



Cisco

Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Topic 4)

Graphical user interface, text, application, email Description automatically generated

Refer to the Exhibit. Running the script causes the output in the exhibit. What should be the first line of the script?

- A. from ncclient import manager
- B. import manager
- C. from ncclient import *
- D. ncclient manager import

Answer: C

NEW QUESTION 2

- (Topic 4)

```
SW1# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
-----+-----+-----+-----
1 Po1(S D ) PAgP Gi1/0(I) Gi1/1(I)

SW2# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
-----+-----+-----+-----
1 Po1(S D ) LACP Gi1/0(I) Gi1/1(I)
```

Refer to the exhibit. The EtherChannel between SW1 and SW2 is not operational. Which action will resolve the issue?

- A. Configure channel-group 1 mode active on GVO and G1 1 of SW2.
- B. Configure trunks on SW1 and SW2.
- C. Configure channel-group 1 mode active on Gi0 and Gi1 of SW1.
- D. Configure switchport mode dynamic desirable on SW1 and SW2

Answer: C

NEW QUESTION 3

- (Topic 4)

```
FastEthernet1/0/47 - Group 1 (version 2)
State is Standby
 7 state changes, last state change 00:00:02
Virtual IP address is 10.1.1.1
Active virtual MAC address is 0000.0c9f.f001
  Local virtual MAC address is 0000.0c9f.f001 (v2 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.375 secs
Authentication MD5, key-string "cisco"
Preemption enabled, delay min 5 secs
Active router is 10.1.1.2, priority 255 (expires in 9.396 sec)
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fal/0/47-1" (default)
```

Refer to the exhibit. An engineer configures HSRP and enters the show standby command. Which two facts about the network environment are derived from the output? (Choose two.)

- A. The local device has a higher priority selling than the active router
- B. The virtual IP address of the HSRP group is 10.1.1.1.
- C. If the local device fails to receive a hello from the active router for more than 5 seconds, it becomes the active router.
- D. The hello and hold timers are set to custom values.
- E. If a router with a higher IP address and same HSRP priority as the active router becomes available, that router becomes the new active router 5 seconds later.

Answer: BE

NEW QUESTION 4

- (Topic 4)

Which activity requires access to Cisco DNA Center CLI?

- A. provisioning a wireless LAN controller
- B. creating a configuration template
- C. upgrading the Cisco DNA Center software
- D. graceful shutdown of Cisco DNA Center

Answer: D

NEW QUESTION 5

- (Topic 4)

Refer to the exhibit.

```
Router#show running-config | include aaa
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
aaa session-id common
```

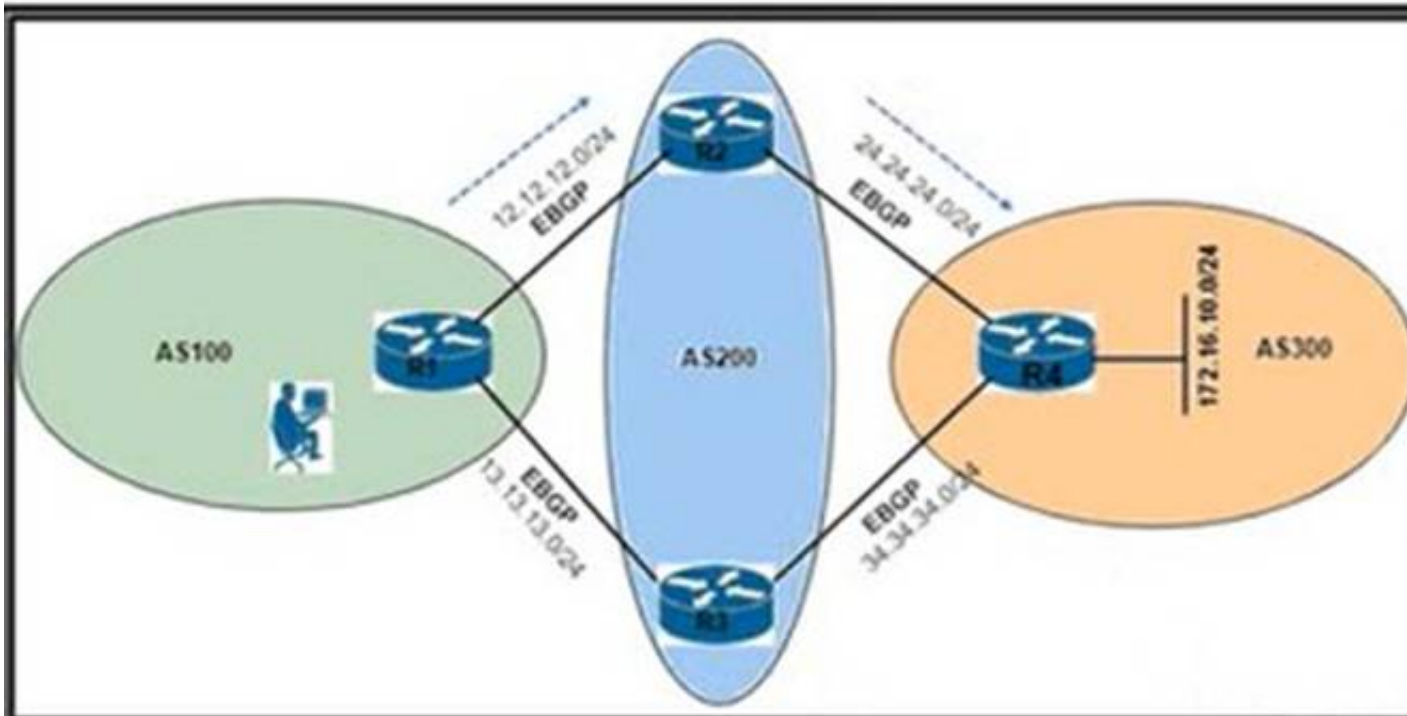
Which configuration enables fallback to local authentication and authorization when no TACACS+ server is available?

- A. Router(config)# aaa authentication login default local Router(config)# aaa authorization exec default local
- B. Router(config)# aaa authentication login default group tacacs+ local Router(config)# aaa authorization exec default group tacacs+ local
- C. Router(config)# aaa fallback local
- D. Router(config)# aaa authentication login FALLBACK local Router(config)# aaa authorization exec FALLBACK local

Answer: B

NEW QUESTION 6

- (Topic 4)



```
R1#sh ip bgp
BGP table version is 2, local router ID is 13.13.13.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
                r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter,
                x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
   Network          Next           Weight      Path
Hop  Metric      LocPrf
* 172.16.1.0/24      13.13.13.3          0
  200 300 i
*>
    12.12.12.2          0
  200 300 i
```

Refer to the exhibit. An engineer is reaching network 172.16.10.0/24 via the R1-R2-R4 path. Which configuration forces the traffic to take a path of R1-R3-R4?
A)

```
R2(config)#route-map RM_MED permit 10
R2(config-route-map)#set metric 1
R2(config-route-map)#exit
R2(config)#router bgp 200
R2(config-router)#neighbor 12.12.12.1 route-map RM_MED out
R2(config-router)#end
R2#clear ip bgp 12.12.12.1 soft out
```

B)

```
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 weight 1
R1(config-router)#end
```

C)

```
R1(config)#route-map RM_AS_PATH_PREPEND
R1(config-route-map)#set as-path prepend 200 200
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 12.12.12.2 route-map RM_AS_PATH_PREPEND in
R1(config-router)#end
R1#clear ip bgp 12.12.12.2 soft in
```

D)

```
R1(config)#route-map RM_LOCAL_PREF permit 10
R1(config-route-map)#set local-preference 101
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 route-map RM_LOCAL_PREF in
R1(config-router)#end
R1#clear ip bgp 13.13.13.3 soft in
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 7

- (Topic 4)

An engineer must configure router R1 to validate user logins via RADIUS and fall back to the local user database if the RADIUS server is not available. Which configuration must be applied?

- A. aaa authorization exec default radius local
- B. aaa authorization exec default radius
- C. aaa authentication exec default radius local
- D. aaa authentication exec default radius

Answer: C

NEW QUESTION 8

- (Topic 4)

A customer requires their wireless network to be fully functional, even if the wireless controller fails. Which wireless design supports these requirements?

- A. FlexConnect
- B. mesh
- C. centralized
- D. embedded

Answer: A

Explanation:

This is because FlexConnect is a feature that allows wireless access points to operate in standalone mode when they lose connectivity to the wireless LAN controller. FlexConnect enables the access points to switch the data traffic locally, without sending it to the controller, and to perform local authentication, without relying on the central server. FlexConnect also allows the access points to maintain the wireless network functionality, such as SSIDs, security policies, and QoS, even if the wireless controller fails. FlexConnect is suitable for branch locations or remote offices that have limited WAN bandwidth or reliability. The source of this answer is the Cisco ENCOR v1.1 course, module 7, lesson 7.3: Implementing FlexConnect.

NEW QUESTION 9

- (Topic 4)

What is a benefit of Cisco TrustSec in a multilayered LAN network design?

- A. Policy or ACLS are nor required.
- B. There is no requirements to run IEEE 802.1X when TrustSec is enabled on a switch port.
- C. Applications flows between hosts on the LAN to remote destinations can be encrypted.
- D. Policy can be applied on a hop-by-hop basis.

Answer: C

NEW QUESTION 10

- (Topic 4)

Which JSON script is properly formatted?

A)

```
"car":{
  {
    "type":"A New Book",
    "model":"J Doe",
    "year":"1"
  }
}
```

B)

```
{
  "host":
  {
    "name":"SwitchA,
    "model":"Catalyst",
    "serial":"0438045649",
  }
}
```

C)

```
{
  "book": [
    {
      "title": "A New Book",
      "author": "J P Doe",
      "edition": "2"
    }
  ]
}
```

D)

```
{
  "class": {
    "title": "Science",
    "grade": "11",
    "location": "Room C"
  }
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 10

- (Topic 4)

```
S1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3     S - Layer2
      U - in use     f - failed to allocate aggregator

      M - not in use, minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1 (SD)          -         Fa0/1 (D) Fa0/2 (D)

S1# show run | begin interface port-channel
interface Port-channel1
switchport mode trunk
|
interface FastEthernet0/1
switchport mode trunk
channel-group 1 mode on
|
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode on
|
<Output omitted>
```

```
S2# show run | begin interface port-channel
interface Port-channel1
switchport mode trunk
|
interface FastEthernet0/1
switchport mode trunk
channel-group 1 mode desirable
|
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode desirable
|
<Output omitted>
```

Refer to the exhibit. Traffic is not passing between SW1 and SW2. Which action fixes the issue?

- A. Configure LACP mode on S1 to passive.
- B. Configure switch port mode to ISL on S2.
- C. Configure PAgP mode on S1 to desirable.
- D. Configure LACP mode on S1 to active.

