

[Home](#) > AAA Quiz

AAA Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of AAA Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
6	70	90%	70	100.00%	00:00:43

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit.

```
aaa new-model
aaa authentication login default local-case enable
aaa authentication login ADMIN local-case
username CCNP secret Str0ngP@ssw0rd!
line 0 4
login authentication ADMIN
```

How can you change this configuration so that when user CCNP logs in, the show run command is executed and the session is terminated?

- A. Assign privilege level 14 to the CCNP username
- B. Add the access-class keyword to the username command
- C. Add the access-class keyword to the aaa authentication command
- D. Add the autocommand keyword to the aaa authentication command
- **E. Add the autocommand keyword to the username command** ✓
- F. Assign privilege level 15 to the CCNP username

Explanation

The “autocommand” causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and can contain embedded spaces, commands using the autocommand keyword must be the last option on the line. In this specific question, we have to enter this line “username CCNP autocommand show running-config”.

Question 2

The login method is configured on the VTY lines of a router with these parameters.

- **The first method for authentication is TACACS**
- **If TACACS is unavailable, login is allowed without any provided credentials**

Which configuration accomplishes this task?

A. R1#sh run | include aaa
aaa new-model
aaa authentication login telnet group tacacs+ none
aaa session-id common

R1#sh run | section vty
line vty 0 4

R1#sh run | include username

- R1#

B. R1#sh run | include aaa
aaa new-model
aaa authentication login default group tacacs+
aaa session-id common

R1#sh run | section vty
line vty 0 4
transport input none

- R1#

- **C. R1#sh run | include aaa
aaa new-model
aaa authentication login default group tacacs+ none
aaa session-id common**

**R1#sh run | section vty
line vty 0 4
password 7 0202039485748**



```
D. R1#sh run | include aaa
aaa new-model
aaa authentication login VTY group tacacs+ none
aaa session-id common
```

```
R1#sh run | section vty
line vty 0 4
password 7 0202039485748
```

```
R1#sh run | include username
```

- R1#

Explanation

According to the requirements (first use TACACS+, then allow login with no authentication), we have to use “aaa authentication login ... **group tacacs+ none**” for AAA command.

The next thing to check is if the “aaa authentication login **default**” or “aaa authentication login *list-name*” is used. The ‘**default**’ keyword means we want to apply for all login connections (such as tty, vty, console and aux). If we use this keyword, we don’t need to configure anything else under tty, vty and aux lines. If we don’t use this keyword then we have to specify which line(s) we want to apply the authentication feature.

From above information, we can find out answer 'R1#sh run | include aaa
aaa new-model
aaa authentication login default group tacacs+ none
aaa session-id common

```
R1#sh run | section vty
line vty 0 4
password 7 0202039485748
```

If you want to learn more about AAA configuration, please read our [AAA TACACS+ and RADIUS Tutorial – Part 2](#).

For your information, answer 'R1#sh run | include aaa
aaa new-model
aaa authentication login telnet group tacacs+ none
aaa session-id common

```
R1#sh run | section vty
line vty 0 4
```

```
R1#sh run | include username
```

R1# would be correct if we add the following command under vty line (“line vty 0 4”): “login authentication telnet” (“telnet” is the name of the AAA list above)

Question 3

Refer to the exhibit.

```
aaa new-model
aaa authentication login local tacacs+
tacacs-server host 10.1.1.1
tacacs-server key CISCO

line con 0
 login authentication local
line aux 0
line vty 0 4
!
username tommy password 0 Cisco
end
```

TACACS+ Server Passwords

```
username tommy password 0 Tommy
```

Which password allows access to line con 0 for a username of “tommy” under normal operation?

- A. Tommy
- **B. Cisco** ✓
- C. local
- D. 0 Cisco

Explanation

In this question, there are two different passwords for user “tommy”:

- + In the TACACS+ server, the password is “Tommy”
- + In the local database of the router, the password is “Cisco”.

From the line “login authentication local” we know that the router uses the local database for authentication so the password should be “Cisco”.

Note: “... password 0 ...” here means unencrypted password.

Question 4

A network administrator applies the following configuration to an IOS device.

```
aaa new-model
aaa authentication login default local group tacacs+
```

What is the process of password checks when a login attempt is made to the device?

- A. A TACACS+ server is checked first. If that check fail, a RADIUS server is checked. If that check fail, a local database is checked
- B. A local database is checked first. If that fails, a TACACS+server is checked, if that check fails, a RADIUS server is checked
- C. A TACACS+ server is checked first. If that check fail, a database is checked
- **D. A local database is checked first. If that check fails, a TACACS+server is checked** ✓

Explanation

The “aaa authentication login default local group tacacs+” command is broken down as follows:

- + The ‘**aaa authentication**’ part is simply saying we want to configure authentication settings.
- + The ‘**login**’ is stating that we want to prompt for a username/password when a connection is made to the device.
- + The ‘**default**’ means we want to apply for all login connections (such as tty, vty, console and aux). If we use this keyword, we don’t need to configure anything else under tty, vty and aux lines. If we don’t use this keyword then we have to specify which line(s) we want to apply the authentication feature.
- + The ‘**local group tacacs+**’ means all users are authenticated using router’s local database (the first method). If the credentials are not found on the local database, then the TACACS+ server is used (the second method).

Question 5

Which two statements about AAA authentication are true? (Choose two)

- A. Local user names are case-insensitive
- B. RADIUS authentication queries the router’s local username database
- **C. KRB5 authentication disables user access when an incorrect password is entered** ✓
- D. TACACS+ authentication uses an RSA server to authenticate users
- **E. Local authentication is maintained on the router** ✓

Question 6

Refer to the exhibit.

```
aaa new-model
aaa authentication login authorizationlist tacacs+
tacacs-server host 192.168.0.202
tacacs-server key ciscotestkey
line vty 0 4
login authentication authorizationlist
```

What is the effect of the configuration?

- **A. The device will authenticate all users connecting to vty lines 0 through 4 against TACACS+** ✓
- B. When users attempt to connect to vty lines 0 through 4, the device will authenticate them against TACACS+ if local authentication fails
- C. The device will allow only users at 192.168.0.202 to connect to vty lines 0 through 4
- D. The device will allow users at 192.168.0.202 to connect to vty lines 0 through 4 using the password ciscotestkey

Comments

1. Ludmilla
February 13th, 2021

In the explanation under question 5 you state the following:

```
answer 'R1#sh run | include aaa
aaa new-model
aaa authentication login telnet group tacacs+ none
aaa session-id common
```

```
R1#sh run | section vty
line vty 0 4
```

```
R1#sh run | include username
```

R1# would be correct if we add the following command under vty line ("line vty 0 4"): "login authentication telnet" ("telnet" is the name of the AAA list above)

So, it follows that 'telnet' is simply the name of a list. I assume it is a local list with usernames and passwords.

On basis of this I would expect that in question 6, 'authorizationlist' is also a list like 'telnet' in question 5. Therefore, it is expected that answer A is applicable. If answer D is the correct answer, what then is the function of the term 'authorizationlist' in the command 'aaa authentication login authorizationlist tacacs+' and what does that term refer to?

Looking forward to your response.
Thanks for that.

2. Don Quijote
February 15th, 2021

I'm agree with Ludmilla, 9tut could you please explain or correct the answerd

1. No trackbacks yet.

Add a Comment



I'm not a robot

reCAPTCHA
[Privacy](#) - [Terms](#)

[Subscribe to comments feed](#)

[Wireless 3 Quiz](#) [Drag Drop 2 Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)

- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Access-list 2 Quiz

Access-list 2 Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Access-list 2 Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
2	20	90%	20	100.00%	00:00:12

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

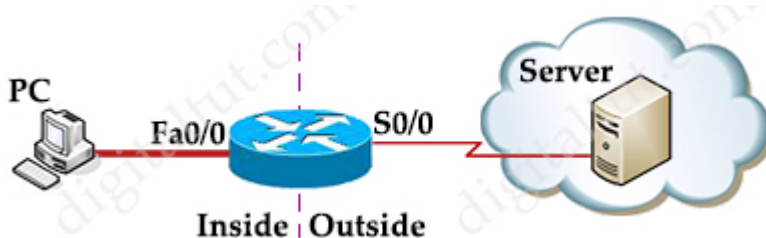
Question 1

An engineer must configure a ACL that permits packets which include an ACK in the TCP header. Which entry must be included in the ACL?

- **A. access-list 110 permit tcp any any eq 21 established** ✓
- B. access-list 10 permit tcp any any eq 21 established
- C. access-list 110 permit tcp any any eq 21 tcp-ack
- D. access-list 10 permit ip any any eq 21 tcp-ack

Explanation

The **established** keyword is only applicable to TCP access list entries to match TCP segments that have the ACK and/or RST control bit set (regardless of the source and destination ports), which assumes that a TCP connection has already been established in one direction only. Let's see an example below:



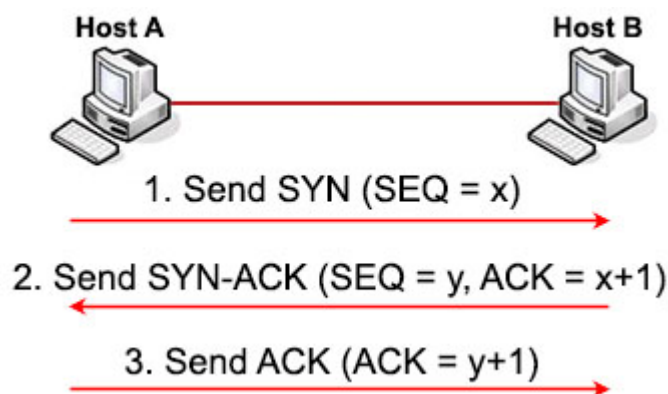
Suppose you only want to allow the hosts inside your company to telnet to an outside server but not vice versa, you can simply use an “established” access-list

like this:

```
access-list 100 permit tcp any any established
access-list 101 permit tcp any any eq telnet
!
interface S0/0
ip access-group 100 in
ip access-group 101 out
```

Note:

Suppose hostA wants to start communicating with hostB using TCP. Before they can send real data, a three-way handshake must be established first. Let's see how this process takes place:



1. First hostA will send a **SYN message** (a TCP segment with SYN flag set to 1, SYN is short for SYNchronize) to indicate it wants to setup a connection with hostB. This message includes a sequence (SEQ) number for tracking purpose. This sequence number can be any 32-bit number (range from 0 to 2^{32}) so we use "x" to represent it.

2. After receiving SYN message from hostA, hostB replies with **SYN-ACK message** (some books may call it "SYN/ACK" or "SYN, ACK" message. ACK is short for ACKnowledge). This message includes a SYN sequence number and an ACK number:

- + SYN sequence number (let's called it "y") is a random number and does not have any relationship with Host A's SYN SEQ number.
- + ACK number is the next number of Host A's SYN sequence number it received, so we represent it with "x+1". It means "I received your part. Now send me the next part (x + 1)".

The SYN-ACK message indicates hostB accepts to talk to hostA (via ACK part). And ask if hostA still wants to talk to it as well (via SYN part).

3. After Host A received the SYN-ACK message from hostB, it sends an **ACK message** with ACK number "y+1" to hostB. This confirms hostA still wants to talk to hostB.

Question 2

Refer to the exhibit.

```
line vty 0 4
 session-timeout 30
 exec-timeout 120 0
 session-limit 30
```

```
login local
line vty 5 15
  session-timeout 30
  exec-timeout 30 0
  session-limit 30
login local
```

Only administrators from the subnet 10.10.10.0/24 are permitted to have access to the router. A secure protocol must be used for the remote access and management of the router instead of clear-text protocols. Which configuration achieves this goal?

Option A access-list 23 permit 10.10.10.0 0.0.0.255 line vty 0 4 access-class 23 in transport input ssh	Option B access-list 23 permit 10.10.10.0 0.0.0.255 line vty 0 15 access-class 23 in transport input ssh
Option C access-list 23 permit 10.10.10.0 0.0.0.255 line vty 0 15 access-class 23 out transport input all	Option D access-list 23 permit 10.10.10.0 255.0.0.0 line vty 0 15 access-class 23 in transport input ssh

- **A. Option B** ✓
- B. Option D
- C. Option C
- D. Option A

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[HSRP & VRRP 2 Quiz](#) [SD-WAN & SD-Access Solutions 3 Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)

- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Access-list Quiz

Access-list Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Access-list Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
10	100	90%	100	100.00%	00:21:43

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which outbound access list, applied to the WAN interface of a router, permits all traffic except for http traffic sourced from the workstation with IP address 10.10.10.1?

- A. ip access-list extended 10
deny tcp host 10.10.10.1 any eq 80
 - permit ip any any
- B. ip access-list extended 200
deny tcp host 10.10.10.1 eq 80 any
 - permit ip any any
- **C. ip access-list extended 100**
deny tcp host 10.10.10.1 any eq 80 ✓
permit ip any any
- D. ip access-list extended NO_HTTP
 - deny tcp host 10.10.10.1 any eq 80

Question 2

Refer to the exhibit. An engineer must modify the access control list EGRESS to allow all IP traffic from subnet 10.1.10.0/24 to 10.1.2.0/24. The access control list is applied in the outbound direction on router interface GigabitEthernet 0/1.

Extended IP access list EGRESS
10 permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
20 deny ip any any

Which configuration commands can the engineer use to allow this traffic without disrupting existing traffic flows?

- A. config t
ip access-list extended EGRESS
• permit ip 10.1.10.0 255.255.255.0 10.1.2.0 255.255.255.0
- B. config t
ip access-list extended EGRESS
• permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
- **C. config t
ip access-list extended EGRESS
5 permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255** ✓
- D. config t
ip access-list extended EGRESS2
permit ip 10.1.10.0 0.0.0.295 10.1.2.0 0.0.0.299
permit ip 10.1.100.0 0.0.0.299 10.1.2.0 0.0.0.299
deny ip any any
!
interface g0/1
no ip access-group EGRESS out
• ip access-group EGRESS2 out

Explanation

We can insert a line (statement) between entries into an existing ACL by a number in between.

```
R1#sh access-list
Extended IP access list EGRESS
 10 permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
 20 deny ip any any
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list extended EGRESS
R1(config-ext-nacl)#5 permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
R1(config-ext-nacl)#do sh access-list
Extended IP access list EGRESS
 5 permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
10 permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
20 deny ip any any
```

So what will happen if we just enter a statement without the number? Well, that statement would be added at the bottom of an ACL. But in this case we already had an explicit “deny ip any any” statement so we cannot put another line under it.

Question 3

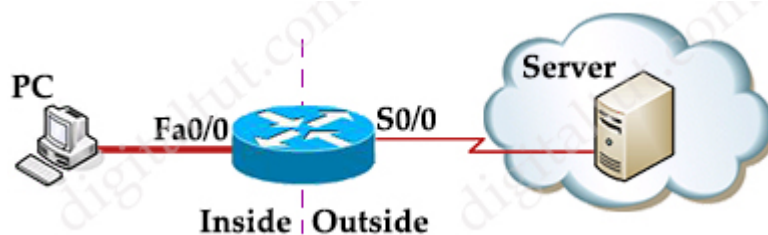
What is the result of applying this access control list?

```
ip access-list extended STATEFUL
10 permit tcp any any established
20 deny ip any any
```

- A. TCP traffic with the URG bit set is allowed
- B. TCP traffic with the DF bit set is allowed
- **C. TCP traffic with the ACK bit set is allowed** ✓
- D. TCP traffic with the SYN bit set is allowed

Explanation

The **established** keyword is only applicable to TCP access list entries to match TCP segments that have the ACK and/or RST control bit set (regardless of the source and destination ports), which assumes that a TCP connection has already been established in one direction only. Let's see an example below:

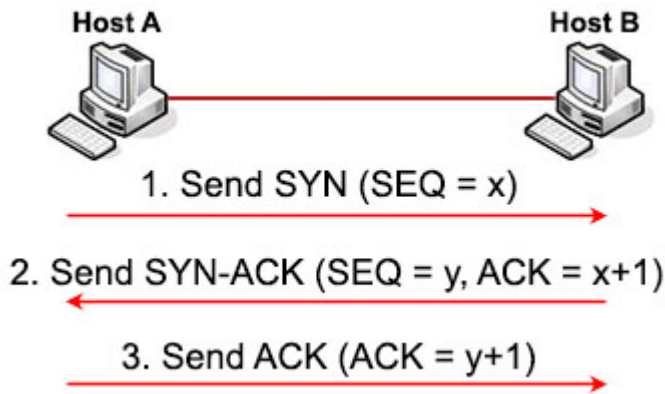


Suppose you only want to allow the hosts inside your company to telnet to an outside server but not vice versa, you can simply use an “established” access-list like this:

```
access-list 100 permit tcp any any established
access-list 101 permit tcp any any eq telnet
!
interface S0/0
ip access-group 100 in
ip access-group 101 out
```

Note:

Suppose hostA wants to start communicating with hostB using TCP. Before they can send real data, a three-way handshake must be established first. Let's see how this process takes place:



1. First hostA will send a **SYN message** (a TCP segment with SYN flag set to 1, SYN is short for SYNchronize) to indicate it wants to setup a connection with hostB. This message includes a sequence (SEQ) number for tracking purpose. This sequence number can be any 32-bit number (range from 0 to 2^{32}) so we use “x” to represent it.

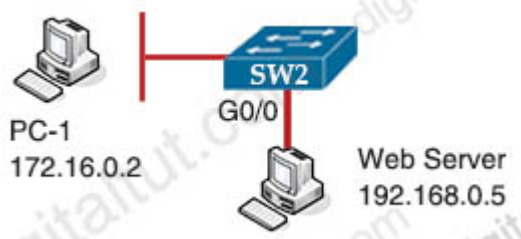
2. After receiving SYN message from hostA, hostB replies with **SYN-ACK message** (some books may call it “SYN/ACK” or “SYN, ACK” message. ACK is short for ACKnowledge). This message includes a SYN sequence number and an ACK number:
 + SYN sequence number (let’s called it “y”) is a random number and does not have any relationship with Host A’s SYN SEQ number.
 + ACK number is the next number of Host A’s SYN sequence number it received, so we represent it with “x+1”. It means “I received your part. Now send me the next part (x + 1)”.

The SYN-ACK message indicates hostB accepts to talk to hostA (via ACK part). And ask if hostA still wants to talk to it as well (via SYN part).

3. After Host A received the SYN-ACK message from hostB, it sends an **ACK message** with ACK number “y+1” to hostB. This confirms hostA still wants to talk to hostB.

Question 4

Refer to the exhibit. PC-1 must access the web server on port 8080. To allow this traffic, which statement must be added to an access control list that is applied on SW2 port G0/0 in the inbound direction?



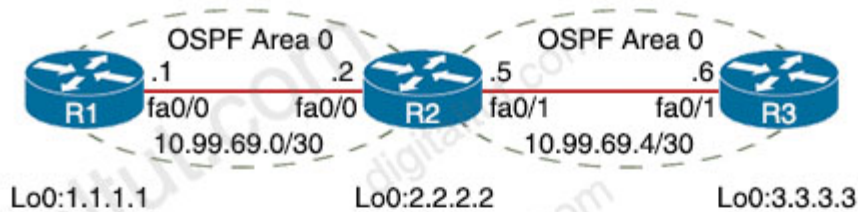
- A. permit host 172.16.0.2 host 192.168.0.5 eq 8080
- **B. permit host 192.168.0.5 eq 8080 host 172.16.0.2** ✓
- C. permit host 192.168.0.5 it 8080 host 172.16.0.2
- D. permit host 192.168.0.5 host 172.16.0.2 eq 8080

Explanation

The inbound direction of G0/0 of SW2 only filter traffic from Web Server to PC-1 so the source IP address and port is of the Web Server.

Question 5

Refer to the exhibit.



```
R1#traceroute
Protocol [ip]:
Target IP address: 3.3.3.3
Source address: 1.1.1.1
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [9]:
Loose, Strict, Record, Timestamp, Verbose [RV]:
Type escape sequence to abort.
```

Continued --->

```
Tracing the route to 3.3.3.3
 1 10.99.69.2 36 msec
Received packet has options
Total option bytes = 40, padded length=40
Record route:
(10.99.69.1) <*>
(0.0.0.0)
(0.0.0.0)
End of list
---output omitted---

 2 10.99.69.6 !A
Received packet has options
Total option bytes = 40, padded length=40
Record route:
(10.99.69.1)
(10.99.69.5) <*>
(0.0.0.0)
(0.0.0.0)
End of list
!A
---output omitted---
```

The

traceroute fails from R1 to R3. What is the cause of the failure?

- **A. An ACL applied inbound on fa0/1 of R3 is dropping the traffic** ✓
- B. Redistribution of connected routes into OSPF is not configured
- C. The loopback on R3 is in a shutdown state
- D. An ACL applied inbound on loopback0 of R2 is dropping the traffic

Explanation

We see in the traceroute result the packet could reach 10.99.69.5 (on R2) but it could not go any further so we can deduce an ACL on R3 was blocking it.

Note: Record option displays the address(es) of the hops (up to nine) the packet goes through.

Comments

Question 6

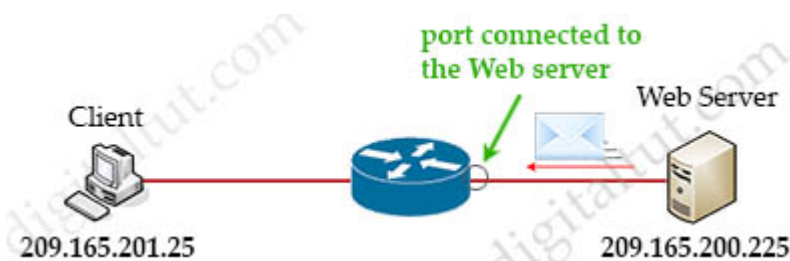
A client with IP address 209.165.201.25 must access a web server on port 80 at 209.165.200.225. To allow this traffic, an engineer must add a statement to an access control list that is applied in the inbound direction on the port connecting to the web server. Which statement allows this traffic?

- A. permit tcp host 209.165.200.225 host 209.165.201.25 eq 80
- B. permit tcp host 209.165.201.25 eq 80 host 209.165.200.225
- **C. permit tcp host 209.165.200.225 eq 80 host 209.165.201.25** ✓
- D. permit tcp host 209.165.201.25 host 209.165.200.225 eq 80

Explanation

The syntax of an extended ACL is shown below:

access-list *access-list-number* {permit | deny} *protocol* source {source-mask} [eq source-port] destination {destination-mask} [eq destination-port]



According to the request in this question, we must apply the ACL on the port connected to the Web Server and with inbound direction. So it can only filter traffic sent from the Web Server to the Client. Please notice that the Client communicate to the Web Server with destination port of 80 but with random source port. So the Web Server must answer the Client with this random port (as the destination port) -> Therefore the destination port in the required ACL must be ignored. Also the Web Server must use port 80 as its source port.

So the structure of the ACL should be: permit tcp host <IP-address-of-Web-Server> eq 80 host <IP-address-of-Client>

-> Answer 'permit tcp host 209.165.200.225 eq 80 host 209.165.201.25' is correct.

Question 7

Which access controls list allows only TCP traffic with a destination port range of 22-443, excluding port 80?

- **A. Deny tcp any any eq 80**
Permit tcp any any gt 21 lt 444 ✓
- B. Deny tcp any any neq 80
- Permit tcp any any range 22 443
- C. Permit tcp any any neq 80
- D. Permit tcp any any range 22 443
- Deny tcp any any eq 80

Explanation

Although the statement “permit tcp any any gt ... lt ...” seems to be correct but in fact it is not. Each ACL statement only supports either “gt” or “lt” but not both:

```
R1(config)#ip access-list extended test2
R1(config-ext-nacl)#deny tcp any any eq 80
R1(config-ext-nacl)#permit tcp any any gt 21 lt 444
^
% Invalid input detected at '^' marker.

R1(config-ext-nacl)#permit tcp any any lt 444 gt 21
^
% Invalid input detected at '^' marker.

R1(config-ext-nacl)#permit tcp any any gt 21
R1(config-ext-nacl)#permit tcp any any lt 444
```

But it is still the best choice here.

Answer 'Permit tcp any any range 22 443
Deny tcp any any eq 80

Permit tcp any any range 22 443' is only correct if the first statement is “Deny tcp any any eq 80”.

Question 8

Refer to the exhibit. An engineer must block all traffic from a router to its directly connected subnet 209.165.200.0/24. The engineer applies access control list EGRESS in the outbound direction on the GigabitEthernet0/0 interface of the router. However, the router can still ping hosts on the 209.165.200.0/24 subnet. Which explanation of this behavior is true?

```
Extended IP access list EGRESS
10 permit ip 10.0.0.0 0.0.0.255 any
!
---output omitted---
!
interface GigabitEthernet0/0
 ip address 209.165.200.255 255.255.255.0
 ip access-group EGRESS out
 duplex auto
 speed auto
 media-type rj45
!
```

- A. After an access control list is applied to an interface, that interface must be shut and no shut for the access control list to take effect
- B. The access control list must contain an explicit deny to block traffic from the router
- C. Access control lists that are applied outbound to a router interface do not affect traffic that is sourced from the router
- D. Only standard access control lists can block traffic from a source IP address



Question 9

Which standard access control entry permits from odd-numbered hosts in the 10.0.0.0/24 subnet?

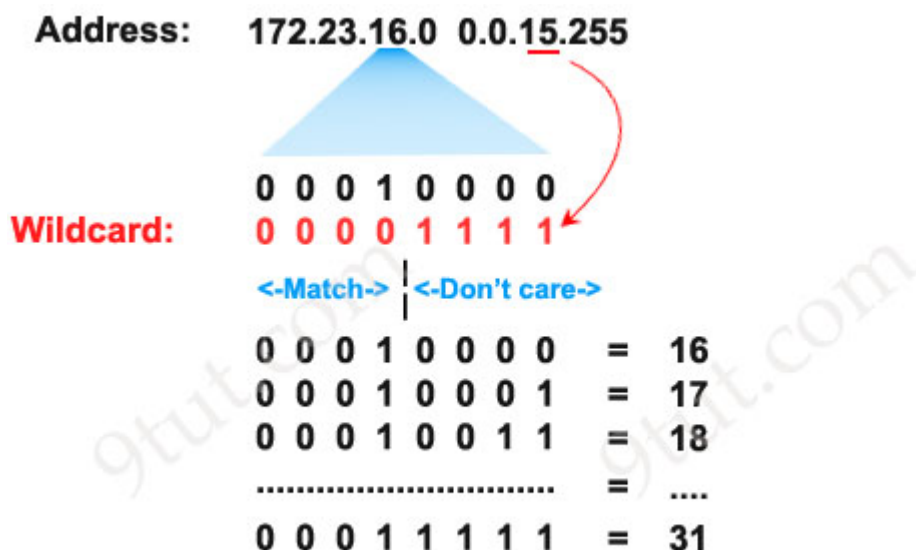
- A. Permit 10.0.0.0 255.255.255.254
- B. Permit 10.0.0.1 0.0.0.0
- **C. Permit 10.0.0.1 0.0.0.254** ✓
- D. Permit 10.0.0.0 0.0.0.1

Explanation

Remember, for the wildcard mask, **1's are I DON'T CARE**, and **0's are I CARE**. So now let's analyze a simple ACL:

access-list 1 permit 172.23.16.0 0.0.15.255

Two first octets are all 0's meaning that we care about the network **172.23.x.x**. The third octet of the wildcard mask, 15 (0000 1111 in binary), means that we care about first 4 bits but don't care about last 4 bits so we allow the third octet in the form of 0001xxxx (minimum: 00010000 = 16; maximum: 00011111 = 31).



172.23.16.0 0.0.15.255 <=> from 172.23.16.0 to 172.23.31.255

The fourth octet is 255 (all 1 bits) that means I don't care.

Therefore **network 172.23.16.0 0.0.15.255** ranges from **172.23.16.0** to **172.23.31.255**.

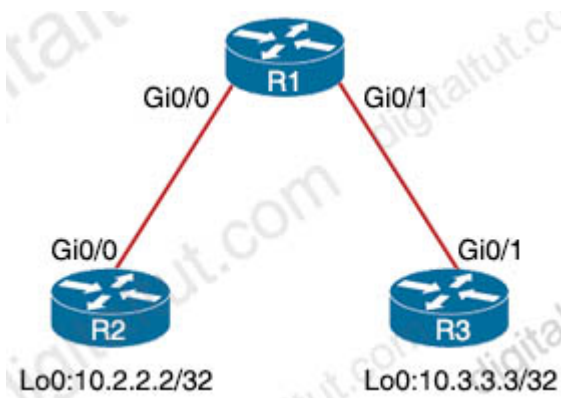
Now let's consider the wildcard mask of 0.0.0.254 (four octet: 254 = 1111 1110) which means we only care the last bit. Therefore if the last bit of the IP address is a "1" (0000 0001) then only odd numbers are allowed. If the last bit of the IP address is a "0" (0000 0000) then only even numbers are allowed.

Note: In binary, odd numbers are always end with a "1" while even numbers are always end with a "0".

Therefore in this question, only the statement "permit 10.0.0.1 0.0.0.254" will allow all odd-numbered hosts in the 10.0.0.0/24 subnet.

Question 10

Refer to the exhibit.



An engineer must deny Telnet traffic from the loopback interface of router R3 to the loopback interface of router R2 during the weekend hours. All other traffic between the loopback interfaces of routers R3 and R2 must be allowed at all times. Which command accomplish this task?

- A. 3(config)#time-range WEEKEND
 R3(config-time-range)#periodic weekend 00:00 to 23:59
 R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
 R3(config)#access-list 150 permit ip any any time-range WEEKEND
 R3(config)#interface Gi0/1
 • R3(config-if)#ip access-group 150 out
- B. R1(config)#time-range WEEKEND
 R1(config-time-range)#periodic Friday Sunday 00:00 to 00:00
 R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
 R1(config)#access-list 150 permit ip any any
 R1(config)#interface Gi0/1
 • R1(config-if)#ip access-group 150 in
- C. R3(config)#time-range WEEKEND
 R3(config-time-range)#periodic Saturday Sunday 00:00 to 23:59
 R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
 R3(config)#access-list 150 permit ip any any time-range WEEKEND
 R3(config)#interface Gi0/1
 • R3(config-if)#ip access-group 150 out

- **D. R1(config)#time-range WEEKEND**

R1(config-time-range)#periodic weekend 00:00 to 23:59

R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND

R1(config)#access-list 150 permit ip any any 

R1(config)#interface Gi0/1

R1(config-if)#ip access-group 150 in

Explanation

We cannot filter traffic that is originated from the local router (R3 in this case) so we can only configure the ACL on R1 or R2. “Weekend hours” means from Saturday morning through Sunday night so we have to configure: “periodic weekend 00:00 to 23:59”.

Note: The time is specified in 24-hour time (hh:mm), where the hours range from 0 to 23 and the minutes range from 0 to 59.

They really should remove the question about port range 22 443 because none of the answers are right. At first you think the gt 21 and lt 444 is right but you can't use both lt and gt in the same statement,

so the only other option is permit tcp any any range 22 443 then Deny tcp any any. This ACL would not exclude port 80 because it would allow it before it got to the Deny rule

2. Streber2

July 19th, 2020

Question 1

A client with IP address 209.165.201.25 must access a web server on port 80 at 209.165.200.225. To allow this traffic, an engineer must add a statement to an access control list that is applied in the inbound direction on the port connecting to the web server. Which statement allows this traffic?

- A. permit tcp host 209.165.201.25 host 209.165.200.225 eq 80
- B. permit tcp host 209.165.201.25 eq 80 host 209.165.200.225
- C. permit tcp host 209.165.200.225 eq 80 host 209.165.201.25 correct
- D. permit tcp host 209.165.200.225 host 209.165.201.25 eq 80

In my opinion answer D should be right!
Please correct me if I am wrong.

3. Qwerty

August 9th, 2020

@Anonymous so the answer should be:

deny tcp any any eq 80
permit tcp any any range 22 443

right?

4. hershel

August 9th, 2020

Hi Streber2, Answer D is incorrect because what that command is doing is allowing traffic from server IP to the Client IP with dst port 80 (HTTP) however the client's port is likely a random port instead the number 80, and the Server is the one that has to be reached at port 80, so traffic coming from the server to the client will have source port of 80, reason why the correct answer is C, hope this helps.

5. MAC

November 30th, 2020

Which access controls list allows only TCP traffic with a destination port range of 22-443, excluding port 80?

Shouldn't the answer be B. Permit tcp any any neq 80.

If I am reading it correctly, all TCP traffic at any port is passed except for port 80

6. Dzoni

January 6th, 2021

Hello Digitaltut team,

Can you please add more detailed explanation about question:

Which access controls list allows only TCP traffic with a destination port range of 22-443, excluding port 80?

A. Permit tcp any any neq 80

B. Deny tcp any any neq 80

Permit tcp any any range 22 443

C. Deny tcp any any eq 80

Permit tcp any any gt 21 lt 444

correct

D. Permit tcp any any range 22 443

Deny tcp any any eq 80

wrong

Thank you in advance!

7. sonda_mexico

January 14th, 2021

9tut entonces en la pregunta cual es la correcta

Which access controls list allows only TCP traffic with a destination port range of 22-443, excluding port 80?

wich one is the best option?

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[Automation Quiz](#) [Security Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)

- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)

- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Architecture Quiz

Architecture Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Architecture Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
5	60	90%	60	100.00%	00:00:41

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

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

- A. Cloud deployments require long implementation times due to capital expenditure processes. OnPrem deployments can be accomplished quickly using operational expenditure processes
- B. In a cloud environment, the company is in full control of access to their data. On-prem risks access to data due to service provider outages
- C. Cloud resources scale automatically to an increase in demand. On-prem requires additional capital expenditure** ✓
- D. In a cloud environment, the company controls technical issues. On-prem environments rely on the service provider to resolve technical issue
- E. Cloud costs adjust up or down depending on the amount of resources consumed. On- Prem costs for hardware, power, and space are ongoing regardless of usage** ✓

Question 2

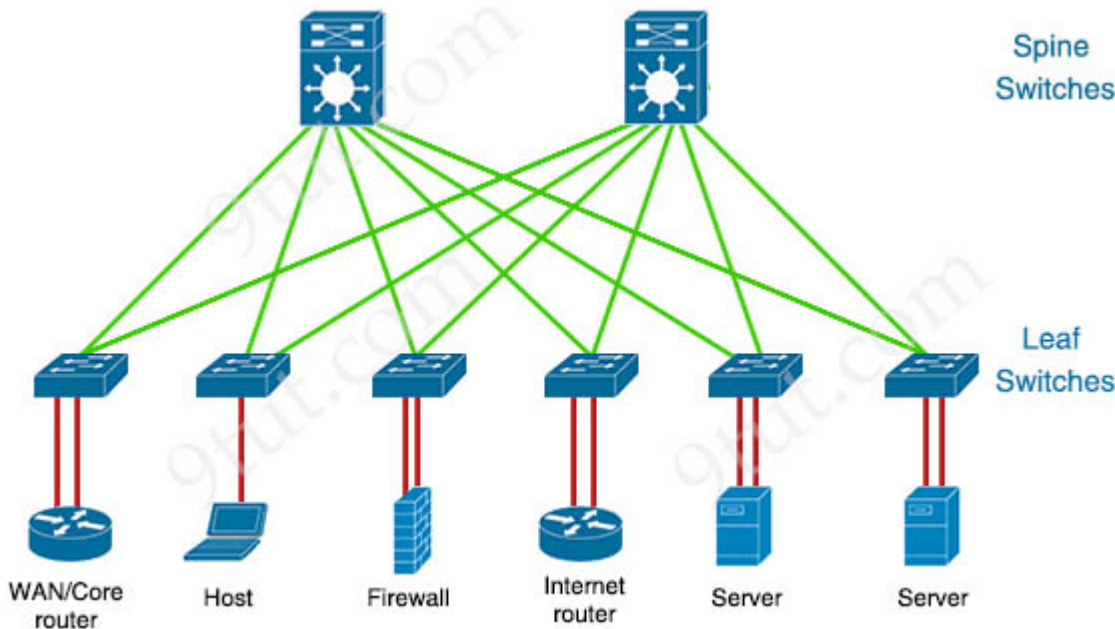
A company plans to implement intent-based networking in its campus infrastructure. Which design facilities a migrate from a traditional campus design to a programmer fabric designer?

- A. two-tier** ✓
- B. Layer 2 access

- C. routed access
- D. three-tier

Explanation

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



Question 3

In a Cisco Catalyst switch equipped with two supervisor modules an administrator must temporally remove the active supervisor from the chassis to perform hardware maintenance on it. Which mechanism ensure that the active supervisor removal is not disruptive to the network operation?

- A. NSF/NSR
- B. HSRP
- C. SSO ✓
- D. VRRP

Explanation

Stateful Switchover (SSO) provides protection for network edge devices with dual Route Processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

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

Comments

Question 4

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

- **A. efficient scalability** ✓
- B. supported systems
- C. storage capacity
- D. virtualization

Question 5

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

- A. ability to quickly increase compute power without the need to install additional hardware
- B. faster deployment times because additional infrastructure does not need to be purchased
- **C. lower latency between systems that are physically located near each other** ✓
- D. less power and cooling resources needed to run infrastructure on-premises

Explanation

The difference between on-premise and cloud is essentially where this hardware and software resides. On-premise means that a company keeps all of this IT environment onsite either managed by themselves or a third-party. Cloud means that it is housed offsite with someone else responsible for monitoring and maintaining it.

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[Wireless 2 Quiz](#) [DNA Center Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

<https://t.me/learningnets>

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > BGP Quiz

BGP Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of BGP Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
8	90	90%	90	100.00%	00:01:50

Congratulations!

You passed this test!

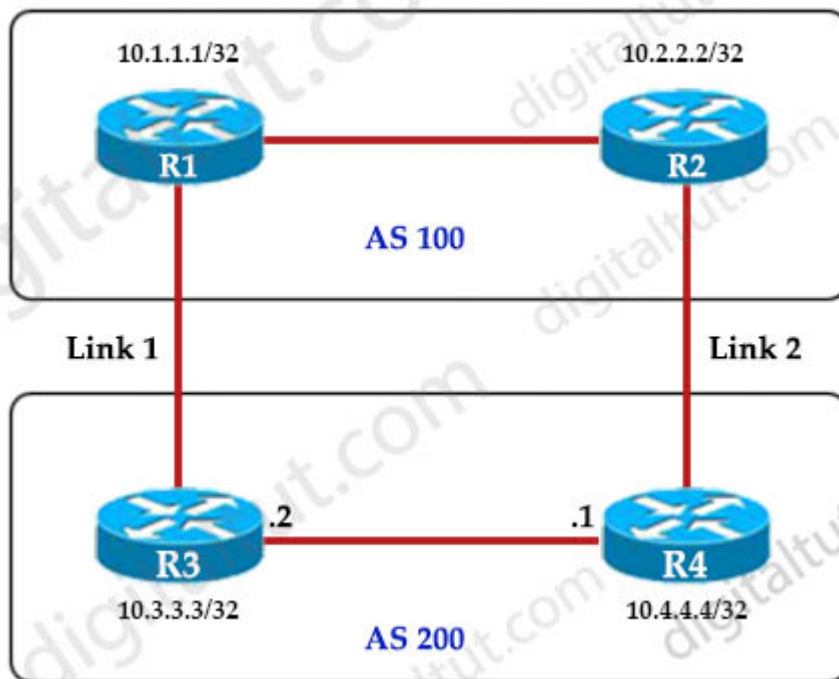
If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit.

An engineer must ensure that all traffic leaving AS 200 will choose Link 2 as the exit point. Assuming that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers, which configuration accomplish task?



- **A. R4(config-router)#bgp default local-preference 200** ✓
- B. R4(config-router)#neighbor 10.2.2.2 weight 200
- C. R3(config-router)#bgp default local-preference 200
- D. R3(config-router)#neighbor 10.1.1.1 weight 200

Explanation

Local preference is an indication to the AS about which path has preference to exit the AS in order to reach a certain network. A path with a higher local preference is preferred. The default value for local preference is 100.

Unlike the weight attribute, which is only relevant to the local router, local preference is an attribute that routers exchange in the same AS. The local preference is set with the “bgp default local-preference *value*” command.

In this case, both R3 & R4 have exit links but R4 has higher local-preference so R4 will be chosen as the preferred exit point from AS 200.

(Reference:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800c95bb.shtml#localpref)

Question 2

A local router shows an EBGP neighbor in the Active state. Which statement is true about the local router?

- A. The local router has BGP passive mode configured for the neighboring router
- B. The local router has active prefix in the forwarding table from the neighboring router
- **C. The local router is attempting to open a TCP session with the neighboring router.** ✓
- D. The local router is receiving prefixes from the neighboring router and adding them in RIB-IN

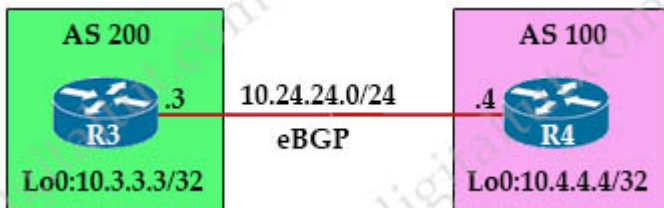
Explanation

The BGP session may report in the following states

- 1 – Idle:** the initial state of a BGP connection. In this state, the BGP speaker is waiting for a BGP start event, generally either the establishment of a TCP connection or the re-establishment of a previous connection. Once the connection is established, BGP moves to the next state.
- 2 – Connect:** In this state, BGP is waiting for the TCP connection to be formed. If the TCP connection completes, BGP will move to the OpenSent stage; if the connection cannot complete, BGP goes to Active
- 3 – Active:** In the Active state, the BGP speaker is attempting to initiate a TCP session with the BGP speaker it wants to peer with. If this can be done, the BGP state goes to OpenSent state.
- 4 – OpenSent:** the BGP speaker is waiting to receive an OPEN message from the remote BGP speaker
- 5 – OpenConfirm:** Once the BGP speaker receives the OPEN message and no error is detected, the BGP speaker sends a KEEPALIVE message to the remote BGP speaker
- 6 – Established:** All of the neighbor negotiations are complete. You will see a number, which tells us the number of prefixes the router has received from a neighbor or peer group.

Question 3

Refer to the exhibit.



An engineer must establish eBGP peering between router R3 and router R4. Both routers should use their loopback interfaces as the BGP router ID. Which configuration set accomplishes this task?

- A. 3(config)#router bgp 200
R3(config-router)#neighbor 10.24.24.4 remote-as 100
R3(config-router)#neighbor 10.24.24.4 update-source loopback0
- R4(config)#router bgp 100
R4(config-router)#neighbor 10.24.24.3 remote-as 200
- R4(config-router)#neighbor 10.24.24.3 update-source loopback0
- B. R3(config)#router bgp 200
R3(config-router)#neighbor 10.4.4.4 remote-as 100
R3(config-router)#neighbor 10.4.4.4 update-source loopback0
- R4(config)#router bgp 100
R4(config-router)#neighbor 10.3.3.3 remote-as 200
- R4(config-router)#neighbor 10.3.3.3 update-source loopback0
- **C. R3(config)#router bgp 200**
R3(config-router)#neighbor 10.24.24.4 remote-as 100
R3(config-router)#bgp router-id 10.3.3.3
- R4(config)#router bgp 100**
R4(config-router)#neighbor 10.24.24.3 remote-as 200
R4(config-router)#bgp router-id 10.4.4.4



Question 4

What is the correct EBGp path attribute list, ordered from most preferred to the least preferred, that the BGP best-path algorithm uses?

