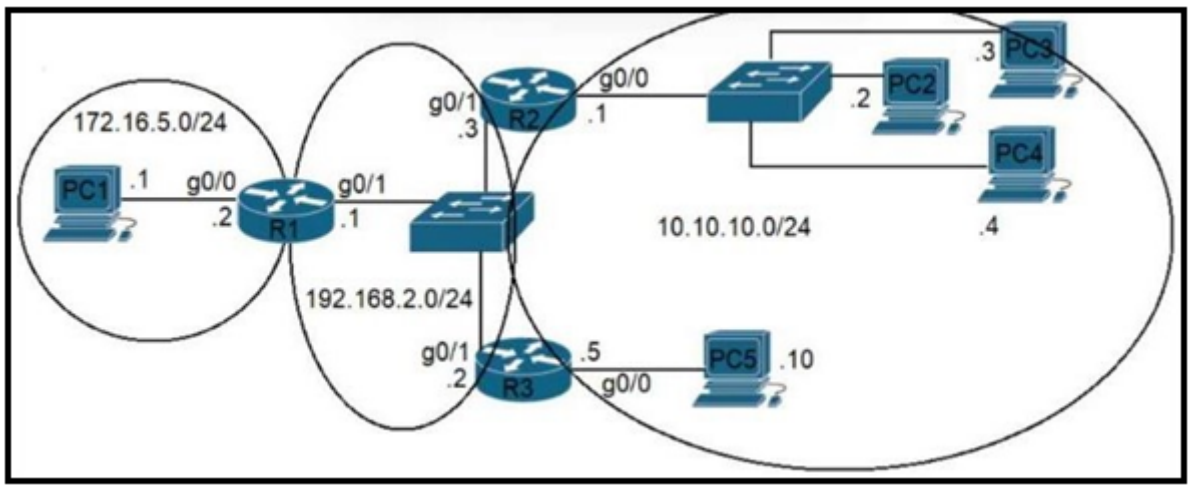
upvoted 2 times

Sutokuto 12 months ago

intergface

upvoted 4 times

Question #488 *Topic 1*



Refer to the exhibit. The router R1 is in the process of being configured. Routers R2 and R3 are configured correctly for the new environment. Which two commands must be configured on R1 for PC1 to communicate to all PCs on the 10.10.10.0/24 network? (Choose two.)

A. ip route 10.10.10.0 255.255.255.0 192.168.2.3

B. ip route 10.10.10.10 255.255.255.255 192.168.2.2

C. ip route 10.10.10.10 255.255.255.255 g0/1

D. ip route 10.10.10.8 255.255.255.248 g0/1

E. ip route 10.10.10.0 255.255.255.248 192.168.2.2

Correct Answer: *AE*

Freddy01 Highly Voted 9 months, 4 weeks ago

A is 100% correct while the confusion between B and E is down to people missing two important differences for those two options. B is a direct host route and it will show up in the routing table as 10.10.10.10/32 and it is called a host route. Hence subnet mask being 255.255.255.255. Whereas, E option does NOT cover the host 10.10.10.10 address as if you calculate the subnet range for the subnet in option E it only goes up to 10.10.10.0 - 10.10.10.6 and .7 being its broadcast address. It's incrementing in blocks of 8 as the subnet mask clearly states 255.255.255.248 or /29. So, how exactly the router would send traffic to host .10 which is NOT even in the subnet range. Therefore, option E route will NEVER reach .10 host hanging off that router.

Correct answer is A is the network route and B is direct host route, hope this helps :)

upvoted 18 times

Cracked76 Highly Voted 1 year ago

A and B

upvoted 16 times

fabitadj Most Recent 5 days, 21 hours ago

A y B es la correcta

upvoted 1 times

BAT47 3 weeks ago

A and B

upvoted 2 times

mda2h 1 month, 3 weeks ago

Selected Answer: AB

Anyone knows why C is wrong?

upvoted 1 times

Jessi2302 1 month, 3 weeks ago

if you send the packet through the interface Gi0/1, you have 2 ways, R2 and R3, so we need specify the next hop in this case, with the IP.

upvoted 2 times

gewe 7 months ago

AB is correct.

can't be E coz mask is not appropriate

upvoted 5 times

4aynick 8 months ago

Selected Answer: AB

10.10.10.0 255.255.255.248
Usable address range 10.10.10.1 to 10.10.10.6

upvoted 2 times

leooel 9 months ago

Selected Answer: AB

AB is correct

upvoted 1 times

Netcmd 10 months ago

Selected Answer: AE

A for sure but for our next answer is E
Lets take a look at the other two posiible answer below:
B)ip route 10.10.10.10 255.255.255.255 192.168.2.2
E) ip route 10.10.10.0 255.255.255.248 192.168.2.2
B tells the router it can only go to the 10.10.10.10 host. We can see that this is not a valid host.
We are left with E. which if you do subletting can see you can reach each host that is configured.
The problem with both B and E is that they are configure with the wrong next hop address for the intended network. We will relay on the router to route us over to the correct network

upvoted 1 times

[Removed] 2 months, 3 weeks ago

How is 10.10.10.10 not a valid host? It's PC5's ip address. It's valid. Answer B is the host route to PC5.

upvoted 1 times

enzo86 5 months ago

you need to study more if you want to pass that exam

upvoted 4 times

Netcmd 9 months, 4 weeks ago

after looking at this the Answer is AB

upvoted 6 times

DoBronx 10 months, 3 weeks ago

Selected Answer: AB

AB for sure

upvoted 1 times

Etidic 10 months, 3 weeks ago

Selected Answer: AB

A & B is correct

upvoted 1 times

payam_avar 11 months, 2 weeks ago

This question is false.
A is right, But none other one seems to be correct!

upvoted 3 times

[Removed] 11 months, 2 weeks ago

I almost punched my computer. Are they purposely trying give us wrong answers? A and B is the answer. E ranges from 10.10.10.0-10.10.10.7. 10.10.10.10 is out of the range.

upvoted 2 times

FALARASTA 4 months, 2 weeks ago

10.10.10.10 is in another network

upvoted 1 times

arenjenkins 11 months, 2 weeks ago

a and b, the subnet of d does not exist

upvoted 1 times

ukguy 11 months, 4 weeks ago

A AND B for sure

upvoted 1 times

g_mindset 1 year ago

Selected Answer: AB

A & B! Why would it be E??