Answer: C

NEW QUESTION 14

- (Topic 4)

Which Python code snippet must be added to the script to store the changed interface configuration to a local JSON-formatted file?

```
import json
import requests

Creds = ("user", "Z#418208328$mnV")
Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

BaseURL = https://cpe/restconf/data"
URL = BaseURL + "/Cisco-IOS-XE-native:native/interface"

Response = requests.get(URL, auth = Creds, headers = Headers, verify = False)
UpdatedConfig = Response.text.replace("2001:db8:1:", "2001:db8:café:"
```

- ☐ `OutFile = open("ifaces.json", "w")`
`json.dump(UpdatedConfig, OutFile)`
`OutFile.close()`
- ☐ `OutFile = open("ifaces.json", "w")`
`OutFile.write(UpdatedConfig)`
`OutFile.close()`
- ☐ `OutFile = open("ifaces.json", "w")`
`OutFile.write(Response.text)`
`OutFile.close()`
- ☐ `OutFile = open("ifaces.json", "w")`
`OutFile.write(Response.json())`
`OutFile.close()`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 17

DRAG DROP - (Topic 4)

Drag and drop the automation characteristics from the left onto the corresponding tools on the right. Not all options are used.

based on Python

proprietary syntax in configuration files based on Ruby

high availability offered through a multi-primary architecture

Ruby syntax in configuration files

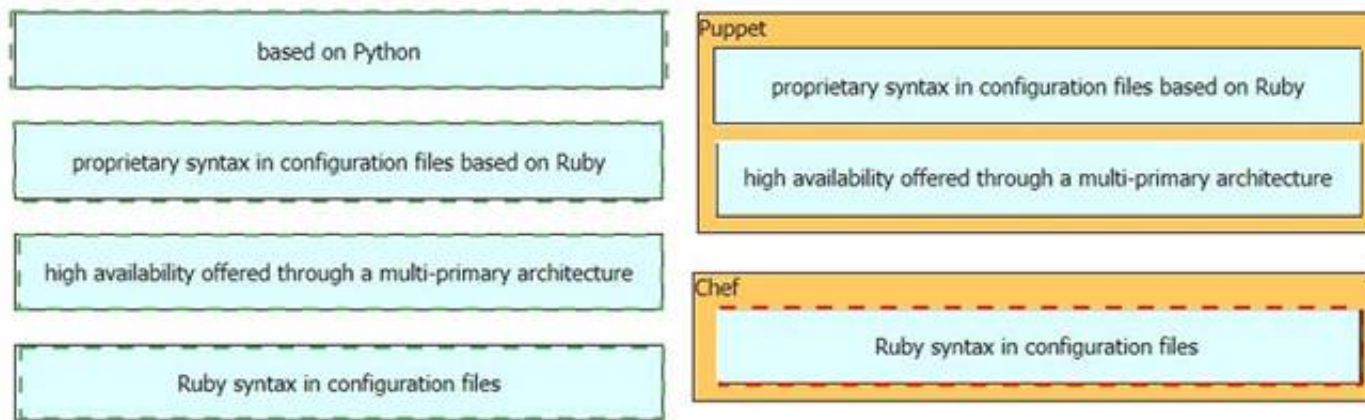
Puppet

Chef

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 20

- (Topic 4)

Which DNS lookup does an access point perform when attempting CAPWAP discovery?

- A. CISCO-DNA-CONTROLLER local
- B. CAPWAP-CONTROLLER local
- C. CISCO-CONTROLLER local
- D. CISCO-CAPWAP-CONTROLLER local

Answer: D

NEW QUESTION 21

- (Topic 4)

A wireless administrator must create a new web authentication corporate SSID that will be using ISE as the external RADIUS server. The guest VLAN must be specified after the authentication completes. Which action must be performed to allow the ISE server to specify the guest VLAN?

- A. Set AAA Policy name.
- B. Enable AAA Override
- C. Set RADIUS Profiling
- D. Enable Network Access Control State.

Answer: C

NEW QUESTION 25

- (Topic 4)

```

line con 0
 password cisco
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 !
end

router#sh run | i username|aaa
no aaa new-model
username user password 0 user
router#
  
```

Refer to the exhibit Which configuration enables password checking on the console line, using only a password?

A)

```

router(config)# line con 0
router(config-line)# exec-timeout 0 0
  
```

B)

```

router(config)# line con 0
router(config-line)# login
  
```

C)

```
router(config)# line con 0
router(config-line)# login local
```

D)

```
router(config)# line vty 0 4
router(config-line)# login
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 29

- (Topic 4)

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.

Answer: D

NEW QUESTION 31

- (Topic 4)

Where in Cisco DNA Center is documentation of each API call, organized by its functional area?

- A. Developer Toolkit
- B. platform management
- C. platform bundles
- D. Runtime Dashboard

Answer: A

Explanation:

<https://developer.cisco.com/docs/dna-center/#!api-quick-start/cisco-dna-center-platform-api-overview>

NEW QUESTION 34

- (Topic 4)

Which function does a Cisco SD-Access extended node perform?

- A. provides fabric extension to nonfabric devices through remote registration and configuration
- B. performs tunneling between fabric and nonfabric devices to route traffic over unknown networks
- C. used to extend the fabric connecting to downstream nonfabric enabled Layer 2 switches
- D. in charge of establishing Layer 3 adjacencies with nonfabric unmanaged node

Answer: C

Explanation:

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKCRS-2832.pdf>

NEW QUESTION 36

- (Topic 4)

Which collection contains the resources to obtain a list of fabric nodes through the vManage API?

- A. device management
- B. administration
- C. device inventory
- D. monitoring

Answer: C

Explanation:

The collection that contains the resources to obtain a list of fabric nodes through the vManage API is the device inventory collection. This collection can be accessed through the Cisco Encor Documents and provides resources such as the Fabric Visualization, Device List, and Fabric Node Inventory APIs. These APIs can be used to obtain information about the fabric nodes, such as the device inventory, status, and version.

NEW QUESTION 38

- (Topic 4)

Where is the wireless LAN controller located in a mobility express deployment?

- A. There is no wireless LAN controller in the network.
- B. The wireless LAN controller is embedded into the access point.
- C. The wireless LAN controller exists in the cloud.
- D. The wireless LAN controller exists in a server that is dedicated for this purpose.

Answer: B

NEW QUESTION 42

DRAG DROP - (Topic 4)

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

uses virtual links to link an area that does not have a connection to the backbone	EIGRP
hello packets are sent by default every 5 seconds on high-bandwidth links	
default cost is based on interface bandwidth only	OSPF
metric is calculated using bandwidth and delay by default	

- A. Mastered
- B. Not Mastered

Answer: A

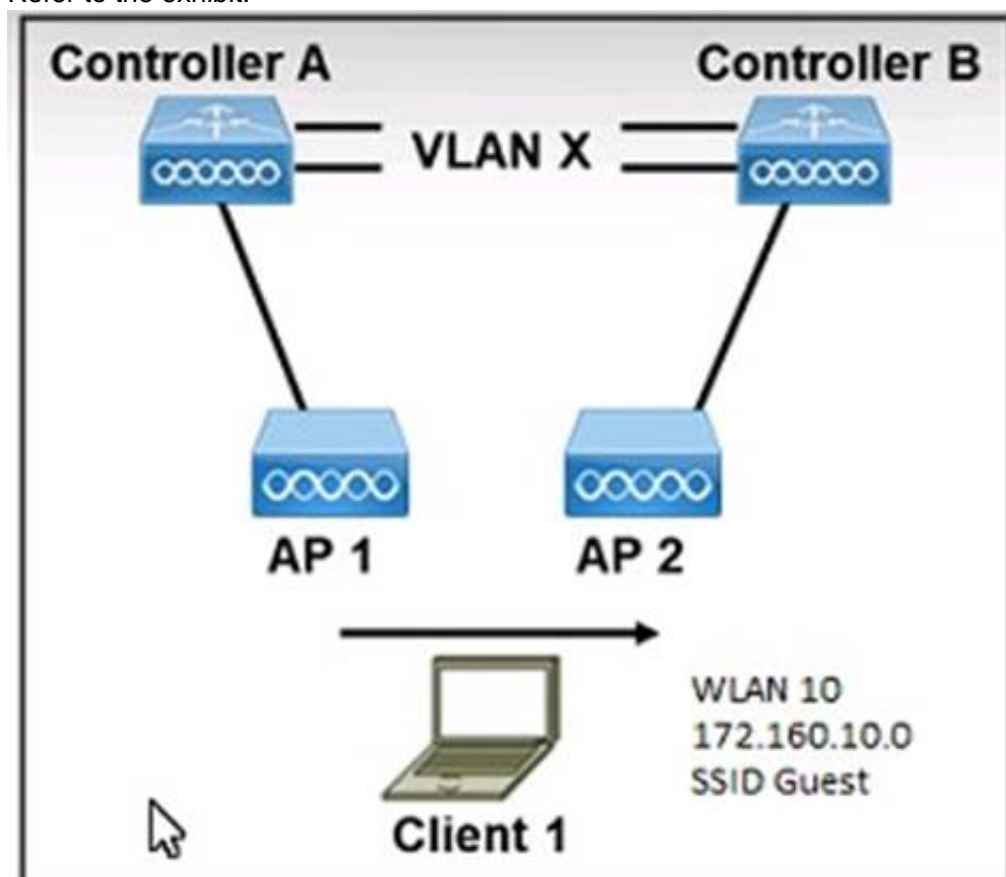
Explanation:

uses virtual links to link an area that does not have a connection to the backbone	EIGRP
hello packets are sent by default every 5 seconds on high-bandwidth links	hello packets are sent by default every 5 seconds on high-bandwidth links
default cost is based on interface bandwidth only	metric is calculated using bandwidth and delay by default
metric is calculated using bandwidth and delay by default	OSPF
	uses virtual links to link an area that does not have a connection to the backbone
	default cost is based on interface bandwidth only

NEW QUESTION 43

- (Topic 4)

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. Client 1 contact controller B by using an EoIP tunnel.
- B. CAPWAP tunnel is created between controller A and controller B.
- C. Client 1 users an EoIP tunnel to contact controller A.
- D. The client database entry moves from controller A to controller B.

Answer: D

NEW QUESTION 46

- (Topic 4)

Based on the router's API output in JSON format below, which Python code will display the value of the "hostname" key?

```
{
  "response": [{
    "family": "Switches",
    "macAddress": "00:42:50:62:99:00",
    "hostname": "SwitchIDF14",
    "upTime": "352 days, 6:17:26:10",
    "lastUpdated": "2020-07-12 21:15:29"
  }]
}
```

- ☐ `json_data = json.loads(response.text)`
`print(json_data[response][0][hostname])`
- ☐ `json_data = json.loads(response.text)`
`print(json_data["response"]["family"]["hostname"])`
- ☐ `json_data = response.json()`
`print(json_data["response"][0]["hostname"])`
- ☐ `json_data = response.json()`
`print(json_data["response"][family][hostname])`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 49

- (Topic 1)

What is used to perform OoS packet classification?

- A. the Options field in the Layer 3 header
- B. the Type field in the Layer 2 frame
- C. the Flags field in the Layer 3 header
- D. the TOS field in the Layer 3 header

Answer: D

Explanation:

Type of service, when we talk about PACKET, means layer 3

NEW QUESTION 52

- (Topic 2)

An engineer must export the contents of the devices object in JSON format. Which statement must be used?


```
from json import dumps, loads

Devices=[
{
    'name' : 'distsw1',
    'ip' : '192.168.255.1',
    'type' : 'Catalyst C9407R',
    'user' : 'netadmin',
    'pass' : '66674431c3577d399739655c0bfb6fe5'
}]
```

- A. json.repr(Devices)
- B. json.dumps(Devices)
- C. json.prints(Devices)
- D. json.loads(Devices)

Answer: B

NEW QUESTION 53

- (Topic 2)

Refer to the exhibit.

```
configure terminal
ip flow-export destination 192.168.10.1 9991
ip flow-export version 9
```

What is required to configure a second export destination for IP address 192.168.10.1?

- A. Specify a VRF.
- B. Specify a different UDP port.
- C. Specify a different flow ID
- D. Configure a version 5 flow-export to the same destination.
- E. Specify a different TCP port.

Answer: B

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

NEW QUESTION 58

- (Topic 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-modelaaa authentication login VTY group tacacs+ none aaa session-id commonR1#sh run | section vty line vty 0 4password 7 0202039485748 R1#sh run | include username R1#
- B. R1#sh run | include aaa aaa new-modelaaa authentication login telnet group tacacs+ none aaa session-id commonR1#sh run | section vty line vty 0 4R1#sh run | include username R1#
- C. R1#sh run | include aaa aaa new-modelaaa authentication login default group tacacs+ none aaa session-id commonR1#sh run | section vty line vty 0 4password 7 0202039485748
- D. R1#sh run | include aaa aaa new-modelaaa authentication login default group tacacs+ aaa session-id commonR1#sh run | section vty line vty 0 4transport input none R1#

Answer: C

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 the 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)

NEW QUESTION 61

DRAG DROP - (Topic 2)

Drag and drop the snippets onto the blanks within the code to construct a script that shows all logging that occurred on the appliance from Sunday until 9:00 p.m Thursday Not all options are used.