- **A. weight, local preference, AS path, MED** ✓
- B. local preference, weight, MED, AS path
- C. local preference, weight, AS path, MED
- D. weight, AS path, local preference, MED

Explanation

Path Selection Attributes: Weight > Local Preference > Originate > AS Path > Origin > MED > External > IGP Cost > eBGP Peering > Router ID

Question 5

Refer to the exhibit. Which IP address becomes the next active next hop for 192.168.102.0/24 when 192.168.101.2 fails?

```
R1#show ip bgp
BGP table version is 32, local router ID is 192.168.101.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.168.102.0	192.168.101.18	80		0	64517 i
*	192.168.101.14	80	80	0	64516 i
*	192.168.101.10			0	64515 64515 i
*>	192.168.101.2			0	64513 i
*	192.168.101.6		80	0	64514 64514 i

- **A. 192.168.101.18** ✓
- B. 192.168.101.14
- C. 192.168.101.10
- D. 192.168.101.6

Explanation

The ‘>’ shown in the output above indicates that the path with a next hop of 192.168.101.2 is the current best path.

Path Selection Attributes: Weight > Local Preference > Originate > AS Path > Origin > MED > External > IGP Cost > eBGP Peering > Router ID

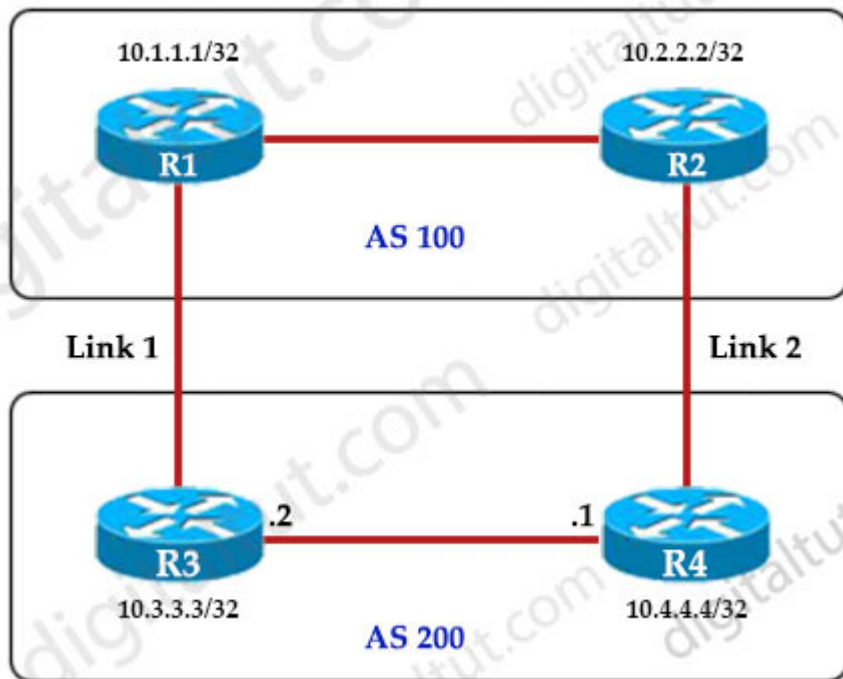
BGP prefers the path with highest weight but the weights here are all 0 (which indicate all routes that are not originated by the local router) so we need to check the Local Preference. A path without LOCAL_PREF (LocPrf column) means it has the default value of 100. Therefore we can find the two next best paths with the next hop of 192.168.101.18 and 192.168.101.10.

We have to move to the next path selection attribute: Originate. BGP prefers the path that the local router originated (which is indicated with the “next hop 0.0.0.0”). But none of the two best paths is self-originated.

The AS Path of the next hop 192.168.101.18 (one AS away) is shorter than the AS Path of the next hop 192.168.101.10 (two ASes away) so the next hop 192.168.101.18 will be chosen as the next best path.

Question 6

Refer to the exhibit.



An engineer must ensure that all traffic entering AS 200 will choose Link 2 as an entry point. Assuming that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers, which configuration accomplish task?

Option A

```
R3(config)#route-map PREPEND permit 10
R3(config-route-map)#set as-path prepend 200 200
200
```

```
R3(config)# router bgp 200
```

```
R3(config-router)#neighbor 10.1.1.1 route-map
PREPEND out
```

Option B

```
R3(config)#route-map PREPEND permit 10
R3(config-route-map)#set as-path prepend 100 100
100
```

```
R3(config)# router bgp 200
```

```
R3(config-router)#neighbor 10.2.2.2 route-map
PREPEND in
```

Option C

```
R3(config)#route-map PREPEND permit 10
R3(config-route-map)#set as-path prepend 100 100
100
```

```
R3(config)# router bgp 200
```

```
R3(config-router)#neighbor 10.1.1.1 route-map
PREPEND in
```

Option D

```
R3(config)#route-map PREPEND permit 10
R3(config-route-map)#set as-path prepend 200 200
200
```

```
R3(config)# router bgp 200
```

```
R3(config-router)#neighbor 10.2.2.2 route-map
PREPEND out
```

- A. Option B

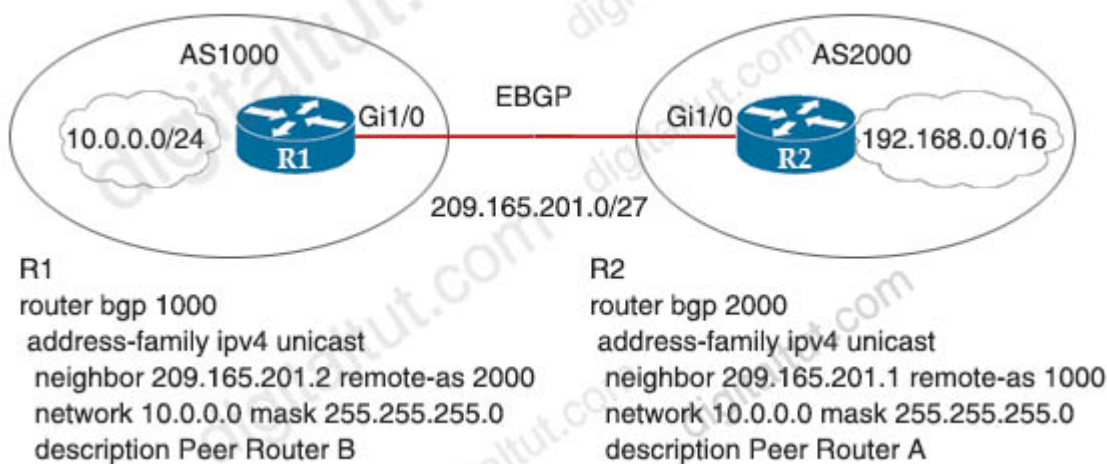
- **B. Option A** ✓
- C. Option D
- D. Option C

Explanation

R3 advertises BGP updates to R1 with multiple AS 100 so R3 believes the path to reach AS 200 via R3 is farther than R2 so R3 will choose R2 to forward traffic to AS 200.

Question 7

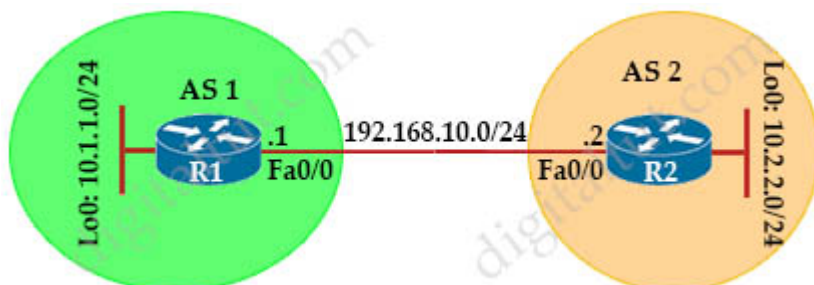
Refer to the exhibit. Which two commands are needed to allow for full reachability between AS 1000 and AS 2000? (Choose two)



- **A. R2#network 192.168.0.0 mask 255.255.0.0** ✓
- B. R1#network 19.168.0.0 mask 255.255.0.0
- C. R2#network 209.165.201.0 mask 255.255.192.0
- D. R1#no network 10.0.0.0 255.255.255.0
- **E. R2#no network 10.0.0.0 255.255.255.0** ✓

Question 8

Refer to the exhibit. Which configuration establishes EBGP neighborship between these two directly connected neighbors and exchanges the loopback network of the two routers through BGP?



- A. R1(config)#router bgp 1
 R1(config-router)#neighbor 192.168.10.2 remote-as 2
 R1(config-router)#network 10.0.0.0 mask 255.0.0.0
- R2(config)#router bgp 2
 R2(config-router)#neighbor 192.168.10.1 remote-as 1
- R2(config-router)#network 10.0.0.0 mask 255.0.0.0
- B. R1(config)#router bgp 1**
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0
- R2(config)#router bgp 2** 
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
- C. R1(config)#router bgp 1
 R1(config-router)#neighbor 10.2.2.2 remote-as 2
 R1(config-router)#neighbor 10.2.2.2 update-source lo0
 R1(config-router)#network 10.1.1.0 mask 255.255.255.0
- R2(config)#router bgp 2
 R2(config-router)#neighbor 10.1.1.1 remote-as 1
 R2(config-router)#neighbor 10.1.1.1 update-source lo0
- R2(config-router)#network 10.2.2.0 mask 255.255.255.0
- D. R1(config)#router bgp 1
 R1(config-router)#neighbor 10.2.2.2 remote-as 2
 R1(config-router)#network 10.1.1.0 mask 255.255.255.0
- R2(config)#router bgp 2
 R2(config-router)#neighbor 10.1.1.1 remote-as 1
- R2(config-router)#network 10.2.2.0 mask 255.255.255.0

Explanation

With BGP, we must advertise the correct network and subnet mask in the “network” command (in this case network 10.1.1.0/24 on R1 and network 10.2.2.0/24 on R2). BGP is very strict in the routing advertisements. In other words, BGP only advertises the network which exists exactly in the routing table. In this case, if you put the command “network x.x.0.0 mask 255.255.0.0” or “network x.0.0.0 mask 255.0.0.0” or “network x.x.x.x mask 255.255.255.255” then BGP will not advertise anything.

It is easy to establish eBGP neighborship via the direct link. But let’s see what are required when we want to establish eBGP neighborship via their loopback interfaces. We will need two commands:

- + The command “neighbor 10.1.1.1 ebgp-multihop 2” on R1 and “neighbor 10.2.2.2 ebgp-multihop 2” on R1. This command increases the TTL value to 2 so that BGP updates can reach the BGP neighbor which is two hops away.
- + A route to the neighbor loopback interface. For example: “ip route 10.2.2.0 255.255.255.0 192.168.10.2” on R1 and “ip route 10.1.1.0 255.255.255.0 192.168.10.1” on R2

Comments

1. Chen

December 11th, 2020

Hello Admins, Can you update all the BGP questions that were on your other lists please?
Similarly for other groups too. We can work on our weak areas.
This is a great help!
Thank you!

2. Anno

December 21st, 2020

Yes. Chen is correct. There are many similar qs. It is a great help if u can New q part 1-2-3 to classified sections.

1. No trackbacks yet.

Add a Comment



I'm not a robot

reCAPTCHA
[Privacy](#) - [Terms](#)

[Subscribe to comments feed](#)

[Wireless Quiz](#) [EIGRP & OSPF Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)

- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)

- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > CoPP Quiz

CoPP Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of CoPP Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
2	20	90%	20	100.00%	00:00:53

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit. An engineer configures CoPP and enters the show command to verify the implementation. What is the result of the configuration?

```
Router2#show policy-map control-plane

Control Plane
Service-policy input:CISCO
Class-map:CISCO (match-all)
  20 packets, 11280 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:access-group 120
  police:
    8000 bps, 1500 limit, 1500 extended limit
    conformed 15 packets, 6210 bytes; action:transmit
    exceeded 5 packets, 5070 bytes; action:drop
    violated 0 packets, 0 bytes; action:drop
    conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-any)
  105325 packets, 11415151 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:any
```

- A. ICMP will be denied based on this configuration
- B. Class-default traffic will be dropped
- C. If traffic exceeds the specified rate, it will be transmitted and remarked
- **D. All traffic will be policed based on access-list 120** ✓

Question 2

Which configuration restricts the amount of SSH that a router accepts 100 kbps?

Option A class-map match-all CoPP_SSH match access-group name CoPP_SSH ! policy-map CoPP_SSH class CoPP_SSH police cir 100000 exceed-action drop ! ! ! interface GigabitEthernet0/1 ip address 209.165.200.225 255.255.255.0 ip access-group CoPP_SSH out duplex auto speed auto media-type rj45 service-policy input CoPP_SSH ! ip access-list extended CoPP_SSH permit tcp any any eq 22 !	Option B class-map match-all CoPP_SSH match access-group name CoPP_SSH ! policy-map CoPP_SSH class CoPP_SSH police cir CoPP_SSH exceed-action drop ! ! ! interface GigabitEthernet0/1 ip address 209.165.200.225 255.255.255.0 ip access-group CoPP_SSH out duplex auto speed auto media-type rj45 service-policy input CoPP_SSH ! ip access-list extended CoPP_SSH deny tcp any any eq 22 !
Option C class-map match-all CoPP_SSH match access-group name CoPP_SSH ! policy-map CoPP_SSH class CoPP_SSH police cir 100000 exceed-action drop ! ! ! control-plane service-policy input CoPP_SSH ! ip access-list extended CoPP_SSH permit tcp any any eq 22 !	Option D class-map match-all CoPP_SSH match access-group name CoPP_SSH ! policy-map CoPP_SSH class CoPP_SSH police cir 100000 exceed-action drop ! ! ! control-plane transit service-policy input CoPP_SSH ! ip access-list extended CoPP_SSH permit tcp any any eq 22 !

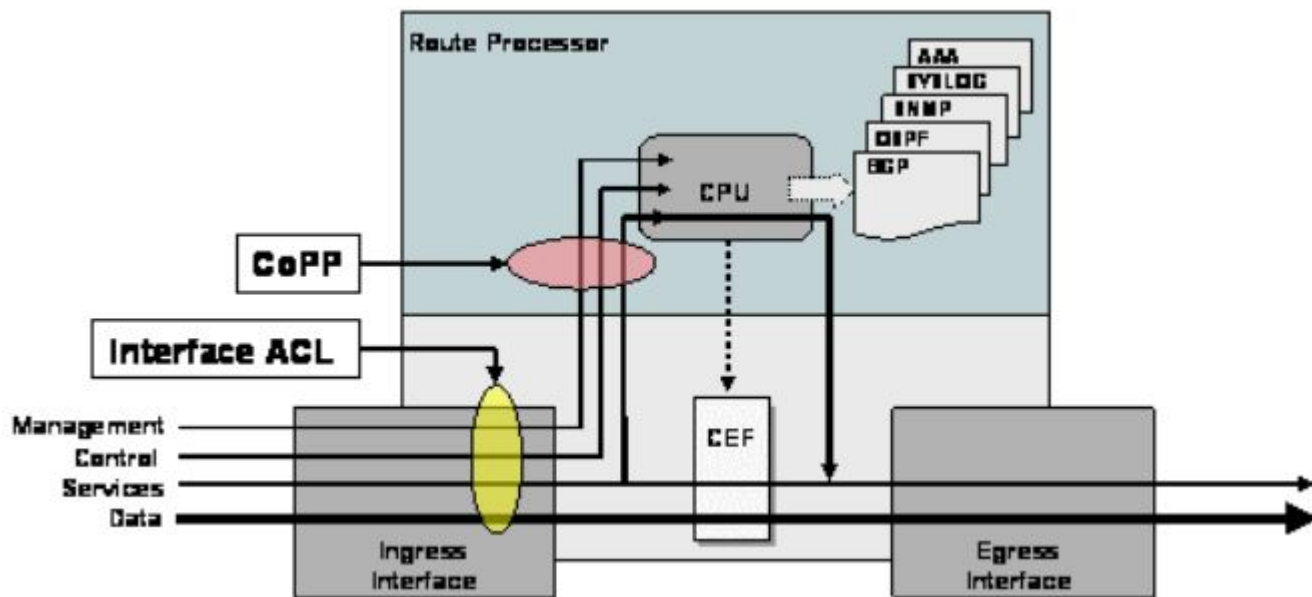
- A. Option B
- **B. Option C** ✓
- C. Option D

- D. Option A

Explanation

CoPP protects the route processor on network devices by treating route processor resources as a separate entity with its own ingress interface (and in some implementations, egress also). CoPP is used to police traffic that is destined to the route processor of the router such as:

- + Routing protocols like OSPF, EIGRP, or BGP.
- + Gateway redundancy protocols like HSRP, VRRP, or GLBP.
- + Network management protocols like telnet, SSH, SNMP, or RADIUS.



Therefore we must apply the CoPP to deal with SSH because it is in the management plane. CoPP must be put under “control-plane” command. But we cannot name the control-plane (like “transit”).

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)
[Automation 3 Quiz](#) [Multicast Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)

- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > DNA Center Quiz

DNA Center Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of DNA Center Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
10	140	90%	140	100.00%	00:01:10

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which three methods does Cisco DNA Center use to discover devices? (Choose three)

- A. NETCONF
- B. SNMP
- C. CDP ✓
- D. a specified range of IP addresses ✓
- E. ping
- F. LLDP ✓

Question 2

Refer to the exhibit.



Cisco DNA Center has obtained the username of the client and the multiple devices that the client is using on the network. How is Cisco DNA Center getting these context details?

- A. User entered those details in the Assurance app available on iOS and Android devices
- B. The administrator had to assign the username to the IP address manually in the user database tool on Cisco DNA Center
- **C. Cisco DNA Center pulled those details directly from the edge node where the user connected** ✓
- D. Those details are provided to Cisco DNA Center by the Identity Services Engine

Explanation

Features of the Cisco DNA Assurance solution includes Device 360 and client 360, which provides a detailed view of the performance of any device or client over time and from any application context. Provides very granular troubleshooting in seconds.

Question 3

At which layer does Cisco DNA Center support REST controls?

- A. Session layer
- B. EEM applets or scripts
- **C. Northbound APIs** ✓
- D. YML output from responses to API calls

Question 4

Which two characteristics define the Intent API provided by Cisco DNA Center? (Choose two)

- **A. northbound API** ✓
- **B. business outcome oriented** ✓
- C. procedural
- D. southbound API
- E. device-oriented

Explanation

The Intent API is a **Northbound REST API** that exposes specific capabilities of the Cisco DNA Center platform. The Intent API provides policy-based abstraction of **business intent, allowing focus on an outcome** rather than struggling

with individual mechanisms steps.

Reference: <https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/intent-api-northbound>

Question 5

What does the Cisco DNA Center use to enable the delivery of applications through a network and to yield analytics for innovation?

- A. Command Runner
- B. process adapters
- C. domain adapters
- **D. intent-based APIs** ✓

Explanation

The Cisco DNA Center open platform for intent-based networking provides 360-degree extensibility across multiple components, including:

+ **Intent-based APIs** leverage the controller to enable business and IT applications to deliver intent to the network and to reap network analytics and insights for IT and business innovation. These enable APIs that allow Cisco DNA Center to receive input from a variety of sources, both internal to IT and from line-of-business applications, related to application policy, provisioning, software image management, and assurance.

...

Reference: <https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-cent-plat-sol-over-cte-en.html>

Question 6

Which two steps are required for a complete Cisco DNA Center upgrade? (Choose two)

- **A. system update** ✓
- B. automation backup
- **C. application updates** ✓
- D. golden image selection
- E. proxy configuration

Explanation

A complete Cisco DNA Center upgrade includes “System Update” and “Appplication Updates”

System Update

System 1.3.0.109

 Your system package is up to date. Proceed with Application updates.

Application Updates

Update All



Cisco DNA Center Core

	Size	Version	
Automation - Base	493.25 MB	2.1.78.60109	Update failed
NCP - Base	167.84 MB	2.1.78.60109	Update failed
NCP - Services	326.84 MB	2.1.78.60109	Update failed
Network Controller Platform	3.65 GB	2.1.78.60109	Update failed

Automation

	Size	Version	
Command Runner	55.20 MB	2.1.78.60109	Update failed
Device Onboarding	162.41 MB	2.1.78.60109	Update failed
Image Management	362.85 MB	2.1.78.60109	Update failed

Question 7

Which devices does Cisco DNA Center configure when deploying an IP-based access control policy?

- A. All devices integrating with ISE
- B. selected individual devices
- C. all wired devices
- D. all devices in selected sites

Explanation

When you click **Deploy**, Cisco DNA Center requests the Cisco Identity Services Engine (Cisco ISE) to send notifications about the policy changes to the network devices.

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-1-0/user_guide/b_cisco_dna_center_ug_1_3_1_0/b_cisco_dna_center_ug_1_3_1_0_chapter_01011.html

Question 8

Which tool is used in Cisco DNA Center to build generic configurations that are able to be applied on device with similar network settings?

- A. Application Policies
- B. Command Runner
- C. Authentication Template
- D. Template Editor

Explanation

Cisco DNA Center provides an interactive editor called Template Editor to author CLI templates. Template Editor is a centralized CLI management tool to help design a set of device configurations that you need to build devices in a branch. When you have a site, office, or branch that uses a similar set of devices and configurations, you can use Template Editor to build generic configurations and apply the configurations to one or more devices in the branch.

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3/user_guide/b_cisco_dna_center_ug_1_3/b_cisco_dna_center_ug_1_3_chapter_0111.html

Question 9

Which method does Cisco DNA Center use to allow management of non-Cisco devices through southbound protocols?

- **A. It creates device packs through the use of an SDK** ✓
- B. It obtains MIBs from each vendor that details the APIs available.
- C. It uses an API call to interrogate the devices and register the returned data.
- D. It imports available APIs for the non-Cisco device in a CSV format.

Explanation

Cisco DNA Center allows customers to manage their non-Cisco devices through the use of a Software Development Kit (SDK) that can be used to create Device Packages for third-party devices.

Reference: <https://developer.cisco.com/docs/dna-center/#!/cisco-dna-center-platform-overview/multivendor-support-southbound>

Question 10

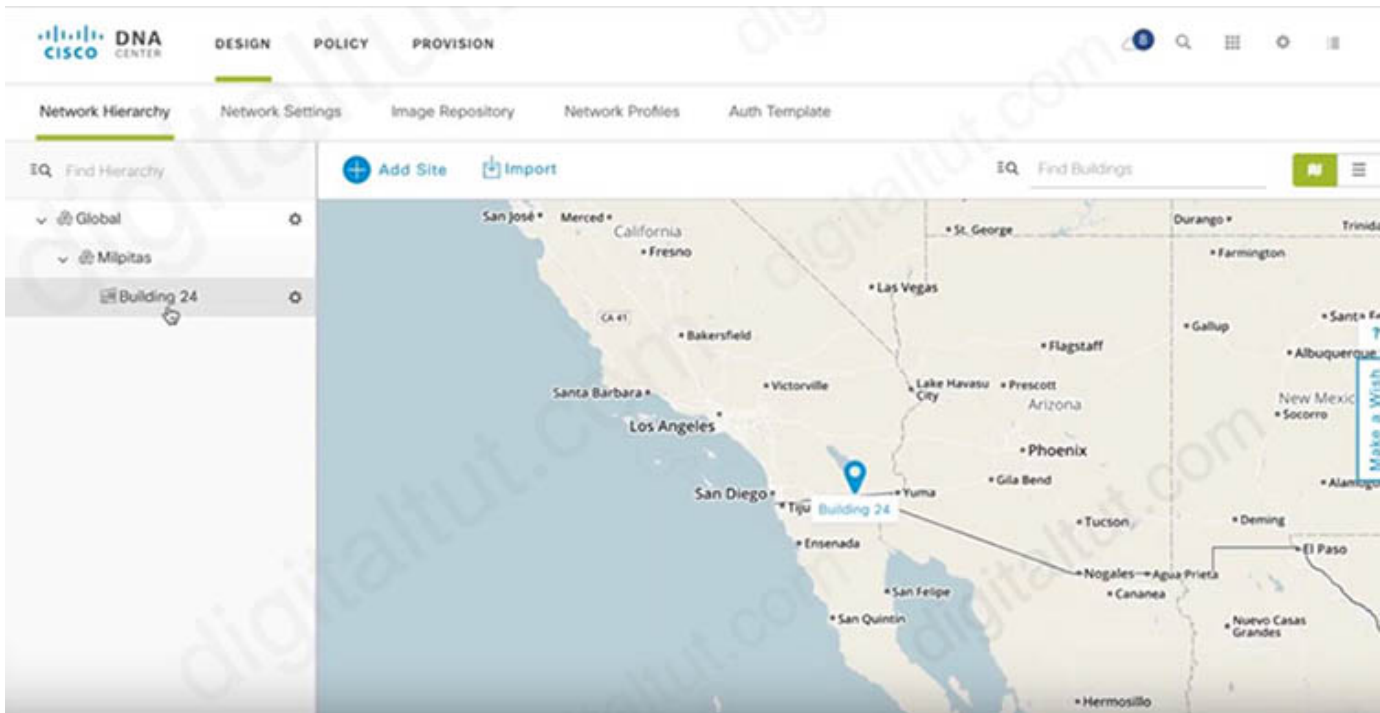
An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?

- A. by hostname naming convention
- B. by role
- C. by organization
- **D. by location** ✓

Explanation

You can create a network hierarchy that represents your network's geographical locations. Your network hierarchy can contain sites, which in turn contain buildings and areas. You can create site and building IDs to easily identify where to apply design settings or configurations later.

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-5/user_guide/b_dnac_ug_1_2_5/b_dnac_ug_1_2_4_chapter_0110.html



Comments

1. No comments yet.
1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[Architecture Quiz SD-WAN & SD-Access Solutions 2 Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH



[Home](#) > Drag Drop 2 Quiz

Drag Drop 2 Quiz

 January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Drag Drop 2 Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
3	165	90%	165	100.00%	00:11:33

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Drag and drop the characteristics from the left onto the routing protocols they describe on the right.

Please type the corresponding numbers of each item on the left to the blank below and arrange them ascendingly. For example: 136245 (which means 136 for first group, 245 for second group).

1	Link State Protocol	OSPF
2	selects routes using the DUAL algorithm	
3	maintains alternative loop-free backup path if available	
4	supports only equal multipath load balancing	EIGRP
5	Advanced Distance Vector Protocol	
6	quickly computes new path upon link failure	

Please type your answer here: **146235** ✓

Explanation

EIGRP maintains alternative loop-free backup via the feasible successors. To qualify as a feasible successor, a router must have an Advertised Distance (AD) less than the Feasible distance (FD) of the current successor route.

Advertised distance (AD): the cost from the neighbor to the destination.

Feasible distance (FD): The sum of the AD plus the cost between the local router and the next-hop router

Question 2

Drag and drop the DHCP messages that are exchanged between a client and an AP into the order they are exchanged on the right.

Note: You just need to click on one of the boxes on the right to match it with the corresponding box on the left.

Step 1 DHCP Discover ✓

Step 2 DHCP Offer ✓

Step 3 DHCP Request ✓

Step 4 DHCP ACK ✓

Explanation

There are four messages sent between the DHCP Client and DHCP Server: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACKNOWLEDGEMENT. This process is often abbreviated as **DORA** (for Discover, Offer, Request, Acknowledgement).

Question 3

Drag and drop the LIPS components on the left to the correct description on the right.

Note: You just need to click on one of the boxes on the right to match it with the corresponding box on the left.

IPv4 or IPv6 address of an endpoint within a LISP site

EID ✓

network infrastructure component that learns of EID-prefix mapping entries from an ETR

map server ✓

de-encapsulates LISP packets coming from outside of the LISP site to destinations inside

ETR ✓

of the site

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[AAA Quiz](#) [Troubleshooting Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)

- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)

- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > EIGRP & OSPF 2 Quiz

EIGRP & OSPF 2 Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of EIGRP & OSPF 2 Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
7	70	90%	70	100.00%	00:00:41

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

How does the EIGRP metric differ from the OSPF metric?

- A. The EIGRP metric is calculated based on hop count and bandwidth. The OSPF metric is calculated on bandwidth and delay.
- B. The EIGRP metric is calculated based on delay only. The OSPF metric is calculated on bandwidth and delay.
- C. The EIGRP metric is calculated based on bandwidth and delay. The OSPF metric is calculated on bandwidth only.**
- D. The EIGRP metric is calculated based on bandwidth only. The OSPF metric is calculated on delay only.



Explanation

By default, EIGRP metric is calculated:

metric = bandwidth + delay

While OSPF is calculated by:

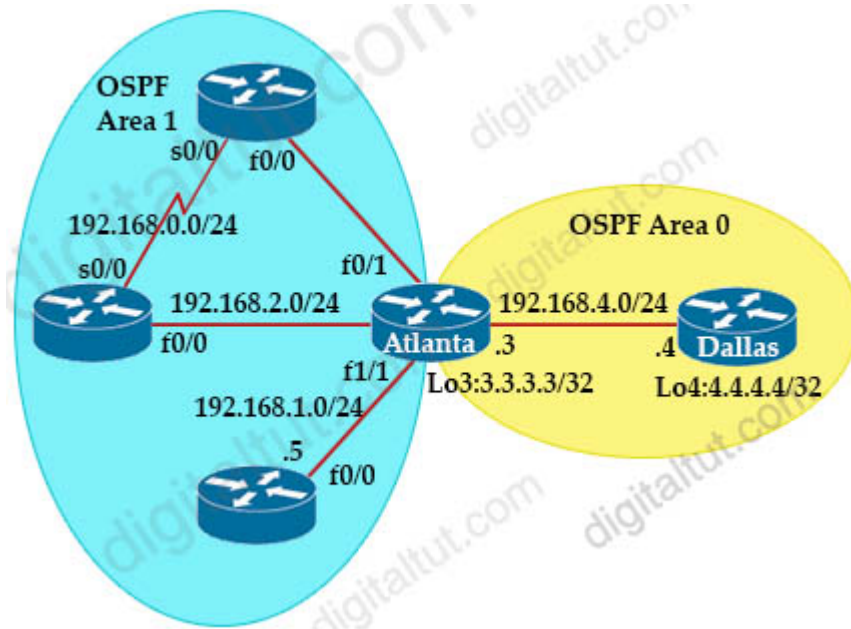
OSPF metric = Reference bandwidth / Interface bandwidth in bps

(Or Cisco uses 100Mbps (10^8) bandwidth as reference bandwidth. With this bandwidth, our equation would be:

Cost = 10^8 /interface bandwidth in bps)

Question 2

Refer to the exhibit.



Dallas#show ip route ospf

3.0.0.0/32 i subnetted, 1 subnets

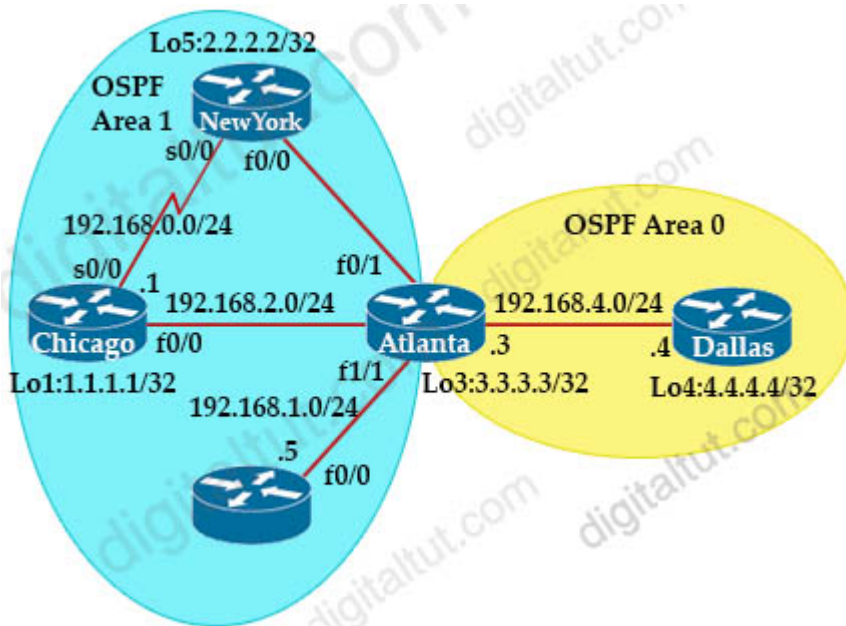
```
O 3.3.3.3 [110/40001] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.0.0/24 [110/145535] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.1.0/24 [110/80000] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.2.0/24 [110/80000] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.3.0/24 [110/44000] via 192.168.4.3, 00:33:32, FastEthernet0/0
```

Which command when applied to the Atlanta router reduces type 3 LSA flooding into the backbone area and summarizes the inter-area routes on the Dallas router?

- A. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.248.0
- B. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.248.0
- C. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.252.0
- **D. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.252.0** ✓

Question 3

Refer the exhibit.



```
Chicago#show ip ospf nei
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/BDR	00:00:35	192.168.2.3	FastEthernet0/0
2.2.2.2	0	FULL/-	00:00:35	192.168.0.2	Serial0/0

```
Chicago#show ip ospf int bri
```

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Fa0/0	1	1	192.168.2.1/24	40444	DR	1/1	
Se0/0	1	1	192.168.0.1/24	65535	P2P	1/1	

Which router is the designated router on the segment 192.168.0.0/24?

- **A. This segment has no designated router because it is a p2p network type.** ✓
- B. Router NewYork because it has a higher router ID
- C. This segment has no designated router because it is a nonbroadcast network type.
- D. Router Chicago because it has a lower router ID

Question 4

Which feature of EIGRP is not supported in OSPF?

- A. per-packet load balancing over multiple paths
- **B. load balancing of unequal-cost paths** ✓
- C. load balance over four equal-costs paths
- D. uses interface bandwidth to determine best path

Question 5

Refer to the exhibit. An engineer attempts to configure a router on a stick to route packets between Clients, Servers, and Printers; however, initial tests show that this configuration is not working. Which command set resolves this issue?

```

interface Vlan10
ip vrf forwarding Clients
ip address 192.168.1.1 255.255.255.0
!
interface Vlan20
ip vrf forwarding Servers
ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
ip vrf forwarding Printers
ip address 10.1.1.1 255.255.255.0
<output omitted>
router eigrp 1
network 10.0.0.0
network 172.16.0.0
network 192.168.1.0

```

Option A router eigrp 1 network 10.0.0.0 255.0.0.0 network 172.16.0.0 255.255.0.0 network 192.168.1.0 255.255.0.0	Option B router eigrp 1 network 10.0.0.0 255.255.255.0 network 172.16.0.0 255.255.255.0 network 192.168.1.0 255.255.255.0
Option C interface Vlan10 no ip vrf forwarding Clients ! interface Vlan20 no ip vrf forwarding Servers ! interface Vlan30 no ip vrf forwarding Printers	Option D interface Vlan10 no ip vrf forwarding Clients ip address 192.168.1.2 255.255.255.0 ! interface Vlan20 no ip vrf forwarding Servers ip address 172.16.1.2 255.255.255.0 ! interface Vlan30 no ip vrf forwarding Printers ip address 10.1.1.2 255.255.255.0

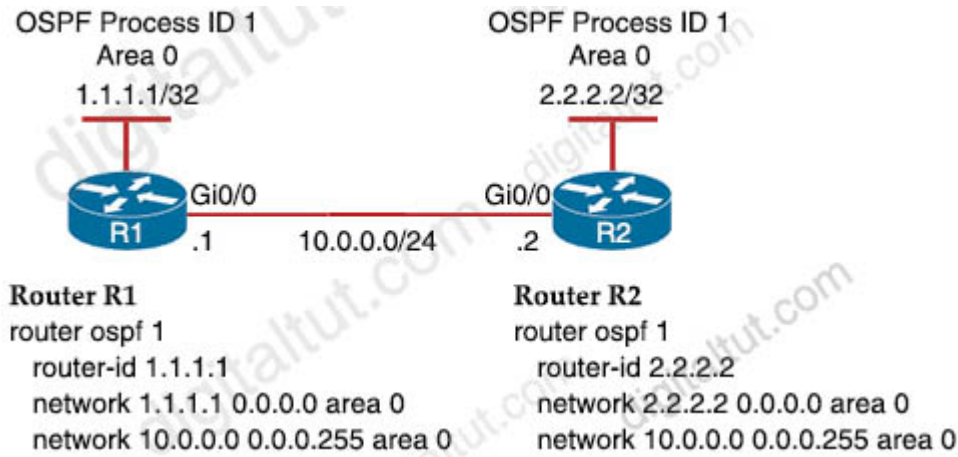
- **A. Option D** ✓
- B. Option A
- C. Option C
- D. Option B

Explanation

We must reconfigure the IP address after assigning or removing an interface to a VRF. Otherwise that interface does not have an IP address.

Question 6

Refer to the exhibit.



A network engineer is configuring OSPF between router R1 and router R2. The engineer must ensure that a DR/BDR election does not occur on the Gigabit Ethernet interfaces in area 0. Which configuration set accomplishes this goal?

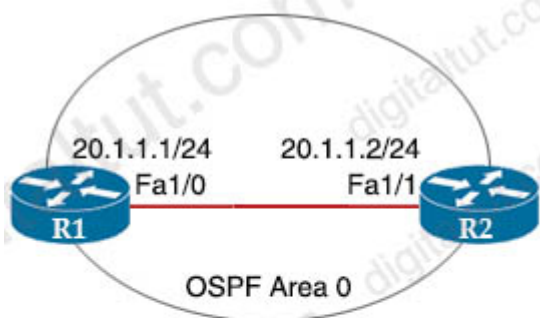
- A. R1(config-if)#interface Gi0/0
 R1(config-if)#ip ospf database-filter all out
- R2(config-if)#interface Gi0/0
 • R2(config-if)#ip ospf database-filter all out
- B. R1(config-if)#interface Gi0/0
 R1(config-if)#ip ospf network broadcast
- R2(config-if)#interface Gi0/0
 • R2(config-if)#ip ospf network broadcast
- **C. R1(config-if)#interface Gi0/0
 R1(config-if)#ip ospf network point-to-point**
- R2(config-if)#interface Gi0/0**
R2(config-if)#ip ospf network point-to-point
- D. R1(config-if)#interface Gi0/0
 R1(config-if)#ip ospf priority 1
- R2(config-if)#interface Gi0/0
 • R2(config-if)#ip ospf priority 1

Explanation

Broadcast and Non-Broadcast networks elect DR/BDR while Point-to-point/multipoint do not elect DR/BDR. Therefore we have to set the two Gi0/0 interfaces to point-to-point or point-to-multipoint network to ensure that a DR/BDR election does not occur.

Question 7

Refer to the exhibit.



```

hostname R1
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
auto-cost reference-bandwidth 1000
!
hostname R2
router ospf 2
network 20.0.0.0 0.0.0.255 area 0

```

Which command must be applied to R2 for an OSPF neighborship to form?

- A. network 20.1.1.2 0.0.255.255 area 0
- **B. network 20.1.1.2 0.0.0.0 area 0** ✓
- C. network 20.1.1.2 255.255.255.255 area 0
- D. network 20.1.1.2 255.255.0.0. area 0

Explanation

The “network 20.0.0.0 0.0.0.255 area 0” command on R2 did not cover the IP address of Fa1/1 interface of R2 so OSPF did not run on this interface. Therefore we have to use the command “network 20.1.1.2 0.0.255.255 area 0” to turn on OSPF on this interface.

Note: The command “network 20.1.1.2 0.0.255.255 area 0” can be used too so this answer is also correct but answer 'network 20.1.1.2 0.0.0.0 area 0' is the best answer here.

The “network 0.0.0.0 255.255.255.255 area 0” command on R1 will run OSPF on all active interfaces of R1.

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms[Submit Comment](#)[Subscribe to comments feed](#)[Multicast Quiz](#) [Wireless 2 Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)

- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > EIGRP & OSPF Quiz

EIGRP & OSPF Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of EIGRP & OSPF Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
10	110	90%	110	100.00%	00:00:44

Congratulations!

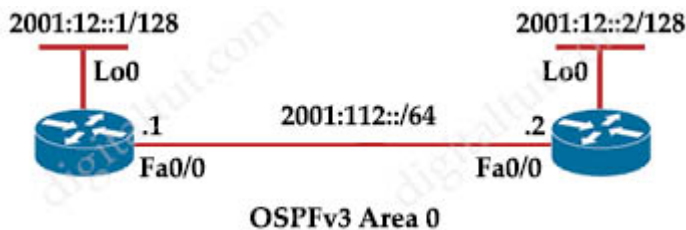
You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit. Which IPv6 OSPF network type is applied to interface Fa0/0 of R2 by default?



- A. Ethernet
- B. multipoint
- C. point-to-point
- **D. broadcast** ✓

Explanation

The Broadcast network type is the default for an OSPF enabled ethernet interface (while Point-to-Point is the default OSPF network type for Serial interface with HDLC and PPP encapsulation).

Reference: <https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch08s15.html>

Question 2

Which EIGRP feature allows the use of leak maps?

- A. neighbor
- **B. stub** ✓
- C. address-family
- D. offset-list

Explanation

If we configured an EIGRP stub router so that it only advertises connected and summary routes. But we also want to have an exception to this rule then we can configure a leak-map. For example:

```
R4(config-if)#router eigrp 1
R4(config-router)#eigrp stub
R4(config)#ip access-list standard R4_L0opback0
R4(config-std-nacl)#permit host 4.4.4.4
R4(config)#route-map R4_L0opback0_LEAKMAP
R4(config-route-map)#match ip address R4_L0opback0
R4(config)#router eigrp 1
R4(config-router)#eigrp stub leak-map R4_L0opback0_LEAKMAP
```

As we can see the leak-map feature goes long with 'eigrp stub' command.

Question 3

Which statement about LISP encapsulation in an EIGRP OTP implementation is true?

- A. OTP maintains the LISP control plane
- **B. OTP uses LISP encapsulation for dynamic multipoint tunneling** ✓
- C. LISP learns the next hop
- D. OTP uses LISP encapsulation to obtain routes from neighbors

Explanation

OTP leverages existing LISP encapsulation which:

+ Allows dynamic multi-point tunneling (-> Answer 'OTP uses LISP encapsulation for dynamic multipoint tunneling' is correct)

+ Provides instance ID field to optionally support virtualization across WAN (see EVN WAN Extension section)

OTP does NOT use LISP control plane (map server/resolver, etc.) (-> Therefore answer 'OTP maintains the LISP control plane' is not correct) **instead it uses EIGRP to exchange routes and provide the next-hop** (-> answer 'OTP uses LISP encapsulation to obtain routes from neighbors' and answer 'LISP learns the next hop' are not correct), which LISP encapsulation uses to reach remote prefixes.

Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ip-routing/whitepaper_C11-730404.html

Question 4

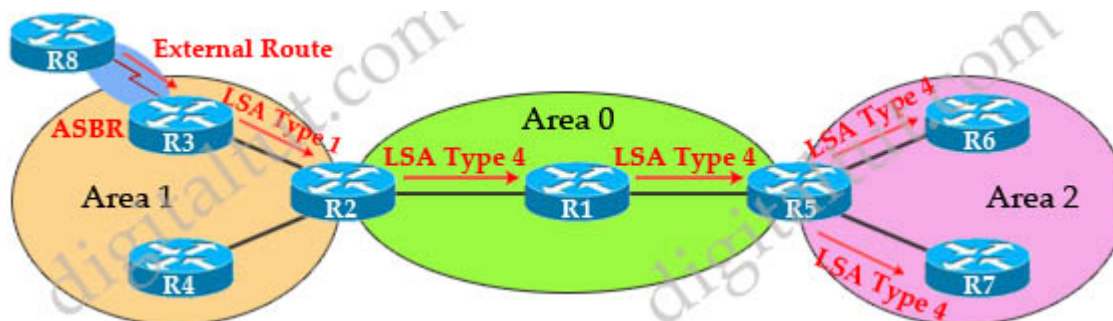
In OSPF, which LSA type is responsible for pointing to the ASBR router?

- A. type 3
- B. type 1
- C. type 2
- **D. type 4** ✓

Explanation

Summary ASBR LSA (Type 4) – Generated by the ABR to describe an ASBR to routers in other areas so that routers in other areas know how to get to external routes through that ASBR. For example, suppose R8 is redistributing external route (EIGRP, RIP...) to R3. This makes R3 an Autonomous System Boundary Router (ASBR). When R2 (which is an ABR) receives this LSA Type 1 update, R2 will create LSA Type 4 and flood into Area 0 to inform them how to reach R3. When R5 receives this LSA it also floods into Area 2.

In the above example, the only ASBR belongs to area 1 so the two ABRs (R2 & R5) send LSA Type 4 to area 0 & area 2 (not vice versa). This is an indication of the existence of the ASBR in area 1.



Note:

- + Type 4 LSAs contain the router ID of the ASBR.
- + There are no LSA Type 4 injected into Area 1 because every router inside area 1 knows how to reach R3. R3 only uses LSA Type 1 to inform R2 about R8 and inform R2 that R3 is an ASBR.

Question 5

Which OSPF network types are compatible and allow communication through the two peering devices?

- A. point-to-multipoint to nonbroadcast
- B. point-to-multipoint to broadcast
- **C. broadcast to nonbroadcast** ✓
- D. broadcast to point-to-point

Explanation

The following different OSPF types are compatible with each other:

- + Broadcast and Non-Broadcast (adjust hello/dead timers)
- + Point-to-Point and Point-to-Multipoint (adjust hello/dead timers)

Broadcast and Non-Broadcast networks elect DR/BDR so they are compatible. Point-to-point/multipoint do not elect DR/BDR so they are compatible.

Question 6

Based on this interface configuration, what is the expected state of OSPF adjacency?

```
R1
interface GigabitEthernet0/1
 ip address 192.0.2.1 255.255.255.252
 ip ospf 1 area 0
 ip ospf hello-interval 2
 ip ospf cost 1
```

```
R2
interface GigabitEthernet0/1
 ip address 192.0.2.2 255.255.255.252
 ip ospf 1 area 0
 ip ospf cost 500
```

- **A. not established** ✓
- B. Full on both routers
- C. FULL/BDR on R1 and FULL/BDR on R2
- D. 2WAY/DROTHER on both routers

Explanation

On Ethernet interfaces the OSPF hello interval is 10 second by default so in this case there would be a Hello interval mismatch -> the OSPF adjacency would not be established.

Question 7

Refer to the exhibit. Which statement about the OPSF debug output is true?

```
R1#debug ip ospf hello
R1#debug condition interface fa0/1
Condition 1 set
```

- A. The output displays OSPF hello and LSACK messages which router R1 has sent or received
- B. The output displays all OSPF messages which router R1 has sent or received on interface Fa0/1
- **C. The output displays OSPF hello messages which router R1 has sent or received on interface Fa0/1** ✓
- D. The output displays all OSPF messages which router R1 has sent or received on all interfaces

Explanation

This combination of commands is known as “Conditional debug” and will filter the debug output based on your conditions. Each condition added, will behave like an ‘And’ operator in Boolean logic. Some examples of the “debug ip ospf hello” are shown below:

```
*Oct 12 14:03:32.595: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet1/0 from 192.168.12.2
*Oct 12 14:03:33.227: OSPF: Rcv hello from 1.1.1.1 area 0 on FastEthernet1/0 from 192.168.12.1
*Oct 12 14:03:33.227: OSPF: Mismatched hello parameters from 192.168.12.1
```

Comments

Question 8

Which feature is supported by EIGRP but is not supported by OSPF?

- A. route filtering
- B. equal-cost load balancing
- C. route summarization
- **D. unequal-cost load balancing** ✓

Explanation

EIGRP support unequal-cost load balancing via the “variance ...” while OSPF only supports equal-cost load balancing.

Question 9

Which two statements about EIGRP load balancing are true? (Choose two)

- A. EIGRP supports unequal-cost paths by default
- **B. EIGRP supports 6 unequal-cost paths** ✓
- C. Cisco Express Forwarding is required to load-balance across interfaces
- **D. A path can be used for load balancing only if it is a feasible successor** ✓
- E. Any path in the EIGRP topology table can be used for unequal-cost load balancing

Explanation

EIGRP provides a mechanism to load balance over unequal cost paths (or called unequal cost load balancing) through the “variance” command. In other words, EIGRP will install all paths with **metric < variance * best_metric** into the local routing table, provided that it meets the feasibility condition to prevent routing loop. The path that meets this requirement is called a feasible successor. If a path is not a feasible successor, it is not used in load balancing.

Note: The feasibility condition states that, the Advertised Distance (AD) of a route must be lower than the feasible distance of the current successor route.

Question 10

Which reason could cause an OSPF neighborship to be in the EXSTART/EXCHANGE state?

- A. Mismatched OSPF network type
- **B. Mismatched MTU size** ✓
- C. Mismatched areas
- D. Mismatched OSPF link costs

Explanation

When OSPF adjacency is formed, a router goes through several state changes before it becomes fully adjacent with its neighbor. The states are Down -> Attempt (optional) -> Init -> 2-Way -> Exstart -> Exchange -> Loading -> Full. Short descriptions about these states are listed below:

Down: no information (hellos) has been received from this neighbor.

Attempt: only valid for manually configured neighbors in an NBMA environment. In Attempt state, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval.

Init: specifies that the router has received a hello packet from its neighbor, but the receiving router's ID was not included in the hello packet

2-Way: indicates bi-directional communication has been established between two routers.

Exstart: Once the DR and BDR are elected, the actual process of exchanging link state information can start between the routers and their DR and BDR.

Exchange: OSPF routers exchange database descriptor (DBD) packets

Loading: In this state, the actual exchange of link state information occurs

Full: routers are fully adjacent with each other

(Reference: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml)

Neighbors Stuck in Exstart/Exchange State

The problem occurs most frequently when attempting to run OSPF between a Cisco router and another vendor's router. The problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces don't match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

1. VK

September 23rd, 2020

What's the correct answer for this question "Which statement about LISP encapsulation in an EIGRP OTP implementation is true?"

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)
[BGP Quiz](#) [Virtualization Quiz](#)

Premium Member Zone

Welcome [Ashwin Tharan!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)

- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH



[Home](#) > Etherchannel Quiz

Etherchannel Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Etherchannel Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
3	30	90%	30	100.00%	00:04:37

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which PAgP mode combination prevents an Etherchannel from forming?

- A. auto/desirable
- B. desirable
- C. desirable/desirable
- **D. auto/auto** ✓

Explanation

There are two PAgP modes:

Auto	Responds to PAgP messages but does not aggressively negotiate a PAgP EtherChannel. answer 'auto/auto' channel is formed only if the port on the other end is set to Desirable. This is the default mode.
Desirable	Port actively negotiates channeling status with the interface on the other end of the link. answer 'auto/auto' channel is formed if the other side is Auto or Desirable.

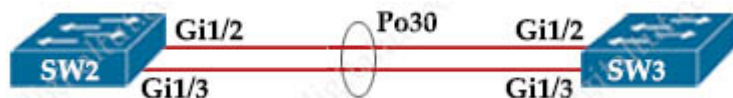
The table below lists if an EtherChannel will be formed or not for PAgP:

PAgP	Desirable	Auto
Desirable	Yes	Yes
Auto	No	No

Auto	Yes	No

Question 2

Refer to the exhibit. A port channel is configured between SW2 and SW3. SW2 is not running Cisco operating system. When all physical connections are made, the port channel does not establish. Based on the configuration excerpt of SW3, what is the cause of the problem?



```
interface gi1/2
channel-group 30 mode desirable
port-channel load-balance src-ip
```

```
interface gi1/3
channel-group 30 mode desirable
port-channel load-balance src-ip
```

```
interface PortChannel 30
switchport mode trunk
switchport encapsulation dot1q
switchport trunk allowed vlan 10-100
```

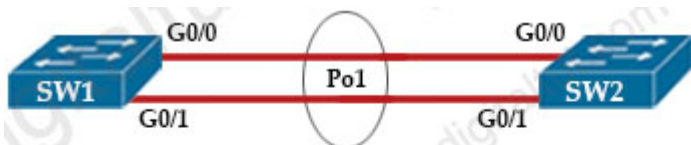
- A. The port channel on SW2 is using an incompatible protocol ✓
- B. The port-channel should be set to auto
- C. The port-channel interface load balance should be set to src-mac
- D. The port-channel trunk is not allowing the native VLAN

Explanation

The Cisco switch was configured with PAgP, which is a Cisco proprietary protocol so non-Cisco switch could not communicate.