upvoted 4 times

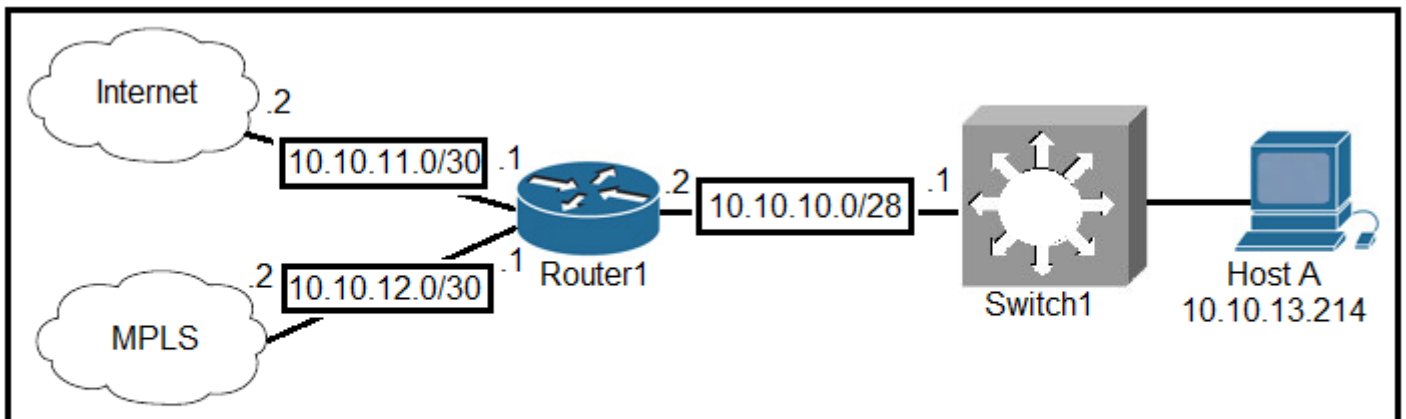
guynetwork 1 year ago

Selected Answer: AB

its a and b

upvoted 4 times

Question #489 *Topic 1*




```
Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0

  209.165.200.0/27 is subnetted, 1 subnets
B   209.165.200.224 [20/0] via 10.10.12.2, 03:22:14
  209.165.201.0/27 is subnetted, 1 subnets
B   209.165.201.0 [20/0] via 10.10.12.2, 02:26:33
  209.165.202.0/27 is subnetted, 1 subnets
B   209.165.202.128 [20/0] via 10.10.12.2, 02:26:03
   10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C  10.10.10.0/28 is directly connected, GigabitEthernet0/0
C  10.10.11.0/30 is directly connected, FastEthernet2/0
C  10.10.12.0/30 is directly connected, GigabitEthernet0/1
O  10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O  10.10.13.128/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O  10.10.13.144/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O  10.10.13.160/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O  10.10.13.208/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
S* 0.0.0.0/0 [1/0] via 10.10.11.2
```

Refer to the exhibit. What is the subnet mask of the route to the 10.10.13.160 prefix?

A. 255.255.255.240

B. 255.255.255.128

C. 255.255.248.0

D. 255.255.255.248

Correct Answer: *D*

dozer86 Highly Voted 5 months, 2 weeks ago

D THE DESTINATION IS THE NETWORK 10.10.13.160 WITH MASK /29 WHICH IS THE ANSWER D. THE OTHER ROUTES DO NOT COVER THE NETWORK.160

upvoted 7 times

e072f83 Most Recent 1 week, 6 days ago

Selected Answer: D

D = correct

upvoted 1 times

lennylopes 2 weeks, 3 days ago

Selected Answer: D

/29 is 255.255.255.248 or /5 in the last octet, which is 11111000, which is 248.

upvoted 1 times

raul_kapone 2 weeks, 6 days ago

Selected Answer: D

- Analyzing the subnet:
10.10.13.144/28

- Last octet:
.144 = 1001/0000

- Range of addresses in this subnet:
10.10.13.144/28
...
10.10.13.159/29

- So, 10.10.13.144/28 never reaches to the 10.10.13.60 route.
upvoted 1 times

Yinxs 3 weeks, 5 days ago

Selected Answer: D

THe route is the record ""O 1010.13.160/29 [110/2] via 10.10.10.1...", It's not specific to the ip of next hop. So the network mask of the route is 29.
upvoted 1 times

VarDav 1 month ago

Selected Answer: D

So many wrong answers in the comments
upvoted 1 times

tubirubs 1 month, 1 week ago

Selected Answer: A

f$ck this DUMP! lol. another question wrong..... i dont know. if anyone try the ccna 200-301 only for this dump questions, you spend your money!
upvoted 2 times

dropspablo 1 month, 2 weeks ago

Selected Answer: D

route 10.10.13.160/29 (MAK=255.255.255.248). Answer correct is D
upvoted 1 times

mda2h 1 month, 3 weeks ago

Selected Answer: A

subnet mask of the route, i.e.: 10.10.10.1
upvoted 1 times

valekky 3 months ago

A is the answer with the prefix /29 which is 255.255.255.240 subnet mask
upvoted 1 times