```
event manager applet Logging
event timer cron name Logging cron-entry " "
action 2.0 cli command "enable"
action  cli command "show logging | "

```

1.0

3.0

redirect
ftp://cisco:cisco@192.168.1.1

0 21 * * 0-4

0 21 * * 1-5

ftp://cisco:cisco@192.168.1.1

- A. Mastered
B. Not Mastered

Answer: A

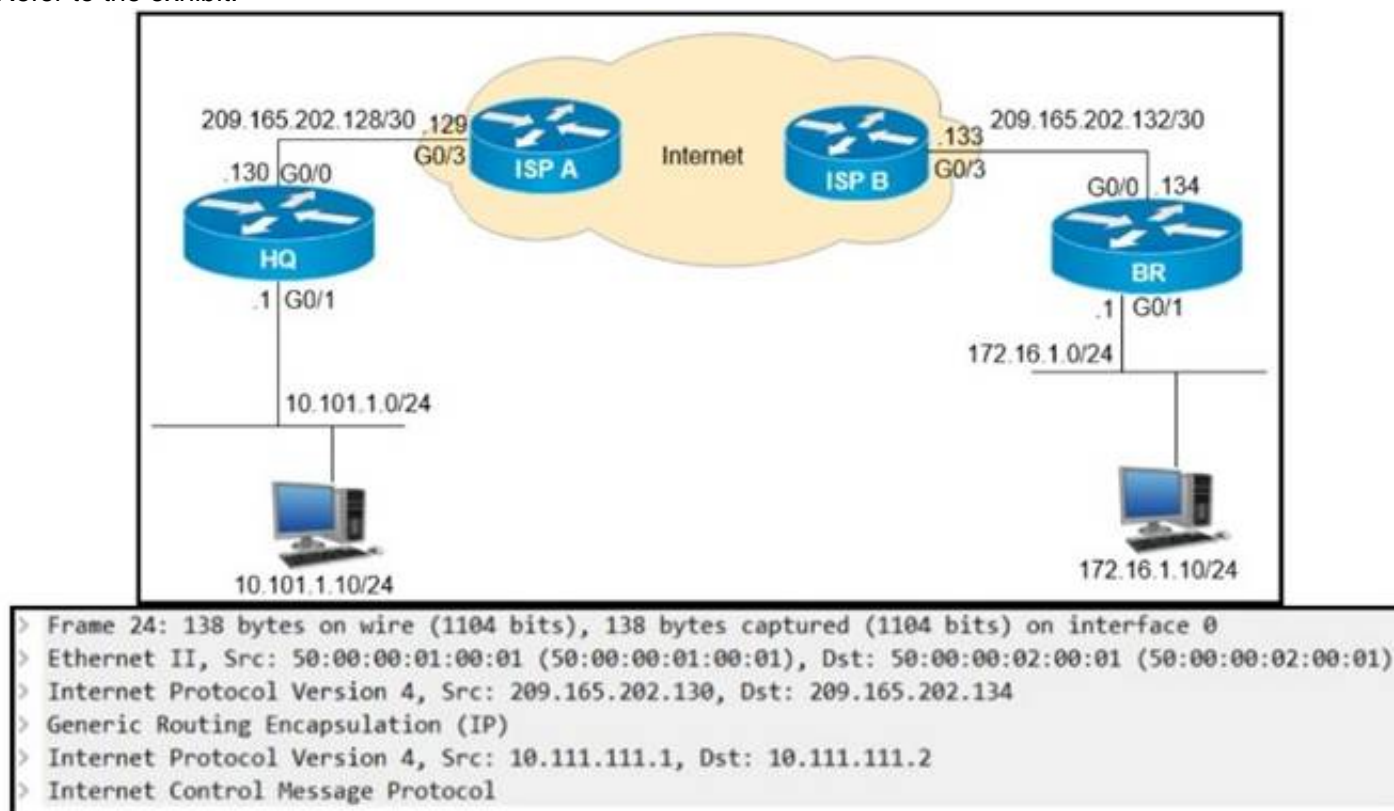
Explanation:

Graphical user interface, text, application Description automatically generated

NEW QUESTION 62

- (Topic 2)

Refer to the exhibit.



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

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

Answer: A

NEW QUESTION 65

- (Topic 2)

In a Cisco SD-WAN solution, which two functions are performed by OMP? (Choose two.)

- A. advertisement of network prefixes and their attributes
B. configuration of control and data policies
C. gathering of underlay infrastructure data
D. delivery of crypto keys

E. segmentation and differentiation of traffic

Answer: AB

Explanation:

OMP is the control protocol that is used to exchange routing, policy, and management information between Cisco vSmart Controllers and Cisco IOS XE SD-WAN devices in the overlay network. These devices automatically initiate OMP peering sessions between themselves, and the two IP end points of the OMP session are the system IP addresses of the two devices.

NEW QUESTION 69

- (Topic 2)

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. SE-connect mode
- C. sensor mode
- D. sniffer mode

Answer: C

Explanation:

As these wireless networks grow especially in remote facilities where IT professionals may not always be onsite, it becomes even more important to be able to quickly identify and resolve potential connectivity issuesideally 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 PerformanceAnalytics, Real-time Client Troubleshooting, and Proactive Health Assessment. Using a supported AP ordedicated sensor the device can actually function much like a WLAN client would associating andidentifying client connectivity issues within the network in real time without requiring an IT or technician to beon 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

NEW QUESTION 73

- (Topic 2)

Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

- A. bridge domain
- B. VLAN
- C. VRF
- D. VNI

Answer: D

Explanation:

VXLAN has a 24-bit VXLAN network identifier (VNI), which allows for up to 16 million (= 224) VXLAN segments to coexist within the same infrastructure. This surely solve the small number of traditional VLANs.

NEW QUESTION 78

DRAG DROP - (Topic 2)

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

The default Administrative Distance is equal to 110.

It requires an Autonomous System number to create a routing instance for exchanging routing information.

It uses virtual links to connect two parts of a partitioned backbone through a non-backbone area.

It is an Advanced Distance Vector routing protocol.

It relies on the Diffused Update Algorithm to calculate the shortest path to a destination.

It requires a process ID that is local to the router.

EIGRP

OSPF

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The default Administrative Distance is equal to 110.	EIGRP
It requires an Autonomous System number to create a routing instance for exchanging routing information.	It requires an Autonomous System number to create a routing instance for exchanging routing information.
It uses virtual links to connect two parts of a partitioned backbone through a non-backbone area.	It is an Advanced Distance Vector routing protocol.
It is an Advanced Distance Vector routing protocol.	It relies on the Diffused Update Algorithm to calculate the shortest path to a destination.
It relies on the Diffused Update Algorithm to calculate the shortest path to a destination.	OSPF
It requires a process ID that is local to the router.	The default Administrative Distance is equal to 110.
	It uses virtual links to connect two parts of a partitioned backbone through a non-backbone area.
	It requires a process ID that is local to the router.

NEW QUESTION 80

- (Topic 2)

An engineer is implementing a Cisco MPLS TE tunnel to improve the streaming experience for the clients of a video-on-demand server. Which action must the engineer perform to configure extended discovery to support the MPLS LDP session between the headend and tailend routers?

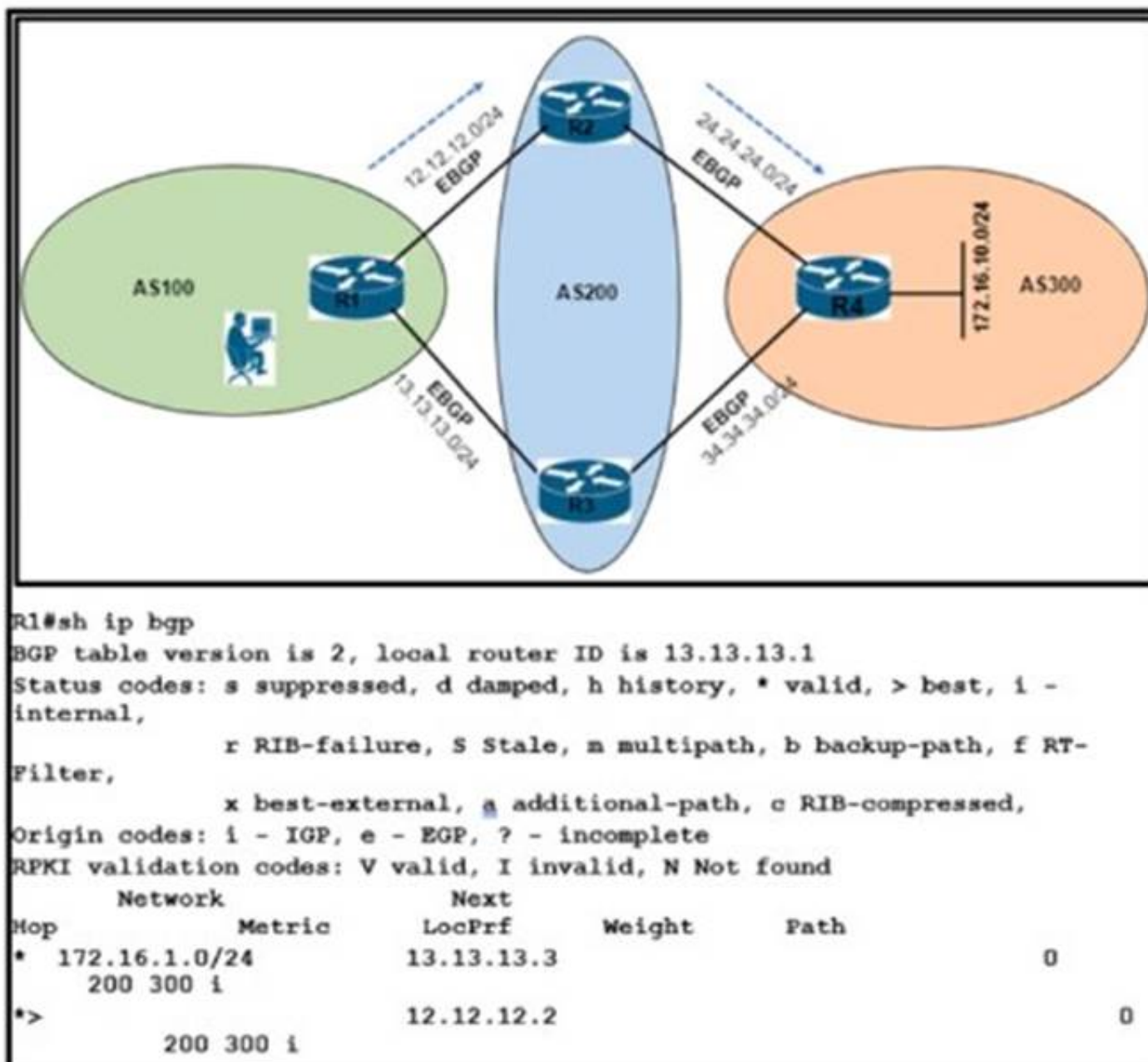
- A. Configure the interface bandwidth to handle TCP and UDP traffic between the LDP peers
- B. Configure a Cisco MPLS TE tunnel on both ends of the session
- C. Configure an access list on the interface to permit TCP and UDP traffic
- D. Configure a targeted neighbor session.

Answer: B

NEW QUESTION 85

- (Topic 2)

Refer to the exhibit.



An engineers reaching network 172 16 10 0/24 via the R1-R2-R4 path. Which configuration forces the traffic to take a path of R1-R3-R4?

A)


```
R1(config)#route-map RM_AS_PATH_PREPEND
R1(config-route-map)#set as-path prepend 200 200
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 12.12.12.2 route-map RM_AS_PATH_PREPEND in
R1(config-router)#end
R1#clear ip bgp 12.12.12.2 soft in
```

B)

```
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 weight 1
R1(config-router)#end
```

C)

```
R2(config)#route-map RM_MED permit 10
R2(config-route-map)#set metric 1
R2(config-route-map)#exit
R2(config)#router bgp 200
R2(config-router)#neighbor 12.12.12.1 route-map RM_MED out
R2(config-router)#end
R2#clear ip bgp 12.12.12.1 soft out
```

D)

```
R1(config)#route-map RM_LOCAL_PREF permit 10
R1(config-route-map)#set local-preference 101
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 route-map RM_LOCAL_PREF in
R1(config-router)#end
R1#clear ip bgp 13.13.13.3 soft in
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 90

- (Topic 2)

Refer to the exhibit.

```
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name SNMP
police:
  cir 8000 bps, bc 1500 bytes
  conformed 0 packets, 0 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    drop
  conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
  13858 packets, 1378745 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any
```

How does the router handle traffic after the CoPP policy is configured on the router?

