



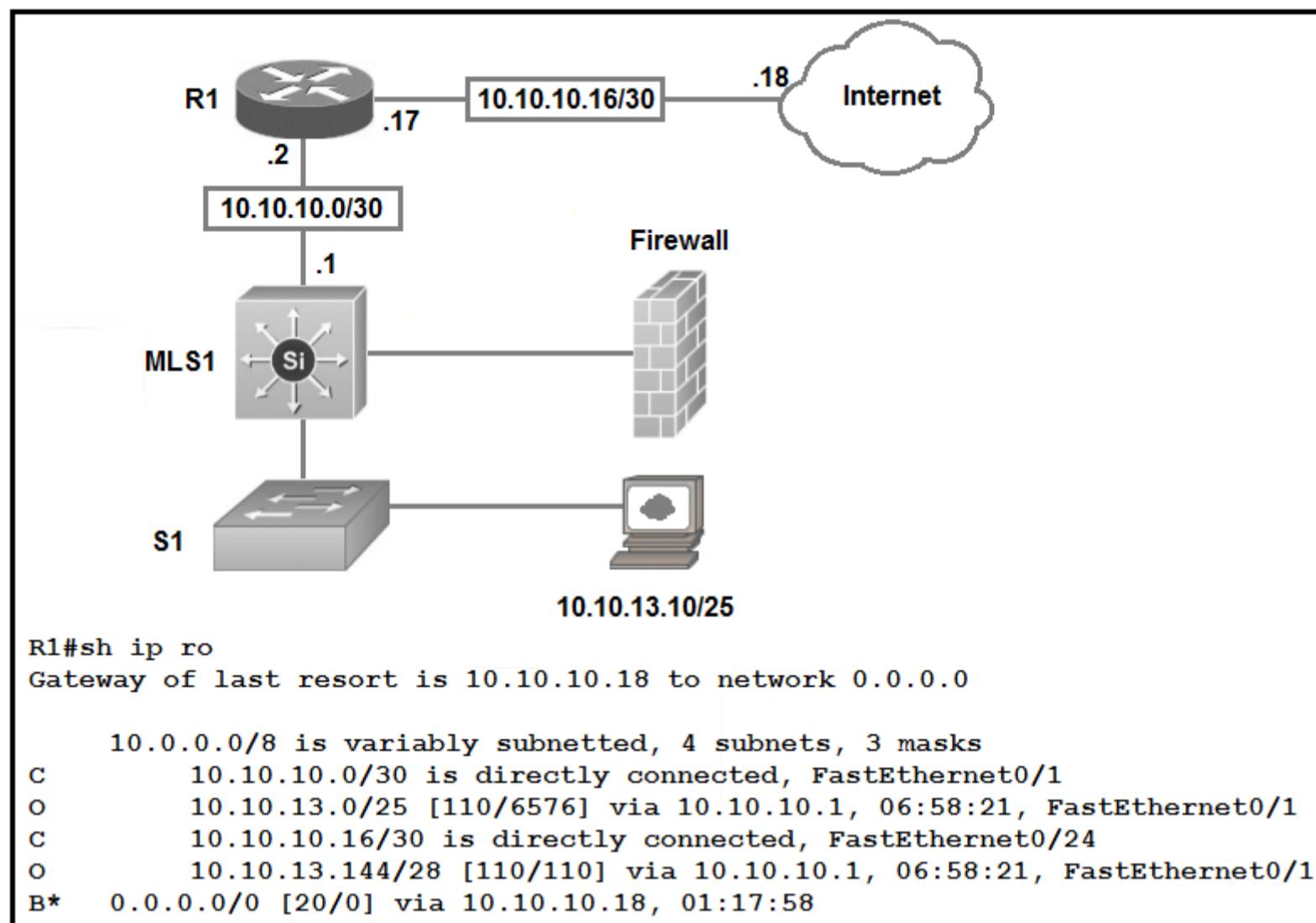
- Expert Verified, Online, **Free**.

Custom View Settings

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 (93%)

7%

LOST40 Highly Voted 1 year, 2 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 17 times

GreatDane Highly Voted 5 months, 1 week 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 12 times

 **Hope_12** Most Recent ⓘ 1 month, 1 week 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 1 times

 **Mgardini** 1 month, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

 **zeromoves** 3 months, 1 week ago

Great!

upvoted 1 times

 **[Removed]** 4 months, 2 weeks ago

Selected Answer: B

I think the answer is B

upvoted 1 times

 **rapide** 5 months, 3 weeks ago

How can i download in pdf ?

upvoted 1 times

 **rachidi07** 3 months, 3 weeks ago

by taking contributor access plan

upvoted 1 times

 **Request7108** 5 months, 3 weeks 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 1 times

 **javachip** 6 months, 1 week ago

Selected Answer: B

network is keyword

upvoted 1 times

 **cristip** 6 months, 3 weeks ago

Selected Answer: B

correct

upvoted 2 times

 **NetworkRookie** 7 months ago

Selected Answer: B

Connected Network, so route is network route

upvoted 1 times

 **Customexit** 7 months, 2 weeks ago

Selected Answer: B

like others said, if the routing table read "10.10.13.10/32" then yeah host route. But it reads "10.10.13.0/25", that's a network route.

upvoted 3 times

 **PEEPIE** 9 months, 1 week ago

A host route is /32. That is the best way to tell the difference and clears up any confusion. The answer is B.

upvoted 2 times

 **nyasalandi123** 9 months, 4 weeks ago

B is correct

upvoted 1 times

 **sasquatchshrimp** 10 months, 2 weeks ago

I would have to guess that B is correct, here is why. Remember, when you set up a route, if you can do a route summary. For example, if you have a router connected to a bunch of other routers with 10.1.1.0/24, 10.1.2.0/24, 10.1.3.0/24 and so on, you could just set one route to 10.1.0.0/16, and the router will forward all traffic that is 10.1.X.X to that location. Since the route table shows a /25 network that is 10.10.13.X/25 that is the route it goes to. That route is discovered by OSPF, a network protocol, aka, the answer is a network path. Hope this clears up some confusion. I did some serious study before looking at this, and CCNA is really just trying to screw with us.

upvoted 12 times

 **HansZ** 10 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

 **SamuelSami** 11 months ago

Selected Answer: C

What is Host Routing? The routing process that occurs when a host (computer) on a network forwards a packet to a destination host on the network. This is different from router routing, which is what happens when a router receives a packet that needs to be forwarded to a destination host.

A "host route" is route to a single host, a "network route" is route to a network of more than one host.

The local routes define a route for the one specific IP address configured on the router interface. Each local route has a /32 prefix length, defining a host route, which defines a route just for that one IP address. For example, the last local route, for 172.16.5.1/32, defines a route that matches only the IP

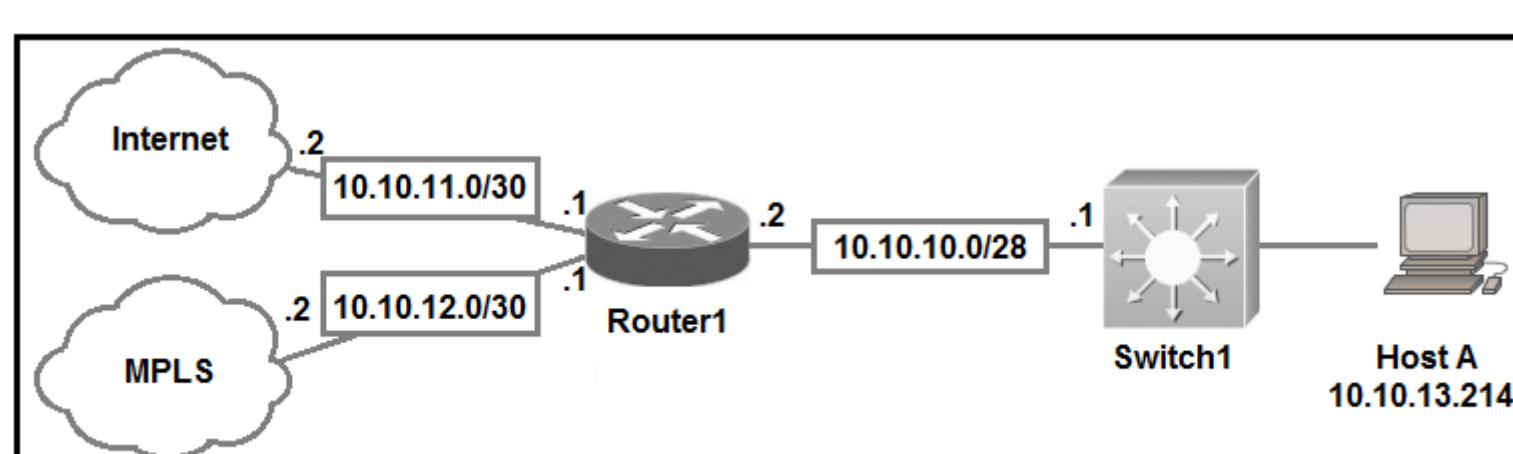
upvoted 2 times

 **RougePotatoe** 7 months, 2 weeks ago

From the question: "Which type of route does R1 use to reach host 10.10.13.10/32?"

That route is not in the routing table. Closest match is a network route 10.10.13.0/25 thus the router will use the closest matching route.

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. 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 the longest prefix will be matched first, in this case is 29/29.

Community vote distribution

D (100%)

mikachu85 Highly Voted 1 year, 5 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 11 times

ZUMY Highly Voted 2 years, 2 months ago

D is correct:
*Router selects longest Prefix path from routing table.
upvoted 8 times

ZUMY 6 months, 2 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

Hope_12 Most Recent 1 month, 1 week 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 1 times

Mgardini 1 month, 1 week ago

Selected Answer: D

Answer is D

Due to Longest Prefix path

upvoted 1 times

  **GreatDane** 5 months, 1 week 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 3 times

  **Request7108** 5 months, 2 weeks 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** 5 months, 4 weeks ago**Selected Answer: D**

D is correct

upvoted 1 times

  **javachip** 6 months, 1 week ago**Selected Answer: D**

router selects longest prefix path

upvoted 1 times

  **NetworkRookie** 7 months ago**Selected Answer: D**

Router selects longest Prefix path from routing table.

upvoted 1 times

  **keokkeo_123** 7 months, 3 weeks ago**Selected Answer: D**

is correct

upvoted 1 times

  **nyasalandi123** 9 months, 4 weeks ago

D is correct as it is in the same network range

upvoted 1 times

  **Chieftings** 12 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, 1 month ago**Selected Answer: D**

correct

upvoted 1 times

  **Samir_123** 1 year, 4 months ago

Selected Answer: D

correct

upvoted 2 times

  **vira5489** 1 year, 5 months ago**Selected Answer: D**

correct

upvoted 3 times

  **aman87** 1 year, 8 months ago

D is correct.

upvoted 1 times

  **Adam128** 1 year, 11 months ago

what is the signifcation of ".2" or ".1" ?

upvoted 2 times

  **dave1992** 1 year, 11 months ago

i believe it is a shortened way of saying 10.10.10.1 and 10.10.10.2

since you can see on the other side the subnet, i think you can assume the .1 or .2 goes at the end there.

upvoted 8 times

  **Adam128** 1 year, 11 months ago

Thnx dave1992

upvoted 2 times

  **netlol** 1 year, 5 months ago

this is true!

upvoted 1 times

Question #3

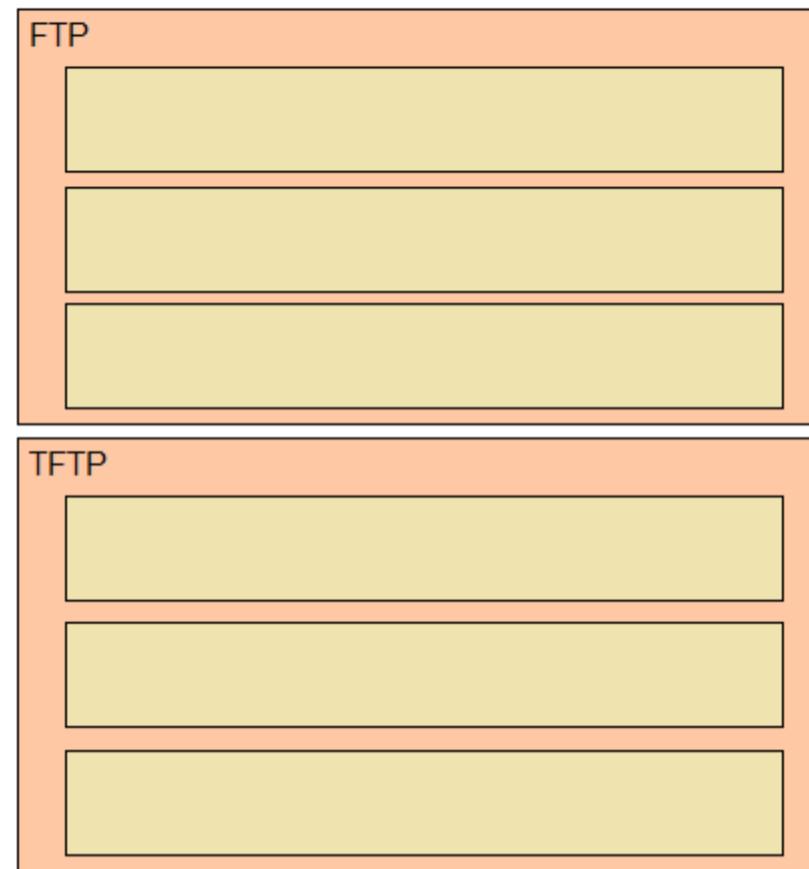
DRAG DROP -

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

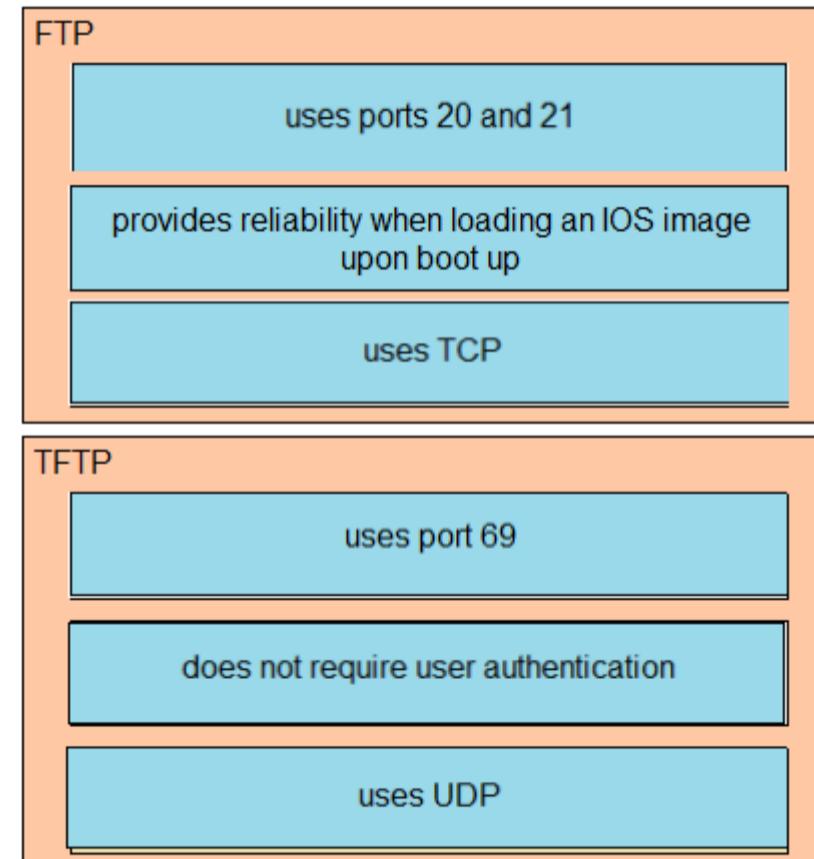
Select and Place:

Answer Area

- provides reliability when loading an IOS image upon boot up
- does not require user authentication
- uses port 69
- uses ports 20 and 21
- uses TCP
- uses UDP

**Correct Answer:****Answer Area**

- provides reliability when loading an IOS image upon boot up
- does not require user authentication
- uses port 69
- uses ports 20 and 21
- uses TCP
- uses UDP



Ali526 Highly Voted 2 years, 5 months ago

Correct.

upvoted 10 times

Request7108 Most Recent 5 months, 2 weeks 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 4 times

 **ac891** 3 weeks ago

Drink coffee my friend

upvoted 2 times

 **SamuelSami** 8 months, 1 week ago

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

upvoted 2 times

 **Rramos37** 1 year, 7 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** 1 year, 8 months 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** 1 year, 9 months ago

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

upvoted 1 times

 **ZUMY** 2 years, 2 months ago

Correct Answer

upvoted 4 times

Question #4

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 `input errors` includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.

The output below show the interface counters with the `show interface s0/0/0` 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%)

 **ZUMY** Highly Voted 2 years, 2 months ago

A,D is correct.

upvoted 11 times

 **DatBroNZ** Highly Voted 1 year, 2 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

runt: Frames that did not meet the minimum size (64 bytes). Can be caused by collisions

Therefore CRC and INPUT ERRORS will be increased.

upvoted 9 times

 **kilticespi** Most Recent 1 month, 1 week ago

It is correct

upvoted 1 times

 **kilticespi** 1 month, 1 week ago

It is correct

upvoted 1 times

 **jonathan126** 1 month, 2 weeks ago

A and D is correct

upvoted 1 times

 **diegoherreras** 3 months, 1 week ago

Selected Answer: AD

opciones a y d

upvoted 1 times

 **JORGED** 4 months ago

A,D options
upvoted 1 times

 **GreatDane** 5 months, 1 week 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** 5 months, 3 weeks ago

Selected Answer: AD

A,D is correct.
upvoted 1 times

 **NetworkRookie** 7 months ago

Selected Answer: AD

A,D is correct.
upvoted 2 times

 **aosroyal** 1 year, 1 month ago

Selected Answer: AD

correct
upvoted 2 times

 **Bigc0ck** 1 year, 3 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, 2 months ago

Switch port status
*Runts
*Gaint
*Input errors
*CRC
*Output errors
*Frame
upvoted 2 times

Question #5

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

172.28.228.144/21

172.28.228.144/23

172.28.228.144/25

172.28.228.144/29

172.28.228.1 - 172.28.229.254

172.28.224.1 - 172.28.231.254

172.28.228.129 - 172.28.228.254

172.28.228.145 - 172.28.228.150

172.28.192.1 - 172.28.255.254

Correct Answer:**Answer Area**

172.28.228.144/18

172.28.228.144/21

172.28.228.144/23

172.28.228.144/25

172.28.228.144/29

172.28.228.144/23

172.28.228.144/21

172.28.228.144/25

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**  5 months 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 17 times

 **paniguavo** Highly Voted 9 months 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 8 times

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

D R

1 = 5 2 = 2 3 = 1 4 = 3 5 = 4

upvoted 1 times

 **Garfieldcat** 7 months, 2 weeks ago

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

upvoted 2 times

 **Request7108** 5 months, 2 weeks 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, 2 months ago

A is correct

upvoted 9 times

 **Mgardini** Most Recent 1 month, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

 **Zafferano** 1 month, 3 weeks 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** 5 months ago

A is right

upvoted 1 times

 **diidiuQldama** 5 months, 3 weeks ago

Selected Answer: A

easy one

upvoted 1 times

 **Masquerade** 5 months, 3 weeks 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, 5 months ago

A is correct.

upvoted 3 times

 **SScott** 2 years, 4 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, 4 months ago

"A" is correct - great video on the 3 types of 802.11 frames
<https://www.youtube.com/watch?v=PCpnRqKCWCQ>

upvoted 28 times

 **Nae_Kun** 1 year, 5 months ago

wow this video is a must watch, if your coming from ccna v3
upvoted 4 times

 **SScott** 2 years, 2 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 2 years, 9 months ago

The answer is management if i'm not wrong
upvoted 6 times

 **nuridelon** Most Recent 3 months, 1 week ago

A is correct
upvoted 1 times

 **Alizadeh** 5 months, 3 weeks 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** 5 months, 3 weeks 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** 10 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **ScorpionNet** 1 year, 1 month ago

Management

upvoted 2 times

 **Ayie** 1 year, 10 months ago

management

upvoted 2 times

 **ZUMY** 2 years, 2 months ago

A is correct

upvoted 2 times

 **ZUMY** 2 years, 2 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

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 (82%)

A (18%)

 **ZUMY** Highly Voted  2 years, 2 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 12 times

 **Mgardini** Most Recent  1 month, 1 week ago

Selected Answer: C

answer is c

upvoted 2 times

 **GreatDane** 5 months, 1 week 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** 5 months, 3 weeks 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 3 times

 **Masquerade** 5 months, 3 weeks 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** 5 months, 2 weeks 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** 11 months, 2 weeks ago

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

upvoted 1 times

 **Jbcrggddfhh** 1 year, 1 month 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, 4 months ago

Selected Answer: C

Is correct

upvoted 1 times

 **chosonenone** 2 years, 7 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** 2 years, 9 months ago

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

upvoted 4 times

 **Enycon** 2 years, 8 months ago

I think you don't use lacp between spine and leaf but I'm a newbie myself

upvoted 2 times

 **pokemonmoon** 2 years, 8 months ago

OCG doesn't say anything about it

upvoted 2 times

 **Demi_UY_Scuti** 2 years, 7 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, 1 month ago

The answer is C because you can only connect leaf switches to more spine switches. Spine switches do 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, 4 months ago

just me or is the question supposed to be "check the most correct statement regarding hypervisors"?
upvoted 12 times

✉  **Yasin_Alsabah** 1 year, 4 months ago

I agree with you :)
upvoted 2 times

✉  **sasquatchshrimp** 10 months, 2 weeks 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

✉  **BigcOck** Highly Voted 1 year, 3 months ago

This seems more like a MCSA question than CCNA...
upvoted 6 times

✉  **Mgardini** Most Recent 1 month, 1 week ago

Selected Answer: C
Answer is C
upvoted 1 times

✉  **namyou** 2 months, 2 weeks ago

Selected Answer: C
I think it's c
upvoted 1 times

✉  **GreatDane** 5 months, 1 week 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** 5 months, 3 weeks 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** 6 months, 2 weeks ago

C is ok

upvoted 1 times

 **DARKEDGE** 1 year, 3 months ago

Selected Answer: C

C is the right answer

upvoted 2 times

 **Eric852** 1 year, 3 months ago

Selected Answer: C

It's C

upvoted 1 times

 **SollyMalwane** 1 year, 4 months ago

Selected Answer: C

I agree with you

upvoted 1 times

Question #10

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 `ipv6 address autoconfig` 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:

Its interface identifier (EUI-64 address)

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 3 years 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, 6 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 16 times

Thodoris85 2 years, 12 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 14 times

iRodimusPrime 2 years, 11 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, 5 months ago

I think its B because it says "specified IPv6 prefix"

upvoted 12 times

JWMcInSC 2 years, 11 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 2 years, 8 months ago

Answer is B

upvoted 10 times

Dunedrifter 2 weeks, 3 days 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 1 times

 **Ciscoparty** 3 weeks 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 1 times

 **cr0minus** 1 month, 2 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** 1 month, 3 weeks ago

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

upvoted 1 times

 **Ciscoman021** 2 months, 2 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** 2 months, 2 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** 3 months, 1 week ago

Selected Answer: B

The correct answer it's B

upvoted 1 times

 **oatmealturkey** 3 months, 2 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** 3 months, 2 weeks ago

Selected Answer: B

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

upvoted 2 times

 **AA3590** 3 months, 4 weeks ago

Selected Answer: D

its d because THATS HOW YOU GENERATE THE IPV6 ADDRESS

upvoted 1 times

 **sartaro** 4 months, 3 weeks ago

Answer is b, SLAAC is a method of autoconfiguring IPv6 addresses on an interface, and EUI-64 is a method of autoconfiguring IPv6 addresses using the interface's MAC address. Both are used to automatically generate an IPv6 address on an interface.

upvoted 1 times

 **Kosheema** 5 months, 2 weeks ago

Selected Answer: B

An EUI-64 IPv6 address is generated based on the specified prefix and the automatically generated interface identifier and is displayed by using the display ipv6 interface command.

upvoted 1 times

 **diidiuQldama** 5 months, 3 weeks ago

Selected Answer: C

the pc will ask the default gateway for the specific prefix then use eui to generate its own ipv6 address

upvoted 2 times

 **Masquerade** 5 months, 3 weeks ago

Selected Answer: B

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

This command automatically generates an IPv6 address from a specified prefix and MAC address of an interface. The prefix must be in the IPv6 format, followed by the keyword "eui-64". This command will create a 64-bit interface identifier based on the MAC address of the interface.

upvoted 1 times

 **ZUMY** 6 months, 2 weeks ago

Going for B

upvoted 1 times

Question #11

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 2 years, 11 months ago

All-nodes link-local multicast group FF02::1
All-routers link-local multicast group FF02::2
upvoted 21 times

✉  **Gelo29** Highly Voted 2 years, 8 months ago

Multicast - FF
Global Unicast - 2/3
Unique Local - FC/FD
Link Local - FE80
upvoted 21 times

✉  **Demi_UY_Scuti** 2 years, 7 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

✉  **ricky1802** Most Recent 4 months, 1 week 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** 5 months, 1 week 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** 5 months, 3 weeks 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** 7 months ago

FF02::1 - all nodes/hosts

FF02::2 - all routers

upvoted 2 times

 **Bram99** 7 months, 1 week ago

DE correct answer

upvoted 1 times

 **exilify** 8 months, 2 weeks ago

Selected Answer: DE

dededdedededede

upvoted 1 times

 **lock12333** 11 months, 3 weeks ago

Selected Answer: DE

dededdedededede

upvoted 1 times

 **ZUMY** 2 years, 1 month 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, 6 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

Question #12

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 `ip route` and `ip addr show eth1` are Linux commands.` `ip route`: display the routing table` `ip addr show eth1`: get depth information (only on eth1 interface) about your network interfaces like IP Address, MAC Address information✉ **Robertlars** Highly Voted 8 months 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 26 times

Question #13

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 2 years, 11 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, 1 month 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

 **BeautifulSmile** Most Recent 4 days, 19 hours 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 1 times

 **Taju711** 1 month, 2 weeks ago

did any have latest exam result for CCNA?

upvoted 1 times

 **GreatDane** 5 months, 1 week 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** 5 months, 3 weeks 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** 8 months, 1 week ago

I believe its C

But shouldnt it say flood 'frames' not packets

upvoted 1 times

 **msomali** 1 year, 1 month 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, 6 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, 7 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** 2 years, 9 months ago

Option C is the correct answer.

upvoted 3 times

 **Anton2020** 2 years, 10 months ago

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

upvoted 3 times

 **Enycon** 2 years, 8 months ago

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

upvoted 2 times

 **relliott** 2 years, 4 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** 2 years, 10 months 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-XXXX:XXXX ip address 10.2.1.3 255.255.255.252
- B. interface e0/0 description to XX-XXXX:XXXX ip address 192.168.1.1 255.255.255.248
- C. interface e0/0 description to XX-XXXX:XXXX ip address 172.16.1.4 255.255.255.248
- D. interface e0/0 description to XX-XXXX:XXXX ip address 209.165.201.2 225.255.255.252

Correct Answer: D

Community vote distribution

D (100%)

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

answer is D. The up in A is a broadcast
upvoted 37 times

 **dendio** 1 year, 4 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 ago

Wait? What? Did you look at the subnet mask? 225.255.255.252?
upvoted 18 times

 **Ali526** 2 years, 5 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, 2 months ago

To be honest, I didn't even notice the typo LOL
upvoted 3 times

 **Tengereni** 2 years ago

thats a typo
upvoted 3 times

 **Taku2023** Most Recent 1 month ago

225.255.255.252 Is an invalid subnet mask
upvoted 1 times

 **Rydaz** 4 weeks ago

its a typo
upvoted 1 times

 **Taju711** 1 month, 2 weeks ago

Did anyone have any latest exam re
upvoted 2 times

 **GreatDane** 5 months, 1 week ago

Selected Answer: D
A. interface e0/0 description to XX-XXXX:XXXX 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-XXXX:XXXX 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-XXXX:XXXX 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-XXXX:XXXX 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 4 times

 **michael1001** 5 months, 3 weeks ago

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

upvoted 1 times

 **Layfon** 8 months, 3 weeks ago

If these are updated questions how is this typo still here

upvoted 3 times

 **france60** 1 year, 1 month ago

la réponse D est correcte

upvoted 2 times

 **rictorres333** 1 year, 1 month ago

Selected Answer: D

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

upvoted 1 times

 **country_rooted** 1 year, 1 month 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, 2 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, 3 months ago

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

upvoted 1 times

 **Nagib** 1 year, 3 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, 3 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

 **Sauceboyzzjp** 1 year, 3 months ago

yeah i know it might be typo but cause of that i discard that first

upvoted 1 times

 **mr_reyes** 1 year, 6 months ago

You guys know that Cisco supports /31 CIDR for point-to-point links, right? Yes, in theory, the study guides tell us that /30 is the highest possible CIDR with only two usable addresses. But in reality, /31 can be used and there is no broadcast there. Look it up on the Cisco forums.

With that said, the answer would depend on whether there is a typo in the question or not! For this particular question is A (which is a broadcast indeed), simply because 225.255.255.252. is no a VALID subnet mask! But, if answer D has a typo and the subnet mask is actually 255.255.255.252, then the correct answer is definitely D! Be careful when you take the actual exam.

upvoted 3 times

 **Hope_12** 1 month, 1 week ago

I agree with this.

upvoted 1 times

 **dave1992** 1 year, 7 months ago

ill simplify the answer. its D because a /30 means 2 host bits left over = $2^2=4$. subtract 2 to give us 2 usable host ip addresses.
and based on the mask of a /30 = .252

the only thing that meets the fields is D
upvoted 5 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 2 years, 11 months ago

Private Address Ranges

Class A 10.0.0.0 to 10.255.255.255

Class B 172.16.0.0 to 172.31.255.255

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 21 times

 **Sr_Moe** 2 years, 7 months ago

Class B should be 172.16.0.0 to 172.31.255.255

upvoted 10 times

 **iRodimusPrime** Highly Voted 2 years, 11 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

 **GreatDane** Most Recent 5 months, 1 week ago

Selected Answer: B

An IP network, which is not connected to the public Internet, uses private IP addresses.

There is a private IP address 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, 3 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** 3 months ago

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

upvoted 1 times

 **ZUMY** 2 years, 1 month 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, 4 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, 4 months ago

Definitely B

upvoted 3 times

 **dcouch** 2 years, 8 months ago

why wouldn't C work?

upvoted 1 times

 **Benonie** 2 years, 8 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** 2 years, 11 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 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 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, 6 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, 1 month ago

For /28 network, There (2^4)=16 Subnets with each having (2^4-2)=14 host (14 + 1 Network ID + 1 Broadcast 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 21 times

 **ZUMY** 2 years, 1 month ago

Shortcut to find
 1. First calculate subnets (borrowed 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 15 times

 **Micah_TENGWA** Highly Voted 2 years ago

D is correct because the next subnet address is 192.168.16.144
 upvoted 7 times

 **Customexit** Most Recent 7 months, 2 weeks 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 6 times

 **tonyisabel** 1 year, 2 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 5 times

 **DatBroNZ** 1 year, 2 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, 3 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 6 times

 **kalistro** 1 year, 4 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, 8 months ago

D is correct

upvoted 2 times

 **Shaz313** 1 year, 10 months ago

D is definitely correct.

upvoted 4 times

 **Giuseppe_001** 2 years ago

zumy insegnami la via

upvoted 3 times

 **Alsaher** 2 years, 1 month ago

D is correct

upvoted 4 times

 **ZUMY** 2 years, 1 month 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, 1 month ago

Dear moderator

Please remove this comment.Thx

upvoted 2 times

 **marcojmnez** 2 years, 3 months ago

255.255.255.240 -->/28

Block size=256-240=16 Usable IPs.

last 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, 5 months ago

D is definitely correct.

upvoted 4 times

Question #17

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, 1 month ago

B is correct

upvoted 7 times

 **Alizadeh** Most Recent  5 months, 3 weeks 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 2 times

 **Vlad_Is_Love_ua** 9 months 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, 2 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

 **DUMPlidore** 5 months, 3 weeks ago

Found this on Jeremy's IT Lan YT

- Uses the address block FC00: : / 7 (FC00: : 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, 4 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 2 times

 **shakyak** 1 year, 6 months ago

Keyword

Global-Public IP

Local-Private IP

upvoted 2 times

 **dave1992** 1 year, 9 months ago

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

upvoted 1 times

 **ProgSnob** 1 year, 6 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, 8 months ago

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

upvoted 1 times

 **Jonasye** 2 years, 4 months ago

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

upvoted 3 times

 **Bubu3k** 2 years, 3 months ago

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

upvoted 4 times

 **Jonfernz** 2 years, 1 month ago

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

upvoted 4 times

 **hippyjm** 2 years, 4 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 2 years, 11 months ago

IPv6

- 1.Uncast
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 23 times

 **Delajan** 2 years, 1 month ago

Actually Unique Local: Assigned from the FC00::/7 range

upvoted 1 times

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

Somehow the FF seemed to be a hint.

upvoted 11 times

 **cormorant** Most Recent 7 months, 1 week ago

FC00::/7 - private networks (intranet)

FE80::/10 - private networks (intranets)

FF00::/8 - multicast

upvoted 1 times

 **Vlad_Is_Love_usa** 9 months 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, 6 months ago

FF AS MULTICAST

upvoted 3 times

 **Shamwedge** 1 year, 11 months ago

I read the question as in block i.e. prevent

Do do that

upvoted 2 times

Question #19

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 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** 1 month, 3 weeks ago

half-duplex as it is, can't be a cause of collision.

upvoted 1 times

✉  **John248** Highly Voted 2 years, 11 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, 5 months ago

This is correct, but the answers have been moved around

upvoted 5 times

✉  **vuhidus** Most Recent 10 months, 1 week ago

Selected Answer: BE

The answer is BE

upvoted 1 times

✉  **wojabagooya** 11 months, 2 weeks 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** 12 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 ago

B and E are correct options.
upvoted 1 times

lock12333 1 year ago

Selected Answer: AE

a and e
upvoted 1 times

Hodicek 1 year, 6 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 1 year, 10 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, 1 month 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, 4 months ago

Definitely B and E
upvoted 3 times

Lakshmi_200_301 2 years, 5 months ago

I think questions B and E are correct answers
upvoted 3 times

jowill 2 years, 5 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, 5 months ago

B and E
upvoted 2 times

daslux4 2 years, 6 months ago

B and E certainly
upvoted 2 times

boghota 2 years, 6 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 mismatch or am I wrong here?
upvoted 2 times

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, 7 months ago

B and E
upvoted 1 times

Question #20

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 2 years, 11 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, 1 month 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

 **cormorant** Most Recent 7 months ago

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

can someone well versed in this area chime in?

upvoted 1 times

 **Request7108** 5 months, 2 weeks 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, 4 months ago

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

upvoted 1 times

 **ragekod** 1 year, 8 months ago

A incorrect

upvoted 1 times

 **nav2802** 2 years, 3 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, 4 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, 4 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** 5 months, 2 weeks ago

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

upvoted 1 times

 **DatBroNZ** 2 years, 7 months ago

Easy one, option A

upvoted 3 times

 **AgustD** 2 years, 7 months ago

Option D is the answer

upvoted 1 times

 **sarsat** 2 years, 10 months ago

answer is correct

upvoted 4 times

Question #21

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_ether.pdf

✉  **John248**  2 years, 11 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, 2 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_ether.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_ether.html#:~:text=the%20syslog%20message%20was%20an

upvoted 2 times

✉  **GreatDane**  1 year 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

✉  **Alsafer** 2 years, 1 month ago

A is correct

upvoted 2 times

Question #22

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**  2 years, 1 month ago

Given answer C is correct
upvoted 10 times

✉  **SScott**  2 years, 2 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 7 times

✉  **GreatDane**  5 months, 1 week 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 1 times

✉  **Shamwedge** 1 year, 5 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, 4 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** 1 year, 9 months ago

C is correct

upvoted 3 times

✉  **nav2802** 2 years, 3 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, 1 month ago

A is correct!

upvoted 9 times

 **Bhrino** Most Recent 4 weeks ago

Since the traffic doesn't traverse the internet there shouldn't be any conflict with multiple companies have the same private ips in different networks

upvoted 1 times

 **Alokhai580** 1 month, 3 weeks 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** 2 months ago

A is Correct.This is where NAT is used also.

upvoted 1 times

 **Bilal1992** 5 months ago

A is correct.

upvoted 1 times

 **CrazeY** 2 years, 8 months ago

Repeating question

upvoted 1 times

Question #24

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 1 year, 9 months 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, 2 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 11 times

 **GangsterDady** 1 year, 7 months ago

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

upvoted 21 times

 **maw619** 1 year, 9 months ago

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

upvoted 72 times

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

C is the answer

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

upvoted 10 times

 **Da_Costa** Most Recent 5 days, 23 hours ago

Enable Stateless Address Auto-Configuration (SLAAC)

upvoted 1 times

 **dsolaide** 1 week, 4 days 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** 2 weeks, 5 days ago

Has anyone done the exam recently?

upvoted 2 times

 **GreatDane** 5 months, 1 week 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]** 11 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, 4 months ago

Selected Answer: C

C is right

upvoted 1 times

 **SScott** 2 years, 1 month ago

C is right.

<https://www.amarchaudhari.me/enable-ipv6-slaac-on-cisco-routers/>

upvoted 2 times

 **MD100MD101FUCKER** 2 years, 7 months ago

Correct Answer: C

upvoted 2 times

 **CrazeY** 2 years, 8 months ago

Repeating question

upvoted 1 times

 **emmet0713** 2 years, 8 months ago

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

upvoted 3 times

Question #25

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 (71%)

CE (26%)

 **Raymond9** Highly Voted 2 years, 6 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 5GHz (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 19 times

 **chr** Highly Voted 2 years, 1 month 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 11 times

 **naise** 1 year, 10 months ago

is it sure the AC are the correct ones?

upvoted 1 times

 **Nicocisco** 1 year, 3 months ago

No because 5GHz has 24 non-overlapping channels

upvoted 11 times

 **SScott** 1 year, 10 months ago

Yes an informative article and supporting A

upvoted 1 times

 **dsolaide** Most Recent 1 week, 4 days 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 1 times

 **lolungos** 2 weeks, 6 days ago

A and C are correct

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

Source: CWNP curriculum

upvoted 1 times

 **dropsable** 1 month, 1 week 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 1 times

 **jonathan126** 1 month, 2 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** 1 month, 3 weeks ago

5g ghz have 24 non-overlaping channels

upvoted 1 times

 **Alokhai580** 1 month, 3 weeks 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** 1 month, 3 weeks ago

Selected Answer: CE

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

upvoted 1 times

 **Rether16** 2 months 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** 2 months, 2 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** 2 months, 2 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** 3 months, 2 weeks ago

chatgpt chose A and C

upvoted 1 times

 **keokkeo_123** 3 months, 3 weeks ago

Selected Answer: AC

correcto

upvoted 1 times

  **Yannik123** 4 months ago**Selected Answer: CE**

A cant be right. There are 24 non-overlapping channels.

upvoted 2 times

  **ricky1802** 4 months, 1 week ago**Selected Answer: AC**

A. The 5GHz frequency band provides increased network capacity because it has more nonoverlapping channels available than the 2.4GHz frequency band. This allows for more devices to connect to the network and increases the overall capacity of the network.

C. When designing a wireless network, it is important to ensure that cells (coverage areas) do not overlap one another. If cells overlap, it can cause interference and negatively impact the performance of the network. To prevent this, cells that overlap should be configured to use nonoverlapping channels. This allows the devices in those cells to communicate without interfering with each other.

B, D, E options are not the standard design for coverage cells, the selection of channel depends on the environment, and it's not a requirement to have autonomous access point, repeater access point or dynamic channel selection.

upvoted 2 times

  **GreatDane** 5 months, 1 week ago**Selected Answer: AC**

A. 5GHz provides increased network capacity with up to 23 non-overlapping channels.

This is a 5GHz very useful feature.

Correct answer.

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

Dynamic Frequency Selection (DFS) is a 5GHz feature, but it's not a design best practice.

Wrong answer.

C. Cells that overlap one another are configured to use non-overlapping channels.

Correct answer.

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

Adjacent cells SHOULD NOT USE overlapping channels.

Wrong answer.

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

Ref: Cisco Wireless Controller Configuration Guide, Release 7.5

"...

C H A P T E R 125
Configuring RRM

..."

Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision.

"..."

Wrong answer.

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, 1 month ago

B is correct

upvoted 7 times

 **GreatDane** Most Recent 5 months, 1 week 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** 7 months, 4 weeks ago

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

upvoted 3 times

 **rarehunter5** 11 months ago

why not c?

upvoted 1 times

 **Knobbler** 1 year, 3 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** 1 year, 9 months 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, 8 months ago

Repeating question

upvoted 1 times

 **Shamwedge** 1 year, 11 months ago

different answers

upvoted 3 times

 **jerry19** 2 years ago

Repeating response.

upvoted 6 times

Question #27

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, 6 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 46 times

 **NICE_ANSWERS** 1 week, 5 days ago

Thank you very much Raymond.. Very helpful 

upvoted 1 times

 **XBfoundX** 2 years, 5 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, 5 months ago

You are right; good research.

upvoted 4 times

 **SScott** 2 years, 1 month ago

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

upvoted 5 times

 **tigertoo** Most Recent 2 weeks ago

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

upvoted 2 times

 **Smaritz** 3 months, 3 weeks ago

B and D.

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

upvoted 1 times

 **BakedPotato** 3 months, 3 weeks 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** 5 months, 1 week 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** 1 year, 9 months 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, 1 month ago

B & D are correct

upvoted 3 times

 **SUKABLED** 2 years, 4 months ago

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

upvoted 2 times

 **Futchihore** 2 years, 6 months ago

Yes it is, I had this question last time

upvoted 2 times

 **Bach999** 2 years, 6 months ago

Is this a real CCNA exam question?

upvoted 3 times

Question #28

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 1 year, 11 months ago

A, B, and C all are connection related. D is the only answer that relates to "communication"
upvoted 12 times

 **Alokhai580** Most Recent 1 month, 3 weeks 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 3 times

 **Ciscoman021** 2 months, 2 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 2 times

 **GreatDane** 1 year 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 1 times

 **ismatdmour** 1 year, 3 months ago

Selected Answer: D

D is most correct and is the general case.

upvoted 2 times

 **ostralo** 1 year, 8 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 3 times

✉ **dave1992** 1 year, 9 months ago

CAPWAP doesn't communicate, the communication is called CAPWAP. It's a tunnel from the core layer that terminates on the access layer.
upvoted 4 times

✉ **Nhan** 2 years, 3 months ago

This is split-Mac address topic
upvoted 3 times

✉ **martco** 2 years, 3 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, 4 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, 5 months ago

Is this topic relevant in the CCNA? Nowhere 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** 1 year, 9 months 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. There's no way you can read the material without seeing this.
upvoted 3 times

✉ **Raymond9** 2 years, 6 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, 1 month 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, 8 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, 3 months ago
FF <- easiest way to remember multicast.
upvoted 34 times
- ✉  **cormorant** 7 months ago
'FF <- easiest way to remember multicast.'

i'm putting this on a shirt
upvoted 7 times
- ✉  **boghota** Highly Voted 2 years, 6 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 15 times

- ✉  **boghota** 2 years, 6 months ago
A) Global Unicast
B) Unique Local Unicast
C) Link Local Unicast
D) Multicast
upvoted 5 times
- ✉  **boghota** 2 years, 6 months ago
Sorry I mean Correct Answer: D
upvoted 8 times
- ✉  **Ciscoman021** Most Recent 2 months, 2 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, 4 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, 1 month ago
All nice, but we want visual feedback
upvoted 2 times

✉  **Bibi20** 8 months, 3 weeks ago
Bel nome 😊😊
upvoted 1 times

- ✉  **ZUMY** 2 years, 1 month ago
D is correct
upvoted 3 times

✉  **nenotronix** 2 years, 2 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, 6 months ago

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

upvoted 2 times

✉  **dave369** 2 years, 11 months ago

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

upvoted 4 times

✉  **Pras86** 2 years, 9 months ago

so which is the correct ans?

upvoted 2 times

✉  **Timohyng** 2 years, 12 months ago

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

upvoted 9 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%)

 **GreatDane** 5 months, 1 week 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 2 times

 **braeiv123** 8 months, 1 week ago

D is correct

upvoted 2 times

 **Hansain** 8 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 3 times

 **Kaizer5** 11 months, 4 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

 **kentsing** 1 year ago

D is correct

upvoted 2 times

 **DARKK** 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

 **Nebulise** 1 year, 4 months ago

D is correct

upvoted 1 times

 **mrb23** 1 year, 5 months ago

D is correct

upvoted 1 times

 **ragekod** 1 year, 8 months ago

D is correct

upvoted 1 times

 **Giuseppe_001** 2 years ago

D is correct

upvoted 1 times

 **ZUMY** 2 years, 1 month ago

D is correct

upvoted 1 times

 **SScott** 2 years, 1 month 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 2 years, 9 months 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, 5 months ago

You have written a long story, but no answer.