Question 3

Refer to the exhibit.



```
SW1# show etherchannel summary
```

```
! output omitted
```

Group	Port-channel	Protocol	Ports
1	Po1 (SD)	-	

```
SW2#
```

```
08:33:23: %PM-4-ERR_DISABLE: channel-misconfig error detection on Gi0/0, putting Gi0/0 in err-
```

disable state

08:33:23: %PM-4-ERR_DISABLE: channel-misconfig error detection on Gi0/1, putting Gi0/1 in err-disable state

After an engineer configures an EtherChannel between switch SW1 and switch SW2, this error message is logged on switch SW2.

Based on the output from SW1 and the log message received on Switch SW2, what action should the engineer take to resolve this issue?

- A. Define the correct port members on the EtherChannel on switch SW1.
- **B. Configure the same protocol on the EtherChannel on switch SW1 and SW2. ✓**
- C. Connect the configuration error on interface Gi0/1 on switch SW1.
- D. Correct the configuration error on interface Gi0/0 switch SW1.

Explanation

In this case, we are using your EtherChannel without a negotiation protocol. As a result, if the opposite switch is not also configured for EtherChannel operation on the respective ports, there is a danger of a switching loop. The EtherChannel Misconfiguration Guard tries to prevent that loop from occurring by disabling all the ports bundled in the EtherChannel.

Comments

1. d3p

November 19th, 2020

“When all physical connections are mode”... when all physical connections are *made*?

2. digitaltut

November 20th, 2020

@d3p: Thanks for your detection, we have just updated it!

3. Sonda de Mexico

January 30th, 2021

9tut I don't see the picture of question # 3

4. Sonda de Mexico

January 30th, 2021

30 00:11:58: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

i dont see the picture

5. digitaltut

January 30th, 2021

@Sonda de Mexico: Thanks for your detection, we have just fixed it!

1. No trackbacks yet.

Add a Comment



I'm not a robot

reCAPTCHA
Privacy - Terms[Subscribe to comments feed](#)[Trunking Quiz](#) [OSPF LSA Types Tutorial](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)

- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)

- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > GRE Tunnel Quiz

GRE Tunnel Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of GRE Tunnel Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
10	120	90%	120	100.00%	00:06:52

Congratulations!

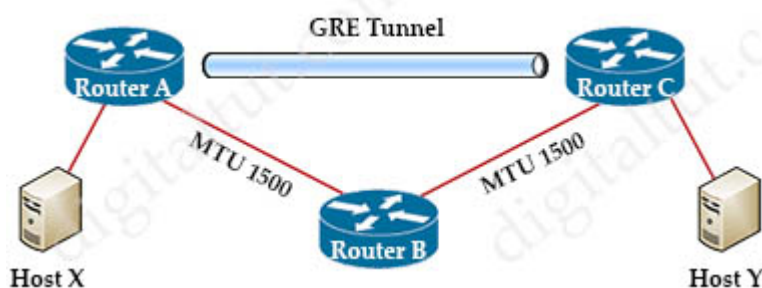
You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to exhibit.



MTU has been configured on the underlying physical topology, and no MTU command has been configured on the tunnel interfaces. What happens when a 1500-byte IPv4 packet traverses the GRE tunnel from host X to host Y, assuming the DF bit is cleared?

- A. The packet arrives on router C without fragmentation.
- B. The packet is discarded on router A
- **C. The packet arrives on router C fragmented.** ✓
- D. The packet is discarded on router B

Explanation

If the DF bit is set to clear (not set), routers can fragment packets regardless of the original DF bit setting.

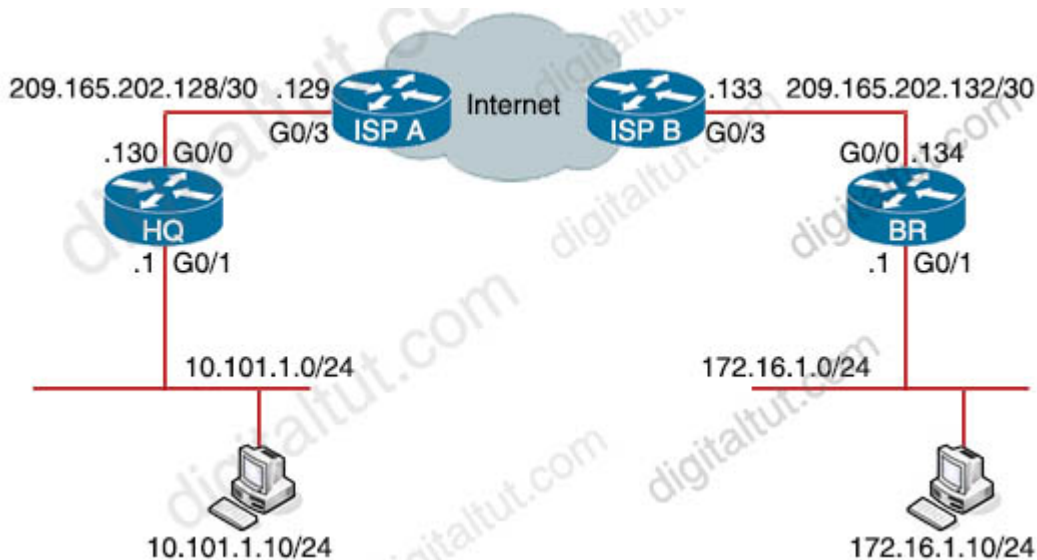
Whenever we create tunnel interfaces, the GRE IP MTU is automatically configured 24 bytes less than the outbound physical interface MTU. Ethernet interfaces have an MTU value of 1500 bytes so tunnel interfaces by default will have 1476 bytes MTU, which is 24 bytes less the physical interface. The process of sending a 1500-byte IPv4 packet (with DF bit set to clear) is shown below:

1. The sender sends a 1500-byte packet (20 byte IPv4 header + 1480 bytes of TCP payload).
2. Since the MTU of the GRE tunnel is 1476, the 1500-byte packet is broken into two IPv4 fragments of 1476 and 44 bytes, each in anticipation of the additional 24 bytes of GRE header.
3. The 24 bytes of GRE header is added to each IPv4 fragment. Now the fragments are 1500 (1476 + 24) and 68 (44 + 24) bytes each.
4. The GRE + IPv4 packets that contain the two IPv4 fragments are forwarded to the GRE tunnel peer router.
5. The GRE tunnel peer router removes the GRE headers from the two packets.
6. This router forwards the two packets to the destination host.
7. The destination host reassembles the IPv4 fragments back into the original IPv4 datagram.

Reference: <https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html> (Scenario 5)

Question 2

Refer to the exhibit.



Option A interface Tunnell ip address 209.165.202.130 255.255.255.252 tunnel source GigabitEthernet0/0 tunnel destination 209.165.202.129	Option B interface Tunnell ip address 10.111.111.1 255.255.255.0 tunnel source GigabitEthernet0/0 tunnel destination 209.165.202.133
Option C interface Tunnell ip address 10.111.111.1 255.255.255.0 tunnel source GigabitEthernet0/0 tunnel destination 209.165.202.134	Option D interface Tunnell ip address 10.111.111.1 255.255.255.0 tunnel source GigabitEthernet0/0 tunnel destination 209.165.202.129

Which configuration must be applied to the HQ router to set up a GRE tunnel between the HQ and BR routers?

- A. Option B
- **B. Option C** ✓
- C. Option D
- D. Option A

Question 3

Refer to the exhibit.

```
Router1#
Router1#show run int tunnel 0
Building configuration...

Current configuration : 93 bytes
!
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel destination 192.168.10.2
end
```

```
Router1#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.1.1	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/3	unassigned	YES	unset	administratively down	down
Loopback0	192.168.10.1	YES	manual	up	up
Tunnel0	172.16.1.1	YES	manual	up	down

Which command must be applied to Router1 to bring the GRE tunnel to an up/up state?

- A. Router1(config-if)#tunnel source GigabitEthernet0/1
- **B. Router1(config-if)#tunnel source Loopback0** ✓
- C. Router1(config)#interface tunnel0
- D. Router1(config-if)#tunnel mode gre multipoint

Explanation

In order to make a Point-to-Point GRE Tunnel interface in up/up state, two requirements must be met:

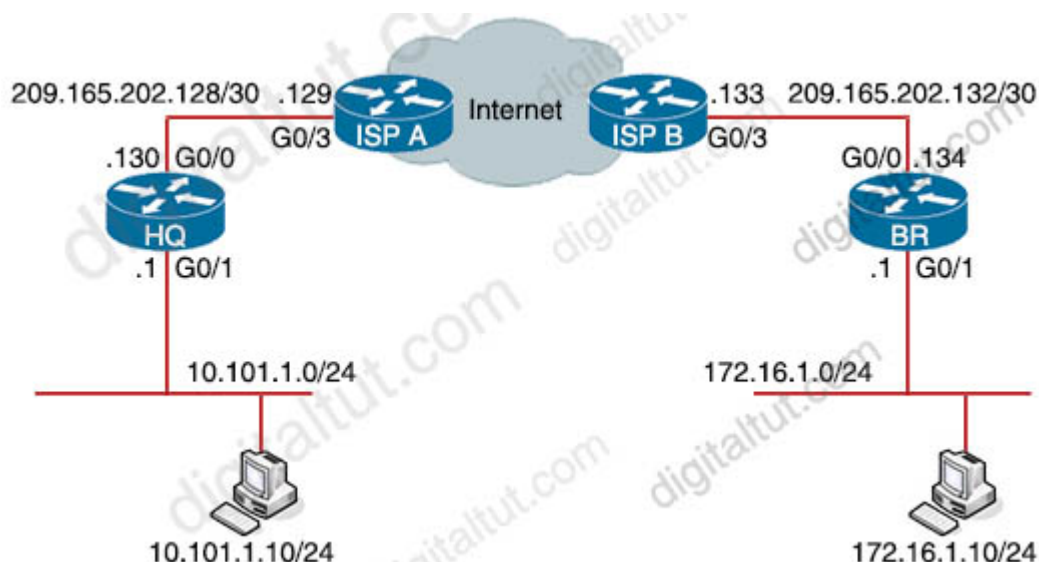
+ A **valid tunnel source (which is in up/up state)** and has an IP address configured on it) and tunnel destination must be configured

+ A valid tunnel destination is one which is routable. However, it does not have to be reachable.

-> In this question we are missing an up/up source so we can choose Loopback 0 interface.

Question 4

Refer to the exhibit.



> Frame 24: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
 > Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 50:00:00:02:00:01 (50:00:00:02:00:01)
 > Internet Protocol Version 4, Src: 209.165.202.130, Dst: 209.165.202.134
 > Generic Routing Encapsulation (IP)
 > Internet Protocol Version 4, Src: 10.111.111.1, Dst: 10.111.111.2
 > Internet Control Message Protocol

A GRE tunnel has been created between HQ and BR routers. What is the tunnel IP on the HQ router?

- A. 10.111.111.2
- B. 209.165.202.134
- C. 209.165.202.130
- **D. 10.111.111.1** ✓

Explanation

In the above output, the IP address of “209.165.202.130” is the tunnel source IP while the IP 10.111.111.1 is the tunnel IP address.

An example of configuring GRE tunnel is shown below:

R1 (GRE config only) interface s0/0/0 ip address 63.1.27.2 255.255.255.0 interface tunnel0 ip address 10.0.0.1 255.255.255.0 tunnel mode gre ip //this command can be ignored tunnel source s0/0 tunnel destination 85.5.24.10	R2 (GRE config only) interface s0/0/0 ip address 85.5.24.10 255.255.255.0 interface tunnel1 ip address 10.0.0.2 255.255.255.0 tunnel source 85.5.24.10 tunnel destination 63.1.27.2

Question 5

A GRE tunnel is down with the error message %TUN-5-RECUR DOWN:

Tunnel0 temporarily disabled due to recursive routing error.

Which two options describe possible causes of the error? (Choose two)

- **A. The tunnel destination is being routed out of the tunnel interface** ✓
- **B. There is instability in the network due to route flapping** ✓
- C. The tunnel mode and tunnel IP address are misconfigured
- D. There is link flapping on the tunnel
- E. Incorrect destination IP addresses are configured on the tunnel

Explanation

The **%TUN-5-RECURDOWN: Tunnel0 temporarily disabled due to recursive routing error** message means that the generic routing encapsulation (GRE) tunnel router has discovered a recursive routing problem.

This condition is usually due to one of these causes:

- + A misconfiguration that causes the router to try to route to the tunnel destination address using the tunnel interface itself (recursive routing)
- + A temporary instability caused by route flapping elsewhere in the network

Reference: <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/22327-gre-flap.html>

Question 6

Which statement about dynamic GRE between a headend router and a remote router is true?

- A. GRE tunnels can be established when the remote router has a dynamic IP address
- B. A GRE tunnel without an IP address has a status of administratively down
- **C. The remote router initiates the tunnel connection** ✓
- D. The headend router learns the IP address of the remote end router statically

Question 7

Which IPv6 migration method relies on dynamic tunnels that use the 2002::/16 reserved address space?

- A. GRE
- **B. 6to4** ✓
- C. 6RD
- D. ISATAP

Explanation

6to4 tunnel is a technique which relies on reserved address space 2002::/16 (you must remember this range). These tunnels determine the appropriate destination address by combining the IPv6 prefix with the globally unique destination 6to4 border router's IPv4 address, beginning with the 2002::/16 prefix, in this format:

2002:border-router-IPv4-address::/48

For example, if the border-router-IPv4-address is 64.101.64.1, the tunnel interface will have an IPv6 prefix of 2002:4065:4001:1::/64, where 4065:4001 is the hexadecimal equivalent of 64.101.64.1. This technique allows

IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel setup but we have to implement it on all routers on the path.

Question 8

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

- A. TCP window size
- B. MTU ignore
- **C. TCP MSS** ✓
- D. DF bit Clear
- **E. PMTUD** ✓
- F. IP MTU

Explanation

The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 65535, most transmission links enforce a smaller maximum packet length limit, called an MTU. The value of the MTU depends on the type of the transmission link. The design of IP accommodates MTU differences since it allows routers to fragment IP datagrams as necessary. The receiving station is responsible for the reassembly of the fragments back into the original full size IP datagram.

Fragmentation and Path Maximum Transmission Unit Discovery (PMTUD) is a standardized technique to determine the maximum transmission unit (MTU) size on the network path between two hosts, usually with the goal of **avoiding IP fragmentation**. PMTUD was originally intended for routers in IPv4. However, all modern operating systems use it on endpoints.

The TCP Maximum Segment Size (TCP MSS) defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. This TCP/IP datagram might be fragmented at the IP layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. Contrary to popular belief, the MSS value is not negotiated between hosts. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.

TCP MSS takes care of fragmentation at the two endpoints of a TCP connection, but it does not handle the case where there is a smaller MTU link in the middle between these two endpoints. PMTUD was developed in order to avoid fragmentation in the path between the endpoints. It is used to dynamically determine the lowest MTU along the path from a packet's source to its destination.

Reference: <http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html> (there is some examples of how TCP MSS avoids IP Fragmentation in this link but it is too long so if you want to read please visit this link)

Note: IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later.

If the DF bit is set to clear, routers can fragment packets regardless of the original DF bit setting -> Answer 'DF bit Clear' is not correct.

Question 9

Refer to the exhibit. A network engineer configures a GRE tunnel and enters the show interface tunnel command. What does the output confirm about the configuration?

```
Tunnel100 is up, line protocol is up
Hardware is Tunnel
Internet address is 192.168.200.1/24
MTU 17912 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive set (10 sec), retries 3
Tunnel source 209.165.202.129 (GigabitEthernet0/1)
Tunnel Subblocks:
src-track:
Tunnel100 source tracking subblock associated with GigabitEthernet0/1
Set of tunnels with source GigabitEthernet0/1, 1 members (includes iterators),
on interface <OK>
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
```

- A. The physical interface MTU is 1476 bytes.
- B. The keepalive value is modified from the default value.
- **C. The tunnel mode is set to the default.** ✓
- D. Interface tracking is configured.

Explanation

From the “Tunnel protocol/transport GRE/IP” line, we can deduce this tunnel is using the default IPv4 Layer-3 tunnel mode. We can return to this default mode with the “tunnel mode gre ip” command.

Question 10

Which TCP setting is tuned to minimize the risk of fragmentation on a GRE/IP tunnel?

- A. MRU
- **B. MSS** ✓
- C. Window size
- D. MTU

Explanation

The TCP Maximum Segment Size (TCP MSS) defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. This TCP/IP datagram might be fragmented at the IP layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. Contrary to popular belief, the MSS value is not negotiated between hosts. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.

TCP MSS takes care of fragmentation at the two endpoints of a TCP connection, but it does not handle the case where there is a smaller MTU link in the middle between these two endpoints. PMTUD was developed in order to avoid fragmentation in the path between the endpoints. It is used to dynamically determine the lowest MTU along the path from a packet's source to its destination.

Reference: <http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html> (there is some examples of how TCP MSS avoids IP Fragmentation in this link but it is too long so if you want to read please visit this link)

Note: IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later.

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
[Privacy](#) - [Terms](#)

Submit Comment

[Subscribe to comments feed](#)

[HSRP & VRRP Questions 2](#) [Wireless 3 Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)

- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)

<https://t.me/learningnets>

- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH



[Home](#) > HSRP & VRRP 2 Quiz

HSRP & VRRP 2 Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of HSRP & VRRP 2 Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
4	70	90%	70	100.00%	00:00:21

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit.

R1
key chain cisco123
key 1
key-string Cisco123!

Ethernet0/0 - Group 10
State is Active
8 state changes, last state change 00:03:33
Virtual IP address is 192.168.0.1
Active virtual MAC address is 0000.0c07.ac0a
Local virtual MAC address is 0000.0c07.ac0a (v1 default)
Hello time 5 sec, hold time 15 sec
Next hello sent in 2.704 secs
Authentication MD5, key-chain "cisco123"
Preemption enabled
Active router is local
Standby router is unknown
Priority 255 (configured 255)
Group name is "workstation-group" (cfgd)

R2
key chain cisco123
key 1
key-string cisco123!

Ethernet0/0 - Group 10
State is Active
17 state changes, last state change 00:03:33
Virtual IP address is 192.168.0.1
Active virtual MAC address is 0000.0c07.ac0a
Local virtual MAC address is 0000.0c07.ac0a (v1 default)
Hello time 10 sec, hold time 30 sec
Next hello sent in 6.704 secs
Authentication MD5, key-chain "cisco123"
Preemption disabled
Active router is local
Standby router is unknown
Priority 200 (configured 200)
Group name is "workstation-group" (cfgd)

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

<https://www.it-ebooks.info>

resolve the configuration error?

- A. configure matching priority values
- B. configure unique virtual IP addresses
- **C. configure matching key-strings** ✓
- D. configure matching hold and delay timers

Explanation

From the output exhibit, we notice that the key-string of R1 is “Cisco123!” (letter “C” is in capital) while that of R2 is “cisco123!”. This causes a mismatch in the authentication so we have to fix their key-strings.

Note:

key-string [encryption-type] *text-string*: Configures the text string for the key. The text-string argument is alphanumeric, case-sensitive, and supports special characters.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_chapter_01111.pdf

Question 2

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

- **A. standby 300 priority 110** ✓
- B. standby 300 timers 1 110
- C. standby version 1
- D. standby 300 priority 90
- **E. standby version 2** ✓
- **F. standby 300 preempt** ✓

Question 3

Refer to the exhibit.

```
R1
interface GigabitEthernet0/0
 ip address 192.168.250.2 255.255.255.0
 standby 20 ip 192.168.250.1
 standby 20 priority 120
```

```
R2
interface GigabitEthernet0/0
 ip address 192.168.250.3 255.255.255.0
 standby 20 ip 192.168.250.1
 standby 20 priority 110
```

What are two effects of this configuration? (Choose two)

- A. If R2 goes down, R1 becomes active but reverts to standby when R2 comes back online

- **B. If R1 goes down, R2 becomes active and remains the active device when R1 comes back online** ✓
- C. R1 becomes the standby router
- D. If R1 goes down, R2 becomes active but reverts to standby when R1 comes back online
- **E. R1 becomes the active router** ✓

Question 4

Refer to the exhibit.

R1	R2
key chain cisco123	key chain cisco123
key 1	key 1
key-string Cisco123!	key-string Cisco123!
Ethernet0/0 - Group 10	Ethernet0/0 - Group 10
State is Active	State is Active
8 state changes, last state change 00:03:33	17 state changes, last state change 00:03:33
Virtual IP address is 192.168.0.1	Virtual IP address is 192.168.0.1
Active virtual MAC address is 0000.0c07.ac0a	Active virtual MAC address is 0000.0c07.ac0a

An engineer is installing a new pair of routers in a redundant configuration. Which protocol ensures that traffic is not disrupted in the event of a hardware failure?

- **A. HSRPv1** ✓
- B. GLBP
- C. VRRP
- D. HSRPv2

Explanation

The “virtual MAC address” is 0000.0c07.acXX (XX is the hexadecimal group number) so it is using HSRPv1.

Note: HSRP Version 2 uses a new MAC address which ranges from 0000.0C9F.F000 to 0000.0C9F.FFFF.

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real i

☐

I'm not a robot

reCAPTCHA
Privacy - Terms

[Subscribe to comments feed](#)[SPAN Quiz](#) [Access-list 2 Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)

- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

<https://t.me/learningnets>

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > HSRP & VRRP Quiz

HSRP & VRRP Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of HSRP & VRRP Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
12	160	90%	150	93.75%	00:01:29

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which statement about VRRP is true?

- A. It supports IPv4 and IPv6
- **B. It can be configured with HSRP on a switch or switch stack** ✓
- C. It supports load balancing
- D. It supports encrypted authentication

Question 2

Which First Hop Redundancy Protocol maximizes uplink utilization and minimizes the amount of configuration that is necessary?

- A. HSRP v1
- **B. GLBP** ✓
- C. VRRP
- D. HSRP v2

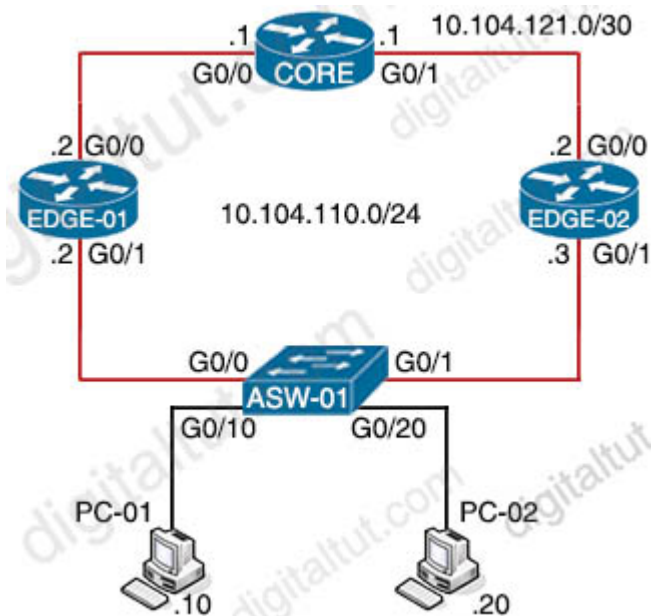
Explanation

The main disadvantage of HSRP and VRRP is that only one gateway is elected to be the active gateway and used to forward traffic whilst the rest are unused until the active one fails. Gateway Load Balancing Protocol (GLBP) is a Cisco proprietary protocol and performs the similar function to HSRP and VRRP but it supports load balancing among members in a GLBP group.

Note: Although GLBP is not a topic for this exam but not sure why we still have this question!

Question 3

Refer to the exhibit.



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

- A. G0/0 and G0/1 on ASW-01 ❌
- B. G0/0 and G0/1 on Core
- C. G0/0 on Edge-01 and G0/0 on Edge-02
- D. G0/1 on Edge-01 and G0/1 on Edge-02 ✔️

Question 4

What are three valid HSRP states? (Choose three)

- A. learning ✔️
- B. established
- C. full
- D. speak ✔️
- E. INIT
- F. listen ✔️

Explanation

HSRP consists of 6 states:

State	Description
Initial	This is the beginning state. It indicates HSRP is not running. It happens when the configuration changes or the interface is first turned on
Learn	The router has not determined the virtual IP address and has not yet seen an authenticated hello message from the active router. In this state, the router still waits to hear from the active router.
Listen	The router knows both IP and MAC address of the virtual router but it is not the active or standby router. For example, if there are 3 routers in HSRP group, the router which is not in active or standby state will remain in listen state.
Speak	The router sends periodic HSRP hellos and participates in the election of the active or standby router.
Standby	In this state, the router monitors hellos from the active router and it will take the active state when the current active router fails (no packets heard from active router)
Active	The router forwards packets that are sent to the HSRP group. The router also sends periodic hello messages

Please notice that not all routers in a HSRP group go through all states above. In a HSRP group, only one router reaches active state and one router reaches standby state. Other routers will stop at listen state.

Question 5

If a VRRP master router fails, which router is selected as the new master router?

- A. router with the highest loopback address
- **B. router with the highest priority** ✓
- C. router with the lowest priority
- D. router with the lowest loopback address

Question 6

An engineer must configure interface GigabitEthernet0/0 for VRRP group 10. When the router has the highest priority in the group, it must assume the master role. Which command set must be added to the initial configuration to accomplish this task?

Initial Configuration

```
interface GigabitEthernet0/0
description to IDF
ip address 172.16.13.2 255.255.255.0
```

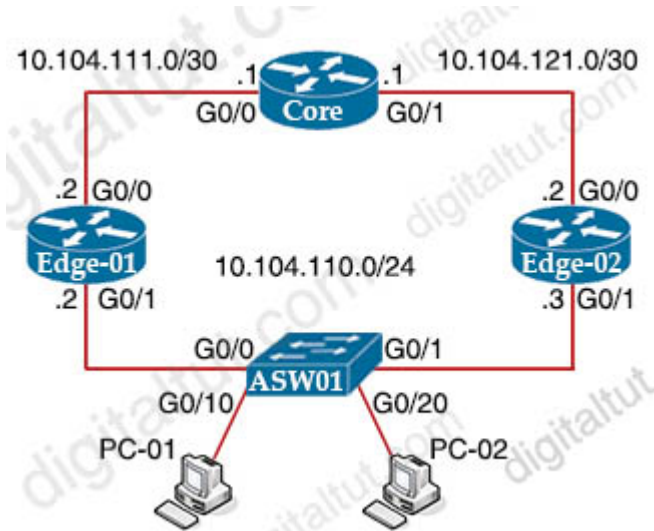
- A. vrrp group 10 ip 172.16.13.254 255.255.255.0
- vrrp group 10 priority 120
- B. tandby 10 ip 172.16.13.254 255.255.255.0
- standby 10 preempt
- **C. vrrp 10 ip 172.16.13.254** ✓
- **vrrp 10 preempt**
- D. standby 10 ip 172.16.13.254
- standby 10 priority 120

Explanation

In fact, VRRP has the preemption enabled by default so we don't need the "vrrp 10 preempt" command. The default priority is 100 so we don't need to configure it either. But notice that the correct command to configure the virtual IP address for the group is "vrrp 10 ip {ip-address}" (not "vrrp group 10 ip ...") and this command does not include a subnet mask.

Question 7

Refer to the exhibit. Edge-01 is currently operational as the HSRP primary with priority 110. Which command on Edge-02 causes it to take over the forwarding role when Edge-01 is down?



- A. standby 10 timers
- B. standby 10 priority
- C. standby 10 track
- **D. standby 10 preempt** ✓

Explanation

The "preempt" command enables the HSRP router with the highest priority to immediately become the active router.

Question 8

How does SSO work with HSRP to minimize network disruptions?

- A. It enables HSRP to elect another switch in the group as the active HSRP switch
- B. It ensures fast failover in the case of link failure
- C. It enables data forwarding along known routes following a switchover, while the routing protocol reconverges
- **D. It enables HSRP to failover to the standby RP on the same device** ✓

Explanation

SSO HSRP alters the behavior of HSRP when a device with redundant Route Processors (RPs) is configured for stateful switchover (SSO) redundancy mode. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails.

The SSO HSRP feature enables the Cisco IOS HSRP subsystem software to detect that a standby RP is installed and the system is configured in SSO redundancy mode. Further, if the active RP fails, no change occurs to the HSRP group itself and traffic continues to be forwarded through the current active gateway device.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-s/fhrp-15-s-book/fhrp-hsrp-ss0.html

Question 9

Which two statements about HSRP are true? (Choose two)

- **A. It supports tracking** ✓
- **B. Its virtual MAC is 0000.0C07.ACxx** ✓
- C. It supports unique virtual MAC addresses
- D. Its multicast virtual MAC is 0000.5E00.01xx
- E. Its default configuration allows for pre-emption

Explanation

When you change the HSRP version, Cisco NX-OS reinitializes the group because it now has a new virtual MAC address. HSRP version 1 uses the MAC address range 0000.0C07.ACxx while HSRP version 2 uses the MAC address range 0000.0C9F.F0xx.

HSRP supports interface tracking which allows to specify another interface on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group.

Question 10

Which two statements about VRRP are true? (Choose two)

- **A. Three versions of the VRRP protocol have been defined.** ✓
- B. Its IP address number is 115.
- C. It supports both MD5 and SHA1 authentication.
- D. It is assigned multicast address 224.0.0.8.
- E. It is assigned multicast address 224.0.0.9.
- **F. The TTL for VRRP packets must be 255.** ✓

Explanation

A VRRP router receiving a packet with the TTL not equal to 255 must discard the packet (only one possible hop) -> B is correct.

Currently there are three VRRP versions which are versions 1, 2 and 3 -> E is correct.

VRRP uses multicast address 224.0.0.18 and supports plaintext or MD5 authentication.

Question 11

Which behavior can be expected when the HSRP versions is changed from 1 to 2?

- A. Each HSRP group reinitializes because the multicast address has changed
- B. No changes occur because the standby router is upgraded before the active router
- C. No changes occur because version 1 and 2 use the same virtual MAC OUI
- **D. Each HSRP group reinitializes because the virtual MAC address has changed** ✓

Explanation

If you change the version for existing groups, Cisco NX-OS reinitializes HSRP for those groups because the virtual MAC address changes.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3548/sw/unicast/503_A1_1/13_nx-os/13_hsrp.html

Question 12

Which First Hop Redundancy Protocol should be used to meet a design requirements for more efficient default bandwidth usage across multiple devices?

- A. LCAP
- B. VRRP
- C. HSRP
- **D. GLBP** ✓

Explanation

The main disadvantage of HSRP and VRRP is that only one gateway is elected to be the active gateway and used to forward traffic whilst the rest are unused until the active one fails. Gateway Load Balancing Protocol (GLBP) is a Cisco proprietary protocol and performs the similar function to HSRP and VRRP but it supports load balancing among members in a GLBP group.

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms[Subscribe to comments feed](#)[Network Assurance Quiz](#) [Wireless Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)

- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > IP SLA Quiz

IP SLA Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of IP SLA Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
4	60	90%	60	100.00%	00:00:22

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which two statements about IP SLA are true? (Choose two)

- **A. It is Layer 2 transport-independent** ✓
- B. SNMP access is not supported
- **C. It uses active traffic monitoring** ✓
- D. It can measure MOS
- E. It uses NetFlow for passive traffic monitoring
- F. The IP SLA responder is a component in the source Cisco device

Explanation

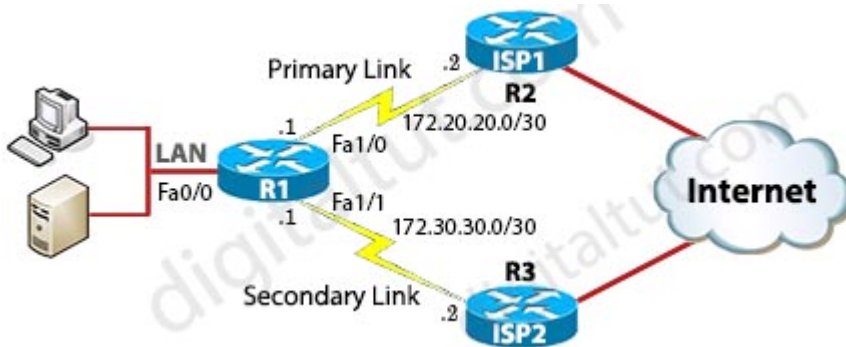
IP SLAs allows Cisco customers to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages. **IP SLAs uses active traffic monitoring**—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance.

Being **Layer-2 transport independent**, IP SLAs can be configured end-to-end over disparate networks to best reflect the metrics that an end-user is likely to experience.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_overview.html

Question 2

Refer to exhibit. What are two reasons for IP SLA tracking failure? (Choose two)



```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 172.20.20.2 source-interface FastEthernet0/0
R1(config-ip-sla-echo)#timeout 5000
R1(config-ip-sla-echo)#frequency 10
R1(config-ip-sla-echo)#threshold 500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track 10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10
R1(config)#no ip route 0.0.0.0 0.0.0.0 172.20.20.2
R1(config)#ip route 0.0.0.0 0.0.0.0 172.30.30.2 5
```

- **A. A route back to the R1 LAN network is missing in R2** ✓
- B. The source-interface is configured incorrectly
- **C. The threshold value is wrong** ✓
- D. The destination must be 172.30.30.2 for icmp-echo
- E. The default route has wrong next hop IP address

Explanation

There is no problem with the Fa0/0 as the source interface as we want to check the ping from the LAN interface -> A is not correct.

Answer 'The destination must be 172.30.30.2 for icmp-echo' is not correct as we must track the destination of the primary link, not backup link.

In this question, R1 pings R2 via its LAN Fa0/0 interface so maybe R1 (which is an ISP) will not know how to reply back as an ISP usually does not configure a route to a customer's LAN -> C is correct.

There is no problem with the default route -> D is not correct.

For answer 'The threshold value is wrong', we need to understand about how timeout and threshold are defined:

Timeout (in milliseconds) sets the amount of time an IP SLAs operation waits for a response from its request packet. In other words, the timeout specifies how long the router should wait for a response to its ping before it is considered failed. **Threshold** (in milliseconds too) sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation. Threshold is used to activate a response to IP SLA violation, e.g. send SNMP trap or start secondary SLA operation. In other words, the threshold value is only

used to indicate over threshold events, which do not affect reachability but may be used to evaluate the proper settings for the timeout command.

For reachability tracking, if the return code is OK or OverThreshold, reachability is up; if not OK, reachability is down.

Therefore in this question, we are using “Reachability” tracking (via the command “track 10 ip sla 1 reachability”) so threshold value is not important and can be ignored -> Answer 'The threshold value is wrong' is correct. In fact, answer 'The threshold value is wrong' is not wrong but it is the best option left.

This tutorial can help you revise IP SLA tracking topic: <http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/813-cisco-router-ipsla-basic.html> and <http://www.ciscozine.com/using-ip-sla-to-change-routing/>

Note: Maybe some of us will wonder why there are these two commands:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10
R1(config)#no ip route 0.0.0.0 0.0.0.0 172.20.20.2
```

In fact the two commands:

```
ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10
ip route 0.0.0.0 0.0.0.0 172.20.20.2
```

are different. These two static routes can co-exist in the routing table. Therefore if the tracking goes down, the first command will be removed but the second one still exists and the backup path is not preferred. So we have to remove the second one.

Question 3

Refer to the exhibit.

```
ip sla 10
 icmp-echo 192.168.10.20
 timeout 500
 frequency 3
 ip sla schedule 10 life forever start-time now
 track 10 ip sla 10 reachability
```

The IP SLA is configured in a router. An engineer must configure an EEM applet to shut down the interface and bring it back up when there is a problem with the IP SLA. Which configuration should the engineer use?

- A. event manager applet EEM_IP_SLA
 - event track 10 state unreachable
- **B. event manager applet EEM_IP_SLA**
 - event track 10 state down** 
- C. event manager applet EEM_IP_SLA
 - event sla 10 state unreachable
- D. event manager applet EEM_IP_SLA
 - event sla 10 state down

Explanation

The “ip sla 10” will ping the IP 192.168.10.20 every 3 seconds to make sure the connection is still up. We can configure an EEM applet if there is any problem with this IP SLA via the command “event track 10 state down”.

Reference: <https://www.theroutingtable.com/ip-sla-and-cisco-eem/>

Question 4

Which IP SLA operation requires the IP SLA responder to be configured on the remote end?

- **A. UDP jitter** ✓
- B. ICMP echo
- C. TCP connect
- D. CMP jitter

Explanation

Cisco IOS IP SLA Responder is a Cisco IOS Software component whose functionality is to respond to Cisco IOS IP SLA request packets. The IP SLA source sends control packets before the operation starts to establish a connection to the responder. Once the control packet is acknowledged, test packets are sent to the responder. **The responder inserts a time-stamp when it receives a packet** and factors out the destination processing time **and adds time-stamps to the sent packets**. This feature allows the calculation of unidirectional packet loss, latency, and jitter measurements with the kind of accuracy that is not possible with ping or other dedicated probe testing.

Reference:

https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806bfb52.html

The IP SLAs responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLAs request packets. The responder provides accurate measurements without the need for dedicated probes.

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/46sg/configuration/guide/Wrapper-46SG/swipsla.html>

UDP Jitter measures the delay, delay variation(jitter), corruption, misordering and packet loss by generating periodic UDP traffic. This operation always requires IP SLA responder.

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/BRKNMS-3043.pdf>

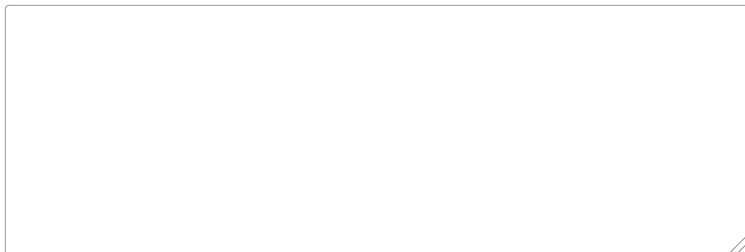
Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[NetFlow Quiz](#) [NTP Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)

- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)

- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > LISP & VXLAN Quiz

LISP & VXLAN Quiz

May 30th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of LISP & VXLAN Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
11	140	90%	120	85.71%	00:03:11

Sorry!

You failed :(but surely you will do it better next time!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which statement about VXLAN is true?

- A. VXLAN extends the Layer 2 Segment ID field to 24-bits, which allows up to 4094 unique Layer 2 segments over the same network
- B. VXLAN encapsulates a Layer 2 frame in an IP-UDP header, which allows Layer 2 adjacency across router boundaries**
- C. VXLAN uses the Spanning Tree Protocol for loop prevention
- D. VXLAN uses TCP 35 the transport protocol over the physical data center network



Explanation

802.1Q VLAN identifier space is only 12 bits. The VXLAN identifier space is 24 bits. This doubling in size allows the VXLAN ID space to support 16 million Layer 2 segments -> Answer 'VXLAN extends the Layer 2 Segment ID field to 24-bits, which allows up to 4094 unique Layer 2 segments over the same network' is not correct.

VXLAN is a MAC-in-UDP encapsulation method that is used in order to extend a Layer 2 or Layer 3 overlay network over a Layer 3 infrastructure that already exists.

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/vlan/212682-virtual-extensible-lan-and-ethernet-virt.html>

Question 2

Which LISP infrastructure device provides connectivity between non-LISP sites and LISP sites by receiving non-LISP traffic with a LISP site destination?

- A. map server
- **B. PITR** ✓
- C. map resolver
- D. PETR

Explanation

Proxy ingress tunnel router (PITR): A PITR is an infrastructure LISP network entity that receives packets from non-LISP sites and encapsulates the packets to LISP sites or natively forwards them to non-LISP sites.

Reference: <https://www.ciscopress.com/articles/article.asp?p=2992605>

Note: The proxy egress tunnel router (PETR) allows the communication from the LISP sites to the non-LISP sites. The PETR receives LISP encapsulated traffic from ITR.

Question 3

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

- **A. ETR** ✓
- B. MS
- C. ITR
- D. MR

Explanation

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

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

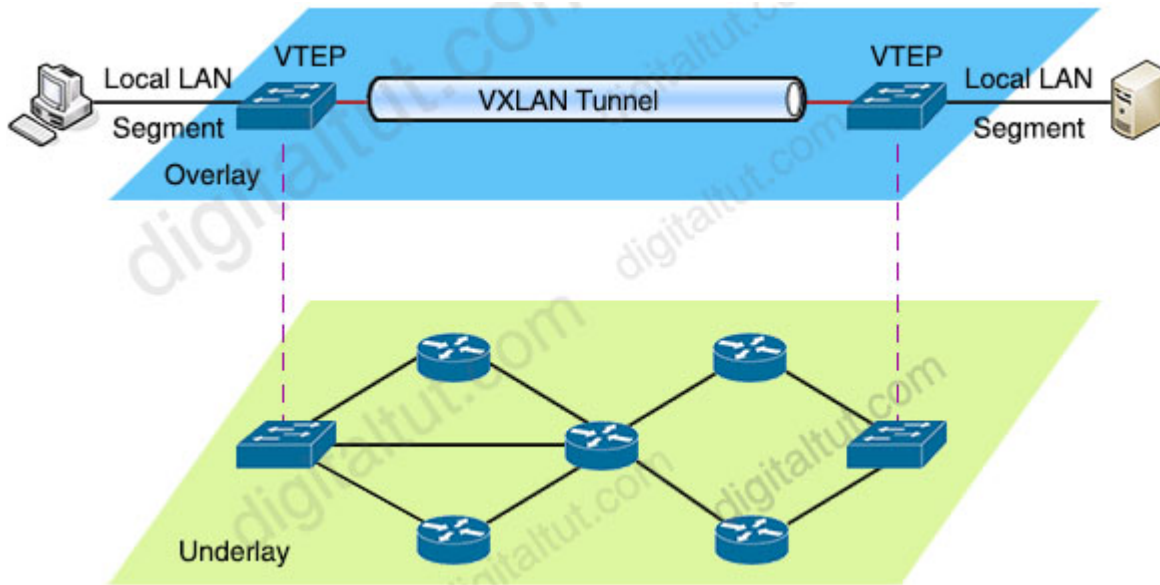
Question 4

Which action is a function of VTEP in VXLAN?

- A. allowing encrypted communication on the local VXLAN Ethernet segment
- B. tunneling traffic from IPv6 to IPv4 VXLANs
- **C. encapsulating and de-encapsulating VXLAN Ethernet frames** ✓
- D. tunneling traffic from IPv4 to IPv6 VXLANs

Explanation

VTEPs connect between Overlay and Underlay network and they are responsible for encapsulating frame into VXLAN packets to send across IP network (Underlay) then decapsulating when the packets leaves the VXLAN tunnel.



Question 5

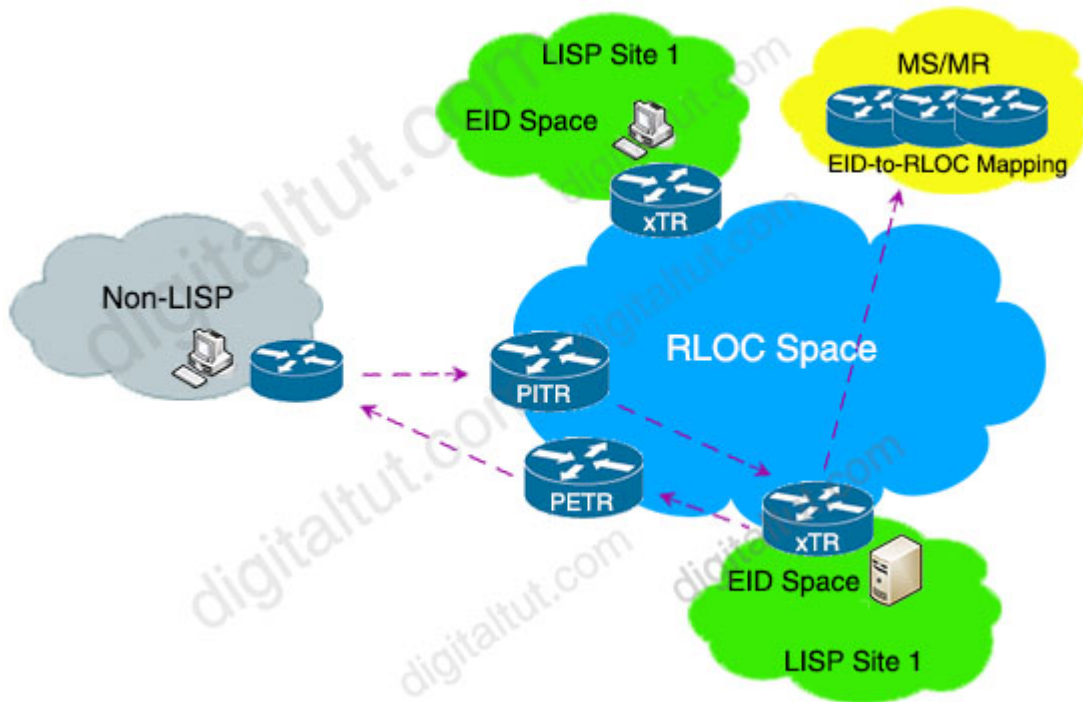
Which two LISP infrastructure elements are needed to support LISP to non-LISP internetworking? (Choose two)

- A. MR ✓
- B. ALT
- C. PITR
- D. PETR ✓
- E. MS ✗

Explanation

In this question we suppose that we only need to send packets from LISP site to non-LISP site successfully. We don't care about the way back (if we care about the way back then all PETR, PITR, MS & MR are needed).

Proxy Egress Tunnel Router (PETR): A LISP device that de-encapsulates packets from LISP sites to deliver them to non-LISP sites.



When the xTR in LISP Site 1 want to sends traffic to Non-LISP site, the ITR (not PETR) needs a Map Resolver (MR) to send Map Request to. When the ITR (the xTR in LISP Site 1 in the figure above) receives negative MAP-Reply packet from MR, it caches that prefix and map it to the PETR.

Good reference: <https://netmindblog.com/2019/12/04/lisp-locator-id-separation-protocol-part-ii-pxtr/>

Question 6

What is the purpose of the LISP routing and addressing architecture?

- A. It allows multiple instances of a routing table to co-exist within the same router.
- **B. It creates two entries for each network node, one for its identity and another for its location on the network.** ✓
- C. It creates head-end replication used to deliver broadcast and multicast frames to the entire network.
- D. It allows LISP to be applied as a network visualization overlay though encapsulation.

Explanation

Locator ID Separation Protocol (LISP) solves this issue by separating the location and identity of a device through the Routing locator (RLOC) and Endpoint identifier (EID):

- + **Endpoint identifiers** (EIDs) – assigned to end hosts.
- + **Routing locators** (RLOCs) – assigned to devices (primarily routers) that make up the global routing system.

Question 7

What function does VXLAN perform in an SD-Access deployment?

- A. control plane forwarding
- B. policy plane forwarding

- **C. data plane forwarding** ✓
- D. systems management and orchestration

Question 8

Refer to the exhibit. Which LISP component do routers in the public IP network use to forward traffic between the two networks?



- A. map server
- B. map resolver
- C. EID
- **D. RLOC** ✓

Explanation

Locator ID Separation Protocol (LISP) is a network architecture and protocol that implements the use of two namespaces instead of a single IP address:

- + Endpoint identifiers (EIDs) – assigned to end hosts.
- + Routing locators (RLOCs) – assigned to devices (primarily routers) that make up the global routing system.

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

Question 9

Which two namespaces does the LISP network architecture and protocol use? (Choose two)

- **A. RLOC** ✓
- B. DNS
- **C. EID** ✓
- D. VTEP
- E. TLOC

Explanation

Locator ID Separation Protocol (LISP) is a network architecture and protocol that implements the use of two namespaces instead of a single IP address:

- + Endpoint identifiers (EIDs)—assigned to end hosts.
- + Routing locators (RLOCs)—assigned to devices (primarily routers) that make up the global routing system.

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

Question 10

Into which two pieces of information does the LISP protocol split the device identity? (Choose two)

- A. Resource Location
- B. LISP ID
- **C. Routing Locator** ✓
- D. Device ID
- E. Enterprise Identifier
- **F. Endpoint Identifier** ✓

Explanation

Locator ID Separation Protocol (LISP) is a network architecture and protocol that implements the use of two namespaces instead of a single IP address:

+ Endpoint identifiers (EIDs)—assigned to end hosts.