- A. Traffic coming to R1 that does not match access list SNMP is dropped.
- B. Traffic coming to R1 that matches access list SNMP is policed.
- C. Traffic passing through R1 that matches access list SNMP is policed.
- D. Traffic generated by R1 that matches access list SNMP is policed.

Answer: C

NEW QUESTION 91

- (Topic 2)

A customer wants to provide wireless access to contractors using a guest portal on Cisco ISE. The portal is also used by employees. A solution is implemented, but contractors receive a certificate error when they attempt to access the portal. Employees can access the portal without any errors. Which change must be implemented to allow the contractors and employees to access the portal?

- A. Install a trusted third-party certificate on the Cisco ISE.
- B. Install an Internal CA signed certificate on the contractor devices.
- C. Install an internal CA signed certificate on the Cisco ISE.
- D. Install a trusted third-party certificate on the contractor devices.

Answer: C

NEW QUESTION 93

- (Topic 2)

Which element enables communication between guest VMs within a virtualized environment?

- A. hypervisor
- B. vSwitch
- C. virtual router
- D. pNIC

Answer: B

NEW QUESTION 98

- (Topic 2)

An engineer configures GigabitEthernet 0/1 for VRRP group 115. The router must assume the primary role when it has the highest priority in the group. Which command set is required to complete this task?

```
interface GigabitEthernet0/1
ip address 10.10.10.2 255.255.255.0
vrrp 115 ip 10.10.10.1
vrrp 115 authentication 406530697
```

- ☐ Router(config-if)# vrrp 115 priority 100
- ☐ Router(config-if)# standby 115 priority 100
Router(config-if)# standby 115 preempt
- ☐ Router(config-if)# vrrp 115 track 1 decrement 10
Router(config-if)# vrrp 115 preempt
- ☐ Router(config-if)# vrrp 115 track 1 decrement 100
Router(config-if)# vrrp 115 preempt

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 101

- (Topic 2)

Why would a log file contain a * next to the date?

- A. The network device was receiving NTP time when the log messages were recorded.
- B. The network device was unable to reach the NTP server when the log messages were recorded.
- C. The network device is not configured to use NTP.
- D. The network device is not configured to use NTP time stamps for logging.

Answer: B

NEW QUESTION 103

DRAG DROP - (Topic 2)

Drag and drop the descriptions from the left onto the routing protocol they describe on the right.

summaries can be created anywhere in the IGP topology	OSPF
uses areas to segment a network	
summaries can be created in specific parts of the IGP topology	EIGRP

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

summaries can be created anywhere in the IGP topology

uses areas to segment a network

summaries can be created in specific parts of the IGP topology

OSPF

summaries can be created anywhere in the IGP topology

uses areas to segment a network

EIGRP

summaries can be created in specific parts of the IGP topology

NEW QUESTION 108

- (Topic 2)

Refer to the exhibit.

```
R1#show ip bgp sum
BGP router identifier 1.1.1.1, local AS number 65001
<output omitted>
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.168.50.2	4	65002	0	0	1	0	0	00:00:46	Idle (Admin)

Which command set changes the neighbor state from Idle (Admin) to Active?

- A)
- ```
R1(config)#router bgp 65002
R1(config-router)#neighbor 192.168.50.2 activate
```
- B)
- ```
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 activate
```
- C)
- ```
R1(config)#router bgp 65001
R1(config-router)#no neighbor 192.168.50.2 shutdown
```
- D)
- ```
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 remote-as 65001
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 112

DRAG DROP - (Topic 2)

Drag and drop the characteristics from the left onto the infrastructure deployment models they describe on the right.

easy to scale the capacity up and down

infrastructure requires large and regular investments

highly agile

highly customizable

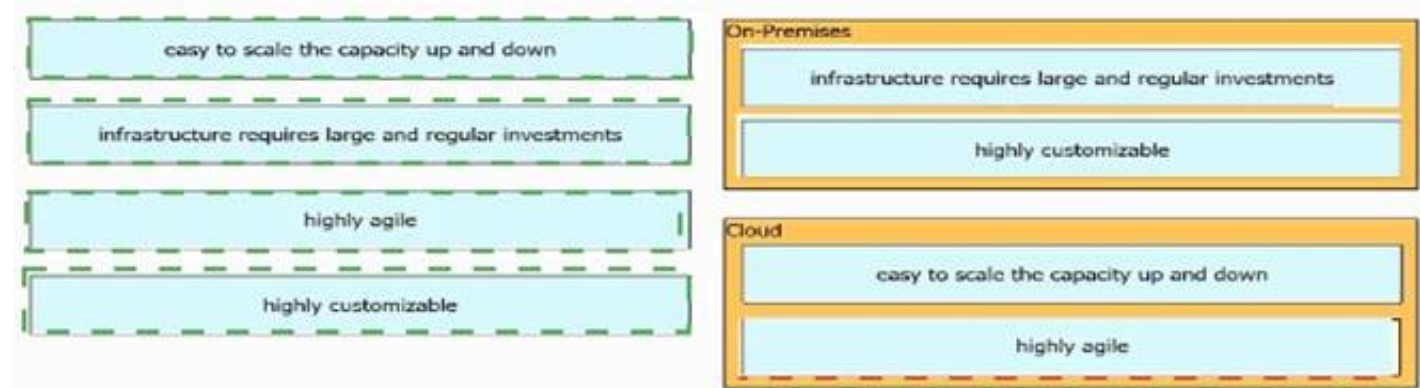
On-Premises

Cloud

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 117

- (Topic 2)

What is the structure of a JSON web token?

- A. three parts separated by dots: header payload, and signature
- B. header and payload
- C. three parts separated by dots: version header and signature
- D. payload and signature

Answer: A

Explanation:

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA.

JSON Web Tokens are composed of three parts, separated by a dot (.): Header, Payload, Signature. Therefore, a JWT typically looks like the following:

xxxxx.yyyyy.zzzzz

The header typically consists of two parts: the type of the token, which is JWT, and the signing algorithm being used, such as HMAC SHA256 or RSA.

The second part of the token is the payload, which contains the claims. Claims are statements about an entity (typically, the user) and additional data.

To create the signature part you have to take the encoded header, the encoded payload, a secret, the algorithm specified in the header, and sign that. Reference: <https://jwt.io/introduction/>

NEW QUESTION 118

- (Topic 2)

Which protocol infers that a YANG data model is being used?

- A. SNMP
- B. NX-API
- C. REST
- D. RESTCONF

Answer: D

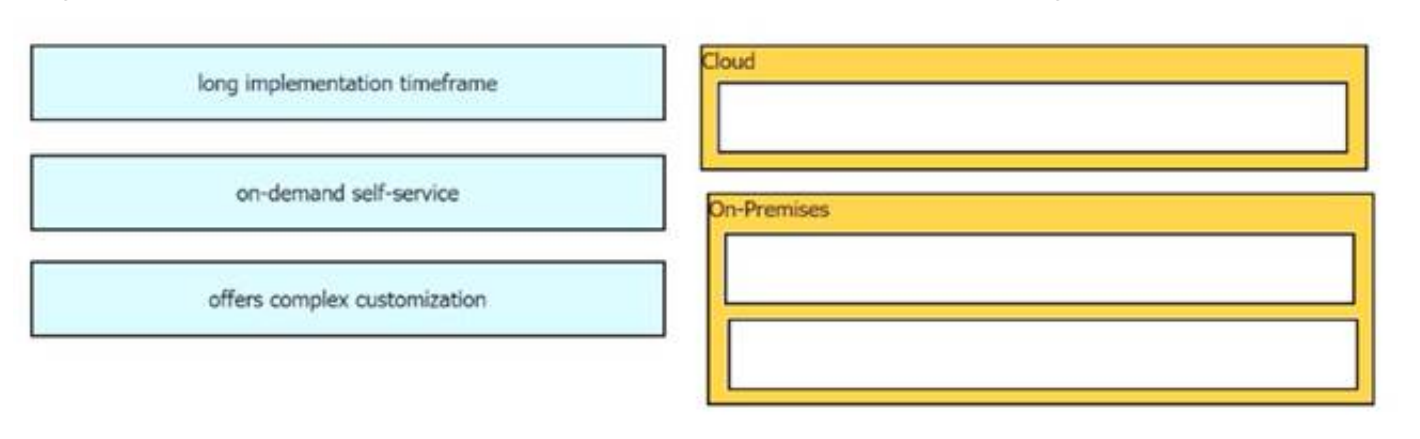
Explanation:

YANG (Yet another Next Generation) is a data modeling language for the definition of data sent over network management protocols such as the NETCONF and RESTCONF.

NEW QUESTION 122

DRAG DROP - (Topic 2)

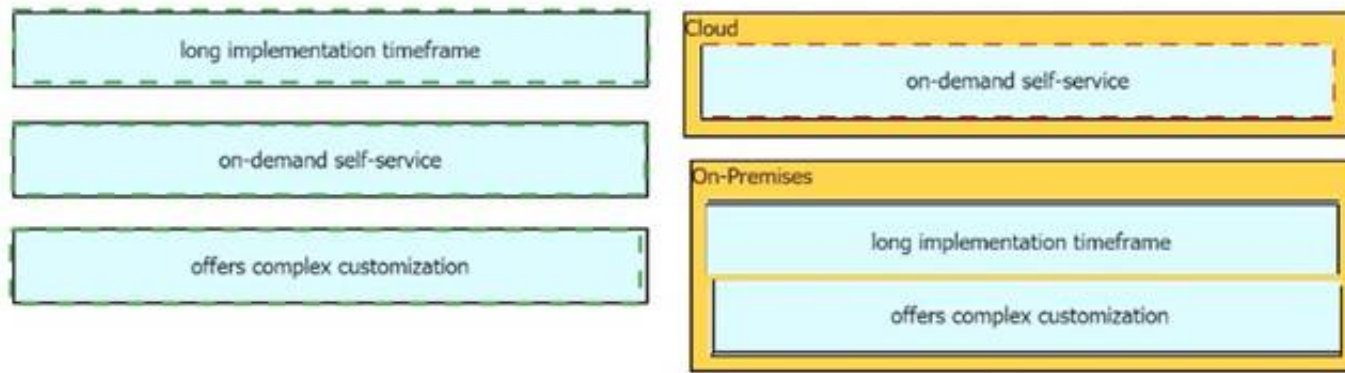
Drag and drop the characteristics from the left onto the deployment models on the right.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 125

DRAG DROP - (Topic 2)

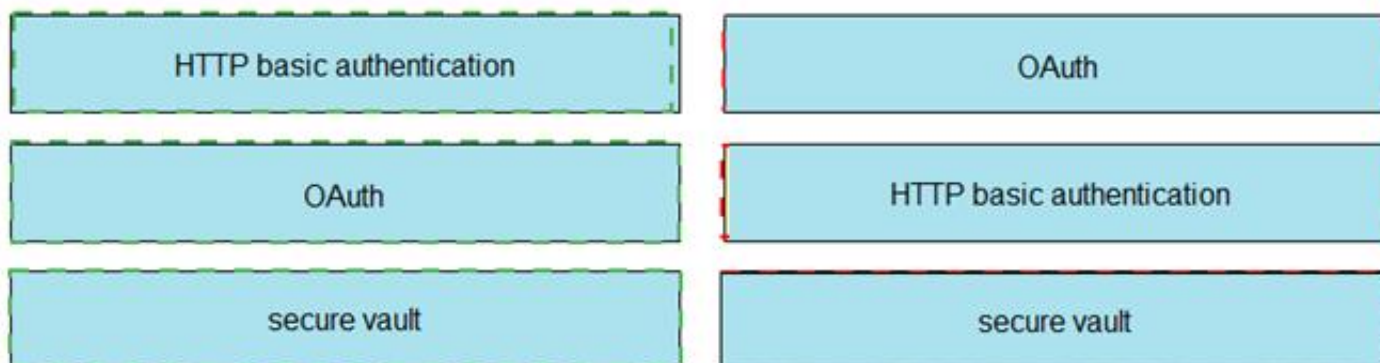
Drag and drop the REST API authentication methods from the left onto their descriptions on the right.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 130

- (Topic 2)

A customer wants to use a single SSID to authenticate IoT devices using different passwords. Which Layer 2 security type must be configured in conjunction with Cisco ISE to achieve this requirement?