AB is correct.

upvoted 42 times

 **Jazzy_147369** 2 years, 4 months ago

I think copy and paste is more like it

upvoted 11 times

 **netlol** Highly Voted 1 year, 4 months ago

A correct because distribution layer has multilayer switches (L2 and L3 technologies)

B correct core 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 10 times

 **Ciscoman021** Most Recent 2 months, 2 weeks ago

Selected Answer: AB

The correct answers are A and B.

upvoted 1 times

 **MSTAHIR** 4 months, 2 weeks ago

AB correct.

upvoted 1 times

 **jnanofrancisco** 4 months, 3 weeks ago

AB is the correct here

upvoted 1 times

 **Vile_Yogabear** 6 months, 3 weeks 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** 1 month, 2 weeks ago

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

upvoted 1 times

 **keokkeo_123** 7 months, 1 week ago

Selected Answer: AB

AB is the answer

upvoted 1 times

 **Bram99** 7 months, 1 week ago

A,B Is correct

upvoted 1 times

 **Xcape** 12 months ago

AB IS THE BEST CHOICE

upvoted 1 times

 **LingLingW** 1 year, 5 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, 1 month 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, 3 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 1 year, 10 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

 **Lego_Las** Most Recent 1 month ago

Selected Answer: D

what?! yessirr

upvoted 1 times

 **gugugulo** 3 months, 2 weeks 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** 4 months, 2 weeks ago

D is correct

upvoted 1 times

 **GreatDane** 5 months, 1 week 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 111111010. 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 1 times

 **Alizadeh** 5 months, 3 weeks 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, 1 month 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, 8 months ago

D is correct

upvoted 1 times

 **kadamske** 1 year, 8 months ago

Correct answer "D"

upvoted 1 times

 **Harry0210** 1 year, 10 months ago

D is correct

upvoted 1 times

 **ZUMY** 2 years, 1 month ago

D is correct

upvoted 1 times

 **marcojmnez** 2 years, 3 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, 5 months ago

D is correct.

upvoted 4 times

Question #33

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, 1 month 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 21 times

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

C is correct. <https://geek-university.com/ccna/ipv6-eui-64-calculation/>
upvoted 11 times

 **GreatDane** Most Recent 5 months, 1 week 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 0xFFFF 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 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** 8 months 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** 8 months, 3 weeks ago

Selected Answer: C
C is correct
upvoted 2 times

 **Vlad_Is_Love_ue** 9 months, 1 week 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** 10 months, 1 week ago

Selected Answer: C

C is the answer
upvoted 2 times

 **GohanF2** 10 months, 2 weeks 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** 10 months, 2 weeks ago

Selected Answer: C
FFFE goes in the middle, then the 7th bit is inverted
upvoted 1 times

 **saeed_huhu** 10 months, 3 weeks ago

Selected Answer: B
EUI-64
upvoted 1 times

 **onikafei** 1 year, 4 months ago

Selected Answer: C
C is correct
upvoted 1 times

 **Shaz313** 1 year, 10 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, 2 months ago

Thanks for the expanciation.
upvoted 1 times

 **nенотронix** 2 years, 2 months ago

Thanks "examcol"
upvoted 2 times

 **ZayaB** 2 years, 4 months ago

Thanks
upvoted 2 times

Question #34

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 1 year, 12 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
 $103 \leq 2^{H-2}$
 $H=7$
will give N=1
Therefore/25,,, i hope u got ans in short, tht is C
upvoted 22 times

 **Danielki** 1 year, 1 month ago

Where did N came from? I'm lost....
upvoted 1 times

 **ScorpionNet** 1 year, 1 month ago

N is the Network, U is the usable host, H is the host
upvoted 2 times

 **Customexit** Highly Voted 7 months, 2 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 16 times

 **NICE_ANSWERS** 1 week, 5 days ago

please, what's it's significance?
upvoted 1 times

 **hayo** 6 days, 9 hours ago

Number of addresses per subnet
upvoted 1 times

 **flash93933** 5 months ago

love you

upvoted 1 times

 **MSTAHIR** Most Recent ⓘ 4 months, 2 weeks 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** 7 months, 1 week ago

Selected Answer: C

cccccccccccccccc

upvoted 2 times

 **lock12333** 11 months, 3 weeks ago

Selected Answer: C

cccccccccccccc

upvoted 1 times

 **GreatDane** 1 year 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:

255.255.255.1xxxxxx = 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 ago

16 addresses per floor is not enough so 32 per floor is needed

simply count from $/32=1$ $/31=2$ $/30=4\dots\dots$ $/27=32$

/27 per floor is the answer

upvoted 4 times

 **DaveDaSpade** 1 year ago

That's how I got the answer quickly :)

upvoted 1 times

 **Shamwedge** 1 year, 7 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, 1 month 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, 1 month ago

C is correct

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

upvoted 3 times

 **ZUMY** 2 years, 1 month 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, 1 month 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, 4 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, 4 months ago

C is correct. given a /27 mask
upvoted 2 times

jasten 2 years, 5 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, 5 months ago

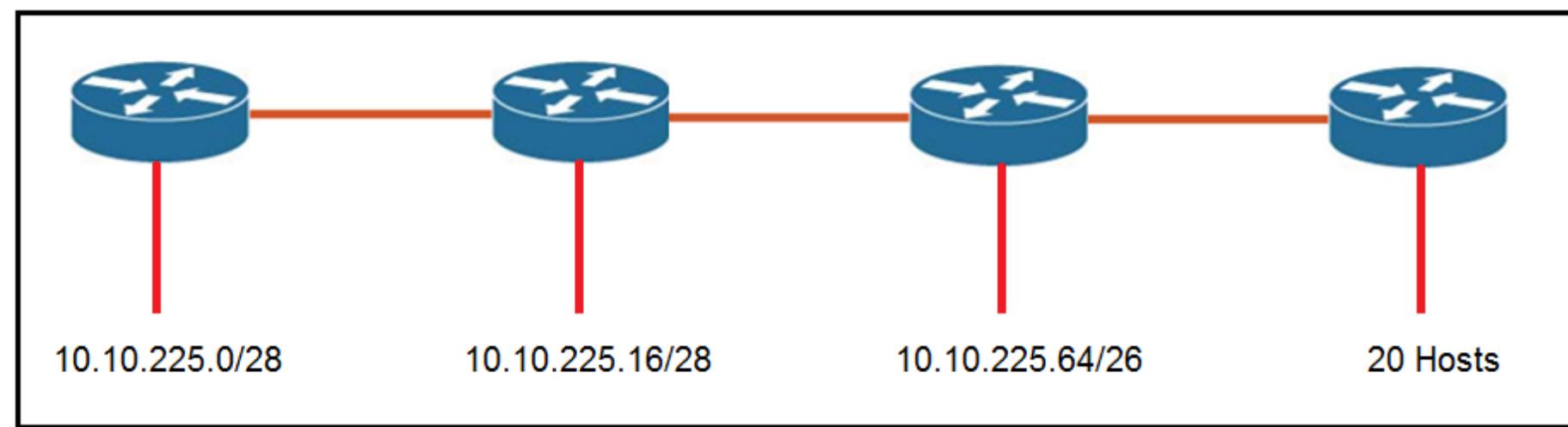
This question does not have sufficient information to reach at a unique conclusion.
upvoted 3 times

Ali526 2 years, 4 months ago

Sorry. It does. C is correct.
upvoted 3 times

Siegfried 1 year, 6 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



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, 1 month 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 38 times

diidiuQldama 5 months, 3 weeks 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

diidiuQldama 5 months, 3 weeks ago

Sorry .128

upvoted 1 times

suriyaprakash 1 year, 3 months ago

Thank you

upvoted 1 times

GreatDane Highly Voted 1 year 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 8 times

 **hoisin** Most Recent 4 months, 1 week ago

That is a good explanation for this question.

upvoted 1 times

 **HeinyHo** 8 months, 2 weeks ago

Selected Answer: D

Definitely D

upvoted 2 times

 **bhurishravas** 1 year, 5 months ago

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

upvoted 1 times

 **bhurishravas** 1 year, 5 months ago

I apologize)). Confuse myself!

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

upvoted 1 times

 **taku03** 1 year, 6 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, 7 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, 4 months ago

Simple maths - D!

upvoted 1 times

 **BurekMaster1** 2 years, 4 months ago

Why not C?

upvoted 3 times

 **Roberts132** 1 year, 10 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, 4 months ago

got it!

upvoted 2 times

 **rlelliott** 2 years, 4 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, 5 months ago

D is correct.

upvoted 4 times

Question #36

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 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 6 times

 **jonathan126** Most Recent 1 month, 2 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 1 times

 **ManKilla** 1 year, 9 months ago

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

upvoted 2 times

 **Shaz313** 1 year, 10 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, 1 month 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, 1 month ago

Moderator Please delete this comment.
upvoted 11 times

✉  **IxlJustinIxl** 2 years ago

^^ for Q35
upvoted 2 times

✉  **admin1982** 2 years, 4 months ago

D is correct.
upvoted 3 times

✉  **jasten** 2 years, 5 months ago

There are no direct links between leaf nor between spine
upvoted 3 times

✉  **Miskoolak** 2 years, 9 months ago

Correct answer is "A"
bc. of absence of stp all links are active and pass the traffic .
upvoted 1 times

✉  **smote** 2 years, 8 months ago

But there are no direct links between leaf switches, so D is correct.
upvoted 8 times

✉  **Chenet** 1 year, 8 months ago

no, you are wrong mate
upvoted 1 times

Question #37

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 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 33 times

 **Hmaw** 8 months ago

Reading your explain make me hearing Jeremy voice saying "Save the hosts". Nicely done.
upvoted 4 times

 **re_roy** 8 months, 3 weeks ago

Well explained brother
upvoted 1 times

 **AKA1987** Highly Voted  1 year, 9 months 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 ago

how you give $H=9$?
upvoted 2 times

 **Naetan0809** Most Recent  1 month, 1 week 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** 3 months, 3 weeks 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** 3 months, 2 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** 4 months, 3 weeks ago

Correct

upvoted 1 times

 **Vile_Yogabear** 6 months, 3 weeks ago

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

$8 \times 40 = 320$ 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** 7 months, 1 week ago

Selected Answer: B

BBBBBBB

upvoted 1 times

 **Vishalb86** 1 year, 4 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, 6 months ago

Sorry B is the correct answer as $8 \times 40 = 320$ so it should be B not C

upvoted 2 times

 **Hodicek** 1 year, 6 months ago

Answer is C

upvoted 1 times

 **SScott** 1 year, 9 months 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** 1 year, 12 months ago

$40 \times 8 <= 2^H - 2$, 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** 1 year, 12 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** 1 year, 11 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** 1 year, 11 months ago

Thanks for your explanation

upvoted 2 times

 **Doad** 1 year, 12 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** 1 year, 9 months 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** 3 months, 3 weeks 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.

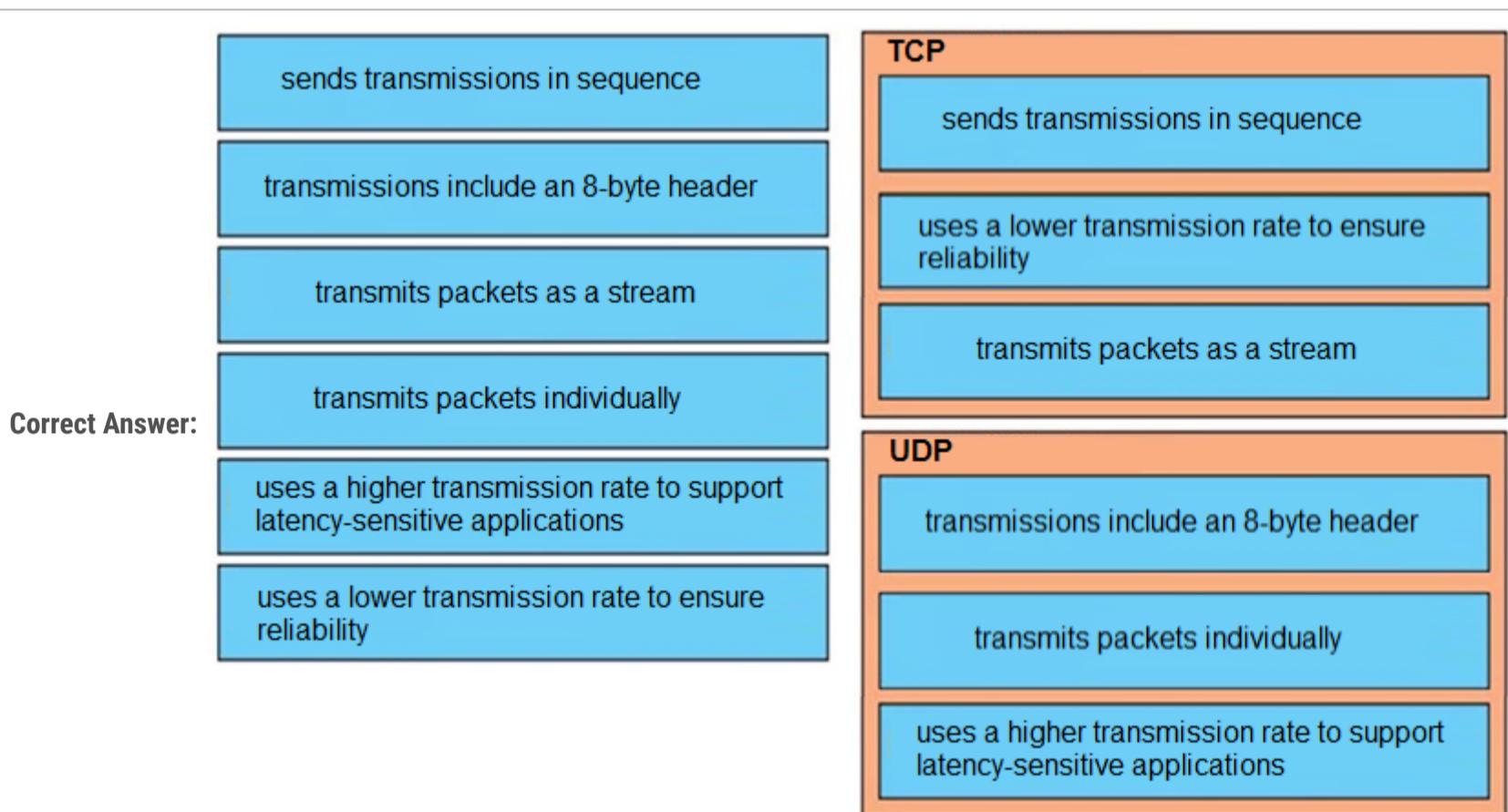
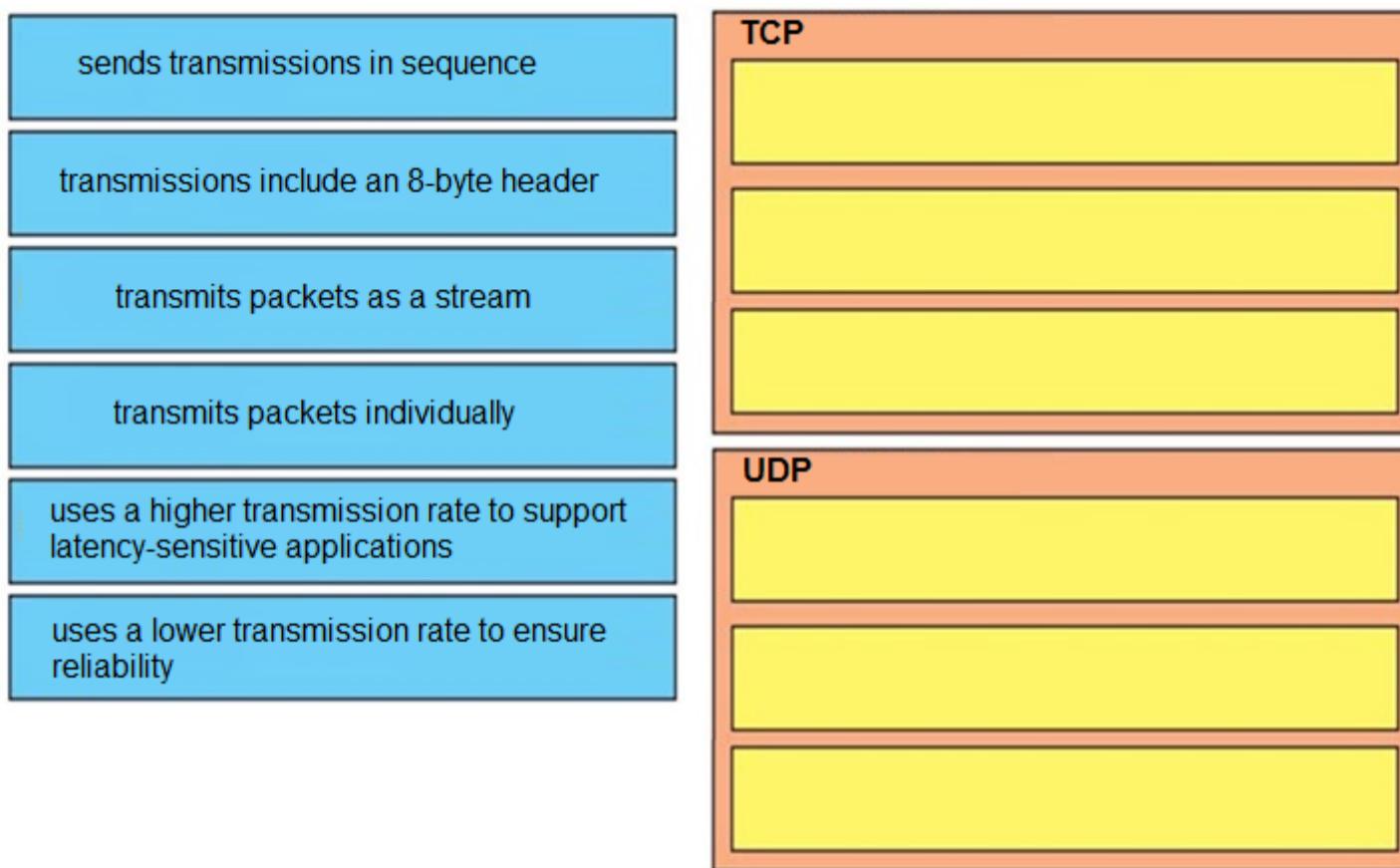
upvoted 1 times

Question #38

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, 5 months ago

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

upvoted 28 times

rlelliott 2 years, 4 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%20E2%80%94%20TCP%2FIP,flowing%20in%20the%20opposite%20direction.>

upvoted 18 times

amrith501 2 years, 5 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 8 times

SScott 2 years, 1 month 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, 6 months ago

If you've ever used Wireshark you would know that viewing a TCP stream is an important part of troubleshooting.
upvoted 4 times

 **ProgSnob** Most Recent 5 months 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, 4 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, 5 months ago

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

upvoted 1 times

 **dabears** 1 year, 6 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, 7 months ago

answers are up to scratch

upvoted 1 times

 **Duketernity** 1 year, 10 months 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, 1 month ago

Given answers are correct

upvoted 2 times

 **Robin999** 2 years, 3 months ago

Answers are correct

upvoted 2 times

Question #39

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*

C (67%)	B (33%)
---------	---------

 **Raooff** Highly Voted 2 years, 5 months ago

C is right
Collision happens after 512 bits =64 byte =late collision
upvoted 13 times

 **oooMooo** Highly Voted 2 years, 1 month 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 11 times

 **dsolaide** Most Recent 1 week, 4 days 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** 5 months, 1 week 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** 5 months, 3 weeks 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, 8 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 6 times

 **mariodesa** 1 year, 4 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, 1 month ago

C is correct

upvoted 3 times

 **Aval0n1** 2 years, 3 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, 6 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

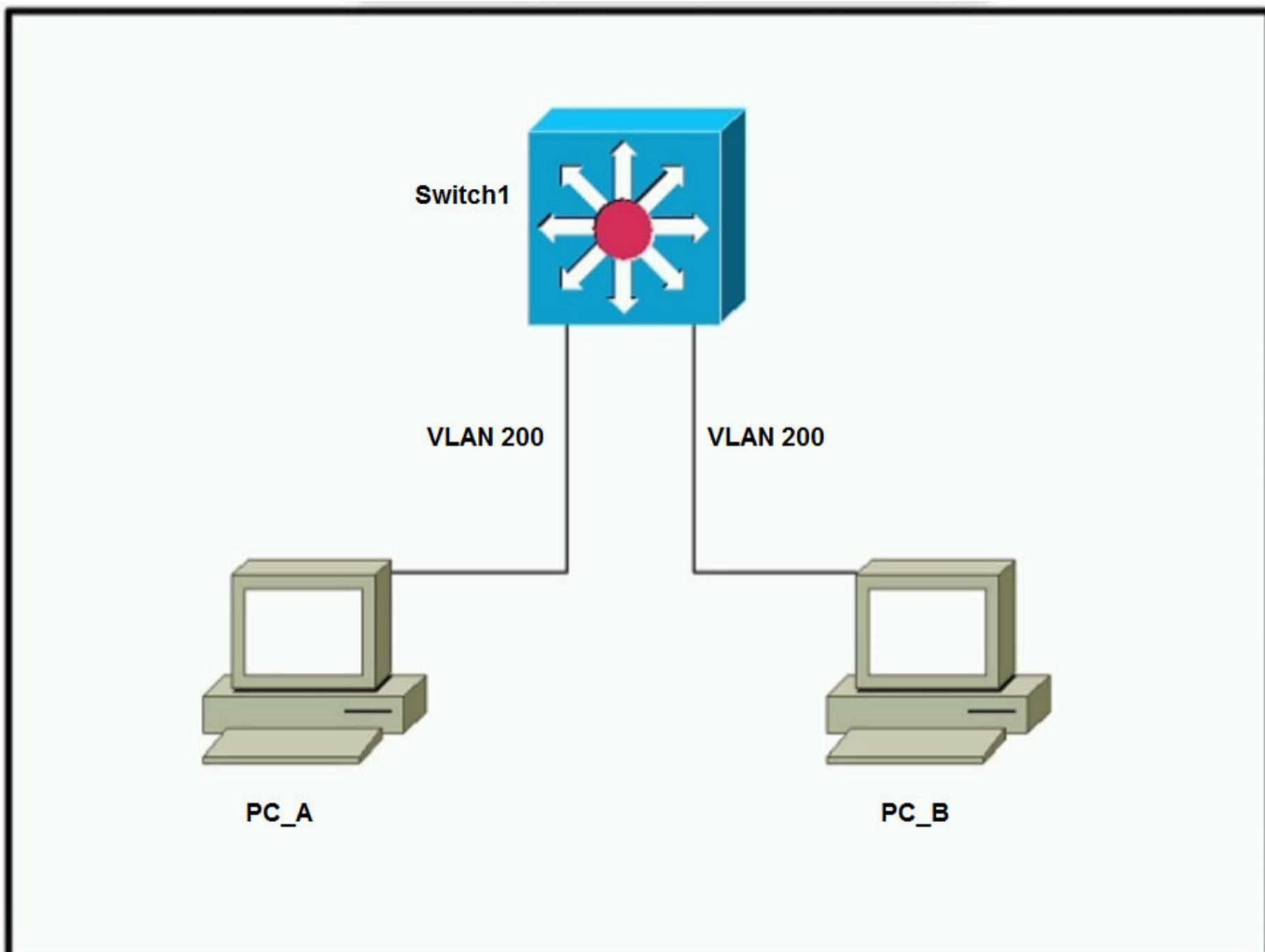
 **SScott** 2 years, 1 month ago

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 ago

key work is after their initial communication
upvoted 18 times

laurvy36 1 year ago
good point noted
upvoted 2 times

GreatDane Highly Voted 1 year 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 11 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, 2 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, 5 months ago

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

 **GreatDane** Most Recent 5 months, 1 week 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** 5 months, 3 weeks 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** 7 months ago

2.4 Ghz uses 5-hop metrics for limiting collisions

upvoted 2 times

 **keokkeo_123** 7 months, 1 week ago

Selected Answer: C

CCCCCC

upvoted 1 times

 **ZUMY** 1 year, 1 month ago

1,6,11 is correct

upvoted 1 times

 **Gaurabdon** 1 year, 1 month 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, 2 months ago

congestion and interference happen in a wireless network

upvoted 2 times

 **marcojmnez** 2 years, 3 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** 5 months, 1 week 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** 7 months, 1 week ago

Selected Answer: C

CCCCCCCCCc
upvoted 3 times

 **Jackie_Manuas12** 1 year, 2 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, 4 months ago

Selected Answer: C

100% is correct
upvoted 2 times

 **ZUMY** 2 years, 1 month ago

C is correct
upvoted 3 times

 **Avalon1** 2 years, 3 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, 7 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 5 months, 1 week 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 6 times

 **Goh0503** Most Recent 7 months, 2 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, 4 months ago

A is correct,

[https://rscciew.wordpress.com/2014/10/26/cisco-band-select-feature/#:~:text=We%20can%20configure%20this%20feature,applications%20\(Like%3A%20Voice\).](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, 4 months ago

reewrewrwe

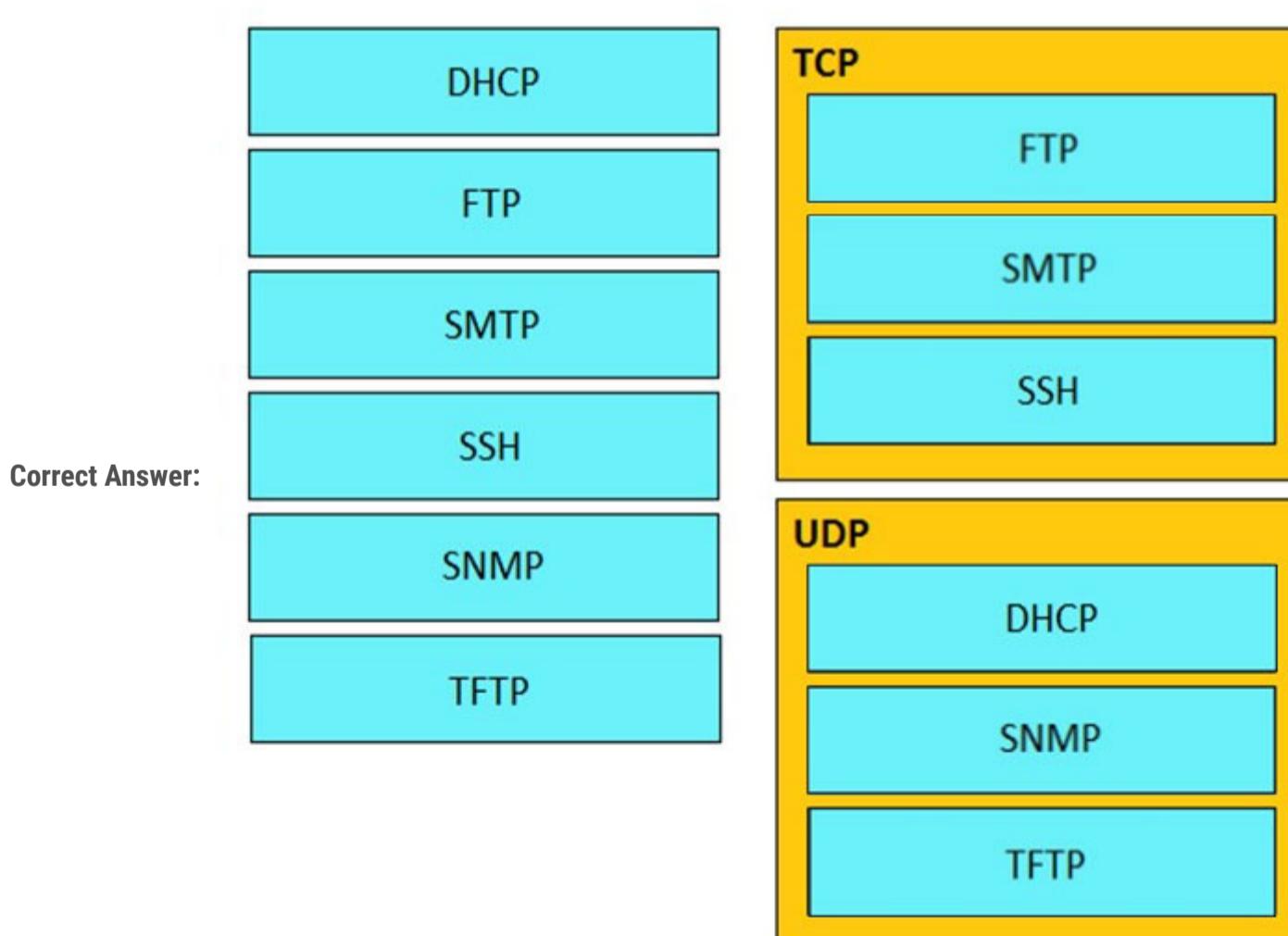
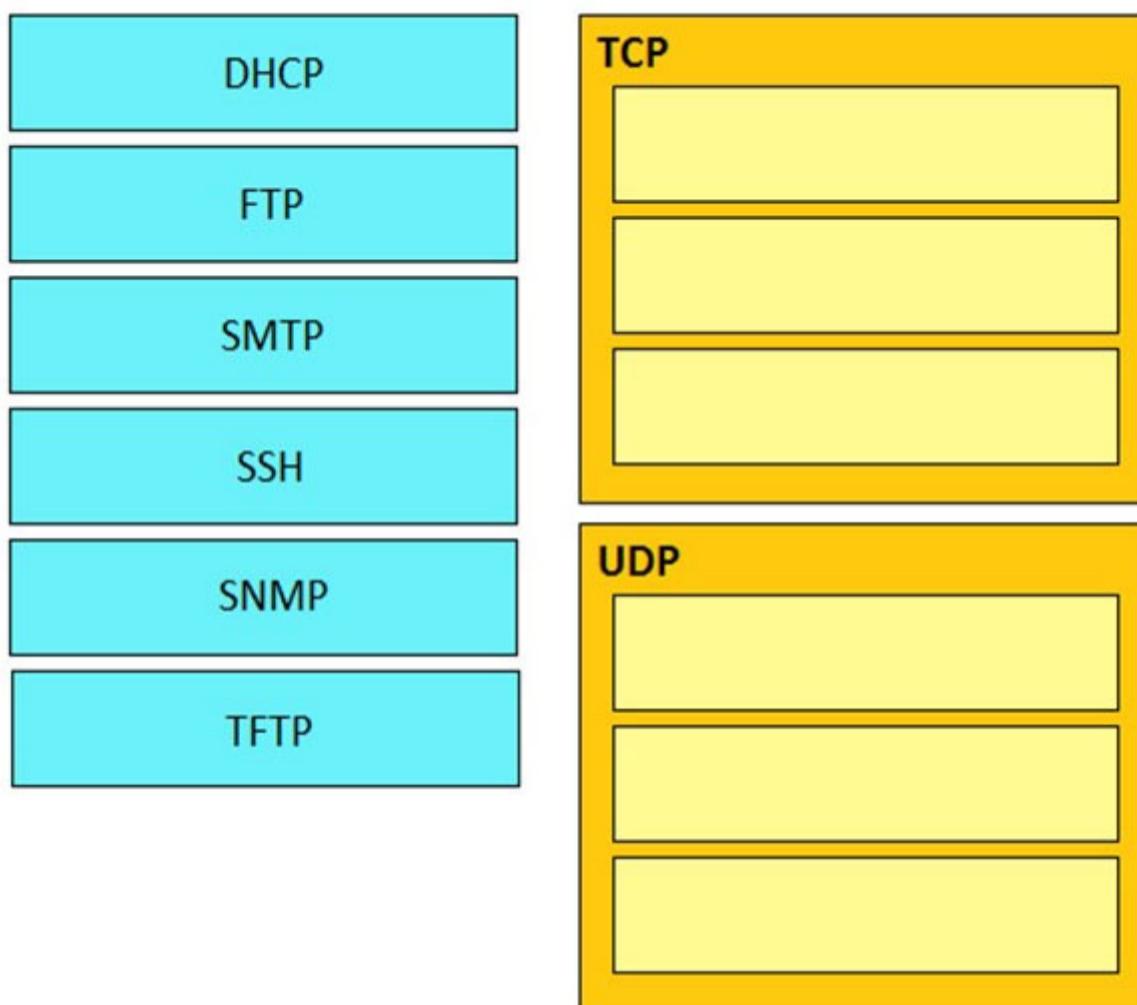
upvoted 2 times

Question #44

DRAG DROP -

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

Select and Place:



 **Mani_Baarathi** Highly Voted  1 year, 10 months ago

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

upvoted 20 times

 **Luinus** Most Recent 6 months, 1 week ago

Coorect

upvoted 1 times

 **creaguy** 8 months 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** 3 months, 3 weeks ago

In that case, RIP and SSH what did you do? .

Thanks in advance!!

upvoted 4 times

 **john1247** 1 month, 2 weeks ago

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

upvoted 2 times

 **NICE_ANSWERS** 1 week, 5 days ago

Please must you specify the port number?

upvoted 1 times

 **dabears** 1 year, 6 months ago

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

upvoted 2 times

 **SasithCCNA** 1 year, 5 months ago

Nope, it can be in any order.

upvoted 5 times

 **ZUMY** 2 years, 1 month ago

Given answers are correct

upvoted 3 times

 **wirlernenman** 2 years, 3 months ago

Correct

upvoted 3 times

 **Ali526** 2 years, 5 months ago

This is correct.

upvoted 3 times

 **SScott** 1 year, 10 months ago

That's right DHCP, SNMP, and TFTP all use UDP.

http://web.deu.edu.tr/doc/oreilly/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, 5 months ago

This is correct.
upvoted 6 times

 **GreatDane** Most Recent 5 months, 1 week 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** 7 months, 1 week ago

Selected Answer: B
BBBBBBBBBBB
upvoted 3 times

 **cortib** 1 year, 8 months 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, 1 month ago

Correct Answer
upvoted 4 times

 **hippyjm** 2 years, 2 months ago

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

upvoted 2 times

Question #46

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, 4 months ago

Physical address is MAC address

upvoted 11 times

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

A & E are correct

upvoted 11 times

 **virab4** Most Recent 1 month, 3 weeks ago

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

upvoted 1 times

 **ViShawnn** 5 days, 2 hours ago

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

upvoted 1 times

 **daddydagoth** 3 months, 2 weeks ago

Specify that we need to choose 2, thank you

upvoted 1 times

 **GreatDane** 5 months, 1 week 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 ago

Selected Answer: AE

Are correct

upvoted 3 times

 **ian77ex** 1 year, 3 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 ago

The questions says for what two purpose
So that's saying select two
upvoted 4 times

✉  **youtri** 2 years, 1 month 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, 4 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, 5 months ago

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

✉  **sinear** 2 years, 4 months ago

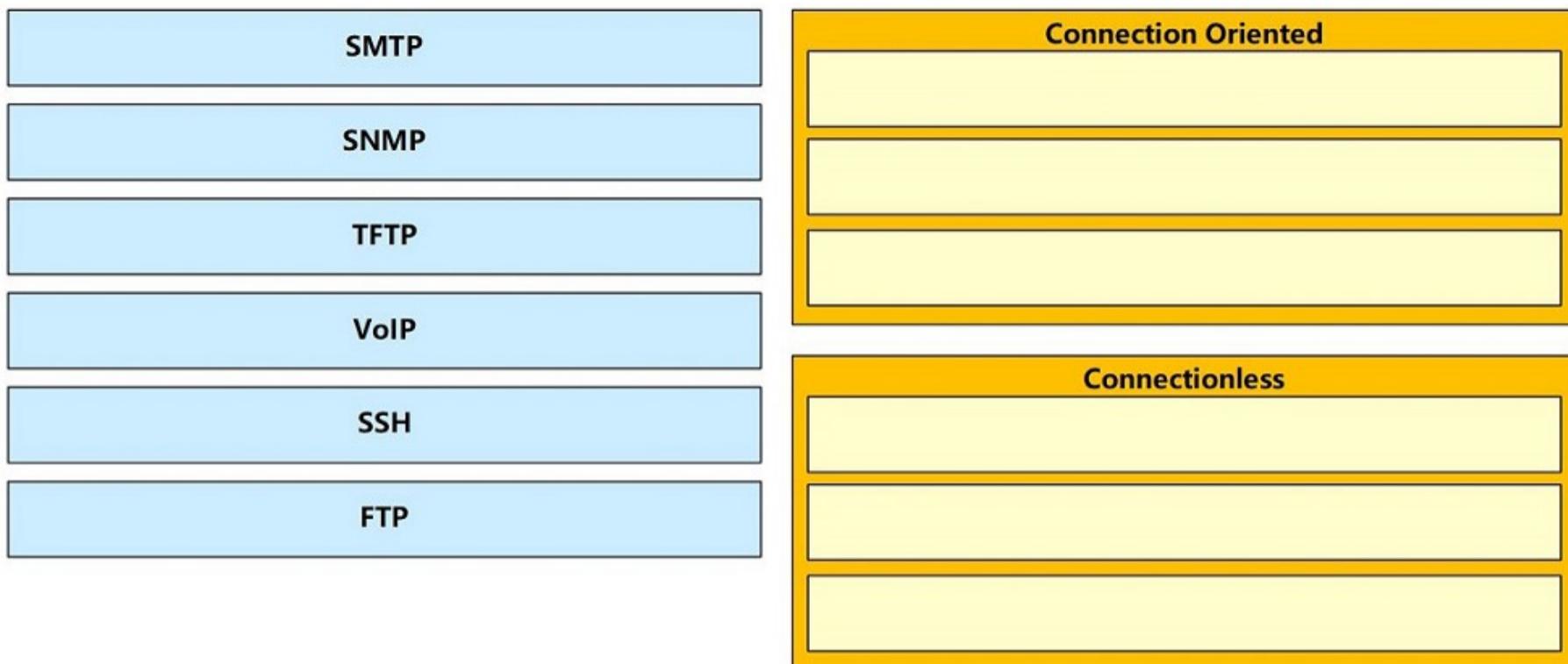
Don't think so. F describes the ARP protocol.
upvoted 3 times

Question #47

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 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

✉ **Black0** Most Recent 1 year, 6 months ago

literally UDP and TCP protocol grouping

upvoted 1 times

✉ **MMAXY** 2 years, 1 month ago

yea correct

upvoted 3 times

✉ **ZUMY** 2 years, 1 month ago

Given answer is correct

upvoted 4 times

✉ **Ali526** 2 years, 5 months ago

This is correct.

upvoted 3 times

Question #48

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%)	13%
---------	-----

 **Alizadeh**  5 months, 3 weeks 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 6 times

 **Dutch012**  3 months, 3 weeks ago

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

upvoted 1 times

 **iMo7ed** 4 months ago

Selected Answer: C

C is correct

upvoted 2 times

 **ProgSnob** 5 months 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 to come.

upvoted 1 times

 **GreatDane** 5 months, 1 week 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** 5 months, 3 weeks ago

Selected Answer: C

C is correct
upvoted 1 times

✉ **Ioannis_Vos** 5 months, 3 weeks 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** 6 months, 3 weeks ago

Selected Answer: C

C is correct
upvoted 2 times

✉ **keokkeo_123** 7 months, 1 week ago

Selected Answer: A

PREEEEE
upvoted 2 times

✉ **seeemo** 9 months, 1 week 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, 6 months ago

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

✉ **ProgSnob** 1 year, 6 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, 6 months ago

A is correct
upvoted 1 times

✉ **DonnerKomet** 1 year, 9 months ago

According to CISCO preamble is 8 Bytes
upvoted 1 times

7 bytes and not 8
upvoted 1 times

✉ **cormorant** 7 months ago

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

✉ **ZUMY** 2 years, 1 month ago

C is correct
upvoted 4 times

✉ **ZayaB** 2 years, 4 months ago

This might help to understand Ethernet frame:
[https://www.geeksforgeeks.org/ethernet-frame-format/#:~:text=Ethernet%20\(IEEE%20802.3\)%20Frame%20Format,starts%20with%207%2DBytes%20Preamble.&text=Destination%20Address%20%E2%80%93%20This%20is%206,MAC%20address%20of%20source%20machine.](https://www.geeksforgeeks.org/ethernet-frame-format/#:~:text=Ethernet%20(IEEE%20802.3)%20Frame%20Format,starts%20with%207%2DBytes%20Preamble.&text=Destination%20Address%20%E2%80%93%20This%20is%206,MAC%20address%20of%20source%20machine.)
upvoted 3 times

✉ **Ali526** 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, 3 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, 3 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, 2 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, 1 month ago

D is the answer
R1(config)#int Gi0/0
R1(config-if)#ip address dhcp
upvoted 6 times

 **GreatDane** Most Recent  5 months, 1 week 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, 2 months ago

I am sure I have seen "ip address dynamic or negotiate" somewhere? Anyway I picked dhcp which is correct.
upvoted 1 times

 **Black0** 1 year, 6 months ago

right answer
upvoted 1 times

 **Ali526** 2 years, 5 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, 5 months ago

D is correct.
upvoted 2 times

Question #50

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 1 year, 10 months 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 14 times

 **Belinda** 1 year, 2 months ago

Thanks

upvoted 4 times

 **Joe_Q** Highly Voted 2 years, 2 months ago

The keyword is "Purpose".

upvoted 6 times

 **Dutch012** Most Recent 3 months, 3 weeks 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 2 times

 **timtgh** 3 months, 3 weeks 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** 5 months, 1 week 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** 9 months, 1 week 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, 3 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, 3 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, 1 month 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, 1 month ago

A & B are correct

OSI model is an structure for Both TCP and UDP. So it doesn't ensure reliable delivery always (For UDP)

upvoted 5 times

 **Claudiu1** 2 years, 2 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

 **ronanncir1** 2 years, 3 months ago

Not D as its not always reliable delivery

upvoted 3 times

 **ZayaB** 2 years, 4 months ago

Yes, I also see D is also somehow right. But best and relevant answer is AB

upvoted 2 times

 **Ali526** 2 years, 5 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, 5 months ago

ADE are the answers.

upvoted 13 times

 **GreatDane** Most Recent 5 months, 1 week 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** 7 months, 1 week ago

Selected Answer: ADE

ADE is coorrect ans

upvoted 3 times

 **WINDSON** 1 year ago

I agree ADE are correct. But why C is wrong ?

upvoted 1 times

 **Dezun** 11 months, 2 weeks ago

administrator cannot assign mac address.

upvoted 1 times

 **Adaya** 2 years ago

Yes correct answers

upvoted 3 times

 **ZUMY** 2 years, 1 month 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, 1 month 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 24 times

 **virab4** 1 month, 3 weeks ago

yes inner and outer ip addresses
upvoted 1 times

 **soRwatches** Most Recent 3 months ago

is this type of question in the scope of CCNA?
upvoted 3 times

 **GreatDane** 5 months, 1 week 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, 3 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, 5 months ago

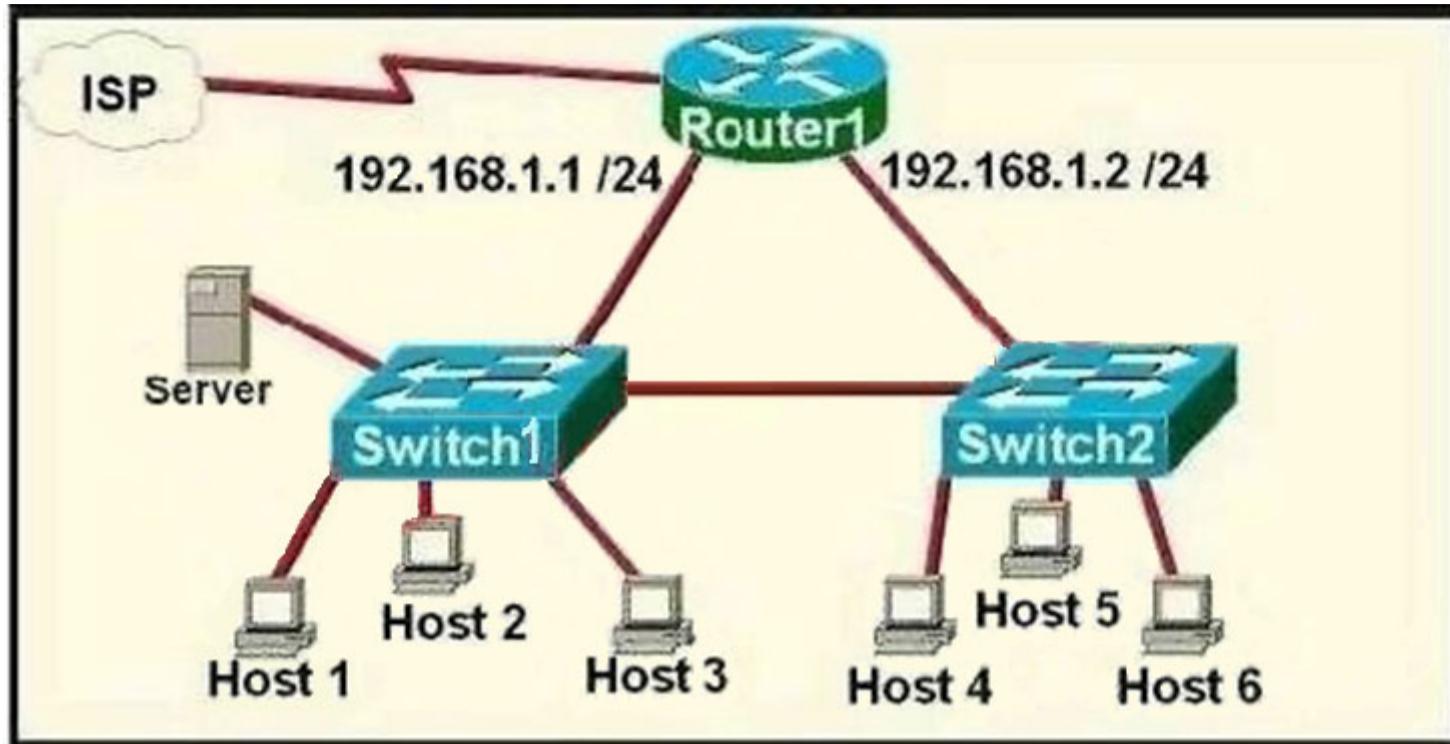
B is the correct answer... 6 to 4

[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.](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

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, 1 month ago

C is correct!