+ Routing locators (RLOCs)—assigned to devices (primarily routers) that make up the global routing system.

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

Question 11

Which entity is responsible for maintaining Layer 2 isolation between segments in a VXLAN environment?

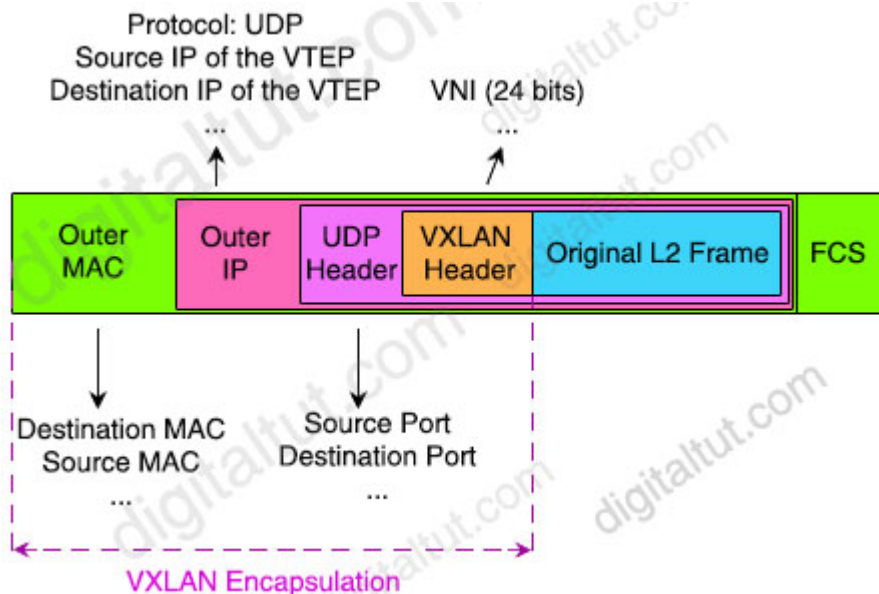
- A. host switch
- **B. VNID** ✓
- C. VTEP
- D. switch fabric

Explanation

VXLAN uses an 8-byte VXLAN header that consists of a 24-bit VNID and a few reserved bits. The VXLAN header together with the original Ethernet frame goes in the UDP payload. The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x_chapter_010.html

Let's see the structure of a VXLAN packet to understand how (note: VNI = VNID)



The key fields for the VXLAN packet in each of the protocol headers are:

- + **Outer MAC header** (14 bytes with 4 bytes optional) – Contains the MAC address of the source VTEP and the MAC address of the next-hop router. Each router along the packet's path rewrites this header so that the source address is the router's MAC address and the destination address is the next-hop router's MAC address.
- + **Outer IP header** (20 bytes)- Contains the IP addresses of the source and destination VTEPs.
- + **(Outer) UDP header** (8 bytes)- Contains source and destination UDP ports:
 - Source UDP port: The VXLAN protocol repurposes this standard field in a UDP packet header. Instead of using this field for the source UDP port, the protocol uses it as a numeric identifier for the particular flow between VTEPs. The VXLAN standard does not define how this number is derived, but the source VTEP usually calculates it from a hash of some combination of fields from the inner Layer 2 packet and the Layer 3 or Layer 4 headers of the original frame.
 - Destination UDP port: The VXLAN UDP port. The Internet Assigned Numbers Authority (IANA) allocates port 4789 to VXLAN.
- + **VXLAN header** (8 bytes)- Contains the 24-bit VNI (or VNID)
- + **Original Ethernet/L2 Frame** – Contains the original Layer 2 Ethernet frame.

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms[Submit Comment](#)[Subscribe to comments feed](#)[VXLAN Tutorial](#) [Composite Quiz 102 Questions](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)

- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH



[Home](#) > Miscellaneous Quiz

Miscellaneous Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Miscellaneous Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
5	70	90%	70	100.00%	00:00:26

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which action is performed by Link Management Protocol in a Cisco stackwise virtual domain?

- A. It determines if the hardware is compatible to form the stackwise virtual domain
- B. It discovers the stackwise domain and brings up SVL interfaces
- C. It determines which switch becomes active or standby
- **D. It rejects any unidirectional link traffic forwarding** ✓

Explanation

The Link Management Protocol (LMP) performs the following functions:

- + Verifies link integrity by establishing bidirectional traffic forwarding, and rejects any unidirectional links
- + Exchanges periodic hellos to monitor and maintain the health of the links
- + Negotiates the version of StackWise Virtual header between the switches StackWise Virtual link role resolution

Reference: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html>

Question 2

An engineer reviews a router's logs and discovers the following entry. What is the event's logging severity level?

Router# *Feb 03 11:13:44 334: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up

- A. warning
- B. notification
- **C. error** ✓
- D. informational

Explanation

Syslog levels are listed below:

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist

6	informational	Informational messages
7	debugging	Debugging messages

Number “3” in “%LINK-3-UPDOWN” is the severity level of this message so in this case it is “errors”.

Question 3

What does Call Admission Control require the client to send in order to reserve the bandwidth?

- A. Wi-Fi multimedia
- B. VoIP media session awareness
- C. SIP flow information
- **D. traffic specification** ✓

Explanation

The application residing on Device 1 originates an RSVP message called Path, which is sent to the same destination IP address as the data flow for which a reservation is requested (that is, 10.60.60.60) and is sent with the “router alert” option turned on in the IP header. **The Path message contains**, among other things, the following objects:

...

–The “sender T-Spec” (**traffic specification**) object, which characterizes the data flow for which a reservation will be requested. The T-Spec basically defines the maximum IP bandwidth required for a call flow using a specific codec. The T-Spec is typically defined using values for the data flow’s average bit rate, peak rate, and burst size.

Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/9x/uc9x/cac.html

Question 4

A network administrator is implementing a routing configuration change and enables routing debugs to track routing behavior during the change. The logging output on the terminal is interrupting the command typing process. Which two actions can the network administrator take to minimize the possibility of typing commands incorrectly? (Choose two)

- **A. Press the TAB key to reprint the command in a new line** ✓
- **B. Configure the logging synchronous command under the vty** ✓
- C. Configure the logging delimiter feature
- D. Configure the logging synchronous global configuration command
- E. Increase the number of lines on the screen using the terminal length command

Explanation

Although some Cisco webpages (like [this one](#)) mentioned about “logging synchronous” command in global configuration mode, which means “Router(config)#logging synchronous”, but in fact we cannot use it under global configuration mode. We can only use this command in line mode. Therefore answer 'Configure the logging synchronous command under the vty' is better than answer 'Configure the logging synchronous global configuration command'.

Let’s see how the “logging synchronous” command affect the typing command:

Without this command, a message may pop up and you may not know what you typed if that message is too long. When trying to erase (backspace) your command, you realize you are erasing the message instead.

```
NVbos2811-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
NVbos2811-1(config)#^Z
NVbos2811-1#sh
Jan 18 16:38:02: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (10.0.1.11)
```

With this command enabled, when a message pops up you will be put to a new line with your typing command which is very nice:

```
NVbos2811-1(config)#line con 0
NVbos2811-1(config-line)#logging synch
NVbos2811-1(config-line)#line vty 0 4
NVbos2811-1(config-line)#logging synchr
NVbos2811-1(config-line)#logging synchronous
NVbos2811-1(config-line)#^Z
NVbos2811-1#sh ip
Jan 18 16:39:33: %SYS-5-CONFIG_I: Configured from console by admin
NVbos2811-1#sh ip
```

Question 5**What are two considerations when using SSO as a network redundancy feature? (Choose two)**

- A. both supervisors must be configured separately
- **B. must be combined with NSF to support uninterrupted Layer 3 operations** ✓
- C. the multicast state is preserved during switchover
- **D. requires synchronization between supervisors in order to guarantee continuous connectivity** ✓
- E. must be combined with NSF to support uninterrupted Layer 2 operations

Explanation

Cisco IOS Nonstop Forwarding(NSF) always runs with stateful switchover (SSO) and provides redundancy for Layer 3 traffic.

Reference:

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_01101110.pdf

Comments

1. NET-Student
October 26th, 2020

I just wondering the Number 10,
if the cause of recursive routing error is A misconfiguration then why the answer is There is instability in the network due to route flapping

2. Grizzly
November 10th, 2020

Question 3 (NAT) Question:

C and E appears to be correct but the explanation includes answer D, (one to one Nat) is also achieved and states its a valid answer. to me this seems questionable ?

I believe one-to-one NAT mappings do not require an ACL within the NAT statement. Does anybody agree with this ? Please double check me.
Thanks :)

3. Hi
January 24th, 2021

I agree with NET-Student, that question should be reviewed.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real i



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[Drag Drop Quiz Automation Quiz 2](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)

- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Multicast Quiz

Multicast Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Multicast Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
5	50	90%	50	100.00%	01:03:42

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which router is elected the IGMP Querier when more than one router is in the same LAN segment?

- A. The router with the longest uptime
- B. The router with the highest IP address
- **C. The router with the lowest IP address** ✓
- D. The router with the shortest uptime

Explanation

Query messages are used to elect the IGMP querier as follows:

1. When IGMPv2 devices start, they each multicast a general query message to the all-systems group address of 224.0.0.1 with their interface address in the source IP address field of the message.
2. When an IGMPv2 device receives a general query message, the device compares the source IP address in the message with its own interface address. **The device with the lowest IP address on the subnet is elected the IGMP querier.**
3. All devices (excluding the querier) start the query timer, which is reset whenever a general query message is received from the IGMP querier. If the query timer expires, it is assumed that the IGMP querier has gone down, and the election process is performed again to elect a new IGMP querier.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_2_e/multicast/configuration_guide/b_mc_1522e_3750x_3560x_cg/b_ipmc_3750x_3560x_chapter_01000.html

Question 2

What mechanism does PIM use to forward multicast traffic?

- A. PIM dense mode uses a pull model to deliver multicast traffic
- B. PIM sparse mode uses a flood and prune model to deliver multicast traffic
- **C. PIM sparse mode uses a pull model to deliver multicast traffic** ✓
- D. PIM sparse mode uses receivers to register with the RP

Explanation

PIM dense mode (PIM-DM) uses a push model to flood multicast traffic to every corner of the network. This push model is a brute-force method of delivering data to the receivers. This method would be efficient in certain deployments in which there are active receivers on every subnet in the network. PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune the unwanted traffic. This process repeats every 3 minutes.

PIM Sparse Mode (PIM-SM) uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data receive the traffic. PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees (at least initially), it requires the use of an RP. The RP must be administratively configured in the network.

Answer 'PIM sparse mode uses receivers to register with the RP' seems to be correct but it is not, PIM sparse mode uses sources (not receivers) to register with the RP. Sources register with the RP, and then data is forwarded down the shared tree to the receivers.

Reference: Selecting MPLS VPN Services Book, page 193

Question 3

What is the role of the RP in PIM sparse mode?

- **A. The RP is the multicast that is the root of the PIM-SM shared multicast distribution tree** ✓
- B. The RP maintains default aging timeouts for all multicast streams requested by the receivers
- C. The RP acts as a control-plane node and does not receive or forward multicast packets
- D. The RP responds to the PIM join messages with the source of requested multicast group

Explanation

The concept of joining the rendezvous point (RP) is called the RPT (Root Path Tree) or shared distribution tree. The RP is the root of our tree which decides where to forward multicast traffic to. Each multicast group might have different sources and receivers so we might have different RPTs in our network.

Question 4

What is the purpose of an RP in PIM?

- A. secure the communication channel between the multicast sender and receiver.
- **B. receive IGMP joins from multicast receivers.** ✓
- C. ensure the shortest path from the multicast source to the receiver.

- D. send join messages toward a multicast source SPT

Question 5

Which statement about multicast RPs is true?

- A. RPs are required for protocol independent multicast sparse mode and dense mode
- **B. By default, the RP is needed only to start new sessions with sources and receivers** ✓
- C. RPs are required only when using protocol independent multicast dense mode
- D. By default, the RP is needed periodically to maintain sessions with sources and receivers

Explanation

A rendezvous point (RP) is required only in networks running Protocol Independent Multicast sparse mode (PIM-SM).

By default, the RP is needed only to start new sessions with sources and receivers.

Reference: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

For your information, in PIM-SM, only network segments with active receivers that have explicitly requested multicast data will be forwarded the traffic. This method of delivering multicast data is in contrast to the PIM dense mode (PIM-DM) model. In PIM-DM, multicast traffic is initially flooded to all segments of the network. Routers that have no downstream neighbors or directly connected receivers prune back the unwanted traffic.

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[CoPP Quiz](#) [EIGRP & OSPF 2 Quiz](#)

Premium Member Zone

Welcome [Ashwin Tharan!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)

- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH



[Home](#) > NAT Quiz

NAT Quiz

 January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of NAT Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
5	60	90%	60	100.00%	00:00:51

Congratulations!

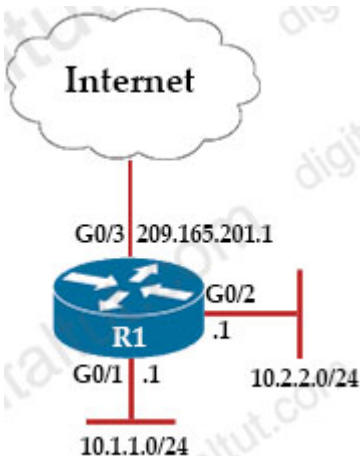
You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit.



An engineer must allow all users in the 10.2.2.0/24 subnet to access the Internet. To conserve address space, the public interface address of 209.165.201.1 must be used for all external communication. Which command set accomplishes these requirements?

Option A

access-list 10 permit 10.2.2.0 0.0.0.255

Option B

<pre>interface G0/3 ip nat outside interface G0/2 ip nat inside ip nat inside source list 10 interface G0/2 overload</pre>	<pre>access-list 10 permit 10.2.2.0 0.0.0.255 interface G0/3 ip nat outside interface G0/2 ip nat inside ip nat inside source list 10 209.165.201.1</pre>
Option C <pre>access-list 10 permit 10.2.2.0 0.0.0.255 interface G0/3 ip nat outside interface G0/2 ip nat inside ip nat inside source list 10 interface G0/3</pre>	Option D <pre>access-list 10 permit 10.2.2.0 0.0.0.255 interface G0/3 ip nat outside interface G0/2 ip nat inside ip nat inside source list 10 interface G0/3 overload</pre>

- A. Option B
- **B. Option D** ✓
- C. Option A
- D. Option C

Explanation

The command “ip nat inside source list 10 interface G0/3 overload” configures NAT to overload (PAT) on the address that is assigned to the G0/3 interface.

Question 2

Refer to the exhibit.

```
access-list 1 permit 172.16.1.0 0.0.0.255
ip nat inside source list 1 interface gigabitethernet0/0 overload
```

The inside and outside interfaces in the NAT configuration of this device have been correctly identified. What is the effect of this configuration?

- A. dynamic NAT
- B. NAT64
-
- **C. PAT** ✓
- D. static NAT

Explanation

The command “ip nat inside source list 1 interface gigabitethernet0/0 overload” translates all source addresses that pass access list 1, which means 172.16.1.0/24 subnet, into an address assigned to gigabitethernet0/0 interface. **Overload** keyword allows to map multiple IP addresses to a single registered IP address (many-to-one) by using different ports so it is called Port Address Translation (PAT).

Question 3

Refer to the exhibit. What are two effect of this configuration? (Choose two)

```
access-list 1 permit 10.1.1.0 0.0.0.31
ip nat pool CISCO 209.165.201.1 209.165.201.30 netmask 255.255.255.224
ip nat inside source list 1 pool CISCO
```

- A. The 10.1.1.0/27 subnet is assigned as the inside global address range
- **B. Inside source addresses are translated to the 209.165.201.0/27 subnet** ✓
- C. It establishes a one-to-one NAT translation
- **D. The 10.1.1.0/27 subnet is assigned as the inside local addresses** ✓
- E. The 209.165.201.0/27 subnet is assigned as the outside local address range

Explanation

In this question, the inside local addresses of the 10.1.1.0/27 subnet are translated into 209.165.201.0/27 subnet. This is one-to-one NAT translation as the keyword “overload” is missing so in fact answer 'It establishes a one-to-one NAT translation' is also correct.

Question 4

Refer to the exhibit.



```
R1(config)# ip nat inside source static 10.70.5.1 10.45.1.7
```

A network architect has partially configured static NAT. which commands should be asked to complete the configuration?

- A. 1(config)#interface GigabitEthernet0/0
R1(config)#ip pat inside
- R1(config)#interface GigabitEthernet0/1
- R1(config)#ip pat outside

- **B. R1(config)#interface GigabitEthernet0/0
R1(config)#ip nat outside**

**R1(config)#interface GigabitEthernet0/1
R1(config)#ip nat inside** ✓

C. R1(config)#interface GigabitEthernet0/0
R1(config)#ip nat inside

- R1(config)#interface GigabitEthernet0/1
- R1(config)#ip nat outside

D. R1(config)#interface GigabitEthernet0/0
R1(config)#ip nat outside

- R1(config)#interface GigabitEthernet0/1
- R1(config)#ip nat inside

Question 5

Refer to the exhibit.

```
interface FastEthernet0/1
ip address 209.165.200.225 255.255.255.224
ip nat outside
!
interface FastEthernet0/2
ip address 10.10.10.1 255.255.255.0
ip nat inside
!
access-list 10 permit 10.10.10.0 0.0.0.255
!
```

Which command allows hosts that are connected to FastEthernet0/2 to access the Internet?

- **A. ip nat inside source list 10 interface FastEthernet0/1 overload** ✓
- B. ip nat inside source list 10 interface FastEthernet0/2 overload
- C. ip nat outside source static 209.165.200.225 10.10.10.0 overload
- D. ip nat outside source list 10 interface FastEthernet0/2 overload

Explanation

The command “ip nat inside source list 10 interface FastEthernet0/1 overload” configures NAT to overload on the address that is assigned to the Fa0/1 interface.

Comments

1. No comments yet.
1. No trackbacks yet.

Add a Comment



I'm not a robot

reCAPTCHA
[Privacy](#) - [Terms](#)

[Subscribe to comments feed](#)

[STP Quiz](#) [HSRP & VRRP Questions 2](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)

- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)

- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > NetFlow Quiz

NetFlow Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of NetFlow Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
4	50	90%	50	100.00%	00:00:23

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit. How can you configure a second export destination for IP address 192.168.10.1?

```
configure terminal
ip flow-export destination 192.168.10.1 9991
ip flow-export version 9
```

- A. Specify a different flow ID
- B. Specify a different TCP port
- C. Specify a VRF
- D. Configure a version 5 flow-export to the same destination
- **E. Specify a different UDP port** ✓

Explanation

To configure multiple NetFlow export destinations to a router, use the following commands in global configuration mode:

Step 1: Router(config)# **ip flow-export destination** *ip-address udp-port*

Step 2: Router(config)# **ip flow-export destination** *ip-address udp-port*

The following example enables the exporting of information in NetFlow cache entries:

```
ip flow-export destination 10.42.42.1 9991
```

```
ip flow-export destination 10.0.101.254 1999
```

Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/12s_mdnf.html

Question 2

Refer to the exhibit.

<https://t.me/learningnets>

```

flow record v4_r1
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!
flow monitor FLOW-MONITOR-1
 record v_r1
 exit
!
sampler SAMPLER-1
 mode random 1 out-of 2
 exit
!
ip cef
!
interface GigabitEthernet0/0/0
 ip address 172.16.6.2 255.255.255.0

```

Option A sampler SAMPLER-1 mode random 1-out-of 2 flow FLOW-MONITOR-1 interface GigabitEthernet0/0/0 ip flow monitor SAMPLER-1 input	Option B sampler SAMPLER-1 no mode random 1-out-of 2 mode percent 50 interface GigabitEthernet0/0/0 ip flow monitor FLOW_MONITOR-1 sampler SAMPLER-1 input
Option C interface GigabitEthernet0/0/0 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input	Option D flow monitor FLOW-MONITOR-1 record v4_r1 sampler SAMPLER-1 interface GigabitEthernet0/0/0 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input

Which command set must be added to the configuration to analyze 50 packets out of every 100?

- **A. Option D** ✓
- B. Option A
- C. Option C
- D. Option B

Question 3

A network is being migrated from IPv4 to IPv6 using a dual-stack approach. Network management is already 100% IPv6 enabled. In a dual-stack network with two dual-stack NetFlow collections, how many flow exporters are needed per network device in the flexible NetFlow configuration?

- **A. 2** ✓
- B. 4
- C. 8
- D. 1

Comments

Question 4

A network engineer is configuring Flexible NetFlow and enters these commands:

```
Sampler Netflow1
mode random one-out-of 100
interface fastethernet 1/0
flow-sampler netflow1
```

Which are two results of implementing this feature instead of traditional NetFlow? (Choose two)

- **A. CPU and memory utilization are reduced** ✓
- B. The data export flow is more secure
- C. Only the flows of top 100 talkers are exported
- D. The accuracy of the data to be analyzed is improved
- **E. The number of packets to be analyzed are reduced** ✓

Explanation

The “mode random one-out of 100” specifies that sampling uses the random mode and only take one sample out of every 100 packets.

1. userA
February 2nd, 2021

Shouldnt question 4 be B, which is option C? sampler doesnt need to be configured under the flow monitor.

2. Nick
February 7th, 2021

@userA I think so.

3. Anonymous
February 13th, 2021

Option D gives the correct record name. If the record name is not corrected, it will not work.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[SD-WAN & SD-Access Solutions 3 Quiz](#) [IP SLA Quiz](#)

Premium Member Zone

Welcome [Ashwin Tharan!](#)

<https://t.me/learningnets>

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)

- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Network Assurance Quiz

Network Assurance Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Network Assurance Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
3	30	90%	30	100.00%	00:01:20

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

When using TLS for syslog, which configuration allows for secure and reliable transportation of messages to its default port?

- **A. logging host 10.2.3.4 vrf mgmt transport tcp port 6514** ✓
- B. logging host 10.2.3.4 vrf mgmt transport tcp port 514
- C. logging host 10.2.3.4 vrf mgmt transport udp port 6514
- D. logging host 10.2.3.4 vrf mgmt transport udp port 514

Explanation

The TCP port 6514 has been allocated as the default port for syslog over Transport Layer Security (TLS).

Reference: <https://tools.ietf.org/html/rfc5425>

Question 2

Which component of the Cisco Cyber Threat Defense solution provides user and flow context analysis?

- A. Cisco Firepower and FireSIGHT
- **B. Cisco Stealthwatch system** ✓
- C. Cisco Web Security Appliance

- D. Advanced Malware Protection

Explanation

The goal of the Cyber Threat Defense solution is to introduce a design and architecture that can help facilitate the discovery, containment, and remediation of threats once they have penetrated into the network interior.

Cisco Cyber Threat Defense version 2.0 makes use of several solutions to accomplish its objectives:

- * NetFlow and the Lancope StealthWatch System
 - Broad visibility
 - **User and flow context analysis**
 - Network behavior and anomaly detection
 - Incident response and network forensics
- * Cisco FirePOWER and FireSIGHT
 - Real-time threat management
 - Deeper contextual visibility for threats bypassing the perimeters
 - URL control
- * Advanced Malware Protection (AMP)
 - Endpoint control with AMP for Endpoints
 - Malware control with AMP for networks and content
- * Content Security Appliances and Services
 - Cisco Web Security Appliance (WSA) and Cloud Web Security (CWS)
 - Dynamic threat control for web traffic
 - Outbound URL analysis and data transfer controls
 - Detection of suspicious web activity
 - Cisco Email Security Appliance (ESA)
 - Dynamic threat control for email traffic
 - Detection of suspicious email activity
- * Cisco Identity Services Engine (ISE)
 - User and device identity integration with Lancope StealthWatch
 - Remediation policy actions using pxGrid

Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

Question 3

Refer to this output What is the logging severity level?

**R1#Feb 14 37:15:12:429: %LINEPROTO-5-UPDOWN Line protocol on interface GigabitEthernet0/1.
Change state to up**

- A. Critical
- B. Emergency
- **C. Notification** ✓
- D. Alert

Explanation

Syslog levels are listed below:

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

Number “5” in “%LINEPROTO-5- UPDOWN” is the severity level of this message so in this case it is “notification”.

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real i



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[Security Quiz](#) [HSRP & VRRP Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)

- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > New ENCOR Questions – Part 5 Question 16 to 31

New ENCOR Questions – Part 5 Question 16 to 31

February 25th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of New ENCOR Questions – Part 5 Question 16 to 31:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
16	210	90%	210	100.00%	00:04:29

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

What is YANG used for?

- A. providing a transport for network configuration data between client and server
- B. processing SNMP read-only polls
- C. scraping data via CLI
- **D. describing data models** ✓

Explanation

YANG is used to model each protocol based on RFC 6020.

Reference: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/datamodels/configuration/xe-16/data-models-xe-16-book/yang-netconf.html>

Question 2

The following system log message is presented after a network administrator configures a GRE tunnel:

```
%TUN-RECURDOWN: Interface Tunnel 0 temporarily disabled due to recursive routing.
```

Why is Tunnel 0 disabled?

<https://www.digitaltut.com/encor-questions-part-5-question-16-to-31>

- A. Because the tunnel cannot reach its tunnel destination
- B. Because dynamic routing is not enabled
- **C. Because the best path to the tunnel destination is through the tunnel itself** ✓
- D. Because the router cannot recursively identify its egress forwarding interface

Explanation

The **%TUN-5-RECURDOWN: Tunnel0 temporarily disabled due to recursive routing error** message means that the generic routing encapsulation (GRE) tunnel router has discovered a recursive routing problem. This condition is usually due to one of these causes:

- + A misconfiguration that causes the router to try to route to the tunnel destination address using the tunnel interface itself (recursive routing)
- + A temporary instability caused by route flapping elsewhere in the network

Reference: <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/22327-gre-flap.html>

===== This is the end of this update =====

Question 3

In a Cisco SD-Access solution, what is the role of the Identity Services Engine?

- A. It manages the LISP EID database.
- **B. It is leveraged for dynamic endpoint to group mapping and policy definition.** ✓
- C. It is used to analyze endpoint to app flows and monitor fabric status.
- D. It provides GUI management and abstraction via apps that share context.

Explanation

DNA Controller – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context

Identity Services – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition

Analytics Engine – External Data Collector(s) (e.g. NDP) are leveraged to analyze Endpoint to App flows and monitor fabric status

Reference: https://www.cisco.com/c/dam/global/da_dk/assets/training/seminaria-materials/Software_Defined_Access_2017.pdf

Question 4

Which outcome is achieved with this Python code?

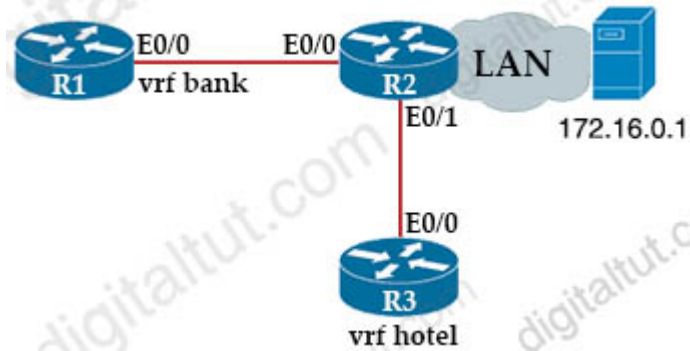
```
client.connect(ip, port=22, username=usr, password=pswd)
stdin, stdout, stderr = client.exec_command('show ip bgp 192.168.10100 bestpath\n')
print(stdout)
```

- A. connects to a Cisco device using SSH and exports the routing table information
- B. connects to a Cisco device using Telnet and exports the routing table information
- **C. connects to a Cisco device using SSH and exports the BGP table for the prefix** ✓

- D. displays the output of the show command in a formatted way

Question 5

Refer to the exhibit.



R2:

```
vrf definition hotel
 address-family ipv4
 exit-address-family
```

```
vrf definition bank
 address-family ipv4
 exit-address-family
```

```
interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.4 255.255.0.0
```

```
interface Ethernet0/1
 vrf forwarding hotel
 ip address 172.1.0.5 255.255.0.0
```

```
router ospf 42 vrf bank
 router-id 1.1.1.1
 network 172.16.0.0 0.0.255.255 area 0
```

```
router ospf 43 vrf hotel
 router-id 3.3.3.3
 network 172.16.0.0 0.0.255.255 area 0
```

R1:

```
vrf definition bank
 !
 address-family ipv4
 exit-address-family
```

Which configuration must be applied to R1 to enable R1 to reach the server at 172.16.0.1?

Option A

```
interface Ethernet0/0
 ip address 172.16.0.7 255.255.0.0
 !
router ospf 44 vrf hotel
 network 172.16.0.0 0.0.255.255
```

Option B

```
interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.7 255.255.0.0
 !
router ospf 44 vrf bank
 network 172.16.0.0 0.0.255.255 area 0
```

```
Option C
interface Ethernet0/0
vrf forwarding hotel
ip address 172.16.0.7 255.255.0.0
!
router ospf 44 vrf hotel
network 172.16.0.0 0.0.255.255 area 0
```

```
Option D
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0
!
router ospf 44 vrf bank
network 172.16.0.0 255.255.0.0
```

- A. Option A
- B. Option C
- C. Option D
- **D. Option B** ✓

Question 6

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

- A. misrouted network packets
- B. duplicate IP addresses
- **C. bandwidth-related packet loss** ✓
- D. port flapping
- **E. excess jitter** ✓

Question 7

Which two actions, when applied in the LAN network segment, will facilitate Layer 3 CAPWAP discovery for lightweight AP? (Choose two)

- A. Enable port security on the switch port
- **B. Configure an ip helper-address on the router interface** ✓
- C. Utilize DHCP option 17
- D. Configure WLC IP address on LAN switch
- **E. Utilize DHCP option 43** ✓

Explanation

In a Cisco Unified Wireless network, the LAPs must first discover and join a WLC before they can service wireless clients.

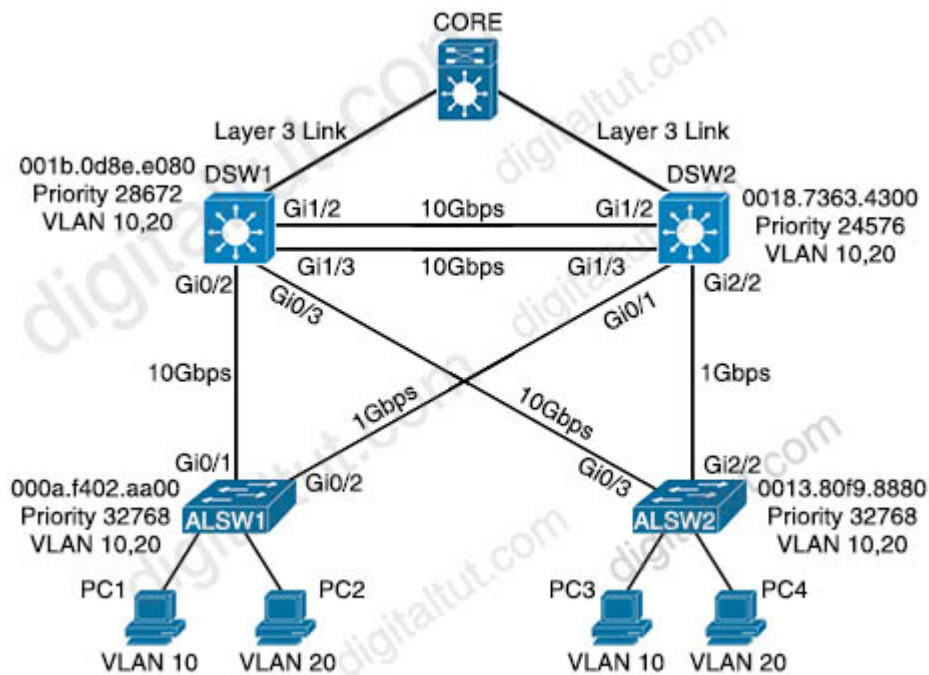
However, this presents a question: how did the LAPs find the management IP address of the controller when it is on a different subnet?

If you do not tell the LAP where the controller is **via DHCP option 43**, DNS resolution of “Cisco-capwap-controller.local_domain”, or statically configure it, the LAP does not know where in the network to find the management interface of the controller.

Reference: <https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html>

Question 8

Refer to the exhibit.



How to make DSW1 the primary root for VLAN 10? (Choose two)

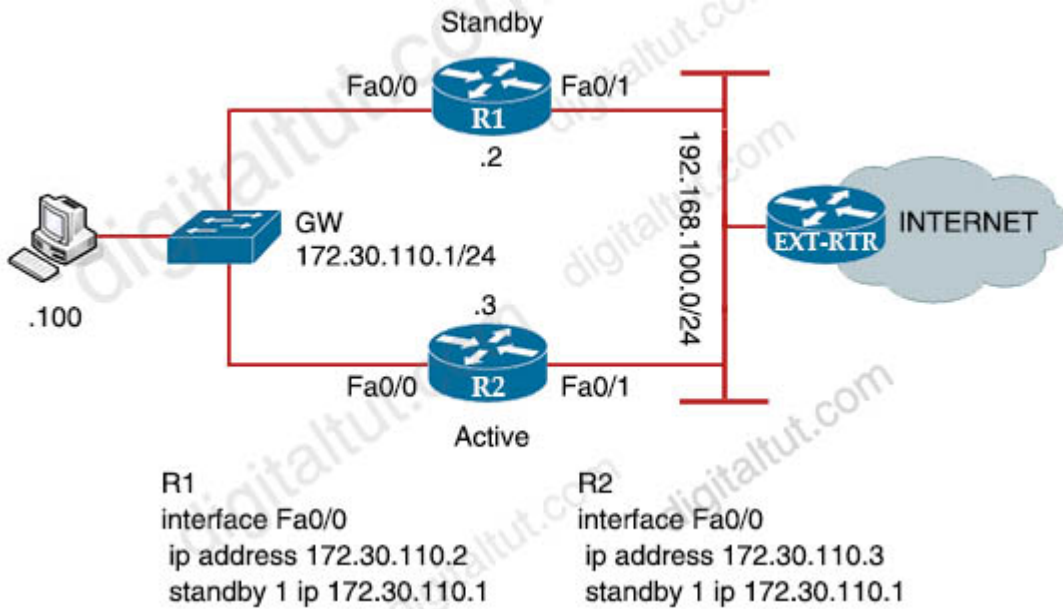
- A. DSW2(config-if)#spanning-tree port-priority 128
- B. DSW2(config-if)#spanning-tree port-priority 16
- **C. DSW1(config-if)#spanning-tree port-priority 0** ✓
- D. DSW2(config-if)#interface gi1/3
- **E. DSW1(config-if)#interface gi1/3** ✓

Explanation

Maybe something was wrong with this question but we still have to choose the best answers.

Question 9

Refer to the exhibit.



Which configuration change ensures that R1 is the active gateway whenever it is in a functional state for the 172.30.110.0/24 network?

Option A R1 standby 1 preempt R2 standby 1 priority 90	Option B R1 standby 1 preempt R2 standby 1 priority 100
Option C R2 standby 1 priority 100 standby 1 preempt	Option D R2 standby 1 priority 110 standby 1 preempt

- **A. Option A** ✓
- B. Option D
- C. Option C
- D. Option B

Explanation

By default, HSRP does not have preemption enabled so we have to enable it on R1 so that R1 can take the active role of R2. We also need to lower the priority of R2 (to 90) than that of R1 (the default HSRP priority is 100) so that R1 can take the active role.

Question 10

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

- A. provide QoS prioritization services such as marking, queueing, and classification for critical network traffic
- B. provide redundant aggregation for access layer devices and first-hop redundancy protocols such as VRRP
- C. provide redundant Layer 3 point-to-point links between the core devices for more predictable and faster convergence** 
- D. provide advanced network security features such as 802.1X, DHCP snooping, VACLs, and port security

Explanation

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.

Considerations at the core layer include

- Providing high-speed switching (i.e., fast transport)
- Providing reliability and fault tolerance
- Scaling by using faster, and not more, equipment
- Avoiding CPU-intensive packet manipulation caused by security, inspection, quality of service (QoS) classification, or other processes

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

Question 11

Based on the output below, which Python code shows the value of the “upTime” key?

```
{
  "response": [{
    "family": "Routers",
    "type": "Cisco ASR 1001-X Router",
    "errorCode": null,
    "location": null,
    "macAddress": "00:c8:8b:80:bb:00",
    "hostname": "asr1001-x.abc.inc",
    "role": "BORDER ROUTER",
    "lastUpdateTime": 1577391299537,
    "serialNumber": "FXS1932Q1SE",
    "softwareVersion": "16.3.2",
    "locationName": null,
    "upTime": "49 days, 13:43:44:13",
    "lastUpdated": "2019-12-22 16:35:21"
  }]
}
```

Option A

```
json_data = response.json()
print(json_data[response][0][upTime])
```

Option B

```
json_data = response_json()
print(json_data['response']['family']['upTime'])
```

Option C

```
json_data = response.json()
print(json_data['response'][0]['upTime'])
```

Option D

```
json_data = json.loads(response.text)
print(json_data['response']['family']['upTime'])
```

- A. Option A
- **B. Option C** ✓
- C. Option B
- D. Option D

Explanation

You can test this question in Python and see the output below:

```
C:\Users\PC>python
Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018,
Type "help", "copyright", "credits" or "licen
>>> import json
>>> json_string = """
... {
...   "response": [{
...     "family": "Routers",
...     "type": "Cisco ASR 1001-X Router",
...     "errorCode": null,
...     "location": null,
...     "macAddress": "00:c8:8b:80:bb:00",
...     "hostname": "asr1001-x.abc.inc",
...     "role": "BORDER ROUTER",
...     "lastUpdateTime": 1577391299537,
...     "serialNumber": "FXS1932Q1SE",
...     "softwareVersion": "16.3.2",
...     "locationName": null,
...     "upTime": "49 days, 13:43:44:13",
...     "lastUpdated": "2019-12-22 16:35:21"
...   }]
... }
... """
>>> json_data = json.loads(json_string)
>>> print(json_data['response'][0]['upTime'])
49 days, 13:43:44:13
>>>
```

Note: We need to call the first element “[0]” in “json_data[‘response’][0][‘upTime’]” command because “response” is an array with only one element.

Question 12

Drag and drop the descriptions of the VSS technology from the left to the right. Not all options are used.

1 supported on the Cisco 4500 and 6500 series	
2 combines exactly two devices	VSS
3 supports devices that are geographically separated	
4 supported on Cisco 3750 and 3850 devices	
5 supports up to nine devices	
6 uses proprietary cabling	

Note: Please type the corresponding numbers of each item on the left to the blank below and arrange them ascendingly. For example: 136 (which means 136 for the three answers at the right side).

Please type your answer here: 123 ✓

Explanation

The following characteristics are correct for StackWise (but not VSS):

- + can be connected in up to 9 devices
- + is supported only on line 3750 and (2960/3650/3850/3750+)
- + uses proprietary cable for connection

Question 13

A customer has completed the installation of a Wi-Fi 6 greenfield deployment at their new campus. They want to leverage Wi-Fi 6 enhanced speeds on the trusted employee WLAN. To configure the employee WLAN, which two Layer 2 security policies should be used? (Choose two)

- A. WPA2 (AES) + WEP
- B. OPEN ✓
- C. WPA (AES)
- D. 802.1X ✓

Explanation

Wi-Fi 6 (IEEE 802.11ax)

In greenfield we don't need to use any security policy to reduce the wasting time of encryption/decryption.

Wi-Fi 6 does not support WPA with AES while WPA2 (AES) would slow down the connection -> Only 802.1X is the best choice left.

Question 14

Refer to the exhibit.

```
Vlan503 - Group 1
State is Active
  1 state change, last state change 32w6d
Virtual IP address is 10.0.3.241
Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.064 secs
Preemption enabled
Active router is local
Standby router is 10.0.3.242, priority 100 (expires in 10.624 sec)
Priority 110 (configured 110)
Group name is "hsrp-VI503-1" (default)
```

Which two facts does the device output confirm? (Choose two)

- A. The device is configured with the default HSRP priority
- **B. The standby device is configured with the default HSRP priority** ✓
- **C. The device is using the default HSRP hello timer** ✓
- D. The device's HSRP group uses the virtual IP address 10.0.3.242.
- E. The device sends unicast messages to its peers

Question 15

Refer to the exhibit.

```
Person#1:
First Name is Johnny
Last Name is Table
Hobbies are:
• Running
• Video games

Person#2
First Name is Billy
Last Name is Smith
Hobbies are:
• Napping
• Reading
```

Which JSON syntax is derived from this data?

Option A
 { 'Person': [{ 'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games'] }, { 'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading'] }] }

Option B
 { { { 'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Hobbies': 'Video games' }, { 'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Hobbies': 'Reading' } } }

Option C

```
{'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Reading'}]}
```

Option D

```
{{{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}}}
```

- A. Option C
- B. Option B
- **C. Option A** 
- D. Option D

Explanation

Option B and Option D are not correct because the first square bracket in “{{[” should not be there.

Option C “Hobbies” should be an array, not “‘Hobbies’: ‘Running’, ‘Video games’”

Option A is correct and we also format it in a more comprehensive way below:

```
{
  'Person': [
    {
      'First Name': 'Johnny',
      'Last Name': 'Table',
      'Hobbies': [
        'Running',
        'Video games'
      ]
    },
    {
      'First Name': 'Billy',
      'Last Name': 'Smith',
      'Hobbies': [
        'Napping',
        'Reading'
      ]
    }
  ]
}
```

Question 16

An engineer creates the configuration below. Drag and drop the authentication methods from the left into the order of priority on the right. Not all options are used.

```
R1#sh run | i aaa
aaa new-model
aaa authentication login default group ACE group AAA_RADIUS local-case
aaa session-id common
R1#
```


1	AAA servers of AAA_RADIUS group	Step 1
2	tacacs servers of group ACE	Step 2
3	AAA servers of ACE group	Step 3
4	local configured username in non-case-sensitive format	Step 4
5	local configured username in case-sensitive format	
6	If no method works, then deny login	

Note: Please type the corresponding numbers of each item on the left to the blank below to match from Step 1 to Step 4. For example: 1642 (which means 1 for Step 1; 6 for Step 2; 4 for Step 3 and 2 for Step 4). Please type your answer here: 3156 ✓

Explanation

The “aaa authentication login default group ACE group AAA_RADIUS local-case” command is broken down as follows:

- + The ‘**aaa authentication**’ part is simply saying we want to configure authentication settings.
- + The ‘**login**’ is stating that we want to prompt for a username/password when a connection is made to the device.
- + The ‘**default**’ means we want to apply for all login connections (such as tty, vty, console and aux). If we use this keyword, we don’t need to configure anything else under tty, vty and aux lines. If we don’t use this keyword then we have to specify which line(s) we want to apply the authentication feature.
- + The ‘**group ACE group AAA_RADIUS**’ means all users are authenticated using group ACE (the first method). If the credentials are not found on this group, then the group AAA_RADIUS is used (the second method).
- + The ‘**local-case**’ option uses case-sensitive local usernames.

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real !)



I'm not a robot

reCAPTCHA
Privacy - Terms[Subscribe to comments feed](#)[New ENCOR Questions – Part 5 Questions 1 to 15](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [New ENCOR Questions- Part 5](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)

- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > New ENCOR Questions – Part 5 Questions 1 to 15

New ENCOR Questions – Part 5 Questions 1 to 15

February 25th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of New ENCOR Questions – Part 5 Questions 1 to 15:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
15	250	90%	240	96.00%	00:01:30

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which encryption hashing algorithm does NTP use for authentication?

- **A. MD5** ✓
- B. SSL
- C. AES128
- D. AES256

Explanation

An example of configuring NTP authentication is shown below:

```
Router1(config)#ntp authentication-key 2 md5 9tut
Router1(config)#ntp authenticate
Router1(config)#ntp trusted-key 2
```

Question 2

Refer to the exhibit.



```

London(config)#interface fa0/1
London(config-if)#switchport trunk encapsulation dot1q
London(config-if)#switchport mode trunk
  
```

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
  
```

```

London(config-if)#end
NewYork#show dtp interface fa0/1
DTP information for FastEthernet0/1:
  TOS/TAS/TNS:      ACCESS/AUTO/ACCESS
  TOT/TAT/TNT:      NATIVE/ISL/NATIVE
  
```

Communication between London and New York is down. Which command set must be applied to resolve this issue?

Option A NewYork(config)#int f0/1 NewYork(config)#switchport nonegotiate NewYork(config)#end NewYork#	Option B NewYork(config)#int f0/1 NewYork(config)#switchport trunk encap dot1q NewYork(config)#end NewYork#
Option C NewYork(config)#int f0/1 NewYork(config)#switchport mode dynamic desirable NewYork(config)#end NewYork#	Option D NewYork(config)#int f0/1 NewYork(config)#switchport mode trunk NewYork(config)#end NewYork#

- A. Option D
- **B. Option B** ✓
- C. Option A
- D. Option C

Explanation

From the output line “TOT/TAT/TNT: NATIVE/ISL/NATIVE”, we see interface f0/1 of NewYork router is hard coded ISL which is mismatched with 802.1Q so we have to change trunking encapsulation on NewYork router to 802.1Q.

Note: The TOS/TAS/TNS of “ACCESS/AUTO/ACCESS” shows it is currently operating as an Access Port, in Dynamic Auto mode, and its negotiated to be an Access Port (but it can be negotiated to become a trunk port).

Good reference: <https://loopedback.com/2017/08/26/dtp-dynamic-trunking-protocol-the-exam-information-and-a-lot-of-live-cli-output-to-demonstrate-behaviors-of-dtp/>

Note:

TOS = Trunk Operational Status
TAS = Trunk Administrative Status
TNS = Trunk Negotiation Status
TOT = Trunk Operational Type
TAT = Trunk Administrative Type
TNT = Trunk Negotiation Type

Question 3

Question 5

Refer to the exhibit.