- A. Fast Transition
- B. Central Web Authentication
- C. Cisco Centralized Key Management
- D. Identity PSK

Answer: D

NEW QUESTION 134

- (Topic 2)

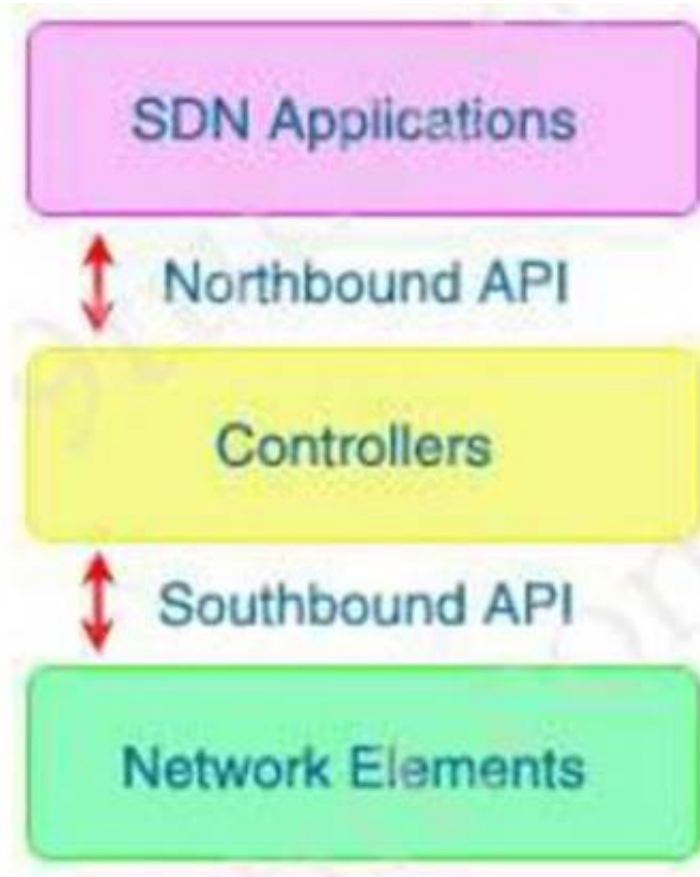
What do Cisco DNA southbound APIs provide?

- A. Interface between the controller and the network devices
- B. NETCONF API interface for orchestration communication
- C. RESful API interface for orchestrator communication
- D. Interface between the controller and the consumer

Answer: A

Explanation:

The Southbound API is used to communicate with network devices.



NEW QUESTION 136

- (Topic 2)

Refer to the exhibit.

```

Hello due in 00:00:07
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 1 msec, maximum is 1 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
    
```

An engineer configures OSPF and wants to verify the configuration. Which configuration is applied to this device?

A)
R1(config)#router ospf 1
R1(config-router)#network 192.168.50.0 0.0.0.255 area 0

B)
R1(config)#router ospf 1
R1(config-router)#network 0.0.0.0 0.0.0.0 area 0
R1(config-router)#no passive-interface Gi0/1

C)
R1(config)#interface Gi0/1
R1(config-if)#ip ospf enable
R1(config-if)#ip ospf network broadcast
R1(config-if)#no shutdown

D)
R1(config)#interface Gi0/1
R1(config-if)#ip ospf 1 area 0
R1(config-if)#no shutdown

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 140

- (Topic 2)

Refer to the exhibit.

```
headers = {
    'Accept': 'application/yang-data+json',
    'Content-Type': 'application/yang-data+json'
},
data = json.dumps({
    'Cisco-IOS-XE-native:GigabitEthernet': {
        'ip': {
            'address': {
                'primary': {
                    'address': '10.10.10.1',
                    'mask': '255.255.255.0'
                }
            }
        }
    }
}),
verify = False)

# Print the HTTP response code
print('Response Code: ' + str(response.status_code))
```

After the code is run on a Cisco IOS-XE router, the response code is 204. What is the result of the script?

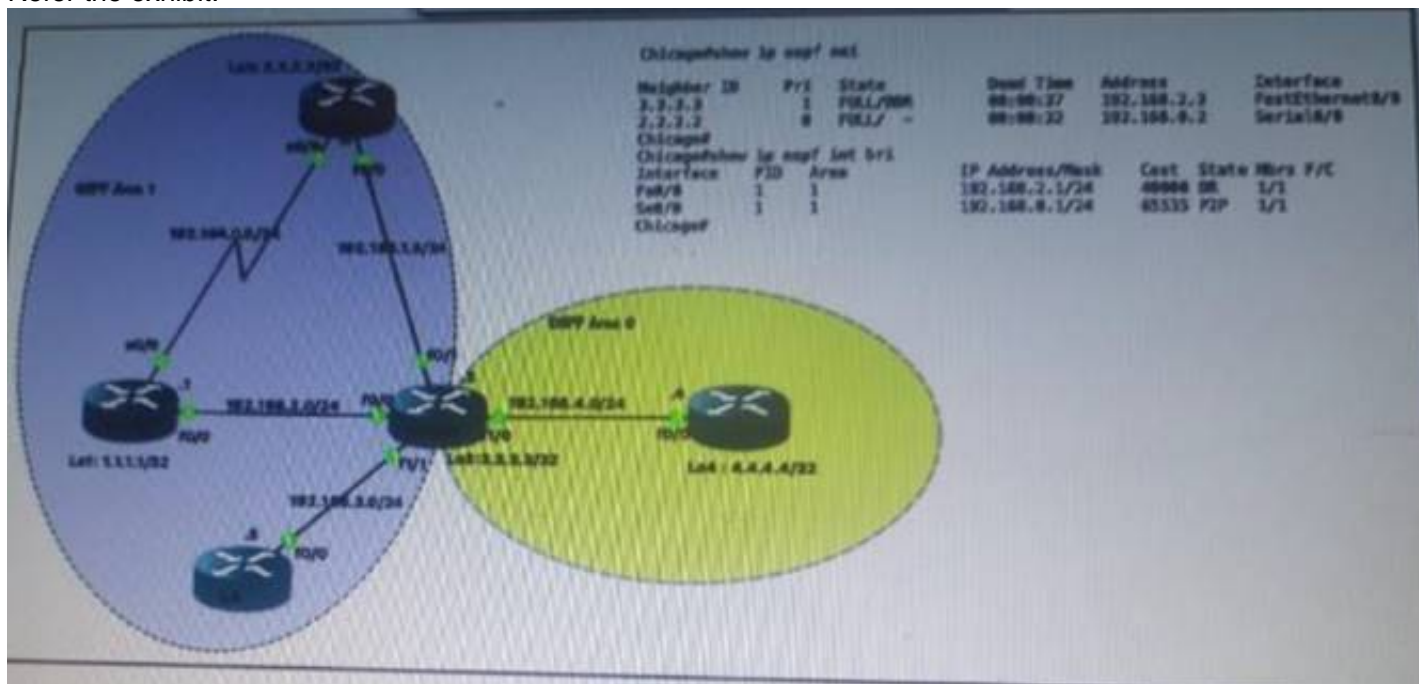
- A. The configuration fails because another interface is already configured with IP address 10.10.10.1/24.
- B. The configuration fails because interface GigabitEthernet2 is missing on the target device.
- C. The configuration is successfully sent to the device in cleartext.
- D. Interface GigabitEthernet2 is configured with IP address 10.10.10.1/24

Answer: D

NEW QUESTION 141

- (Topic 2)

Refer the exhibit.



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

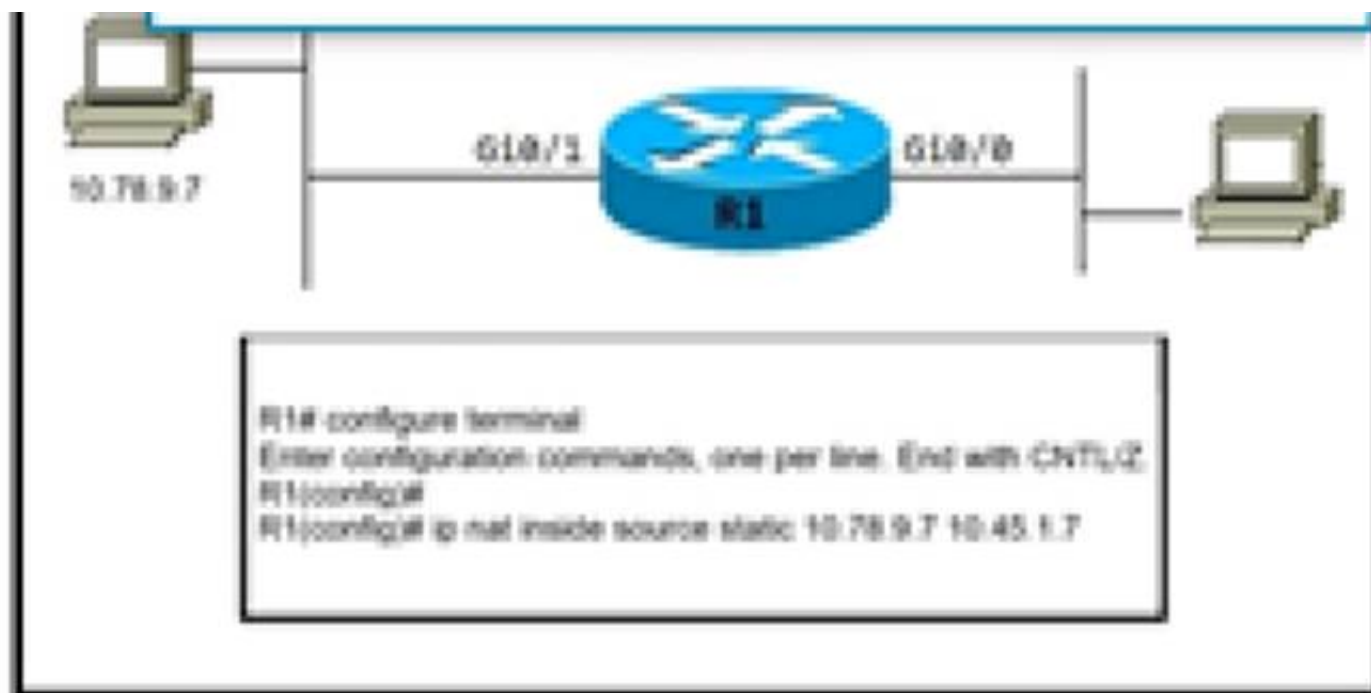
- A. This segment has no designated router because it is a nonbroadcast network type.
- B. This segment has no designated router because it is a p2p network type.
- C. Router Chicago because it has a lower router ID
- D. Router NewYork because it has a higher router ID

Answer: B

NEW QUESTION 143

- (Topic 2)

Refer to the exhibit.



A network architect has partially configured static NAT. which commands should be asked to complete the configuration?

- A. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat outside R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat inside
- 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 inside R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat outside

Answer: B

NEW QUESTION 148

- (Topic 2)

An engineer must create an EEM script to enable OSPF debugging in the event the OSPF neighborhood goes down. Which script must the engineer apply?