Each router interface Must be in different network.

upvoted 9 times

SScott 2 years 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, 3 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 6 times

timtgh Most Recent 3 months, 3 weeks 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 1 times

elixirwell 2 months, 2 weeks ago

If it was an L3 SW why would they show a router? I guess it was safe to assume.

upvoted 1 times

GreatDane 5 months, 1 week 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, 1 month ago

C is right because Routers are meant to route through different networks

upvoted 2 times

 **CISCO2022** 2 years 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, 3 months ago

Both Rs interfaces overlapping.

upvoted 4 times

 **sinear** 2 years, 4 months ago

Why not also B ? STP is needed as there are 2 SW no ?

upvoted 2 times

 **Chun9** 2 years, 4 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, 4 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

 **lordnano** 2 years, 3 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 make STP necessary.

upvoted 10 times

 **pianetaperez** 2 years, 5 months ago

ip address overlaps

upvoted 3 times

Question #54

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 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 9 times

 **liselsia** 1 year, 7 months ago

i think the static route should have default AD of 1

upvoted 11 times

 **Ali526** Highly Voted  2 years, 5 months ago

AE are correct.

upvoted 7 times

 **PacketFapper** Most Recent  2 weeks, 2 days 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

 **Bhrino** 4 weeks 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 1 times

 **GreatDane** 5 months, 1 week 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** 7 months 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** 7 months, 1 week ago

Selected Answer: AE

AE answer

upvoted 2 times

 **VarDav** 8 months 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** 10 months, 1 week 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, 7 months ago

Why is D not correct?

upvoted 2 times

 **shiv3003** 1 month, 1 week ago

yes it can be D.. AD can be manually be set

upvoted 1 times

 **Taku2023** 3 months, 3 weeks ago

D is correct for me also. it is the next hop ip.

upvoted 1 times

 **laurvy36** 1 year, 5 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 doesn't know the destination

upvoted 2 times

 **Coffeezw** 1 year, 7 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, 1 month ago

AE is correct

upvoted 2 times

 **ZUMY** 2 years, 1 month ago

A & E are correct!

upvoted 2 times

 **jerry19** 2 years, 1 month 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, 1 month 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

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, 1 month ago

B & C are correct!
upvoted 13 times

 **lucky1559** Highly Voted 1 year, 9 months ago

E is not quite that wrong. If not the private addresses, there would be less addresses 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 duplicate 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 than something greater than it, but here it suggests that private costs something which is wrong.
upvoted 8 times

 **Marius_Mario** Most Recent 2 weeks, 1 day ago

I think the right answer are C and E.
upvoted 1 times

 **Jorro99404** 3 weeks, 2 days ago

Selected Answer: BC
B and C are correct
upvoted 1 times

 **Isuzu** 1 month, 1 week 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 weeks ago

While it helps to eliminate duplicate IP problems it doesn't fix it completely and using private address are free making B correct instead of E
upvoted 1 times

 **dearc** 2 months, 1 week 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** 3 months, 2 weeks ago

"they are less costly" is an absolute awful answer considering that they cost nothing but it is technically correct...
upvoted 5 times

✉ **timtgh** 3 months, 3 weeks 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** 5 months, 3 weeks ago

Selected Answer: BC

B and C

upvoted 1 times

✉ **RougePotatoe** 6 months, 3 weeks 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** 4 months, 1 week ago

They are NOT routed the same way as public ipv4 addresses, they are not route-able on the internet

upvoted 6 times

✉ **RougePotatoe** 7 months ago

Anyone knows why A. They are routed the same as public IP addresses. couldn't be an answer?

upvoted 1 times

✉ **diidiuQIdama** 5 months, 3 weeks ago

public router will drop those packets from private addresses so they are not routable on puiblic network

upvoted 4 times

✉ **ian77ex** 1 year, 3 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, 7 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** 2 weeks, 1 day 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** 1 year, 9 months ago

should be C + E imo

upvoted 6 times

✉ **ronanncir1** 2 years, 3 months ago

They are less costly (albeit free) than a public IP Address so the statement is correct. Also, they don't eliminate duplicate IPs.

upvoted 4 times

✉ **timtgh** 3 months, 3 weeks ago

They don't eliminate duplicate IPs, but they do eliminate duplicate IP conflicts, which is what the question says.

upvoted 2 times

✉ **martco** 2 years, 3 months ago

Answer BC

in the real world you pay very handsomely for a static Public IP address assignment lol

not E as they don't eliminate IP conflicts particularly one way or the other

upvoted 2 times

✉ **hokieman91** 2 years, 4 months ago

Voting CE - I think B is a red herring

upvoted 2 times

✉ **hokieman91** 2 years, 4 months ago

After research, I think answer given is correct since even though private IP scheming is "free", there is still chance for duplicate IP's to occur and just by using private IP's doesn't eliminate that.

upvoted 2 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

 **Ali526** Highly Voted 2 years, 5 months ago

AE are correct.

upvoted 9 times

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

A & E are correct!

upvoted 7 times

 **Tobilest** Most Recent 1 month ago

AE are correct

upvoted 1 times

 **MSTAHIR** 4 months, 2 weeks ago

A & E are correct

upvoted 2 times

 **Nebulise** 1 year, 4 months ago

A and E are correct!

upvoted 4 times

 **SUKABLED** 2 years, 4 months ago

AEsy...

upvoted 2 times

 **Nicocisco** 1 year, 3 months ago

EAsty :D

upvoted 1 times

 **Zerotime0** 2 years, 4 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 1 year, 10 months 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 18 times

✉ **nastynasty** 1 year, 5 months ago

haha true

upvoted 1 times

✉ **ZUMY** Highly Voted 2 years, 1 month ago

B & D are correct!

upvoted 7 times

✉ **Manu_FR** Most Recent 1 day, 13 hours ago

Selected Answer: BD

B and D are correct

upvoted 1 times

✉ **cpinac** 3 months 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 4 times

✉ **properchad** 3 weeks, 3 days 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** 3 weeks, 3 days 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** 2 months, 1 week 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, 2 months ago

Terribly worded question, the answers actually tell you what the question is.

upvoted 4 times

✉ **setarehsabz** 1 year, 4 months ago

B and D are correct

upvoted 3 times

 **Doopfenel** 1 year, 6 months ago

Why does it reduce the breach security?

upvoted 6 times

 **Chupacabro** 1 year, 5 months ago

In a scenario that the network isn't connected to the internet.

upvoted 5 times

 **WINDSON** 1 year ago

if your network don't have internet connectivity, how can i hack you ?

upvoted 5 times

 **ismatdmour** 1 year, 3 months ago

private addresses are hidden behind a NAT hence they are not exposed to external reconnaissance attacks from outside the network

upvoted 2 times

 **AlexMD** 1 year, 7 months ago

B & D are correct

upvoted 1 times

 **DavidFitzgerald** 2 years ago

Think there is a typo in the question shouldn't it be: "which two goals ARE reasons..?"

upvoted 2 times

 **Ali526** 2 years, 5 months ago

BD are correct.

upvoted 4 times

 **il_pelato_di_casalbruciato** 2 years, 1 month 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, 1 month ago

A is correct!
upvoted 10 times

 **Manu_FR** Most Recent 1 day, 13 hours ago

Selected Answer: A
A is correct.
upvoted 1 times

 **GreatDane** 5 months, 1 week 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** 11 months, 2 weeks 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** 5 months ago

ISDN is dial up man....
upvoted 5 times

 **all4one** 4 months, 3 weeks ago

hahaha

upvoted 1 times

 **hippyjm** 2 years, 3 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](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, 5 months ago

A .broadband is correct for Small office.

upvoted 3 times

Question #59

Which two WAN architecture options help a business scalability and reliability for the network? (Choose two.)

- A. asynchronous 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 (73%)	AC (27%)
----------	----------

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

Should be C and E for me.
Dynamic routing serves scalability as compared to static routing.
upvoted 27 times

 **Zerotime0** 2 years, 4 months ago

Agree here too e provides and defines scalability in this scenario.
upvoted 2 times

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

C and E for me too..who the hell come up with those questions
upvoted 14 times

 **SUKABLED** 2 years, 4 months ago

However, I guess in the real exam, A and C will count for correct..
upvoted 6 times

 **Isuzu** Most Recent 1 month, 1 week 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 1 times

 **Ciscoman021** 2 months, 2 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** 4 months, 1 week ago

Selected Answer: CE
I am guessing this answer; but I do not think dynamic routing is not an architecture
upvoted 3 times

 **Kosheema** 5 months, 3 weeks ago

Should be A and C
upvoted 1 times

 **HMaw** 5 months, 3 weeks 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** 6 months ago

Selected Answer: AC

According to Google

upvoted 2 times

 **TR3Y** 3 weeks, 6 days 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** 7 months, 2 weeks ago

Selected Answer: AC

I prefer A and C

upvoted 2 times

 **esther18** 7 months, 3 weeks ago

A & C is the correct answer, you guys can google it

upvoted 2 times

 **AWSEMA** 11 months, 2 weeks ago

Selected Answer: CE

I guess c&e

upvoted 1 times

 **ScorpionNet** 1 year, 1 month ago

A and C are correct because it's asking for 2 WAN architecture

upvoted 3 times

 **SelamB** 1 year, 2 months ago

Selected Answer: CE

The answer is C and E. Before the emergence 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, 3 months ago

WAN technologies are very difficult to assign dynamic routing so A,C are correct answers

upvoted 3 times

 **Kane002** 1 year, 4 months ago

How does asynchronous routing provide redundancy or scalability? Suppose you have device 1 and device 2 with 2 segments, A and B, you conduct asynchronous routing on these 2 such that traffic comes in on A and leaves on B, now if either A or B goes out your network is cooked.

upvoted 2 times

 **Lucashrns** 1 year, 5 months ago

Selected Answer: CE

C for reliability and E for scalability

upvoted 1 times

 **gvofke** 1 year, 5 months ago

Selected Answer: CE

C for reliability e E for scalability

upvoted 1 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

D (50%)	B (50%)
---------	---------

 **Santhoshabraham1969** Highly Voted  2 years, 4 months ago

According to latest RFC, unique local address is FD00::/8. Hence option should be D
upvoted 29 times

 **Rob2000** Highly Voted  1 year, 8 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 17 times

 **dearc** 2 months, 1 week 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

 **Jorro99404** Most Recent  3 weeks, 2 days ago

Selected Answer: B
B) FC00 = 11111100
upvoted 1 times

 **jonathan126** 1 month, 2 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 2 times

 **Zortex** 2 months, 3 weeks ago

Selected Answer: D
According to latest RFC, unique local address is FD00::/8.
upvoted 2 times

 **Nutanix_Dummy** 3 months, 2 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** 7 months, 3 weeks 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** 8 months, 2 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** 8 months, 2 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** 8 months, 3 weeks ago

Selected Answer: D

Answer is D

upvoted 2 times

 **g_mindset** 9 months 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** 9 months ago

EXTRACT 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 1 times

 **GreatDane** 1 year ago

Ref: Unique local address – Wikipedia

"...

Definition

...

Unique local addresses use prefix fc00::/7, extended with an 'L' bit which indicates that the address is locally assigned.

...

The prefix field contains the binary value 1111110. The L bit is one for locally assigned addresses; the address range with L set to zero is currently not defined.

..."

A. 00000000

Wrong answer.

B. 11111100

Wrong answer.

C. 11111111

Wrong answer.

D. 11111101

Correct answer.

upvoted 2 times

 **ian77ex** 1 year, 3 months ago

Selected Answer: B

The answer is B.

If the question says: "ipv6 unique local" we must answer FC00::/7 or 11111100

If the question says "locally specified ipv6 unique local" then we must answer FD00::/8 or 11111101

There's a catch in the words and phrases.

The last bit is called the L bit. L=0 is not defined yet. L=1 means "locally specified".

If the question doesn't ask for "locally specified" then we must stick to the more general rule that is FC00::/7 or 11111100

upvoted 5 times

 **Sonieta** 1 year, 8 months ago

The important thing is which is considered the correct answer in the exam. Has anyone had this question? I take the exam in two weeks !! Thank you

upvoted 2 times

 **SSESSE2021** 1 year, 7 months ago

how did you go with the exa,?

upvoted 4 times

 **AlexPlh** 1 year, 10 months ago

CCNA 200-300 Volum 1 Book page 551

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.

D

upvoted 4 times

 **Chutiyapa** 1 year, 11 months ago

If you read the question carefully it says what is the binary pattern, now as per Wiki/IETF the unique local starts with fc /7 address i.e. 0x1111 0x1100. /7 indicates first 7 bits will always be fixed so we just have option to flip 8th bit , 0x1111 0x110 (0) <--if we flip this 8th bit it becomes 0x1111 0x1101 i.e. FD, hence the conclusion unique local starts with fc/7 and the answer is correct. Refer below link from Cisco press to verify the same

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

upvoted 3 times

 **Bne_Pradhan** 1 year, 11 months ago

Will Go with B, Unique local starts with FD= 1111 (F) ,1100(D=12), clean question, dont overthink guys

upvoted 3 times

 **Cocha** 1 year, 11 months ago

sorry A equals 10, B is 11, C is 12 and D is 13 So...your answer should be letter D.

upvoted 3 times

Question #61

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 (83%)	AB (17%)
----------	----------

 **Ali526** Highly Voted 2 years, 5 months ago

AD correct.

upvoted 8 times

 **Isuzu** Most Recent 1 month, 1 week ago

I see no one is looking at E.... Correct Answer: D & E

upvoted 1 times

 **dearc** 2 months, 1 week 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** 4 months ago

Selected Answer: AD

A and D are correct

upvoted 2 times

 **Bilal1992** 4 months, 1 week ago

AD IS CORRECT

upvoted 2 times

 **DB_Cooper** 4 months, 3 weeks 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 1 times

 **DB_Cooper** 4 months, 3 weeks ago

i change my answer to AD. disregard my comment

upvoted 8 times

 **jnanofrancisco** 4 months, 3 weeks ago

A & D are correct

upvoted 1 times

 **onikafei** 1 year, 3 months ago

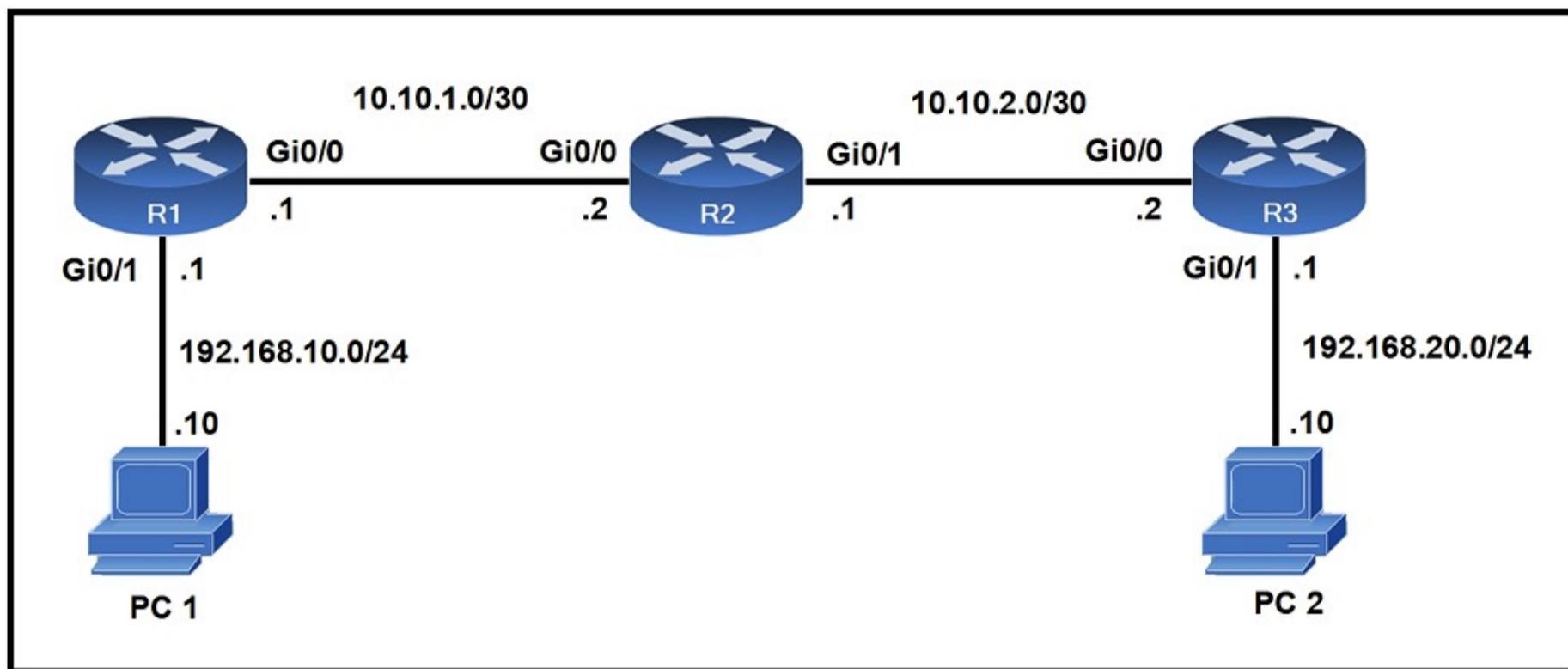
Selected Answer: AD

A and D are correct
upvoted 1 times

 **ZUMY** 2 years, 1 month ago
A & D are correct
upvoted 3 times

Question #62

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%)

Aie_7 4 months, 4 weeks 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 ago

C is the correct answer

upvoted 2 times

Cyberops 1 year, 1 month ago

c is correct answer

upvoted 1 times

sovalaf192 1 year, 4 months ago

Selected Answer: C

No NAT in place, so C is OK.

upvoted 2 times

Heymannicerouter 1 year, 9 months 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**  1 year, 9 months ago

C is correct
Hot-Swap-Component that of device can be removed or install without powering down the device.
upvoted 10 times

✉  **peplegal** 1 month, 3 weeks 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 Zумy!
upvoted 1 times

✉  **dearc**  2 months, 1 week 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** 2 months, 2 weeks ago

Selected Answer: C

right answer is c
upvoted 1 times

✉  **erikkkkka** 1 year 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

✉  **Jbcrggddfh** 1 year, 1 month 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, 1 month 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 5 months, 3 weeks ago

Selected Answer: AE

If an answer choice has definitive language like "exclusively" or "solely" it's usually wrong.
upvoted 5 times

 **huykg009** Most Recent 6 months ago

the Correct Answer is B and C
upvoted 1 times

 **huykg009** 6 months 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 1 year, 9 months ago

low cost at first but will be difficult to scale in future, because cable requirement increase, each new site require full mesh 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

 **JulietaMT98** Highly Voted 1 year, 3 months ago

Selected Answer: A

In collapsed core architecture, the core and distribution layers are combined, simplifying the design.

upvoted 5 times

 **Isuzu** Most Recent 1 month, 1 week 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

 **Ciscoman021** 2 months, 2 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 2 times

 **moise_amo** 4 months ago

Selected Answer: A

A is the corect answer

upvoted 3 times

 **ZUMY** 1 year, 9 months ago

A is correct

upvoted 2 times

 **SScott** 1 year, 9 months 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 weeks ago

Layer 3 = different network

Layer 2: same network

upvoted 1 times

 **Ciscoman021** 2 months, 2 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** 4 months, 4 weeks 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** 7 months, 4 weeks 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, 1 month ago

Basically functions between Routers, Layer 3 switches especially the Firewall enabled

upvoted 1 times

 **RichyES** 1 year, 4 months ago

Selected Answer: D

D is the the answer

upvoted 4 times

 **Hodicek** 1 year, 6 months ago

ROUTER FUNSTION IN SUMMARY

upvoted 3 times

 **ZUMY** 1 year, 9 months ago

D is correct

upvoted 2 times

Question #67

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, 1 month 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 6 times

 **sany11** Most Recent 1 month, 1 week ago

Selected Answer: AC

this layer is concerned with speed and ensures reliable delivery of packets.

upvoted 2 times

 **ricky1802** 4 months 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 4 times

 **Sauceboyzzjp** 1 year, 3 months ago

this design is very clear it only meant to forward traffic as fast as possible

upvoted 4 times

 **ZUMY** 1 year, 9 months ago

A,C Correct

upvoted 3 times

 **ZUMY** 1 year, 9 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** 1 year, 10 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** 1 year, 10 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** 1 year, 11 months ago

given answers are correct

upvoted 2 times

 **lordnano** 2 years, 2 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 physical layers.

I would stick to A and C. That fits also to the reference link.

upvoted 4 times

 **1Mohit1** 1 year, 11 months ago

Agreed A and C make the most sense.

upvoted 2 times

 **SScott** 1 year, 9 months 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, 3 months ago

Agreed, answer is A and B

upvoted 2 times

 **Nicocisco** 1 year, 3 months ago

Policy is in distribution layer

upvoted 1 times

 **imad** 2 years, 3 months ago

correct answers are a and b

upvoted 3 times

 **Nicocisco** 1 year, 3 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 1 year, 9 months 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 channels, or you have co-channel interference, which slows down your wireless operation. (Adjacent channel interference causes collisions)

upvoted 15 times

 **ZUMY** Highly Voted 1 year, 9 months ago

A is correct

upvoted 8 times

 **dearc** Most Recent 2 months, 1 week 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** 3 months, 2 weeks ago

Selected Answer: A

1,6,11 channels to avoid co-channel interruption.

upvoted 1 times

 **Mokonyana** 4 months ago

i think the keyword is "co-channel". I would say the right answer is A.

upvoted 2 times

 **Fab79** 5 months, 2 weeks ago

Selected Answer: A

A correct

upvoted 4 times

 **Abdullahalbsheesh** 6 months ago

Selected Answer: C

C is correct

upvoted 2 times

 **dendentester** 8 months ago

C IS CORRECT

upvoted 1 times

 **saeed_huhu** 10 months, 3 weeks 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 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 ago

I think they are referring to multiple access points, not just 2.
upvoted 2 times

✉ **Nebulise** 1 year, 4 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** 1 month ago

aswer D
upvoted 1 times

✉ **Ciscoman021** 2 months, 2 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, 7 months ago

D is the right answer.
upvoted 2 times

✉ **ZUMY** 1 year, 9 months ago

D is correct
upvoted 3 times

✉ **DonnerKomet** 1 year, 9 months ago

SaaS provides te required Software, operating system and network:
Provides ready-to-use application or software
upvoted 3 times

✉ **SScott** 1 year, 9 months ago

Yes D occasional hosted application is SaaS
<https://www.cloudflare.com/learning/cloud/what-is-saas/>
upvoted 1 times

✉ **shakyak** 1 year, 7 months ago

Occasionally has nothing to do with Saas. It's just there to trick you.
upvoted 2 times

Question #70

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, 3 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

 **Ciscoman021** Most Recent  2 months, 2 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** 5 months, 1 week 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** 10 months, 3 weeks ago

Selected Answer: CE

You need Router On Stick to route VLAN - so A-E

D is incorrect

upvoted 1 times

 **ismatdmour** 1 year, 3 months ago

I meant to say "encapsulates a L2 frame which in turn embed a MAC address"

upvoted 2 times

✉  **panagiss** 1 year, 6 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, 3 months ago

We need L3 switches to transfer different VLAN
upvoted 3 times

✉  **ScorpionNet** 1 year, 1 month ago

Or a Router with subinterfaces configured
upvoted 1 times

✉  **babaKazoo** 1 year, 7 months ago

C and E are correct put a switch moves frames and not packets.
upvoted 3 times

✉  **ZUMY** 1 year, 9 months ago

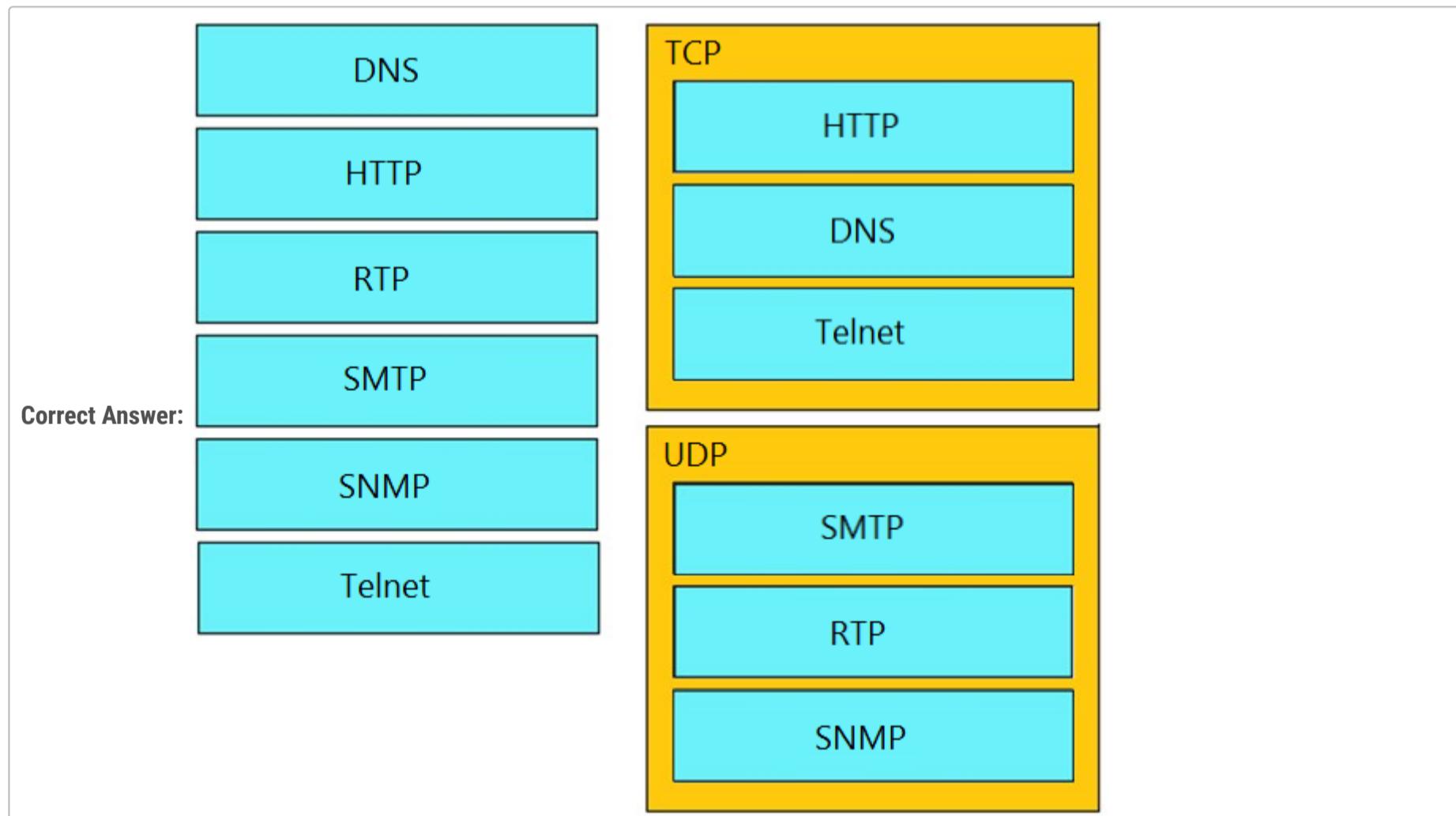
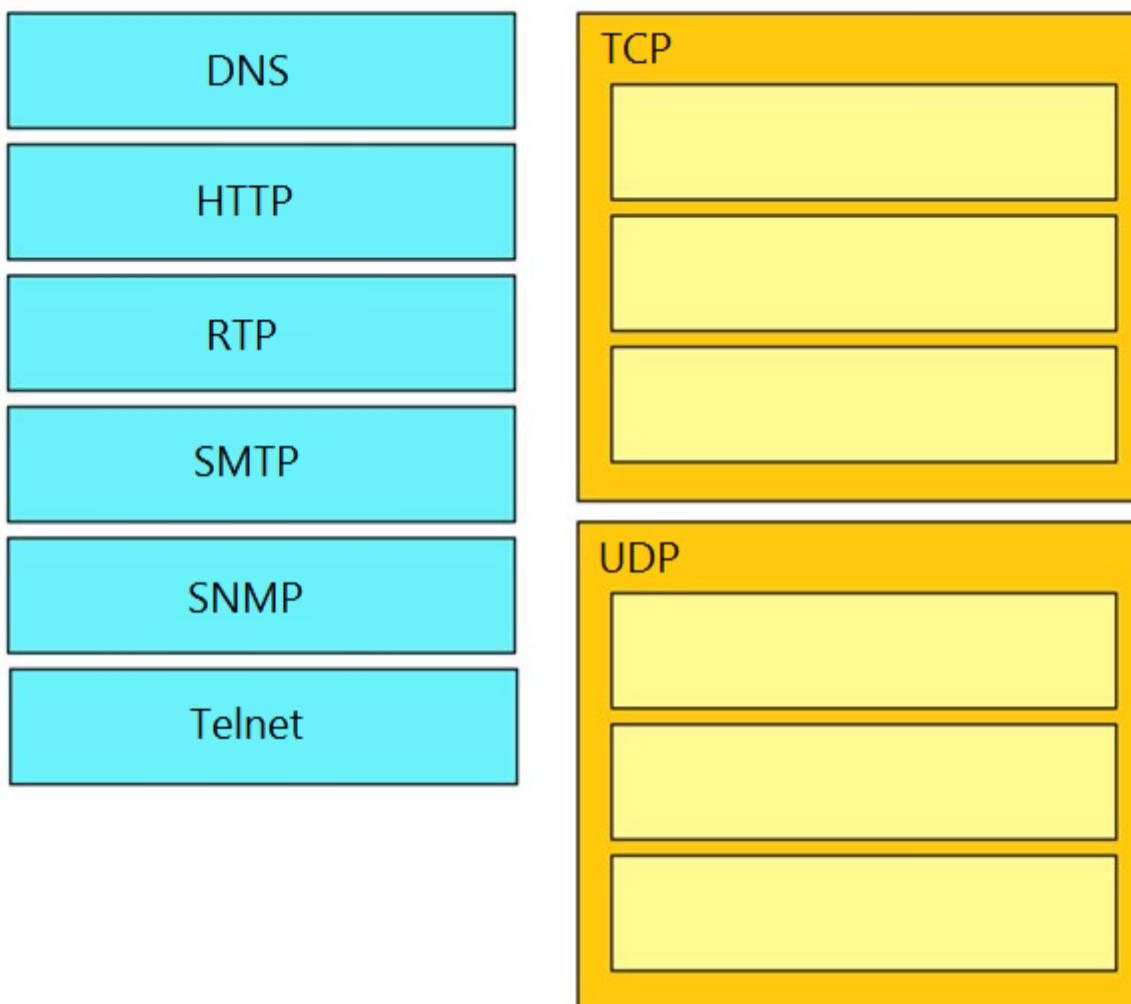
C,E are correct
upvoted 2 times

Question #71

DRAG DROP -

Drag and drop the TCP/IP protocols from the left onto their primary transmission protocols on the right.

Select and Place:



splashy Highly Voted 9 months 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 start, 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 44 times

✉  **esther18** Highly Voted 7 months, 3 weeks ago

TCP- HTTP, SMTP, Telnet

UDP- DNS, RTP, SNMP

upvoted 19 times

✉  **Danishh** Most Recent 1 month ago

TCP - HTTP, SMTP, Telnet, FTP, SSH, POP3, HTTPS

UDP - DHCP, DHCP(client), TFTP, SNMP,

TCP & UDP - DNS (53)

upvoted 1 times

✉  **Hope_12** 1 month 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** 4 months, 3 weeks ago

HTTP, SMTP, TELNET

DNS, RTP, SNMP

upvoted 2 times

✉  **freaknowledge123** 5 months ago

smtp use tcp please correct the answer

upvoted 6 times

✉  **Kosheema** 5 months, 2 weeks ago

TCP:SMTP, Telnet, HTTP

UDP: RTP, DNS, SNMP

upvoted 2 times

✉  **Kosheema** 5 months, 2 weeks ago

SMTP is a TCP. Are the answers of this pool correct?

upvoted 2 times

✉  **Garfieldcat** 7 months, 2 weeks ago

SMTP is TCP

upvoted 4 times

✉  **santoshSre** 7 months, 2 weeks ago

SMTP and DNS are TCP right?

upvoted 3 times

✉  **SamuelSami** 7 months, 3 weeks 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** 8 months, 2 weeks ago

SMTP is TCP

upvoted 2 times

✉  **j6** 8 months, 1 week ago

thank you i thought it was

upvoted 1 times

✉  **Danielki** 1 year, 1 month ago

Isn't it DNS use both UDP AND TCP?

upvoted 3 times

✉  **ZUMY** 1 year, 1 month ago

Given answers are correct!

upvoted 1 times

✉  **Bibi20** 8 months, 3 weeks ago

Nope SMTP is TCP

upvoted 3 times

✉  **mikey822** 1 year, 3 months ago

TCP= Internet (HTTP), Mail (SMTP), and Telnet

upvoted 4 times

 **kljw5** 1 year, 3 months ago

Wondering if anyone had an easy way to remember these i seem to always get them confused

upvoted 1 times

 **yuh** 1 month ago

Frequently asked port number 20s is TCP.

ftp20-21,SSH22,TELNET23,SMTP25

upvoted 1 times

 **znabbe** 1 year, 2 months ago

With the usual FTP, TFTP, DHCP, SNMP, SMTP and HTTP i place the ones ending with TP except for TFTP in tcp. Haven't figured out an easy way to remember the other protocols

upvoted 3 times

 **Alvaro13** 11 months, 2 weeks ago

SNMP is UDP

upvoted 1 times

 **dropspablo** 1 month, 1 week ago

yes, he said only those ending in TP (minus TFTP). But RTP is also UDP, be careful with that hahaha

upvoted 1 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 1 year, 10 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 5 months, 1 week 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

geober Most Recent 7 months, 1 week 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 9 months, 1 week 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, 1 month ago

A is correct

upvoted 2 times

AlexMD 1 year, 7 months ago

A is correct answer

upvoted 1 times

Shaz313 1 year, 10 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

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 1 year, 10 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** 1 year, 9 months ago

I think, this question refers to SDN terminology, so the data plane takes care of forwarding and uses the tables created by control plane to do it.
upvoted 3 times

 **Kane002** Highly Voted 1 year, 4 months ago

The data plane is also sometimes referred to as the "Forwarding plane".
upvoted 11 times

 **Ciscoman021** Most Recent 1 month, 3 weeks 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** 4 months ago

Selected Answer: D

It is D

upvoted 1 times

 **GreatDane** 5 months, 1 week 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** 5 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 3 times

 **guynetwork** 9 months ago

It is D

upvoted 1 times

 **sasquatchshrimp** 10 months, 2 weeks 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 adheres 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** 10 months, 2 weeks ago

I recant my answer. D sounds better with how silly the question and answers are worded.

upvoted 2 times

 **splashy** 10 months 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

 **Jbcrggddfh** 1 year, 1 month 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

 **Jbcrggddfh** 1 year, 1 month 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 11 months, 2 weeks 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

 **iMo7ed** Most Recent 4 months ago

Selected Answer: C

C is correct
upvoted 1 times

 **remoto** 5 months, 3 weeks ago

Selected Answer: C

ok the answer
upvoted 1 times

 **santoshSre** 7 months, 2 weeks 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** 8 months, 3 weeks 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, 1 month ago

C is the correct answer
upvoted 1 times

 **ZUMY** 1 year, 1 month ago

C : is correct
upvoted 1 times

 **JonCCNA12** 1 year, 2 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, 2 months ago

C is the most correctness.
upvoted 1 times

 **chrisp31** 1 year, 3 months ago

Selected Answer: C

C is most correct. Connection based, need to get packets and verify.
upvoted 1 times

 **ismatdmour** 1 year, 3 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, 3 months ago

Selected Answer: C

A and C are both correct, however in this case you're going to want to pick TCP to transmit critical data. You aren't going to pick TCP or UDP over latency upvoted 2 times

Namek 1 year, 4 months ago

Selected Answer: C

The correct answer is C

upvoted 1 times

Nicocisco 1 year, 4 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, 4 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 that 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, 3 months ago