dropspablo 1 month, 2 weeks ago

prefix /29 is 255.255.255.248. Answer correct is D
upvoted 2 times

Goena 7 months, 2 weeks ago

Selected Answer: A

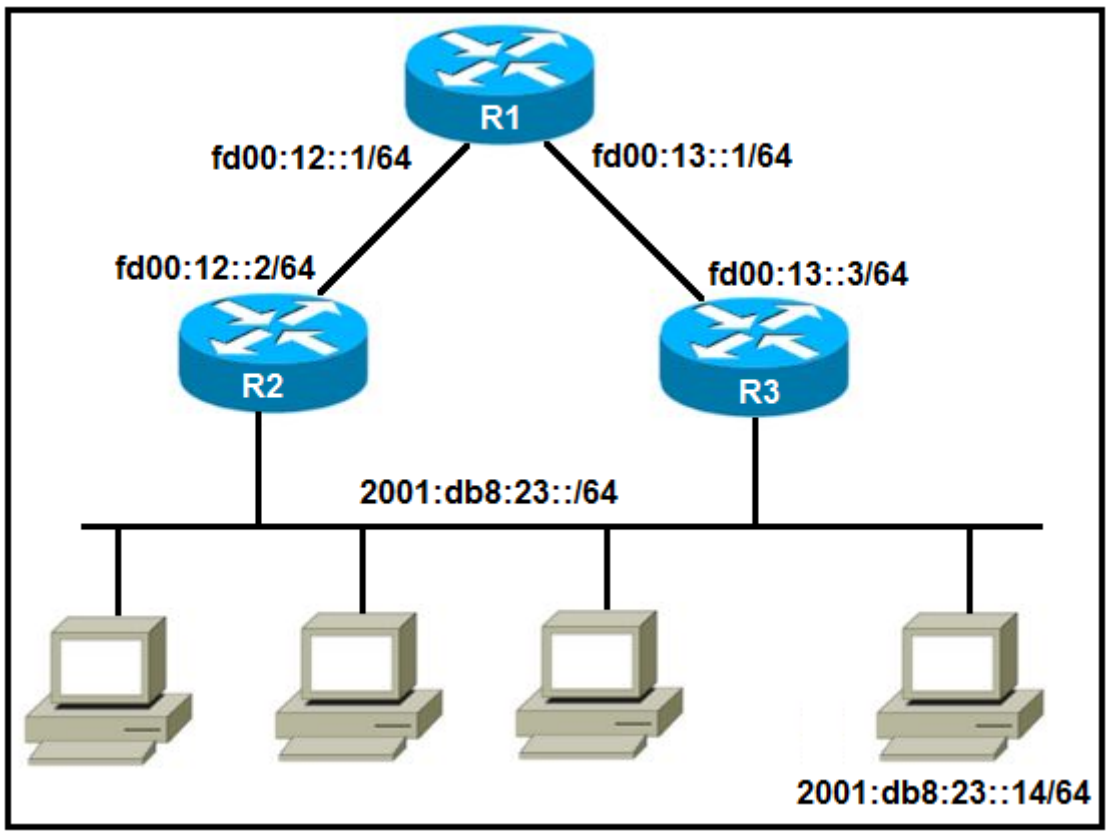
Answer A
upvoted 2 times

Vimal_1211 8 months, 3 weeks ago

Selected Answer: A

The route is 10.10.10.1 which is the IP address of G0/0. The latter forms part of the 10.10.10.0/28 network.
upvoted 1 times

Question #490 *Topic 1*



Refer to the exhibit. Which two commands, when configured on router R1, fulfill these requirements? (Choose two.)

☞ Packets toward the entire network 2001:db8:23::/64 must be forwarded through router R2.

Packets toward host 2001:db8:23::14 preferably must be forwarded through R3.

▪

A. ipv6 route 2001:db8:23::/128 fd00:12::2

B. ipv6 route 2001:db8:23::14/128 fd00:13::3

C. ipv6 route 2001:db8:23::/64 fd00:12::2

D. ipv6 route 2001:db8:23::14/64 fd00:12::2 200

E. ipv6 route 2001:db8:23::14/64 fd00:12::2

Correct Answer: *BC*

Cynthia2023 1 month ago

Selected Answer: BC

Give answers are correct

upvoted 1 times

Chopaka 2 months, 3 weeks ago

Can someone explain why the prefix of b 128 is? Makes confuse.. (Heb niet toegevoegd)

upvoted 1 times

studying_1 2 months, 3 weeks ago

because the destination is a host address(meaning ip address of the PC), not a network address, /128 in ipv6 is like /32 in ipv4