- ☐ event manager applet ENABLE_OSPF_DEBUG
 event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL"
 action 1.0 cli command "enable"
 action 2.0 cli command "debug ip ospf event"
 action 3.0 cli command "debug ip ospf adj"
 action 4.0 syslog priority informational msg "ENABLE_OSPF_DEBUG"
- ☐ event manager applet ENABLE_OSPF_DEBUG
 event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL"
 action 1.0 cli command "debug ip ospf event"
 action 2.0 cli command "debug ip ospf adj"
 action 3.0 syslog priority informational msg "ENABLE_OSPF_DEBUG"
- ☐ event manager applet ENABLE_OSPF_DEBUG
 event syslog pattern "%OSPF-5-ADJCHG: Process 6, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWN"
 action 1.0 cli command "enable"
 action 2.0 cli command "debug ip ospf event"
 action 3.0 cli command "debug ip ospf adj"
 action 4.0 syslog priority informational msg "ENABLE_OSPF_DEBUG"
- ☐ event manager applet ENABLE_OSPF_DEBUG
 event syslog pattern "%OSPF-1-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWN"
 action 1.0 cli command "debug ip ospf event"
 action 2.0 cli command "debug ip ospf adj"
 action 3.0 syslog priority informational msg "ENABLE_OSPF_DEBUG"

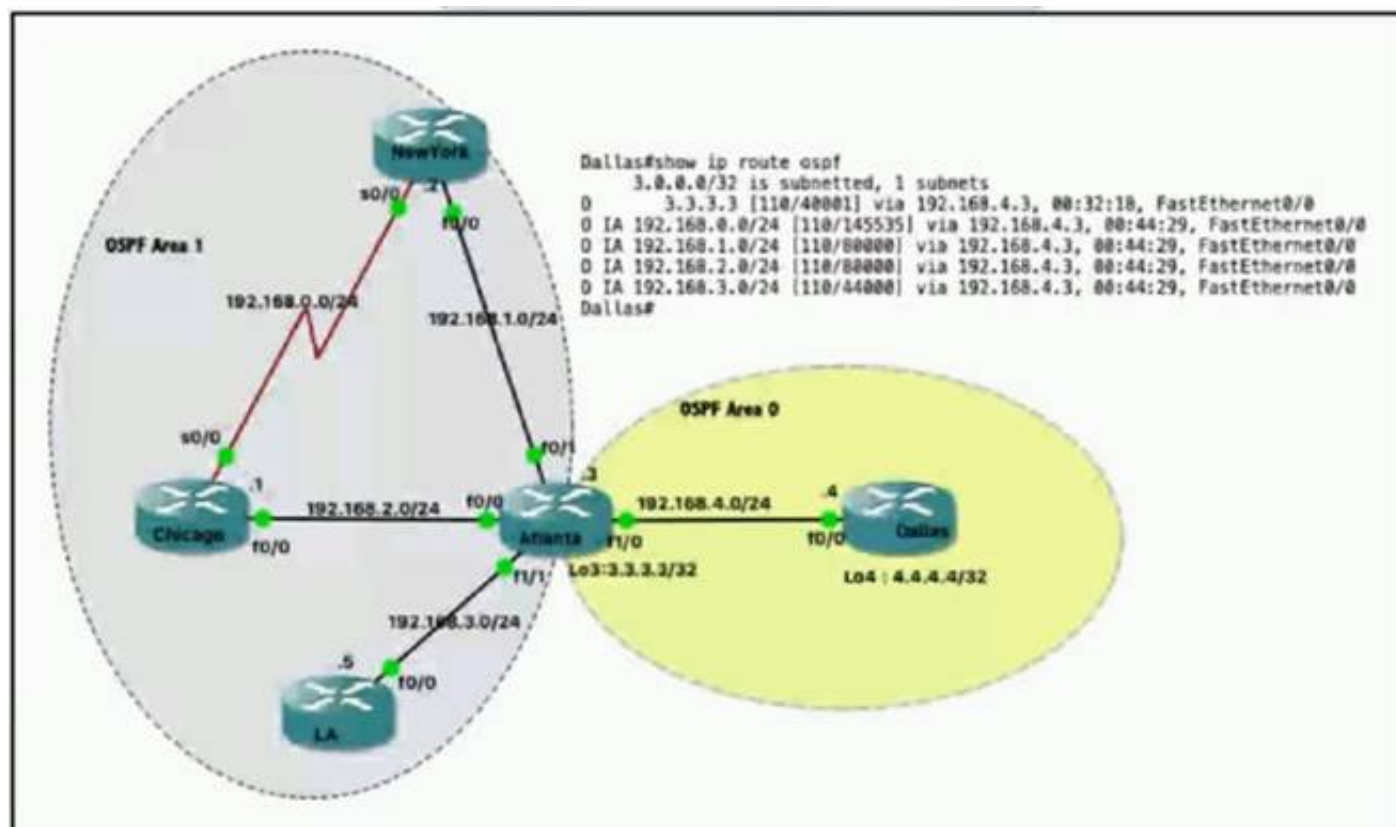
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 151

- (Topic 2)

Refer to the exhibit.



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

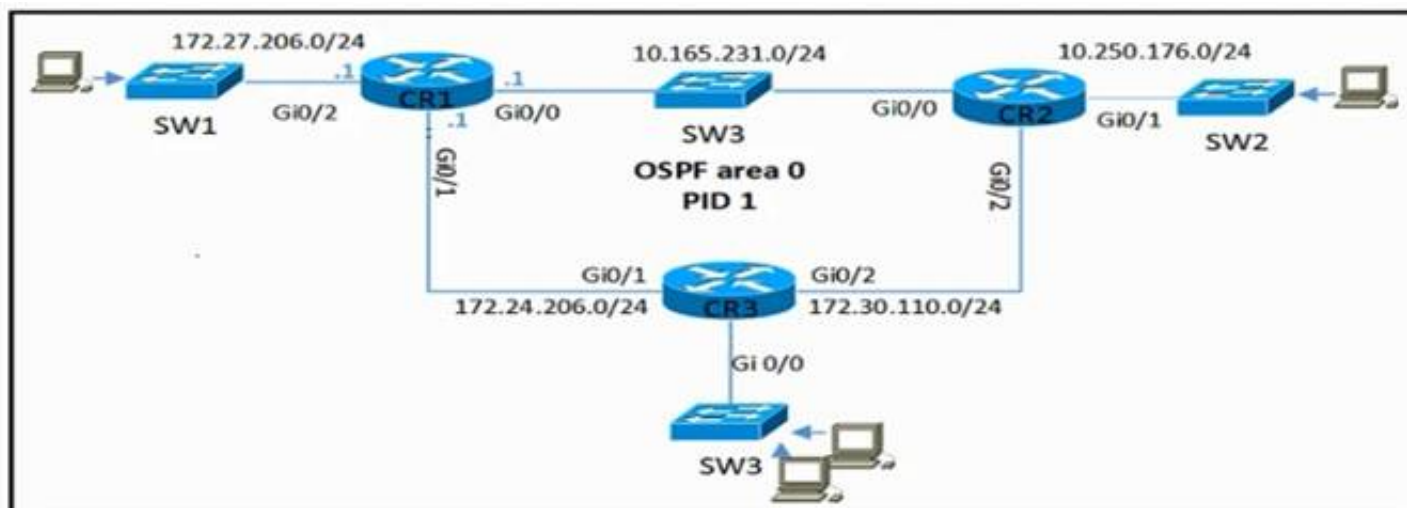
- A. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.248.0
- B. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.252.0
- C. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.252.0
- D. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.248.0

Answer: C

NEW QUESTION 156

- (Topic 2)

Refer to the exhibit.



CR2 and CR3 are configured with OSPF. Which configuration, when applied to CR1, allows CR1 to exchange OSPF Information with CR2 and CR3 but not with other network devices or on new Interfaces that are added to CR1?

A)

```

router ospf 1
network 0.0.0.0 255.255.255.255 area 0
passive-interface GigabitEthernet0/2
  
```

B)

```

router ospf 1
network 10.165.231.0 0.0.0.255 area 0
network 172.27.206.0 0.0.0.255 area 0
network 172.24.206.0 0.0.0.255 area 0
  
```

C)

```

interface Gi0/2
ip ospf 1 area 0

router ospf 1
passive-interface GigabitEthernet0/2
  
```

D)

```
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
network 172.16.0.0 0.15.255.255 area 0
passive-interface GigabitEthernet0/2
```

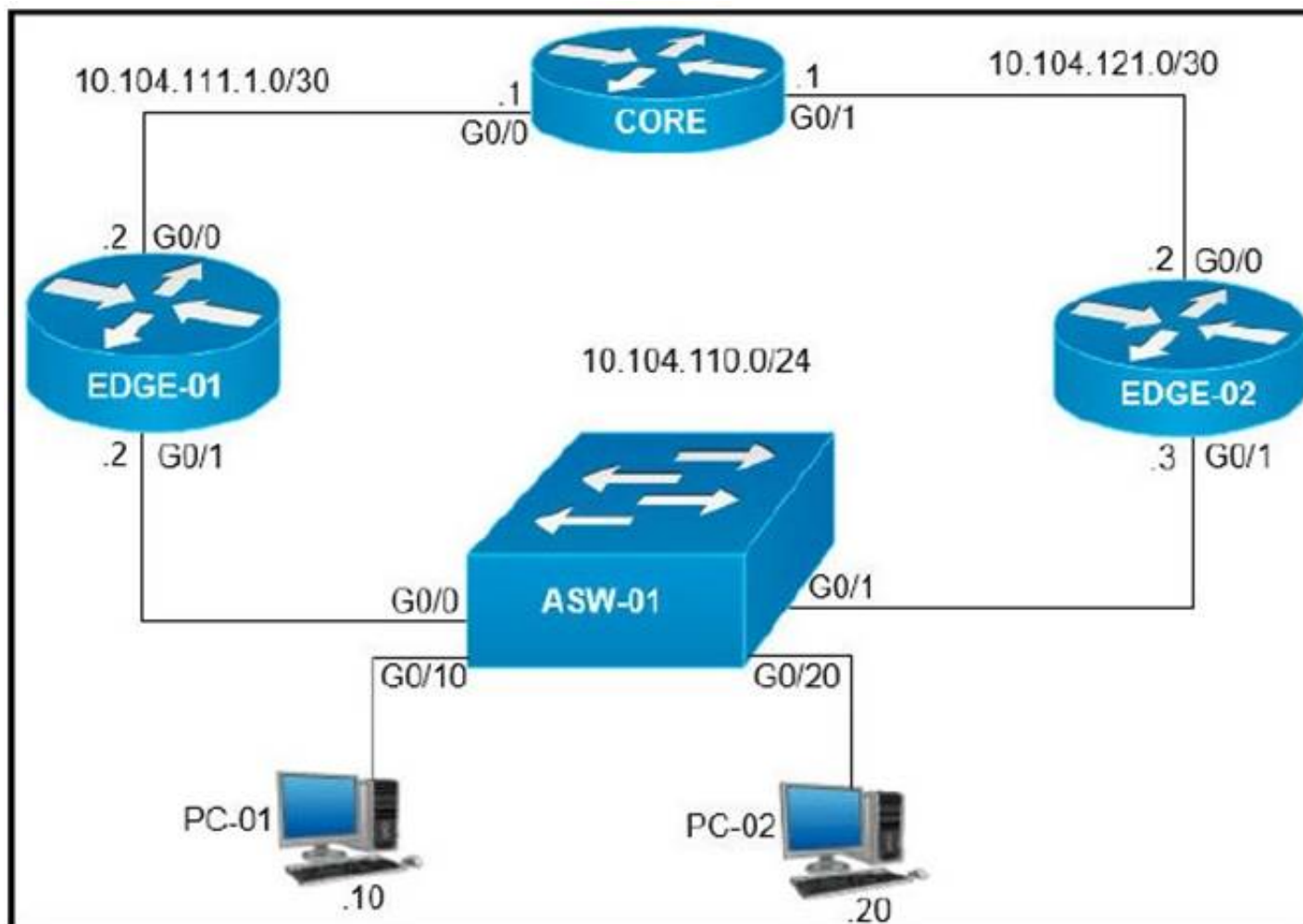
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 160

- (Topic 2)

Refer to the exhibit.



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

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

Answer: C

NEW QUESTION 165

- (Topic 2)

How does a fabric AP fit in the network?