I think you're overthinking the question. Option C would be the best response as TCP is used 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, 5 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

shehabdawood 1 year, 5 months ago

think A, C are true answers

upvoted 1 times

Question #75

Topic 1

```

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 (75%)

B (25%)

 **Zara2stra**  1 year, 11 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 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. So answer A is correct.

upvoted 16 times

 **LordScorpius** 1 year, 1 month 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

 **SScott** 1 year, 9 months 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**  7 months, 2 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 6 times

⊕ **Hope_12** Most Recent 1 month ago

Selected Answer: B

A is result not the cause which is the one asked in the question.

upvoted 1 times

⊕ **Rydaz** 4 weeks ago

txload and rxload are low... so it can't be high usage right?

upvoted 1 times

⊕ **VictorCisco** 1 month, 3 weeks ago

Error increase is not the cause of the issue is the consequence/result of the issue!! A wrong cable could be an issue...

upvoted 1 times

⊕ **gc999** 2 months, 4 weeks ago

I think A is the outcome, not the cause. So answer is B

upvoted 1 times

⊕ **shutie** 3 months, 3 weeks ago

I had had an confusing idea why A is correct, not B because of what the question says UNTIL I found rx/rxload indicator 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 1 times

⊕ **iMo7ed** 4 months ago

Selected Answer: A

A is correct

upvoted 1 times

⊕ **GreatDane** 5 months, 1 week 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 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.

..."

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** 7 months 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** 9 months 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** 10 months, 1 week 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** 10 months, 2 weeks 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 ago

Selected Answer: A

A, 166/255

upvoted 2 times

LordScorpius 1 year, 1 month ago

Selected Answer: B

Again, not what is the problem but, what is the cause: B.

upvoted 1 times

LordScorpius 1 year, 1 month 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, 1 month 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 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.

<https://networklessons.com/cisco/ccnp-tshoot/cisco-ios-show-interface-explained>

upvoted 1 times

ZUMY 1 year, 1 month 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 3 times

jahinchains 1 year, 1 month ago

and the question is what causes it? B!

upvoted 3 times

Vinarino 1 year, 4 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 1 year, 9 months ago

C is the right compressed address.
<https://iplocation.io/ipv6-compress>
upvoted 5 times

 **Jorro99404** Most Recent 1 week, 1 day ago

Selected Answer: C
The correct one
upvoted 2 times

 **cormorant** 7 months ago

at last a question with a correct answer that makes sense
upvoted 4 times

 **keokkeo_123** 7 months, 1 week ago

Selected Answer: C
C is correct
upvoted 3 times

 **ZUMY** 1 year, 1 month ago

C is correct!
upvoted 2 times

 **onikafei** 1 year, 4 months ago

Dumbed it down to c or a, a however was incorrect. 0000 should have been shortened
upvoted 1 times

 **priya17** 1 year, 7 months ago

C correct answer
upvoted 1 times

 **Sonieta** 1 year, 8 months ago

Yes, C is the better way to compress
upvoted 1 times

 **NZIAKOU** 1 year, 9 months 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 10 months, 3 weeks ago

Answer is D as a firewall is used for stateful packet inspection.

upvoted 5 times

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

Selected Answer: D

D is correct!

upvoted 2 times

 **ZUMY** 1 year, 1 month ago

D is correct!

upvoted 3 times

 **AlexMD** 1 year, 7 months ago

D is correct answer

upvoted 3 times

 **ABlboyscorner** 1 year, 7 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 1 year, 11 months ago

C is correct.
upvoted 9 times

✉️  **Petermwathe** Most Recent 4 months, 1 week ago

C is correct
upvoted 1 times

✉️  **ZUMY** 1 year, 1 month ago

C is correct!
upvoted 3 times

✉️  **Nebulise** 1 year, 6 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%)

 **ABlboycorner** Highly Voted  1 year, 7 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 13 times

 **iMo7ed** Most Recent  4 months ago

Selected Answer: B

It is B

upvoted 2 times

 **sasquatchshrimp** 10 months, 2 weeks ago

read it as, "what give a virtual computer access to physical hardware?" Hypervisor.

upvoted 1 times

 **ZUMY** 1 year, 1 month ago

B is correct

upvoted 2 times

Question #80

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 manufacturers 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 (79%) D (21%)

 **SScott** Highly Voted 1 year, 9 months 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** 1 year, 9 months 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** 1 year, 9 months ago

I agree with you SScott.

upvoted 5 times

 **Ciscoman021** Most Recent 2 months, 1 week 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 3 times

 **oatmealturkey** 3 months, 3 weeks 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** 4 months ago

Selected Answer: C

the question is for channel overlaps principally, not for band select

upvoted 1 times

 **Anas_Ahmad** 4 months, 2 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** 5 months, 1 week 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 too 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** 6 months, 2 weeks ago

C is the Best

upvoted 1 times

 **mzu_sk8** 6 months, 3 weeks ago

D on another site without explanation

upvoted 1 times

 **splashy** 9 months 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** 10 months, 1 week 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** 10 months, 1 week ago

Selected Answer: D

I think it's D

upvoted 1 times

 **saeed_huhu** 10 months, 3 weeks ago

Selected Answer: C

C - Dynamic Channel Assignment DCA

upvoted 1 times

 **SH_** 11 months, 1 week 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, 1 month 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, 1 month ago

Selected Answer: D

the parameter on C are client load and background noise? how does it concern in channel overlap? D is good...
upvoted 1 times

 **D0nkey_h0t** 11 months, 3 weeks ago

when channels overlap the noise level is high
upvoted 1 times

 **ZUMY** 1 year, 1 month 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

 **asyouwish007** 1 year, 1 month ago

Selected Answer: C

C is correct
upvoted 1 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 11 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 5 times

 **ZUMY** Most Recent 1 year, 1 month ago

Going with C:

upvoted 3 times

 **Bigc0ck** 1 year, 2 months ago

Isn't private IP addressing just the same as saying NAT?

upvoted 1 times

 **DoBronx** 7 months, 2 weeks ago

ur name tho]

upvoted 3 times

 **awashenko** 1 year, 3 months ago

Selected Answer: C

Best answers is C

upvoted 2 times

 **ian77ex** 1 year, 3 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, 4 months ago

Selected Answer: C

Sorry, I checked that the correct one is C.

upvoted 2 times

 **hector255** 1 year, 4 months ago

Selected Answer: D

Sorry, I checked that the correct one is C.

upvoted 1 times

 **hector255** 1 year, 4 months ago

Selected Answer: A

Option A is the correct.

upvoted 1 times

 **kijken** 1 year, 4 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, 4 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, 4 months ago

Selected Answer: C

Private IP address are used to conserve IP addresses

upvoted 1 times

 **gvofke** 1 year, 5 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, 6 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(WAN)

upvoted 2 times

 **marked** 1 year, 7 months ago

As far I know subnet is done to save and utilise address space in the network. So I opt C

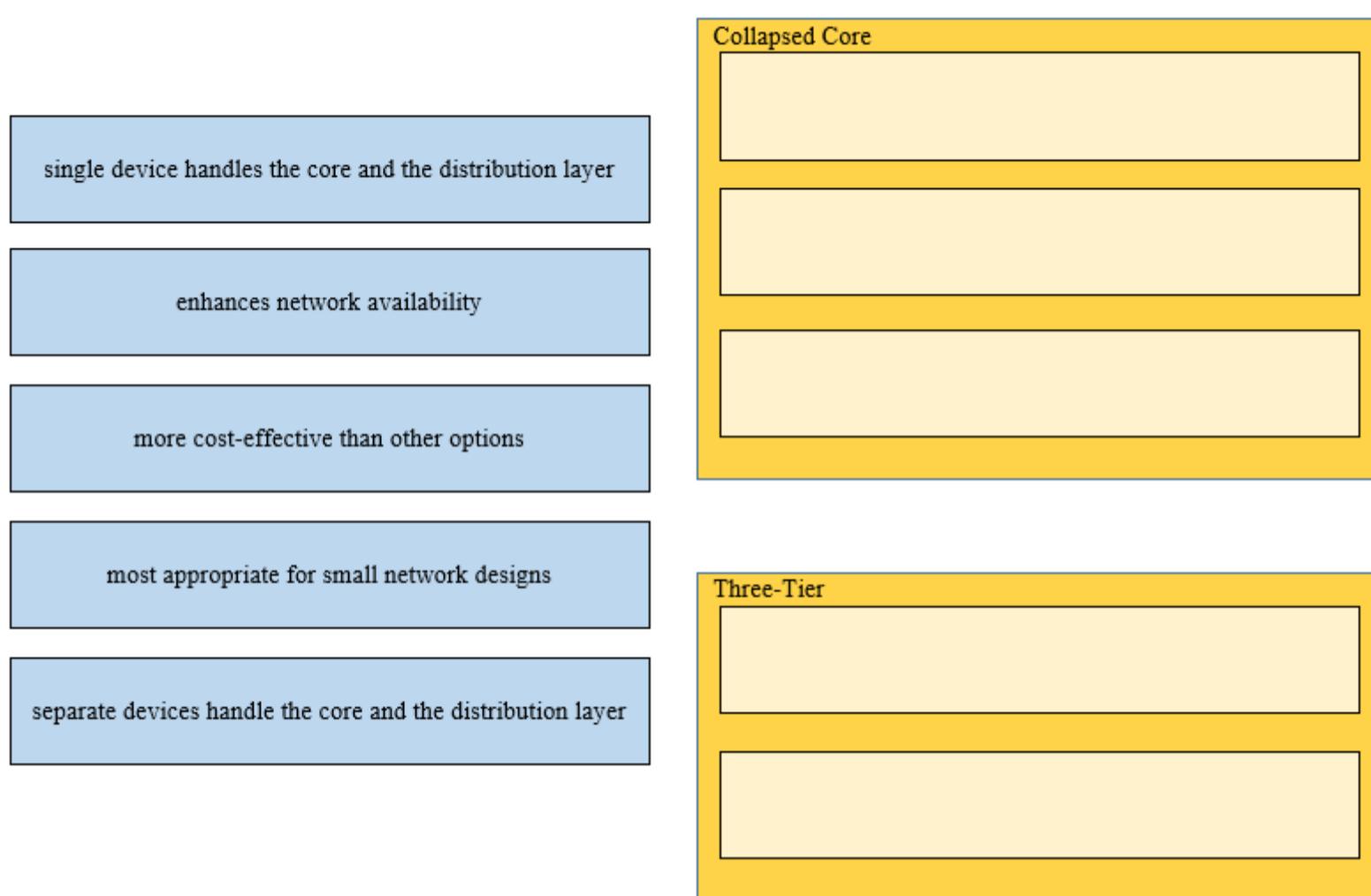
upvoted 1 times

Question #82

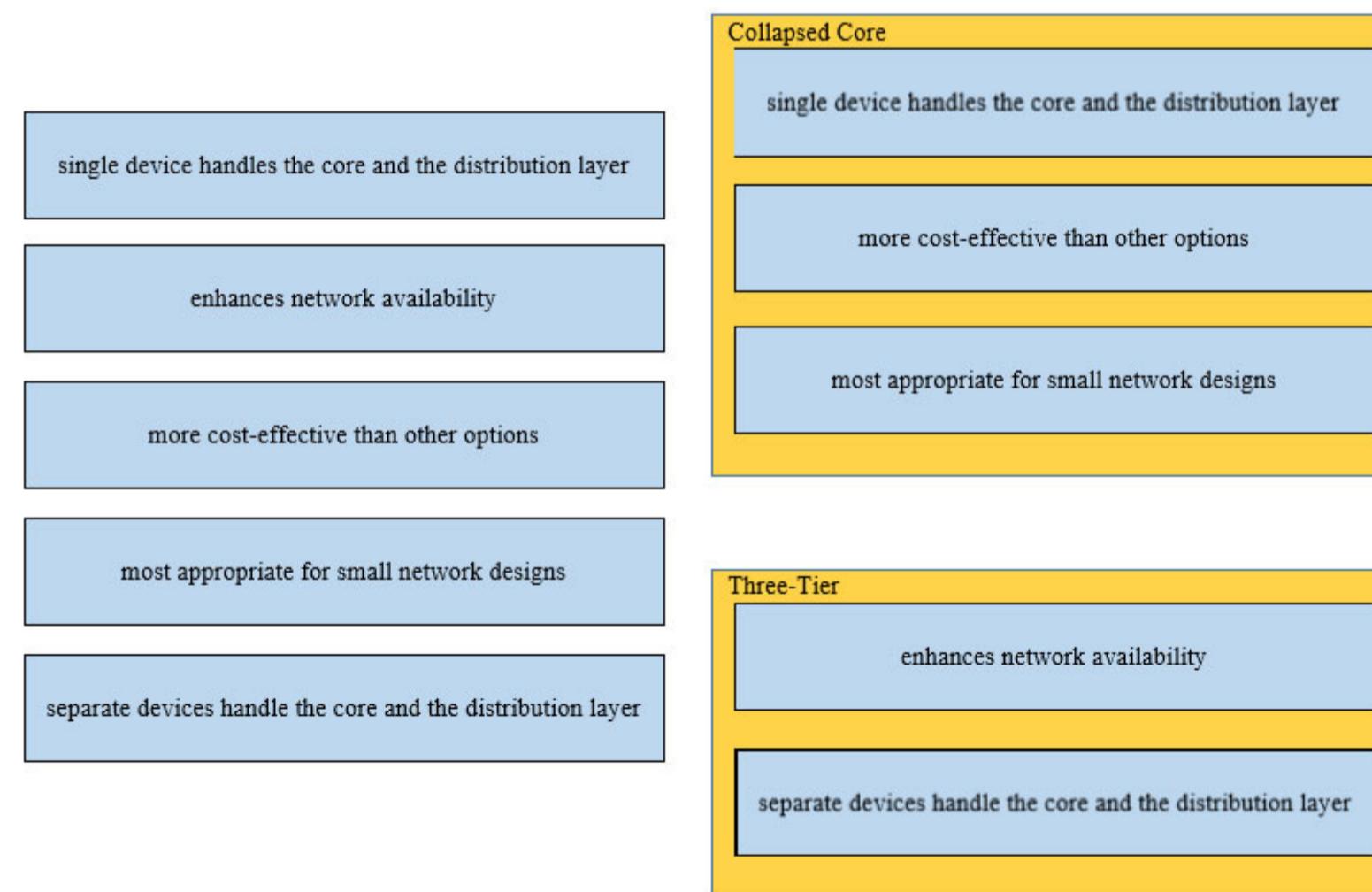
DRAG DROP -

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  6 months, 1 week ago

Given Answers Are Correct....

upvoted 6 times

 **ELHAZ** Most Recent  2 months, 2 weeks ago

Collapsed core :

Single device handles the core and the distribution layer

more cost-effective than other option

most appropriate for small network designs

Tree-Thier:

enhances network availability
separate devices handles the core and the distribution layer
upvoted 1 times

 **harkindeylee** 3 months, 1 week 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, 1 month 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 19 times

 **TA77** 1 year ago

Thank you

upvoted 2 times

 **VirtuaTech** Most Recent 4 weeks, 1 day ago

repeated question

upvoted 1 times

 **harkindeyee** 3 months, 1 week ago

B is correct

upvoted 1 times

 **GreatDane** 5 months, 1 week 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 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** 6 months, 3 weeks 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** 11 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 2 times

 **[Removed]** 1 year, 4 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, 1 month ago

B is correct
upvoted 8 times

 **Smaritz** Highly Voted 1 year, 3 months ago

B is correct
upvoted 6 times

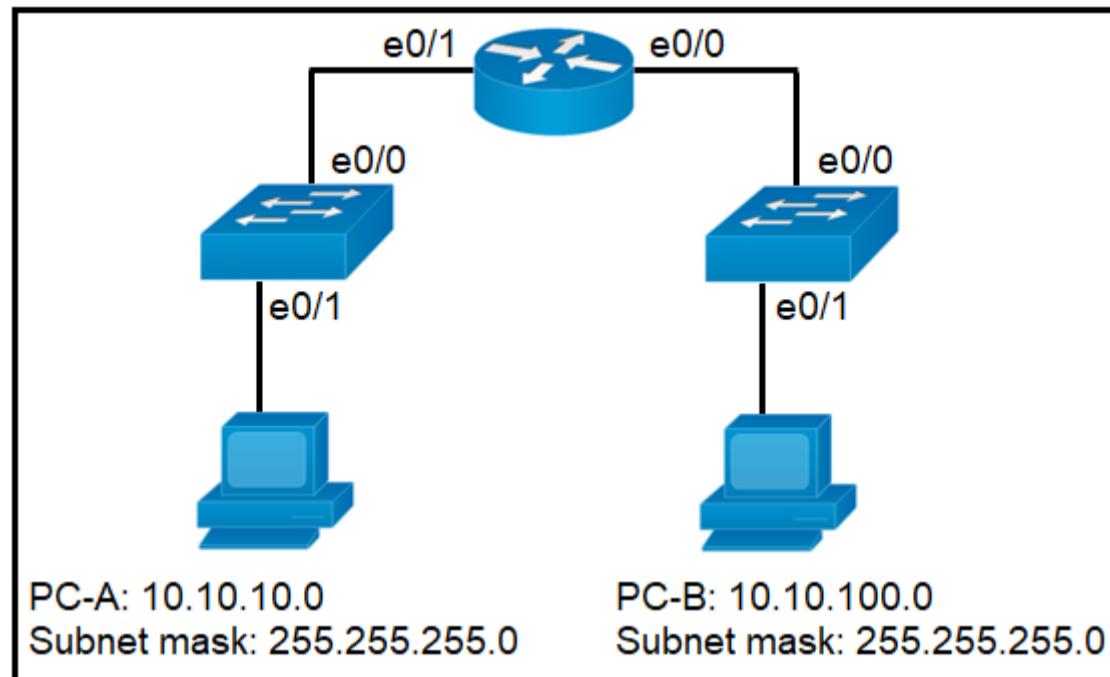
 **Manu_FR** Most Recent 1 day, 12 hours ago

Selected Answer: B
B is the correct answer.
upvoted 1 times

 **Yunus_Empire** 6 months, 1 week ago

B is correct
upvoted 4 times

Question #85



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, 4 months ago

the key point is "verifying the IP addresses," it is done by router .since the sw do things with MAC
upvoted 10 times

harkindeylee Most Recent 3 months, 1 week ago

Packet is received by the router. A is perfect
upvoted 2 times

country_rooted 1 year, 1 month ago

From the time the question asks to verify you already know the answer is A.
upvoted 2 times

ZUMY 1 year, 1 month ago

A is correct!
upvoted 3 times

richtorres333 1 year, 1 month ago

Selected Answer: A
The key word is "packet".
upvoted 3 times

Belinda 1 year, 4 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, 5 months ago

- A. T1
- B. E1
- C. E3
- D. T3

<https://www.ciscopress.com/articles/article.asp?p=2202411&seqNum=7>

upvoted 10 times

 **Vlad_Is_Love_ua** Most Recent 9 months, 1 week 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 ago

Why is this even tested if it is specific to the US?

upvoted 4 times

 **sasquatchshrimp** 10 months, 2 weeks 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

 **Smaritz** 1 year, 3 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

 **hassanhady** 1 year, 5 months ago

what is T1 means ?

upvoted 2 times

 **Yasin_Alsabah** 1 year, 4 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 5 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**  11 months, 2 weeks ago

B and D are correct.

UTP Cables CAT 5e:
Frequency: 100 MHz
Max. Bandwidth: 1 Gbps
Max. Distance: 100 m

UTP Cables CAT 6a:
Frequency: 500 MHz
Max. Bandwidth: 10 Gbps
Max. Distance: 100 m
upvoted 12 times

 **Smaritz**  1 year, 2 months ago

At least 1 Gbps is a bit misleading, they support at least 10 Mbps also.

upvoted 7 times

 **ricky1802**  4 months 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 3 times

 **RougePotatoe** 7 months, 2 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 1 times

 **iGlitch** 1 year, 1 month ago

B should be: Both support a maximum speed of 1 Gigabit.

upvoted 3 times

 **Bonesaw** 8 months, 2 weeks ago

The maximum speed on Cat6a is 10G, so that would be incorrect

upvoted 1 times

 **ZUMY** 1 year, 1 month 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** 6 months, 2 weeks ago

D is correct

upvoted 2 times

 **ZUMY** 1 year, 1 month ago

D is fine

upvoted 3 times

 **AvroMax** 1 year, 3 months ago

Selected Answer: D

D correct

upvoted 3 times

 **onikafei** 1 year, 4 months ago

D would be correct

Definitely 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 referring to shared resources on a network between workstations and not on cloud.

upvoted 2 times

 **onikafei** 1 year, 4 months ago

Correctme if im wrong :)

upvoted 2 times

Question #89

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

D (86%)	14%
---------	-----

✉️  **Dante_Dan** Highly Voted 1 year, 4 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, 3 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 8 times

✉️  **jose01210** 1 year ago

igual me pasa a mi

upvoted 1 times

✉️  **MDK94** Highly Voted 11 months, 1 week 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 11 times

✉️  **michael1001** 5 months, 3 weeks ago

Underrated

upvoted 1 times

✉️  **iMo7ed** Most Recent 3 months, 4 weeks ago

Selected Answer: D

It's D

upvoted 2 times

✉️  **splashy** 4 months, 3 weeks 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, 1 month 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

 **ZUMY** 1 year, 1 month 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, 1 month 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

 **BigCock** 1 year, 2 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, 3 months ago

Selected Answer: A

I'm going with A :)

upvoted 1 times

 **debut01** 1 year, 3 months ago

je pense que c'est la B

upvoted 1 times

 **Nicocisco** 1 year, 4 months ago

Selected Answer: A

C'est la A car la dataplane forward le trafic

upvoted 1 times

 **reagan_donald** 1 year, 4 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, 4 months ago

Selected Answer: D

Agree. RESPONDING to ICMP is in the data pane

upvoted 1 times

 **daanderud** 1 year, 4 months ago

I meant A!

upvoted 1 times

 **AndersonMr** 1 year, 4 months ago

Selected Answer: D

icmp is control plane

upvoted 1 times

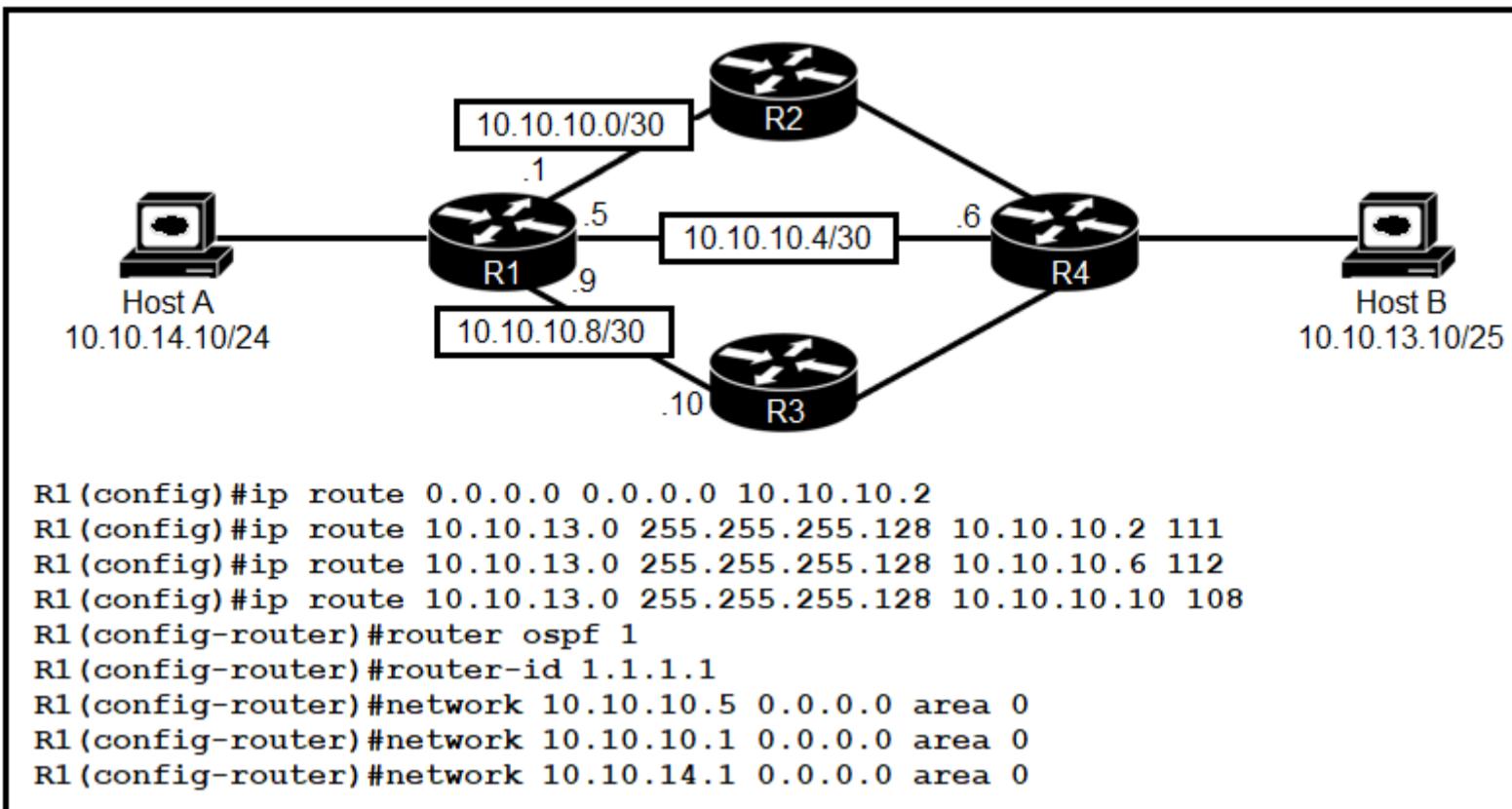
 **Kane002** 1 year, 4 months ago

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



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 (100%)

Jbcrggddfhh (Highly Voted) 1 year, 1 month 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 15 times

properchad (Most Recent) 3 weeks 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 1 times

Nutanix_Dummy 3 months, 2 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

freaknowledge123 4 months, 4 weeks 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 5 months ago

Choice B coz it has lowest AD and it is the most specific one

upvoted 1 times

BlkWatches 6 months, 1 week ago

Very tricky haha

upvoted 1 times

RougePotatoe 7 months, 2 weeks ago

Selected Answer: B

OSPF 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 10 months, 2 weeks 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 10 months, 3 weeks ago

Know your default routing protocol ADs!

upvoted 1 times

ZUMY 1 year ago

B is correct!

Router prefers static route over dynamic route

Router prefers Lowest AD

upvoted 1 times

timskis2 1 year ago

IT WILL USE THE DEFAULT / STATIC ROUTE 10.10.10.2 IT'S THE ONLY ONE ON THE DIAGRAM

upvoted 3 times

TA77 1 year 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 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

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 (100%)

 **mantest** Highly Voted 1 year, 1 month ago

C&D are correct ans..
upvoted 11 times

 **Anas_Ahmad** Highly Voted 6 months 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 6 times

 **Isuzu** Most Recent 1 month, 1 week 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 1 times

 **WOP_TO** 10 months, 1 week 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 3 times

 **saeed_huhu** 10 months, 3 weeks ago

Selected Answer: CD

C and D
Please correct it
upvoted 1 times

 **MDK94** 11 months, 1 week 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** 11 months, 1 week 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 ago

Going with C & D

upvoted 2 times

✉ **jossyda** 1 year 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 2 times

✉ **mytime** 1 year 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 ago

C&D are the answers. ICMP is part of control plane

upvoted 1 times

✉ **msomali** 1 year, 1 month 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, 1 month ago

Selected Answer: CD

ICMP is part of the control plane, therefor E is wrong.

upvoted 1 times

✉ **Scrvfvce** 1 year, 1 month ago

Selected Answer: CD

C&D should be the right answer

upvoted 3 times

✉ **gamer goddess123** 1 year, 1 month 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

 **Darrien1301** 1 year, 1 month ago

A & D are correct

Explanation: Actions 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 1 times

 **Darrien1301** 1 year, 1 month ago

Mein c&d sorry

upvoted 1 times

 **Darrien1301** 1 year, 1 month ago

Q.89 was the answer with the icmp wrong now its correct?

upvoted 4 times

 **ctoklu** 11 months, 1 week ago

I'd go with C and D indeed.

upvoted 1 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%)

 **everchosen13** Highly Voted 8 months, 1 week ago

I mean, essentially any portion of your network is a threat if it is compromised...
upvoted 12 times

 **Smaritz** Highly Voted 1 year ago

Strangely worded question and answer
upvoted 10 times

 **TA77** 1 year ago

Indeed
upvoted 1 times

 **Wes_60** Most Recent 2 months, 2 weeks ago

The most useless question so far
upvoted 4 times

 **GreatDane** 5 months, 1 week 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 4 times

 **Marcos9410** 11 months, 2 weeks 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 ago

Going with B
upvoted 1 times

 **jose01210** 1 year ago

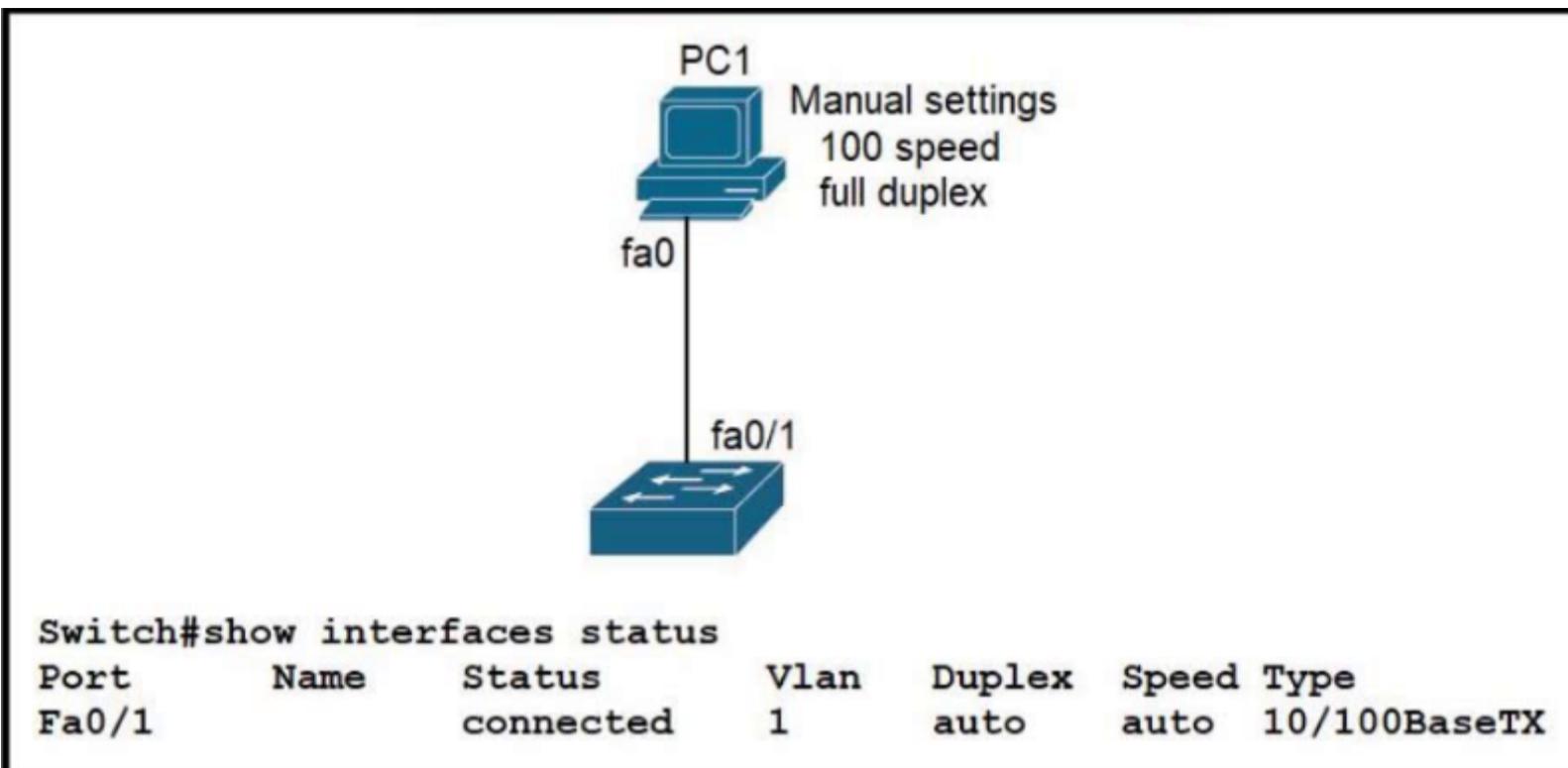
I think that is A
upvoted 2 times

 **CCAL** 1 year, 1 month 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, 1 month 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 13 times

GreatDane Most Recent 5 months, 1 week 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 10 months, 3 weeks 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 3 times

 **ZUMY** 1 year 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

 **hp2wx** 10 months, 3 weeks 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 ago

A is correct!

upvoted 2 times

 **erikkkkkka** 1 year 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

 **Jbcrggddfh** 1 year, 1 month 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

Question #95

DRAG DROP -

Drag and drop the TCP or UDP details from the left onto their corresponding protocols on the right.

Select and Place:

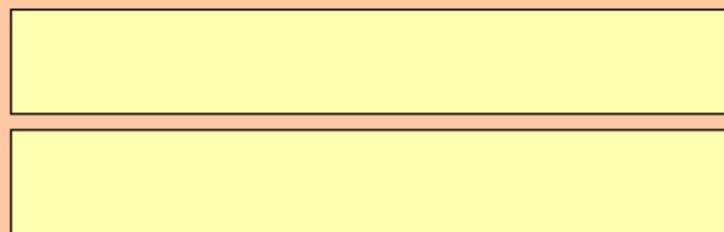
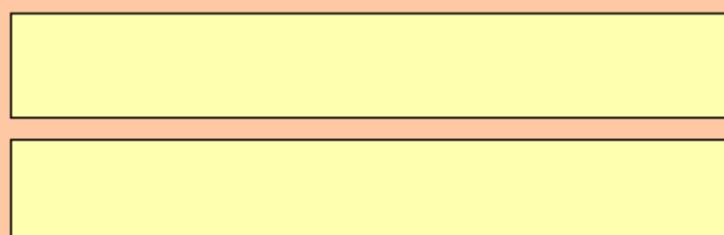
Answer Area

transmitted based on data contained in the packet without the need for a data channel

requires the client and the server to establish a connection before sending the packet

provides best-effort service

supports reliable data transmission

TCP**UDP****Correct Answer:****Answer Area**

transmitted based on data contained in the packet without the need for a data channel

requires the client and the server to establish a connection before sending the packet

provides best-effort service

supports reliable data transmission

TCP

requires the client and the server to establish a connection before sending the packet

supports reliable data transmission

UDP

transmitted based on data contained in the packet without the need for a data channel

provides best-effort service

  **Manu_FR** 1 day, 11 hours ago

The answer is correct

upvoted 1 times

  **yousfs1212** 2 months, 2 weeks ago

The question is simple and the answer is correct

upvoted 2 times

  **NetStef** 5 months, 3 weeks ago

Answer is correct

upvoted 4 times

Question #96

DRAG DROP -

Drag and drop the IPv6 addresses from the left onto the corresponding address types on the right.

Select and Place:

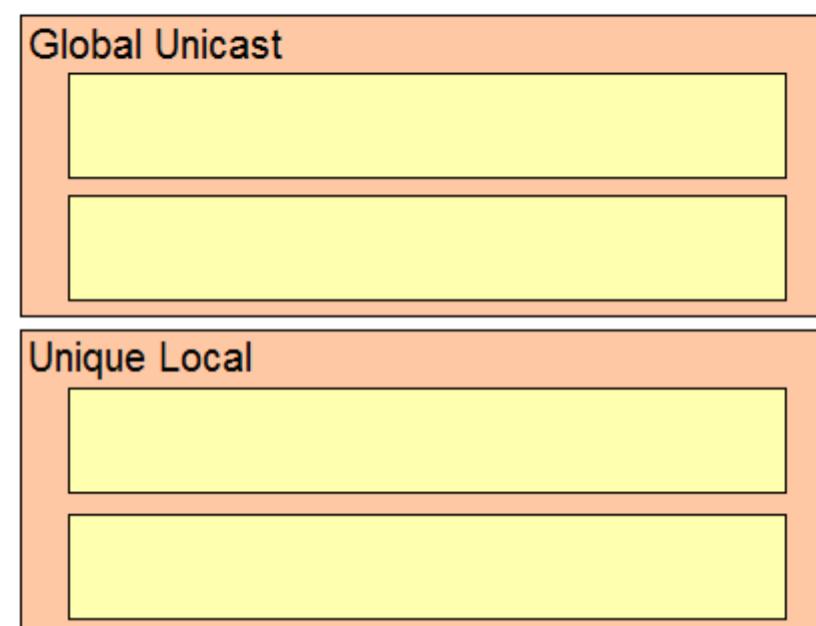
Answer Area

2001:db8:600d:cafe::123

fcba:926a:e8e:7a25:b1:c6d2:1a76:8fdc

fd6d:c83b:5cef:b6b2::1

3ffe:e54d:620:a87a::f00d

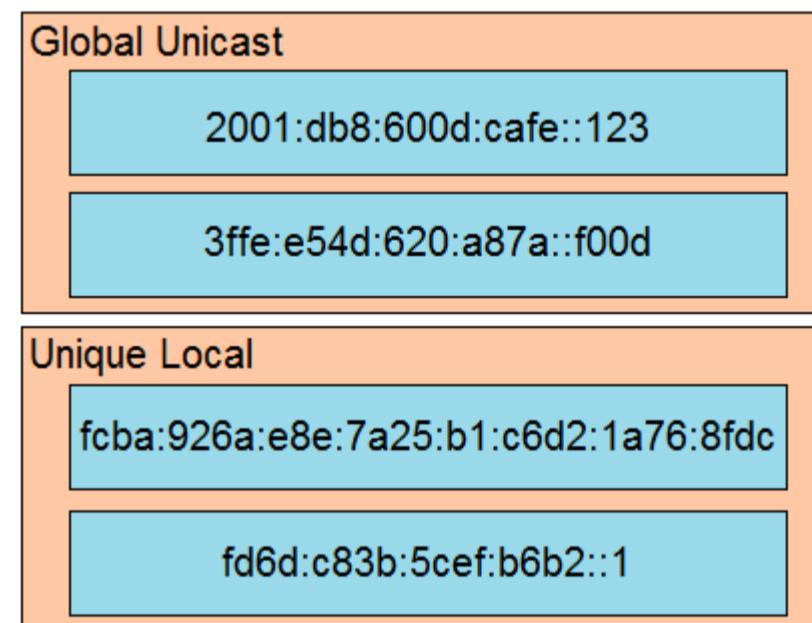
**Correct Answer:****Answer Area**

2001:db8:600d:cafe::123

fcba:926a:e8e:7a25:b1:c6d2:1a76:8fdc

fd6d:c83b:5cef:b6b2::1

3ffe:e54d:620:a87a::f00d



Reference:

<https://learningnetwork.cisco.com/s/question/0D53i00000Kt6kl/ipv6-unique-local-addresses>

netzwork Highly Voted 8 months, 1 week 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 11 times

NetStef Most Recent 5 months, 3 weeks 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 ago

A is correct

upvoted 2 times

 **Jbcrggddfh** 1 year 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%)

  **Eyad_Alotaibi** 5 months, 3 weeks ago**Selected Answer: D**

Correct answer is D

upvoted 3 times

  **Yunus_Empire** 6 months, 1 week ago**Selected Answer: D**

Correct D

upvoted 4 times

  **MisterK_77** 9 months, 1 week ago**Selected Answer: D**

DDDDDDDD

upvoted 3 times

  **[Removed]** 10 months 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** 10 months 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** 10 months, 1 week ago**Selected Answer: D**

DDDDDDDD

upvoted 3 times

  **coralreef** 10 months, 2 weeks 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** 10 months, 3 weeks 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** 10 months, 3 weeks ago**Selected Answer: D**

It's 2200. D

upvoted 1 times

  **ratu68** 11 months, 1 week ago**Selected Answer: D**

D 100% sure !

upvoted 4 times

 **SH_** 11 months, 1 week ago

Selected Answer: D

D because 2200 cannot be shortened to 22

upvoted 3 times

 **MDK94** 11 months, 1 week ago

D is 100% correct, no way its wrong

upvoted 1 times

 **battery1979** 11 months, 2 weeks ago

A would be correct if the fourth octet was 0022.

upvoted 2 times

 **Patrick69** 11 months, 2 weeks ago

Selected Answer: D

D only!

upvoted 3 times

 **Marcos9410** 11 months, 2 weeks ago

Selected Answer: D

D is the correct answer.

Only LEADING 0s can be removed (compressed)

upvoted 2 times

 **ctoklu** 11 months, 3 weeks ago

D is correct for 100% sure

upvoted 1 times

 **thazmalt** 12 months ago

Selected Answer: D

2200 is different to 22

upvoted 2 times

Question #99

Topic 1

DRAG DROP -

Drag and drop the IPv6 addresses from the left onto the corresponding address types on the right.

Select and Place:

fe80::a00:27ff:feeb:89aa	Global Unicast
3ffe:e54d:620:a87a::f00d	Link-Local Unicast
ff05::1:3	Multicast
2001:db8:600d:cafe::123	

Correct Answer:	3ffe:e54d:620:a87a::f00d	Global Unicast
	fe80::a00:27ff:feeb:89aa	
	2001:db8:600d:cafe::123	
	ff05::1:3	Link-Local Unicast
	fe80::a00:27ff:feeb:89aa	
	2001:db8:600d:cafe::123	Multicast
	ff05::1:3	

 **Danielki** 2 months 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** 5 months, 3 weeks ago

Answer is correct

upvoted 3 times

 **DoBronx** 7 months, 2 weeks ago

I'm just going to assume Link Local starts with FE cuz of SNEAKEEE 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 5 months, 1 week 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.

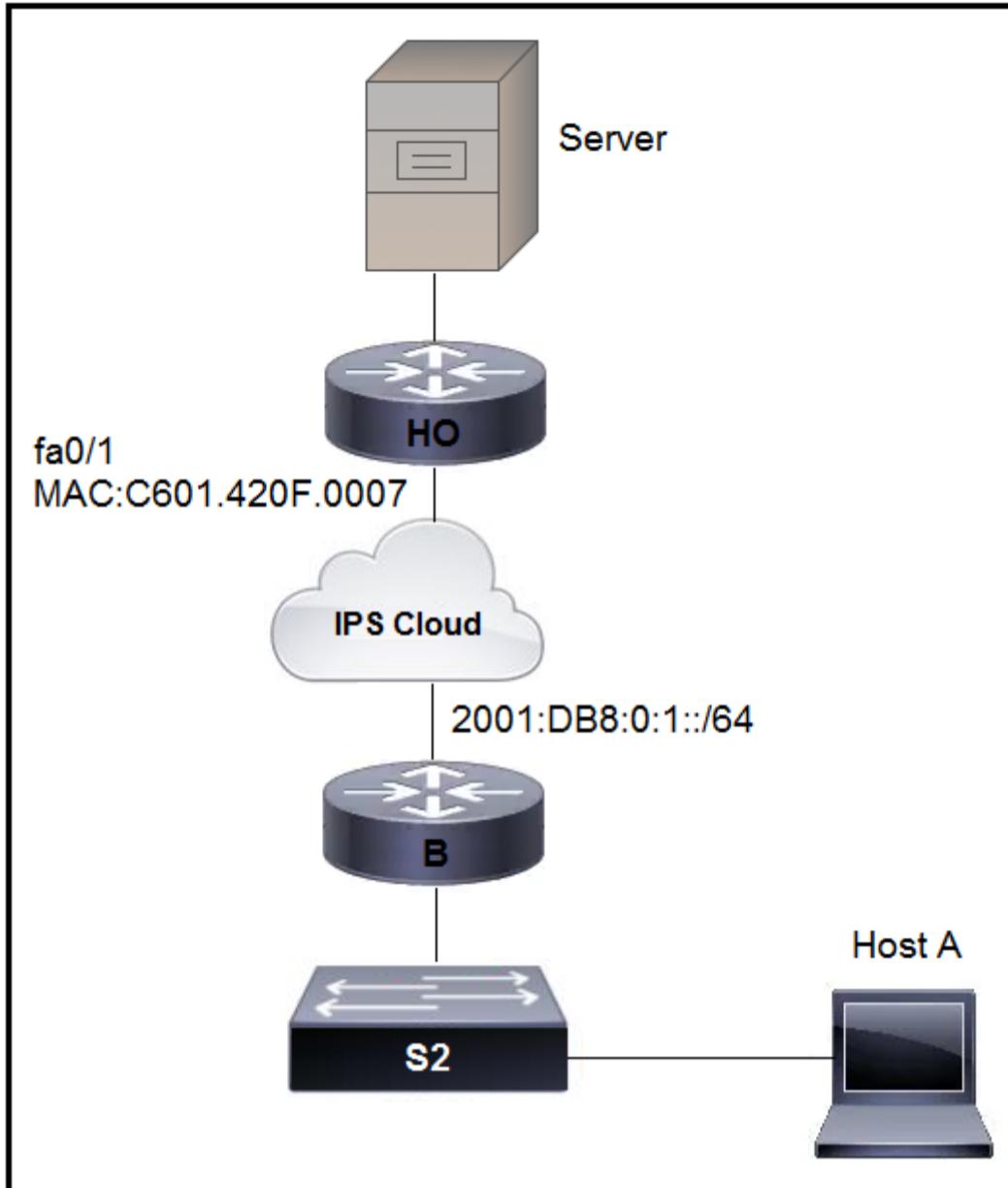
upvoted 6 times

 **ridhoc** Highly Voted 7 months ago

It's obviously D!!

upvoted 5 times

Question #101



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 7 months 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 15 times

Equiano Highly Voted 8 months, 2 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 7 times

Loq Most Recent 3 weeks, 5 days ago

Letter C should be the closest answer. The eui-64 process was not followed though.

upvoted 1 times

Vikramaditya_J 3 weeks, 6 days 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 3 times

HSong 1 month, 2 weeks ago

Selected Answer: C

The correct answer is C

upvoted 1 times

JBORBON 1 month, 3 weeks ago

C is correct

upvoted 1 times

dearc 2 months, 1 week ago

Selected Answer: C

LETTER C IS THE CORRECT ANSWER

upvoted 1 times

elixirwell 2 months, 1 week 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 4 months, 2 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 4 times

uditpatel1 1 month, 2 weeks ago

Yes, you are right but if the we invert 7th bit then 6 = 0110 so no 0100 = 4

So, thechnicly as per my suggestion there is no option to C4 like answers.

upvoted 1 times

ProgSnob 5 months 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 5 months ago

seems to me someone forgot to invert the 7 bit, there is no other explanation

upvoted 1 times

SemStrond 7 months ago

Why can't it be all of them??

upvoted 1 times

Garfieldcat 7 months, 2 weeks ago

why interface ID comes a link local ? it should be C

upvoted 1 times

Sam7007 8 months ago

Selected Answer: B

B is correct answer

upvoted 2 times

j6 8 months, 1 week ago

Selected Answer: C

CCCCCCCC

upvoted 2 times

✉ **splashy** 8 months, 2 weeks ago

Selected Answer: B

D = I want to do eui 64 manually because I'm an Awesome Cisco Engineer,
but i didn't get my ice-cream so i forgot to flip the 7th bit = wrong or "more wrong" then

B = Is it forbidden or wrong to use FE80 + mac address in the Interface ID section? Nope
Is it a good practice? Nope
Does anybody seem to care? Nope

B is right

upvoted 2 times

✉ **Dontguess** 7 months, 2 weeks ago

But using same logic, also answer A would be correct ?

upvoted 3 times

✉ **Bonesaw** 8 months, 2 weeks ago

C is the wrong answer because the 7th bit is not inverted, should be 2001:DB8:0:1:C401:42FF:FE0F:7/64 which isn't even an option
upvoted 4 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 4 months 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 5 times

✉ **Fermento** Most Recent 8 months ago

Selected Answer: A

A is fine.
upvoted 3 times

Question #103

```
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%)