```
SW2# show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
```

Group	Port-channel	Protocol	Ports
1	Pol(SD)	PAgP	Gi0/0(I) Gi0/1(I)

```
SW3# show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
```

Group	Port-channel	Protocol	Ports
1	Pol(SD)	LACP	Gi0/0(I) Gi0/1(I)

Which action resolves the EtherChannel issue between SW2 and SW3?

- A. Configure switchport nonegotiate on SW3
- **B. Configure channel-group 1 mode desirable on both interfaces** ✓
- C. Configure switchport mode trunk on SW2
- D. Configure channel-group 1 mode active on both interfaces ✓

Explanation

From the output we learn that SW2 is running PAgP while Sw3 is running LACP so they cannot form Etherchannel. Therefore we need to configure only LACP (active mode) or PAgP (desirable mode) on both switches.

Question 6

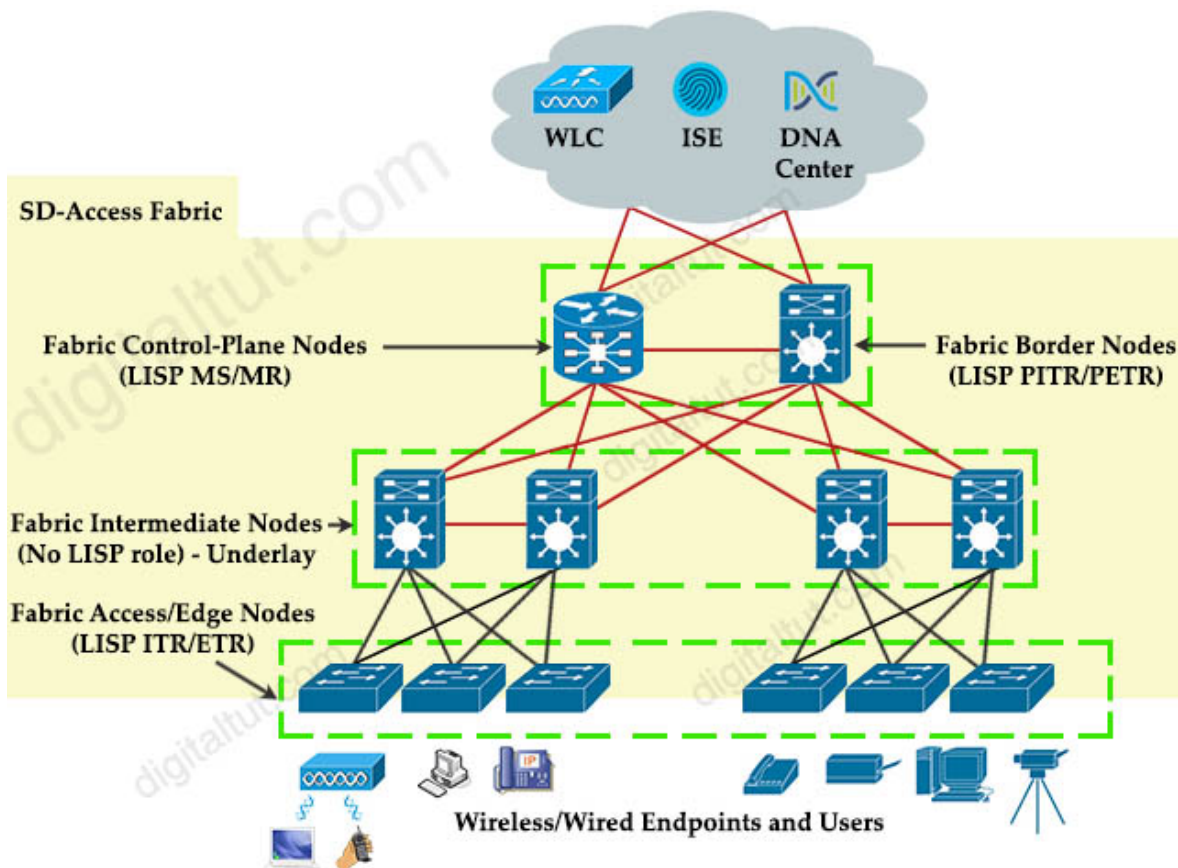
What are two characteristics of Cisco SD-Access elements? (Choose two)

- A. The border node has the full RLOC-to-EID mapping database
- **B. The control plane node has the full RLOC-to-EID mapping database** ✓
- C. Traffic within the fabric always goes through the control plane node
- D. Fabric endpoints are connected directly to the border node
- **E. The border node is required for communication between fabric and nonfabric devices** ✓

Explanation

There are five basic device roles in the fabric overlay:

- + Control plane node: This node contains the settings, protocols, and mapping tables to provide the endpoint-to-location (EID-to-RLOC) mapping system for the fabric overlay.
- + Fabric border node: This fabric device (for example, core layer device) connects external Layer 3 networks to the SDA fabric.
- + Fabric edge node: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.
- + Fabric WLAN controller (WLC): This fabric device connects APs and wireless endpoints to the SDA fabric.
- + Intermediate nodes: These are intermediate routers or extended switches that do not provide any sort of SD-Access fabric role other than underlay services.

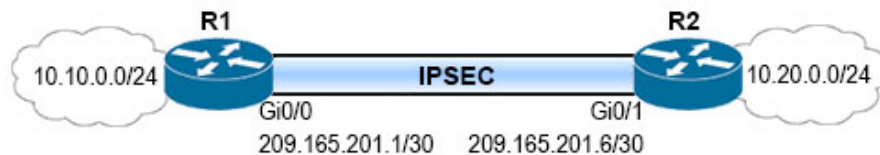


Reference: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

Question 7

Refer to the exhibit.

<pre> access-list 100 permit gre host 209.165.201.1 host 209.165.201.6 crypto isakmp policy 5 authentication pre-share hash sha256 encryption aes group 14 crypto isakmp key D@t@c3nt3r address 209.165.201.6 crypto ipsec transform-set My_Set esp-aes esp-sha-hmac mode transport crypto map MAP 10 ipsec-isakmp set peer 209.165.201.6 set transform-set My_Set match address 100 interface GigabitEthernet0/0 description outside_interface no switchport ip address 209.165.201.1 255.255.255.252 crypto map MAP interface Tunnel 100 ip address 192.168.100.1 255.255.255.0 ip mtu 1400 tunnel source GigabitEthernet0/0 tunnel destination 209.165.201.6 ip route 10.20.0.0 255.255.255.0 192.168.100.2 Tunnel100 </pre>	<pre> access-list 100 permit gre host 209.165.201.6 host 209.165.201.1 crypto isakmp policy 5 authentication pre-share hash sha256 encryption aes group 14 crypto isakmp key D@t@c3nt3r address 209.165.201.1 crypto ipsec transform-set My_Set esp-aes esp-sha-hmac mode transport crypto map MAP 10 ipsec-isakmp set peer 209.165.201.1 set transform-set My_Set match address 100 interface GigabitEthernet0/1 description outside_interface no switchport ip address 209.165.201.6 255.255.255.252 crypto map MAP interface Tunnel 100 ip address 192.168.100.2 255.255.255.0 ip mtu 1400 tunnel source GigabitEthernet0/0 tunnel destination 209.165.201.1 ip route 10.10.0.0 255.255.255.0 192.168.100.1 Tunnel100 </pre>



A network engineer must simplify the IPsec configuration by enabling IPsec over GRE using IPsec profiles. Which two configuration changes accomplish this? (Choose two)

- A. Remove the crypto map and modify the ACL to allow traffic between 10.10.0.0/24 to 10.20.0.0/24
- **B. Create an IPsec profile, associate the transform-set, and apply the profile to the tunnel interface** ✓
- C. Apply the crypto map to the tunnel interface and change the tunnel mode to tunnel mode ipsec ipv4 ✓
- **D. Remove all configuration related to crypto map from R1 and R2 and eliminate the ACL 100** ✗

Question 8

Which two methods are used to reduce the AP coverage area? (Choose two)

- **A. Reduce AP transmit power** ✓
- B. Disable 2.4 GHz and use only 5 GHz
- C. Enable Fastlane
- D. Reduce channel width from 40 MHz to 20 MHz
- **E. Increase minimum mandatory data rate** ✓

Explanation

The **transmit power of an AP affects the wireless coverage area** and the maximum achievable signal-to-noise ratio. Proper configuration of transmit power is important for ensuring a wireless network is operating at its highest capacity.

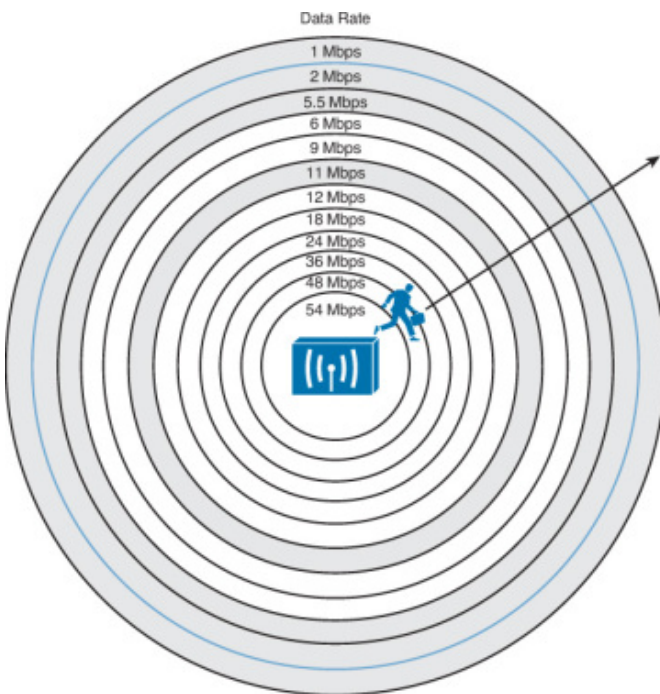
Reference: https://documentation.meraki.com/MR/Radio_Settings/Transmit_Power_and_Antenna_Configuration

AP coverage area or the cell size, according to this [Cisco link](#), there are two ways to reduce the AP coverage area:

- + Tuning Cell Size with Transmit Power
- + Tuning Cell Size with Data Rates

Setting the transmit power level is a simplistic approach to defining the cell size, but that is not the only variable involved. The cell size of an AP is actually a compromise between its transmit power and the data rates that it offers.

To design a wireless LAN for best performance, you would most likely need to **disable some of the lower data rates**. For example, you could disable the 1, 2, and 5.5 Mbps rates to force clients to use higher rates and better modulation and coding schemes. That would improve throughput for individual clients and would also benefit the BSS as a whole by eliminating the slower rates that use more time on a channel.



-> Therefore increasing minimum mandatory data rate would reduce coverage area but enhance performance.

Question 9

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

- **A. virtualized environment that provides traffic isolation and segmentation in the SD-WAN fabric** ✓
- B. common exchange point between two different services
- C. attribute to identify a set of services offered in specific places in the SD-WAN fabric
- D. virtual channel used to carry control plane information

Question 10

Drag and drop the solutions that comprise Cisco Cyber Threat Defense from the left onto the objectives they accomplish on the right.

Note: You just need to click on one of the boxes on the right to match it with the corresponding box on the left.

detects suspicious web activity	Web Security Appliance ✓
analyzes network behavior and detects anomalies	StealthWatch ✓
uses pxGrid to remediate security threats	Identity Services Engine ✓

Question 11

Drag and drop the characteristic from the left onto the orchestration tools that they describe on the right.

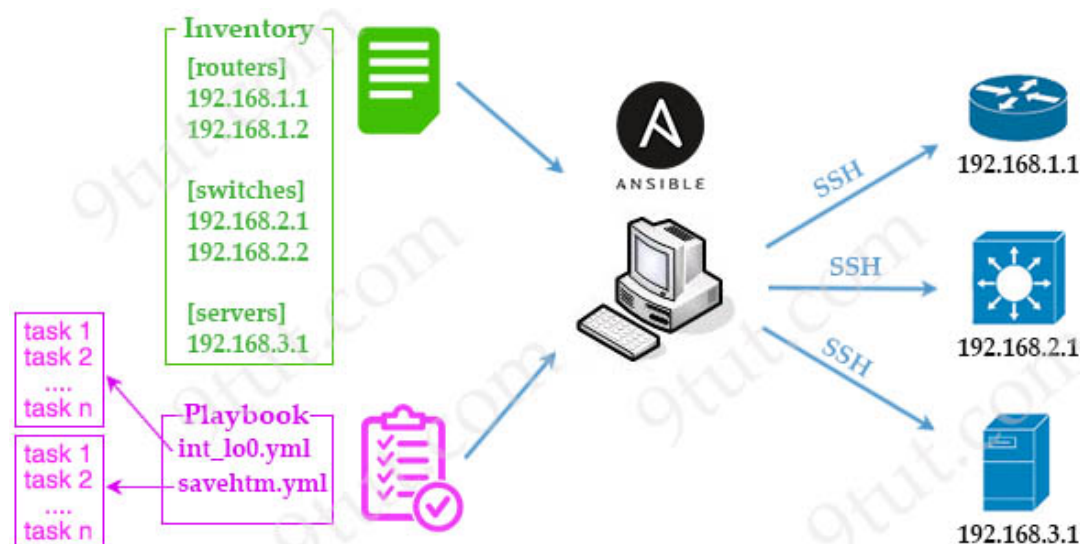
1 uses playbooks	Ansible
2 uses a pull model	
3 procedural	
4 declarative	Puppet

Please type the corresponding numbers of each item on the left to the blank below and arrange them ascendingly. For example: 1423 (which means 14 for first group, 23 for second group).

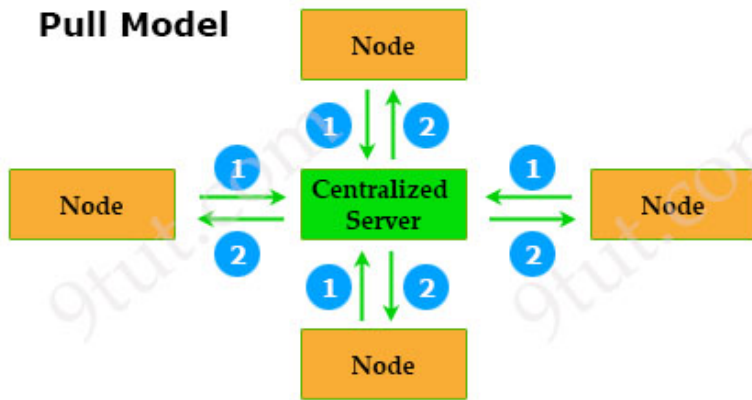
Please type your answer here: 1324 ✓

Explanation

In Ansible, **Playbooks** are files that provide actions and logic about what Ansible should do. Ansible playbooks are files that contain tasks to configure hosts. Ansible playbooks are written in YAML format.



Puppet is based on a Pull deployment model, where the nodes check in regularly after every 1800 seconds with the Master to see if anything needs to be updated in the agent. If anything needs to be updated the agent pulls the necessary Puppet codes from the Master and performs required actions.



Chef and Ansible encourage a procedural style where you write code that specifies, step-by-step, how to achieve some desired end state. Terraform, SaltStack, and Puppet all encourage a more declarative style where you write code that specifies your desired end state, and the IAC tool itself is responsible for figuring out how to achieve that state.

Question 12

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

- A. group of services tested to guarantee devices and links liveliness within the SD-WAN overlay
- B. list of ordered statements that define node configurations and authentication used within the SD-WAN overlay
- **C. Set of statements that defines how data is forwarded based on IP packet information and specific VPNs** ✓
- D. detailed database mapping several kinds of addresses with their corresponding location

Explanation

Data policy operates on the data plane in the Cisco SD-WAN overlay network and affects how data traffic is sent among Cisco SD-WAN devices in the network. The Cisco SD-WAN architecture defines two types of data policy, centralized data policy, which controls the flow of data traffic based on the IP header fields in the data packets and based on network segmentation, and localized data policy, which controls the flow of data traffic into and out of interfaces and interface queues on the devices.

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

Question 13

What is an emulated machine that has dedicated compute, memory, and storage resources and a fully installed operating system?

- A. container
- **B. virtual machine** ✓
- C. mainframe
- D. host

Question 14

Refer to the exhibit.

TYPE	PROT	SYSTEM IP	ID	ID	PRIVATE IP	PORT	LOCAL	COLOR	PROXY	STATE	UPTIME	PORT
PUBLIC IP												ID

vsmart	dtls	0.0.0.0	100	1	192.168.100.80							
12346	10.10.20.70				12446	default			No	up		
0:02:24:09	0											
vbond	dtls	0.0.0.0	0	0	192.168.100.81							
12346	10.10.20.80				12346	default			-	up		
0:02:24:10	0											
vmanage	dtls	4.4.4.90	100	0	192.168.100.82							
12446	10.10.20.90				12446	default						

POST

https://192.168.100.80:12442/i_security_check

Send

Params

Authorization

Headers (8)

Body

Pre-request Script

Tests

Settings

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

KEY	VALUE	DESCRIPTION
☒ i_username	admin	
☒ i_password	admin	
Key	Value	Description

Could not get any response

There was an error connecting to https://192.168.100.80:12442/i_security_check

Why this might have happened:

- The server couldn't send a response: Ensure that the backend is working properly
- Self-signed SSL certificates are being blocked: Fix this by turning off 'SSL certificate verification' in *Settings > General*
- Proxy configured incorrectly: Ensure that proxy is configured correctly in *Settings > Proxy*
- Request timeout: Change request timeout in *Settings > General*

What step resolves the authentication issue?

- A. target 192.168.100.82 in the URI ✓
- B. use basic authentication
- C. change the port to 12446
- D. restart the vsmart host

Explanation

The first figure is the output of the “show control connections” command. From this figure we learned that the vManage IP address is 192.168.100.82 so we need to connect to this IP address (not 192.168.100.80).

Question 15

Refer to the exhibit.


```

No Hellos (Passive interface)
Supports Link-local Signaling (LLS)
! lines omitted for brevity
GigabitEthernet0/1 is up, line protocol is up
Internet Address 72.16.30.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 72.16.11.29, Network Type BROADCAST, Cost: 1
Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                1          no            no             Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 172.16.11.29, Interface address 172.16.30.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
No Hellos (Passive interface)
Supports Link-local Signaling (LLS)
! lines omitted for brevity
GigabitEthernet0/0 is up, line protocol is up
Internet Address 72.16.11.29/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 72.16.11.29, Network Type BROADCAST, Cost: 1
Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                1          no            no             Base
Transmit Delay is 1 sec, State DROTHER, Priority 1
Designated Router (ID) 172.16.11.27, Interface address 172.16.11.27
Backup Designated router (ID) 172.16.11.30, Interface address 172.16.11.30
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:07
Supports Link-local Signaling (LLS)
! lines omitted for brevity

```

A network engineer configures OSPF and reviews the router configuration. Which interface or interfaces are able to establish OSPF adjacency?

- A. only GigabitEthernet0/1
- **B. only GigabitEthernet0/0** ✓
- C. Gigabit Ethernet0/0 and GigabitEthernet0/1
- D. GigabitEthernet0/1 and GigabitEthernet0/1.40

Explanation

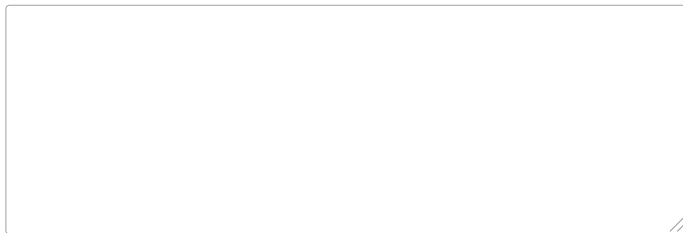
This is the output of command “show ip ospf interface”. From the line “No hellos (Passive interface)”, we learn that interface Gi0/1 was configured passive interface -> It cannot establish OSPF adjacency. Only Gi0/0 established OSPF adjacency.

Note: DROTHER is just a sign of FULL state in OSPF but this router is not a DR or BDR. Therefore DROTHER means interface was established adjacency successfully with the neighbor interface.

Comments

1. No comments yet.
1. No trackbacks yet.

Add a Comment



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[New ENCOR Questions – Part 5 Question 16 to 31](#) [New ENCOR Questions – Part 5](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [New ENCOR Questions- Part 5](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)

- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH



[Home](#) > New ENCOR Questions 4 – Part 1

New ENCOR Questions 4 – Part 1

 February 13th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of New ENCOR Questions 4 - Part 1:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
20	420	90%	420	100.00%	00:03:21

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

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

- A. to implement policies and communicate with networks outside the fabric
- B. to connect APs and wireless endpoints to the SD-Access fabric
- C. to connect external Layer 3 networks to the SD Access fabric
- **D. to run a mapping system that manages endpoint to network device relationships** ✓

Explanation

Control-Plane Nodes – Map System that manages Endpoint to Device relationships

Fabric Border Nodes – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric

Fabric Edge Nodes – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric

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

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

Question 2

What is a characteristic of para-virtualization?

- A. Para-virtualization allows direct access between the guest OS and the hypervisor
- **B. Para-virtualization allows the host hardware to be directly accessed** ✓
- C. Para-virtualization lacks support for containers
- D. Para-virtualization guest servers are unaware of one another

Explanation

Paravirtualization works differently from the full virtualization. It doesn't need to simulate the hardware for the virtual machines. The hypervisor is installed on a physical server (host) and a guest OS is installed into the environment. Virtual guests aware that it has been virtualized, unlike the full virtualization (where the guest doesn't know that it has been virtualized) to take advantage of the functions.

In full virtualization, guests will issue a hardware calls but in paravirtualization, guests will directly communicate with the host (hypervisor) using drivers.

Question 3

Which two southbound interfaces originate from Cisco DNA Center and terminate at fabric underlay switches? (Choose two)

- A. UDP 6007: NetFlow
- B. UDP 67: DHCP
- C. TCP 23: Telnet
- **D. ICMP: Discovery** ✓
- **E. UDP 162: SNMP** ✓

Explanation

In the figure below, we can see ICMP & SNMP can reach to underlay switches.

The screenshot shows the Cisco DNA Center Discovery page. On the left, the 'Discoveries' section shows a 'MasterEN' discovery with a range of 10.0.255.1-10.0.255.9. The 'DISCOVERY DETAILS' section shows CDP Level: None, Protocol Order: ssh, Retry Count: 3, Timeout: 5, IP Range: 10.0.255.1-10.0.255.9, IP Filter List: None, Preferred Management IP: Use LoopBack. The 'HISTORY' section shows a single completed run. On the right, the 'Devices' section shows a list of discovered devices with columns for IP Address, Device Name, Status, and various protocols (ICMP, CLI, HTTP(S), NETCONF). A red box highlights the 'ICMP' and 'SNMP' columns, indicating that these protocols are successful for the discovered devices.

IP Address	Device Name	Status	ICMP	SNMP	CLI	HTTP(S)	NETCONF
10.0.255.9	SW-MCU	Success	✓	✓	✓	✓	✓
10.0.255.9	SW-SP-East	Success	✓	✓	✓	✓	✓
10.0.255.1	N7K-CORE1	Success	✓	✓	✓	✓	✓
10.0.255.2	N7K-CORE2	Success	✓	✓	✓	✓	✓
10.14.200.1	RTR-IVAN-MPLS prime site (sftrace.com)	Success	✓	✓	✓	✓	✓
10.0.255.4	RTR-IVAN-IVNET prime.cisco (sftrace.com)	Success	✓	✓	✓	✓	✓
10.0.255.8	DC-2	Success	✓	✓	✓	✓	✓
10.0.255.7	DC-1 prime.cisco (sftrace.com)	Success	✓	✓	✓	✓	✓
172.17.254.205	CT5508	Success	✓	✓	✓	✓	✓
10.0.255.6	SW-SP-West	Success	✓	✓	✓	✓	✓

Question 4

Refer to the exhibit.

```
vlan 222
  remote-span
!
vlan 223
  remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
```

What happens to access interfaces where VLAN 222 is assigned?

- A. A description "RSPAN" is added
- B. They cannot provide PoE
- C. STP BPDU guard is enabled
- **D. They are placed into an inactive state** ✓

Explanation

Access ports (including voice VLAN ports) on the RSPAN VLAN are put in the inactive state.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html

Question 5

What is a characteristic of MACsec?

- A. 802.1AE is built between the host and switch using the MKA protocol using keys generated via the Diffie-Hellman algorithm (anonymous encryption mode)
- B. 802.1AE provides encryption and authentication services
- **C. 802.1AE is built between the host and switch using the MKA protocol, which negotiates encryption keys based on the master session key from a successful 802.1X session** ✓
- D. 802.1AE is negotiated using Cisco AnyConnect NAM and the SAP protocol

Explanation

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/sec/b_169_sec_9300_cg/macsec_encryption.html

-> MACsec only provides encryption, not authentication -> Answer '802.1AE provides encryption and authentication services' is not correct.

Successful IEEE 802.1X authentication is the first step in establishing a MACsec session. IEEE 802.1X provides primary key material to the supplicant and switch that will subsequently be used by MACsec -> Answer '802.1AE is built between the host and switch using the MKA protocol, which negotiates encryption keys based on the master session key from a successful 802.1X session' is correct.

If an MKA cryptographic algorithm is not configured, a default cryptographic algorithm of AES-CMAC-128 (Cipher-based Message Authentication Code with 128-bit Advanced Encryption Standard) is used -> Answer '802.1AE is built between the host and switch using the MKA protocol using keys generated via the Diffie-Hellman algorithm (anonymous encryption mode)' is not correct.

Reference: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-16/macsec-xe-16-book/wan-macsec-mka-support-enhance.html>

802.1AE is negotiated using MKA Protocol so answer '802.1AE is negotiated using Cisco AnyConnect NAM and the SAP protocol' is not correct.

Question 6

A customer requests a network design that supports these requirements:

- * FHRP redundancy
- * multivendor router environment
- * IPv4 and IPv6 hosts

Which protocol does the design include?

- A. VRRP version 2
- **B. VRRP version 3** ✓
- C. GLBP
- D. HSRP version 2

Explanation

Unlike HSRP or GLBP, VRRP is an open standard. Only VRRPv3 supports both IPv4 and IPv6.

Question 7

Refer to the exhibit.

```
DSW2#sh spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority 24596
    Address   0018.7363.4300
      Cost     2
    Port      13 (FastEthernet1/0/11)
  Hello Time 2 sec Max Age 20 sec
        Forward Delay 15 sec

  Bridge ID Priority 28692 (priority 28672 sys-id-ext 20)
    Address   001b.0d8e.e080
  Hello Time 2 sec Max Age 20 sec
        Forward Delay 15 sec
    Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
-----
Fa1/0/7   Desg FWD 2    128.9   P2p
Fa1/0/10  Desg FWD 2    128.12  P2p
Fa1/0/11  Root FWD 2    128.13  P2p
Fa1/0/12  Altn BLK 2    128.14  P2p
```

What does the output confirm about the switch's spanning tree configuration?

- A. The spanning-tree operation mode for this switch is IEEE
- B. The spanning-tree mode stp ieee command was entered on this switch
- **C. The spanning-tree operation mode for this switch is PVST+ ✓**
- D. The spanning-tree operation mode for this switch is PVST

Explanation

The default spanning-tree mode in Cisco switch is PVST+. This spanning-tree mode is based on the IEEE 802.1D standard and Cisco proprietary extensions. PVST+ is same as standard IEEE 802.1D but it runs on each VLAN. In the output we see the line "Spanning tree enabled protocol ieee" under "VLAN 20" so it can say the switch is running in PVST+ mode.

Question 8

Which solution do IaaS service providers use to extend a Layer 2 segment across a Layer 3 network?

- A. VRF
- **B. VXLAN ✓**
- C. VLAN
- D. VTEP

Question 9

How does EIGRP differ from OSPF?

- A. EIGRP uses more CPU and memory than OSPF
- B. EIGRP has a full map of the topology, and OSPF only knows directly connected neighbors
- **C. EIGRP supports equal or unequal path cost, and OSPF supports only equal path cost. ✓**
- D. EIGRP is more prone to routing loops than OSPF

Explanation

Both EIGRP and OSPF is not susceptible to routing loops and EIGRP is not more prone to routing loops than OSPF -> Answer 'EIGRP is more prone to routing loops than OSPF' is not correct.

Both EIGRP and OSPF has a full map of the topology -> Answer 'EIGRP has a full map of the topology, and OSPF only knows directly connected neighbors' is not correct.

OSPF maintains information about all the networks and running routers in its area. Each time there is a change within the area, all routers need to re-sync their database and then run SPF again. This process makes it more CPU intensive. EIGRP, on the other hand, has triggered and incremental updates. Therefore EIGRP is more efficient in terms of CPU usage and memory.

Question 10

After a redundant route processor failure occurs on a Layer 3 device, which mechanism allows for packets to be forwarded from a neighboring router based on the most recent tables?

- A. RP failover
- **B. NSF** ✓
- C. BFD
- D. RPVST+

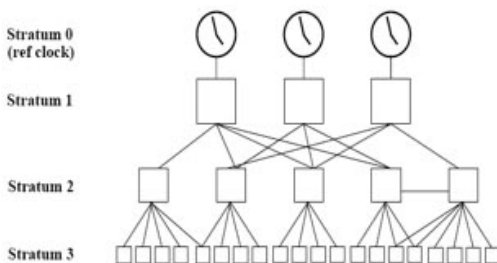
Question 11

Which measure is used by an NTP server to indicate its closeness to the authoritative time source?

- A. time zone
- B. hop count
- **C. stratum** ✓
- D. latency

Explanation

The stratum levels define the distance from the reference clock. A reference clock is a stratum 0 device that is assumed to be accurate and has little or no delay associated with it. Stratum 0 servers cannot be used on the network but they are directly connected to computers which then operate as stratum-1 servers. A stratum 1 time server acts as a primary network time standard.



A stratum 2 server is connected to the stratum 1 server; then a stratum 3 server is connected to the stratum 2 server and so on. A stratum 2 server gets its time via NTP packet requests from a stratum 1 server. A stratum 3 server gets its time via NTP packet requests from a stratum-2 server...

Question 12

Which two components are supported by LISP? (Choose two)

- **A. egress tunnel router** ✓
- **B. proxy ETR** ✓
- C. route reflector
- D. HMAC algorithm
- E. spoke

Explanation

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

A LISP proxy ETR (PETR) implements ETR functions on behalf of non-LISP sites. A PETR is typically used when a LISP site needs to send traffic to non-LISP sites but the LISP site is connected through a service provider that does not accept nonroutable EIDs as packet sources. PETRs act just like ETRs but for EIDs that send traffic to destinations at non-LISP sites.

Question 13

Which unit measures the power of a radio signal with reference to 1 milliwatt?

- A. dBw
- **B. dBm** ✓
- C. mW
- D. dBi

Explanation

dBm is an abbreviation for “decibels relative to one milliwatt,” where one milliwatt (1 mW) equals 1/1000 of a watt. It follows the same scale as dB. Therefore 0 dBm = 1 mW, 30 dBm = 1 W, and -20 dBm = 0.01 mW

Question 14

Drag and drop the virtual component from the left onto their descriptions on the right.

Note: You just need to click on one of the boxes on the right to match it with the corresponding box on the left.

configuration file containing settings for a virtual machine such as guest OS	VMX ✓
component of a virtual machine responsible for sending packets to the hypervisor	vNIC ✓
zip file containing a virtual machine configuration file and a virtual disk	OVA ✓
file containing a virtual machine disk drive	VMDK ✓

Explanation

The VMX file simply holds the virtual machine configuration.

VMDK (short for Virtual Machine Disk) is a file format that describes containers for virtual hard disk drives to be used in virtual machines like VMware Workstation or VirtualBox.

An OVA file is an Open Virtualization Appliance that contains a compressed, “installable” version of a virtual machine. When you open an OVA file it extracts the VM and imports it into whatever virtualization software you have installed on your computer.

Question 15

Refer to the exhibit. What is the result when a switch that is running PVST+ is added to this network?

DSW2#sh spanning-tree vlan 10

```
VLAN0010
Spanning tree enabled protocol rstp
Root ID    Priority 4106
           Address 0018.7363.4300
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID   Priority 4106 (priority 4096 sys-id-ext 20)
           Address 0018.7363.4300
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa1/0/7	Desg	FWD	2	128.9	P2p Peer(STP)
Fa1/0/10	Desg	FWD	4	128.12	P2p Peer(STP)
Fa1/0/11	Desg	FWD	2	128.13	P2p Peer(STP)
Fa1/0/12	Desg	FWD	2	128.14	P2p Peer(STP)

- A. Both switches operate in the Rapid PVST+ mode
- B. Both switches operate in the PVST+ mode
- C. Spanning tree is disabled automatically on the network
- **D. DSW2 operates in Rapid PVST+ and the new switch operates in PVST+ ✓**

Explanation

From the output we see DSW2 is running in RSTP mode (in fact Rapid PVST+ mode as Cisco does not support RSTP alone). When a new switch running PVST+ mode is added to the topology, they keep running the old STP instances as RSTP (in fact Rapid PVST+) is compatible with PVST+.

Question 16

What is a characteristic of a next-generation firewall?

- A. filters traffic using Layer 3 and Layer 4 information only
- B. required in each layer of the network
- C. only required at the network perimeter
- **D. provides intrusion prevention ✓**

Explanation

A next generation firewall adds additional features such as application control, integrated **intrusion prevention (IPS)** and often more advanced threat prevention capabilities like sandboxing.

Question 17

A customer has recently implemented a new wireless infrastructure using WLC-5520S at a site directly next to a large commercial airport. Users report that they intermittently lose Wi-Fi connectivity, and troubleshooting reveals it is due to frequent channel changes. Which two actions fix this issue? (Choose two)

- **A. Remove UNII-2 and Extended UNII-2 channels from the 5 GHz channel list ✓**
- B. Enable DFS channels because they are immune to radar interference
- C. Configure channels on the UNII-2 and the Extended UNII-2 sub-bands of the 5 GHz band only
- **D. Disable DFS channels to prevent interference with Doppler radar ✓**
- E. Restore the DCA default settings because this automatically avoids channel interference

Explanation

In the 5GHz spectrum some of the channels used by 802.11 are subject to Dynamic Frequency Selection (DFS) requirements. This is due to our clients coexistence with other RF technologies such as Maritime, Aviation and Weather RADAR.

Dynamic Frequency Selection (DFS) is the process of detecting radar signals that must be protected against interference from 5.0 GHz (802.11a/h) radios, and upon detection switching the operating frequency of the 5.0 GHz (802.11a/h) radio to one that is not interfering with the radar systems.

Reference: <https://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RadioChannelDFS.pdf>

Although DFS helps reduce interference with radar systems but “DFS channels” refer to the 5GHz channels that require DFS check. In other words, DFS channels are channels that may interfere with radar signal. Therefore we should disable these DFS channels -> Answer 'Disable DFS channels to prevent interference with Doppler radar' is correct.

UNII-2 (5.250-5.350 GHz and 5.470-5.725 GHz) which contains channels 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140 are permitted in the United States, but shared with radar systems. Therefore, APs operating on UNII-2 channels are required to use Dynamic Frequency Selection (DFS) to avoid interfering with radar signals. If an AP detects a radar signal, it must immediately stop using that channel and randomly pick a new channel.

Reference: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Channel_Planning_Best_Practices

-> Therefore we should remove UNII-2 channels from 5GHz channel list.

Comments

Question 18

Which two results occur if Cisco DNA Center loses connectivity to devices in the SD-Access fabric? (Choose two)

- A. User connectivity is unaffected ✓
- B. Cisco DNA Center is unable to collect monitoring data in Assurance ✓
- C. All devices reload after detecting loss of connection to Cisco DNA Center
- D. Already connected users are unaffected, but new users cannot connect
- E. Users lose connectivity

Explanation

If you have Cisco SD-Access implemented and DNA Center becomes unreachable then the wired and wireless network will continue to forward packets as usual. There will be no impact to network performance or behavior. Yes you will be able to SSH / telnet / console into switches and wireless network infrastructure as usual. For the period DNA Center is unreachable, Assurance data will be lost, and you will not be able to make configuration changes to the Cisco SD-Access network.

Question 19

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

- A. The MAC address table is contained in CAM. ACL and QoS information is stored in TCAM ✓
- B. TCAM is used to make Layer 2 forwarding decisions. CAM is used to build routing tables
- C. The MAC address table supports partial matches. TCAM requires an exact match
- D. Router prefix lookups happen in CAM. MAC address table lookups happen in TCAM

Explanation

When using **Ternary Content Addressable Memory (TCAM)** inside routers it's used for faster address lookup that enables fast routing.

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

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

Question 20

Drag and drop the characteristics from the left onto the QoS components they describe on the right.

Note: You just need to click on one of the boxes on the right to match it with the corresponding box on the left.

applied on traffic to convey information to a downstream device	marking ✓
process used to buffer traffic that exceeds a predefined rate	shaping ✓
distinguishes traffic types	classification ✓
permits traffic to pass through the device while retaining DSCP/COS value	trust ✓

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real i



I'm not a robot

reCAPTCHA
Privacy - Terms[Submit Comment](#)[Subscribe to comments feed](#)[New ENCOR Questions – Part 5 Welcome Premium Member!](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [New ENCOR Questions- Part 5](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)

- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > NTP Quiz

NTP Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of NTP Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
4	60	90%	60	100.00%	00:08:06

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which two security features are available when implementing NTP? (Choose two)

- **A. encrypted authentication mechanism** ✓
- B. broadcast association mode
- **C. access list based restriction scheme** ✓
- D. symmetric server passwords
- E. clock offset authentication

Explanation

The time kept on a machine is a critical resource and it is strongly recommend that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. **The two security features available are an access list-based restriction scheme and an encrypted authentication mechanism.**

Reference: <https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html>

Question 2

Which two mechanisms are available to secure NTP? (Choose two)

- A. IP prefix list-based

- B. IPsec
- **C. IP access list-based** ✓
- D. TACACS-based authentication
- **E. Encrypted authentication** ✓

Explanation

The time kept on a machine is a critical resource and it is strongly recommend that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. **The two security features available are an access list-based restriction scheme and an encrypted authentication mechanism.**

Reference: <https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html>

Question 3

Why would a log file contain a * next to the date?

- A. The network device is not configured to use NTP
- B. The network device is not configured to use NTP time stamps for logging.
- **C. The network device was unable to reach the NTP server when the log messages were recorded.** ✓
- D. The network device was receiving NTP time when the log messages were recorded

Explanation

If the system clock has not been set, the date and time are preceded by an asterisk (*) to indicate that the date and time are probably not correct.

Reference: https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/service_timestamps.htm

Although there is no obvious correct answer in this question but the best answer should be “the device was unable to reach the NTP server” (and date time are probably not correct).

Question 4

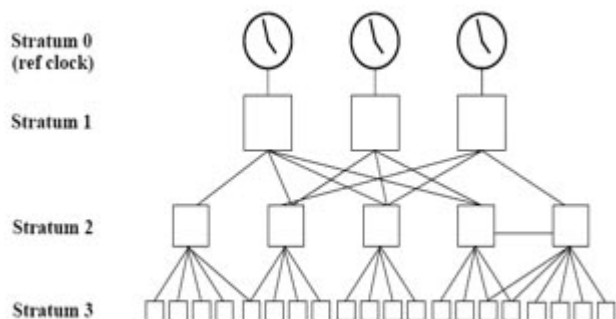
What NTP stratum level is a server that is connected directly to an authoritative time source?

- **A. Stratum 1** ✓
- B. Stratum 14
- C. Stratum 0
- D. Stratum 15

Explanation

The stratum levels define the distance from the reference clock. A reference clock is a stratum 0 device that is assumed to be accurate and has little or no delay associated with it. Stratum 0 servers cannot be used on the

network but they are directly connected to computers which then operate as stratum-1 servers. A stratum 1 time server acts as a primary network time standard.



A stratum 2 server is connected to the stratum 1 server; then a stratum 3 server is connected to the stratum 2 server and so on. A stratum 2 server gets its time via NTP packet requests from a stratum 1 server. A stratum 3 server gets its time via NTP packet requests from a stratum-2 server... A stratum server may also peer with other stratum servers at the same level to provide more stable and robust time for all devices in the peer group (for example a stratum 2 server can peer with other stratum 2 servers).

NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. **A stratum 1 time server typically has an authoritative time source** (such as a radio or atomic clock, or a Global Positioning System (GPS) time source) directly attached, a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on.

Reference: <https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/bsm/16-6-1/b-sm-xe-16-6-1-asr920/bsm-time-calendar-set.html>

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[IP SLA Quiz](#) [All Old ROUTE Links In One Page](#)

Premium Member Zone

Welcome [Ashwin Tharan!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)

- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > QoS Quiz

QoS Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of QoS Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
8	90	90%	90	100.00%	00:00:28

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which QoS mechanism will prevent a decrease in TCP performance?

- **A. WRED** ✓
- B. LLQ
- C. Policer
- D. Fair-Queue
- E. Rate-Limit
- F. Shaper

Explanation

Weighted Random Early Detection (WRED) is just a congestion avoidance mechanism. WRED drops packets selectively based on IP precedence. Edge routers assign IP precedences to packets as they enter the network. When a packet arrives, the following events occur:

1. The average queue size is calculated.
2. If the average is less than the minimum queue threshold, the arriving packet is queued.
3. If the average is between the minimum queue threshold for that type of traffic and the maximum threshold for the interface, the packet is either dropped or queued, depending on the packet drop probability for that type of traffic.
4. If the average queue size is greater than the maximum threshold, the packet is dropped.

WRED reduces the chances of tail drop (when the queue is full, the packet is dropped) by selectively dropping packets when the output interface begins to show signs of congestion (thus it can mitigate congestion by preventing the queue from filling up). By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once and minimizes the chances of global synchronization. Thus, WRED allows the transmission line to be used fully at all times.

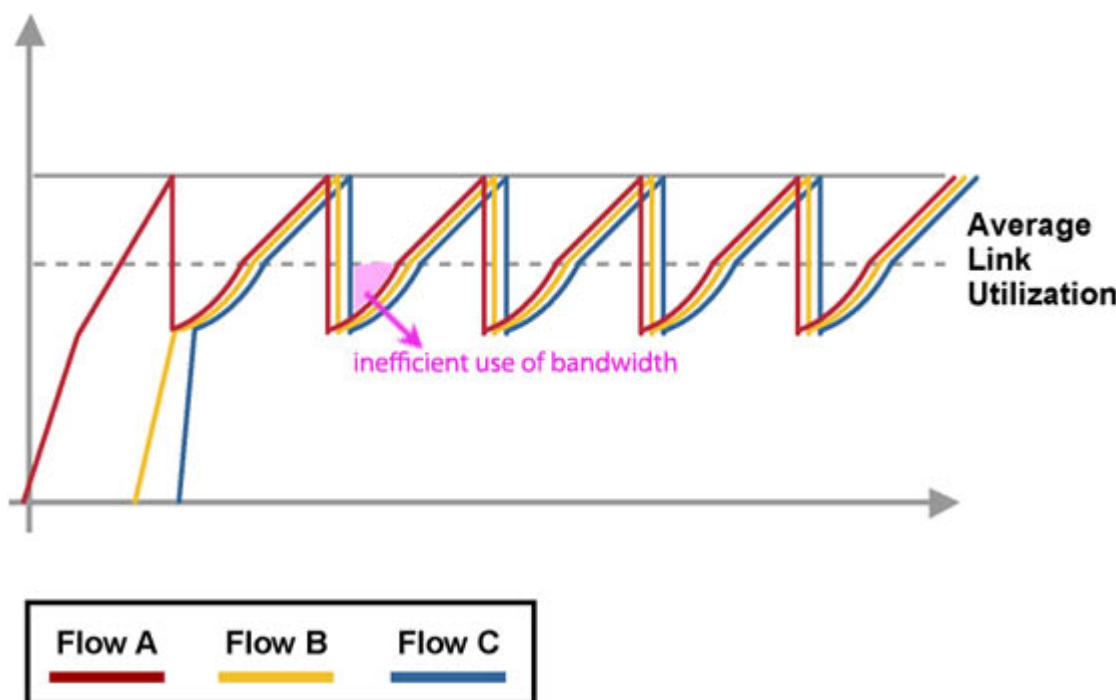
WRED generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, the higher the priority of a packet, the higher the probability that the packet will be delivered.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/15-mt/qos-conavd-15-mt-book/qos-conavd-cfg-wred.html

WRED is only useful when the bulk of the traffic is TCP/IP traffic. With TCP, dropped packets indicate congestion, so the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/xe-16/qos-conavd-xe-16-book/qos-conavd-overview.html

Note: Global synchronization occurs when multiple TCP hosts reduce their transmission rates in response to congestion. But when congestion is reduced, TCP hosts try to increase their transmission rates again simultaneously (known as slow-start algorithm), which causes another congestion. Global synchronization produces this graph:



Question 2

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

- A. Policing typically delays the traffic, rather than drops it
- **B. Policing drops traffic that exceeds the defined rate** ✓
- C. Policing adapts to network congestion by queuing excess traffic
- **D. Policing should be performed as close to the source as possible** ✓

- E. Policing should be performed as close to the destination as possible

Explanation

Traffic policing propagates bursts. When the traffic rate reaches the configured maximum rate (or committed information rate), excess traffic is dropped (or remarked). The result is an output rate that appears as a saw-tooth with crests and troughs.

Unlike traffic shaping, traffic policing does not cause delay.

Classification (which includes traffic policing, traffic shaping and queuing techniques) should take place at the network edge. It is recommended that classification occur as close to the source of the traffic as possible.

Also according to this [Cisco link](#), “policing traffic as close to the source as possible”.

Question 3

Which statement about the default QoS configuration on a Cisco switch is true?

- **A. The Port Cos value is 0** ✓
- B. All traffic is sent through four egress queues
- C. The Cos value of each tagged packet is modified
- D. Port trust is enabled

Question 4

Which QoS queuing method transmits packets out of the interface in the order the packets arrive?

- A. priority
- **B. FIFO** ✓
- C. weighted- fair
- D. custom

Explanation

First-in, first-out (FIFO): FIFO entails no concept of priority or classes of traffic. With FIFO, transmission of packets out the interface occurs in the order the packets arrive, which means no QoS.

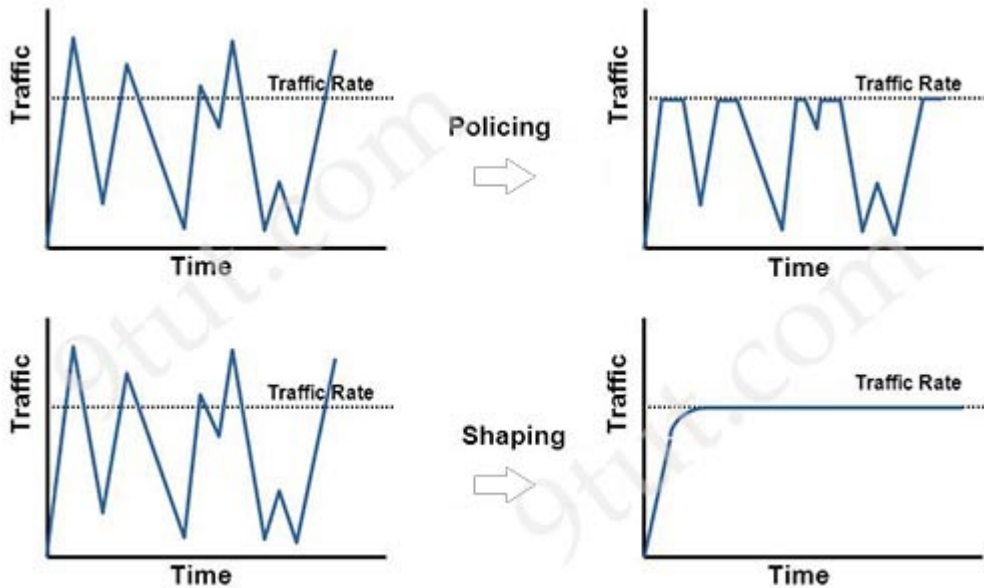
Question 5

How does QoS traffic shaping alleviate network congestion?

- A. It drops packets when traffic exceeds a certain bitrate.
- **B. It buffers and queue packets above the committed rate.** ✓
- C. It fragments large packets and queues them for delivery.
- D. It drops packets randomly from lower priority queues.

Explanation

Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate.



Question 6

Which marking field is used only as an internal marking within a router?

- A. Discard Eligibility
- **B. QOS Group** ✓
- C. IP Precedence
- D. MPLS Experimental

Explanation

Cisco routers allow you to mark two internal values (qos-group and discard-class) that travel with the packet within the router but do not modify the packet's contents.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xr-16-6/qos-mqc-xr-16-6-book/qos-mrkg.html

Question 7

During deployment, a network engineer notices that voice traffic is not being tagged correctly as it traverses the network. Which COS to DSCP map must be modified to ensure that voice traffic is treated properly?

- A. COS of 7 to DSCP 48
- B. COS of 3 to DSCP of 26
- **C. COS of 5 to DSCP 46** ✓
- D. COS of 6 to DSCP 46

Explanation

CoS value 5 is commonly used for VOIP and CoS value 5 should be mapped to DSCP 46. DSCP 46 is defined as being for EF (Expedited Forwarding) traffic flows and is the value usually assigned to all interactive voice and video traffic. This is to keep the uniformity from end-to-end that DSCP EF (mostly for VOICE RTP) is mapped to COS 5.

Note:

- + CoS is a L2 marking contained within an 802.1q tag,. The values for CoS are 0 – 7
- + DSCP is a L3 marking and has values 0 – 63
- + The default DSCP-to-CoS mapping for CoS 5 is DSCP 40

Question 8

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

- **A. Marking** ✓
- B. Classification
- C. Policing
- D. Shaping

Explanation

QoS Packet Marking refers to changing a field within a packet either at Layer 2 (802.1Q/p CoS, MPLS EXP) or Layer 3 (IP Precedence, DSCP and/or IP ECN).