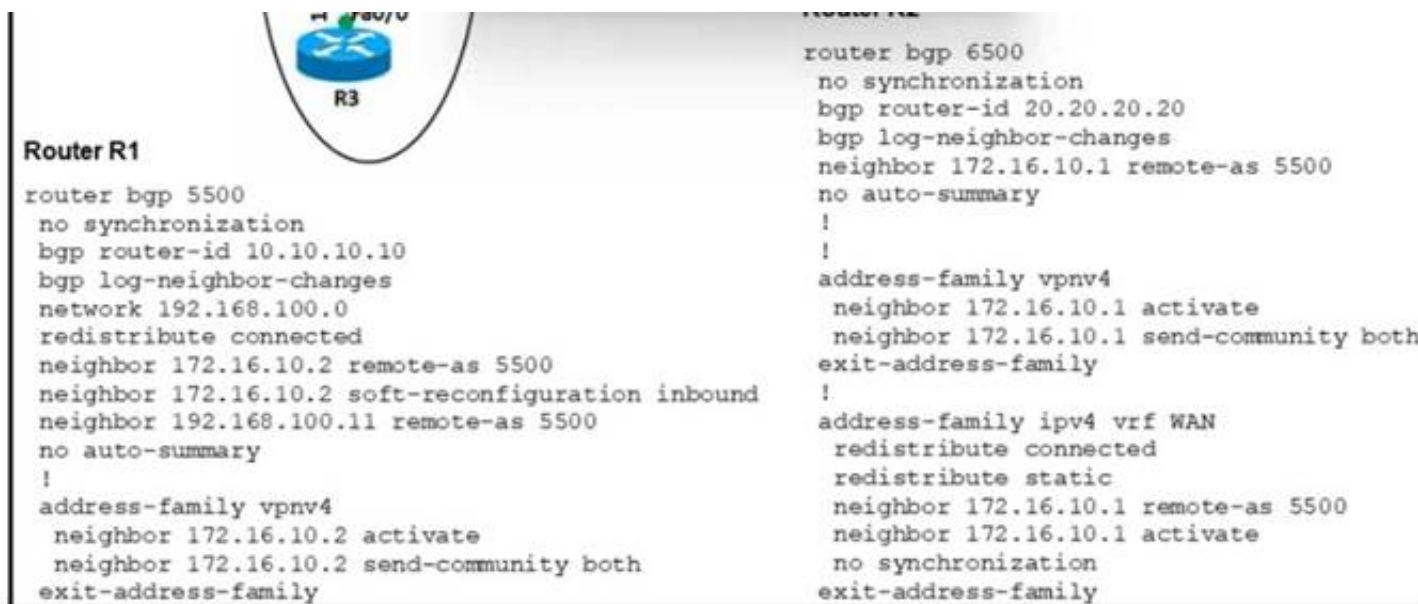
- A. It is in local mode and must be connected directly to the fabric border node
- B. It is in FlexConnect mode and must be connected directly to the fabric edge switch.
- C. It is in FlexConnect mode and must be connected directly to the fabric border node
- D. It is in local mode and must be connected directly to the fabric edge switch.

Answer: D

NEW QUESTION 169

- (Topic 2)

Refer to the exhibit.



An engineer configures the BGP adjacency between R1 and R2, however, it fails to establish Which action resolves the issue?

- A. Change the network statement on R1 to 172.16 10.0
- B. Change the remote-as number for 192 168.100.11.
- C. Enable synchronization on R1 and R2
- D. Change the remote-as number on R1 to 6500.

Answer: D

NEW QUESTION 173

- (Topic 1)

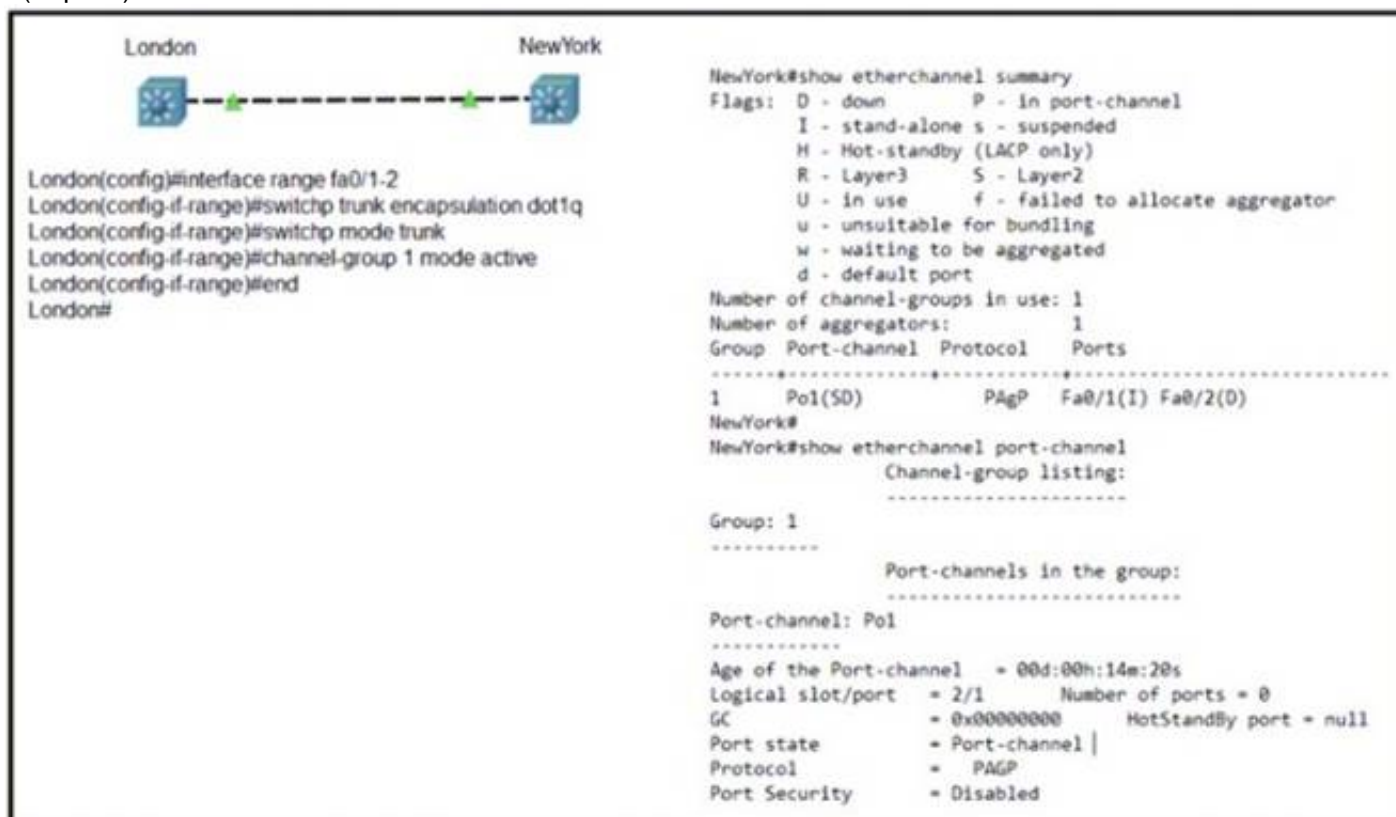
A customer has several small branches and wants to deploy a WI-FI solution with local management using CAPWAP. Which deployment model meets this requirement?

- A. Autonomous
- B. Mobility Express
- C. SD-Access wireless
- D. Local mode

Answer: B

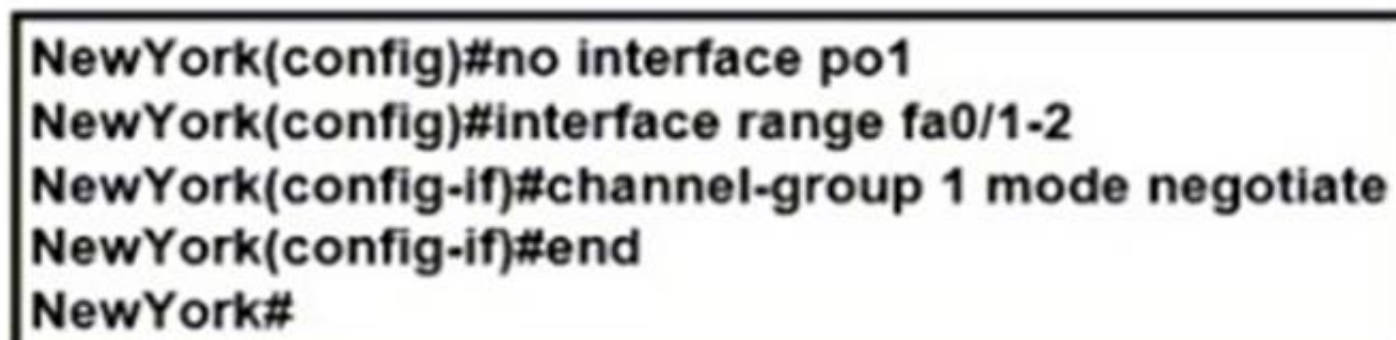
NEW QUESTION 177

- (Topic 1)



Refer to the exhibit. Communication between London and New York is down. Which command set must be applied to the NewYork switch to resolve the issue?

A)



B)


```
NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode on
NewYork(config-if)#end
NewYork#
```

C)

```
NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode auto
NewYork(config-if)#end
NewYork#
```