 **Da_Costa** 1 month, 1 week ago

DNS server resolves addresses such as www.cisco.com
upvoted 3 times

 **Ka_09** 3 months, 3 weeks ago

the given answer was wrong the correct option is DHCP server ip
upvoted 1 times

 **Fermento** 8 months ago

Selected Answer: A

Send for DNS serve, because url should be translate to IP address.
upvoted 3 times

 **j6** 8 months, 1 week ago

Selected Answer: A

A correct - web address uses DNS server
upvoted 3 times

✉  **goms12** 9 months 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**  8 months, 2 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**  2 months, 1 week 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 4 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 4 months 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 7 times

 **sol_ls95** Most Recent 4 months, 3 weeks ago

why not multicast?

upvoted 1 times

 **mrgreat** 9 months 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** 7 months, 1 week ago

in the same network? examples in books are a server in New york and a server in San Francisco

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** 3 months, 4 weeks ago

Selected Answer: C

C is correct

upvoted 3 times

 **Request7108** 5 months, 2 weeks 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** 4 months 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 (100%)

 **Wwnz4** Highly Voted 8 months, 1 week ago

Terribly written answer for C

upvoted 9 times

 **hamish88** Most Recent 1 month, 4 weeks 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 2 times

 **j6** 8 months, 1 week ago

Selected Answer: C

end point AKA host - written okay imo

upvoted 2 times

 **j6** 8 months, 1 week 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** 2 months, 1 week 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 2 times

 **[Removed]** 8 months 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** 7 months, 2 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** 3 months ago

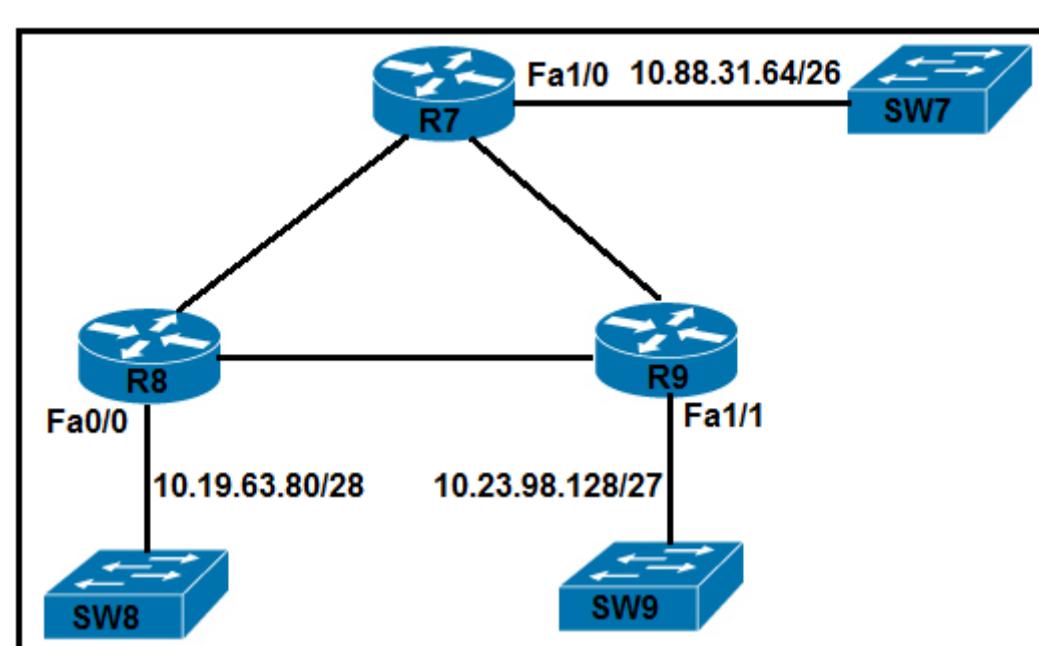
it also confused me, this is a very tricky question if you don't read it at least twice.

upvoted 1 times

 **RougePotatoe** 7 months, 2 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



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 (82%)

B (18%)

Customexit Highly Voted 7 months, 2 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 10 times

Bhrino Most Recent 3 weeks, 6 days 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 3 weeks, 6 days 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 1 month 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 1 times

 **iMo7ed** 3 months, 4 weeks ago

Selected Answer: D

it's D

upvoted 3 times

 **Tropicalsohot** 4 months, 3 weeks ago

Selected Answer: D

Subnet Mask of R7 is /26 thus 255.255.255.192

upvoted 1 times

 **binrayelias** 4 months, 3 weeks ago

I agree that D is the right answer

upvoted 1 times

 **joyboy92** 4 months, 3 weeks ago

Selected Answer: D

it's D

the subnet of first address in B is Wrong

upvoted 2 times

 **flash93933** 4 months, 4 weeks ago

Selected Answer: D

Its D

the subnet masks in B are incorrect

upvoted 1 times

 **shubhambala** 8 months, 4 weeks ago

Selected Answer: B

The right answer is B. As for R9 the last usable address should be .158.

upvoted 2 times

 **EliasM** 8 months, 2 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** 8 months ago

But why it has to be 224 and not 248 ?

upvoted 1 times

 **Customexit** 7 months, 2 weeks ago

Because a /27 is .224

A .248 would be /29. R9 is not /29.

upvoted 2 times

 **rick0813** 7 months, 2 weeks ago

because if 248 then it will be /29.

upvoted 2 times

 **guynetwork** 8 months, 4 weeks 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

 **Prometheus_72** 1 month, 2 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** 1 month, 1 week ago

Agree with B
upvoted 1 times

 **dearc** 2 months, 1 week 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** 7 months, 2 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** 9 months ago

D is correct
<https://www.metageek.com/training/resources/why-channels-1-6-11/>

upvoted 3 times

✉️  **Eagleswing** 9 months ago

Answer D
<https://community.cisco.com/t5/wireless/overlapping-v-s-non-overlapping-channels/td-p/601900>

upvoted 2 times

Question #113

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 (96%)	4%
---------	----

 **mrgreat**  9 months 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 12 times

 **splashy**  7 months, 4 weeks 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 7 times

 **Friday_Night**  3 weeks, 2 days ago

So if this comes up in the Cisco exam, they will consider C as the correct answer?
 upvoted 1 times

 **TR3Y** 3 weeks, 5 days 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** 1 month, 1 week 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** 1 month, 2 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** 1 month, 2 weeks ago

The answer is C??? How come.
 upvoted 1 times

 **thomson_johnson** 2 months, 3 weeks 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

harkindeyee 3 months, 1 week ago

The answer should be unique local

upvoted 2 times

Cue_The_Joy 3 months, 1 week 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 1 times

Yaqub009 4 months 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

Sacuxipo 4 months ago

B: Unique local that works as private IPv4

upvoted 1 times

thatoneguy1234 4 months, 2 weeks ago

Selected Answer: B

Unique local is equivalent to 1918 IPv4 space and only reachable internal.

upvoted 1 times

MSTAHIR 4 months, 2 weeks ago

C is correct Answer

upvoted 1 times

stargate121 4 months, 2 weeks ago

Selected Answer: B

Correct answer is B.

Unique Local are non routable addresses that can be used internally only .

upvoted 1 times

DB_Cooper 4 months, 3 weeks ago

Selected Answer: B

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.

upvoted 1 times

Mister_K 5 months, 2 weeks ago

Link-local addresses may appear as the source or destination of an IPv6 packet.

Routers must not forward IPv6 packets if the source or destination contains a linklocal address.

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** 1 month, 1 week 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** 1 month, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

 **freaknowledge123** 5 months ago

can a guru explain the answer?

upvoted 1 times

 **laurvy36** 5 months ago

you have 1, 6 and 11 as channels, as nonoverlapping ones, not 123 or 456 etc

upvoted 1 times

 **laurvy36** 5 months ago

those channels are discontinuous

upvoted 1 times

Question #115

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 (81%)

D (19%)

 **cyborg7** Highly Voted 8 months ago

D is incorrect as it contains :: which replaced with 0000.0000 will make the address longer than 128bits
 Correct is B
 upvoted 10 times

 **Sacuxipo** 4 months 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's missing the 4th hextet. Guess where it must be?
 D is correct man.
 upvoted 2 times

 **FALARASTA** 1 month, 2 weeks ago

From slide notes

A double colon (:) can replace any single, contiguous string of one or more 16-bit hexets consisting of all zeros.
 Example:
 2001:db8:cafe:1:0:0:1 (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 1 times

 **FALARASTA** 1 month, 2 weeks ago

You should refer the use of :: it means a whole hextet but all are zeros
 upvoted 1 times

 **Dutch012** 3 months, 2 weeks 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** 1 month, 3 weeks 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

 **BI1024** Highly Voted 7 months, 3 weeks ago

Selected Answer: B

D is wrong address is too long
 upvoted 7 times

 **HM01** Most Recent 2 days, 16 hours 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 1 times

 **LexKin** 2 weeks, 1 day 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** 3 weeks, 2 days 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** 1 month, 3 weeks 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 sige or multi 0000 values.
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** 2 months, 1 week 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** 3 months, 1 week ago

Selected Answer: B

D is wrong address is too long
upvoted 1 times

 **Cue_The_Joy** 3 months, 1 week 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 (::) can replace any single, contiguous string of one or more 16-bit hexets consisting of all zeros. Therefore, D would not be too long.
upvoted 6 times

 **TR3Y** 3 weeks, 5 days ago

Exactly I cant argue with the facts here. There is also no rule stating that the "::" must be used at the first 16BitHex. It 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** 4 months, 3 weeks ago

B is the correct one
upvoted 2 times

 **freeknowledge123** 4 months, 4 weeks ago

Selected Answer: D

i think FC is reserved FD is correct.
upvoted 1 times

 **ProgSnob** 5 months 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** 6 months 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 sige 0. D should be abbreviated as fc00:0:aaaa:0:a15d:1234:2343:8aca/64

upvoted 5 times

 **usamahrakib001** 7 months, 2 weeks ago

B and D both are correct

upvoted 1 times

 **Garfieldcat** 7 months, 2 weeks ago

Indeed, this is controversial: someone says range beginning with prefix FC00::/7 but others (at least my teacher) say FD00::/8. I saw cisco books use FC.

upvoted 2 times

 **molly_zheng** 1 month, 3 weeks ago

fc00::/7 - fdff::/7

upvoted 1 times

 **WASBAS** 5 months, 3 weeks ago

FD00 and FC00 work for unique local

upvoted 2 times

 **Binks14** 7 months, 3 weeks ago

B should be the answer since the 8th bit is flipped ...

upvoted 1 times

 **mohdhafizuddinesa** 7 months, 3 weeks ago

Selected Answer: B

FD is the answer

upvoted 3 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 (97%)

✉  DixieNormus  9 months 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 11 times

✉  Rami1996  1 week, 1 day ago

IT'S B & E

upvoted 1 times

✉  MonsieurP 2 weeks, 6 days ago

An SSID is not an identifier of an Access Point. You can configure more than one SSID on an Access Point.
upvoted 2 times

✉  Isuzu 1 month, 1 week 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 1 month, 1 week ago

Selected Answer: BE

I also agree with BE. But why correct answer from Cisco is CD? really do not understand.
upvoted 2 times

✉  Manu_FR 1 day, 7 hours ago

From Cisco?

upvoted 1 times

✉  MohammedRafiq 1 month, 1 week ago

B is incorrect, "SSID is not most 32 characters long, maximum 32 characters "
upvoted 1 times

✉  thomson_johnson 2 months, 3 weeks 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 4 months, 1 week 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** 4 months, 2 weeks ago

For me it's agree B and E.
upvoted 1 times

 **hasbulla01** 6 months, 4 weeks ago

SSID it's only for identification... not have security for default
upvoted 2 times

 **Garfieldcat** 7 months, 2 weeks ago

yeah, I agree BE
upvoted 3 times

 **rick0813** 7 months, 2 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

That's a horrible to explain it C is what the BSSID (MAC address) suppose to do.

upvoted 1 times

 **Sam7007** 8 months ago

Selected Answer: BE
B and E
upvoted 2 times

 **Donut86** 8 months ago

Selected Answer: BE
B and E
upvoted 2 times

 **everchosen13** 8 months, 1 week ago

Selected Answer: BE
An SSID is not secured by default...
upvoted 2 times

 **netzwork** 8 months, 1 week ago

Selected Answer: BC
B and C.

SSID can be at most 32 characters long and is the name given to the access point
upvoted 1 times

 **RougePotatoe** 7 months, 2 weeks ago

C is not best answer because SSID is not used to identify an access point. You use BSSID (the mac address) to identify a specific access point.
upvoted 1 times

 **shubhambala** 8 months, 3 weeks ago

Selected Answer: BE
its BE bois (why? TRUST ME)
upvoted 4 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

 **Firewall2022** 8 months, 2 weeks ago

The answer is C, "a frame for a known destination MAC address"
upvoted 3 times

 **Cracked76** 9 months ago

C it is
upvoted 2 times

 **Cracked76** 9 months ago

A must be
upvoted 1 times

 **j6** 8 months, 1 week ago

question says "known" not "unknown" so answer is C
if was "unknown" would be A
upvoted 1 times

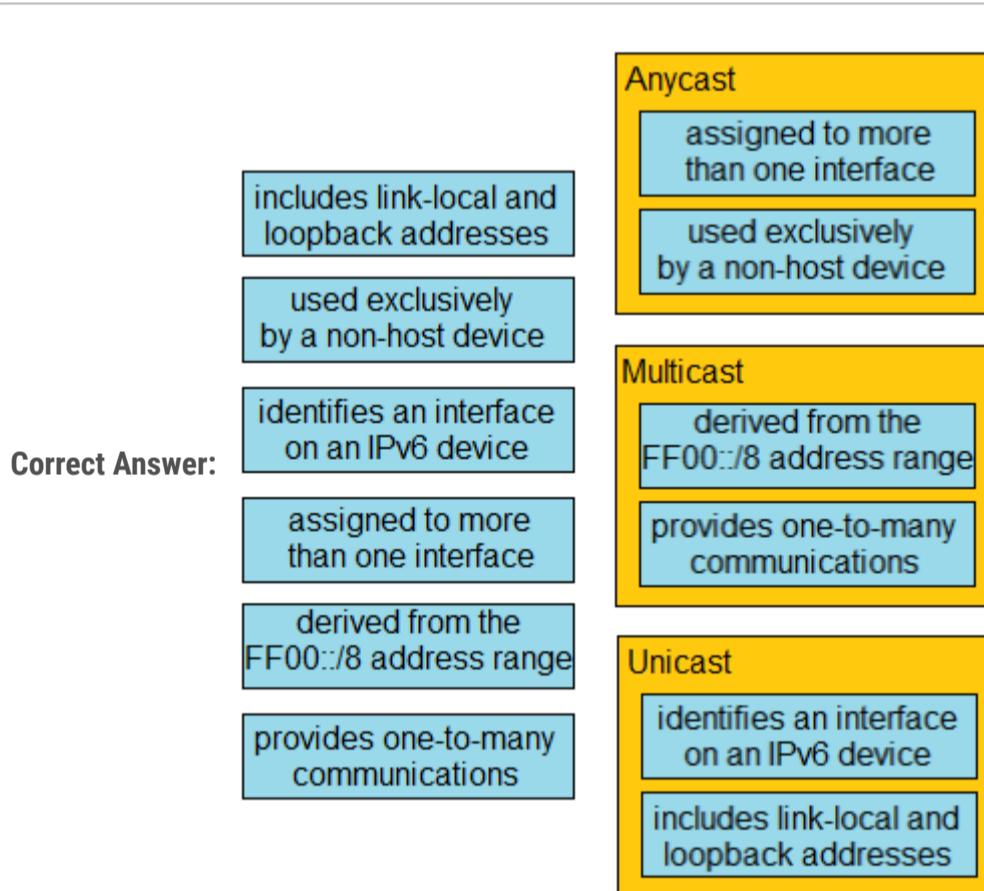
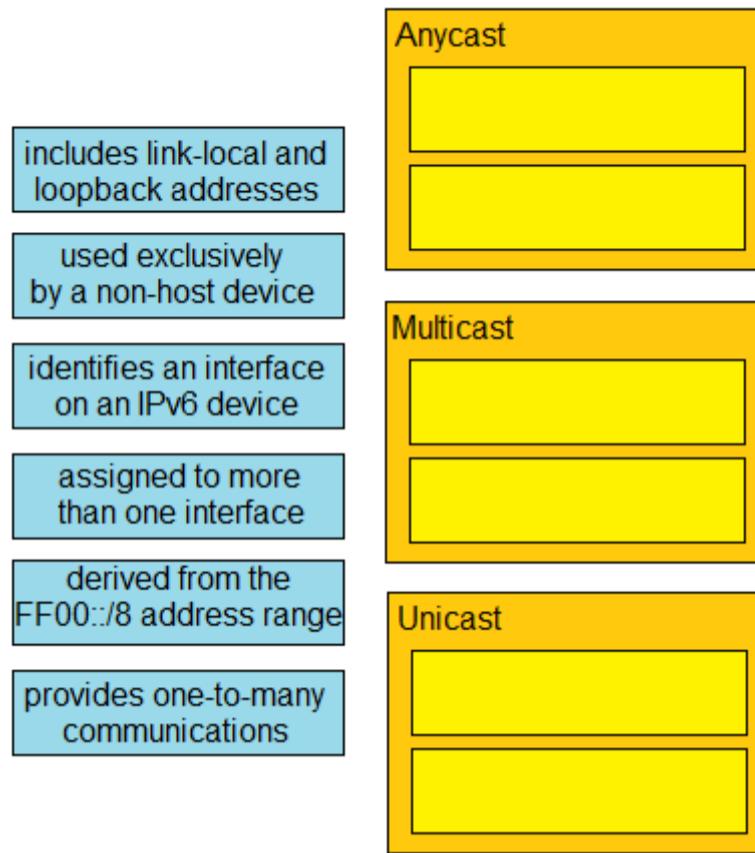
Question #118

Topic 1

DRAG DROP -

Drag and drop the IPv6 address details from the left onto the corresponding types on the right.

Select and Place:



Danny7 4 months, 1 week ago

Can link-local be considered as Uni cast?

upvoted 2 times

cuenca73 4 months, 1 week ago

Actually a link-local address is a type of unicast address

upvoted 4 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 9 months ago

Answer A Correct

https://www.juniper.net/documentation/en_US/release-independent/nce/topics/concept/nce-182-evpn-collapsed-core-evpn-multipointing-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 8 months ago

<https://study-ccna.com/collapsed-core-and-three-tier-architectures/>

upvoted 3 times

 **Vlad_Is_Love_ua** 9 months 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 9 months 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 4 months 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 2 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** 1 month, 3 weeks ago

Selected Answer: A

A its the way, in the SDN architecture the control plane and data plane are decouple.
upvoted 2 times

 **dearc** 2 months, 1 week 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** 5 months, 2 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** 7 months, 1 week ago

Does anyone know what disaggregation means? Its not in the OCCG.

upvoted 2 times

 **GhostWolf** 7 months 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 9 months 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 3 months, 2 weeks ago

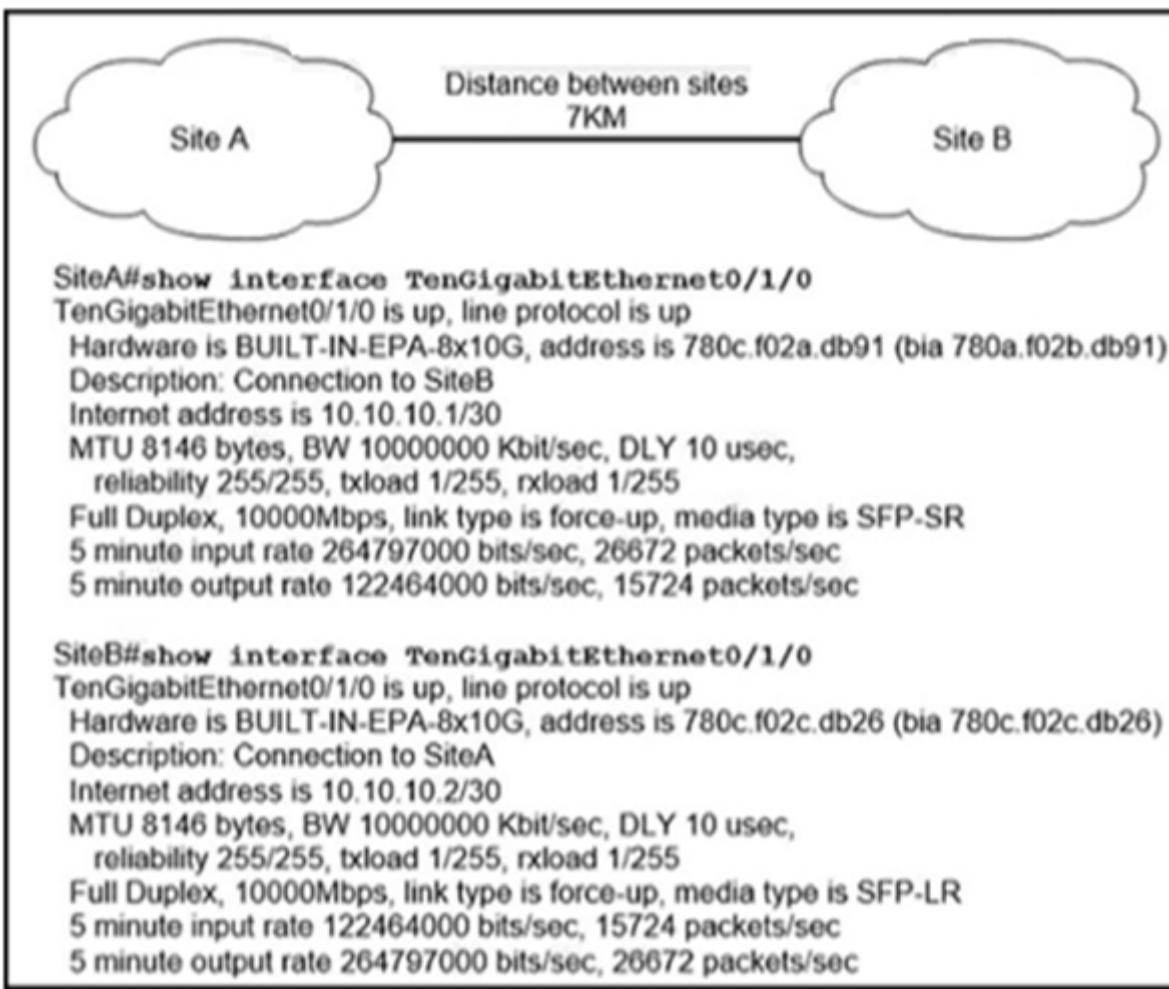
Selected Answer: D

The web server uses HTTP/HTTPS

upvoted 4 times

Question #123

Topic 1



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**  8 months, 3 weeks 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 26 times

✉  **Bonesaw** 8 months ago

I'm back after taking my test and passing and would you believe this was question 101 of 101. Keep studying everyone

upvoted 41 times

✉  **Manu_FR** 1 day, 7 hours 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 1 times

✉  **NICE_ANSWERS** 1 week, 4 days ago

Please how many questions are there on the standard exam?

upvoted 1 times

✉  **Manu_FR** 1 day, 7 hours ago

Approximately 100 from what i've heard. Can be 94,97,101 but yes, about100.

upvoted 1 times

✉  **Wes_60** 2 months, 2 weeks ago

Thanks for the feed back. My exam in less than 2 weeks. This gives me more confidence.

upvoted 2 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  9 months 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  9 months 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  9 months 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 8 months, 1 week 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 6 times

 **Yunus_Empire** 6 months, 1 week 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 1 month, 3 weeks ago

Selected Answer: D

The 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 2 times

 **ike110** 5 months ago

Should it be "segments" and not "packets"?
upvoted 2 times

 **peplegal** 1 month, 3 weeks 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  9 months 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 45 times

✉  DoBronx 7 months, 2 weeks ago

w comment.

upvoted 3 times

✉  Yunus_Empire  6 months, 1 week ago

Selected Answer: AE

These are correct

upvoted 5 times

✉  dropspablo  1 month, 1 week 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 1 month 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

✉  beerbiseps1 2 months 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** 1 month, 3 weeks 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 1 times

 **elixirwell** 2 months, 1 week 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** 7 months ago

Selected Answer: AE

C is wrong because its not only used in SDN ,

upvoted 2 times

 **RougePotatoe** 7 months, 2 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** 8 months, 1 week ago

Selected Answer: AE

An SSID can be supported by MULTIPLE access points

upvoted 4 times

 **netzwork** 8 months, 1 week 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 (75%)

AE (25%)

✉ **Hope_12** 1 month 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 1 times

✉ **Isuzu** 1 month, 1 week 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** 3 months, 1 week 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** 3 months, 2 weeks ago

Selected Answer: BD

A & E for the distribution layer
upvoted 1 times

✉ **hoisin** 3 months, 3 weeks ago

Now, which one is the correct answer BD or AE because Community vote distribution BD (60%) and AE (40%).
upvoted 2 times

✉ **Christopherjd20** 4 months, 1 week 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** 4 months, 3 weeks 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 closest to users
upvoted 3 times

✉  **freeknowledge123** 4 months, 3 weeks ago

Selected Answer: AE

AE seems correct and self explanatory
upvoted 1 times

✉  **DPAD** 5 months, 3 weeks ago

is A and E correct?
upvoted 1 times

✉  **binrayelias** 4 months, 3 weeks ago

B and D is correct for access layer while A and E is for distribution layer.
upvoted 2 times

✉  **Yunus_Empire** 6 months, 1 week 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** 6 months, 1 week 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** 7 months, 2 weeks ago

Selected Answer: AE
A and E are both 'characteristics' that describe the access layer and also are correct.

upvoted 1 times

✉  **RougePotatoe** 7 months, 2 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** 7 months, 2 weeks ago

That sounds like Distribution Layer.
upvoted 6 times

Question #128

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 (59%)

A (38%)

 **BATSIE** Highly Voted 5 months 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; if no value is specified, the maximum is allowed.

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 6 times

 **mrgreat** Highly Voted 9 months 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 6 times

 **JY888** Most Recent 1 week, 6 days 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** 3 weeks, 4 days 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 1 times

 **Isuzu** 1 month ago

Selected Answer: A

The PoE mode that enables powered-devices detection and guarantees power when the device detected is "auto" mode. In "auto" mode, the Power Sourcing Equipment (PSE) detects the powered device (PD) before providing power, and then delivers the appropriate power level to the PD. If the PD is not detected, or if it is not compatible with the PSE, no power is supplied. This ensures that only compatible devices receive power, and that the appropriate power level is delivered to them.

upvoted 2 times

 **dropspablo** 1 month, 1 week ago

Selected Answer: A

Answer A, because there are three configuration modes in PoE, Static, Auto and Dynamic.

The three modes CAN guarantee the power. But only Auto and Dynamic modes DETECT the device (along with the required power). And the Dynamic mode, in addition to guaranteeing energy, detecting the device, it also NEGOTIATES energy, because if the switch has less watts to supply, it can partially feed the device.

As it was only asked in the question to GUARANTEE the energy and DETECT the device, the Auto mode already answers (Answer A). If it asked to also "negotiate", it would have to be Dynamic mode. Static mode is wrong as it cannot detect the device, it just guarantees power. And Active mode does not exist in the configuration.

upvoted 2 times

 **dropspablo** 1 month, 1 week ago

Example:

```
Switch(config-if)# power inline static max 15400
```

```
Switch(config-if)# power inline auto max 15400
```

```
Switch(config-if)# power inline dynamic max 30000
```

The MAX keyword defines the maximum amount of power that can be supplied to the device. In these examples, we have the maximum power 15400 as 15.4 watts and 30000 as 30 watts.

Some switches may use a different keyword for dynamic mode, such as "auto-max".

upvoted 1 times

 **country_rooted** 1 month, 2 weeks ago

STATIC guarantees power when the device is connected
AUTO will only provide power if it is available

Ans=B

upvoted 1 times

 **DL86** 4 months, 3 weeks ago

Selected Answer: B
B, keyword is guarantees power. Auto does not guarantees, static does.

upvoted 3 times

 **enehana_777** 5 months ago

auto mode —The switch automatically detects if the connected device requires power. If the switch discovers a powered device connected to the port and if the switch has enough power, it grants power, updates the power budget, turns on power to the port on a first-come, first-served basis, and updates the LEDs. For LED information, see the hardware installation guide. If the switch has enough power for all the powered devices, they all come up. If enough power is available for all powered devices connected to the switch, power is turned on to all devices.

upvoted 3 times

 **enehana_777** 5 months ago

Auto mode

upvoted 2 times

 **NikkiaNao** 5 months, 1 week ago

Selected Answer: A
answer is A.

upvoted 3 times

 **tonye100** 6 months ago

Selected Answer: D
Active PoE, short for active Power over Ethernet, is also known as standard PoE which refers to any type of PoE that negotiates the proper voltage between the power supply equipment (PSE) and the PD device.

upvoted 1 times

 **tonye100** 6 months ago

sorry i am wrong, correct answer is A
upvoted 3 times

 **Yunus_Empire** 6 months, 1 week ago

Selected Answer: B
Static
upvoted 1 times

 **arenjenkins** 7 months ago

Selected Answer: A
static : The device pre-allocates power to the port (even when no powered device is connected)
upvoted 1 times

 **khaledsh00** 7 months, 1 week ago

Selected Answer: B
static
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 4 times

 **RougePotatoe** 7 months, 2 weeks ago

Selected Answer: B
Static reserves power and guarantees its availability when it detects a device that requires PoE is connected. Auto does NOT guarantee the availability of power. Auto is first come first serve static is pre-allocated.

"Because power is pre-allocated, 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 device powers the port only if it discovers a powered device. Use the static setting on a high-priority interface."

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/switches/lan/catalyst9200/software/release/16-12/configuration_guide/int_hw/b_1612_int_and_hw_9200_cg/configuring_poe.html.xml#id_114542

upvoted 4 times

 **dendentester** 8 months, 2 weeks ago

auto - Enables powered-device detection; if enough power is available, automatically allocates power to the PoE port after device detection (default setting).

upvoted 1 times

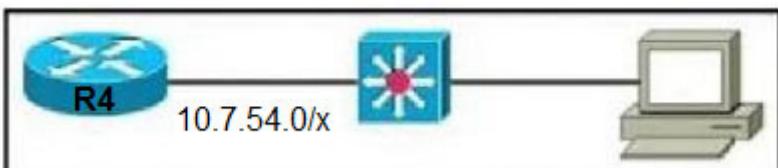
 **dendentester** 8 months, 2 weeks ago

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 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
- 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
- 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
- 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

Correct Answer: D

✉ **Customexit** Highly Voted 7 months, 2 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 8 times

✉ **Goh0503** Highly Voted 8 months, 1 week 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 6 times

✉ **Freddy01** 6 months, 3 weeks 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 3 times

✉ **harkindeylee** Most Recent 3 months ago

D IS CORRECT
upvoted 1 times

✉ **netzwork** 8 months, 1 week ago

D is right.
upvoted 2 times

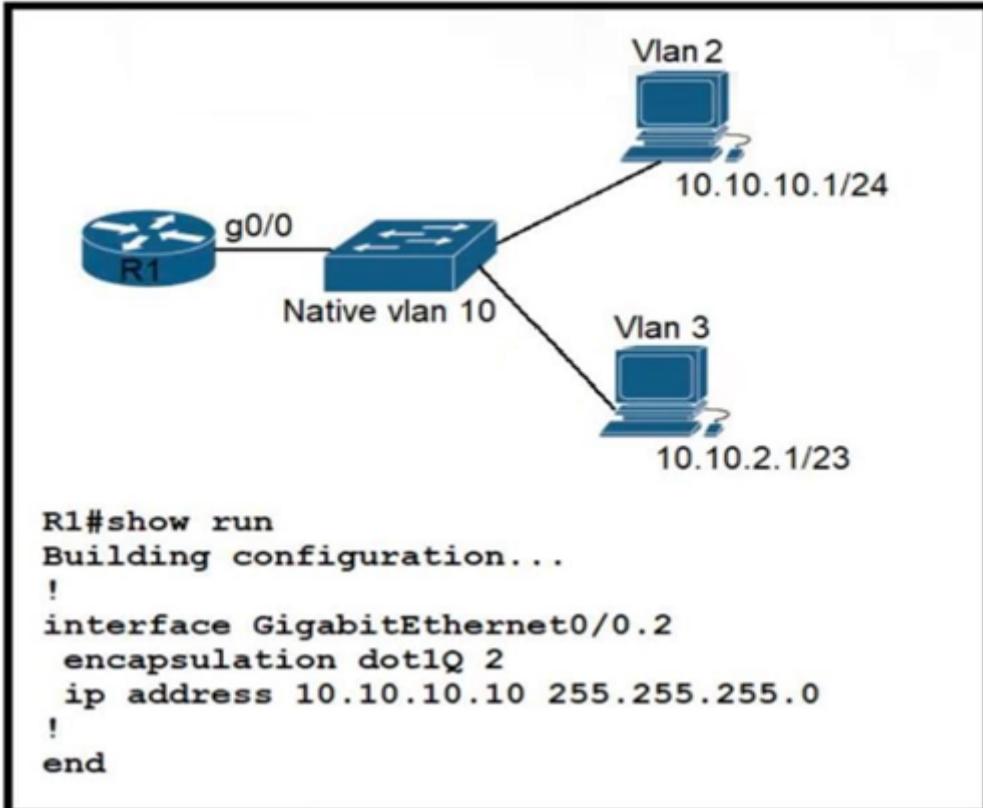
✉ **Goh0503** 8 months, 1 week ago

Answer D
upvoted 2 times

✉ **mrgreat** 9 months ago

D is correct
upvoted 1 times

Question #130



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 8 months 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 11 times

RougePotatoe Highly Voted 7 months, 2 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 10 times

Goh0503 Most Recent 9 months 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>

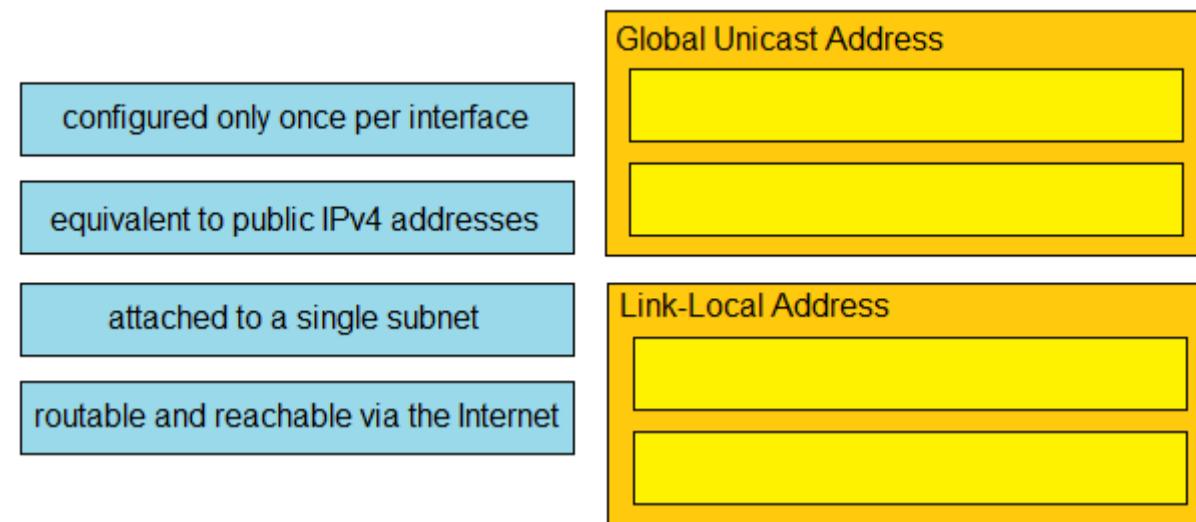
upvoted 4 times

Question #131

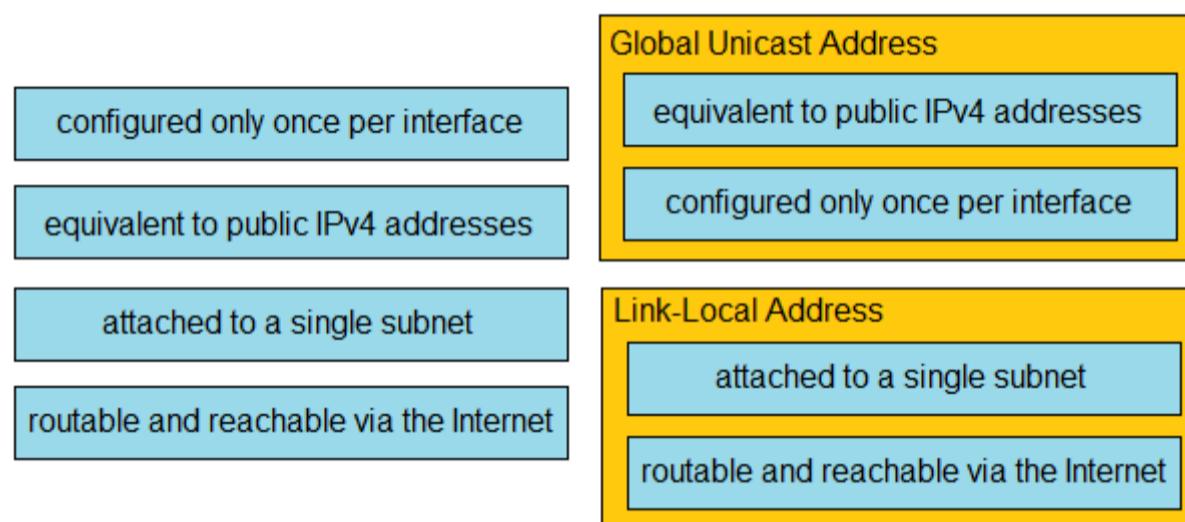
DRAG DROP -

Drag and drop the IPv6 address type characteristics from the left to the right.

Select and Place:



Correct Answer:



 **foreach** Highly Voted 9 months, 1 week 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 97 times

 **g_h_97** 9 months ago

Thanks man, that was a weird mistake tbh

upvoted 12 times

 **GhostWolf** 7 months ago

Bro I was questioning my sanity.

upvoted 16 times

 **Tony5000** Highly Voted 6 months, 2 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 9 times

 **UnbornD9** Most Recent 2 months ago

WTF, who configure the correct answer for this questions? Sometimes I doubt the correctness of this site...

upvoted 3 times

 **jahzz** 3 weeks, 3 days ago

they're 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 1 times

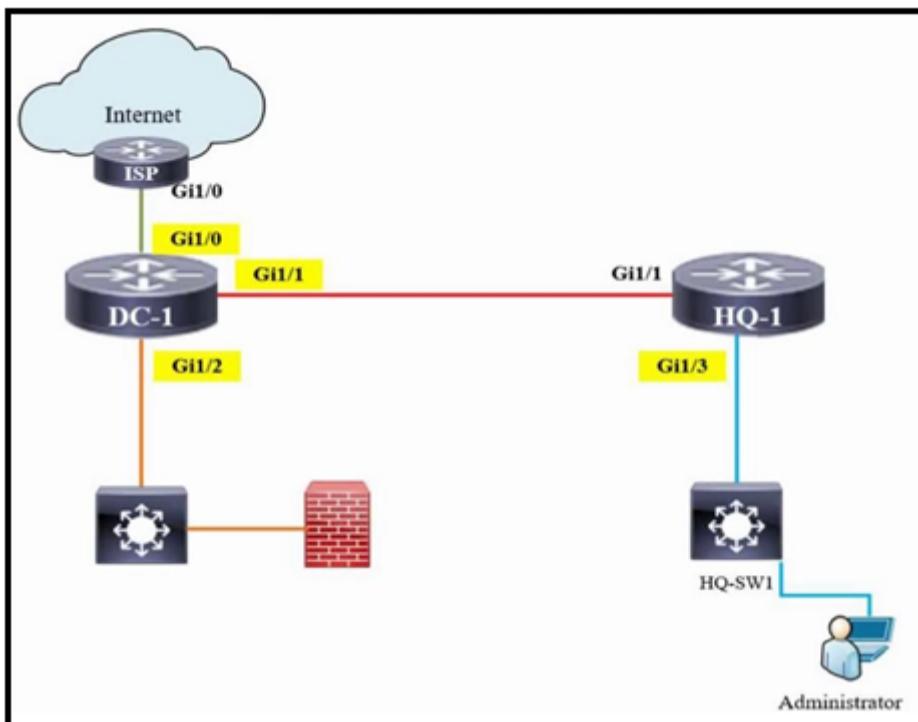
 **binrayelias** 4 months, 3 weeks ago

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

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

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
Correct Answer: 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 7 months, 2 weeks ago

Broadcast: odd
 Network: even
 1st usable: odd
 last usable: even
 upvoted 17 times

✉ **NICE_ANSWERS** 1 week, 4 days ago

Please, what's the significance of this coded info
 upvoted 1 times

✉ **jamesgavin** 1 month, 3 weeks 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 2 times

 **Request7108** (Most Recent) 5 months, 2 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 2 times

 **UnbornD9** 2 months 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

 **beerbiceps1** 2 months ago

I think once you skip and click next you can't go back

upvoted 2 times

 **GigaGremlin** 7 months, 3 weeks 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** 7 months, 3 weeks ago

IMHO someone should correct the 1st Question 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** 8 months, 1 week ago

Key word is "last usable address/ first usable address", check all possible subnet addresses then find if that is the last or first.

upvoted 1 times

 **DUMPLedore** 8 months, 1 week ago

can someone help to explain how the answers were get? I'm confused.

upvoted 1 times

 **netzwork** 8 months, 1 week 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 9 months ago

C is correct

[https://www.techtarget.com/whatis/definition/RFC-1918#:~:text=Along%20with%20NAT%20\(network%20address,before%20the%20adoption%20of%20IPv6.](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 7 months, 2 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** 8 months, 2 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** 7 months, 2 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

DRAG DROP -

Drag and drop the IPv6 address types from the left onto their descriptions on the right.