upvoted 3 times

mustdoit 7 months ago

C and D

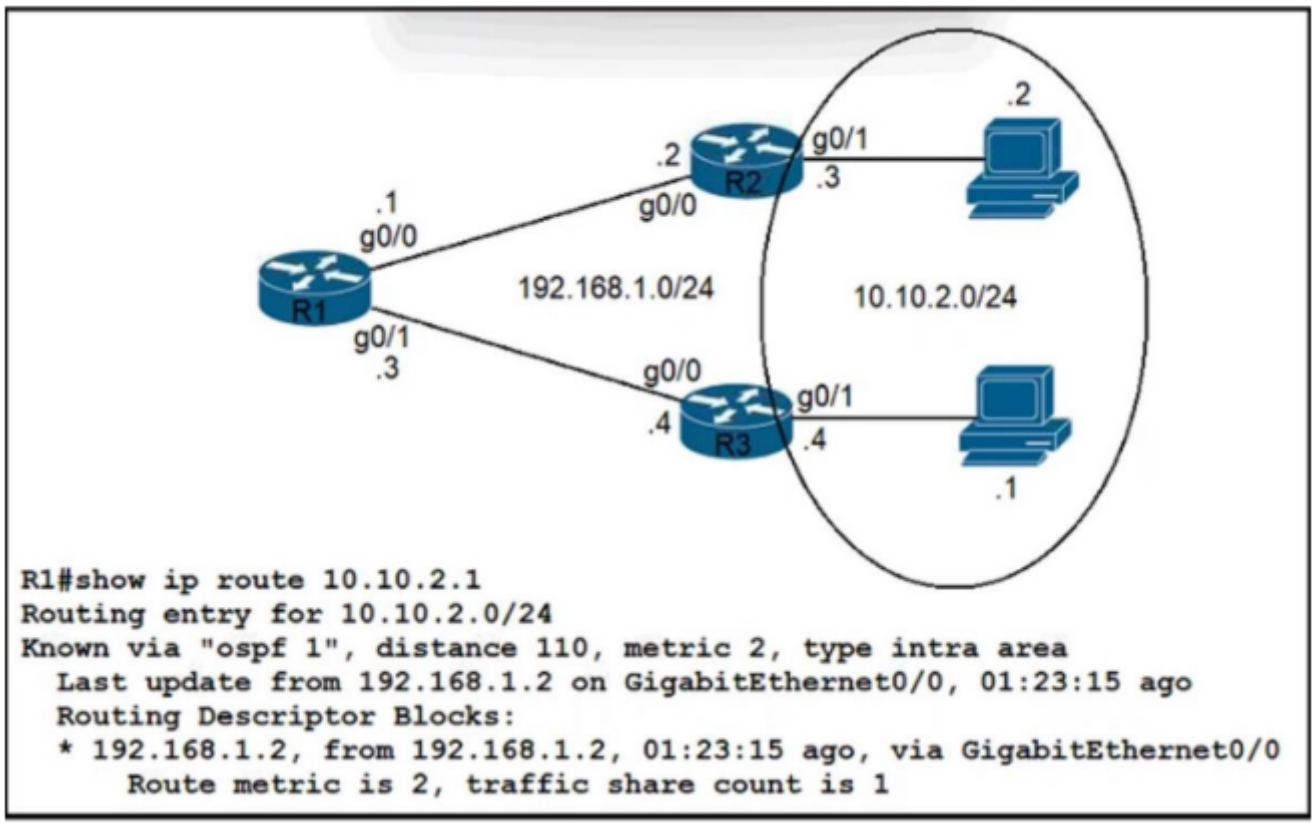
upvoted 1 times

Yannik123 5 months, 3 weeks ago

No B and C are correct

upvoted 6 times

Question #491 *Topic 1*



Refer to the exhibit. Traffic from R1 to the 10.10.2.0/24 subnet uses 192.168.1.2 as its next hop. A network engineer wants to update the R1 configuration so that traffic with destination 10.10 2.1 passes through router R3, and all other traffic to the 10.10.2.0/24 subnet passes through R2. Which command must be used?

A. ip route 10.10.2.1 255.255.255.255 192.168.1.4115

B. ip route 10.10.2.0 255.255.255.0 192.168.1.4115

C. ip route 10.10.2.0 255.255.255.0 192.168.1.4100

D. ip route 10.10.2.1 255.255.255.255192.168.1.4100

Correct Answer: *D*
Here we need to add a host route for the specific 10.10.2.1 host, which means using a subnet mask of 255.255.255.255. We also need to configure an
Administrative Distance that is less than the default OSPF AD of 115.

EliasM Highly Voted 10 months, 4 weeks ago
I dont understand why A and D are different. Host routes (/32) win because they have the longest prefix. Here, both A and D include the destination host, but they differ on AD. If you set the AD to 115, its higher than OSPF (110) but it will still prefer the longest prefix route, so i believe that A and D are both correct in this scenario. Correct me if im wrong.
upvoted 18 times

Garfieldcat Highly Voted 11 months, 1 week ago
by the way, AD of OSFP should be 110
upvoted 6 times

NICE_ANSWERS Most Recent 3 months, 2 weeks ago
Am i the only person seeing 192.168.1."4100" please, where from the last octect?
upvoted 3 times

[Removed] 2 months, 3 weeks ago
No, i do too. A space is missing
upvoted 2 times

TechJ 3 months, 2 weeks ago
Selected Answer: D
I feel like the route would work either with or without the AD(administrative distance).

I can see the reason why the answer is choosing the option with lower AD than 110(AD of OSPF), to prevent 10.10.2.1 route to R2 like all the other hosts in 10.10.2.0 network.

But just like other two comments said, we apply 10.10.2.1/32, the longest mask always win, so AD shouldnt be necessary.
upvoted 2 times

dropspablo 3 months, 3 weeks ago

In this case, I don't think the AD makes any difference (it can be anyone), because the longest mask always wins, it has the "/32 prefix", sending it to a specific host 10.10.2.1, it will go through R3 with any AD. And any other host on the 10.10.2.0/24 network will automatically go the OSPF route through R2. You can ignore the ADs, they are for distraction.

upvoted 3 times

danny43213 7 months, 2 weeks ago

We don't need to change the default AD

upvoted 4 times

alejandro12 9 months, 3 weeks ago

Answer A
The ad should be higher that route 110 ospf learned

upvoted 1 times

xbololi 2 months, 1 week ago

alejandro please don't share your wisdow... its not right to teach people untrue facts.

upvoted 1 times

IAmAlwaysWrongOnExamtopics 9 months, 1 week ago

definitely not, if the ad was higher, all the traffic to the subnet would go through R2, and the end host would never get traffic

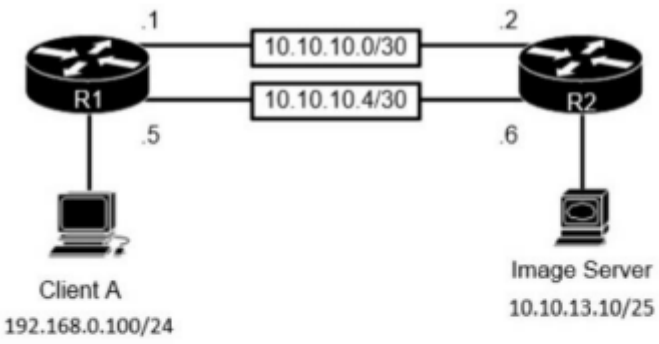
upvoted 11 times

Garfieldcat 11 months, 1 week ago

by default static route has AD 1, so no need to change AD to 100 if OSPF AD is 115

upvoted 1 times

Question #492 *Topic 1*




```
R1#show ip route
Gateway of last resort is 10.10.10.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 10.10.10.2

R2#show ip route
Gateway of last resort is 10.10.10.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 10.10.10.1
```

Refer to the exhibit. The image server and client A are running an application that transfers an extremely high volume of data between the two. An engineer is configuring a dedicated circuit between R1 and R2. Which set of commands must the engineer apply to the routers so that only traffic between the image server and client A is forces to use the new circuit?

A. R1(config)#ip route 10.10.13.10 255.255.255.255 10.10.10.6 R2(config)#ip route 192.168.0.100 255.255.255.255 10.10.10.5

B. R1(config)#ip route 10.10.13.10 255.255.255.128 10.10.10.6 R2(config)#lp route 192.168.0.100 255.255.255.0 10.10.10.5

C. R1(config)#ip route 10.10.13.10 255.255.255.252 10.10.10.6 R2(config)#tp route 192.168.0.100 255.255.255.252 10.10.10.5

D. R1(config)#ip route 10.10.13.10 255.255.255.255 10.10.10.2 R2(config)#ip route 192.168.0.100 255.255.255.255 10.10.10.1

Correct Answer: *D*

splashy Highly Voted 12 months ago

Selected Answer: A

D is "old" circuit
Somebody really needs to clean the answers for the new questions tbh...

upvoted 25 times

daddydagoth 6 months, 3 weeks ago

For real man, I imagine how many poor souls have been confused and even learned things wrongly because of the dumb answers on here. Never do brain dumps if you haven't fully finished studying kids.