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xr-16/qos-mqc-xr-16-book/qos-mrkg.html

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[Switching Mechanism Quiz](#) [SD-WAN & SD-Access Solutions Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)

- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > SD-WAN & SD-Access Solutions 2 Quiz

SD-WAN & SD-Access Solutions 2 Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of SD-WAN & SD-Access Solutions 2 Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
10	100	90%	100	100.00%	00:01:28

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

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

- **A. LISP** ✓
- B. SXP
- C. VXLAN
-
- D. DHCP

Question 2

In an SD-WAN deployment, which action in the vSmart controller responsible for?

- A. handle, maintain, and gather configuration and status for nodes within the SD-WAN fabric
- B. gather telemetry data from vEdge routers
- **C. distribute policies that govern data forwarding performed within the SD-WAN fabric** ✓
- D. onboard vEdge nodes into the SD-WAN fabric

Explanation

Control plane (vSmart) builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, implements control plane policies and distributes data plane policies to network devices for enforcement.

Question 3

In a Cisco SD-WAN solution, how is the health of a data plane tunnel monitored?

- A. with OMP
- B. ARP probing
- C. with IP SLA
- **D. using BFD** ✓

Explanation

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

Question 4

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

- **A. The access point is part the fabric overlay** ✓
- B. The access point is part of the fabric underlay
- C. The WLC is part of the fabric underlay
- D. The wireless client is part of the fabric overlay

Explanation

Access Points

- + AP is directly connected to FE (or to an extended node switch)
- + AP is part of Fabric overlay

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

Question 5

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

- **A. It holds a comprehensive database that tracks endpoints and networks in the fabric.** ✓
- B. It provides integration with legacy nonfabric-enabled environments.
- C. It performs traffic encapsulation and security profiles enforcement in the fabric.
- D. It is responsible for policy application and network segmentation in the fabric.

Explanation

Fabric control plane node (C): One or more network elements that implement the LISP Map-Server (MS) and Map-Resolver (MR) functionality. The control plane node's host tracking database keep track of all endpoints in a fabric site and associates the endpoints to fabric nodes in what is known as an EID-to-RLOC binding in LISP.

Reference: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-macro-segmentation-deploy-guide.html>

Question 6

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

- A. VPN routing/forwarding
- **B. overlay network** ✓
- C. underlay network
- D. easy virtual network

Explanation

An overlay network creates a logical topology used to virtually connect devices that are built over an arbitrary physical underlay topology.

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

SD-Access allows for the extension of Layer 2 and Layer 3 connectivity across the overlay through the services provided by through LISP.

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

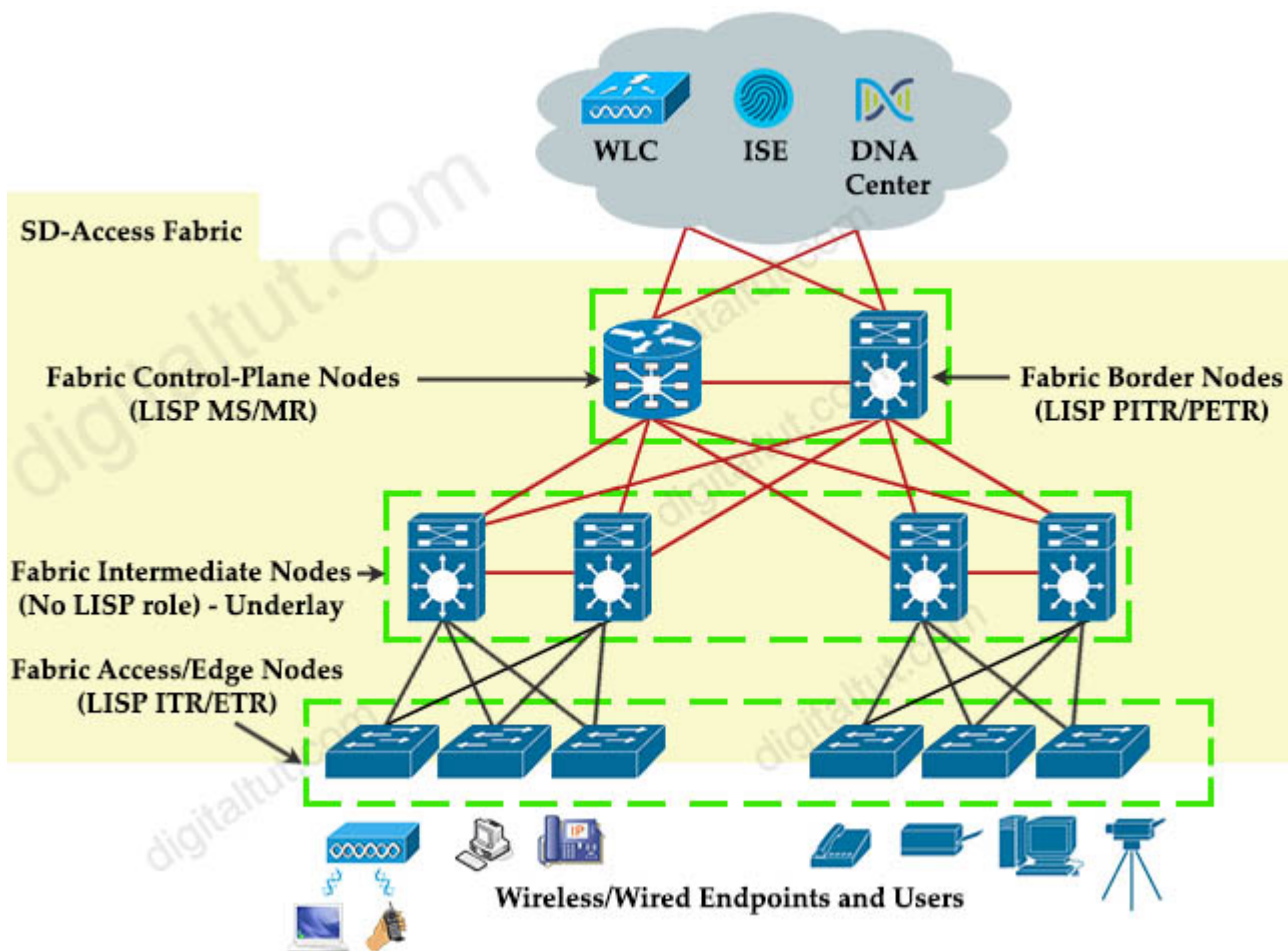
Question 7

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

- A. to connect the fusion router to the SD-Access fabric
- **B. to connect wired endpoint to the SD-Access fabric** ✓
- C. to advertise fabric IP address space to external network
- D. to connect external Layer 3- network to the SD-Access fabric

Explanation

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



Question 8

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

- A. vSmart
- B. vEdge
- C. vBond ✓
- D. vManage

Explanation

+ **Orchestration plane (vBond)** assists in securely onboarding the SD-WAN WAN Edge routers into the SD-WAN overlay. The vBond controller, or orchestrator, authenticates and authorizes the SD-WAN components onto the network. The vBond orchestrator takes an added responsibility to distribute the list of vSmart and vManage controller information to the WAN Edge routers. vBond is the only device in SD-WAN that requires a public IP address as it is the first point of contact and authentication for all SD-WAN components to join the SD-WAN fabric. All other components need to know the vBond IP or DNS information.

Question 9

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

- A. IT performs authentication and authorization

- B. It is the centralized network management system.
- C. It manages the data plane.
- **D. It manages the control plane.** ✓

Explanation

+ **Control plane (vSmart)** builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, implements control plane policies and distributes data plane policies to network devices for enforcement.

Question 10

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

- A. fabric border node
- **B. fabric control plane node** ✓
- C. fabric edge node
- D. fabric wireless controller

Explanation

SD-Access Wireless Architecture Control Plane Node –A Closer Look

Fabric Control-Plane Node is based on a LISP Map Server / Resolver

Runs the LISP Endpoint ID Database to provide overlay reachability information

- + A simple Host Database, that tracks Endpoint ID to Edge Node bindings (RLOCs)
- + Host Database supports multiple types of Endpoint ID (EID), such as IPv4 /32, IPv6 /128* or MAC/48
- + Receives prefix registrations from Edge Nodes for wired clients, and from Fabric mode WLCs for wireless clients
- + Resolves lookup requests from FE to locate Endpoints
- + Updates Fabric Edge nodes, Border nodes with wireless client mobility and RLOC information

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/latam/docs/2018/pdf/BRKEWN-2020.pdf>

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms[Subscribe to comments feed](#)[DNA Center Quiz](#) [Virtualization 2 Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)

- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > SD-WAN & SD-Access Solutions 3 Quiz

SD-WAN & SD-Access Solutions 3 Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of SD-WAN & SD-Access Solutions 3 Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
4	40	90%	40	100.00%	00:21:15

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

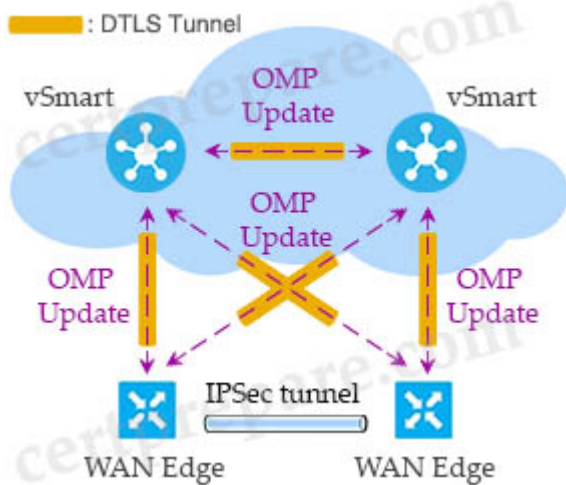
Question 1

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

- A. UDP
- **B. OMP** ✓
- C. BGP
- D. TCP

Explanation

Cisco SD-WAN uses Overlay Management Protocol (OMP) which manages the overlay network. OMP runs between the vSmart controllers and WAN Edge routers (and among vSmarts themselves) where control plane information, such as the routing, policy, and management information, is exchanged over a secure connection.



Question 2

Which tunneling technique is used when designing a Cisco SD-Access fabric data plane?

- A. LISP
- **B. VXLAN** ✓
- C. VRF
- D. VRF Lite

Explanation

The tunneling technology used for the fabric data plane is based on Virtual Extensible LAN (VXLAN). VXLAN encapsulation is UDP based, meaning that it can be forwarded by any IP-based network (legacy or third party) and creates the overlay network for the SD-Access fabric. Although LISP is the control plane for the SD-Access fabric, it does not use LISP data encapsulation for the data plane; instead, it uses VXLAN encapsulation because it is capable of encapsulating the original Ethernet header to perform MAC-in-IP encapsulation, while LISP does not. Using VXLAN allows the SD-Access fabric to support Layer 2 and Layer 3 virtual topologies (overlays) and the ability to operate over any IP-based network with built-in network segmentation (VRF instance/VN) and built-in group-based policy.

Reference: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

Question 3

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

- A. inter-xTR
- B. auto anchor
- C. Layer 3
- **D. fast roam** ✓

Question 4

Which protocol is responsible for data plane forwarding in a Cisco SD-Access deployment?

- A. IS-IS
- B. LISP
- C. OSPF
- **D. VXLAN** ✓

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real i



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[Access-list 2 Quiz](#) [NetFlow Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)

- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)

- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > SD-WAN & SD-Access Solutions Quiz

SD-WAN & SD-Access Solutions Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of SD-WAN & SD-Access Solutions Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
10	110	90%	110	100.00%	00:01:31

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

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

- A. vBond
- B. vSmart
- **C. vManage** ✓
- D. vEdge

Explanation

The primary components for the Cisco SD-WAN solution consist of the **vManage network management system (management plane)**, the vSmart controller (control plane), the vBond orchestrator (orchestration plane), and the vEdge router (data plane).

+ vManage – This centralized network management system provides a GUI interface to easily monitor, configure, and maintain all Cisco SD-WAN devices and links in the underlay and overlay network.

+ vSmart controller – This software-based component is responsible for the centralized control plane of the SD-WAN network. It establishes a secure connection to each vEdge router and distributes routes and policy information via the Overlay Management Protocol (OMP), acting as a route reflector. It also orchestrates the secure data plane connectivity between the vEdge routers by distributing crypto key information, allowing for a very scalable, IKE-less architecture.

+ vBond orchestrator – This software-based component performs the initial authentication of vEdge devices and orchestrates vSmart and vEdge connectivity. It also has an important role in enabling the communication of devices that sit behind Network Address Translation (NAT).

+ vEdge router – This device, available as either a hardware appliance or software-based router, sits at a physical site or in the cloud and provides secure data plane connectivity among the sites over one or more WAN transports. It is responsible for traffic forwarding, security, encryption, Quality of Service (QoS), routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), and more.

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

Question 2

Which description of an SD-Access wireless network infrastructure deployment is true?

- A. The WLC is part of the fabric underlay
- **B. The access point is part the fabric overlay** ✓
- C. The access point is part of the fabric underlay
- D. The wireless client is part of the fabric overlay

Explanation

Access Points

- + AP is directly connected to FE (or to an extended node switch)
- + AP is part of Fabric overlay

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

Question 3

On which protocol or technology is the fabric data plane based in Cisco SD-Access fabric?

- **A. VXLAN** ✓
- B. LISP
- C. Cisco TrustSec
- D. IS-IS

Explanation

The tunneling technology used for the fabric data plane is based on Virtual Extensible LAN (VXLAN). VXLAN encapsulation is UDP based, meaning that it can be forwarded by any IP-based network (legacy or third party) and creates the overlay network for the SD-Access fabric. Although LISP is the control plane for the SD-Access fabric, it does not use LISP data encapsulation for the data plane; instead, it uses VXLAN encapsulation because it is capable of encapsulating the original Ethernet header to perform MAC-in-IP encapsulation, while LISP does not. Using VXLAN allows the SD-Access fabric to support Layer 2 and Layer 3 virtual topologies (overlays) and the ability to operate over any IP-based network with built-in network segmentation (VRF instance/VN) and built-in group-based policy.

Reference: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

Question 4

Which statement about a fabric access point is true?

- A. It is in FlexConnect mode and must be connected directly to the fabric edge switch
- **B. It is in local mode and must be connected directly to the fabric edge switch** ✓
- C. It is in FlexConnect mode and must be connected directly to the fabric border node
- D. It is in local mode and must be connected directly to the fabric border node

Explanation

Fabric mode APs continue to support the same wireless media services that traditional APs support; apply AVC, quality of service (QoS), and other wireless policies; and establish the CAPWAP control plane to the fabric WLC. **Fabric APs join as local-mode APs and must be directly connected to the fabric edge node switch** to enable fabric registration events, including RLOC assignment via the fabric WLC. The fabric edge nodes use CDP to recognize APs as special wired hosts, applying special port configurations and assigning the APs to a unique overlay network within a common EID space across a fabric. The assignment allows management simplification by using a single subnet to cover the AP infrastructure at a fabric site.

Reference: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.html>

Question 5

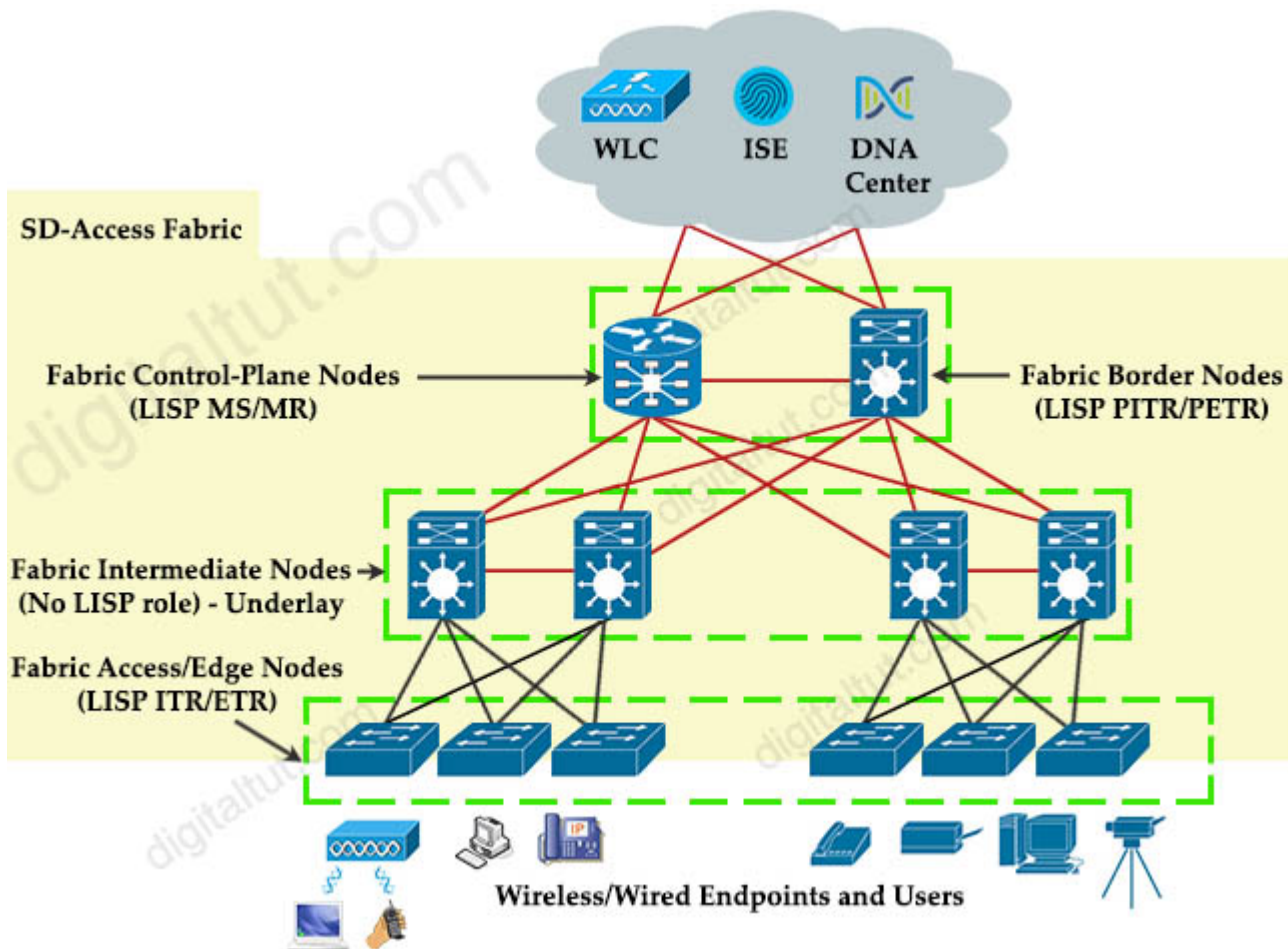
What are two device roles in Cisco SD-Access fabric? (Choose two)

- A. vBond controller
- **B. edge node** ✓
- C. access switch
- D. core switch
- **E. border node** ✓

Explanation

There are five basic device roles in the fabric overlay:

- + Control plane node: This node contains the settings, protocols, and mapping tables to provide the endpoint-to-location (EID-to-RLOC) mapping system for the fabric overlay.
- + **Fabric border node**: This fabric device (for example, core layer device) connects external Layer 3 networks to the SDA fabric.
- + **Fabric edge node**: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.
- + Fabric WLAN controller (WLC): This fabric device connects APs and wireless endpoints to the SDA fabric.
- + Intermediate nodes: These are intermediate routers or extended switches that do not provide any sort of SD-Access fabric role other than underlay services.



Reference: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

Question 6

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

- A. onboard vEdge nodes into the SD-WAN fabric
- B. gather telemetry data from vEdge routers
- C. manage, maintain, and gather configuration and status for nodes within the SD-WAN fabric
- **D. distribute security information for tunnel establishment between vEdge routers** ✓

Explanation

+ **Orchestration plane** (vBond) assists in securely onboarding the SD-WAN WAN Edge routers into the SD-WAN overlay (-> Therefore answer "onboard vEdge nodes into the SD-WAN fabric" mentioned about vBond). The vBond controller, or orchestrator, authenticates and authorizes the SD-WAN components onto the network. The vBond orchestrator takes an added responsibility to distribute the list of vSmart and vManage controller information to the WAN Edge routers. vBond is the only device in SD-WAN that requires a public IP address as it is the first point of contact and authentication for all SD-WAN components to join the SD-WAN fabric. All other components need to know the vBond IP or DNS information.

+ **Management plane** (vManage) is responsible for central configuration and monitoring. The vManage controller is the centralized network management system that provides a single pane of glass GUI interface to easily deploy, configure, monitor and troubleshoot all Cisco SD-WAN components in the network. (-> Answer

"manage, maintain, and gather configuration and status for nodes within the SD-WAN fabric" and answer "gather telemetry data from vEdge routers" are about vManage)

+ **Control plane** (vSmart) builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, implements control plane policies and distributes data plane policies to network devices for enforcement (-> Answer "distribute security information for tunnel establishment between vEdge routers" is about vSmart)

Question 7

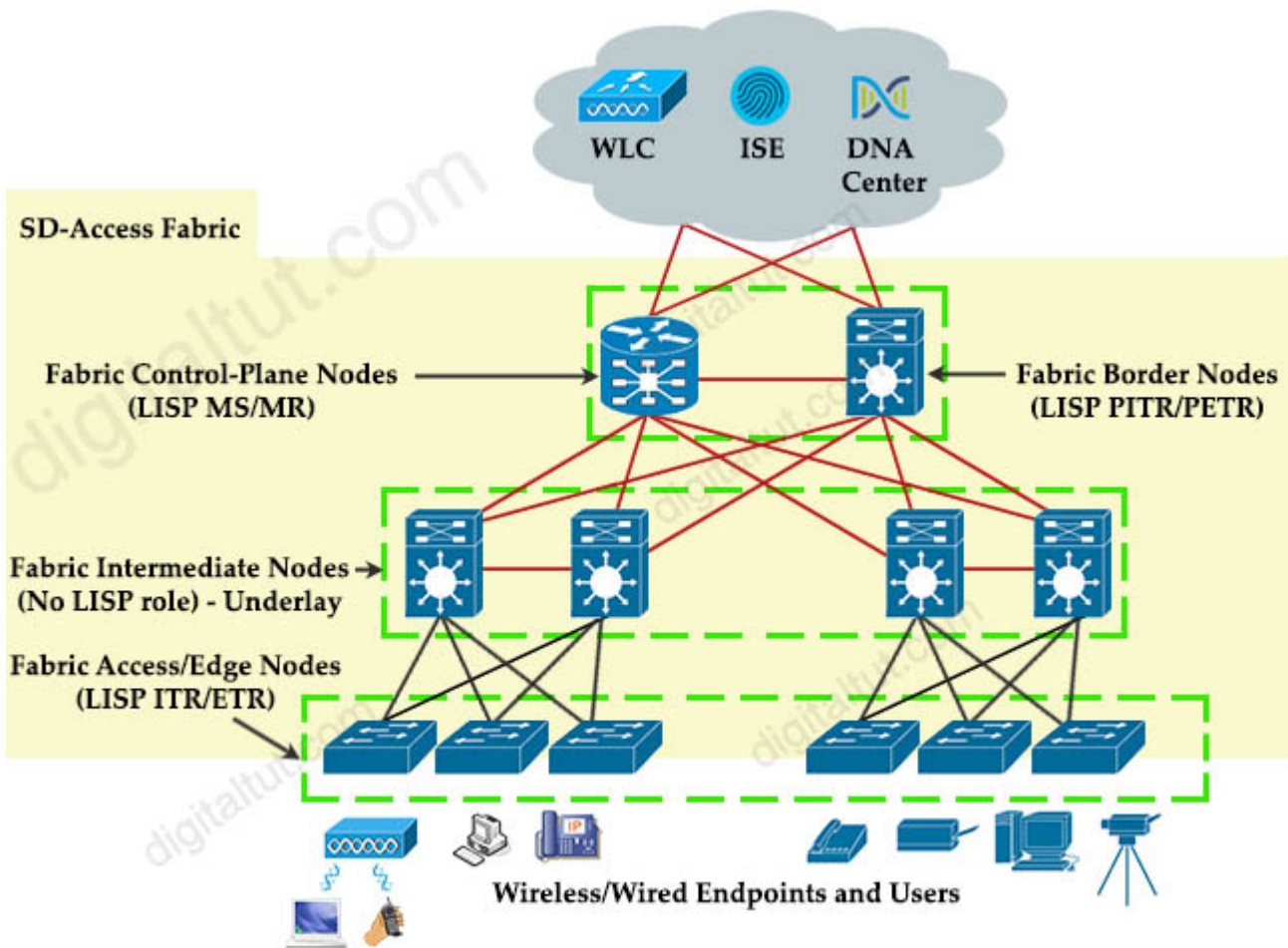
Which function does a fabric edge node perform in an SD-Access deployment?

- A. Connects the SD-Access fabric to another fabric or external Layer 3 networks
- **B. Connects endpoints to the fabric and forwards their traffic** ✓
- C. Encapsulates end-user data traffic into LISP.
-
- D. Provides reachability border nodes in the fabric underlay

Explanation

There are five basic device roles in the fabric overlay:

- + Control plane node: This node contains the settings, protocols, and mapping tables to provide the endpoint-to-location (EID-to-RLOC) mapping system for the fabric overlay.
- + Fabric border node: This fabric device (for example, core layer device) connects external Layer 3 networks to the SDA fabric.
- + Fabric edge node: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.
- + Fabric WLAN controller (WLC): This fabric device connects APs and wireless endpoints to the SDA fabric.
- + Intermediate nodes: These are intermediate routers or extended switches that do not provide any sort of SD-Access fabric role other than underlay services.



Reference: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

Question 8

Which statement about a Cisco APIC controller versus a more traditional SDN controller is true?

- **A. APIC uses a policy agent to translate policies into instructions** ✓
- B. APIC does support a Southbound REST API
- C. APIC uses an imperative model
- D. APIC supports OpFlex as a Northbound protocol

Explanation

The southbound protocol used by APIC is OpFlex that is pushed by Cisco as the protocol for policy enablement across physical and virtual switches.

Southbound interfaces are implemented with some called Service Abstraction Layer (SAL), which talks to the network elements via SNMP and CLI.

Note: Cisco OpFlex is a southbound protocol in a software-defined network (SDN).

Question 9

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

- A. control-plane node
- B. RADIUS server
- **C. Identity Service Engine** ✓
- D. edge node

Question 10

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

- **A. performs route leaking between user-defined virtual networks and shared services** ✓
- B. provides connectivity to external networks
- C. acts as a DNS server
- D. provides additional forwarding capacity to the fabric

Explanation

Today the Dynamic Network Architecture Software Defined Access (DNA-SDA) solution requires a fusion router to perform VRF route leaking between user VRFs and Shared-Services, which may be in the Global routing table (GRT) or another VRF. Shared Services may consist of DHCP, Domain Name System (DNS), Network Time Protocol (NTP), Wireless LAN Controller (WLC), Identity Services Engine (ISE), DNAC components which must be made available to other virtual networks (VN's) in the Campus.

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

Comments

1. xcalliber
August 24th, 2020

How much SDwan is there in thi exam

2. advan
December 6th, 2020

there is an inconsistency for the answer

<https://pict.com/images/2020/12/06/7feN3l.png>

3. advan
December 6th, 2020

ok my mistake, ignore prev comment

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms[Subscribe to comments feed](#)[QoS Quiz](#) [Trunking Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)

- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)

- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Security Quiz

Security Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Security Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
11	110	90%	110	100.00%	00:00:48

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

An engineer must protect their company against ransom ware attacks. Which solution allows the engineer to block the execution stage and prevent file encryption?

- A. Use Cisco Firepower with Intrusion Policy and snort rules blocking SMB exploitation
- **B. Use Cisco AMP deployment with the Malicious Activity Protection engine enabled** ✓
- C. Use Cisco AMP deployment with the Exploit Prevention engine enabled
- D. Use Cisco Firepower and block traffic to TOR networks

Explanation

Ransomware are malicious software that locks up critical resources of the users. Ransomware uses well-established public/private key cryptography which leaves the only way of recovering the files being the payment of the ransom, or restoring files from backups.

Cisco Advanced Malware Protection (AMP) for Endpoints Malicious Activity Protection (MAP) engine defends your endpoints by monitoring the system and identifying processes that exhibit malicious activities when they execute and stops them from running. Because the MAP engine detects threats by observing the behavior of the process at run time, it can generically determine if a system is under attack by a new variant of ransomware or malware that may have eluded other security products and detection technology, such as legacy signature-based malware detection. The first release of the MAP engine targets identification, blocking, and quarantine of ransomware attacks on the endpoint.

Reference: <https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.pdf>

Question 2

Which feature does Cisco TrustSec use to provide scalable, secure communication throughout a network?

- A. security group tag number assigned to each user on a switch
- **B. security group tag number assigned to each port on a network** ✓
- C. security group tag ACL assigned to each port on a switch
- D. security group tag ACL assigned to each router on a network

Explanation

Cisco TrustSec uses tags to represent logical group privilege. This tag, called a Security Group Tag (SGT), is used in access policies. The SGT is understood and is used to enforce traffic by Cisco switches, routers and firewalls. Cisco TrustSec is defined in three phases: classification, propagation and enforcement.

When users and devices connect to a network, the network assigns a specific security group. This process is called classification. Classification can be based on the **results of the authentication or by associating the SGT with an IP, VLAN, or port-profile** (-> Answer 'security group tag ACL assigned to each port on a switch' and answer 'security group tag number assigned to each user on a switch' are not correct as they say “assigned ... on a switch” only. Answer 'security group tag ACL assigned to each router on a network' is not correct either as it says “assigned to each router”).

Question 3

Refer to the exhibit.



An engineer is designing a guest portal on Cisco ISE using the default configuration. During the testing phase, the engineer receives a warning when displaying the guest portal. Which issue is occurring?

- A. The connection is using an unsupported protocol
- **B. The server that is providing the portal has a self-signed certificate** ✓
- C. The connection is using an unsupported browser
- D. The server that is providing the portal has an expired certificate

Explanation

If you're a website owner and your website displays this error message, then there could be two reasons why the browser says the cert authority is invalid:

- + You're using a self-signed SSL certificate, OR
- + The certificate authority (CA) that issued your SSL certificate isn't trusted by your web browser.

Question 4

Which technology provides a secure communication channel for all traffic at Layer 2 of the OSI model?

- A. IPsec
- **B. MACsec** ✓
- C. SSL
- D. Cisco Trustsec

Explanation

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.

A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the MKA peer. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the MKA peer, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The switch compares that ICV to the ICV within the frame. If they are not identical, the frame is dropped. The switch also encrypts and adds an ICV to any frames sent over the secured port (the access point used to provide the secure MAC service to a MKA peer) using the current session key.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/sec/b_169_sec_9300_cg/macsec_encryption.html

Note: Cisco Trustsec is the solution which includes MACsec.

Question 5

Refer to the exhibit.

```
Router#sh run | b vty
```

```
line vty 0 4
  session-timeout 30
  exec-timeout 20 0
  session-limit 30
  login local
line vty 5 15
  session-timeout 30
  exec-timeout 20 0
  session-limit 30
  login local
```

Security policy requires all idle-exec sessions to be terminated in 600 seconds. Which configuration achieves this goal?

- A. line vty 0 15
 - absolute-timeout 600
- B. line vty 0 15
 - exec-timeout
- C. line vty 0 15
 - exec-timeout 10 0 
- D. line vty 0 4
 - exec-timeout 600

Explanation

The “exec-timeout” command is used to configure the inactive session timeout on the console port or the virtual terminal. The syntax of this command is:

exec-timeout *minutes [seconds]*

Therefore we need to use the “exec-timeout 10 0” command to set the user inactivity timer to 600 seconds (10 minutes).

Question 6

Which method does the enable secret password option use to encrypt device passwords?

- **A. MD5** ✓
- B. PAP
- C. AES
- D. CHAP

Question 7

Which NGFW mode block flows crossing the firewall?

- A. Passive
- B. Tap
- **C. Inline** ✓
- D. Inline tap

Explanation

Firepower Threat Defense (FTD) provides six interface modes which are: Routed, Switched, Inline Pair, Inline Pair with Tap, Passive, Passive (ERSPAN).

When Inline Pair Mode is in use, packets can be blocked since they are processed inline

When you use Inline Pair mode, the packet goes mainly through the FTD Snort engine

When Tap Mode is enabled, a copy of the packet is inspected and dropped internally while the actual traffic goes through FTD unmodified

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html>

Question 8

What is the difference between the enable password and the enable secret password when password encryption is enable on an IOS device?

- A. There is no difference and both passwords are encrypted identically
- B. The enable password cannot be decrypted
- **C. The enable secret password is protected via stronger cryptography mechanisms** ✓
- D. The enable password is encrypted with a stronger encryption method

Explanation

The “enable secret” password is always encrypted (independent of the “service password-encryption” command) using MD5 hash algorithm. The “enable password” does not encrypt the password and can be view in clear text in the running-config. In order to encrypt the “enable password”, use the “service password-encryption” command. This command will encrypt the passwords by using the Vigenere encryption algorithm. Unfortunately, the Vigenere encryption method is cryptographically weak and trivial to reverse.

The MD5 hash is a stronger algorithm than Vigenere so answer 'The enable secret password is protected via stronger cryptography mechanisms' is correct.

Question 9

Refer to the exhibit. Which privilege level is assigned to VTY users?

```
R1# sh run | begin line con
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stoppbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stoppbits 1
line vty 0 4
  password 7 03384737389E938
  login
line vty 5 15
  password 7 03384737389E938
  login
!
end

R1#sh run | include aaa | enable
no aaa new-model
R1#
```

- A. 1 
- B. 7
- C. 13
- D. 15

Explanation

Lines (CON, AUX, VTY) default to level 1 privileges.

Question 10

How does Cisco Trustsec enable more access controls for dynamic networking environments and data centers?

- A. classifies traffic based on advanced application recognition
- B. uses flexible NetFlow
- C. assigns a VLAN to the endpoint
- D. classifies traffic based on the contextual identity of the endpoint rather than its IP address 

Explanation

The Cisco TrustSec solution simplifies the provisioning and management of network access control through the use of software-defined segmentation to classify network traffic and enforce policies for more flexible access controls. **Traffic classification is based on endpoint identity, not IP address**, enabling policy change without net-work redesign.

Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Apr2016/User-to-DC_Access_Control_Using_TrustSec_Deployment_April2016.pdf

Question 11

Which deployment option of Cisco NGFW provides scalability?

- **A. clustering** ✓
- B. high availability
- C. tap
- D. inline tap

Explanation

Clustering lets you group multiple Firepower Threat Defense (FTD) units together as a single logical device. Clustering is only supported for the FTD device on the Firepower 9300 and the Firepower 4100 series. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the **increased throughput and redundancy** of multiple devices.

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real i



I'm not a robot

reCAPTCHA
[Privacy](#) - [Terms](#)

Submit Comment

[Subscribe to comments feed](#)

[Access-list Quiz](#) [Network Assurance Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)

- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > SPAN Quiz

SPAN Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of SPAN Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
6	60	90%	60	100.00%	00:01:31

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit.

```
monitor session 1 source vlan 10 -12 rx  
monitor session 1 destination interface gigabitethernet0/1
```

An engineer must configure a SPAN session. What is the effect of the configuration?

- A. Traffic received on VLANs 10 and 12 only is copied and sent to interface g0/1.
- B. Traffic sent on VLANs 10 and 12 only is copied and sent to interface g0/1.
- C. Traffic sent on VLANs 10, 11, and 12 is copied and sent to interface g0/1.
- **D. Traffic received on VLANs 10, 11, and 12 is copied and sent to interface g0/1. ✓**

Question 2

Which statement about an RSPAN session configuration is true?

- A. Only one session can be configured at a time
- B. Only incoming traffic can be monitored
- C. A filter must be configured for RSPAN Regions
- **D. A special VLAN type must be used as the RSPAN destination. ✓**

Explanation

The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches -> This VLAN can be considered a special VLAN type -> Answer 'A special VLAN type must be used as the RSPAN destination' is correct.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html

We can configure multiple RSPAN sessions on a switch at a time, then continue configuring multiple RSPAN sessions on the other switch without any problem -> Answer 'Only one session can be configured at a time' is not correct.

This is how to configure Remote SPAN (RSPAN) feature on two switches. Traffic on FastEthernet0/1 of Switch 1 will be sent to Fa0/10 of Switch2 via VLAN 40.

+ Configure on both switches

Switch1,2(config)#vlan 40

Switch1,2(config-vlan)#remote-span

+ Configure on Switch1

Switch1(config)# monitor session 1 source interface FastEthernet 0/1

Switch1(config)# monitor session 1 destination remote vlan 40

+ Configure on Switch2

Switch2(config)#monitor session 5 source remote vlan 40

Switch2(config)# monitor session 5 destination interface FastEthernet 0/10

Question 3

Refer to the exhibit.

```
vlan 222
  remote-span
!
vlan 223
  remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

What is the result when a technician adds the monitor session 1 destination remote vlan 223 command?

- A. RSPAN traffic is split between VLANs 222 and 223
- B. RSPAN traffic is sent to VLANs 222 and 223
- C. An error is flagged for configuring two destinations
- **D. The RSPAN VLAN is replaced by VLAN 223** ✓

Question 4

Which feature must be configured to allow packet capture over Layer 3 infrastructure?

- A. RSPAN
- **B. ERSPAN** ✓
- C. IPSPAN
- D. VSPAN

Explanation

Encapsulated remote SPAN (ERSPAN): encapsulated Remote SPAN (ERSPAN), as the name says, brings generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains.

Question 5

Refer to the exhibit.

```
SW1#show monitor session all
Session 1
-----
Type                : Remote Destination Session
Source RSPAN VLAN   : 50

Session 2
-----
Type                : Local Session
Source Ports        :
  Both              : Fa0/14
Destination Ports   : Fa0/15
Encapsulation       : Native
Ingress             : Disabled
```

An engineer configures monitoring on SW1 and enters the show command to verify operation. What does the output confirm?

- A. SPAN session 2 only monitors egress traffic exiting port FastEthernet 0/14.
- B. SPAN session 1 monitors activity on VLAN 50 of a remote switch
- **C. RSPAN session 1 is incompletely configured for monitoring** ✓
- D. SPAN session 2 monitors all traffic entering and exiting port FastEthernet 0/15.

Explanation

SW1 has been configured with the following commands:

```
SW1(config)#monitor session 1 source remote vlan 50
SW1(config)#monitor session 2 source interface fa0/14
SW1(config)#monitor session 2 destination interface fa0/15
```

The session 1 on SW1 was configured for Remote SPAN (RSPAN) while session 2 was configured for local SPAN. For RSPAN we need to configure the destination port to complete the configuration.

Note: In fact we cannot create such a session like session 1 because if we only configure “Source RSPAN VLAN 50” (with the command “monitor session 1 source remote vlan 50”) then we will receive a “Type: Remote Source Session” (not “Remote Destination Session”).

Question 6

Refer to the exhibit.

```
vlan 222
  remote-span
!
vlan 223
  remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
```

These commands have been added to the configuration of a switch. Which command flags an error if it is added to this configuration?

- **A. monitor session 1 source vlan 10** ✓
- B. monitor session 1 source interface port-channel 6
- C. monitor session 1 source interface port-channel 7, port-channel 8
- D. monitor session 1 source interface FastEthernet0/1 rx

Explanation

RSPAN consists of at least one RSPAN source session, an RSPAN VLAN, and at least one RSPAN destination session. You separately configure RSPAN source sessions and RSPAN destination sessions on different network devices. To configure an RSPAN source session on a device, **you associate a set of source ports or source VLANs** with an RSPAN VLAN.

Traffic monitoring in a SPAN session has these restrictions:

+ Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html

Therefore in this question, we cannot configure a source VLAN because we configured source ports for RSPAN session 1 already.

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real !)



I'm not a robot

reCAPTCHA
Privacy - Terms[Submit Comment](#)[Subscribe to comments feed](#)[Troubleshooting Quiz HSRP & VRRP 2 Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)

- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > STP Quiz

STP Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of STP Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
8	90	90%	90	100.00%	00:01:21

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit. Which two commands ensure that DSW1 becomes root bridge for VLAN 10 and 20? (Choose two)

DSW1#show spanning-tree

MST1

Spanning tree enabled protocol mstp

Root ID Priority 32769
 Address 0018.7363.4300
 Cost 2
 Port 13 (FastEthernet1/0/11)
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id- ext 1)
 Address 001b.0d8e.e080
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa1/0/7	Desg FWD	2	128.1	P2p Bound (PVST)	
Fa1/0/10	Desg FWD	2	128.12	P2p Bound (PVST)	
Fa1/0/11	Root FWD	2	128.13	P2p	
Fa1/0/12	Altn BLK	2	128.14	P2p	

DSW1#show spanning-tree mst

```
##### MST1
Bridge      vlans mapped: 10,20
Root        address 001b.0d0e.e000 priority 32769 (32768 sysid 1)
            address 0018.7363.4300 priority 32769 (32768 sysid 1)
            port    Fa1/0/11      cost    2      (rem hops 19)
```

----- output omitted -----

- A. spanning-tree mstp 1 priority 0
- **B. spanning-tree mst 1 root primary** ✓
- C. spanning-tree mst 1 priority 1
- D. spanning-tree mstp vlan 10,20 root primary
- E. spanning-tree mst vlan 10,20 priority root
- **F. spanning-tree mst 1 priority 4096** ✓

Explanation

From the second command output (show spanning-tree mst) we learn that MST1 includes VLANs 10 & 20. Therefore if we want DSW1 to become root bridge for these VLANs we need to set the MST 1 region to root -> The command "spanning-tree mst 1 root primary" can do the trick. In fact, this command runs a macro and sets the priority lower than the current root.

Also we can see the current root bridge for these VLANs has the priority of 32769 (default value + sysid) so we can set the priority of DSW1 to a specific lower value. But notice that the priority must be a multiple of 4096. Therefore D is a correct answer.

Question 2

Refer to the exhibit.


```
DSW2#sh spanning-tree vlan 10
```

```
VLAN0010
```

```
Spanning tree enabled protocol ieee
```

```
Root ID      Priority    10
             Address    0018.7363.4300
             Cost        2
             Port        9 (FastEthernet1/0/7)
             Hello Time 2 sec Max Age 20 sec
             Forward Delay 15 sec
```

```
Bridge ID Priority 4106 (priority 4096 sys-id-ext 10)
```

```
Address 001b.0d8e.e080
Hello Time 2 sec Max Age 20 sec
Forward Delay 15 sec
Aging Time 300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa1/0/7	Root	FWD	2	128.9	P2p
Fa1/0/10	Desg	FWD	4	128.12	P2p
Fa1/0/11	Desg	FWD	2	128.13	P2p
Fa1/0/12	Desg	FWD	2	128.14	P2p

```
DSW2#
```

```
*Mar 3 09:33:23.234: #SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/7 with BPDU Guard enabled. Disabling port.
```

```
*Mar 3 09:33:23.234: %PM-4-ERR_DISABLE: bpduguard error detected on Fa1/0/7, putting Fa1/0/7 in err-disable state
```

```
*Mar 3 09:33:23.678: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/7 with BPDU Guard enabled. Disabling port.
```

```
*Mar 3 09:33:23.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/7, changed state to down
```

```
*Mar 3 09:33:23.701: %LINK-3-UPDOWN: Interface FastEthernet1/0/7, changed state to down
```

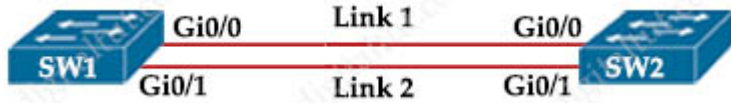
An engineer entered the `no spanning-tree bpduguard enable` on interface `fa1/0/7` command. Which statement describes the effect of this command?