Select and Place:

2001:DB8::bc0d:1234:456d :aacc	multicast address used only locally within the site
FD00:0000:0000:1a2d:a 153:3992:a19d:ccca	address that is automatically created on a link when IPv6 is enabled on an interface
FE80::abcd:f00f:12de:3992	address that is prohibited from routing to the Internet
FF05::23:becf:22:1111	address that is unique and reserved for documentation purposes

2001:DB8::bc0d:1234:456d :aacc	FF05::23:becf:22:1111
FD00:0000:0000:1a2d:a 153:3992:a19d:ccca	FE80::abcd:f00f:12de:3992
FE80::abcd:f00f:12de:3992	FD00:0000:0000:1a2d:a 153:3992:a19d:ccca
FF05::23:becf:22:1111	2001:DB8::bc0d:1234:456d :aacc

Correct Answer:

  **Dutch012** Highly Voted  3 months, 2 weeks ago

"prohibited"..... Cisco, please use simpler words in your questions, not all of us are born in the US.
upvoted 10 times

  **sol_ls95** Highly Voted  4 months, 2 weeks ago

FF: MULTICAST

FD: UNIQUE LOCAL

FE: LINK LOCAL

2001: GLOBAL UNIQUE

upvoted 9 times

  **Manu_FR** Most Recent  1 day, 5 hours 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 1 times

  **iMo7ed** 3 months, 4 weeks 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 6 times

  **binrayelias** 4 months, 3 weeks 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** 4 months, 3 weeks 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** 5 months, 3 weeks ago

Then the solution is wrong?

upvoted 1 times

✉ **sol_ls95** 4 months, 2 weeks ago

the solution is correct

upvoted 1 times

✉ **Robertlars** 5 months, 4 weeks 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

✉ **freaknowledge123** 5 months ago

FF05: is a multicast address used only for local scope<https://learningnetwork.cisco.com/s/question/0D53i00000Z9uywCAB/what-about-address-of-ff052>