upvoted 9 times

NICE_ANSWERS 3 months, 2 weeks ago

I guess i'm part of the poor souls for sure🤣🤣🤣

upvoted 3 times

shubhambala Highly Voted 1 year ago

Selected Answer: A

A answer

upvoted 7 times

shumps Most Recent 19 hours, 2 minutes ago

D is correct,

upvoted 1 times

BarkingSpider 2 days, 20 hours ago

Selected Answer: A

D indicates old circuit. Answer is A

upvoted 1 times

Mollyk 4 days, 20 hours ago

Answer is A- Host route

upvoted 1 times

BAT47 3 weeks ago

Selected Answer: A

Option A is Correct

upvoted 1 times

tubirubs 1 month, 1 week ago

Selected Answer: A

putz. another wrong question in this dump. lol noboddy check tease questions before post???

upvoted 2 times

tubirubs 1 month, 1 week ago

these questions

upvoted 1 times

mfaria 1 month, 1 week ago

Selected Answer: A

A is the circuit

upvoted 1 times

TEO1221768548956 1 month, 2 weeks ago

Selected Answer: A

A is correct because 10.6, and 10.5 are the new circuits, and the question also says just the image server and client so it needs to be host routes

upvoted 1 times

kyleptt 2 months, 3 weeks ago

A is the correct answer

upvoted 1 times

czolgczento 4 months, 1 week ago

Selected Answer: A

D is the old route, a new one has to be configured

upvoted 1 times

FALARASTA 4 months, 2 weeks ago

Selected Answer: A

D is the old route as shown from the configuration. Answer is A

upvoted 1 times

Ciscoman021 5 months, 2 weeks ago

Selected Answer: A

a dedicated circuit between R1 and R2.

upvoted 1 times

Ibrahim_32 7 months ago

A is correct answer

upvoted 1 times

gewe 7 months ago

A for 100%

upvoted 1 times

blue91235 8 months, 1 week ago

Looking at the subnet mask, shouldn't this be B? can somebody explain why is not B ?

upvoted 2 times

ddennis123 8 months ago

The question states that only traffic between those 2 hosts is supposed to go through the new circuit, therefore you need to use /32 masks

upvoted 6 times

NourElMasry 9 months, 4 weeks ago

Selected Answer: A

"A" is for the new circuit - correct answer
D is the old circuit - wrong answer

upvoted 4 times

Question #493 *Topic 1*

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/30 is directly connected, GigabitEthernet0/0
L       10.1.1.2/32 is directly connected, GigabitEthernet0/0
S    192.168.0.0/20 [1/0] via 10.1.1.1
     192.168.1.0/30 is subnetted, 1 subnets
S       192.168.1.0/30 [1/0] via 10.1.1.1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
S       192.168.2.0/28 [1/0] via 10.1.1.1
S       192.168.2.0/29 [1/0] via 10.1.1.1
```

Refer to the exhibit. An engineer is checking the routing table in the main router to identify the path to a server on the network. Which route does the router use to reach the server at 192.168.2.2?

A. S 192.168.0.0/20 [1/0] via 10.1.1.1

B. S 192.168.2.0/29 [1/0] via 10.1.1.1

C. S 192.168.2.0/28 [1/0] via 10.1.1.1

D. S 192.168.1.0/30 [1/0] via 10.1.1.1

Correct Answer: *B*

FALARASTA 4 months, 2 weeks ago

SOmeone to explain why /30 is wrong

upvoted 1 times

kyleptt 2 months, 3 weeks ago

look at the IP range carefully.

upvoted 4 times

studying_1 4 months, 1 week ago

because the range is 192,168.1.0 - 192.168.1.3, destination is 192.168.2.2.... it doesn't cover it, but 192.168.2.0/29 does, 192.168.2.0 - 192.168.2.7, so correct answer is B, hope that helps :)

upvoted 4 times

Hope_12 4 months, 1 week ago

192.168.1.0/30
inc=4

192.168.1.0 - 192.168.1.3
192.168.1.4

192.168.1.1 - 192.168.1.2 (Usable hosts)
192.168.2.2 is not in range in 192.168.1.0/30

Answer is B:192.168.2.0/29

upvoted 2 times

enzo86 5 months, 1 week ago

correct /29

upvoted 2 times

Goena 7 months, 2 weeks ago

Selected Answer: B

Answer B is correct.

upvoted 4 times

Refer to the exhibit. An OSPF neighbor relationship must be configured using these guidelines:

- R1 is only permitted to establish a neighbor with R2.
- R1 will never participate in DR elections.
- R1 will use a router-id of 10.1.1.1.

Which configuration must be used?

A.

```
interface FastEthernet0/0
  ip address 10.100.1.1 255.255.255.252
  ip ospf priority 0
  ip access-group 102 in

router ospf 10
  log-adjacency-changes
  network 10.1.1.1 0.0.0.0 area 0
  network 10.100.1.0 0.0.0.3 area 0
  router-id 10.1.1.1

access-list 102 permit 89 host 10.100.1.2 host 224.0.0.5
access-list 102 deny 89 any any
access-list 102 permit ip any any
```

B.

```
interface Loopback0
  ip address 10.1.1.1 255.255.255.255

interface FastEthernet0/0
  ip address 10.100.1.1 255.255.255.252
  ip ospf priority 100
  ip access-group 102 in

router ospf 10
  log-adjacency-changes
  network 10.1.1.1 0.0.0.0 area 0
  network 10.100.1.0 0.0.0.3 area 0
  ospf router-id 10.1.1.1

access-list 102 permit 88 host 10.100.1.2 host 224.0.0.5
access-list 102 deny 88 any any
access-list 102 permit ip any any
```

C.

```
interface FastEthernet0/0
  ip address 10.100.1.1 255.255.255.252
  ip ospf priority 100
  ip access-group 102 in

router ospf 10
  log-adjacency-changes
  network 10.1.1.1 0.0.0.0 area 0
  network 10.100.1.0 0.0.0.3 area 0
  ospf router-id 10.1.1.1

access-list 102 permit 89 host 10.100.1.2 host 224.0.0.5
access-list 102 deny 89 any any
access-list 102 permit ip any any
```

D.