- A. Interface Fa1/0/7 remains in err-disabled state until the `errdisable recovery cause bpduguard` command is entered in the interface configuration mode
- **B. Fa1/0/7 remains in err-disabled state until the shutdown/no shutdown command is entered in the interface configuration mode** ✓
- C. Fa1/0/7 remains in err-disabled state until the `errdisable recovery bpduguard` command is entered in the interface configuration mode
- D. Interface Fa1/0/7 returns to an up and operational state
- E. Interface Fa1/0/7 remains in err-disabled state until the `spanning-tree portfast bpduguard disable` command is entered in the interface configuration mode

Question 3

Refer to the exhibit. Link1 is a copper connection and Link2 is a fiber connection. The fiber port must be the primary port for all forwarding. The output of the `show spanning-tree` command on SW2 shows that the fiber port is blocked by spanning tree. An engineer enters the `spanning-tree port-priority 32`

command on G0/1 on SW2, but the port remains blocked.



```
SW2#show spanning-tree
```

```
VLAN0010
```

```
Spanning tree enabled protocol ieee
```

```
Root ID      Priority    24596
```

```
Address      0018.7363.4300
```

```
Cost         2
```

```
Port         13 (GigabitEthernet0/0)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID    Priority 28692 (priority 28672 sys-id-ext 20)
```

```
Address      001b.0d8e.e080
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Aging Time 300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	----	----	-----	----
Gi0/0	Root	FWD	4	128.1	P2p
Gi0/1	Atln	BLK	4	32.2	P2p

Which command should be entered on the ports that are connected to Link2 to resolve the issue?

- A. Enter spanning-tree port-priority 4 on SW2
- B. Enter spanning-tree port-priority 64 on SW2
- C. Enter spanning-tree port-priority 224 on SW1
- **D. Enter spanning-tree port-priority 32 on SW1** ✓

Explanation

SW1 needs to block one of its ports to SW2 to avoid a bridging loop between the two switches. Unfortunately, it blocked the fiber port Link2. But how does SW2 select its blocked port? Well, the answer is based on the BPDUs it receives from SW1. A BPDU is superior than another if it has:

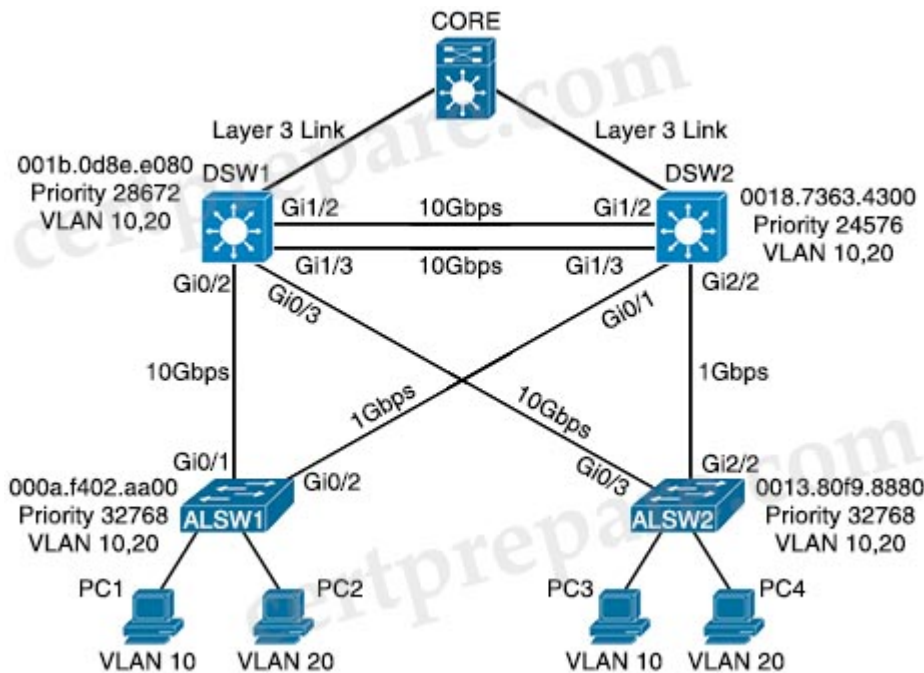
1. A lower Root Bridge ID
2. A lower path cost to the Root
3. A lower Sending Bridge ID
4. A lower Sending Port ID

These four parameters are examined in order. In this specific case, all the BPDUs sent by SW1 have the same Root Bridge ID, the same path cost to the Root and the same Sending Bridge ID. The only parameter left to select the best one is the Sending Port ID (Port ID = port priority + port index). And the port index of Gi0/0 is lower than the port index of Gi0/1 so Link 1 has been chosen as the primary link.

Therefore we must change the port priority to change the primary link. The lower numerical value of port priority, the higher priority that port has. In other words, we must change the port-priority on Gi0/1 of SW1 (not on Gi0/1 of SW2) to a lower value than that of Gi0/0.

Question 4

Refer to the exhibit. Assuming all links are functional, which path does PC1 take to reach DSW1?



- **A. PC1 goes from ALSW1 to DSW2 to DSW1** ✓
- B. PC1 goes from ALSW1 to DSW2 to Core to DSW1
- C. PC1 goes from ALSW1 to DSW1
- D. PC1 goes from ALSW1 to DSW2 to ALSW2 to DSW1

Explanation

In the topology above, we see DSW2 has lowest priority 24576 so it is the root bridge for VLAN 10 so surely all traffic for this VLAN must go through it. All of DSW2 ports must be in forwarding state. And:

- + The direct link between DSW1 and ALSW1 is blocked by STP.
- + The direct link between DSW1 and ALSW2 is also blocked by STP.

Therefore PC1 must go via this path: PC1 -> ALSW1 -> DSW2 -> DSW1.

Question 5

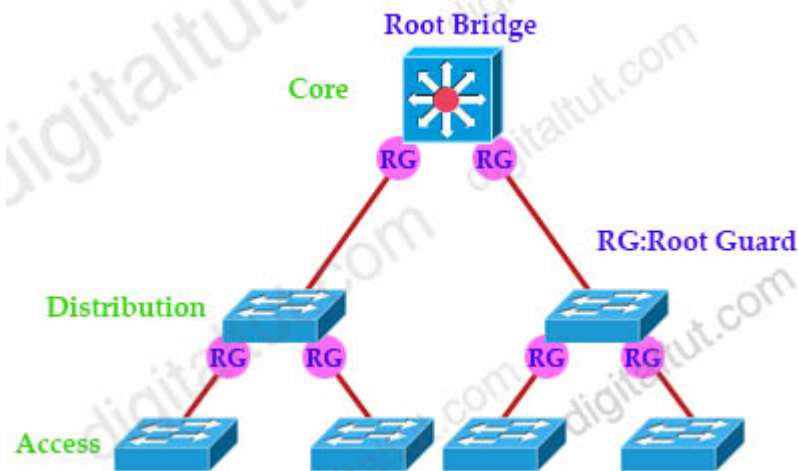
In a traditional 3 tier topology, an engineer must explicitly configure a switch as the root bridge and exclude it from any further election process for the spanning-tree domain. Which action accomplishes this task?

- A. Configure the spanning-tree priority equal to 0
- B. Configure BPDU guard in all switch-to-switch connections
- **C. Configure root guard and portfast on all access switch ports** ✓
- D. Configure the spanning-tree priority to 32768

Explanation

Root guard does not allow the port to become a STP root port, so the port is always STP-designated. If a better BPDU arrives on this port, root guard does not take the BPDU into account and elect a new STP root. Instead, root guard puts the port into the root-inconsistent STP state which is equal to a listening state. No traffic is forwarded across this port.

Below is an example of where to configure Root Guard on the ports. Notice that Root Guard is always configured on designated ports.



To configure Root Guard use this command:

Switch(config-if)# **spanning-tree guard root**

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

Question 6

What is the primary effect of the spanning-tree portfast command?

- A. It enables BPDU messages
- **B. It minimizes spanning-tree convergence time** ✓
- C. It immediately enables the port in the listening state
- D. It immediately puts the port into the forwarding state when the switch is reloaded

Explanation

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.

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

Question 7

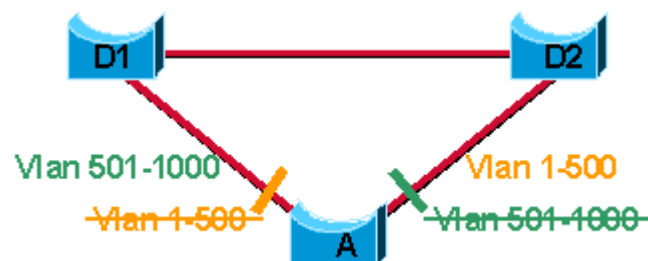
What would be the preferred way to implement a loopless switch network where there are 1500 defined VLANs and it is necessary to load the shared traffic through two main aggregation points based on the VLAN identifier?

- **A. 802.1s** ✓
- B. 802.1AE
- C. 802.1W
- D. 802.1D

Explanation

Where to Use MST

This diagram shows a common design that features access Switch A with 1000 VLANs redundantly connected to two distribution Switches, D1 and D2. In this setup, users connect to Switch A, and the network administrator typically seeks to achieve load balancing on the access switch Uplinks based on even or odd VLANs, or any other scheme deemed appropriate.



Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html>

Question 8

Refer to the exhibit.



An engineer reconfigures the port-channel between SW1 and SW2 from an access port to a trunk and immediately notices this error in SW1's log.

```
%PM-SP-4-ERR_DISABLE: bpduguard error detected on Gi0/0, putting Gi0/0 in err-disable state.
```

Which command set resolves this error?

- A. Sw1(config)# interface G0/0
Sw1(config-if)# no spanning-tree bpduguard enable ✓
Sw1(config-if)# shut
Sw1(config-if)# no shut
- B. w1(config)# interface G0/0
Sw1(config-if)# no spanning-tree bpdufilter
Sw1(config-if)# shut
- Sw1(config-if)# no shut
- C. Sw1(config)# interface G0/0
Sw1(config-if)# spanning-tree bpduguard enable
Sw1(config-if)# shut
- Sw1(config-if)# no shut
- D. Sw1(config)# interface G0/1
Sw1(config-if)# spanning-tree bpduguard enable
Sw1(config-if)# shut
- Sw1(config-if)# no shut

Comments

1. Ennatz

February 2nd, 2021

Question 6 I assume C is right:

What is the primary effect of the spanning-tree portfast command?

C. It immediately puts the port into the forwarding state when the switch is reloaded

Shown Cisco Link shows:

to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge.

So it did not speed up STP convergence time in the switch itself:

B. It minimizes spanning-tree convergence time => only for the port, not for the STP at all

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[Virtualization 2 Quiz](#) [NAT Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)

- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)

- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Switching Mechanism Quiz

Switching Mechanism Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Switching Mechanism Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
7	90	90%	90	100.00%	00:01:17

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

How does the RIB differ from the FIB?

- A. The RIB includes many routes to the same destination prefix. The FIB contains only the best route.
- **B. The RIB is used to create network topologies and routing tables. The FIB is a list of routes to particular network destinations.** ✓
- C. The FIB includes many routes a single destination. The RIB is the best route to a single destination.
- D. The FIB maintains network topologies and routing tables. The RIB is a list of routes to particular network destinations.

Question 2

What is the difference between a RIB and a FIB?

- A. The FIB is where all IP routing information is stored
- **B. The FIB is populated based on RIB content** ✓
- C. The RIB is used to make IP source prefix-based switching decisions
- D. The RIB maintains a mirror image of the FIB

Explanation

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

Note: In order to view the Routing information base (RIB) table, use the “show ip route” command. To view the Forwarding Information Base (FIB), use the “show ip cef” command. RIB is in Control plane while FIB is in Data plane.

Question 3

What is the difference between CEF and process switching?

- A. CEF is more CPU-intensive than process switching.
- **B. CEF uses the FIB and the adjacency table to make forwarding decisions, whereas process switching punts each packet.** ✓
- C. CEF processes packets that are too complex for process switching to manage.
- D. Process switching is faster than CEF.

Explanation

“Punt” is often used to describe the action of moving a packet from the fast path (CEF) to the route processor for handling.

Cisco Express Forwarding (CEF) provides the ability to switch packets through a device in a very quick and efficient way while also keeping the load on the router’s processor low. CEF is made up of two different main components: the **Forwarding Information Base (FIB)** and the **Adjacency Table**.

Process switching is the slowest switching methods (compared to fast switching and Cisco Express Forwarding) because it must find a destination in the routing table. Process switching must also construct a new Layer 2 frame header for every packet. With process switching, when a packet comes in, the scheduler calls a process that examines the routing table, determines which interface the packet should be switched to and then switches the packet. The problem is, this happens for the every packet.

Reference: <http://www.cisco.com/web/about/security/intelligence/acl-logging.html>

Question 4

Which statement about Cisco Express Forwarding is true?

- A. It uses a fast cache that is maintained in a router data plane
- B. The CPU of a router becomes directly involved with packet-switching decisions
- **C. It maintains two tables in the data plane the FIB and adjacency table** ✓
- D. It makes forwarding decisions by a process that is scheduled through the IOS scheduler

Explanation

Cisco Express Forwarding (CEF) provides the ability to switch packets through a device in a very quick and efficient way while also keeping the load on the router's processor low. CEF is made up of two different main components: the **Forwarding Information Base (FIB)** and the **Adjacency Table**. These are automatically updated at the same time as the routing table.

The Forwarding Information Base (FIB) contains destination reachability information as well as next hop information. This information is then used by the router to make forwarding decisions. The FIB allows for very efficient and easy lookups. Below is an example of the FIB table:

```
R2#show ip cef
```

Prefix	Next Hop	Interface
0.0.0.0/0	192.168.201.1	FastEthernet0/0
0.0.0.0/32	receive	
192.168.201.0/27	attached	FastEthernet0/0
192.168.201.0/32	receive	
192.168.201.1/32	192.168.201.1	FastEthernet0/0
192.168.201.2/32	receive	
192.168.201.31/32	receive	
224.0.0.0/4	drop	
224.0.0.0/24	receive	
255.255.255.255/32	receive	

The adjacency table is tasked with maintaining the layer 2 next-hop information for the FIB. An example of the adjacency table is shown below:

```
Router#show adjacency
```

Protocol	Interface	Address
IP	Serial0	192.168.209.130 (2) (incomplete)
IP	Serial0	192.168.209.131 (7)
IP	Ethernet0	192.168.201.1 (7)

Note: A fast cache is only used when fast switching is enabled while CEF is disabled.

Question 5

How are the Cisco Express Forwarding table and the FIB related to each other?

- A. The FIB is used to populate the Cisco Express Forwarding table
- B. There can be only one FIB but multiple Cisco Express Forwarding tables on IOS devices
- **C. Cisco Express Forwarding uses a FIB to make IP destination prefix-based switching decisions** 
- D. The Cisco Express Forwarding table allows route lookups to be forwarded to the route processor for processing before they are sent to the FIB

Explanation

The Forwarding Information Base (FIB) table – CEF uses a FIB to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the

network, the IP routing table is updated, and these changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table.

Reference: <https://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html>

Question 6

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

- A. The FIB is derived from the control plane, and the RIB is derived from the FIB.
- **B. The RIB is a database of routing prefixes, and the FIB is the information used to choose the egress interface for each packet.** ✓
- **C. The RIB is derived from the control plane, and the FIB is derived from the RIB.** ✓
- D. FIB is a database of routing prefixes, and the RIB is the information used to choose the egress interface for each packet.
- E. The FIB is derived from the data plane, and the RIB is derived from the FIB.

Explanation

The Forwarding Information Base (FIB) contains destination reachability information as well as next hop information. This information is then used by the router to make forwarding decisions. The FIB allows for very efficient and easy lookups. Below is an example of the FIB table:

```
R2#show ip cef
```

Prefix	Next Hop	Interface
0.0.0.0/0	192.168.201.1	FastEthernet0/0
0.0.0.0/32	receive	
192.168.201.0/27	attached	FastEthernet0/0
192.168.201.0/32	receive	
192.168.201.1/32	192.168.201.1	FastEthernet0/0
192.168.201.2/32	receive	
192.168.201.31/32	receive	
224.0.0.0/4	drop	
224.0.0.0/24	receive	
255.255.255.255/32	receive	

The FIB maintains next-hop address information based on the information in the IP routing table (RIB).

Note: In order to view the Routing information base (RIB) table, use the “show ip route” command. To view the Forwarding Information Base (FIB), use the “show ip cef” command. RIB is in Control plane while FIB is in Data plane.

Question 7

Which two statements about Cisco Express Forwarding load balancing are true? (Choose two)

- A. Cisco Express Forwarding can load-balance over a maximum of two destinations
- **B. Each hash maps directly to a single entry in the adjacency table** ✓
- C. It combines the source IP address subnet mask to create a hash for each destination
- D. Each hash maps directly to a single entry in the RIB

- **E. It combines the source and destination IP addresses to create a hash for each destination** ✓

Explanation

Cisco IOS software basically supports two modes of CEF load balancing: On per-destination or per-packet basis.

For per destination load balancing a hash is computed out of the source and destination IP address (-> Answer 'It combines the source and destination IP addresses to create a hash for each destination' is correct). **This hash points to exactly one of the adjacency entries in the adjacency table** (-> Answer 'Each hash maps directly to a single entry in the adjacency table' is correct), providing that the same path is used for all packets with this source/destination address pair. If per packet load balancing is used the packets are distributed round robin over the available paths. In either case the information in the FIB and adjacency tables provide all the necessary forwarding information, just like for non-load balancing operation.

The number of paths used is limited by the number of entries the routing protocol puts in the routing table, the default in IOS is 4 entries for most IP routing protocols with the exception of BGP, where it is one entry. **The maximum number that can be configured is 6 different paths** -> Answer 'Cisco Express Forwarding can load-balance over a maximum of two destinations' is not correct.

Reference:

https://www.cisco.com/en/US/products/hw/modules/ps2033/prod_technical_reference09186a00800afeb7.html

Comments

1. Brozzo

November 23rd, 2020

Very clear ... makes the CEF explanation less confusing

2. Anonymous

December 3rd, 2020

q2 rib vs fib – the explanation seems to confirm a different answer (i.e. one is a mirror of the other) to that presented as the actual answer??

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)
[Virtualization Quiz](#) [QoS Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)

- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Troubleshooting Quiz

Troubleshooting Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Troubleshooting Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
1	10	90%	10	100.00%	00:19:21

Congratulations!

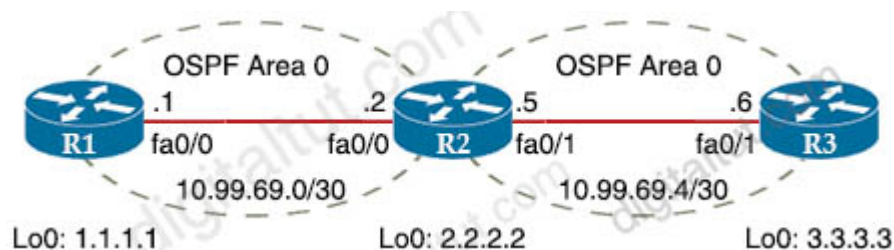
You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit. R1 is able to ping the R3 fa0/1 interface. Why do the extended pings fail?




```

R1#ping
Protocol [ip]:
Target IP address: 3.3.3.3
Repeat count [5]: 3
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]: yes
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [9]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
Packet sent with the DF bit set
Packet has IP options: Total option bytes= 39, padded length=40
Record route: <*>
(0.0.0.0)
(0.0.0.0)

Unreachable from 10.99.69.2, maximum MTU 1492, Received packet has options
Total option bytes= 39, padded length=40
Record route: <*>
(0.0.0.0)
(0.0.0.0)
<output omitted>

```

- A. The maximum packet size accepted by the command is 1476 bytes
- B. R2 and R3 do not have an OSPF adjacency
- C. R3 is missing a return route to 10.99.69.0/30
- **D. The DF bit has been set** ✓

Explanation

If the DF bit is set, routers cannot fragment packets. From the output below, we learn that the maximum MTU of R2 is 1492 bytes while we sent ping with 1500 bytes. Therefore these ICMP packets were dropped.

Note: Record option displays the address(es) of the hops (up to nine) the packet goes through.

Comments

1. No comments yet.
1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[Drag Drop 2 Quiz](#) [SPAN Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)

- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)

- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH



[Home](#) > Trunking Quiz

Trunking Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Trunking Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
3	30	90%	30	100.00%	00:00:22

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit. SwitchC connects HR and Sales to the Core switch. However, business needs require that no traffic from the Finance VLAN traverse this switch. Which command meets this requirement?

```
SwitchC#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 8
VTP Operating Mode          : Transparent
VTP Domain Name             : MyDomain.com
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xCC 0x77 0x02 0x40 0x93 0xB5 0xC1 0xA2
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
```

```
SwitchC#show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Po1
110  Finance                active
210  HR                      active    Fa0/1
```

310 Sales

active

Fa0/2

SwitchC#show int trunk

Port	Mode	Encapsulation	Status	Native vlan
Gig1/1	on	802.1q	trunking	1
Gig1/2	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Gig1/1	1-1005
Gig1/2	1-1005

Port	Vlans allowed and active in management domain
Gig1/1	1,110,210,310
Gig1/2	1,110,210,310

SwitchC#show run interface port-channel 1

```

interface Port-channel 1
description Uplink_to_Core
switchport mode trunk

```

- A. SwitchC(config)#vtp pruning vlan 110
- B. SwitchC(config)#vtp pruning
- **C. SwitchC(config)#interface port-channel 1**
SwitchC(config-if)#switchport trunk allowed vlan remove 110 ✓
- D. SwitchC(config)#interface port-channel 1
- SwitchC(config-if)#switchport trunk allowed vlan add 210,310

Explanation

From the “show vlan brief” we learn that Finance belongs to VLAN 110 and all VLANs (from 1 to 1005) are allowed to traverse the trunk (port-channel 1). Therefore we have to remove VLAN 110 from the allowed VLAN list with the “switchport trunk allowed vlan remove ” command. The pruning feature cannot do this job as Finance VLAN is active.

Question 2

Refer to the exhibit.



Company policy restricts VLAN 10 to be allowed only on SW1 and SW2. All other VLANs can be on all three switches. An administrator has noticed that VLAN 10 has propagated to SW3. Which configuration corrects the issue?

- **A. SW2(config)#interface gi1/2**
SW2(config)#switchport trunk allowed vlan 1-9,11-4094 ✓
- B. SW2(config)#interface gi1/2
- SW2(config)#switchport trunk allowed vlan 10
- C. SW1(config)#interface gi1/1
- SW1(config)#switchport trunk allowed vlan 1-9,11-4094
- D. SW2(config)#interface gi1/1
- SW2(config)#switchport trunk allowed vlan 10

Question 3

Refer to exhibit. VLANs 50 and 60 exist on the trunk links between all switches. All access ports on SW3 are configured for VLAN 50 and SW1 is the VTP server. Which command ensures that SW3 receives frames only from VLAN 50?



- A. SW1(config)>vtp mode transparent
- B. SW3(config)#vtp mode transparent
- **C. SW1 (config)#vtp pruning** ✓
- D. SW2(config)#vtp pruning

Explanation

SW3 does not have VLAN 60 so it should not receive traffic for this VLAN (sent from SW2). Therefore we should configure VTP Pruning on SW3 so that SW2 does not forward VLAN 60 traffic to SW3. Also notice that we need to configure pruning on SW1 (the VTP Server), not SW2.

Comments

1. MAC

February 3rd, 2021

hi guys can we please check q1 as the exhibit shows that a generic trunk has been set up

```
SwitchC#show run interface port-channel 1
interface Port-channel 1
description Uplink_to_Core
switchport mode trunk
```

and your answer is to remove a vlan from this but surely that would only work if the allowed statement is already there? therefore it would be answer

```
D. SwitchC(config)#interface port-channel 1
SwitchC(config-if)#switchport trunk allowed vlan add 210,310
```

although this would drop vlan 1 ie the native vlan

2. MAC

February 3rd, 2021

please ignore my last question i quickly checked it live and the remove command actually adds the allowed statement minus the removed vlan

Thank you

3. Uzi

February 7th, 2021

The exhibit for question#2 is not visible – referring to Finance VLAN traverse

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real i



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[SD-WAN & SD-Access Solutions Quiz](#) [Etherchannel Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)

- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)

- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Virtualization 2 Quiz

Virtualization 2 Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Virtualization 2 Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
7	80	90%	80	100.00%	00:00:40

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

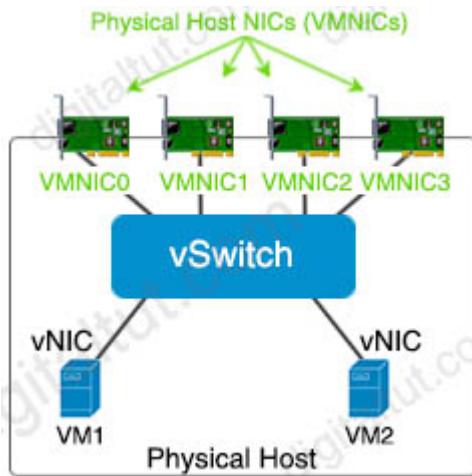
Question 1

Which element enables communication between guest VMs within a virtualized environment?

- **A. vSwitch** ✓
- B. pNIC
- C. virtual router
- D. hypervisor

Explanation

Each VM is provided with a **virtual NIC (vNIC)** that is connected to the virtual switch. Multiple vNICs can connect to a single vSwitch, allowing VMs on a physical host to communicate with one another at layer 2 without having to go out to a physical switch.



Question 2

What is a benefit of using a Type 2 hypervisor instead of a Type 1 hypervisor?

- A. improved density and scalability
- **B. ability to operate on hardware that is running other OSs** ✓
- C. better application performance
- D. improved security because the underlying OS is eliminated

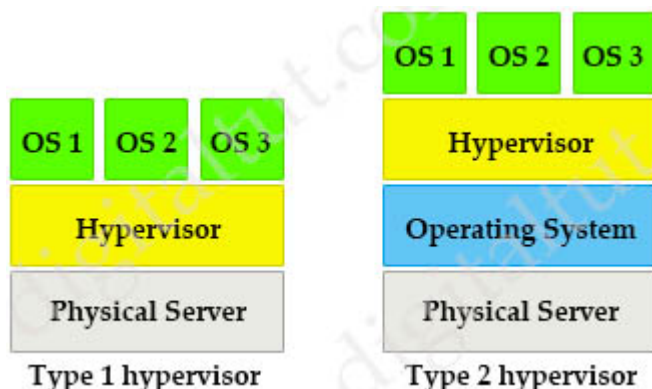
Explanation

There are two types of hypervisors: type 1 and type 2 hypervisor.

In type 1 hypervisor (or native hypervisor), the hypervisor is installed directly on the physical server. Then instances of an operating system (OS) are installed on the hypervisor. Type 1 hypervisor has direct access to the hardware resources. Therefore they are more efficient than hosted architectures. Some examples of type 1 hypervisor are VMware vSphere/ESXi, Oracle VM Server, KVM and Microsoft Hyper-V.

In contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. A big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows).

Type 1 is more efficient and well performing, it is also more secure than type 2 because the flaws and vulnerabilities that are endemic to Operating Systems are often absent from Type 1, bare metal hypervisors. Type 1 has better performance, scalability and stability **but supported by limited hardware**.



Question 3

Which two actions provide controlled Layer 2 network connectivity between virtual machines running on the same hypervisor? (Choose two)

- A. Use VXLAN fabric after installing VXLAN tunnelling drivers on the virtual machines
- **B. Use a virtual switch provided by the hypervisor** ✓
- **C. Use a virtual switch running as a separate virtual machine** ✓
- D. Use a single routed link to an external router on stick
- E. Use a single trunk link to an external Layer2 switch

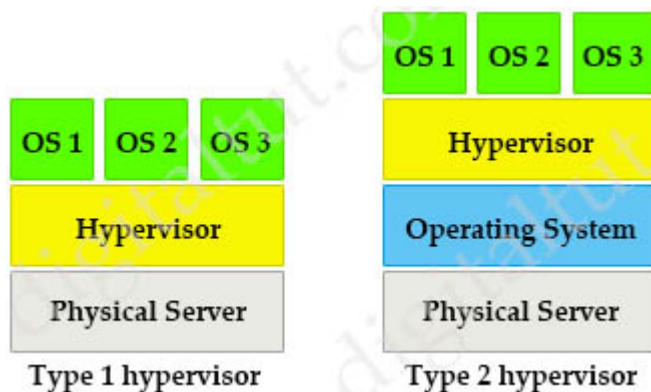
Question 4

A server running Linux is providing support for virtual machines along with DNS and DHCP services for a small business. Which technology does this represent?

- A. hardware pass-through
- **B. Type 2 hypervisor** ✓
- C. Type 1 hypervisor
- D. container

Explanation

In contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. A big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows).



Question 5

What is a Type 1 hypervisor?

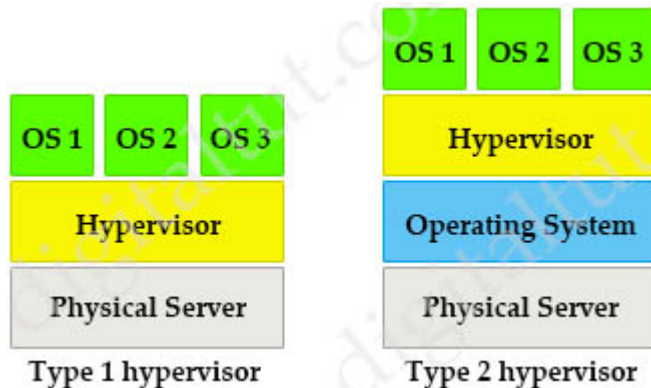
- A. runs directly on a physical server and depends on a previously installed operating system
- **B. runs directly on a physical server and includes its own operating system** ✓
- C. run on a virtual server and includes its own operating system
- D. runs on a virtual server and depends on an already installed operating system

Explanation

There are two types of hypervisors: type 1 and type 2 hypervisor.

In type 1 hypervisor (or native hypervisor), the hypervisor is installed directly on the physical server. Then instances of an operating system (OS) are installed on the hypervisor. Type 1 hypervisor has direct access to the hardware resources. Therefore they are more efficient than hosted architectures. Some examples of type 1 hypervisor are VMware vSphere/ESXi, Oracle VM Server, KVM and Microsoft Hyper-V.

In contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. A big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows).



Question 6

Refer to the exhibit.

```
interface Vlan10
 ip vrf forwarding Customer1
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan20
 ip vrf forwarding Customer2
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
 ip vrf forwarding Customer3
 ip address 10.1.1.1 255.255.255.0
```

Which configuration allows Customer2 hosts to access the FTP server of Customer1 that has the IP address of 192.168.1.200?

- A. `ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 global`
`ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 global`
`ip route 192.168.1.0 255.255.255.0 Vlan10`
`ip route 172.16.1.0 255.255.255.0 Vlan20` ✓
- B. `p route vrf Customer1 172.16.1.1 255.255.255.255 172.16.1.1 global`
`ip route vrf Customer2 192.168.1.200 255.255.255.0 192.168.1.1 global`
`ip route 192.168.1.0 255.255.255.0 Vlan10`
- C. `ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer2`
- `ip route vrf Customer2 192.168.1.200 255.255.255.255 192.168.1.1 Customer1`

- D. `ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer1`
- `ip route vrf Customer2 192.168.1.200 255.255.255.0 192.168.1.1 Customer2`

Explanation

Static routes directly between VRFs are not supported so we cannot configure a direct static route between two VRFs.

The command “`ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 global`” means in VRF Customer1, in order to reach destination 172.16.1.0/24 then we use the next hop IP address 172.16.1.1 in the global routing table. And the command “`ip route 192.168.1.0 255.255.255.0 Vlan10`” tells the router “to reach 192.168.1.0/24, send to Vlan 10”.

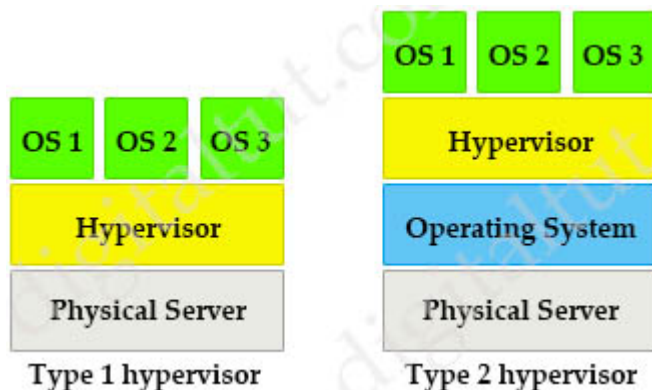
Question 7

A customer has deployed an environment with shared storage to allow for the migration of virtual machines between servers with dedicated operating systems that provide the virtualization platform. What is this operating system described as?

- A. container oriented
- B. type 1 hypervisor
- **C. hosted virtualization** ✓
- D. decoupled

Explanation

Hosted virtualization is type 2 hypervisor. In contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. A big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows).



Comments

1. No comments yet.
1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[SD-WAN & SD-Access Solutions 2 Quiz](#) [STP Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)

- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)

- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Virtualization Quiz

Virtualization Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Virtualization Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
10	150	90%	150	100.00%	00:22:58

Congratulations!

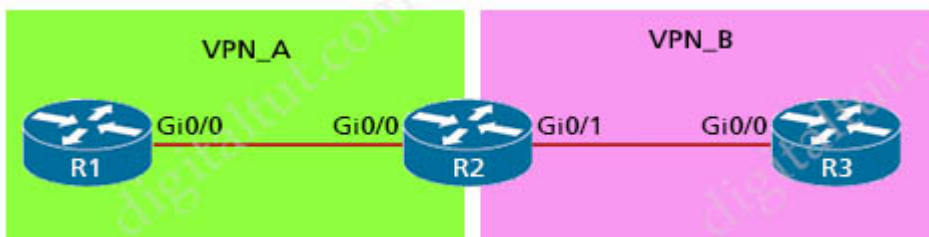
You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Refer to the exhibit. Assuming that R1 is a CE router, which VRF is assigned to Gi0/0 on R1?



- A. VRF VPN_B
- B. Management VRF
- C. VRF VPN_A
- **D. Default VRF** ✓

Explanation

There is nothing special with the configuration of Gi0/0 on R1. Only Gi0/0 interface on R2 is assigned to VRF VPN_A. The default VRF here is similar to the global routing table concept in Cisco IOS

Question 2

<https://t.me/learningnets>

Which two entities are Type 1 hypervisors? (Choose two)

- A. VMware server
- B. Microsoft Virtual PC
- **C. VMware ESX** ✓
- **D. Microsoft Hyper-V** ✓
- E. Oracle VM VirtualBox

Explanation

A bare-metal hypervisor (Type 1) is a layer of software we install directly on top of a physical server and its underlying hardware. There is no software or any operating system in between, hence the name bare-metal hypervisor. A Type 1 hypervisor is proven in providing excellent performance and stability since it does not run inside Windows or any other operating system. These are the most common type 1 hypervisors:

- + VMware vSphere with ESX/ESXi
- + KVM (Kernel-Based Virtual Machine)
- + Microsoft Hyper-V
- + Oracle VM
- + Citrix Hypervisor (formerly known as Xen Server)

Question 3**Which statement explains why Type 1 hypervisor is considered more efficient than Type 2 hypervisor?**

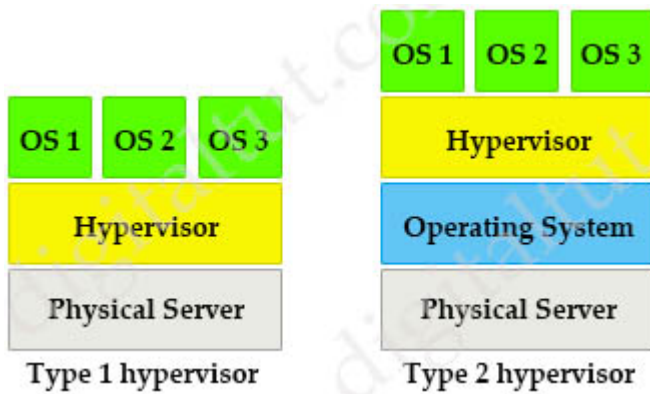
- A. Type 1 hypervisor is the only type of hypervisor that supports hardware acceleration techniques
- **B. Type 1 hypervisor runs directly on the physical hardware of the host machine without relying on the underlying OS** ✓
- C. Type 1 hypervisor enables other operating systems to run on it
- D. Type 1 hypervisor relies on the existing OS of the host machine to access CPU, memory, storage, and network resources

Explanation

There are two types of hypervisors: type 1 and type 2 hypervisor.

In type 1 hypervisor (or native hypervisor), the hypervisor is installed directly on the physical server. Then instances of an operating system (OS) are installed on the hypervisor. Type 1 hypervisor has direct access to the hardware resources. Therefore they are more efficient than hosted architectures. Some examples of type 1 hypervisor are VMware vSphere/ESXi, Oracle VM Server, KVM and Microsoft Hyper-V.

In contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. answer 'Type 1 hypervisor runs directly on the physical hardware of the host machine without relying on the underlying OS' big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows).



Question 4

What are two benefits of virtualizing the server with the use of VMs in data center environment? (Choose two)

- **A. speedy deployment** ✓
- B. increased security
- C. smaller Layer 2 domain
- D. reduced IP and MAC address requirements
- **E. reduced rack space, power, and cooling requirements** ✓

Explanation

Server virtualization and the use of virtual machines is profoundly changing data center dynamics. Most organizations are struggling with the cost and complexity of hosting multiple physical servers in their data centers. The expansion of the data center, a result of both scale-out server architectures and traditional “one application, one server” sprawl, has created problems in housing, powering, and cooling large numbers of underutilized servers. In addition, IT organizations continue to deal with the traditional cost and operational challenges of matching server resources to organizational needs that seem fickle and ever changing.

Virtual machines can significantly mitigate many of these challenges by enabling multiple application and operating system environments to be hosted on a single physical server while maintaining complete isolation between the guest operating systems and their respective applications. Hence, server virtualization facilitates server consolidation by enabling organizations to exchange a number of underutilized servers for a single highly utilized server running multiple virtual machines.

By consolidating multiple physical servers, organizations can gain several benefits:

- + Underutilized servers can be retired or redeployed.
- + Rack space can be reclaimed.
- + Power and cooling loads can be reduced.
- + New virtual servers can be rapidly deployed.
- + CapEx (higher utilization means fewer servers need to be purchased) and OpEx (few servers means a simpler environment and lower maintenance costs) can be reduced.

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

Question 5

Refer to the exhibit. You have just created a new VRF on PE3. You have enabled debug ip bgp vpnv4 unicast updates on PE1, and you can see the route in the debug, but not in the BGP VPNv4 table. Which two statements are true? (Choose two)

```
*Jun19 11:12: BGP(4):10.1.1.2 rcvd UPDATE w/ attr:nexthop 10.1.1.2, origin ?, localpref 100,metric 0,extended community RT:999:999
*Jun19 11:12: BGP(4):10.1.1.2 rcvd 999:999:192.168.1.99/32,label 29-DENIED due to:extended community not supported
```

- A. address-family ipv4 vrf is not configured on PE3
- **B. PE1 will reject the route due to automatic route filtering** ✓
- **C. After you configure route-target import 999:999 for a VRF on PE1, the route will be accepted** ✓
- D. After you configure route-target import 999:999 for a VRF on PE3, the route will be accepted
- E. VPNv4 is not configured between PE1 and PE3

Explanation

Because some PE routers might receive routing information they do not require, a basic requirement is to be able to filter the MP-iBGP updates at the ingress to the PE router so that the router does not need to keep this information in memory.

The **Automatic Route Filtering** feature fulfills this filtering requirement. This feature is available by default on all PE routers, and no additional configuration is necessary to enable it. Its function is to filter automatically VPN-IPv4 routes that contain a route target extended community that does not match any of the PE's configured VRFs. This effectively discards any unwanted VPN-IPv4 routes silently, thus reducing the amount of information that the PE has to store in memory -> Answer 'PE1 will reject the route due to automatic route filtering' is correct.

Reference: MPLS and VPN Architectures Book, Volume 1

The reason that PE1 dropped the route is there is no "route-target import 999:999" command on PE1 (so we see the "DENIED due to:extended community not supported" in the debug) so we need to type this command to accept this route -> Answer 'After you configure route-target import 999:999 for a VRF on PE1, the route will be accepted' is correct.

Question 6

What is the main function of VRF-lite?

- **A. To segregate multiple routing tables on a single device** ✓
- B. To route IPv6 traffic across an IPv4 backbone
- C. To connect different autonomous systems together to share routes
- D. To allow devices to use labels to make Layer 2 Path decisions

Question 7

Which statement describes the IP and MAC allocation requirements for virtual machines on type 1 hypervisors?

- A. Each virtual machine requires a unique MAC address but shares the IP address with the physical server
- B. Each virtual machine requires a unique IP address but shares the MAC address with the physical server
- C. Each virtual machines requires a unique IP address but shares the MAC address with the address of the physical server
- **D. Each virtual machine requires a unique IP and MAC addresses to be able to reach to other nodes** ✓

Explanation

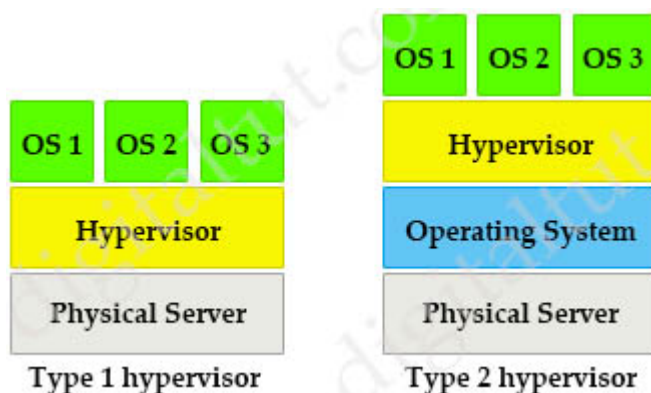
A virtual machine (VM) is a software emulation of a physical server with an operating system. From an application's point of view, the VM provides the look and feel of a real physical server, including all its components, such as CPU, memory, and network interface cards (NICs).

The virtualization software that creates VMs and performs the hardware abstraction that allows multiple VMs to run concurrently is known as a hypervisor.

There are two types of hypervisors: type 1 and type 2 hypervisor.

In type 1 hypervisor (or native hypervisor), the hypervisor is installed directly on the physical server. Then instances of an operating system (OS) are installed on the hypervisor. Type 1 hypervisor has direct access to the hardware resources. Therefore they are more efficient than hosted architectures. Some examples of type 1 hypervisor are VMware vSphere/ESXi, Oracle VM Server, KVM and Microsoft Hyper-V.

In contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. answer 'Each virtual machine requires a unique IP and MAC addresses to be able to reach to other nodes' big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows).



Question 8

Which statement about route targets is true when using VRF-Lite?

- A. When BGP is configured, route targets are transmitted as BGP standard communities
- B. Route targets allow customers to be assigned overlapping addresses
- C. Route targets uniquely identify the customer routing table
- **D. Route targets control the import and export of routes into a customer routing table** ✓

Explanation

Answer 'Route targets allow customers to be assigned overlapping addresses' and answer 'Route targets uniquely identify the customer routing table' are not correct as only route distinguisher (RD) identifies the customer routing table and “allows customers to be assigned overlapping addresses”.

Answer 'When BGP is configured, route targets are transmitted as BGP standard communities' is not correct as “When BGP is configured, route targets are transmitted as BGP **extended** communities”

Question 9

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

- A. Communication between vSwitch and network switch is broadcast based
- B. Communication between vSwitch and network switch is multicast based
- **C. The Layer 2 domain can be large in virtual machine environments** ✓
- D. Virtual machines communicate primarily through broadcast mode
- **E. vSwitch must interrupt the server CPU to process the broadcast packet** ✓

Explanation

Broadcast radiation refers to the processing that is required every time a broadcast is received on a host. Although IP is very efficient from a broadcast perspective when compared to traditional protocols such as Novell Internetwork Packet Exchange (IPX) Service Advertising Protocol (SAP), virtual machines and the vswitch implementation require special consideration. **Because the vswitch is software based, as broadcasts are received the vswitch must interrupt the server CPU** to change contexts to enable the vswitch to process the packet. After the vswitch has determined that the packet is a broadcast, it copies the packet to all the VMNICs, which then pass the broadcast packet up the stack to process. This processing overhead can have a tangible effect on overall server performance if a single domain is hosting a large number of virtual machines.

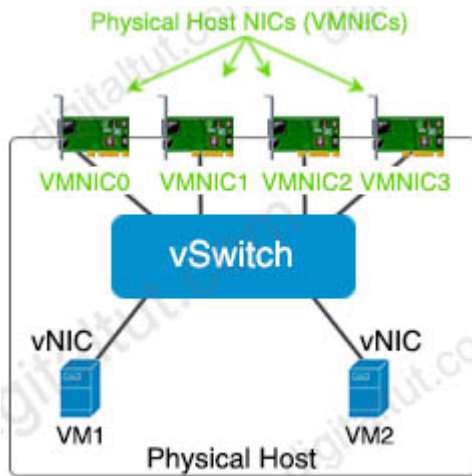
Note: This overhead effect is not a limitation of the vswitch implementation. It is a result of the software-based nature of the vswitch embedded in the ESX hypervisor.

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

Note about the structure of virtualization in a hypervisor:

Hypervisors provide **virtual switch** (vSwitch) that Virtual Machines (VMs) use to communicate with other VMs on the same host. The vSwitch may also be connected to the host's physical NIC to allow VMs to get layer 2 access to the outside world.

Each VM is provided with a **virtual NIC (vNIC)** that is connected to the virtual switch. Multiple vNICs can connect to a single vSwitch, allowing VMs on a physical host to communicate with one another at layer 2 without having to go out to a physical switch.



Although vSwitch does not run Spanning-tree protocol but vSwitch implements other loop prevention mechanisms. For example, a frame that enters from one VMNIC is not going to go out of the physical host from a different VMNIC card.

Question 10

Which two statements about VRF-lite are true? (Choose two)

- A. It supports MPLS-VRF label exchange and labeled packets
- B. It supports most routing protocols, including EIGRP, ISIS, and OSPF
- **C. It can support multiple customers on a single switch ✓**
- **D. It should be used when a customer's router is connected to an ISP over OSPF ✓**
- E. It can increase the packet switching rate

Explanation

In VRF-Lite, Route distinguisher (RD) identifies the customer routing table and allows customers to be assigned overlapping addresses. Therefore it can support multiple customers with overlapping addresses -> Answer 'It can support multiple customers on a single switch' is correct.

VRFs are commonly used for MPLS deployments, when we use VRFs without MPLS then we call it VRF lite -> Answer 'It supports MPLS-VRF label exchange and labeled packets' is not correct.

- VRF-lite does not support IGRP and ISIS. (-> Answer 'It supports most routing protocols, including EIGRP, ISIS, and OSPF' is not correct)
- The capability vrf-lite subcommand under router ospf should be used when configuring OSPF as the routing protocol between the PE and the CE.
- VRF-lite does not affect the packet switching rate. (-> Answer 'It can increase the packet switching rate' is not correct)

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vrf.html#wp1045190>

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment



I'm not a robot

reCAPTCHA
[Privacy](#) - [Terms](#)

[Subscribe to comments feed](#)

[EIGRP & OSPF Quiz](#) [Switching Mechanism Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)

- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)

- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Wireless 2 Quiz

Wireless 2 Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Wireless 2 Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
10	100	90%	100	100.00%	00:01:00

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Why is an AP joining a different WLC than the one specified through option 43?

- A. The WLC is running a different software version
- B. The AP multicast traffic unable to reach the WLC through Layer 3
- C. The APs broadcast traffic is unable to reach the WLC through Layer 2
- **D. The AP is joining a primed WLC** ✓

Question 2

Which DHCP option helps lightweight APs find the IP address of a wireless LAN controller?

- **A. Option 43** ✓
- B. Option 60
- C. Option 67
- D. Option 150

Question 3

Refer to the exhibit.

<https://t.me/learningnets>

WLANs > Edit 'LiveDemo'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface ☒ Enabled

Interface Priority WLAN

	Authentication Servers	Accounting Servers
	☒ Enabled	☒ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Assuming the WLC's interfaces are not in the same subnet as the RADIUS server, which interface would the WLC use as the source for all RADIUS-related traffic?

- A. the controller management interface
- **B. the interface specified on the WLAN configuration** ✓
- C. any interface configured on the WLC
- D. the controller virtual interface

Question 4

When a wireless client roams between two different wireless controllers, a network connectivity outage is experienced for a period of time. Which configuration issue would cause this problem?

- A. Not all of the controllers in the mobility group are using the same mobility group name
- B. All of the controllers in the mobility group are using the same mobility group name
- C. All of the controllers within the mobility group are using the same virtual interface IP address
- **D. Not all of the controllers within the mobility group are using the same virtual interface IP address** ✓

Explanation

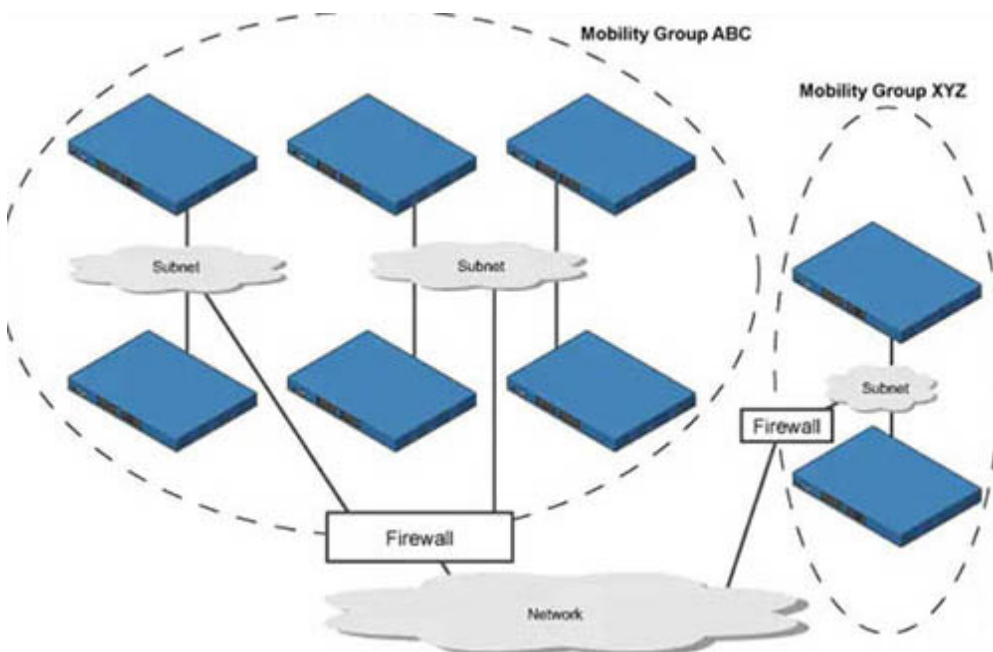
A prerequisite for configuring Mobility Groups is "All controllers must be configured with the same virtual interface IP address". If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming may appear to work, but the handoff does not complete, **and the client loses connectivity for a period of time**. -> Answer 'Not all of the controllers within the mobility group are using the same virtual interface IP address' is correct.

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

Answer 'Not all of the controllers in the mobility group are using the same mobility group name' is not correct because when the client moves to a different mobility group (with different mobility group name), that client would be connected (provided that the new connected controller had information about this client in its mobility list already) or drop (if the new connected controller have not had information about this client in its mobility list). For more information please read the note below.

Note:

A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices.



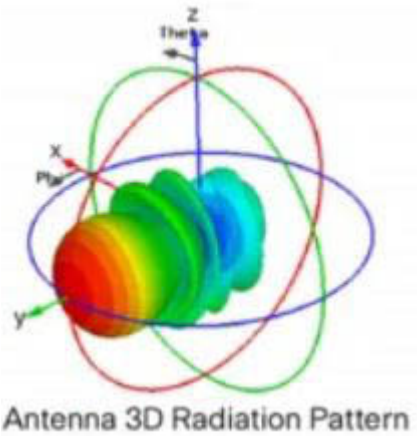
Let's take an example:

The controllers in the ABC mobility group share access point and client information with each other. The controllers in the ABC mobility group do not share the access point or client information with the XYZ controllers, which are in a different mobility group. Therefore if a client from ABC mobility group moves to XYZ mobility group, **and the new connected controller does not have information about this client in its mobility list**, that client will be dropped.

Note: Clients may roam between access points in different mobility groups if the controllers are included in each other's mobility lists.

Question 5

Which type of antenna does the radiation pattern represent?



- A. omnidirectional
- B. multidirectional
- C. Yagi ✓
- D. directional patch

Explanation

A Yagi antenna is formed by driving a simple antenna, typically a dipole or dipole-like antenna, and shaping the beam using a well-chosen series of non-driven elements whose length and spacing are tightly controlled.



Reference: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html

Question 6

Wireless users report frequent disconnections from the wireless network. While troubleshooting a network engineer finds that after the user a disconnect, the connection reestablishes automatically without any input required. The engineer also notices these message logs.

AP 'AP2' is down Reason: Radio channel set. 6:54:04 PM
 AP 'AP4' is down Reason: Radio channel set. 6:44:49 PM
 AP 'AP7' is down Reason: Radio channel set. 6:34:32 PM

Which action reduces the user impact?

- A. increase the AP heartbeat timeout
- B. increase the dynamic channel assignment interval ✓
- C. enable coverage hole detection
- D. increase BandSelect

Explanation

These message logs inform that the radio channel has been reset (and the AP must be down briefly). With dynamic channel assignment (DCA), the radios can frequently switch from one channel to another but it also makes disruption. The default DCA interval is 10 minutes, which is matched with the time of the message logs. By increasing the DCA interval, we can reduce the number of times our users are disconnected for changing radio channels.

Question 7

A client device roams between access points located on different floors in an atrium. The access points joined to the same controller and configuration in local mode. The access points are in different IP addresses, but the client VLAN in the group same. What type of roam occurs?

- A. inter-subnet
- **B. intra-controller** ✓
- C. inter-controller
- D. intra-VLAN

Explanation

Mobility, or roaming, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible. Three popular types of client roaming are:

Intra-Controller Roaming: Each controller supports same-controller client roaming across access points managed by the same controller. This roaming is transparent to the client as the session is sustained, and the client continues using the same DHCP-assigned or client-assigned IP address.

Inter-Controller Roaming: Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group and on the same subnet. This roaming is also transparent to the client because the session is sustained and a tunnel between controllers allows the client to continue using the same DHCP- or client-assigned IP address as long as the session remains active.

Inter-Subnet Roaming: Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01100.html

Question 8

What does the LAP send when multiple WLCs respond to the CISCO_CAPWAP-CONTROLLER.localdomain hostname during the CAPWAP discovery and join process?

- A. Unicast discovery request to the first WLC that resolves the domain name
- B. join request to all the WLCs
- C. broadcast discover request
- **D. unicast discovery request to each WLC** ✓

Explanation

The AP will attempt to resolve the DNS name CISCO-CAPWAP-CONTROLLER.localdomain. When the AP is able to resolve this name to one or more IP addresses, the AP sends a unicast CAPWAP Discovery Message to the resolved IP address(es). Each WLC that receives the CAPWAP Discovery Request Message replies with a unicast CAPWAP Discovery Response to the AP.

Reference: <https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107606-dns-wlc-config.html>

Question 9

Which access point mode allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues?

- A. client mode
- B. sniffer mode
- **C. sensor mode** ✓
- D. SE-connect mode

Explanation

As these wireless networks grow especially in remote facilities where IT professionals may not always be on site, it becomes even more important to be able to quickly identify and resolve potential connectivity issues ideally before the users complain or notice connectivity degradation.

To address these issues we have created Cisco's Wireless Service Assurance and a new AP mode called "sensor" mode. Cisco's Wireless Service Assurance platform has three components, namely, Wireless Performance Analytics, Real-time Client Troubleshooting, and Proactive Health Assessment. Using a supported AP or dedicated sensor **the device can actually function much like a WLAN client would associating and identifying client connectivity issues** within the network in real time without requiring an IT or technician to be on site.

Reference: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-5/b_Cisco_Aironet_Sensor_Deployment_Guide.html.xml

Question 10

What is calculated using the numerical values of the transmitter power level, cable loss and antenna gain?

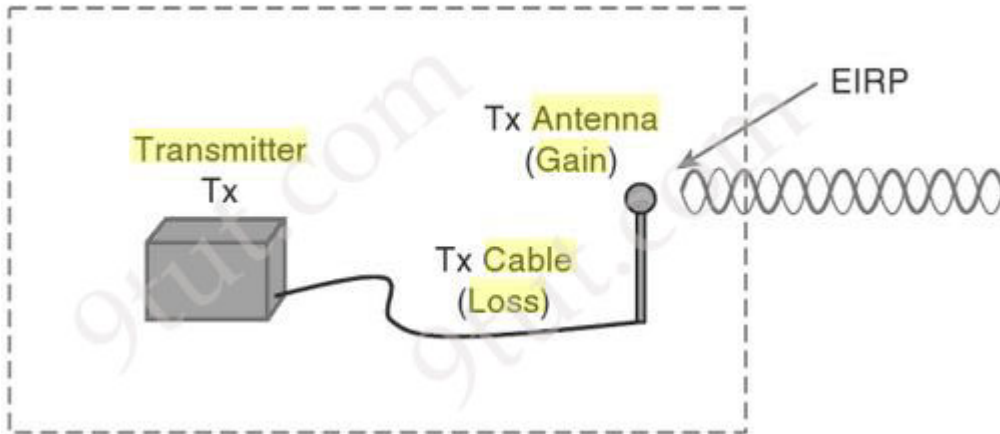
- A. SNR
- B. dBi
- C. RSSI
- **D. EIRP** ✓

Explanation

Once you know the complete combination of transmitter power level, the length of cable, and the antenna gain, you can figure out the actual power level that will be radiated from the antenna. This is known as the effective

isotropic radiated power (EIRP), measured in dBm.

EIRP is a very important parameter because it is regulated by governmental agencies in most countries. In those cases, a system cannot radiate signals higher than a maximum allowable EIRP. To find the EIRP of a system, simply add the transmitter power level to the antenna gain and subtract the cable loss.



$$\text{EIRP} = \text{Tx Power} - \text{Tx Cable} + \text{Tx Antenna}$$

Suppose a transmitter is configured for a power level of 10 dBm (10 mW). A cable with 5-dB loss connects the transmitter to an antenna with an 8-dBi gain. The resulting EIRP of the system is 10 dBm – 5 dB + 8 dBi, or 13 dBm.

You might notice that the EIRP is made up of decibel-milliwatt (dBm), dB relative to an isotropic antenna (dBi), and decibel (dB) values. Even though the units appear to be different, you can safely combine them because they are all in the dB “domain”.

Reference: CCNA Wireless 640-722 Official Cert Guide

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[EIGRP & OSPF 2 Quiz Architecture Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)

- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)

- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training
[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Wireless 3 Quiz

Wireless 3 Quiz

January 29th, 2021 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Wireless 3 Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
12	170	90%	170	100.00%	00:01:36

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

Which DHCP option provides the CAPWAP APs with the address of the wireless controller(s)?

- A. 69
- B. 150
- **C. 43** ✓
- D. 66

Question 2

Refer to the exhibit. Which level message does the WLC send to the syslog server?

The screenshot shows the Cisco IOS configuration interface. On the left is a 'Management' sidebar with options: Summary, SNMP, HTTP-HTTPS, Telnet-SSH, Serial Port, Local Management Users, User Sessions, Logs (selected), Config, Message logs, Mgmt Via Wireless, and Tech Support. The main area is divided into two sections:

- Syslog Server:** Shows a server at 192.168.100.2 with a 'Remove' link. Below are settings: Syslog Level (Errors), Syslog Facility (Local Use 0), IPsec (unchecked), and IPsec Profile Name (none).
- Msg Log Configuration:** Shows settings for buffered logs: Buffered Log Level (Errors), Console Log Level (Disable), File Info (checked), Trace Info (checked), and Traceback Logging Level (Errors).

- A. syslog level errors messages
- **B. syslog level errors and greater severity messages** ✓
- C. syslog level errors and less severity messages
- D. all syslog levels messages

Question 3

What is the responsibility of a secondary WLC?

- **A. It registers the LAPs if the primary controller fails.** ✓
- B. It shares the traffic load of the LAPs with the primary controller.
- C. It enables Layer 2 and Layer 3 roaming between itself and the primary controller.
- D. It avoids congestion on the primary controller by sharing the registration load on the LAPs.

Explanation

When the primary controller (WLC-1) goes down, the APs automatically get registered with the secondary controller (WLC-2). The APs register back to the primary controller when the primary controller comes back on line.

Reference: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/69639-wlc-failover.html>

Question 4

Which two sources cause interference for Wi-Fi networks? (Choose two)

- **A. mirrored wall** ✓
- B. incandescent lights
- **C. fish tank** ✓
- D. 900MHz baby monitor
- E. DECT 6.0 cordless

Explanation

Windows can actually block your WiFi signal. How? Because the signals will be reflected by the glass.

Some new windows have transparent films that can block certain wave types, and this can make it harder for your WiFi signal to pass through.

Tinted glass is another problem for the same reasons. They sometimes contain metallic films that can completely block out your signal.

Mirrors, like windows, can reflect your signal. They're also a source of electromagnetic interference because of their metal backings.

Reference: <https://dis-dot-dat.net/what-materials-can-block-a-wifi-signal/>

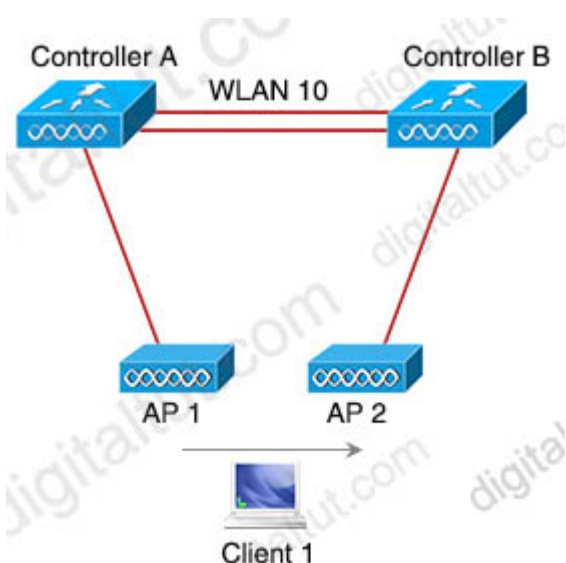
An incandescent light bulb, incandescent lamp or incandescent light globe is an electric light with a wire filament heated until it glows. WiFi operates in the gigahertz microwave band. The FCC has strict regulations on RFI (radio frequency interference) from all sorts of things, including light bulbs -> Incandescent lights do not interfere Wi-Fi networks.

Note:

- + Many baby monitors operate at 900MHz and won't interfere with Wi-Fi, which uses the 2.4GHz band.
 - + DECT cordless phone 6.0 is designed to eliminate wifi interference by operating on a different frequency.
- There is essentially no such thing as DECT wifi interference.

Question 5

Refer to the exhibit.



Both controllers are in the same mobility group. Which result occurs when Client 1 roams between APs that are registered to different controllers in the same WLAN?

- A. CAPWAP tunnel is created between controller A and controller B
- B. Client 1 contact controller B by using an EoIP tunnel
- C. Client 1 users an EoIP tunnel to contact controller A
- **D. The client database entry moves from controller A to controller B** ✓

Explanation

This is called Inter Controller-L2 Roaming. Inter-Controller (normally layer 2) roaming occurs when a client roam between two APs registered to two different controllers, where each controller has an interface in the client subnet. In this instance, controllers exchange mobility control messages (over UDP port 16666) and the client database entry is moved from the original controller to the new controller.

Question 6

What is used to measure the total output energy of a Wi-Fi device?

- A. EIRP
- B. dBi
- **C. mW** ✓
- D. dBm

Explanation

Output power is measured in mW (milliwatts). A milliwatt is equal to one thousandth (10^{-3}) of a watt.

Question 7

Refer to the exhibit.