upvoted 3 times

✉ **sol_ls95** 4 months, 2 weeks ago

2001 its not multicast

upvoted 2 times

Question #135

Topic 1

```

Router# show interface g10/0/0
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	<ol style="list-style-type: none"> 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** 5 months, 3 weeks 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 4 times

 **Yunus_Empire** 6 months, 1 week ago

Selected Answer: C

Given Answer is Correct...

upvoted 1 times

 **NICE_ANSWERS** 1 week, 4 days ago

From the output, how do you know the cable connection is faulty?

upvoted 2 times

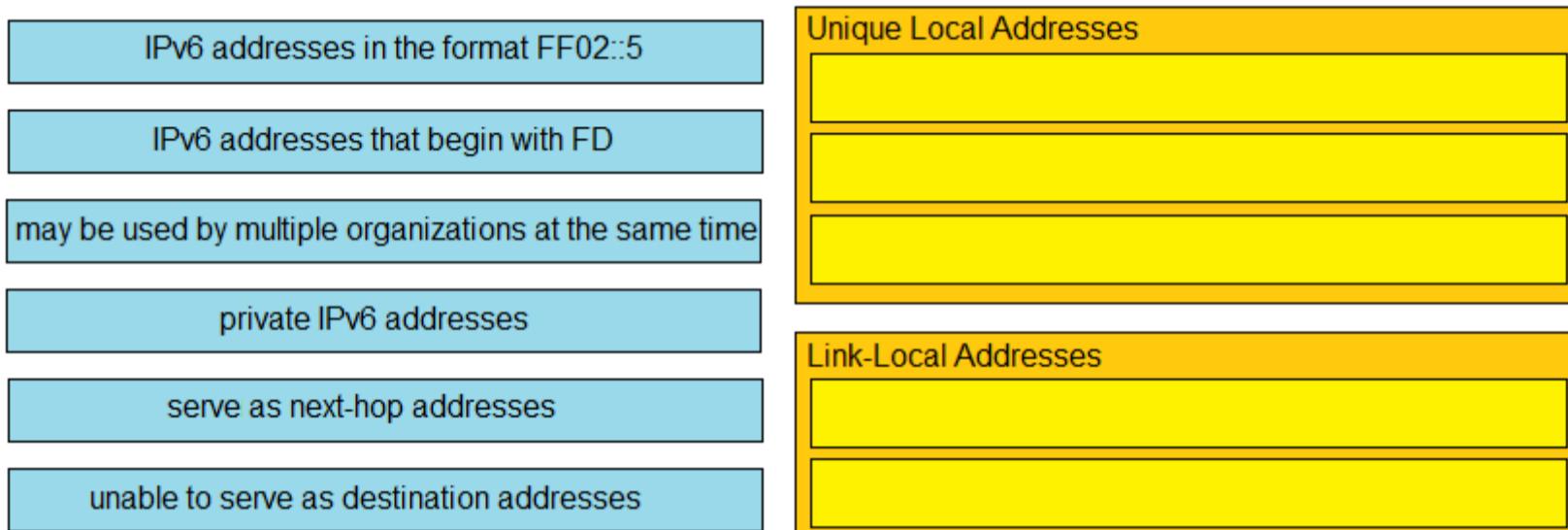
Question #136

Topic 1

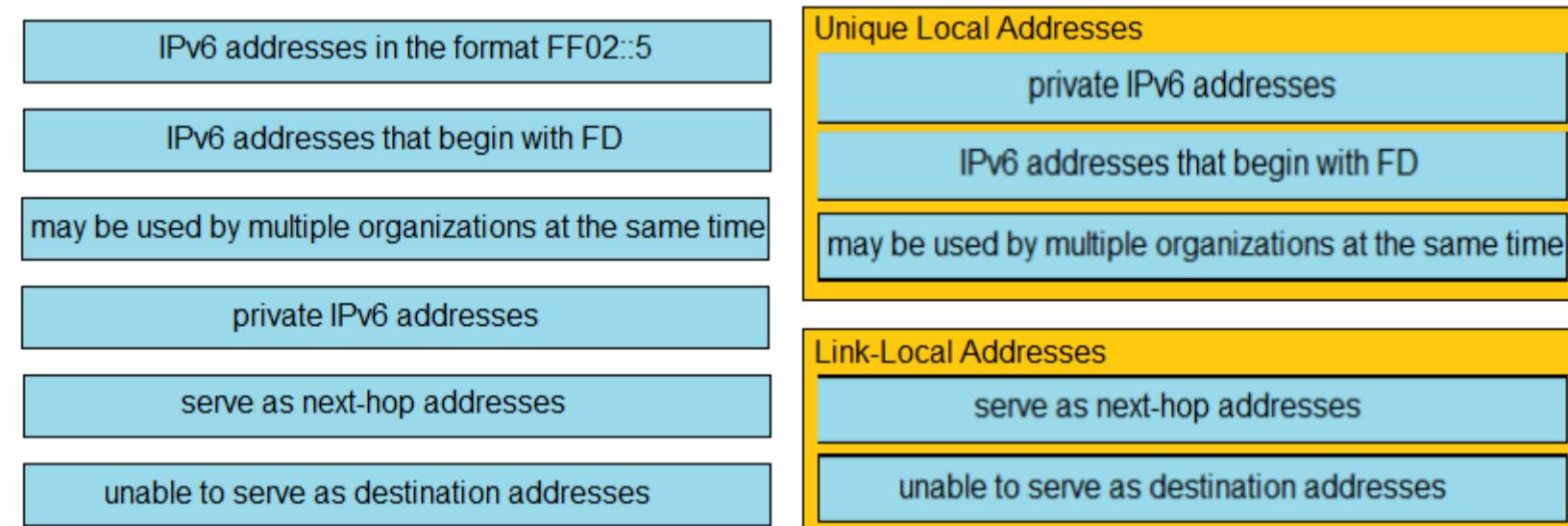
DRAG DROP -

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:



 **Mikeabo** 3 months, 3 weeks ago

Also FF is a multicast not a Unicast which encompasses global, unique local, Link Local

upvoted 2 times

 **Mikeabo** 3 months, 3 weeks ago

ff02::5 all OSPF (Open Shortest Path First) routers ... <https://www.menandmice.com/blog/ipv6-reference-multicast>, I guess that's the reason

upvoted 2 times

 **lololss** 4 months, 3 weeks ago

Why not IPv6 addresses in the format FF02::5?

FF02::5 I know it's a link-local scope.

upvoted 1 times

 **freaknowledge123** 4 months, 3 weeks ago

ff02 is a multicast address, check the documentation

upvoted 5 times

Question #137

DRAG DROP -

Drag and drop the IPv6 addresses from the left onto the corresponding address types on the right.

Select and Place:

	Global Unicast
2001:db8:600d:cafe::123	
	Link-Local Unicast
fcba:926a:e8e:7a25:b1:c6d2:1a76:8fdc	
	Multicast
fe80::a00:27ff:feeb:89aa	
	Unique Local
ff05:1:3	

Correct Answer:

2001:db8:600d:cafe::123	Global Unicast
fcba:926a:e8e:7a25:b1:c6d2:1a76:8fdc	Link-Local Unicast
fe80::a00:27ff:feeb:89aa	Multicast
ff05:1:3	Unique Local

 arjune Highly Voted  2 months ago

All answers are correct
upvoted 8 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

✉️ 🚑 **Destructo** 3 months ago

Reliability = Redundancy, Full Mesh is the only option that gives you that.
upvoted 3 times

✉️ 🚑 **harkindeyee** 3 months, 1 week ago

Full mesh obviously
upvoted 1 times

✉️ 🚑 **Robertlars** 5 months, 3 weeks ago

<https://ipcisco.com/wan-topology-types/> (yes, full mesh is the correct answer)
upvoted 2 times

✉️ 🚑 **mrgreat** 9 months ago

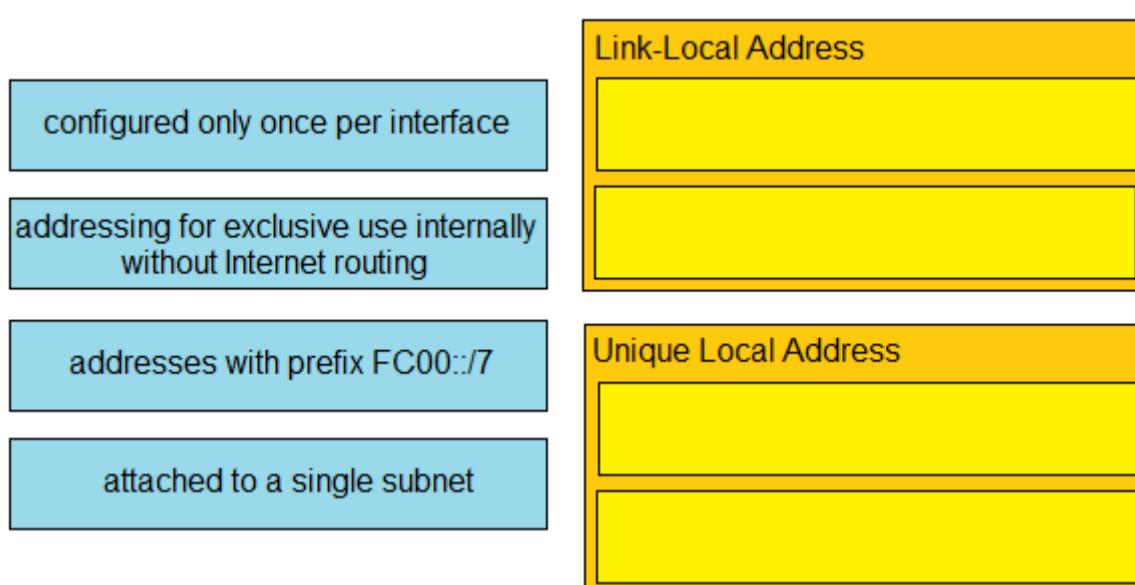
C is correct
<https://www.sciencedirect.com/topics/computer-science/mesh-topology>
upvoted 3 times

Question #139

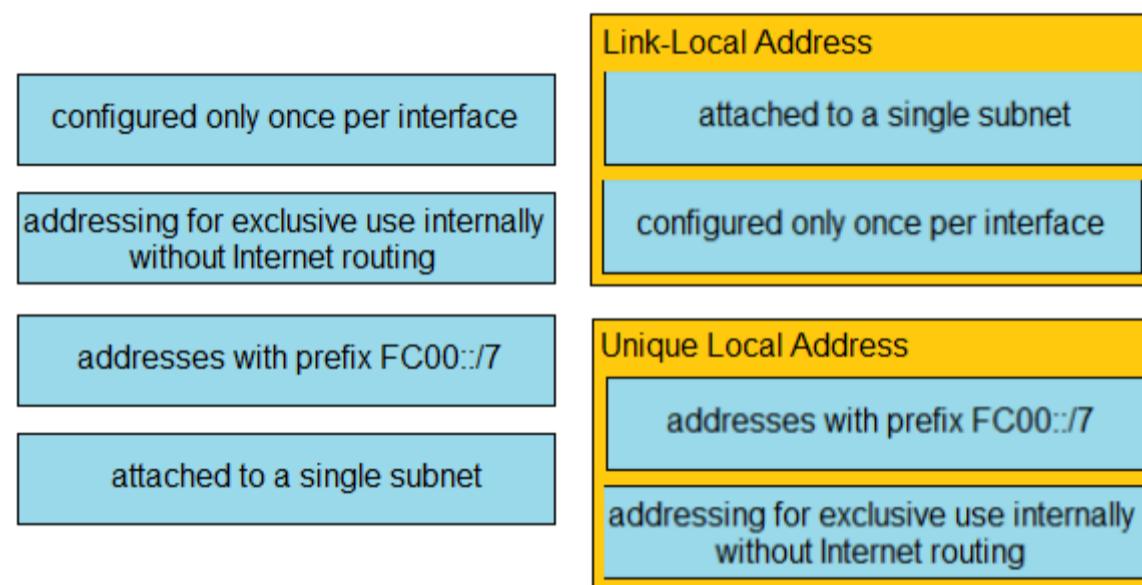
DRAG DROP -

Drag and drop the IPv6 address type characteristics from the left to the right.

Select and Place:



Correct Answer:



everchosen13 8 months, 2 weeks ago

Link-local addresses are not routable on the internet. Answer given is incorrect
upvoted 3 times

BieLey 8 months, 1 week ago

There is no answer about routing to the internet. Given answers are correct.
upvoted 13 times

Webfat 4 months, 2 weeks ago

I think what he means is that both address is not routable on the internet
upvoted 2 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 7 months, 2 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 14 times

 **Vlad_Is_Love_ua** Most Recent 9 months 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 Flooding
- UDLD Failure
- Broadcast Storms
- BPDU Guard

upvoted 4 times

 **Vlad_Is_Love_ua** 9 months ago

Selected Answer: B

<https://learningnetwork.cisco.com/s/question/0D53i00000Kt17xCAB/error-disable-port-state>
upvoted 1 times

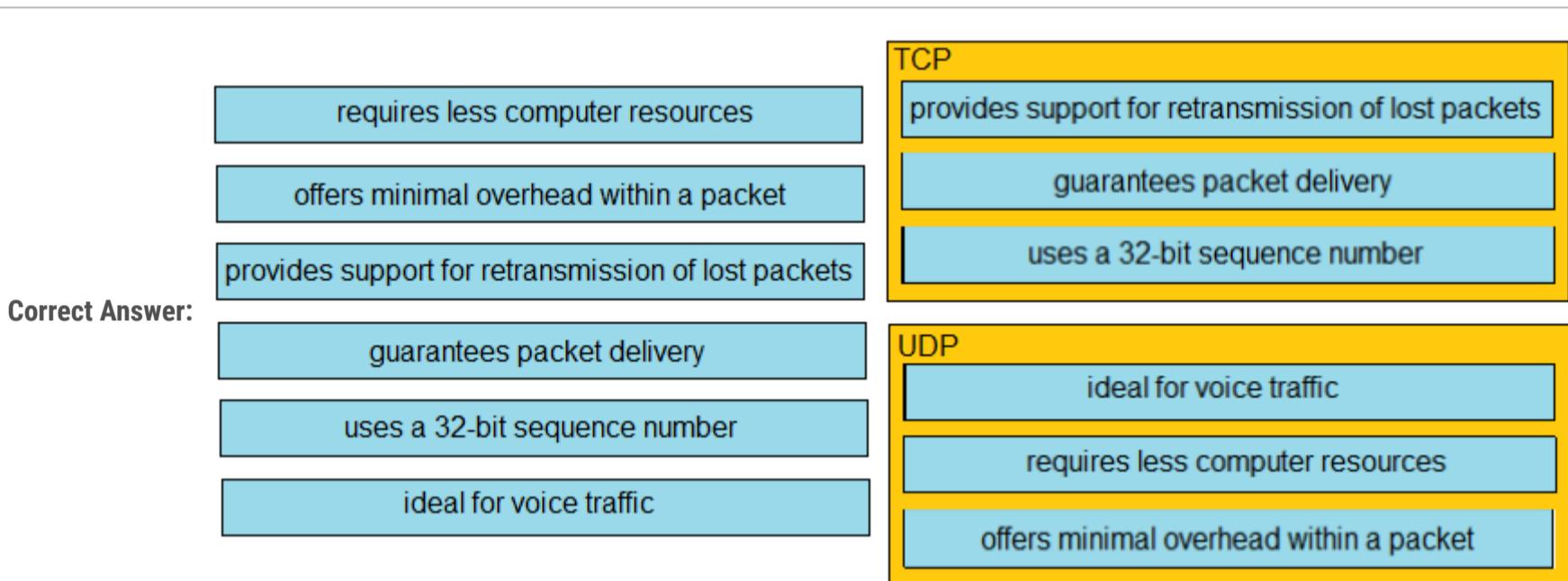
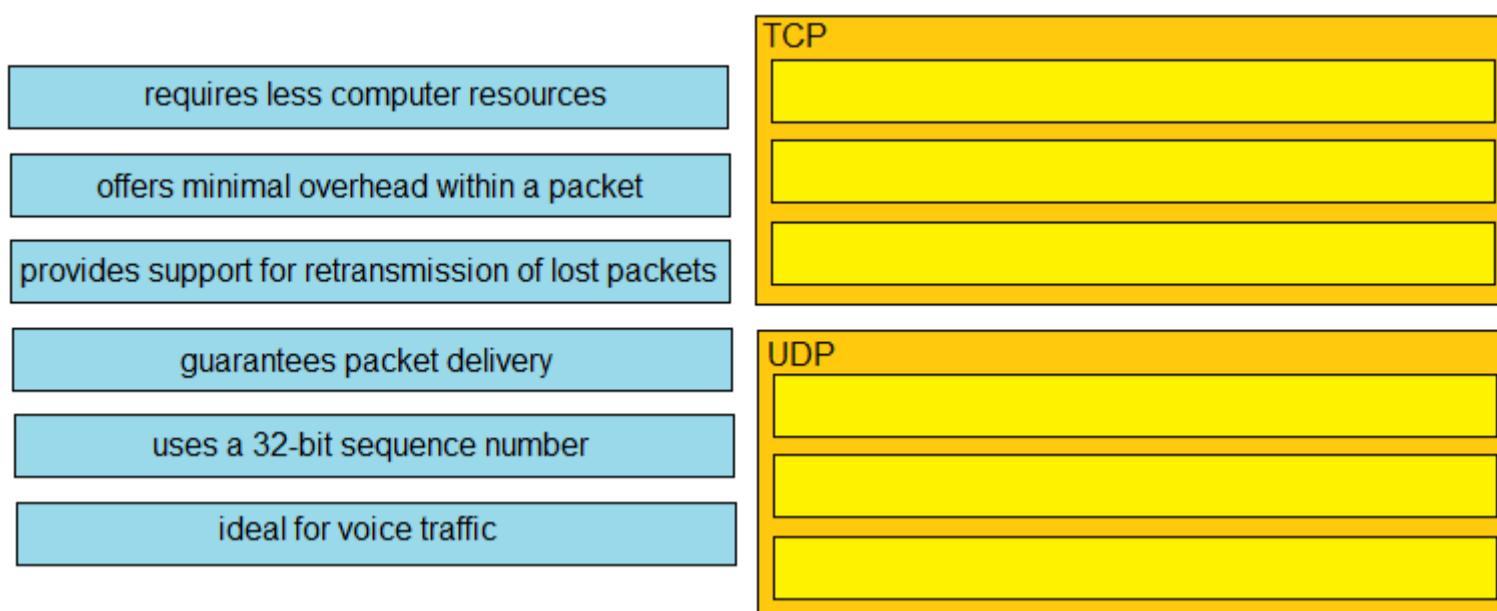
Question #141

Topic 1

DRAG DROP -

Drag and drop the characteristics of transport layer protocols from the left onto the corresponding protocols on the right.

Select and Place:



Fermento Highly Voted 8 months ago

This solution is right
upvoted 6 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%
---------	----

 **Fermento** Highly Voted 8 months ago

Selected Answer: A

Correct

upvoted 8 times

 **Dutch012** Highly Voted 3 months, 2 weeks ago

I hope hundreds of questions like this in my next week exam

upvoted 5 times

 **harkindeylee** 3 months ago

ikr the joy of bonus mark

upvoted 3 times

 **Da_Costa** Most Recent 1 week, 4 days ago

/29 just calculate or add the number of bits

upvoted 1 times

 **Jorro99404** 3 weeks, 2 days ago

Selected Answer: A

A. /29

upvoted 1 times

 **Bhrino** 3 weeks, 6 days ago

Selected Answer: A

If it's not obvious enough just count the ones in the last octet

upvoted 1 times

 **StingVN** 1 month, 1 week ago

Selected Answer: A

This is free point from Cisco i guess.

A

upvoted 2 times

 **deluxeccna** 1 month, 3 weeks ago

Selected Answer: A

A is correct

upvoted 2 times

 **Jack67** 2 months, 2 weeks ago

Selected Answer: A

A ist correct

upvoted 2 times

 **musio** 3 months, 2 weeks ago

Selected Answer: C

Correct

upvoted 1 times

 **Isuzu** 1 month ago

The subnet mask equivalent to 11111111.11111111.11111111.11111000 in dotted decimal notation is 255.255.255.248.

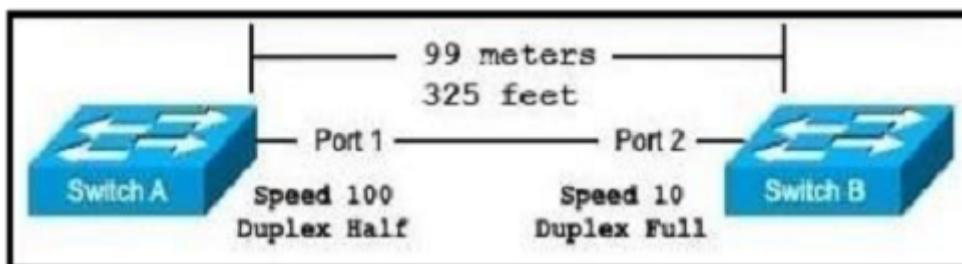
To determine the appropriate subnet mask for the given IP address and subnet mask, we need to identify the number of bits in the network portion of the address.

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 (100%)

zohar7471 Highly Voted 9 months 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 25 times

RougePotatoe 7 months, 1 week 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 4 times

guynetwork Highly Voted 8 months, 4 weeks ago

Selected Answer: A

It is A
upvoted 6 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

BE (58%)

AB (42%)

✉  **kenCapt**  7 months, 1 week 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 9 times

✉  **Rether16**  2 months 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 5 times

✉  **Isuzu**  1 month 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** 2 months, 1 week 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** 1 week, 4 days ago

But what happens to IPv6 addressing then? Can you please help explain that also for me?

upvoted 1 times

Question #145

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 8 months 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
 $255.255.255.224 \text{ or } 11111111.11111111.11111111.11100000$
 8 networks for /27 are 0,32,64,96,128,160,192,224
 upvoted 10 times

 **SVN05** 4 months 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

 **rubzal** Most Recent 1 week, 6 days ago

What does layer 3 interface used means in this question?

upvoted 1 times

 **studying_1** 1 week, 2 days 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 1 times

 **Bhrino** 3 weeks, 6 days 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 2 times

 **iMo7ed** 3 months, 3 weeks ago

Selected Answer: C
 C is correct
 upvoted 2 times

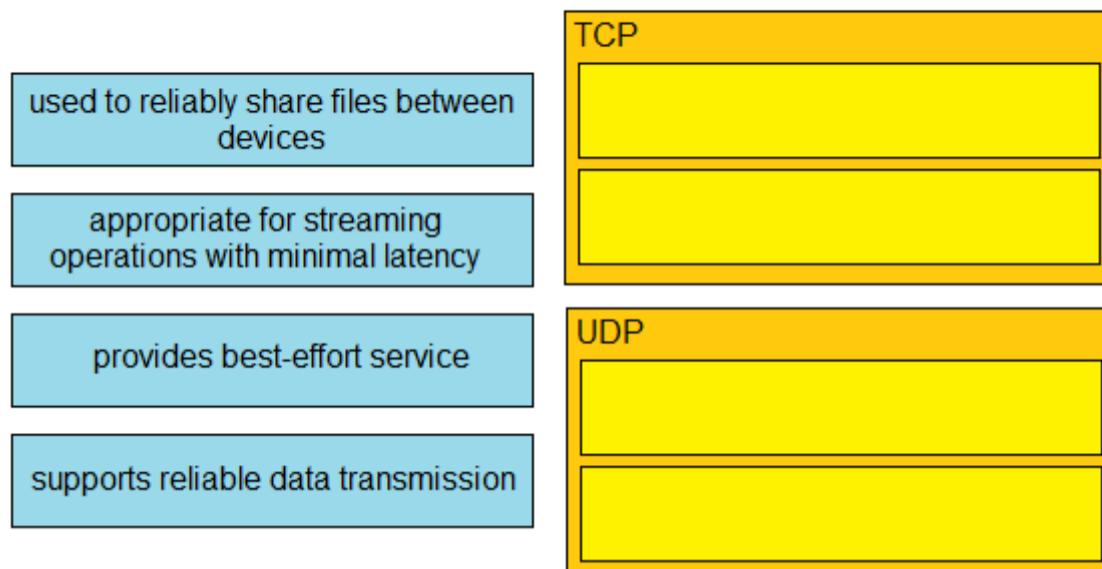
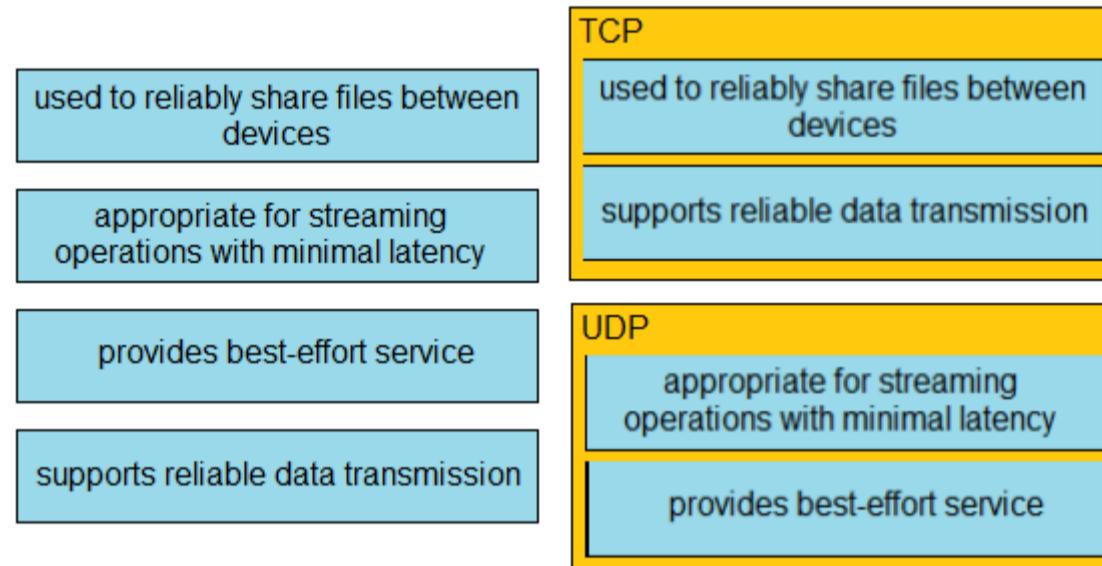
Question #146

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:

Answer Area**Answer Area****Correct Answer:** **alejandro12** 6 months, 3 weeks ago

correct answer is given

upvoted 4 times

 joanb2s 7 months ago

MAL MAL MAL. Correct TCP: provides... & supports. UDP: used to... & appropriate...

upvoted 1 times

 xWhosNext 6 months, 1 week 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

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 (60%)	AD (30%)	10%
----------	----------	-----

✉  **DoBronx** Highly Voted 7 months, 2 weeks ago

This bum ah question
upvoted 7 times

✉  **RougePotatoe** Highly Voted 7 months, 2 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 5 times

✉  **freaknowledge123** 4 months, 4 weeks ago

can't subnet an address when you have a limited address pool
upvoted 1 times

✉  **splashy** 7 months 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** 6 months, 3 weeks 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** 7 months, 2 weeks ago

yea that was weird man.. i could smell that bs from a mile away.
upvoted 2 times

✉  **Kyoxi** Most Recent 1 month, 3 weeks ago

Selected Answer: BC

chat gpt
upvoted 1 times

✉  **Isuzu** 1 month, 1 week ago

its C&D
upvoted 1 times

✉  **dearc** 2 months, 1 week 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** 3 months, 4 weeks 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** 4 months 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

 **ricky1802** 4 months 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** 4 months, 3 weeks 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 2 times

 **freeknowledge123** 5 months 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 your network from outside. the answer mention security within a network it doesn't indicate where the attack comes from

upvoted 3 times

Question #148

DRAG DROP -

Drag and drop the IPv6 DNS record types from the left onto the description on the right.

Select and Place:

AAAA	aliases one name to another
CNAME	associates the domain serial number with its owner
NS	correlates a domain with its authoritative name servers
PTR	correlates a host name with an IP address
SOA	supports reverse name lookups

AAAA	CNAME
CNAME	SOA
NS	NS
PTR	AAAA
SOA	PTR

Correct Answer:

 **TMT91** Highly Voted 8 months, 3 weeks ago

Is this related CCNA 200-301 ?

upvoted 11 times

 **daddydagoth** 3 months, 2 weeks ago

I am almost 99% sure that it is not

upvoted 2 times

 **cormorant** Highly Voted 6 months ago

SSSSSSSSSSOAAAAAA - asssssssssssociatesss the domain sssssssssssserial number with itsss ownaaaaaaaa -
upvoted 6 times

 **dropspable** Most Recent 1 month, 1 week 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** 2 months, 2 weeks ago

I think this is not related CCNA 200-301

upvoted 2 times

 **cpinac** 2 months, 4 weeks ago

This is correct!

upvoted 1 times

 **ricky1802** 3 months, 4 weeks 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 3 times

 **ccna_goaT** 8 months, 2 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** 3 months ago

yeah, technically a robbery.

upvoted 2 times

 **mrgreat** 9 months 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**  4 months 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 7 times

 **reeeda**  9 months 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:

	Global Unicast
3ffe:e54d:620:a87a::f00d	
	Link-Local Unicast
fe80::a00:27ff:feeb:89aa	
	Multicast
ff05::1:3	
	Unique Local
fd6d:c83b:5cef:b6b2::1	

Correct Answer:	Global Unicast
	3ffe:e54d:620:a87a::f00d
	Link-Local Unicast
	fe80::a00:27ff:feeb:89aa
	Multicast
	ff05::1:3
	Unique Local
	fd6d:c83b:5cef:b6b2::1

 FlyingBanana 3 months ago

remember that. unique local is my friend. (short form: fd)

upvoted 3 times

 cormorant 5 months, 4 weeks 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** 8 months, 3 weeks ago

Why not D?

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks

upvoted 1 times

 **Taku2023** 3 months, 2 weeks ago

Device is the keyword

upvoted 1 times

 **TMT91** 8 months, 3 weeks ago

D is Access Points not ACL !

upvoted 9 times

 **Dutch012** 3 months, 2 weeks 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** 4 months 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 3 times

Question #153

Topic 1

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

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) 5 months, 3 weeks 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 6 times

 **NICE_ANSWERS** Most Recent ⓘ 1 week, 4 days ago

Please, how do you know this is the broadcast address and the default gateway?

upvoted 1 times

 **Yunus_Empire** 6 months, 1 week ago

Simplest Question Ever 😊 😊

upvoted 3 times

 **Fermento** 8 months ago

It's correct

upvoted 4 times

Question #154

DRAG DROP -

Drag and drop the DNS lookup components from the left onto the functions on the right.

Select and Place:

domain	service that maps hostname to IP addresses
cache	local database of address mappings that improves name resolution performance
name resolver	in response to client requests, queries a name server for IP address information
DNS	component of a URL that indicates the location or organization type
no ip domain-lookup	disables DNS services on a Cisco device

Correct Answer:

domain	DNS
cache	cache
name resolver	name resolver
DNS	domain
no ip domain-lookup	no ip domain-lookup

  **Jhinminent** 1 month, 1 week ago

Answer is correct

upvoted 4 times

  **Robertlars** 5 months, 3 weeks 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

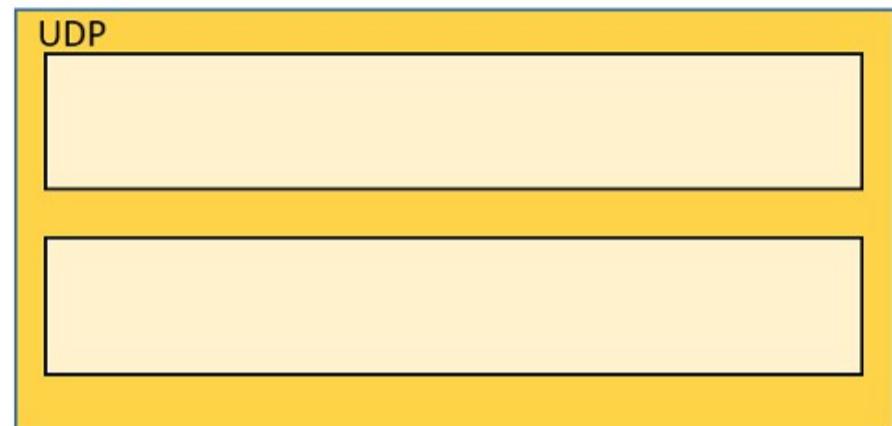
Question #155

DRAG DROP -

Drag and drop the TCP or UDP details from the left onto their corresponding protocols on the right.

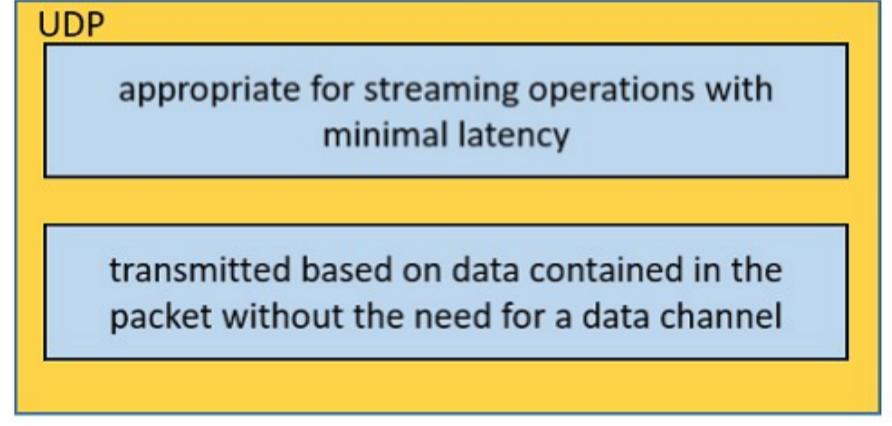
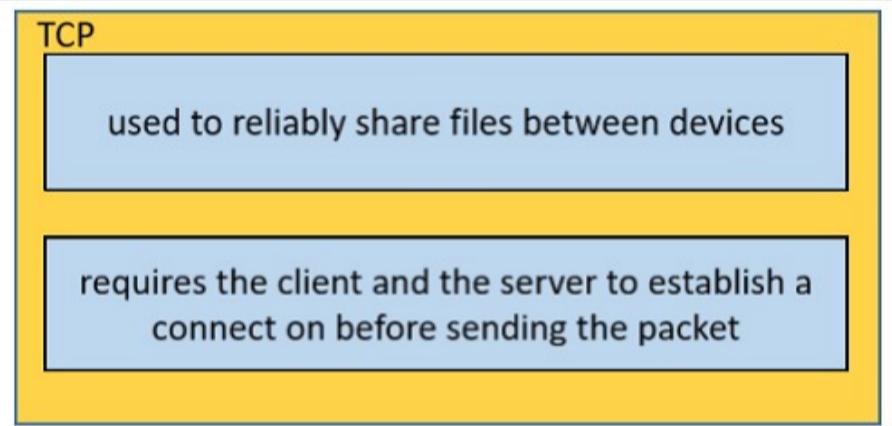
Select and Place:

- transmitted based on data contained in the packet without the need for a data channel
- requires the client and the server to establish a connect on before sending the packet
- used to reliably share files between devices
- appropriate for streaming operations with minimal latency



Correct Answer:

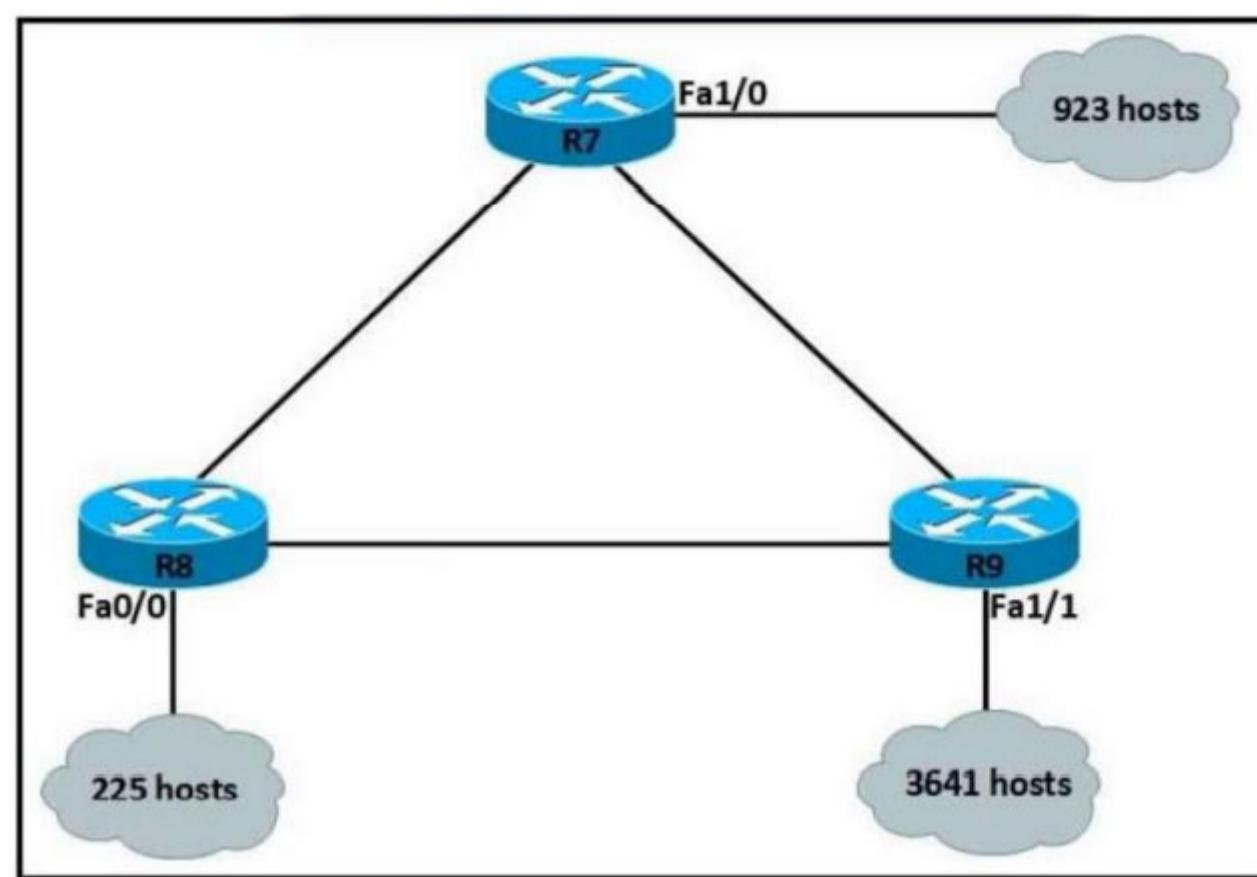
- transmitted based on data contained in the packet without the need for a data channel
- requires the client and the server to establish a connect on before sending the packet
- used to reliably share files between devices
- appropriate for streaming operations with minimal latency



sol_ls95 4 months, 2 weeks ago

correct answer

upvoted 4 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 8 months, 1 week ago

Can pinpoint this easily by only looking at R8:
255.255.255.0 is enough = Answer is C

upvoted 20 times

✉  **Rydaz** 4 weeks ago

by luck I looked at R8 first lol
upvoted 2 times

✉  **iMo7ed** Most Recent 3 months, 3 weeks ago

C is Correct
upvoted 2 times

✉  **sol_ls95** 4 months, 2 weeks ago

select the router with the lowest number of hosts, which is r8, for 225 hosts it would be a minimum of 256 hosts which is /24 which 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 8 months 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_ether.html

upvoted 6 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 3 months, 4 weeks 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

Question #159

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 (100%)

 **FALARASTA** 1 month, 2 weeks ago

B is correct

upvoted 1 times

 **ricky1802** 4 months 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 3 times

 **Bankultimate** 5 months, 3 weeks ago

B is correct.

upvoted 2 times

Question #160

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 9 months 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 9 times

 **dearc** Most Recent 2 months, 1 week 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

 **Netcmd** Highly Voted 6 months, 3 weeks ago

cat5e cant go more than 1GBps
upvoted 9 times

 **Anas_Ahmad** Highly Voted 6 months ago

CAT5e and CAT6 can handle speeds of up to 1000 Mbps, or a Gigabit per second.
upvoted 5 times

 **harkindey lee** Most Recent 3 months ago

cat 5e and base-T
upvoted 1 times

 **[Removed]** 3 months, 3 weeks ago

Why not AB??
upvoted 4 times

 **Shansab** 4 months, 2 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 3 times

 **Mahfuj_01** 6 months, 2 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

 **TKHZRD** Highly Voted 5 months, 1 week ago

The question is formulated in a weird way... Or is it me?

upvoted 10 times

 **NICE_ANSWERS** 1 week, 4 days ago

yes it is

upvoted 1 times

 **Silencer** 3 months, 3 weeks ago

I also noticed.

upvoted 1 times

 **wondaah** Most Recent 3 months ago

terrible question this is

upvoted 1 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

✉  **Customexit** Highly Voted 7 months, 2 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 11 times

✉  **[Removed]** Highly Voted 3 months, 3 weeks 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 5 times

✉  **AbiZ17** Most Recent 5 months 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** 3 months ago

same thought.

upvoted 1 times

✉  **THEKYPTONIAN** 8 months, 2 weeks ago

The subnet must include addresses 100 and 128 so /24 is correct

upvoted 2 times

✉  **g_h_97** 9 months ago

192.168.25.128/25 is the network address, I guess they meant 192.168.25.129/25

upvoted 3 times

✉  **Trdelnik** 8 months, 3 weeks 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** 8 months, 2 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

 **dearc** 2 months, 1 week 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 3 times

 **harkindeylee** 3 months 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** 3 months ago

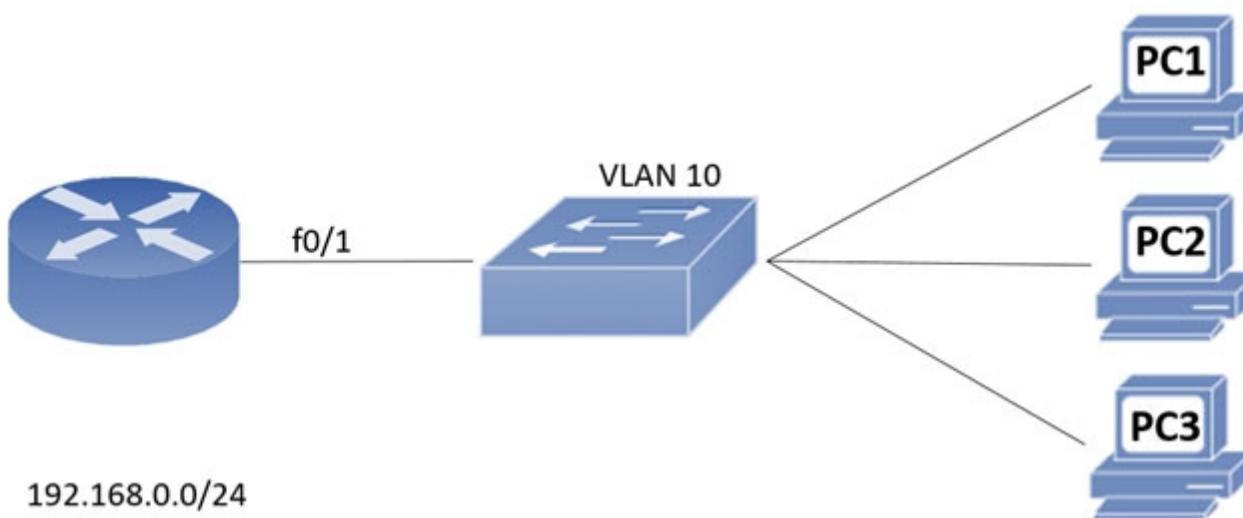
Selected Answer: B

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 scalabilty will be a factor

upvoted 2 times

Question #166



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 (71%)

A (29%)

vladals Highly Voted 8 months, 3 weeks 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 20 times

dendenter Highly Voted 7 months, 4 weeks ago

30 ADDITIONAL SUBNETS , IT MUST BE 32 = 5 BITS
CLASS C /24+5BITS = /29 = 225.255.255.248

upvoted 5 times

Bhrino Most Recent 3 weeks, 5 days 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 1 times

omid8719 1 month, 2 weeks ago

Selected Answer: B

need 31 Subnet

upvoted 2 times

dearc 2 months, 1 week 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 2 times

thomson_johnson 2 months, 3 weeks 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** 3 months 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 receive IPs per subnet. As you need 3 hosts for addressing, Answer B is the correct upvoted 2 times

 **iMo7ed** 3 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 2 times

 **shubhambala** 8 months, 4 weeks 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** 8 months, 2 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 (100%)

✉ **cormorant** Highly Voted 7 months ago

questions like this have convinced me that to pass the CCNA it is necessary to bone up on dumps

upvoted 27 times

✉ **ThomasSmith** 1 month ago

Any idea for a reliable dump please? I cannot find a decent source.

upvoted 1 times

✉ **daddydagoth** 3 months, 2 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 5 times

✉ **DPAD** 5 months, 3 weeks ago

just like Microsoft exams

upvoted 4 times

✉ **GhostWolf** 7 months ago

Exactly, the way CISCO sets their exams you can't just do it from reading a textbook.

upvoted 10 times

✉ **dearc** Highly Voted 2 months, 1 week 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 5 times

✉ **Ciscoman021** Most Recent 2 months, 2 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** 7 months, 1 week 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** 3 months, 4 weeks 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 2 times

✉ **diidiuQldama** 5 months, 2 weeks ago

long cable=high latency
upvoted 1 times

RougePotatoe 4 months, 1 week 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_goa Highly Voted 8 months, 2 weeks ago
another question not related with CCNA. love it. they got brazen recently, im waiting for CCIE questions on CCNA exam.
upvoted 21 times

AshenOne_31 Highly Voted 7 months, 3 weeks ago
such a ridiculous question for the CCNA
upvoted 8 times

[Removed] Most Recent 3 months, 3 weeks ago
I think this is not in CCNA 200-301 exam topic
upvoted 3 times

in2it 4 months 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 4 months 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

sassasasadccadsca 5 months 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 9 months 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

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 (67%)	DE (29%)	5%
----------	----------	----

 **RougePotatoe** Highly Voted 7 months, 2 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 10 times

 **Dutch012** 3 months, 2 weeks ago

it says "external DDOS attack", so I believe D & A are correctt

upvoted 1 times

 **oatmealturkey** 3 months, 4 weeks 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 2 times

 **Dutch012** 3 months, 2 weeks ago

Sorry man I wrote the comment in a hurry, I meant D & E

upvoted 1 times

 **DoBronx** 7 months, 2 weeks ago

Yea i picked A E as well

upvoted 2 times

 **splashy** Highly Voted 4 months, 3 weeks 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 5 times

 **omid8719** Most Recent 1 month, 2 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** 4 days, 16 hours 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** 1 month, 2 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 1 times

 **FALARASTA** 1 month, 2 weeks 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 1 times

 **dearc** 2 months, 1 week 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** 2 months, 1 week 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 2 times

 **elixirwell** 2 months, 1 week 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** 3 months, 3 weeks ago

Selected Answer: DE

the answer is de

upvoted 1 times

 **[Removed]** 3 months, 3 weeks ago

I choose DE

upvoted 1 times

 **AshenOne_31** 6 months ago

Selected Answer: AE

D makes no sense, it's AE

upvoted 1 times

 **daddydagoth** 3 months, 2 weeks ago

How does a prive ip address, reachable only trough the internal network, protecting said network from EXTERNAL attacks, not make sense exactly?

upvoted 1 times

 **Netcmd** 6 months, 3 weeks ago

selected answer:AE

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

Question #171

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 → core → access
- B. access → distribution → distribution → access
- C. access → core → distribution → access
- D. access → distribution → core → distribution → access

Correct Answer: D

✉️  **Dutch012**  3 months, 2 weeks ago

Selected Answer: D

Distribution doesn't connect to another Distribution layer directly, it needs to go through core first
upvoted 10 times

✉️  **RougePotatoe**  7 months, 2 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

✉️  **Hope_12**  1 month ago

Selected Answer: D

Core switches connect distribution switches.
D is the answer.
upvoted 1 times

✉️  **omid8719** 1 month, 2 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** 1 month, 2 weeks 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** 2 months 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** 2 months, 1 week 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

✉️  **Rydaz** 4 weeks ago

no direction connection from device to core brother, C is wrong, it's either B or D

upvoted 2 times

 **Njavwa** 2 months, 2 weeks ago

Selected Answer: D

three tier, 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** 3 months, 2 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]** 3 months, 3 weeks 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** 4 months, 2 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** 4 months, 3 weeks ago

D is correct, if it were access - distribution - access b would have been correct

upvoted 2 times

 **yeret** 4 months, 3 weeks ago

Selected Answer: D

Distribution layer don't directly connected each other, they use core layer to be connected.

<https://www.ictshore.com/free-ccna-course/three-tier-architecture/>

upvoted 2 times

 **Christiandus** 6 months, 1 week ago

Selected Answer: D

IMO D is correct. B would be assuming that it's a different access switch but in the same switch-block. However if the device is in a different switch-block the correct answer would be D.

upvoted 2 times

 **bruno0147** 7 months, 2 weeks ago

B is correct.

upvoted 4 times

 **usamahrakib001** 8 months ago

need routing that is only on core layer

upvoted 1 times

 **WowA** 8 months, 3 weeks ago

Why over the core and not only over the distribution ?

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

 **Naghini** Highly Voted 4 months, 3 weeks ago

Aren't both A and B correct?

upvoted 5 times

 **Ciscoman021** Most Recent 2 months ago

Selected Answer: A

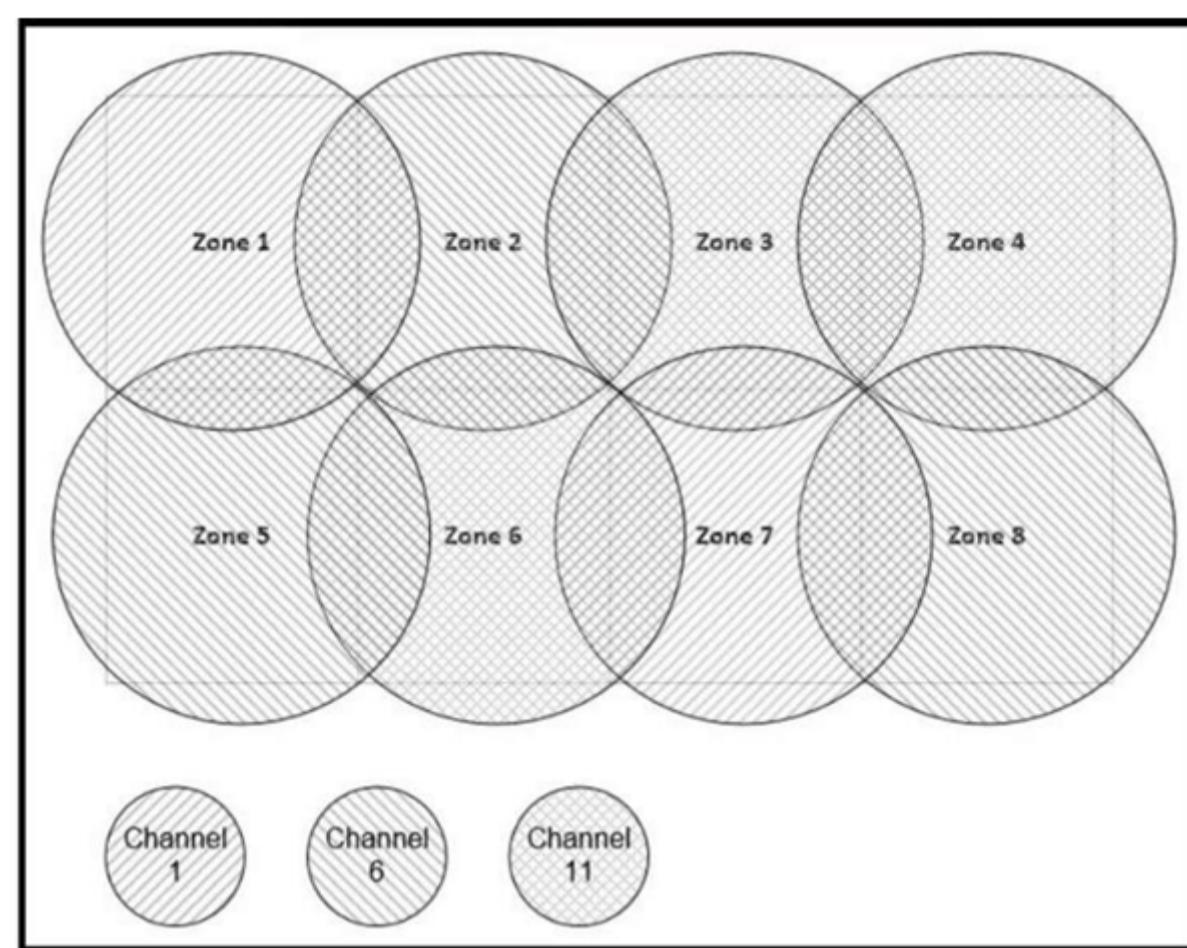
A is correct.

upvoted 2 times

 **Ceruzka** 3 months, 1 week ago

A and B are correct. What's wrong with B?

upvoted 1 times



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

rx78_2 Highly Voted 3 months ago

looks like it is a vision test instead of a network exam
upvoted 11 times

soRwatches Highly Voted 2 months, 4 weeks ago

dafuq is this type of question?
upvoted 7 times

StingVN Most Recent 1 month, 1 week ago

Selected Answer: C
C is correct. Zone 3 and Zone 4 is same channel 11.
upvoted 1 times

daddydagoth 3 months, 2 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 2 times

Anas_Ahmad 5 months ago

Selected Answer: C
Zones 3 and 4 both have Channel 11 and overlapped
upvoted 4 times

Anas_Ahmad 5 months, 1 week 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 6 months ago

in this question: 1 is //// and 6 is \\\\\\ and 11 is ####
upvoted 3 times

✉ **Yunus_Empire** 6 months ago

1 is //// and 6 is \\\\\\ and 11 is ####

upvoted 1 times

✉ **ErnestoAAA** 7 months, 3 weeks ago

why is 3 and 4 zone the answer

upvoted 2 times

✉ **insulated** 7 months, 2 weeks ago

I think because zone 3 and 4 both is use ch 11

upvoted 3 times

✉ **RougePotatoe** 7 months, 2 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

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

 **Alan100** Highly Voted 4 months, 3 weeks 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 9 times

 **StingVN** 1 month, 1 week ago

LOL this is Cisco test anyway. so we must follow Cisco rule.

upvoted 4 times

 **EliasM** Highly Voted 8 months, 2 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_great** 8 months, 2 weeks ago

so-called broken question. yes, it should be partial mesh.

upvoted 5 times

 **Jorro99404** Most Recent 1 week ago

Selected Answer: C

I bet on P2P

upvoted 1 times

 **Isuzu** 1 month 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** 1 month, 2 weeks ago

Selected Answer: D

the advantage of hub and spoke

upvoted 1 times

 **Ciscoman021** 2 months, 1 week 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** 2 months, 1 week 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 1 times

 **deluxeccna** 1 month, 3 weeks ago

thanks, ChatGPT

upvoted 3 times

 **checkoboy88** 3 months 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 1 times

 **Dutch012** 3 months, 2 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

 **ricky1802** 4 months ago

Selected Answer: D

In a hub-and-spoke topology, a central hub device, such as a router, connects to multiple spoke devices, such as remote branch offices. The spoke devices communicate with the hub device, but do not communicate directly with each other. This topology provides a simple and scalable design, as new spoke devices can easily be added to the network without affecting existing connections. It also provides high quality and reliable communication, as the hub device acts as a central point of control and can provide backup and redundancy options.

A partial mesh topology provides more direct connections between devices, but can be more complex to design and maintain. A full mesh topology provides the greatest amount of direct connections, but can be the most complex and expensive to implement. A point-to-point topology provides a direct connection between two devices, but does not provide the central hub for control and redundancy.

upvoted 2 times

 **Mistwalker** 5 months, 1 week ago

Selected Answer: A

Once availability becomes a factor, you can't choose P2P.

upvoted 3 times

 **Panda_man** 6 months, 1 week ago

Selected Answer: A

partial mesh

upvoted 2 times

 **hasbulla01** 6 months, 3 weeks ago

Selected Answer: A

P2P not have availability

upvoted 3 times

 **splashy** 7 months ago

Full mesh and more so partial mesh from an enterprise perspective is anything but simple. Simplicity is the key word as in it's something a SOHO for example would prefer.

A dedicated point-to-point connection is still more available than a normal (consumer) broadband connection, which most people and companies use (with VPN).

upvoted 1 times

 **Garfieldcat** 7 months, 2 weeks ago

I optioned partial mesh too. P2P has single point of failure, i.e. availability issue though simplicity and quality is true

upvoted 2 times

Question #175

DRAG DROP -

Drag and drop the statements about wireless architectures from the left onto the architectures on the right.

Select and Place:

It encapsulates LWAPP traffic between the access point and the WLC in EtherType 0xB BBBB.

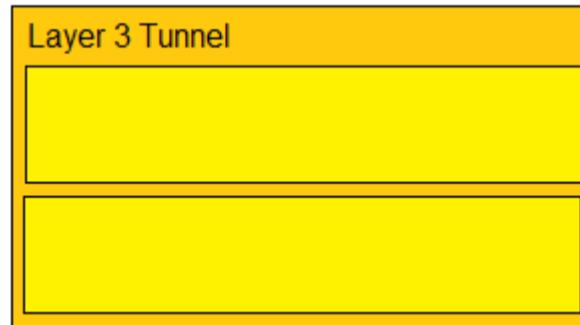
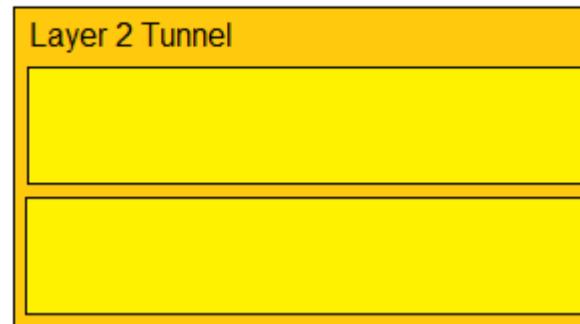
It facilitates Layer 2 connectivity between the WLC's wired interface and the WLAN clients.

It forwards only IP EtherType frames.

It requires IP addresses on the access point and the WLC.

It supports LWAPP tunneling within Ethernet frames and UDP packets.

It uses UDP or UDP Lite for IPv6 deployments.

**Correct Answer:**

It encapsulates LWAPP traffic between the access point and the WLC in EtherType 0xB BBBB.

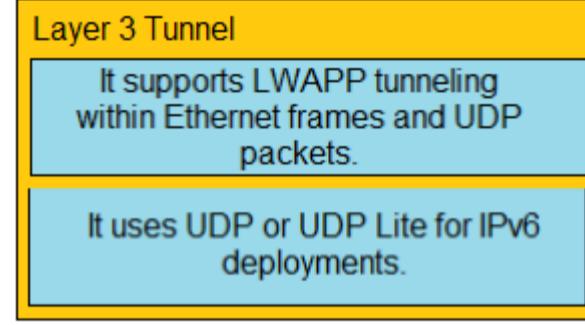
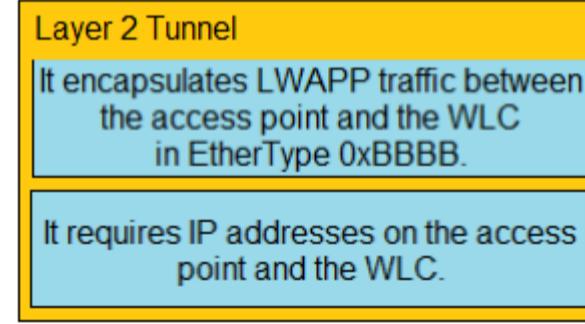
It facilitates Layer 2 connectivity between the WLC's wired interface and the WLAN clients.

It forwards only IP EtherType frames.

It requires IP addresses on the access point and the WLC.

It supports LWAPP tunneling within Ethernet frames and UDP packets.

It uses UDP or UDP Lite for IPv6 deployments.



✉ **RougePotatoe** Highly Voted 6 months, 3 weeks ago

Does anyone have any insights to this question? Couldn't find anything mentioning anything related to the answers in the cert guide.
upvoted 5 times

✉ **Yasyas86** 6 months, 3 weeks ago

Answers giving are correct

<https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/TechArch.pdf>
upvoted 10 times

✉ **daddydagoth** Most Recent 3 months, 2 weeks ago

Not related to CCNA 200-301...
upvoted 2 times

✉ **[Removed]** 3 months, 3 weeks ago

I think this kind of question is not in CCNA 200-301 exam topic
upvoted 4 times

Question #176

DRAG DROP -

Drag and drop the Wi-Fi terms from the left onto the descriptions on the right.

Select and Place:

distribution system	Wi-Fi option in which cells from different access points are linked together
extended service set	Wi-Fi option that enables two or more clients to communicate directly without a central access point
independent basic service set	Wi-Fi option based around one or more access points
infrastructure mode	alphanumeric text string that identifies a wireless network
SSID	entire wireless cell of an access point and the linkage to the wired network

distribution system	distribution system
extended service set	independent basic service set
independent basic service set	infrastructure mode
infrastructure mode	SSID
SSID	extended service set

✉  **splashy**  8 months, 4 weeks 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 38 times

✉  **Mewkzz** 8 months, 3 weeks ago

I concur same order based on the URL shared.
 upvoted 1 times

✉  **dropspable**  1 month 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** 1 month ago

Also according to the textbooks, the Distribution System is the wired link that connects the switch to the APs - this I had already studied. So I see that it is inverted with ESS.

upvoted 1 times

✉ **dearc** 2 months 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** 2 months, 2 weeks ago

the answers are correct check your Netacad notes

WLAN CONCEPTS

CHAPTER 12

upvoted 1 times

✉ **oatmealturkey** 3 months, 2 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 1 times

✉ **freeknowledge123** 5 months ago

again with the voodoo 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 alphanumeric 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** 5 months, 4 weeks ago

The Correct answer is:

- > Distribution System
- > IBSS
- > ESS
- > SSID
- > Infrastructure Mode

upvoted 1 times

✉ **jibon_22** 5 months, 4 weeks ago

Correction:

- > ESS
- > IBSS
- > Distribution System
- > SSID
- > Infrastructure Mode

upvoted 2 times

✉ **everchosen13** 8 months, 2 weeks ago

I think it is Infrastructure mode and Extended Service set that need to be switched

upvoted 1 times

✉ **everchosen13** 8 months, 2 weeks ago

<https://www.lifewire.com/infrastructure-mode-in-wireless-networking-816539>

upvoted 1 times

✉ **nick9898** 8 months, 2 weeks ago

this is a great article on this.

some spelling errors but otherwise a good read.

<https://ipcsisco.com/lesson/wireless-principles/>

upvoted 2 times

 **PiotrMar** 8 months, 3 weeks ago

I think that in the answer: infrastructure mode and extended service set should be swapped.

upvoted 3 times

 **g_mindset** 8 months, 4 weeks 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

 **Vlad_Is_Love_ua** Highly Voted 8 months, 3 weeks 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

 **Isuzu** Most Recent 1 month 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** 1 month, 3 weeks 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** 3 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

 **binrayelias** 4 months, 3 weeks ago

B since each leaf is needed to connect to each spine and not connect to any leaf switch

upvoted 1 times

 **DixieNormus** 9 months 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** 9 months ago

Selected Answer: C

Answer C is correct

<https://community.fs.com/blog/leaf-spine-with-fs-com-switches.html>

upvoted 2 times

 **Request7108** 5 months, 2 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

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

 **Tidestar** Highly Voted 2 years, 11 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 ago

guys, note, the question asks, what is the "primary" effect. Which would be D

upvoted 21 times

 **JWMcInSC** 2 years, 11 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 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 process, i think its a tricky question

upvoted 3 times

 **Isuzu** Most Recent 1 month 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** 1 month, 2 weeks 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** 5 months ago

Selected Answer: D

switch doesn't need to reload for portfast to take effect

upvoted 2 times

 **jibon_22** 5 months, 4 weeks ago

Look at the words "primary effect". Correct answer is:

> B

upvoted 1 times

 **AppleShredder011** 8 months, 2 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

 **ZUMY** 1 year ago

D is correct!

upvoted 1 times

 **jahinchains** 1 year, 1 month ago

Selected Answer: D

there is no need for a switch to be reloaded B is not correct

upvoted 2 times

 **Bigc0ck** 1 year, 2 months ago

Selected Answer: D

Just pick D and stop thinking so hard on it. If people in India can pass this, so can you lol. Better hurry up and learn cloud stuff and automation, because vanilla IT is going the way of the dinosaurs

upvoted 1 times

 **bitree** 1 year, 1 month ago

People in India have brains primed for memorization from the school system, and probably face economic pressures and levels of cutthroat competition I will never know. People who live in flyover country, USA should not insinuate about people in India to compare to other peoples.

upvoted 4 times

 **onikafei** 1 year, 3 months ago

Selected Answer: D

D is correct

upvoted 1 times

 **onikafei** 1 year, 3 months ago

To further elaborate:

A and B are essentially answers for a when you start it up. But its not asking for this in the question, it is asking for the primary effect.

so scratch A and B out.

Then from there I look primarily on D

upvoted 1 times

 **Vinarino** 1 year, 4 months ago

This Q is reiterated again, omitting "when the switch is reloaded" - THEN D is correct.

After entering the command What is your desired (planned) result a week later?

upvoted 1 times

 **pfxwmneydgyqyhekw** 1 year, 5 months ago

"You can use Port Fast on interfaces connected to a single workstation or server to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge."

This is not the same as reducing spanning tree convergence time.

upvoted 6 times

 **YessufAddis** 1 year, 5 months ago

I believe the answer is B. Portfast is a feature for edge ports and it doesn't have anything to do with spanning-tree convergence. Spanning-tree convergence is the issue of other ports which switches are connected with other switches. Thus, portfast is a feature to bring ports connected to user devices to forwarding states as quick as possible.

upvoted 4 times

 **ostralo** 2 years ago

B is wrong hence the answer is D.

the spanning-tree portfast command doesn't put whatever ports into forwarding state as soon as the switch is reloaded. normally we configure portfast on ports where end devices are connected to, and along with the BPDU guard.

upvoted 2 times

 **ZUMY** 2 years, 1 month ago

D is correct

upvoted 5 times

 **edward99** 2 years, 2 months ago

For my understand, the answer is D since although the port bypass the other states like blocking, listening, learning and go to forwarding states, this led to reduce the converges time the switch may use from blocking to forwarding states

upvoted 2 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 `spanning-tree portfast trunk`

 **ratu68** 11 months, 1 week ago

Selected Answer: D

There was no mention of BPDU Guard so answer is D !

upvoted 3 times

 **ZUMY** 1 year ago

D is correct!

upvoted 2 times

 **kijken** 1 year, 4 months ago

I think this is B. The port will go in error disabled state when receiving PBDU messages

upvoted 2 times

 **kijken** 1 year, 4 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 the case. So answer

D is correct

upvoted 26 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 2 years, 9 months ago

WLAN Quality of Service (QoS) list:

- Platinum (voice)
- Gold (video)
- Silver (best effort) is the default value.
- Bronze (background)

upvoted 29 times

✉  **Belinda** 1 year, 2 months ago

Thanks

upvoted 2 times

✉  **Samitha** Highly Voted 2 years, 11 months ago

Bronze--->FTP
Gold----->Video
Platinum--->Voice
upvoted 7 times

✉  **Franklin82** Most Recent 7 months, 1 week 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 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** 1 year, 12 months ago

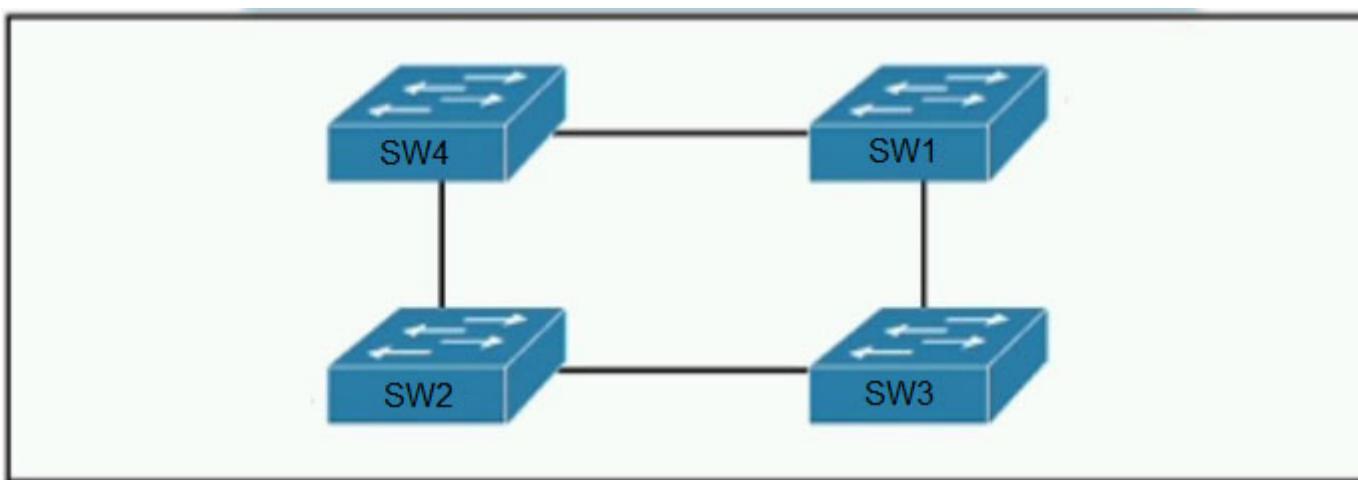
Yes Platinum is correct.
upvoted 1 times

✉  **JWMcInSC** 2 years, 11 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

Ali526 Highly Voted 2 years, 5 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 12 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

dearc Most Recent 2 months, 1 week 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 2 months, 2 weeks ago

not sure why i was thinking 0(zero) is latter O
upvoted 1 times

Antol15 1 month, 2 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

DUMPlidore 5 months, 4 weeks ago

Selected Answer: C

C correct answer
upvoted 2 times

✉ **BlankNothing1** 1 year 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 ago

I think your idea is great for work, but I don't think we can use excel for the exam.
upvoted 6 times

✉ **Cyberops** 1 year, 1 month ago

the Switch which has the lowest Mac address which is SW3
correct answer is C
upvoted 2 times

✉ **bmatthee01** 1 year, 3 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** 1 year, 10 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** 1 year, 10 months ago

maybe correct answer - B?
1a = 26
upvoted 2 times

✉ **Matalongo** 2 months, 3 weeks ago
but 22 in hexadecimal is 34 in decimal
upvoted 1 times

✉ **AWSFastLearner** 1 year, 9 months ago

yes, $1A = 26 = 1 \times 16^1 + 10 \times 16^0$. but $22 = 2 \times 16^1 + 2 \times 16^0 = 34$.
so $1A < 22$. correct answer is C.
upvoted 5 times

✉ **ZUMY** 2 years, 1 month ago

C is correct
Least MAC value is selected incase of all the interface - RootBridge priorities are same
upvoted 3 times

✉ **oooMooo** 2 years, 1 month 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, 3 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, 3 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, 3 months ago

D is the correct answer

upvoted 2 times

✉️  **lordnano** 2 years, 3 months ago

Without a statement why you would choose an other answer, your comment can't help anybody

upvoted 9 times

Question #182

Topic 1

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:

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
1A-76-3F-7C-57-DF	Network address
192.168.1.0	

Correct Answer:

192.168.1.1

192.168.1.20

192.168.1.254

192.168.1.255

B8-76-3F-7C-57-DF

1A-76-3F-7C-57-DF

192.168.1.0

192.168.1.255

192.168.1.1

192.168.1.20

192.168.1.254

B8-76-3F-7C-57-DF

192.168.1.0

✉  **johnnd**  1 year, 4 months ago

Response with connection arrows:

<https://i.imgur.com/qC7SZaH.png>

upvoted 8 times

✉  **Adewal**  1 year, 4 months ago

The answer is very straight forward with a good understanding of IP/subnetting.

upvoted 5 times

✉  **Isuzu**  1 month ago

Same as Q153

upvoted 1 times

✉  **ZUMY** 1 year ago

Given answers are correct!

upvoted 4 times

Question #183

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, 2 months ago

The command should be:

SW(config)#lldp tlv-select port-description

upvoted 26 times

 **IxlJustinlxl** Highly Voted 2 years 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, 5 months ago

How about lldp transmit and lldp receive int-config commands?

upvoted 7 times

 **[Removed]** Most Recent 3 months, 3 weeks ago

I think this question will not be on ccna 200-301 exam topic.

upvoted 3 times

 **Anas_Ahmad** 5 months, 2 weeks ago

Switch(config)#lldp tlv-select port-description

this command exist

upvoted 2 times

 **guisam** 5 months, 4 weeks 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 1 times

 **TA77** 1 year 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 ago

Going with D

The command should be:

SW(config)#lldp tlv-select port-description

upvoted 1 times

 **dave1992** 1 year, 5 months ago

if you were configuring a port description, wouldnt you need to be at the (config-if) level?

upvoted 5 times

 **onikafei** 1 year, 4 months ago

Tested the code multiple times in training. Renaming is just done with the config command. I almost put it in the category of message of the day

upvoted 1 times

 **kokoyul** 1 year, 8 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, 1 month ago

Me parece que nos están intentando a decir lo mismo porque el comando no es correcto.

upvoted 1 times

 **Raymond9** 2 years, 6 months ago

badly written: TLV should be written as Type, Length, Value, or Type-Length-Value, since there are three different columns!

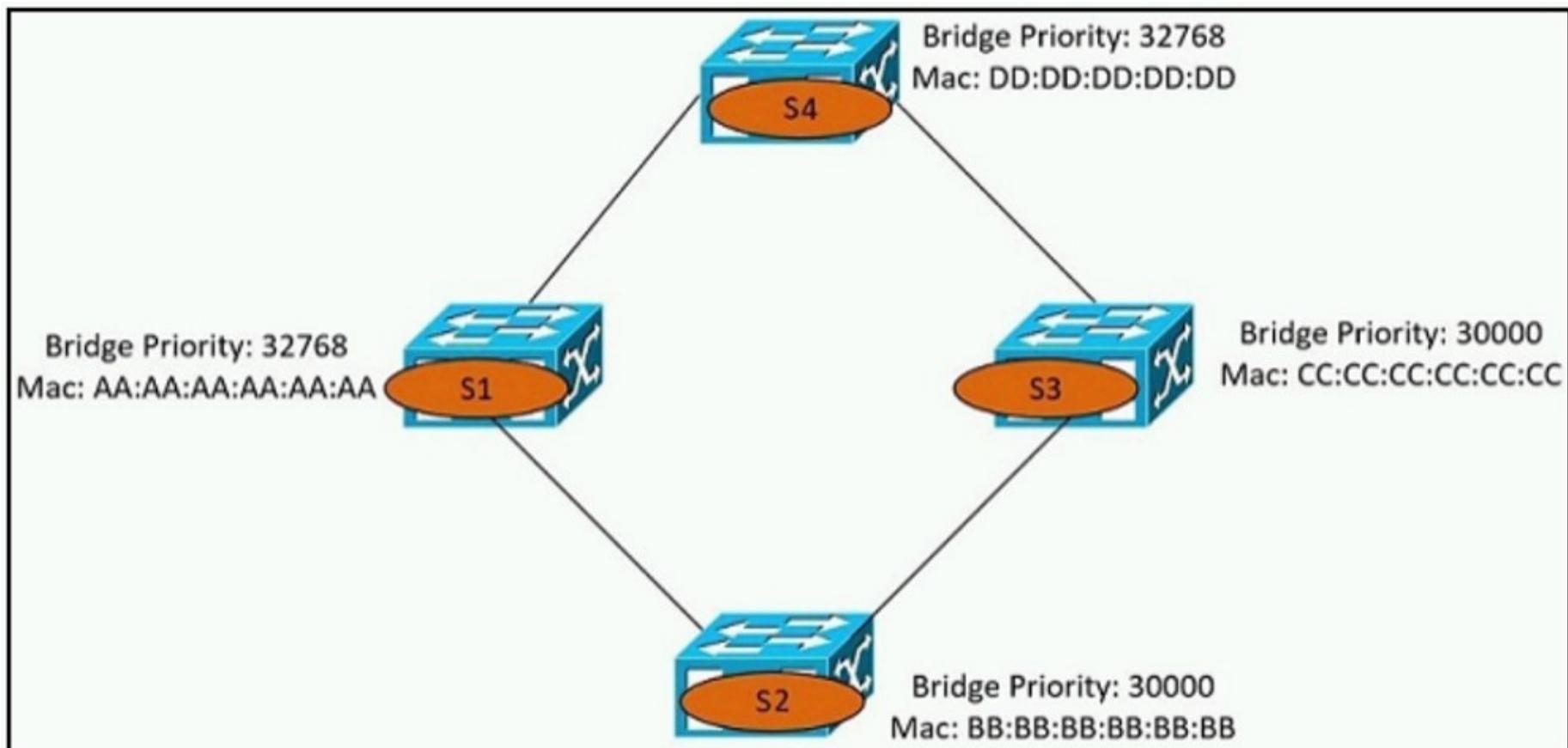
upvoted 4 times

 **Ali526** 2 years, 5 months ago

Many of the questions are.

upvoted 3 times

Question #184



Refer to the exhibit. Which switch becomes the root bridge?

- A. S1
- B. S2
- C. S3
- D. S4

Correct Answer: B

Ali526 Highly Voted 2 years, 5 months ago

B is correct. The lowest value of priority + MAC.
upvoted 19 times

pianetaperez 2 years, 3 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, 8 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 10 times

ThomasSmith 1 month ago

How can the priority be 32768? With default VLAN 1 it should be 32769!
upvoted 1 times

MISS4 1 year, 7 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 question, 30000 seems valid.

upvoted 9 times

melmiosis Most Recent 7 months, 2 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** 5 months, 3 weeks ago

C is more than B

upvoted 1 times

✉ **ZUMY** 1 year ago

B is the answer

Lowest values are selected (Priority + MAC)

upvoted 1 times

✉ **onikafei** 1 year, 4 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, 4 months ago

Selected Answer: B

correct

upvoted 1 times

✉ **Hodicek** 1 year, 6 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

 **Hemn1990** Highly Voted 2 years, 8 months ago

B i correct, note always
upvoted 38 times

 **Gifu** Highly Voted 2 years, 6 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 24 times

 **ian77ex** 1 year, 3 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 10 times

 **dipanjana1990** 1 year, 2 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

 **Jorro99404** Most Recent 1 week ago

Selected Answer: B

Who votes for C? And why?
'root primary' command will set the bridge priority to 24576
upvoted 1 times

 **Shun5566** 2 weeks, 1 day ago

Selected Answer: B
B is always correct
upvoted 1 times

 **Ioannis_Vos** 1 month 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 1 times

 **FALARASTA** 1 month, 2 weeks 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** 1 month, 2 weeks 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** 1 month, 2 weeks ago

I wonder which books I've been reading because, when the priority 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** 2 months, 1 week 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** 2 months, 3 weeks 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** 2 months, 3 weeks 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** 2 months, 4 weeks 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 1 times

 **iMo7ed** 3 months, 3 weeks ago

Selected Answer: B

It's B

upvoted 1 times

 **[Removed]** 3 months, 3 weeks ago

For the official answer, I think C is the one.

upvoted 1 times

 **Anas_Ahmad** 4 months, 2 weeks ago

Selected Answer: B

priority 0 command ensures the bridge priority takes precedence over all other priorities.

upvoted 2 times

sf0 4 months, 2 weeks ago

Definitely "B" would be the correct option. However, nowhere is mentioned that all these commands would be used on the same network. The question is "which command ensures that the switch is always the root", C would make sure it is root even if two switches has priority 0

upvoted 1 times

cormorant 5 months, 3 weeks ago

is 'c' cisco's official answer? can i go with b in teh actual test?

upvoted 2 times

sol_ls95 4 months, 2 weeks ago

x2 same question

upvoted 1 times

leooel 5 months, 3 weeks ago

Selected Answer: B

B 0 is correct

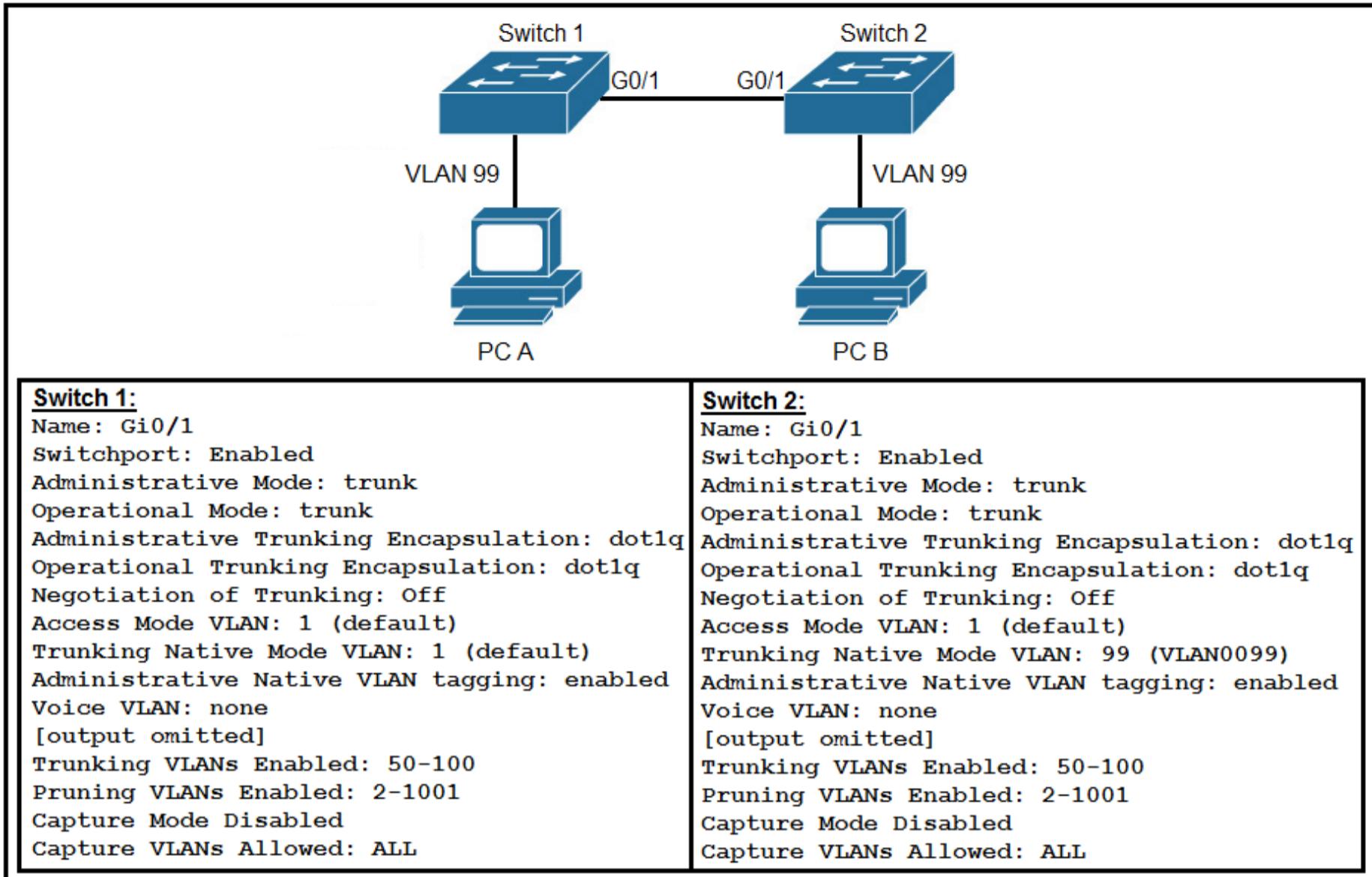
upvoted 1 times

pat1815 6 months, 1 week ago

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. So Correct answer should B

upvoted 1 times

Question #186



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

Kane4555 Highly Voted 1 year, 4 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 8 times

dipanjana1990 10 months, 2 weeks 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

FALARASTA Most Recent 1 month, 2 weeks ago

Selected Answer: D

There is VLAN Mismatch. Remember there is no any intervlan routing on the two switches thus minimising the chance of communication.

Answer is D

<https://www.youtube.com/watch?v=klqpX6U-JY>

upvoted 1 times

elixirwell 2 months, 1 week 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** 10 months, 2 weeks 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** 9 months, 1 week 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_Babaram** 11 months, 2 weeks ago

D IS CORRECT

upvoted 2 times

 **dipanjana1990** 10 months, 2 weeks 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** 7 months, 2 weeks ago

B is incorrect

upvoted 1 times

 **ZUMY** 1 year ago

D is correct

upvoted 2 times

 **dipanjana1990** 10 months, 2 weeks 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, 1 month 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 ping...

upvoted 1 times

 **dipanjana1990** 10 months, 2 weeks 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, 2 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 1 times

 **PoBratsky** 1 year, 5 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, 5 months ago

I'm so sorry. Answer is D. Because PC B in native VLAN. So ping will be failure.

upvoted 1 times

 **dipanjana1990** 10 months, 2 weeks 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, 6 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, 4 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** 10 months, 2 weeks 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 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, 1 month 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, 2 months ago

how is there a native vlan mismatch ?

upvoted 2 times

 **NerdyNerdy** 2 years, 2 months ago

Trunking native vlan on Sw1 is 1, while native vlan on Sw2 is 99

upvoted 6 times

 **dipanjana1990** 10 months, 2 weeks 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, 4 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, 4 months ago

any Explanation to this ?

upvoted 2 times

Question #187

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 for 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 *last resort* 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, 8 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 = Applied to the WLAN for wireless client communication

upvoted 15 times

 **DUMPLedore** Highly Voted  5 months, 4 weeks ago

I think given answers are correct
upvoted 6 times

 **lucky1559** Most Recent ⓘ 1 year, 9 months 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 ago

All the answers are correct
upvoted 4 times

 **SScott** 1 year, 10 months 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

 **poovnair** Highly Voted 🌟 2 years, 8 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 9 times

 **Mauro_Babaram** Most Recent ⓘ 11 months, 2 weeks ago

CORRECT IS C
upvoted 3 times

 **ZUMY** 1 year ago

C is correct!
upvoted 2 times

Question #189

Topic 1

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	Holddown	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, 7 months ago

B is correct
upvoted 6 times

 **SScott** 1 year, 10 months 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 1 year, 11 months ago

B is Correct
upvoted 5 times

 **mt05** Most Recent 3 months ago

why not D?
upvoted 1 times

 **xbobdan** 4 months, 1 week ago

why all the neighbors have the same ID? can this be right?
upvoted 1 times

 **ZUMY** 1 year 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 `on` 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 2 years, 11 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 28 times

 **CJ32** Highly Voted 2 years, 10 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 18 times

 **Sonieta** 1 year, 7 months ago

Very good explanation to remember, thanks!!

upvoted 1 times

 **linuxlife** Most Recent 2 months, 3 weeks 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** 11 months, 3 weeks 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 ago

B is correct!

upvoted 1 times

 **ZUMY** 1 year ago

B is correct

upvoted 1 times

 **Hodicek** 1 year, 6 months ago

NO negotiation mode= ON

NO = ON

upvoted 4 times

 **Bach999** 2 years, 6 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, 8 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 “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.

 **syed5** Highly Voted 2 years, 11 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, 8 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 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**  1 year, 9 months 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 19 times

⊕  **DannySprings**  2 years, 10 months ago

correct

upvoted 5 times

⊕  **GreatDane**  11 months, 3 weeks 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 ago

C & D are correct

upvoted 4 times

⊕  **Shamwedge** 1 year, 5 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 1 year, 9 months 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, 2 months ago

who's doing their CCNA this month coming? April.

upvoted 4 times

Joe_Q 2 years, 2 months ago

May 13th.

upvoted 4 times

Ray12345 2 years, 1 month ago

May 17th

upvoted 3 times

Shehan 1 year, 9 months ago

Did you pass? were the questions same ?

upvoted 4 times

KAT 2 years, 3 months ago

kindly, any explanation

upvoted 2 times

Jacob_Davis18 2 years, 3 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, 5 months ago

So one help me out here. What is the profile name?

upvoted 4 times

SumonHossain 2 years, 8 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

✗ **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

✉  **Ettmoh** Highly Voted 2 years, 9 months 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, 8 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 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>

 **JWMcInSC** Highly Voted 2 years, 11 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 18 times

 **Gelo29** Highly Voted 2 years, 8 months ago

Is VTP still in 200-301 exam? I'm confused.

upvoted 10 times

 **Aie_7** 4 months, 2 weeks ago

It's only mentioned, but i never read "vtp mode transparent" in Network Academy in 2023

upvoted 2 times

 **ZUMY** Most Recent 12 months ago

D is correct

upvoted 2 times

 **netlol** 1 year, 4 months ago

Sorry, why not C?

upvoted 4 times

 **guisam** 5 months, 3 weeks ago

...all locally configured VLANs...

locally

upvoted 1 times

 **Keif** 1 year, 7 months ago

Just took exam 200-301 I can confirm very similar question was on the exam

upvoted 6 times

 **jesserdc16** 1 year, 7 months ago

DId u pass your test?

upvoted 6 times

 **tweesgger** 1 year, 7 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** 7 months, 2 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** 6 months, 4 weeks ago

Lmao exactly.
upvoted 1 times

✉  **DonnerKomet** 1 year, 9 months ago

Guys, but VTP is not out of scope of this 200-301 exam? The topic was removed from CCNA 200-301, isn't?
upvoted 4 times

✉  **GreatDane** 2 years, 7 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, 8 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, 8 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 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, 7 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

```

SW1#sh lacp neighbor
Flags: S - Device is requesting Slow LACPDU
      F - Device is requesting Fast LACPDU
      A - Device is in Active mode          P - Device is in Passive mode

Channel group 35 neighbors

Partner's information:

      LACP port
Port  Flags Priority Dev ID           Admin Oper Port  Port
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 `Flags` are SP. `P` 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 `Port State` in the exhibit is `0x3c` (which equals to `00111100` in binary format). Bit 3 is `1` which means the ports are synchronizing -> the ports are working so the local ports should be in Active mode.