```
interface Loopback0
  ip address 10.1.1.1 255.255.255.255

interface FastEthernet0/0
  ip address 10.100.1.1 255.255.255.252
  ip ospf priority 0
  ip access-group 102 in

router ospf 10
  log-adjacency-changes
  network 10.1.1.1 0.0.0.0 area 0
  network 10.100.1.0 0.0.0.3 area 0
  ospf router-id 10.1.1.1

access-list 102 permit 88 host 10.100.1.2 host 224.0.0.5
access-list 102 deny 88 any any
access-list 102 permit ip any any
```

Correct Answer: *A*

g_mindset Highly Voted 1 year ago

OSPF uses port 89 and does not use a transport protocol. A is the answer.
EIGRP port 88.

upvoted 24 times

f2killer 3 months, 4 weeks ago

if this is the right answer how the router id is gonna be 10.1.1.1?? In answer D the router id it will assign the loopback.

upvoted 1 times

f2killer 3 months, 4 weeks ago

iam wrong. i see now router id ...

upvoted 3 times

EthanhuntMI6 8 months, 3 weeks ago

Thank you.

upvoted 1 times

daddydagoth Highly Voted 6 months, 3 weeks ago

Another thing wrong with answer D is that the command "ospf router ID" is wrong. EIGRP's command is "EIGRP router ID", OSPF uses "Router ID"

upvoted 6 times

[Removed] 4 months ago

B, C, D all use ospf router ID.

upvoted 1 times

kyleptt Most Recent 2 months ago

Setting the Ospf priority as zero is the reason why A is the answer.

upvoted 1 times

OrwellMB 2 months, 1 week ago

Exhibit is:

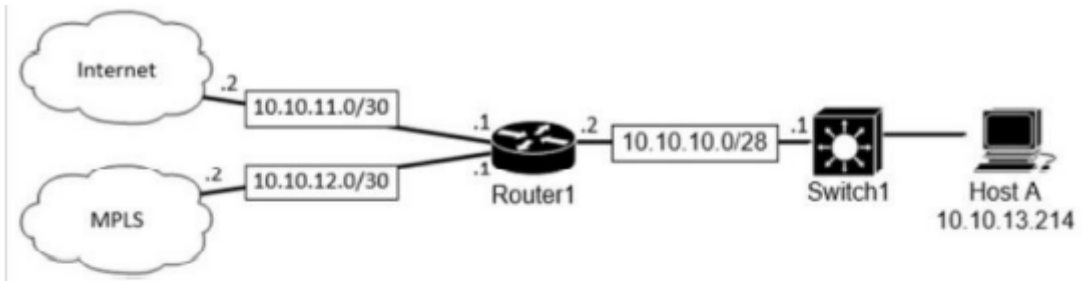
R1 -> Fa0/0 ".1"
connection line: 10.100.1.0
R2 -> Fa0/0 ".2"

that's it, no other info
upvoted 1 times

ccnk 2 months, 4 weeks ago
There is no exhibit.
upvoted 2 times

Olebogeng_G 3 months, 1 week ago
Where is the exhibit?
upvoted 2 times

[Removed] 2 months, 3 weeks ago
It's missing :(
upvoted 1 times




```
Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0

     209.165.200.0/27 is subnetted, 1 subnets
B       209.165.200.224 [20/0] via 10.10.12.2, 03:22:14
     209.165.201.0/27 is subnetted, 1 subnets
B       209.165.201.0 [20/0] via 10.10.12.2, 02:26:33
     209.165.202.0/27 is subnetted, 1 subnets
B       209.165.202.128 [20/0] via 10.10.12.2, 02:26:03
    10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C      10.10.10.0/28 is directly connected, GigabitEthernet0/0
C      10.10.11.0/30 is directly connected, FastEthernet2/0
C      10.10.12.0/30 is directly connected, GigabitEthernet0/1
O      10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O      10.10.13.128/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O      10.10.13.144/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O      10.10.13.160/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O      10.10.13.208/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.10.11.2
```

Refer to the exhibit. What is the prefix length for the route that router1 will use to reach host A?

A. /25

B. /27

C. /28

D. /29

Correct Answer: *D*

divn_01 1 month, 2 weeks ago

The correct Answer is C

The route selected by R1 is 10.10.13.208/29 but the prefix for that route is the 10.10.10.0/28 network prefix . Therefore, /28 . Please correct me if im wrong