```
(WLC) >show interface summary
```

Interface Name	Vlan Id
deadnet	999
users1	14
users2	15
users3	16

```
(WLC) >show wlan 1
```

```
WLAN Identifier . . . . . 1
Network Name (SSID) . . . . . wlan1
AAA Policy Override . . . . . Enabled
Interface . . . . . deadnet
FlexConnect Local Switching . . . . . Enabled
FlexConnect Central Association . . . . . Disabled
flexconnect Central Dhcp Flag . . . . . Disabled
flexconnect nat-pat Flag . . . . . Disabled
flexconnect DNS Override Flag . . . . . Disabled
flexconnect PPPoE pass-through . . . . . Disabled
flexconnect local-switching IP-source-guar . . . . . Disabled
FlexConnect Vlan based Central Switching . . . . . Enabled
FlexConnect Local Authentication . . . . . Disabled
FlexConnect Learn IP Address . . . . . Enabled
```

```
(WLC) >show ap config general FlexAP1
```

```
AP Mode . . . . . FlexConnect
FlexConnect Vlan mode : . . . . . Enabled
    Native ID : . . . . . 1
    WLAN 1 : . . . . . 10 (AP-Specific)
FlexConnect VLAN ACL Mappings
Vlan : . . . . . 10
    Ingress ACL : . . . . . None
    Egress ACL : . . . . . None
VLAN with least priority : . . . . . 13
FlexConnect Group . . . . . flexgroup1
Group VLAN ACL Mappings
Vlan : . . . . . 11
    Ingress ACL : . . . . . None
    Egress ACL : . . . . . None
Vlan : . . . . . 12
```

A wireless client is connecting to FlexAP1 which is currently working standalone mode. The AAA authentication process is returning the following AVPs:

```
Tunnel-Private-Group-Id(81): 15
Tunnel-Medium-Type(65): IEEE-802(6)
Tunnel-Type(64): VLAN(13)
```

Which three behaviors will the client experience? (Choose three)

- A. While the AP is in standalone mode, the client will be placed in VLAN 13.
- B. When the AP is in connected mode, the client will be placed in VLAN 13.
- C. When the AP transitions to connected mode, the client will remain associated.
- **D. When the AP is in connected mode, the client will be placed in VLAN 15. ✓**
- **E. While the AP is in standalone mode, the client will be placed in VLAN 10. ✓**

- **F. When the AP transitions to connected mode, the client will be de-authenticated.** ✓
- G. While the AP is in standalone mode, the client will be placed in VLAN 15.

Explanation

+ From the output of WLC “show interface summary”, we learned that the WLC has four VLANs: 999, 14, 15 and 16.

+ From the “show ap config general FlexAP1” output, we learned that FlexConnect AP has four VLANs: 10, 11, 12 and 13. Also the WLAN of FlexConnect AP is mapped to VLAN 10 (from the line “WLAN 1: 10 (AP-Specific)).

From the reference at: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide/ch7_HREA.html

FlexConnect VLAN Central Switching Summary

Traffic flow on WLANs configured for Local Switching when FlexConnect APs are in connected mode are as follows:

- + If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the FlexConnect AP database, traffic will switch centrally and the client is assigned this VLAN/Interface returned from the AAA server provided that the VLAN exists on the WLC. (-> as VLAN 15 exists on the WLC so the client in connected mode would be assigned this VLAN -> Answer 'When the AP is in connected mode, the client will be placed in VLAN 15' is correct)
- + If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the FlexConnect AP database, traffic will switch centrally. If that VLAN is also not present on the WLC, the client will be assigned a VLAN/Interface mapped to a WLAN on the WLC.
- + If the VLAN is returned as one of the AAA attributes and that VLAN is present in the FlexConnect AP database, traffic will switch locally.
- + If the VLAN is not returned from the AAA server, the client is assigned a WLAN mapped VLAN on that FlexConnect AP and traffic is switched locally.

Traffic flow on WLANs configured for Local Switching when FlexConnect APs are in standalone mode are as follows:

- + If the VLAN returned by the AAA server is not present in the FlexConnect AP database, the client will be put on a default VLAN (that is, a WLAN mapped VLAN on a FlexConnect AP) (-> Therefore answer 'While the AP is in standalone mode, the client will be placed in VLAN 10' is correct). When the AP connects back, this client is de-authenticated (-> Therefore answer 'When the AP transitions to connected mode, the client will be de-authenticated' is correct) and will switch traffic centrally.

Question 8

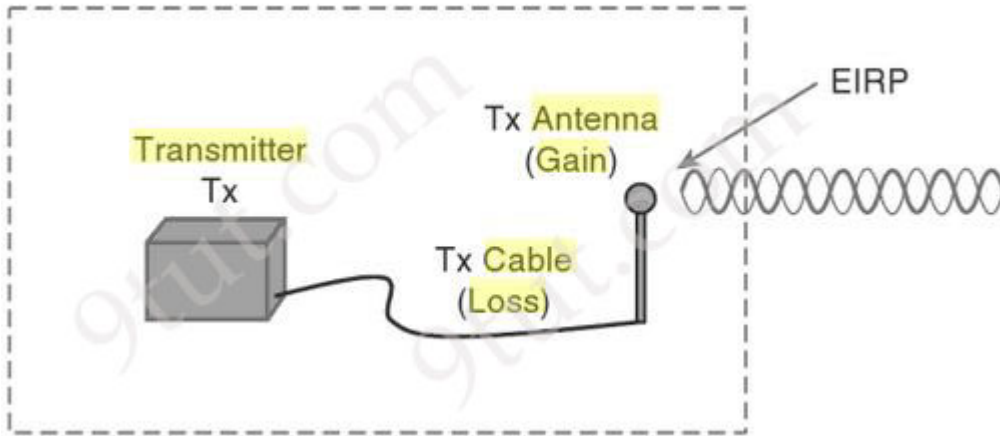
Using the EIRP formula, what parameter is subtracted to determine the EIRP value?

- **A. antenna cable loss** ✓
- B. transmitter power
- C. signal-to-noise ratio
- D. antenna gain

Explanation

Once you know the complete combination of transmitter power level, the length of cable, and the antenna gain, you can figure out the actual power level that will be radiated from the antenna. This is known as the effective isotropic radiated power (EIRP), measured in dBm.

EIRP is a very important parameter because it is regulated by governmental agencies in most countries. In those cases, a system cannot radiate signals higher than a maximum allowable EIRP. To find the EIRP of a system, simply add the transmitter power level to the antenna gain and subtract the cable loss.



$$\text{EIRP} = \text{Tx Power} - \text{Tx Cable} + \text{Tx Antenna}$$

Suppose a transmitter is configured for a power level of 10 dBm (10 mW). A cable with 5-dB loss connects the transmitter to an antenna with an 8-dBi gain. The resulting EIRP of the system is 10 dBm – 5 dB + 8 dBi, or 13 dBm.

You might notice that the EIRP is made up of decibel-milliwatt (dBm), dB relative to an isotropic antenna (dBi), and decibel (dB) values. Even though the units appear to be different, you can safely combine them because they are all in the dB “domain”.

Reference: CCNA Wireless 640-722 Official Cert Guide

Question 9

A wireless consultant is designing a high-density wireless network for a lecture hall for 1000 students. Which antenna type is recommended for this environment?

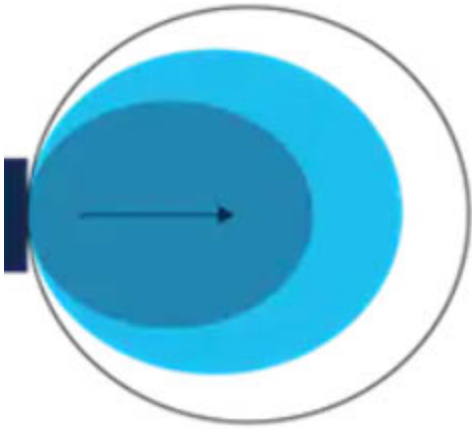
- A. parabolic dish
- **B. omnidirectional antenna** ✓
- C. sector antenna
- D. dipole antenna

Explanation

Directional antennas

Directional antennas come in many different styles and shapes. An antenna does not offer any added power to the signal; it simply redirects the energy it receives from the transmitter. By redirecting this energy, it has the effect of providing more energy in one direction and less energy in all other directions. As the gain of a directional antenna increases, the angle of radiation usually decreases, providing a greater coverage distance but with a reduced coverage angle. Directional antennas include patch antennas and parabolic dishes. Parabolic

dishes have a very narrow RF energy path, and the installer must be accurate in aiming these types of antennas at each other.

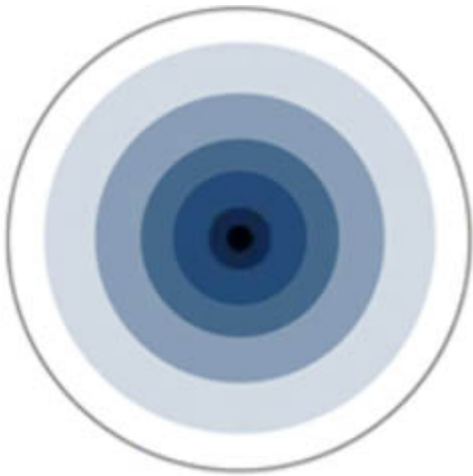


Directional patch antenna

Reference: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/product_data_sheet09186a008008883b.html

Omnidirectional antennas

An omnidirectional antenna is designed to provide a 360-degree radiation pattern. This type of antenna is used when coverage in all directions from the antenna is required. The standard 2.14-dBi “rubber duck” is one style of omnidirectional antenna.



Omnidirectional antenna

-> Therefore Omnidirectional antenna is best suited for a high-density wireless network in a lecture hall.

Question 10

An engineer has deployed a single Cisco 5520 WLC with a management IP address of 172.16.50.5/24. The engineer must register 50 new Cisco AIR-CAP2802I-E-K9 access points to the WLC using DHCP option 43.

The access points are connected to a switch in VLAN 100 that uses the 172.16.100.0/24 subnet. The engineer has configured the DHCP scope on the switch as follows:

Network 172.16.100.0 255.255.255.0
Default Router 172.16.100.1
Option 43 Ascii 172.16.50.5

The access points are failing to join the wireless LAN controller. Which action resolves the issue?

- A. configure option 43 Hex F104.CA10.3205
- **B. configure option 43 Hex F104.AC10.3205** ✓
- C. configure dns-server 172.16.100.1
- D. configure dns-server 172.16.50.5

Explanation

172.16.50.5 in hex is

We will have the answer from this paragraph:

“TLV values for the Option 43 suboption: Type + Length + Value. Type is always the suboption code 0xf1. Length is the number of controller management IP addresses times 4 in hex. Value is the IP address of the controller listed sequentially in hex. For example, suppose there are two controllers with management interface IP addresses, 192.168.10.5 and 192.168.10.20. The type is 0xf1. The length is $2 * 4 = 8 = 0x08$. The IP addresses translates to c0a80a05 (192.168.10.5) and c0a80a14 (192.168.10.20). When the string is assembled, it yields f108c0a80a05c0a80a14. The Cisco IOS command that is added to the DHCP scope is option 43 hex f108c0a80a05c0a80a14.”

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

Therefore in this question the option 43 in hex should be “F104.AC10.3205 (the management IP address of 172.16.50.5 in hex is AC.10.32.05).

Question 11

Which antenna type should be used for a site-to-site wireless connection?

- A. dipole
- **B. Yagi** ✓
- C. Omnidirectional
- D. patch

Question 12

You are configuring a controller that runs Cisco IOS XE by using the CLI. Which three configuration options are used for 802.11w Protected Management Frames? (Choose three)

- **A. saquery-retry-time** ✓
- B. SA teardown protection
- **C. mandatory** ✓
- D. enable
- **E. association-comeback** ✓
- F. comeback-time

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real I



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[GRE Tunnel Quiz](#) [AAA Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)

- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)
- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)

- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH

[Home](#) > Wireless Quiz

Wireless Quiz

May 13th, 2020 in [ENCOR Quizzes](#) [Go to comments](#)

Result of Wireless Quiz:

Total Questions	Full Score	Passing Rate	Your Score	Correct Answer Percentage	Elapsed
15	190	90%	190	100.00%	00:00:46

Congratulations!

You passed this test!

If you want to retake this quiz, please press Ctrl + F5 on Windows or press CMD + R on Mac.

Your answers are shown below:

Question 1

What are two common sources of interference for WI-FI networks? (Choose two)

- **A. radar** ✓
- B. LED lights
- **C. rogue AP** ✓
- D. conventional oven
- E. fire alarm

Explanation

According to the [Meraki webpage](#), radar and rogue AP are two sources of Wireless Interference.

Interference between different WLANs occurs when the access points within range of each other are set to the same RF channel.

Note: Microwave ovens (not conventional oven) emit damaging interfering signals at up to 25 feet or so from an operating oven. Some microwave ovens emit radio signals that occupy only a third of the 2.4-GHz band, whereas others occupy the entire band.

Reference: <https://www.ciscopress.com/articles/article.asp?p=2351131&seqNum=2>

So answer 'conventional oven' is not a correct answer.

Question 2

Refer to the exhibit. The WLC administrator sees that the controller to which a roaming client associates has Mobility Role Anchor configured under Clients > Detail. Which type of roaming is supported?

Clients > Detail

Client Properties

MAC Address	00:09:ee:12:34:d2
IP Address	192.168.100.199
Client Type	Regular
User Name	
Port Number	20
Interface	00:09:ee:12:34:d2
VLAN ID	3602
CCX Version	Not Supported
E2E Version	E2Ev1
Mobility Role	Anchor
Mobility Peer IP Address	172.22.253.20
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	944581
Power Save Mode	OFF
Current TxRateSet	48.0
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

AP Properties

AP Address	
AP Name	172.22.253.20
AP Type	Mobile
WLAN Profile	
Status	Associated
Association ID	16
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Enable

- A. Layer 2 intercontroller
- **B. Layer 3 intercontroller** ✓
- C. Indirect
- D. Intercontroller

Explanation

If the clients roam between APs registered to different controllers and the client WLAN on the two controllers is on different subnet, then it is called inter-controller L3 roam.

In this situation as well controllers exchange mobility messages. Client database entry change is completely different that to L2 roam (instead of move, it will copy). In this situation the original controller marks the client entry as “**Anchor**” where as new controller marks the client entry as “Foreign”. The two controllers now referred to as “Anchor controller” & “Foreign Controller” respectively. Client will keep the original IP address & that is the real advantage.

Note: Inter-Controller (normally layer 2) roaming occurs when a client roam between two APs registered to two different controllers, where each controller has an interface in the client subnet.

Question 3

An engineer configures a WLAN with fast transition enabled. Some legacy clients fail to connect to this WLAN. Which feature allows the legacy clients to connect while still allowing other clients to use fast transition based on their OLTIs?

- **A. adaptive R** ✓
- B. 802.11V
- C. 802.11k

- D. over the DS

Explanation

802.11r Fast Transition (FT) Roaming is an amendment to the 802.11 IEEE standards. It is a new concept for roaming. The initial handshake with the new AP occurs before client roams to the target AP. Therefore it is called Fast Transition. 802.11r provides two methods of roaming:

- + Over-the-air: With this type of roaming, the client communicates directly with the target AP using IEEE 802.11 authentication with the Fast Transition (FT) authentication algorithm.
- + **Over-the-DS** (distribution system): With this type of roaming, the client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the controller.

But both of these methods do not deal with legacy clients.

The **802.11k** allows 11k capable clients to request a neighbor report containing information about known neighbor APs that are candidates for roaming.

Reference: <https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html>

IEEE **802.11v** is an amendment to the IEEE 802.11 standard which describes numerous enhancements to wireless network management. One such enhancement is Network assisted Power Savings which helps clients to improve the battery life by enabling them to sleep longer. Another enhancement is Network assisted Roaming which enables the WLAN to send requests to associated clients, advising the clients as to better APs to associate to. This is useful for both load balancing and in directing poorly connected clients.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/802-11v.pdf

Cisco 802.11r supports three modes:

- + Pure mode: only allows 802.11r client to connect
- + Mixed mode: allows both clients that do and do not support FT to connect
- + Adaptive mode: does not advertise the FT AKM at all, but will use FT when supported clients connect

Therefore “Adaptive mode” is the best answer here.

Question 4

Which two descriptions of FlexConnect mode for Cisco APs are true? (Choose two)

- **A. When connected to the controller, FlexConnect APs can tunnel traffic back to the controller** ✓
- B. FlexConnect mode is used when the APs are set up in a mesh environment and used to bridge between each other
- **C. FlexConnect mode is a wireless solution for branch office and remote office deployments** ✓
- D. APs that operate in FlexConnect mode cannot detect rogue APs
- E. FlexConnect mode is a feature that is designed to allow specified CAPWAP-enabled APs to exclude themselves from managing data traffic between clients and infrastructure

Explanation

FlexConnect is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office.

The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. In the connected mode, the FlexConnect access point can also perform local authentication.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html

Question 5

A client device fails to see the enterprise SSID, but other devices are connected to it. What is the cause of this issue?

- A. The broadcast SSID was not manually configured on the client.
- B. The client has incorrect credentials stored for the configured hidden SSID.
- C. The client has incorrect credentials stored for the configured broadcast SSID.
- **D. The hidden SSID was not manually configured on the client. ✓**

Question 6

Which two pieces of information are necessary to compute SNR? (Choose two)

- A. transmit power
- **B. RSSI ✓**
- C. antenna gain
- D. EIRP
- **E. noise floor ✓**

Explanation

Signal to Noise Ratio (SNR) is defined as the ratio of the transmitted power from the AP to the ambient (noise floor) energy present. To calculate the SNR value, we add the Signal Value to the Noise Value to get the SNR ratio. answer 'EIRP' positive value of the SNR ratio is always better.

Here is an example to tie together this information to come up with a very simple RF plan calculator for a single AP and a single client.

- + Access Point Power = 20 dBm
- + 50 foot antenna cable = - 3.35 dB Loss
- + Signal attenuation due to glass wall with metal frame = -6 dB
- + External Access Point Antenna = + 5.5 dBi gain
- + RSSI at WLAN Client = -75 dBm at 100ft from the AP
- + Noise level detected by WLAN Client = -85 dBm at 100ft from the AP

Based on the above, we can calculate the following information.

- + EIRP of the AP at source = $20 - 3.35 + 5.5 = 22.15$ dBm
- + Transmit power as signal passes through glass wall = $22.15 - 6 = 16.15$ dBm
- + **SNR at Client = -75 + -85 = 10 dBm** (difference between Signal and Noise)

Reference:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/CMX/CMX_RFFund.html

Receive Signal Strength Indicator (RSSI) is a measurement of how well your device can hear a signal from an access point or router. It's a value that is useful for determining if you have enough signal to get a good wireless connection.

EIRP tells you what's the actual transmit power of the antenna in milliwatts.

dBm is an abbreviation for "decibels relative to one milliwatt," where one milliwatt (1 mW) equals 1/1000 of a watt. It follows the same scale as dB. Therefore 0 dBm = 1 mW, 30 dBm = 1 W, and -20 dBm = 0.01 mW

Question 7

Which statement about Cisco EAP-FAST is true?

- **A. It does not require a RADIUS server certificate ✓**

- B. It operates in transparent mode
- C. It is an IETF standard.
- D. It requires a client certificate

Explanation

The EAP-FAST protocol is a publicly accessible IEEE 802.1X EAP type that Cisco developed to support customers that cannot enforce a strong password policy and want to deploy an 802.1X EAP type that does not require digital certificates.

EAP-FAST is also designed for simplicity of deployment since it does not require a certificate on the wireless LAN client or on the RADIUS infrastructure yet incorporates a built-in provisioning mechanism.

Reference: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-fixed/72788-CSSC-Deployment-Guide.html>

Question 8

A customer has several small branches and wants to deploy a WI-FI solution with local management using CAPWAP. Which deployment model meets this requirement?

- A. Autonomous
- **B. Mobility express** ✓
- C. SD-Access wireless
- D. Local mode

Explanation

Mobility Express is the ability to use an access point (AP) as a controller instead of a real WLAN controller. But this solution is only suitable for small to midsize, or multi-site branch locations where you might not want to invest in a dedicated WLC. answer 'Autonomous' Mobility Express WLC can support up to 100 APs. Mobility Express WLC also uses CAPWAP to communicate to other APs.

Note: Local mode is the most common mode that an AP operates in. This is also the default mode. In local mode, the LAP maintains a CAPWAP (or LWAPP) tunnel to its associated controller.

Question 9

An engineer is configuring local web authentication on a WLAN. The engineer chooses the Authentication radio button under the Layer 3 Security options for Web Policy. Which device presents the web authentication for the WLAN?

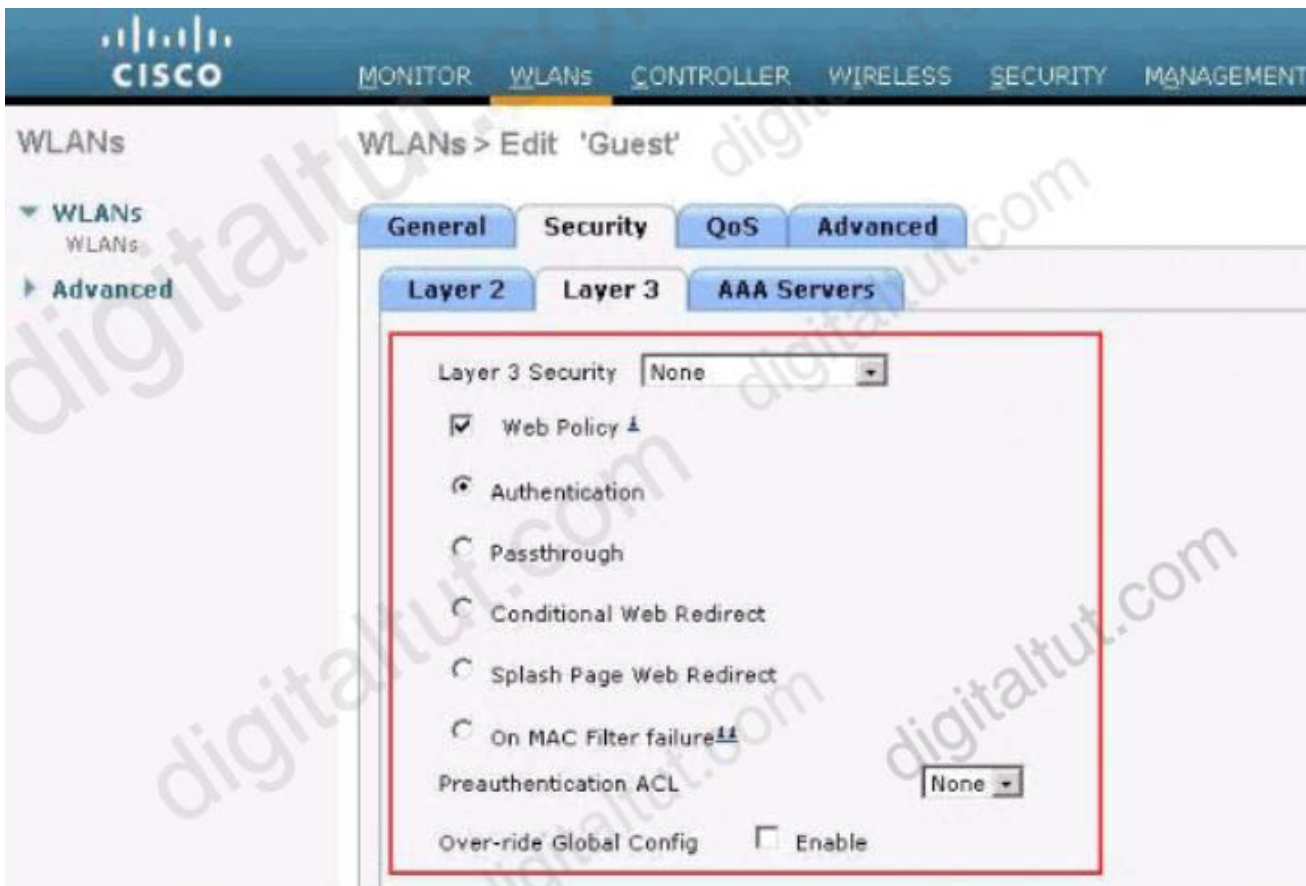
- **A. local WLC** ✓
- B. anchor WLC
- C. ISE server
- D. RADIUS server

Explanation

This paragraph was taken from the link <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/69340-web-auth-config.html#c5>:

“The next step is to configure the WLC for the Internal web authentication. **Internal web authentication is the default web authentication type on WLCs.**”

In step 4 of the link above, we will configure Security as described in this question. Therefore we can deduce this configuration is for Internal web authentication.



Question 10

To increase total throughput and redundancy on the links between the wireless controller and switch, the customer enabled LAG on the wireless controller. Which EtherChannel mode must be configured on the switch to allow the WLC to connect?

- A. Auto
- **B. On** ✓
- C. Active
- D. Passive

Explanation

Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller's distribution system ports into a single 802.3ad port channel.

Restriction for Link aggregation:

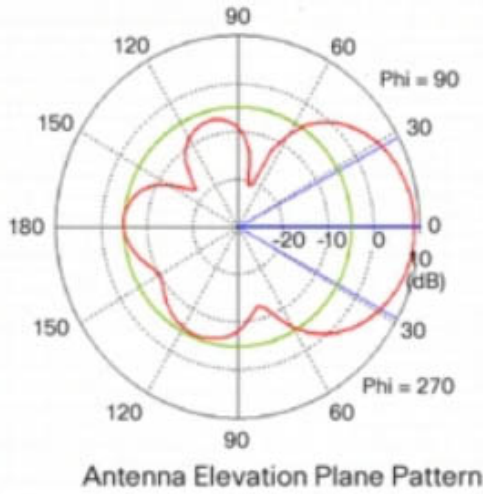
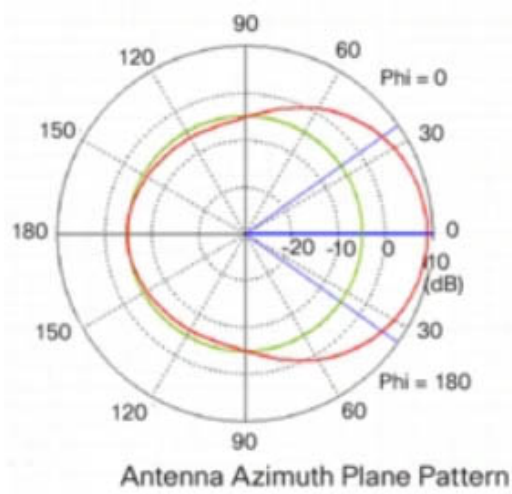
+ LAG requires the EtherChannel to be configured for 'mode on' on both the controller and the Catalyst switch.

...

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_0100010.html

Question 11

Refer to the exhibit. Which type of antenna do the radiation patterns present?

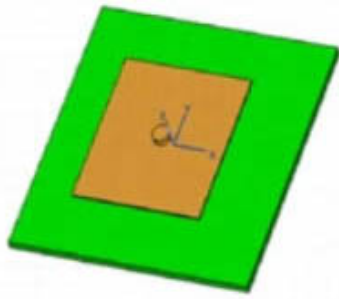


- A. Yagi
- **B. Patch** ✓
- C. Omnidirectional
- D. Dipole

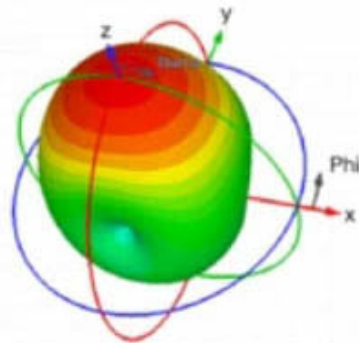
Explanation

A patch antenna, in its simplest form, is just a single rectangular (or circular) conductive plate that is spaced above a ground plane. Patch antennas are attractive due to their low profile and ease of fabrication.

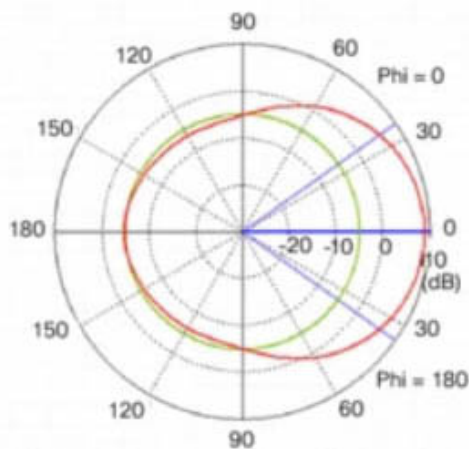
The azimuth and elevation plane patterns are derived by simply slicing through the 3D radiation pattern. In this case, **the azimuth plane pattern is obtained by slicing through the x-z plane, and the elevation plane pattern is formed by slicing through the y-z plane.** Note that there is one main lobe that is radiated out from the front of the antenna. There are three back lobes in the elevation plane (in this case), the strongest of which happens to be 180 degrees behind the peak of the main lobe, establishing the front-to-back ratio at about 14 dB. That is, the gain of the antenna 180 degrees behind the peak is 14 dB lower than the peak gain.



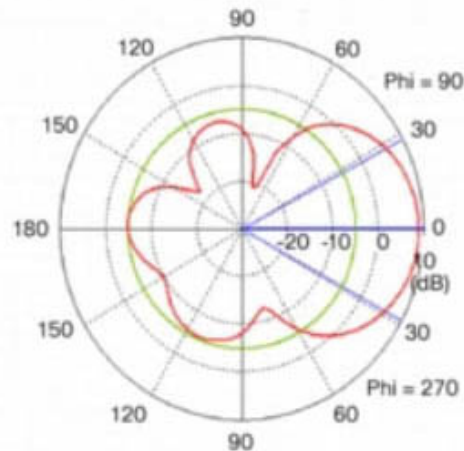
(a) Patch Antenna Model



(b) Patch Antenna 3D Radiation Pattern



(c) Patch Antenna Azimuth Plane Pattern



(d) Patch Antenna Elevation Plane Pattern

Again, it doesn't matter if these patterns are shown pointing up, down, to the left or to the right. That is usually an artifact of the measurement system. answer 'Patch' patch antenna radiates its energy out from the front of the antenna. That will establish the true direction of the patterns.

Reference: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html

Question 12

Refer to the exhibit. Based on the configuration in this WLAN security setting. Which method can a client use to authenticate to the network?

General **Security** **QoS** **Policy-Mapping**

Layer 2 **Layer 3** **AAA Servers**

Fast Transition

Fast Transition ☐

Protected Management Frame

PMF Disabled ▾

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy-AES ☒

Authentication Key Management

802.1X ☐ Enable

CCKM ☐ Enable

PSK ☒ Enable

FT 802.1X ☐ Enable

FT PSK ☐ Enable

PSK Format ASCII ▾

.....

- A. RADIUS token
- B. certificate
- **C. text string** ✓
- D. username and password

Question 13

Which DNS lookup does an access point perform when attempting CAPWAP discovery?

- A. CISCO-DNA-CONTROILLER.local
- B. CAPWAP-CONTROLLER.local
- **C. CISCO-CAPWAP-CONTROLLER.local** ✓
- D. CISCO-CONTROLLER.local

Explanation

The Lightweight AP (LAP) can discover controllers through your domain name server (DNS). For the access point (AP) to do so, you must configure your DNS to return controller IP addresses in response to **CISCO-LWAPP-CONTROLLER.localdomain**, where localdomain is the AP domain name. When an AP receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the AP sends discovery requests to the controllers.

The AP will attempt to resolve the DNS name **CISCO-CAPWAP-CONTROLLER.localdomain**. When the AP is able to resolve this name to one or more IP addresses, the AP sends a unicast CAPWAP Discovery Message to the resolved IP address(es). Each WLC that receives the CAPWAP Discovery Request Message replies with a unicast CAPWAP Discovery Response to the AP.

Reference: <https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107606-dns-wlc-config.html>

Question 14

Which two methods are used by an AP that is trying to discover a wireless LAN controller? (Choose two)

- **A. DHCP Option 43** ✓
- B. querying other APs
- **C. broadcasting on the local subnet** ✓
- D. Cisco Discovery Protocol neighbor
- E. DNS lookup cisco-DNA-PRIMARY.local domain

Explanation

A Cisco lightweight wireless AP needs to be paired with a WLC to function.

An AP must be very diligent to discover any controllers that it can join—all without any preconfiguration on your part. To accomplish this feat, several methods of discovery are used. The goal of discovery is just to build a list of live candidate controllers that are available, using the following methods:

- + Prior knowledge of WLCs
- + DHCP and DNS information to suggest some controllers (DHCP Option 43)
- + Broadcast on the local subnet to solicit controllers

Reference: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

If you do not tell the LAP where the controller is via DHCP option 43, DNS resolution of “Cisco-capwap-controller.local_domain”, or statically configure it, the LAP does not know where in the network to find the management interface of the controller.

In addition to these methods, the LAP does automatically look on the local subnet for controllers with a 255.255.255.255 local broadcast.

Reference: <https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html>

Question 15

When configuration WPA2 Enterprise on a WLAN, which additional security component configuration is required?

- A. NTP server
- **B. RADIUS server** ✓
- C. PKI server
- D. TACACS server

Explanation

Deploying WPA2-Enterprise requires a RADIUS server, which handles the task of authenticating network users access. The actual authentication process is based on the 802.1X policy and comes in several different systems labelled EAP. Because each device is authenticated before it connects, a personal, encrypted tunnel is effectively created between the device and the network.

Reference: <https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified/>

Comments

1. No comments yet.

1. No trackbacks yet.

Add a Comment

Nickname (Please don't use real i



I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Comment

[Subscribe to comments feed](#)

[HSRP & VRRP Quiz](#) [BGP Quiz](#)

Premium Member Zone

Welcome [Ashwin Theran!](#)

- [Welcome Premium Member!](#)
- [New ENCOR Questions](#)
- [New ENCOR Questions- Part 2](#)
- [New ENCOR Questions- Part 3](#)
- [New ENCOR Questions- Part 4](#)
- [Composite Quizzes](#)
- [Logout](#)

ENCOR 350-401

- [Architecture Questions](#)
- [Etherchannel Questions](#)
- [Trunking Questions](#)
- [SD-WAN & SD-Access Solutions](#)
- [SD-WAN & SD-Access Solutions 2](#)
- [SD-WAN & SD-Access Solutions 3](#)
- [QoS Questions](#)
- [Switching Mechanism Questions](#)
- [Virtualization Questions](#)
- [Virtualization Questions 2](#)
- [LISP & VXLAN Questions](#)
- [EIGRP & OSPF Questions](#)
- [EIGRP & OSPF Questions 2](#)
- [BGP Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [Wireless Questions 3](#)
- [HSRP & VRRP Questions](#)
- [HSRP & VRRP Questions 2](#)
- [Network Assurance Questions](#)
- [IP SLA Questions](#)

- [NetFlow Questions](#)
- [SPAN Questions](#)
- [Troubleshooting Questions](#)
- [AAA Questions](#)
- [GRE Tunnel Questions](#)
- [NAT Questions](#)
- [STP Questions](#)
- [DNA Center Questions](#)
- [Security Questions](#)
- [Access-list Questions](#)
- [Access-list Questions 2](#)
- [Multicast Questions](#)
- [NTP Questions](#)
- [CoPP Questions](#)
- [Automation Questions](#)
- [Automation Questions 2](#)
- [Automation Questions 3](#)
- [Miscellaneous Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [ENCOR FAQs & Tips](#)
- [Share your ENCOR Experience](#)

ENCOR Self-Study

- [Basic Labs](#)
- [ENCOR Knowledge](#)

Network Resources

- [CCNA Website](#)
- [ENCOR Website](#)
- [ENSDWI Website](#)
- [ENARSI Website](#)
- [DevNet Website](#)
- [CCIE R&S Website](#)
- [Security Website](#)
- [Wireless Website](#)
- [Design Website](#)
- [Data Center Website](#)
- [Service Provider Website](#)
- [JNCIA - Junos Website](#)

[Top](#)



Copyright © 2020 ENCOR Training

[Privacy Policy](#). Valid XHTML 1.1 and CSS 3.IH