 **DatBroNZ** Highly Voted 1 year, 8 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 17 times

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

B is correct
upvoted 9 times

 **Giuseppe_001** 2 years ago

sure? because the flag is set in SP
upvoted 2 times

 **jehangt3** 2 years 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". Whether your 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 ago

i got a mistake sorry
upvoted 6 times

 **jehangt3** 2 years ago

you didn't make a mistake, you were right the first time.. B is the answer
upvoted 3 times

 **linuxlife** Most Recent 2 months, 3 weeks 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** 9 months, 1 week ago

in which mode is the SW1 port channel configured?
SP = Passive
upvoted 1 times

RoVasq3 9 months, 3 weeks ago

Selected Answer: B

B is the correct one

upvoted 1 times

vuhidus 10 months, 1 week ago

Selected Answer: B

BBBBB based on the neighboring status

upvoted 1 times

hp2wx 10 months, 3 weeks 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 11 months, 4 weeks 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 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 9 months, 1 week 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, 1 month 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

Scrvfce 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

Halop 1 year, 1 month ago

It shows the status of neighbors.B is correct.

upvoted 1 times

JSDH 1 year, 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

qasawq 1 year, 3 months ago

answer is B

upvoted 1 times

AndersonMr 1 year, 4 months ago

Selected Answer: B

SW2 is passive, so SW1 has to be active.

upvoted 1 times

Hyay 1 year, 6 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, 4 months ago

Sorry but you're wrong

upvoted 2 times

ScorpionNet 1 year, 1 month 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, 6 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

 **ayd33n** Highly Voted  2 years, 10 months 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 28 times

 **linuxlife** Most Recent  2 months, 3 weeks 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** 2 months, 3 weeks ago

And yes, D is the right answer

upvoted 1 times

 **icecool2019** 8 months ago

According to the DTP matrix:

Dynamic Auto		Dynamic Desirable		Trunk		Access
Dynamic Auto		Access		Trunk		Access
Dyn Desirable		Trunk		Trunk		Access
Trunk		Trunk		Trunk		Limited Connectivity (LC)
Access		Access		Access		Access

upvoted 1 times

 **lock12333** 11 months, 3 weeks ago

Selected Answer: D

ddddddddd

upvoted 2 times

 **ZUMY** 2 years, 1 month ago

D is correct

upvoted 4 times

 **Nhan** 2 years, 3 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

 **GreatDane** Highly Voted 2 years, 7 months ago
"31 Days Before Your 200-301 CCNA Exam"

Page 85, right under figure 26-1.

upvoted 10 times

 **ayd33n** Highly Voted 2 years, 10 months 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 1 month 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** 1 year, 11 months ago

B is correct

upvoted 3 times

 **ZUMY** 2 years, 1 month 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

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

A is correct

upvoted 8 times

 **karemAbdullah** Highly Voted 2 years, 8 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

 **DUMPlidore** Most Recent 5 months, 4 weeks ago

Selected Answer: A

Given answer is correct

upvoted 2 times

 **hasbulla01** 6 months, 4 weeks ago

Selected Answer: A

A is correct only for discard

upvoted 1 times

 **Shamwedge** 1 year, 7 months ago

Wouldn't it be A for any 801.11 Wi-Fi infrastructure?

upvoted 2 times

 **Nicocisco** 1 year, 3 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 ago

answer is A

upvoted 4 times

 **Artengineer** 3 years ago

the correct answer is C

upvoted 1 times

 **mashiur** 3 years ago

I don't think so..the correct answer is A

upvoted 7 times

 **Ali526** 2 years, 5 months ago

Agreed.

upvoted 3 times

 **ayd33n** 2 years, 10 months 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

 **Cixxcv420** 2 years, 8 months ago

802.11b is support 2.4ghz on 11mbps

upvoted 1 times

 **SUKABLED** 2 years, 4 months ago

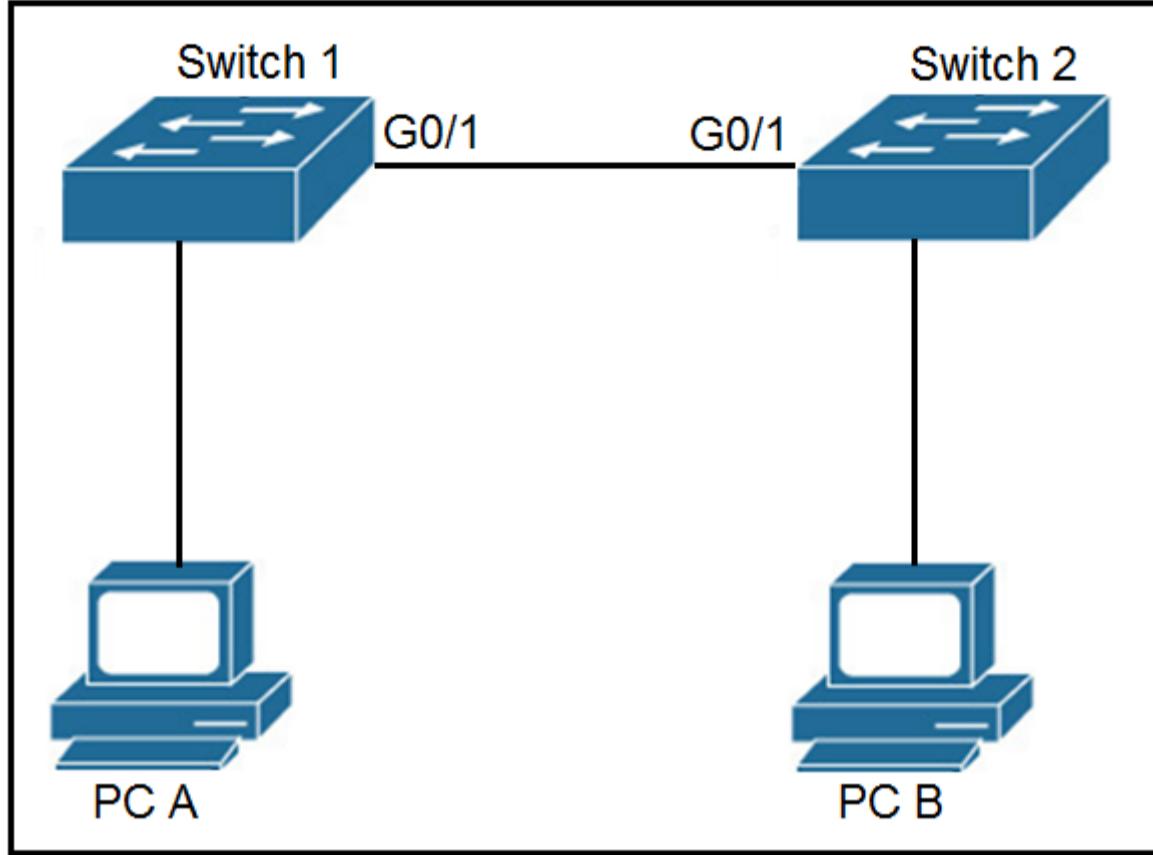
Not enough data to conclude C...for this question- definitely A!

upvoted 3 times

Question #199

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

ZUMY Highly Voted 2 years, 1 month 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, 3 months ago

<https://www.summit360.com/2017/08/30/vlans-types-benefits/>

D is correct

upvoted 5 times

LeonardoMeCabrio Most Recent 5 days, 13 hours ago

Selected Answer: D

D Correct

upvoted 1 times

gc999 2 months, 3 weeks 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 5 months, 2 weeks ago

D IS CORRECT

upvoted 2 times

Yunus_Empire 6 months ago

D is correct

upvoted 3 times

 **helmerpach** 1 year, 5 months ago

D is correct

upvoted 2 times

 **Scipions** 2 years, 1 month ago

Grazie a sta ceppa la nativa ha il non taggato

upvoted 4 times

 **echarles10** 2 years, 5 months ago

D is correct

upvoted 3 times

Question #200

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

 **Dave861** Highly Voted 2 years, 11 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 59 times

 **Ali526** 2 years, 4 months ago

Not only that; the question asks for layer3. When you put in switchport, it becomes layer 2.

upvoted 18 times

 **wizcas** 2 years, 6 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 2 years, 12 months ago

The right answer should be C and D

upvoted 18 times

 **elixirwell** Most Recent 2 months, 1 week 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** 10 months, 1 week ago

C & D for sure are the correct ones.

upvoted 2 times

 **ptfish** 10 months, 1 week 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** 10 months, 1 week ago

Selected Answer: CD

Should be CD
upvoted 1 times

 **ZUMY** 12 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 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, 1 month ago

Yep C and D is correct because IP is Layer 3 and Trunking is Layer 2
upvoted 1 times

 **LordScorpius** 1 year, 1 month 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, 2 months ago

Selected Answer: CD

CD is correct
upvoted 1 times

 **ismatdmour** 1 year, 3 months ago

Selected Answer: CD

E is incorrext, it makes it layer 2
upvoted 2 times

 **HarLikon** 1 year, 4 months ago

Selected Answer: CD

Aswers are C,D
upvoted 3 times

 **SparkySM** 1 year, 4 months ago

Selected Answer: CD

it should be c and d
upvoted 4 times

 **LilGhost_404** 1 year, 4 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, 5 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

The question states it should be an L3 Ether-Channel, not L2?

upvoted 2 times

 **Naj_Val** 1 year, 5 months ago

The question states it should be an L3 Ether-Channel, not L2?

upvoted 2 times

 **Rockrl** 1 year, 5 months ago

Selected Answer: CD

C&D are the correct answer, Layer 3 etherchannel must be configure with noswitchport command
upvoted 2 times

Question #201

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

✉ **legitornot22** Highly Voted 2 years, 2 months ago

Desirable/Auto (PAGP)
Active/Passive (LACP)
upvoted 29 times

✉ **shakyak** 1 year, 6 months ago

L-AC-P has "AC" in the middle which is easier to remember as an Active :D
upvoted 37 times

✉ **Paplewska** Highly Voted 2 years, 1 month 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 1 month, 2 weeks ago

Selected Answer: A

why question has together word?

Correct Answer is: A

upvoted 1 times

✉ **icecool2019** 8 months ago

LACP(vendor natural)form a Ether channel = (Active & Active) / (Active & Passive) / (Passive & Active)
PAgP (CISCO) form a Ether channel = (Desirable & Desirable) / (Desirable & Auto) / (Auto & Desirable)
upvoted 2 times

✉ **ScorpionNet** 1 year, 1 month ago

A and D is right
Easy to know if familiar to Etherchannel
upvoted 1 times

✉ **ScorpionNet** 1 year, 1 month ago

I mean C sorry XD.
upvoted 1 times

✉ **ismatdmour** 1 year, 3 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). These 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 together (on the same switch) the second one will replace the first.

upvoted 2 times

 **Vinarino** 1 year, 5 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, 1 month 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, 1 month ago

PAgP- Disirable/Auto (Link formation)
LACP- Active/Active or Active/Passive (Link formation)

upvoted 2 times

Question #202

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 ago

Shouldn't the answer be C.
The traffic from the workstation is untagged. and there is no indication that the native vlan is vlan1
upvoted 9 times

 **NORLI** 1 year, 1 month ago

By default all ports are in vlan1 until they are configured to be in a separate vlan
upvoted 5 times

 **Unemaru** 2 years 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 explicitly 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** 1 year, 10 months 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](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  4 months, 2 weeks ago

shouldnt the answer be A since the command "switchport mode access" is missing?
upvoted 2 times

 **icecool2019** 8 months ago

Answer B is correct
upvoted 1 times

 **Ronild** 8 months, 4 weeks ago

Should the configured port have "switchport mode access" config in order for B to be the correct answer?
upvoted 2 times

 **michael1001** 5 months, 3 weeks ago

Yes - quite annoying and I got caught there too.
upvoted 1 times

□  **GreatDane** 11 months, 3 weeks 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** 7 months ago

Bro(or Sis), I love how you normally reference your responses with a clear cut and concise statements. Thank you!

upvoted 1 times

□  **ZUMY** 12 months ago

Going with B

upvoted 1 times

□  **babaKazoo** 1 year, 6 months ago

B because the native vlan defaults to 1 if its not changed.

upvoted 2 times

□  **NZIAKOU** 2 years, 2 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, 5 months ago

Untagged and native VLAN go together, so VLAN 5. However, 'switchport mode trunk' and switchport access VLAN 11, no good.
upvoted 16 times

✉  **onikafei** Highly Voted 1 year, 4 months ago

Always remember native=untagged lol
upvoted 8 times

✉  **Smaritz** Most Recent 1 year, 3 months ago

Trunk and Access in one?
upvoted 4 times

✉  **AlexMD** 1 year, 7 months ago

C is correct answer
upvoted 1 times

✉  **ZUMY** 2 years, 1 month ago

C is correct
There is an ambiguity in the question
upvoted 4 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 their 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, 1 month ago

A is correct

```
#lldp run - Globally Enable  
#no lldp run - Globally Disable  
#lldp Recieve -To receive LLDP packets  
#lldp Transmit - To transmit LLDP packets
```

upvoted 14 times

 **linuxlife** Most Recent 2 months, 3 weeks 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** 2 months, 3 weeks 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** 11 months, 3 weeks 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, 2 months ago

But on Cisco it is cdp run and the question says „cisco iOS“

upvoted 3 times

✉ **jose01210** 1 year ago

I think same

upvoted 1 times

✉ **bmatthee01** 1 year, 3 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** 1 year, 10 months 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** 1 year, 8 months ago

Can someone please clarify, isn't LLDP disabled by default on Cisco devices? It is CDP enabled by default.

upvoted 4 times

✉ **Adaya** 1 year, 12 months ago

Thank for the explanation

upvoted 2 times

Question #205

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

✉  dearc 2 months 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 2 times

✉  Dutch012 3 months, 2 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 2 times

✉  iMo7ed 3 months, 3 weeks ago

Selected Answer: D

it's D

upvoted 1 times

✉  sol_ls95 4 months, 2 weeks ago

Selected Answer: D

d correct answer

upvoted 1 times

Question #206

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 `show cdp neighbor detail` command. If the neighbor does not have an IP address then CDP still operates without any problem. But the IP address of that neighbor is not provided.

 **ddban** Highly Voted 2 years, 1 month 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 36 times

 **Bhrino** 3 weeks, 5 days ago

Packet tracer isn't really reliable for something so in theory I believe it should be c

upvoted 3 times

 **Nicocisco** 1 year, 3 months ago

yeah tested in lab to, and the switch don't see other interface of my router

upvoted 4 times

 **Gere** Highly Voted 2 years, 3 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 22 times

 **Avalon1** 2 years, 2 months ago

What is the another interface? The C is correct. CDP does not need IPs to work normally

<https://learningnetwork.cisco.com/s/question/0D53i00000Kt3Mp/how-does-cdp-work-without-ip-addresses>

upvoted 6 times

 **oooMooo** 2 years, 1 month 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 4 times

 **Nicocisco** 1 year, 3 months ago

When tested in the lab, the behaviour described in the link does not occur

upvoted 7 times

 **funkymonksarmy** Most Recent 2 weeks, 6 days ago

I checked it and it shows ip address of another interface

B is correct

upvoted 1 times

 **Jorro99404** 3 weeks, 1 day 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** 1 month ago

Selected Answer: C

answer C is correct

upvoted 1 times

 **Kyoxi** 1 month, 2 weeks ago

Selected Answer: C

c is correct
upvoted 1 times

 **dearc** 2 months ago

Selected Answer: C

<https://learningnetwork.cisco.com/s/question/0D53i00000Kt3MpCAJ/how-does-cdp-work-without-l3-addresses>
upvoted 1 times

 **elixirwell** 2 months, 1 week 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 1 times

 **linuxlife** 2 months, 3 weeks 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** 2 months, 3 weeks 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 1 times

 **daddydagoth** 3 months, 2 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 2 times

 **Dutch012** 3 months, 2 weeks ago

Selected Answer: C

the answer would be B, in the assumption that the adjacent device has another interface with an IP address, but the thing is the question didn't mention another IP interface for the adjacent device, so it's safer to choose C.

upvoted 1 times

 **[Removed]** 3 months, 3 weeks ago

I think the correct answer is C
upvoted 1 times

 **4aynick** 4 months, 3 weeks ago

Selected Answer: B

I was check it in gns3. Correct B
upvoted 3 times

 **khird** 5 months ago

I think C is the answer, as the question says "The device is not configured" meaning any interface on that device has no IP
upvoted 1 times

 **jibon_22** 5 months, 4 weeks ago

100% correct: do it on packet tracer, then you will understand
> C
upvoted 1 times

 **rivera82** 6 months ago

Selected Answer: C

Although CDP is a Layer 2 protocol but we can check the neighbor IP address with the "show cdp neighbor detail" command. If the neighbor does not have an IP address then CDP still operates without any problem. But the IP address of that neighbor is not provided.
upvoted 2 times

Question #207

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:

Dynamic RF Feature	Controller provides centralized management of users and VLANs
Easy Deployment Process	Access points auto adjust signal strength
Optimized user performance	Controller image auto deployed to access Points
Easy upgrade process	Controller uses loadbalancing to maximize throughput

Correct Answer:

Dynamic RF Feature	Easy Deployment Process
Easy Deployment Process	Dynamic RF Feature
Optimized user performance	Easy upgrade process
Easy upgrade process	Optimized user performance

✉  **IxlJustinIxl**  1 year, 12 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 7 times

✉  **Sten111**  1 year, 11 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 6 times

✉  **SScott** 1 year, 10 months 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 affecting users nor VLANs. The answers provided are correct.

https://www.cisco.com/web/AP/wireless/pdf/Benefits_of_centralizedWlan.pdf

upvoted 2 times

✉  **everchosen13**  8 months, 2 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 4 times

✉  **splashy** 8 months, 2 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, 4 months ago

answer with connected points:
<https://i.imgur.com/vbuTKnI.png>

upvoted 5 times

 **shakyak** 1 year, 7 months ago

HINT: Easy-> Central

Dynamic->Auto

Upgrade->Deploy

Max ->Throughput

upvoted 4 times

 **shakyak** 1 year, 6 months ago

Max->Optimize?

upvoted 4 times

 **jehangt3** 2 years 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

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 "passive" will wait for the other side to become "Active" for the Etherchannel to be established.

PAgP is Port-Aggregation Protocol. It is Cisco's proprietary protocol. The modes are On, Desirable or Auto. Desirable or "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
```

  **hokieman91**  2 years, 4 months ago

"A" ---- Answer given is correct. Actually a good question since this verifies the knowledge of how LACP works - remember a "Passive" interface "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 15 times

  **bobert** 2 years, 2 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, 2 months ago

correction ... read again and A is correct

upvoted 2 times

  **sdokmak** 1 year, 11 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, 3 months ago

Good clarity

upvoted 2 times

  **SScott** 1 year, 10 months ago

Right, A is the most direct answer Passive.

<https://www.ccna6rs.com/6-2-4-packet-tracer-configure-etherchannel-answers/>

upvoted 1 times

  **Bhrino**  3 weeks, 5 days ago

Selected Answer: A

I think the wording of the question is weird but the reason it's "Passive" is because the question asks which mode will only activate LACP if it detects LACP which is "Passive". "Passive" in a way listens to what it's being told.

upvoted 1 times

✉ **[Removed]** 3 months, 3 weeks ago

The question is not clear

upvoted 3 times

✉ **gc999** 2 months, 3 weeks 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** 12 months ago

A is correct

upvoted 1 times

✉ **ismatdmour** 1 year, 3 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, 4 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, 4 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, 4 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, 5 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, 6 months ago

LACP ACTIVE PASSIVE, IN THE QUESTION ONE IS DETECTED SO IT IS ACTIVE SO OTHER SHOULD BE PASSIVE

upvoted 2 times

✉ **ProgSnob** 1 year, 7 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 4 times

✉ **Ciscoman021** 5 months ago

you are not alone. :)

upvoted 2 times

✉ **ZUMY** 2 years, 1 month ago

A is correct

upvoted 4 times

✉ **asd34534** 2 years, 2 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, 4 months ago
The correct answer should be E... "Active"
upvoted 3 times

 **gc999** 2 months, 3 weeks ago
Agree. I set the mode to "Active", so it can "detected" the other end.
upvoted 1 times

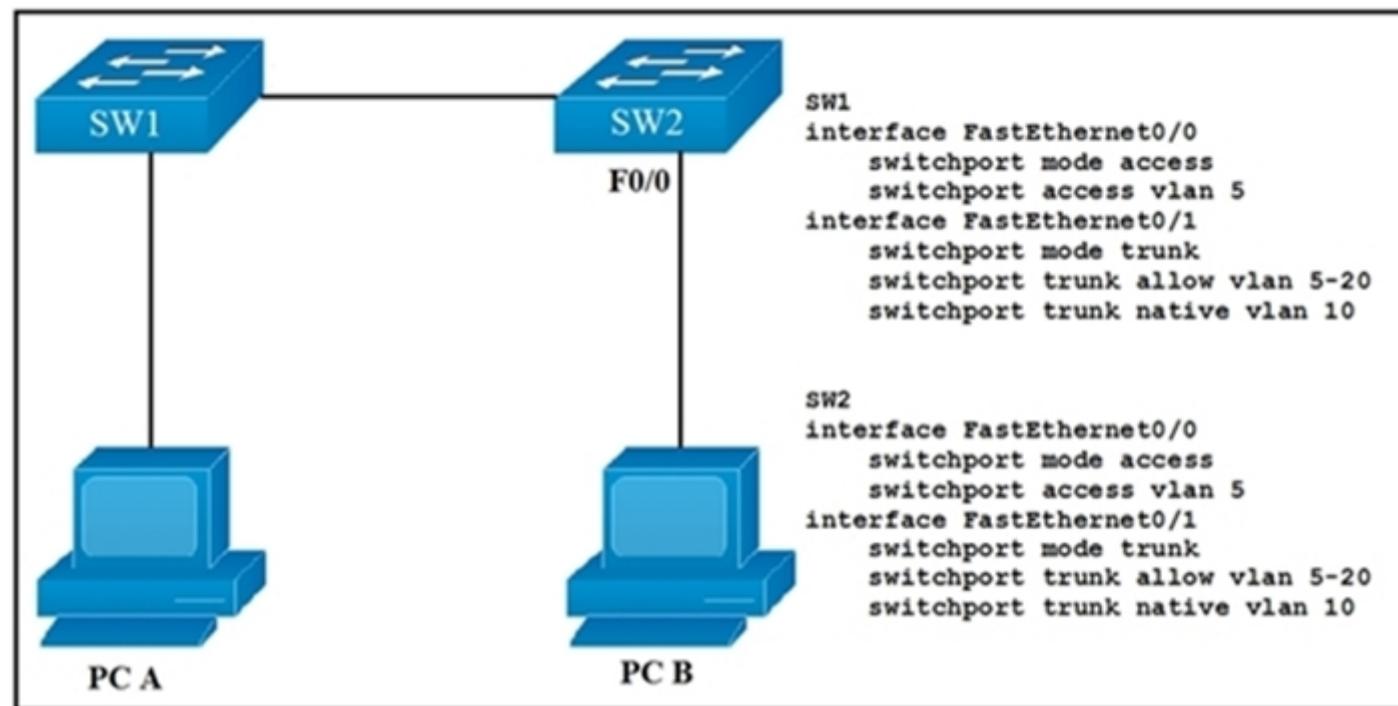
 **Taps** 2 years, 4 months ago
The word passive means the opposite: That it has found a connection and its up and ready. Active is also the opposite: It doesn't have a connection and so its not looking for one.
upvoted 3 times

 **Zerotime0** 2 years, 4 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, 2 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

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

ZayaB Highly Voted 2 years, 3 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 64 times

Zerotime0 2 years, 3 months ago

Ty for clarifying.got it .a is right
upvoted 3 times

velrisan 1 year, 11 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 6 months, 3 weeks ago

Selected Answer: A

DEFAULT VLAN not NATIVE VLAN jeje
upvoted 5 times

Rether16 Most Recent 2 months ago

I fell for this one and selected Vlan10. Dohh!
upvoted 1 times

GreatDane 11 months, 3 weeks 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 is still VLAN 1.

Correct Answer

B. VLAN 5

Wrong answer.

C. VLAN 10

Wrong answer.

D. VLAN 20

Wrong answer.

upvoted 4 times

 **ZUMY** 12 months ago

A is correct
Native vlan can be any #
But default vlan is always 1
upvoted 1 times

 **Ric4444** 1 year 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 there 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

 **DUMPlidore** 8 months, 1 week ago

exactly, it was confusing because of the "given environment" at the question
upvoted 1 times

 **timskis2** 1 year ago

it is vlan 10 because it states "in the given environment"
upvoted 2 times

 **ScorpionNet** 1 year, 1 month ago

A is right because VLAN 1 is used by default.
But a poorly added exhibit.
upvoted 1 times

 **ziok** 1 year, 3 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, 4 months ago

Selected Answer: A
VLAN 1 is always default
upvoted 1 times

 **babaKazoo** 1 year, 4 months ago

VLANs 1 and 1001-1005 are default VLANs and can not be changed.
upvoted 1 times

 **Hodicek** 1 year, 6 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, 6 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** 2 months, 4 weeks ago

exactly, this is BS.

upvoted 1 times

 **firstblood** 1 year, 9 months ago

The buzzed word is "default". Even though VLAN 10 is configured as the native VLAN.

upvoted 2 times

 **aleksos** 1 year, 10 months ago

Tricky one...

A is correct.

upvoted 2 times

 **Micah7** 2 years 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, 1 month 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 used 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.

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

B & C are correct

Default Vlans

1
1002
1003
1004
1005

upvoted 8 times

 **linuxlife** Most Recent 2 months, 3 weeks 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** 6 months, 2 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** 11 months, 3 weeks 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, 1 month ago

B and C are right

upvoted 1 times

 **onikafei** 1 year, 4 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, 5 months ago

BC is correctVLAN 1 is a system default VLAN, you can use this VLAN but you cannot delete it. By default VLAN 1 is used 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, 4 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 29 times

✉  **dicksonpwc** Highly Voted 1 year, 10 months ago

CDP Advertisement includes the following:
VTP Management Domain – 0x0009 (CDPv2)
Native VLAN – 0x000a (CDPv2)

upvoted 5 times

✉  **GreatDane** Most Recent 11 months, 3 weeks 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 3 times

 **ZUMY** 12 months ago

A & C are correct

upvoted 1 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

 **Zerotime0** Highly Voted 2 years, 3 months ago

Found old exams from 200-225 exam and there ,poe and security are the answers....not load bal.
upvoted 23 times

 **Request7108** 5 months, 2 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 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 19 times

 **Kaffi** 1 year, 9 months ago

yeah but then security polices seem like must haves not additional.
upvoted 5 times

 **gc999** 2 months, 3 weeks 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** 11 months, 2 weeks ago

How are we doing Power Over Ethernet via wireless?
upvoted 1 times

 **dropspablo** Most Recent 1 month 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** 1 month, 1 week ago

Selected Answer: DE
I think these are the correct ones
upvoted 2 times

 **dearc** 2 months 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 2 times

 **elixirwell** 2 months, 1 week 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]** 3 months, 2 weeks ago

My answer is BE. Keyword, "after", "additional task"

upvoted 1 times

 **GreatDane** 11 months, 3 weeks 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 5 times

 **ZUMY** 12 months ago

Going with A & E

upvoted 1 times

 **onikafei** 1 year, 4 months ago

Selected Answer: AE

It looks like a&e are correct

upvoted 1 times

 **Dking001** 1 year, 10 months ago

B & E...

Because once a new WLAN is deployed, a network admin 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, 1 month ago

Reference question #101

Optimized user performance - Controller uses loadbalancing to maximize throughput.

A & E are correct.

upvoted 9 times

 **Zerotime0** 2 years, 3 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** 1 year, 9 months 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, 3 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, 4 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, 4 months ago

correction: A&E i mean

upvoted 2 times

 **Ali526** 2 years, 5 months ago

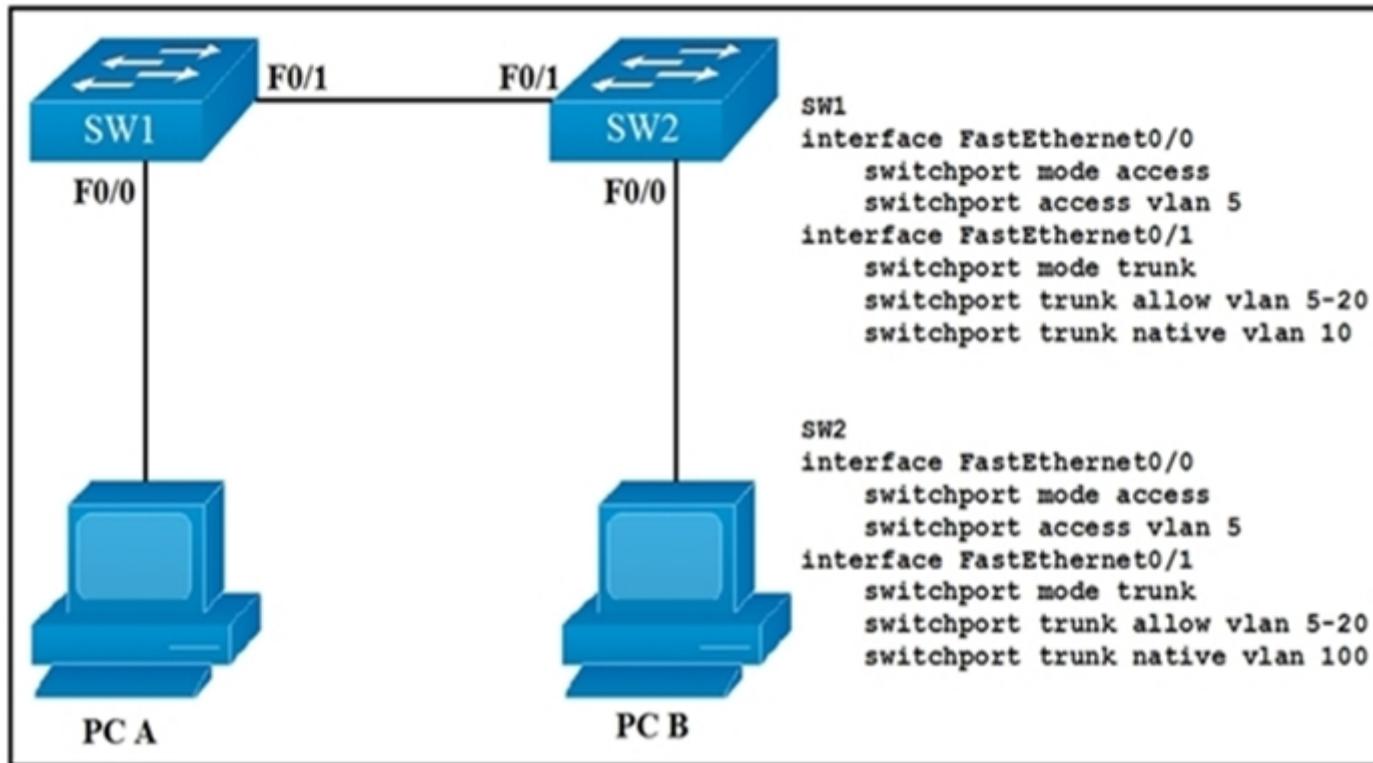
May be.
D is also very important.
upvoted 4 times

 **SScott** 1 year, 12 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

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.

✉ **hokieman91** Highly Voted 2 years, 4 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 23 times

✉ **DARKK** 1 year ago

But VLAN 100 is not allowed (5-20), so it would get dropped if it thinks the traffic is for VLAN 100.

upvoted 2 times

✉ **dropspablo** 1 month 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 1 times

✉ **battery1979** 11 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 10 months 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 12 times

✉ **DoBronx** 7 months, 2 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

 **properchad** Most Recent 2 weeks, 1 day 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

 **ac891** 3 weeks ago

Selected Answer: B

answer is B
 upvoted 1 times

 **Jorro99404** 3 weeks, 1 day 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 weeks 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

 **ThomasSmith** 1 month 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** 2 months, 1 week 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** 2 months, 3 weeks ago

B is correct. Simulated in Packet Tracer.
 upvoted 1 times

 **linuxlife** 2 months, 3 weeks 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
```

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** 3 months, 2 weeks ago

Selected Answer: B

It's B. The switch won't drop the traffic, it will assume that the untagged frame it received the native VLAN. It will thus forward the traffic on VLAN 100.
upvoted 1 times

 **[Removed]** 3 months, 2 weeks ago

My answer is B. VLAN mismatch is still working, but it has become a security issue.
upvoted 1 times

 **Midus** 4 months, 1 week 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** 4 months, 2 weeks ago

Selected Answer: B

untagged traffic goes into the native VLAN from sw2
upvoted 1 times

 **joyboy92** 4 months, 2 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** 4 months, 3 weeks 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 be forwarded normally.
upvoted 1 times

 **Dhruv3390** 4 months, 4 weeks ago

Answer is C. This question is straight forward, if you understand the Native VLAN concept. In the case of native VLAN mismatch, the receiving switch will definitely get the frame but it will discard it as destination will be in VLAN 10. Here is the Jeremy IT lab video: <https://youtu.be/JI9OOzNaBDU?t=924>
upvoted 1 times

 **Yunus_Empire** 6 months, 1 week ago

Selected Answer: C

I THINK C
upvoted 2 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

 **jerry19** Highly Voted 2 years, 1 month ago

D and E, Answer D is used to 'actively negotiate' for PAgP and answer E is used to 'actively negotiate' for LACP.
upvoted 12 times

 **GreatDane** Highly Voted 11 months, 3 weeks 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** 10 months, 3 weeks ago

Thank you for easy explanation
upvoted 2 times

 **Luinus** Most Recent 4 months, 2 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** 5 months, 4 weeks ago

Selected Answer: DE
Agree with GreatDane
upvoted 1 times

 **ZUMY** 12 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, 4 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, 6 months ago

why not c and E?

upvoted 1 times

 **laurvy36** 1 year, 5 months ago

because it doent specify PagP or LACP

upvoted 1 times

 **PraygeForPass** 1 year, 1 month 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, 7 months ago

Shouldn't it be Active and Passive?

upvoted 1 times

 **dave1992** 1 year, 8 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** 1 year, 10 months ago

PagP modes: auto | Desirable

LACP modes: active | pasive

upvoted 10 times

 **Ali526** 2 years, 5 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

 **mikachu85** Highly Voted  1 year, 3 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, 3 months ago

true, that is the explanation

upvoted 1 times

 **dick3311** Most Recent  7 months, 1 week ago

Selected Answer: D

correct is D

upvoted 1 times

 **i_am_confused** 11 months, 2 weeks ago

Selected Answer: D

100% D. As others have said TTL is layer 3

upvoted 1 times

 **ZUMY** 12 months ago

D is correct

upvoted 1 times

 **lohaN73** 12 months ago

TTL is a layer 3 issue, not works at Layer 2

upvoted 1 times

 **onikafei** 1 year, 4 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, 4 months ago

Selected Answer: D

confirmed

upvoted 1 times

 **SparkySM** 1 year, 4 months ago

its should be D. not A

upvoted 1 times

 **wpena** 1 year, 6 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, 4 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 3 times

 **Tengereni** 2 years ago

explanation
upvoted 2 times

 **ZUMY** 2 years, 1 month ago
D is correct
upvoted 4 times

Question #216

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

 [Removed] Highly Voted 2 years, 2 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/swtp.html#wp1107364

A&D are correct
upvoted 30 times

 jerry19 2 years, 1 month 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 1 year, 12 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 1 year, 12 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 1 year, 11 months ago

Do you have a source to back that up because the Cisco documentation disagrees, 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 1 year, 10 months 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

 yuh Most Recent 1 month 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 1 month 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 1 month, 2 weeks ago

Selected Answer: AD

100000%

upvoted 1 times

  **dearc** 2 months 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** 2 months 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** 2 months, 1 week 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/swtp.html#wp1107364

upvoted 1 times

  **zamklio** 2 months, 1 week ago

for D, what happen if there is a VTP transparent with higher revision number in domain?

upvoted 1 times

  **linuxlife** 2 months, 3 weeks 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** 2 months, 3 weeks ago

<https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html>

upvoted 1 times

  **linuxlife** 2 months, 3 weeks ago

A, D, E are correct answers...but only two can be chosen...tricky ones

upvoted 1 times

  **linuxlife** 2 months, 3 weeks 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]** 3 months, 2 weeks ago

AD for me. E is not a CCNA thing, I think.

upvoted 1 times

 **iMo7ed** 3 months, 3 weeks 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/ftp.pdf>

upvoted 2 times

 **ricky1802** 4 months ago

Selected Answer: AD

E definitely 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

 **binrayelias** 4 months, 3 weeks ago

A and E. For vtp to sync info. VTP version must match, domain must match, password must match, switches must be conn in ISL or 802.1q trunk link

upvoted 1 times

 **freeknowledge123** 5 months ago

it's A and E: excerpt from TODD Lammle

You should know these four requirements for VTP to communicate VLAN information between switches:

The VTP version must be set the same

The VTP management domain name of both switches must be set the same.

One of the switches has to be configured as a VTP server.

Set a VTP password if used.

upvoted 2 times

 **diidiuQldama** 5 months, 2 weeks ago

Selected Answer: AE

correct answers are AE. In regards to the vtp version, you dont have to configure which version you are using as long as your switch is capable. They will change to the same version automatically. So vtp version must be the same but you dont need them to be configured the same. Hope this can help you.

upvoted 1 times

 **Request7108** 5 months, 2 weeks ago

Selected Answer: AD

Switches use the highest revision number

All switches must have the same domain name

B is not correct because they do not explicitly have to be

C is wrong because unique domain names would result in unique revisions per domain

E is wrong because multiple versions (not revisions) are allowed.

upvoted 1 times

 **leooel** 5 months, 3 weeks ago

Selected Answer: AD

correct answer is AD

upvoted 1 times

 **usamahrakib001** 6 months, 3 weeks ago

A&E is the answer question is about VTP not what will happen if VTP server has less revision number so question is not talking about D (happening)

upvoted 1 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

 **nenotronix** Highly Voted 2 years, 2 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

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

" The port that receives the best BPDU on a bridge is the root port "

"D" is correct

upvoted 5 times

 **Moctars** Most Recent 3 months ago

Selected Answer: D

Di is correct answer

upvoted 2 times

 **cormorant** 5 months, 3 weeks ago

THE PORT THAT RECEIVES THE BEST BPDU BECOMES THE ROOT PORT. end of story
upvoted 2 times

 **GreatDane** 11 months, 3 weeks 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** 12 months ago

D is correct

upvoted 1 times

 **onikafei** 1 year, 4 months ago

The "best" is root essentially. Whats better than root?

upvoted 3 times

 **RichyES** 1 year, 4 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

 **Claudiu1** Highly Voted 2 years, 2 months ago

This is an STP-related question

upvoted 6 times

 **nenortronix** Highly Voted 2 years, 2 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, 4 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 12 months ago

B is correct

upvoted 1 times

 **BlankNothing1** 1 year 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, 3 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 priority of the port for all VLANs.

Spanning-Tree port-priority value

Else, You can adjust port priority with 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 3 times

 **youtri** 2 years, 1 month 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, 2 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, 3 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 priority of the port for all VLANs

Else, You can adjust port priority with 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

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

This is pure product placement
upvoted 25 times

 **Smaritz** 1 year, 2 months ago

Agreed, although 'proprietary' is a swear word these days LOL
upvoted 2 times

 **Wes_60** Most Recent  2 months, 1 week ago

They put this one on there so no one could be totally wrong.
upvoted 2 times

 **[Removed]** 3 months, 2 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 1 times

 **hasbulla01** 6 months, 4 weeks ago

Selected Answer: A
all is correct less B
upvoted 1 times

 **ratu68** 11 months, 1 week ago

Selected Answer: A
No one better get this wrong ! LOL
upvoted 3 times

 **ZUMY** 12 months ago

A is correct!
upvoted 1 times

 **raresz** 1 year, 2 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, 3 months ago

Selected Answer: A
Other answers are very tricky, but this is most obvious
upvoted 1 times

 **Sara_Yus** 1 year, 3 months ago

NOOO WAYYYYY! I would never have guessed
upvoted 2 times

 **Amirabbas** 2 years, 1 month 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** 5 months, 2 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, 1 month 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, 7 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

 **[Removed]** Highly Voted 3 months, 2 weeks ago

Why not CE?
upvoted 5 times

 **Rether16** Most Recent 2 months ago

Selected Answer: DE
Never use Telnet! :-)
upvoted 1 times

 **Targaryen** 2 years 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** 1 year, 12 months ago

Yes the best two of three correct answers.
upvoted 3 times

 **Sscott** 1 year, 10 months 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 ago

zumy aspettiamo la tua conferma
upvoted 2 times

 **ZUMY** 12 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**  11 months, 3 weeks 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 9 times

✉  **Sutokuto** 5 months, 3 weeks ago

Why do you respond in this format? It's completely useless.

upvoted 9 times

✉  **siredobu** 3 months, 3 weeks ago

Not useless, he/she is giving good explanation on the topic which is good,
rather your comment is useless.

upvoted 7 times

✉  **dicksonpwc**  1 year, 10 months ago

VTP protocol has 3 modes Server, Client & Transparent. There is only 1 server and all other switches in that environment are

Clients. Only server can create, modify and
delete VLAN's so in VTP environment VLAN's are consistent across the network. The changes made on the Server are automatically

propagated to all the clients
through the TRUNK links established between the switches.

upvoted 5 times

✉  **ZUMY**  12 months ago

C & E are right.

upvoted 1 times

✉  **SScott** 1 year, 11 months ago

C and E are right.

upvoted 3 times