upvoted 1 times

ananinamia 1 week, 6 days ago

you are worng. if i am wgron correct me

upvoted 1 times

zamkljo 5 months, 2 weeks ago

I think C is the correct one.
The route is 10.10.10.1 (to reach 10.10.13.214) which is the IP address of G0/0. The latter forms part of the 10.10.10.0/28 network. so should not be /28??

upvoted 1 times

daddydagoth 6 months, 3 weeks ago

Selected Answer: D

IT's D

upvoted 4 times

SVN05 7 months, 1 week ago

Selected Answer: D

Answer D /29 is correct. Why /29 cause lets see why

32 bit mask -29 bit mask=3 bits
2 to the power of 3 is 8 per subnet while 6 host in a subnet(2 power of 3 minus 2)

So 8 bits in a subnet. Take this questions example.
1st Subnet = 10.10.13.0 - 10.10.13.7
2nd Subnet = 10.10.13.8 - 10.10.13.15
3rd Subnet = 10.10.13.16 - 10.10.13.23
....
...
Some numbered Subnet later =10.10.13.208 - 10.10.13.216 so 10.10.13.214 is in the range so that's the answer right there

Reminder
Each subnet has a Network and Broadcast Bit so for knowing how many host in a subnet need to ALWAYS MINUS 2. That's why we minus 2(remember just now with 2 power of 3 minus 2 so yup).

upvoted 4 times

blue91235 8 months, 1 week ago

Why is /29 ?

upvoted 1 times

bertholdt 9 months, 1 week ago

Selected Answer: C

it's /28 on the routing table not /29

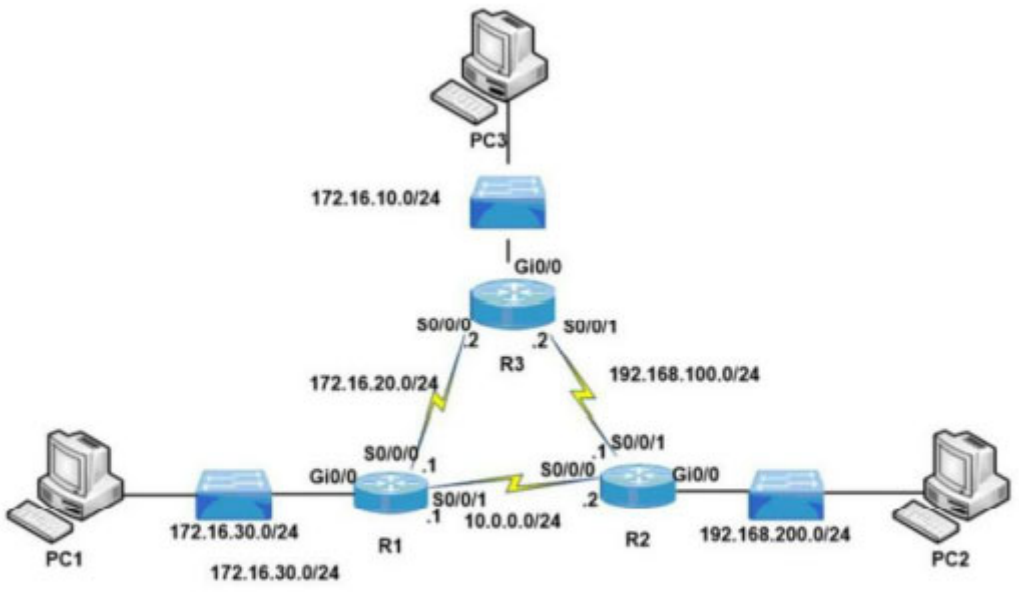
upvoted 2 times

braeiv123 7 months, 3 weeks ago

D makes sense. 10.10.13.208/29 via 10.1.0.10.1

upvoted 2 times

Question #496 *Topic 1*



R1(config)#**ip route 0.0.0.0 .0.0.0.0 172.16.20.2**
R1(config)#**ip route 0.0.0.0 0.0.0.0 10.0.0.2 20**

Refer to the exhibit. After applying this configuration to router R1, a network engineer is verifying the implementation. If all links are operating normally, and the engineer sends a series of packets from PC1 to PC3, how are the packets routed?

A. They are distributed sent round robin to interfaces S0/0/0 and S0/0/1

B. They are routed to 10.0.0.2

C. They are routed to 192.168.100.2

D. They are routed to 172.16.20.2

Correct Answer: *D*

papinski Highly Voted 7 months, 1 week ago

Selected Answer: D

D is correct.

upvoted 6 times

CAMBar Most Recent 5 days, 1 hour ago

Selected Answer: D

Assuming that the image has a typo on the first command, just before the mask (as @dosu01 as pointed out) and that the correct command was inserted as
"R1(Config)#ip route 0.0.0.0 0.0.0.0 172.16.20.2",
the route most packets will follow would be 172.16.20.2, due to the metric value 20 used on route 10.0.0.2 .
If it was not a typo, then the answer would be 10.0.0.2 (B).

upvoted 1 times

kyleptt 1 week ago

Selected Answer: D

correct

upvoted 1 times

Shanku97 2 weeks ago

care to explain anyone ?

upvoted 1 times

kyleptt 1 week ago

ok at the adjusted AD value of 20

upvoted 1 times

dosu01 9 months, 2 weeks ago

if you type the cmd "ip route 0.0.0.0 .0.0.0.0 172.16.20.1" you get "% Invalid input detected at '^' marker.".

upvoted 3 times

mellos 10 months, 2 weeks ago

"D" es correcto

upvoted 1 times

Question #497 *Topic 1*

```
R1#

Gateway of last resort is 10.56.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.56.0.1
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.56.0.0/16 is directly connected, Null0
C        10.56.0.0/26 is directly connected, Vlan58
C        10.56.0.0/17 is directly connected, Vlan59
C        10.56.0.0/24 is directly connected, Vlan60
```

Refer to the exhibit. When router R1 receives a packet with destination IP address 10.56.0.62, through which interface does it route the packet?

A. Vlan58

B. Null0

C. Vlan59

D. Vlan60

Correct Answer: *A*

blue91235 Highly Voted 8 months, 1 week ago

Answer A is the longest prefix and 62 inclusive in /26

upvoted 8 times

Chris1225 Most Recent 7 months ago

Selected Answer: A

I'm sure A is the correct answer
mask /26 seems 2^6 = 64 ,so 10.56.0.0/26 means
10.56.0.0 ~ 10.56.0.63 is the range,the broadcast is 10.56.0.63
and 10.56.0.62 is the final address can be used
refer to the routing table, /26 go to vlan 58, so choose A

upvoted 4 times

humanbot 10 months ago

Selected Answer: D

it uses vlan 60 route because it have the longest prefix length

upvoted 1 times

daddydagoth 6 months, 3 weeks ago

So /24 is longer than /26 in your eyes?

upvoted 5 times

humanbot 10 months ago

sorry A is the right answer

upvoted 10 times

Current Neighbor Relationship

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	FULL/DR	00:00:33	192.168.1.1	GigabitEthernet0/0

Desired Neighbor Relationship

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	0	FULL/-	00:00:31	192.168.1.1	GigabitEthernet0/0

Refer to the exhibit. How much OSPF be configured on the GigabitEthernet0/0 interface of the neighbor device to achieve the destined neighbor relationship?

A. Router(config)#interface GigabitEthernet 0/0 Router(config-if)#ip ospf cost 5

B. Router(config)#interface GigabitEthernet 0/0 Router(config-if)#ip ospf priority 1

C. Router(config)#interface GigabitEthernet 0/0 Router(config-if)#ip ospf area 2

D. Router(config)#interface GigabitEthernet 0/0 Router(config-if)#ip ospf network point-to-point

Correct Answer: *D*

raul_kapone 2 weeks, 6 days ago

Nice question:
1st imagine - Router is in a Broadcast network, and it is participating in a DR/BDR election.

2nd imagine - Router is configured with a Point-to-point network, thus it desn't participate in a DR/BDR election, and it acquire a priority of 0.

upvoted 1 times

Shri_Fcb10 4 months ago

Can we apply p2p on ethernet interface I thought it was for serial int

upvoted 2 times

kyleptt 2 months, 3 weeks ago

yes it's not only for serial connections it just forces no DR & BDR selection to occur

upvoted 1 times

Ciscoman021 5 months ago

Selected Answer: D

D is right answer.

upvoted 2 times

therandomjoke 5 months ago

Selected Answer: D

point to point no dr/bdr election----- connection ppp/hdlc h10 d40
broadcast use dr/bdr election-----connection eth/FDDI h10 d40

upvoted 2 times

VictorCisco 5 months, 3 weeks ago

I'm just curious , if it possible to configure PPP on Ethernet ports? I mean in OSPF?

upvoted 2 times

alejandro12 9 months, 4 weeks ago

Answer D
ip ospf network point-to-point -->no dr/bdr election
B is not correct -->the router would be dr/bdr

upvoted 2 times

icecool2019 11 months, 1 week ago

In a point to point routing setup, there would be no need to select DR/BDR, and also priority is 0.

upvoted 3 times

GigaGremlin 11 months, 1 week ago

Selected Answer: D

It took me a While to understand this Question and it would be very helpful to exchange it like:
How must OSPF be configured on the GigabitEthernet0/0 interface of the neighbor device to achieve the desired neighbor relationship?

upvoted 4 times

DoBronx 10 months, 3 weeks ago

THIS much OSPF

upvoted 3 times

IAmAlwaysWrongOnExamtopics 9 months, 1 week ago

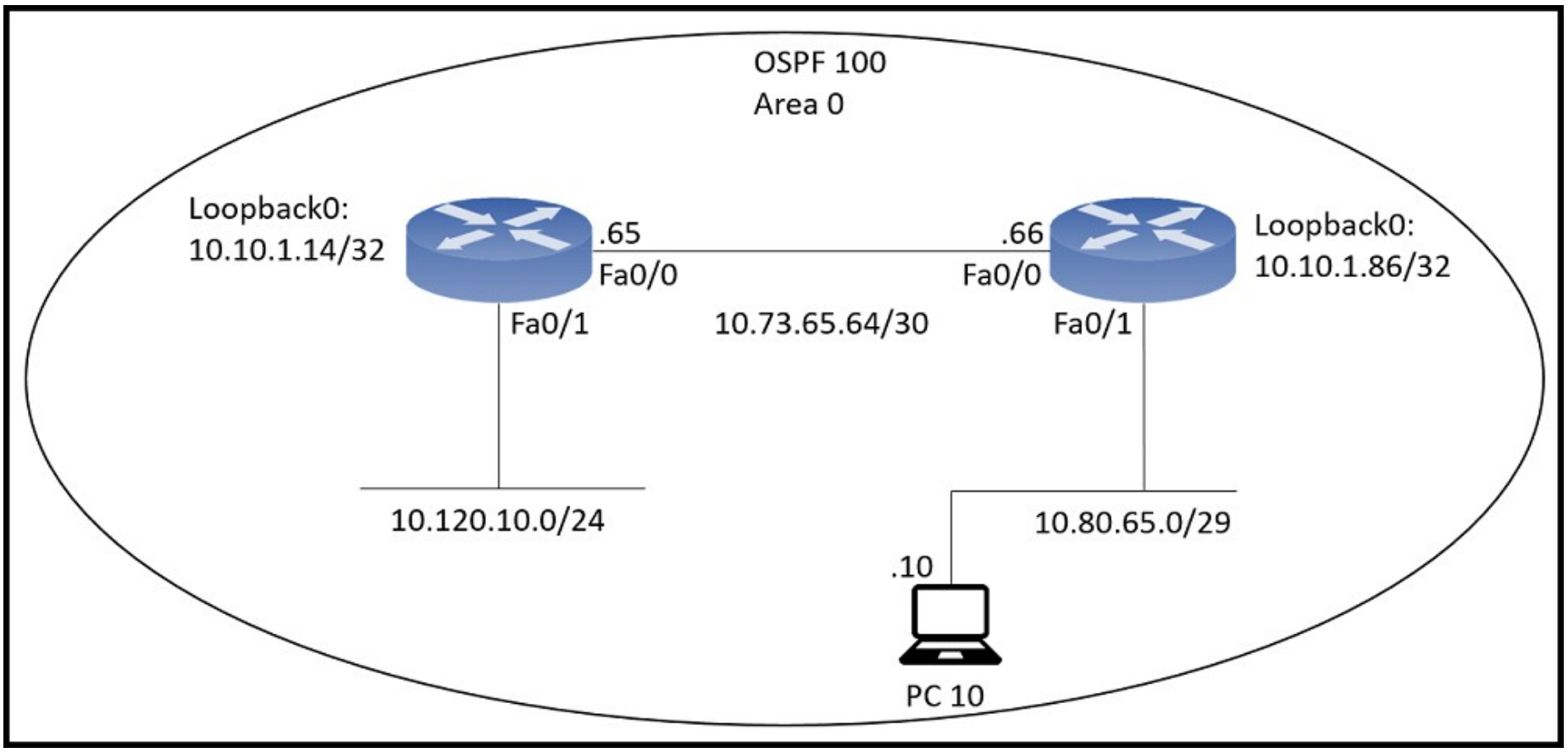
That's a lot of ospf

upvoted 1 times

Goh0503 11 months, 1 week ago

Answer D
https://study-ccna.com/ospf-network-types/#:~:text=A%20Point%2Dto%2DPoint%20network,always%20have%20precisely%20one%20recipient.

upvoted 2 times



An engineer just installed network 10.120.10.0/24. Which configuration must be applied to the R14 router to add the new network to its OSPF routing table?

A. Router ospf 100 Network 10.120.10.0 0.0.0.255 area 0

B. Router ospf 120 Network 10.120.10.0 255.255.255.0 area 0 Ip route 10.120.10.0 255.255.255.0 fa0/1

C. Router ospf 100 area 0 Network 10.120.10.0 0.0.0.255

D. Router ospf 100 Network 10.120.10.0 255.255.255.0 area 0

Correct Answer: *A*

shubhambala Highly Voted 1 year ago

Selected Answer: A

the answer is A and not D because OSPF configuration needs wildcard(inverted bits)

upvoted 15 times

melmiosis 10 months, 2 weeks ago

Quick and astute observation there Shubhambala

upvoted 4 times

blue91235 Most Recent 8 months, 1 week ago

Answer is A

upvoted 2 times

alejandro12 9 months, 4 weeks ago

Answer A

is tricky because the latest versions can use "normal mask"

upvoted 2 times

Question #500 *Topic 1*

What are two benefits of FHRPs? (Choose two.)

A. They allow encrypted traffic

B. They prevent loops in the Layer 2 network.

C. They are able to bundle multiple ports to increase bandwidth

D. They enable automatic failover of the default gateway

E. They allow multiple devices to serve as a single virtual gateway for clients in the network

Correct Answer: *DE*

papibarbu 8 months, 2 weeks ago

yes my man

upvoted 3 times