D)

```
NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode passive
NewYork(config-if)#end
NewYork#
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 180

- (Topic 1)

Which two operational models enable an AP to scan one or more wireless channels for rouge access points and at the same time provide wireless services to clients? (Choose two.)

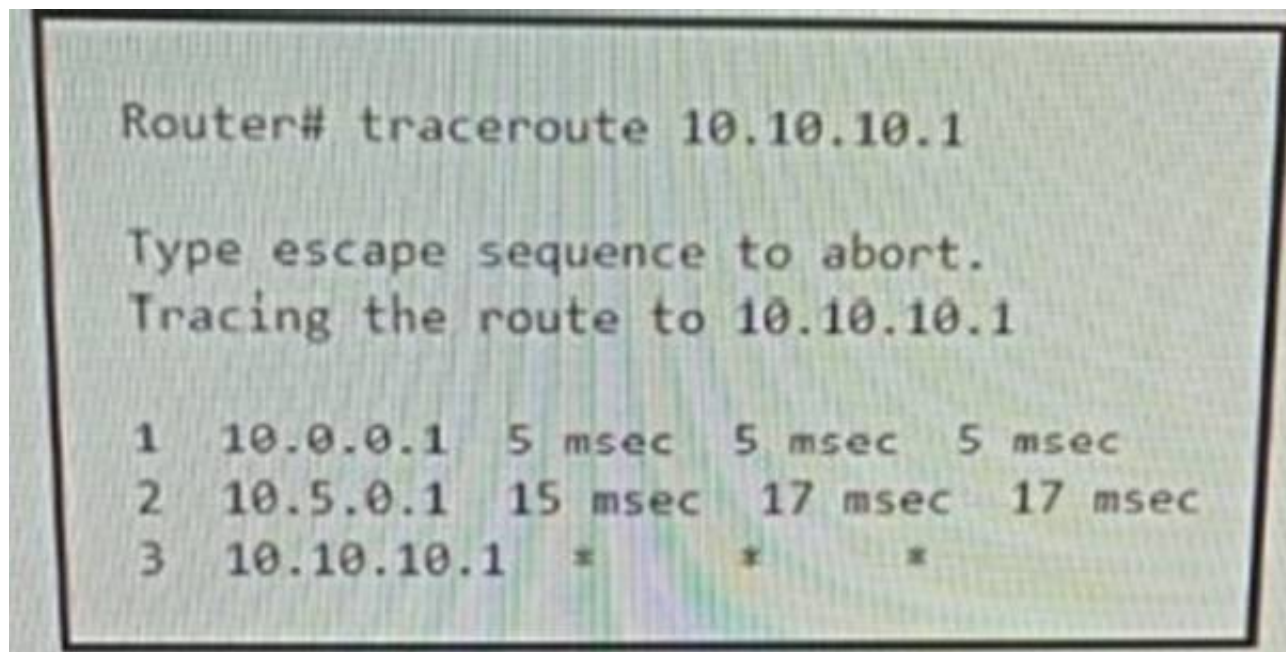
- A. Rouge detector
- B. Sniffer
- C. FlexConnect
- D. Local
- E. Monitor

Answer: DE

NEW QUESTION 184

- (Topic 1)

Refer to the exhibit.



An engineer is troubleshooting a connectivity issue and executes a traceoute. What does the result confirm?

- A. The destination server reported it is too busy
- B. The protocol is unreachable
- C. The destination port is unreachable
- D. The probe timed out

Answer: D

Explanation:

In Cisco routers, the codes for a traceroute command reply are:

! — success* — time outN — network unreachableH — host unreachableP — protocol unreachableA — admin deniedQ — source quench received (congestion)? — unknown (any other ICMP message)

In Cisco routers, the codes for a traceroute command reply are:
! — success* — time outN — network unreachableH — host unreachableP — protocol unreachableA — admin deniedQ — source quench received (congestion)? — unknown (any other ICMP message)

NEW QUESTION 186

- (Topic 1)

Which measurement is used from a post wireless survey to depict the cell edge of the access points?

- A. SNR
- B. Noise
- C. RSSI
- D. CCI

Answer: A

Explanation:

Coverage defines the ability of wireless clients to connect to a wireless AP with a signal strength and quality high enough to overcome the effects of RF interference. The edge of the coverage for an AP is based on the signal strength and SNR measured as the client device moves away from the AP. The signal strength required for good coverage varies dependent on the specific type of client devices and applications on the network. To accommodate the requirement to support wireless Voice over IP (VoIP), refer to the RF guidelines specified in the Cisco 7925G Wireless IP Phone Deployment Guide. The minimum recommended wireless signal strength for voice applications is -67 dBm and the minimum SNR is 25 dB. The first step in the analysis of a post site survey is to verify the 'Signal Coverage'. The signal coverage is measured in dBm. You can adjust the color-coded signal gauge to your minimum-allowed signal level to view areas where there are sufficient and insufficient coverage. The example in Figure 8 shows blue, green, and yellow areas in the map have signal coverage at -67 dBm or better. The areas in grey on the coverage maps have deficient coverage. Source from Cisco https://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan_troubleshoot/8_Site_Survey_RF_Design_Valid.html

NEW QUESTION 191

DRAG DROP - (Topic 1)

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

supports unequal path load balancing

link state routing protocol

distance vector routing protocol

metric is based on delay and bandwidth by default

makes it easy to segment the network logically

constructs three tables as part of its operation: neighbor table, topology table, and routing table

OSPF

EIGRP

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

supports unequal path load balancing

link state routing protocol

distance vector routing protocol

metric is based on delay and bandwidth by default

makes it easy to segment the network logically

constructs three tables as part of its operation: neighbor table, topology table, and routing table

OSPF

link state routing protocol

makes it easy to segment the network logically

constructs three tables as part of its operation: neighbor table, topology table, and routing table

EIGRP

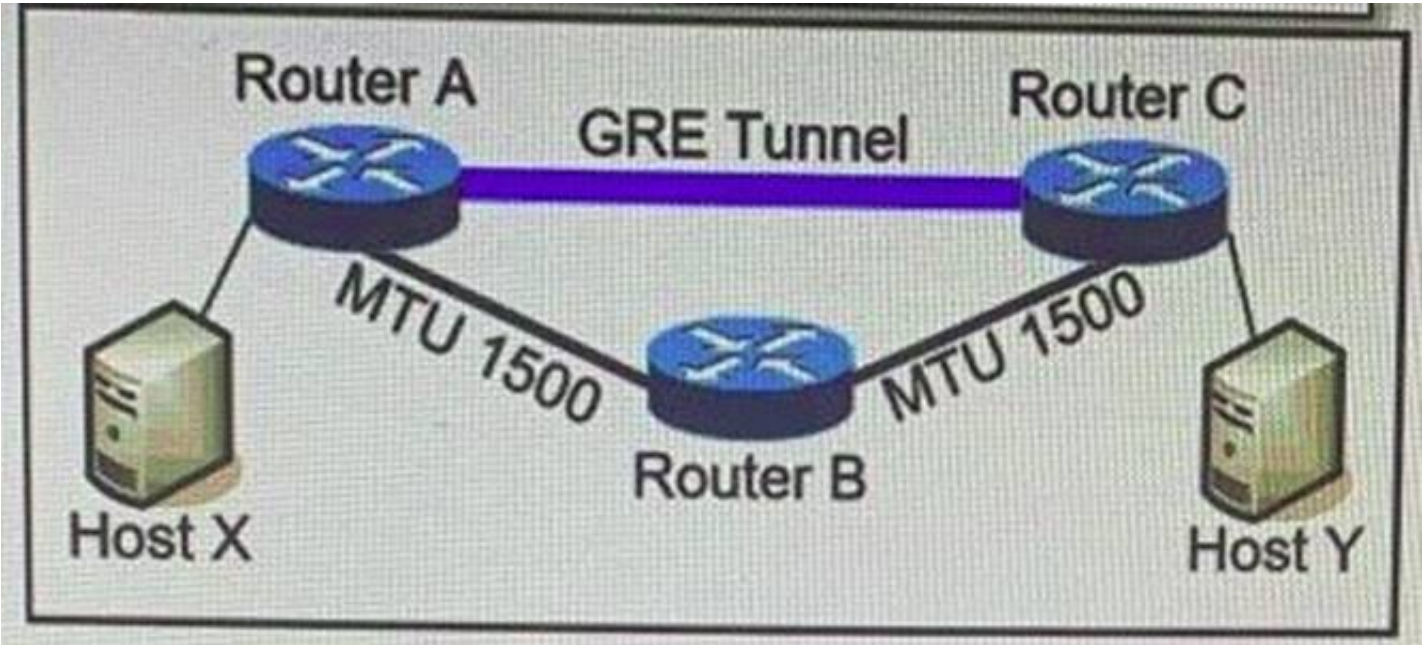
supports unequal path load balancing

distance vector routing protocol

metric is based on delay and bandwidth by default

NEW QUESTION 193

- (Topic 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 is discarded on router B
- D. The packet arrives on router C fragmented.

Answer: D

Explanation:

Like any protocol, using GRE adds a few bytes to the size of data packets. This must be factored into the MSS and MTU settings for packets. If the MTU is 1,500 bytes and the MSS is 1,460 bytes (to account for the size of the necessary IP and TCP headers), the addition of GRE 24-byte headers will cause the packets to exceed the MTU:

1,460 bytes [payload] + 20 bytes [TCP header] + 20 bytes [IP header] + 24 bytes [GRE header + IP header] = 1,524 bytes

As a result, the packets will be fragmented. Fragmentation slows down packet delivery times and increases how much compute power is used, because packets that exceed the MTU must be broken down and then reassembled.

NEW QUESTION 194

- (Topic 1)

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 globalip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 globalip route 192.168.1.0 255.255.255.0 Vlan1Oip route 172.16.1.0 255.255.255.0 Vlan20
- B. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer2ip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customer1
- C. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customerlip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customer2
- D. ip route vrf Customer1 172.16.1.1 255.255.255.255 172.16.1.1 globalip route vrf Customer 192.168.1.200 255.255.255.0 192.168.1.1 globalip route 192.168.1.0 255.255.255.0 Vlan1Oip route 172.16.1.0 255.255.255.0 Vlan20

Answer: A

NEW QUESTION 195

- (Topic 1)

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. classifies traffic based on the contextual identity of the endpoint rather than its IP address correct
- D. assigns a VLAN to the endpoint

Answer: C

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.

NEW QUESTION 198

- (Topic 1)

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

- A. handle, maintain, and gather configuration and status for nodes within the SD-WAN fabric
- B. distribute policies that govern data forwarding performed within the SD-WAN fabric

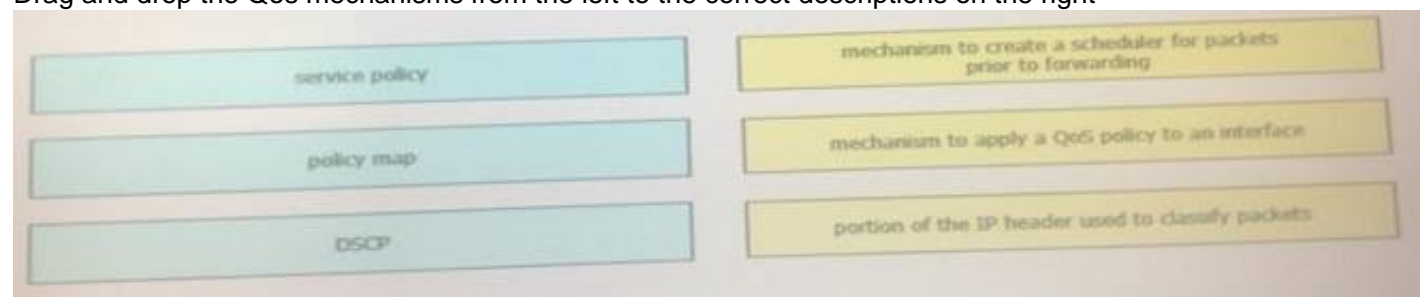
- C. gather telemetry data from vEdge routers
- D. onboard vEdge nodes into the SD-WAN fabric

Answer: B

NEW QUESTION 199

DRAG DROP - (Topic 1)

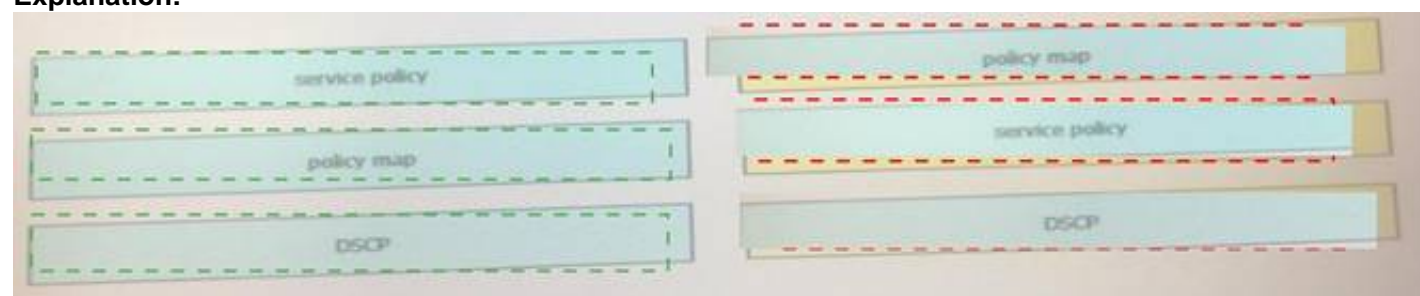
Drag and drop the Qos mechanisms from the left to the correct descriptions on the right



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 200

- (Topic 1)

Refer to the exhibit.

```
PYTHON CODE:
import requests
import json

url="http://YOURIPins"
switchuser="USERID"
switchpassword="PASSWORD"

myheaders={content-type:"application/json"}
payload={
  "ins_api": {
    "version": "1.0",
    "type": "cli_show",
    "chunk": "0",
    "sid": "1",
    "input": "show version",
    "output_format": "json"
  }
}
response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword)) json()
print(response[ins_api][outputs][output][body][kickstart_ver_str])

HTTP JSON Response:
{
  "ins_api": {
    "type": "cli_show",
    "version": "1.0",
    "sid": "eoc",
    "outputs": {
      "output": {
        "input": "show version",
        "msg": "Success",
        "code": "200",
        "body": {
          "bios_ver_str": "07.61",
          "kickstart_ver_str": "7.0(3)I7(4)",
          "bios_cmpt_time": "04/06/2017",
          "kick_file_name": "bootflash://rxos.7.0.3.I7.4.bin",
          "kick_cmpt_time": "6/14/1970 2:00:00",
          "kick_tmstamp": "06/14/1970 09:49:04",
          "chassis_id": "Nexus6000 03180YC-EX chassis",
          "cpu_name": "Intel(R) Xeon(R) CPU @ 1.80GHz",
          "memory": 24633488,
          "mem_type": "x8",
          "n_insecs": 134703,
          "n_time": "Sun Mar 10 15:41:46 2019",
          "n_reason": "Reset Requested by CLI command reload",
          "n_sys_ver": "7.0(3)I7(4)",
          "n_service": "",
          "manufacturer": "Cisco Systems, Inc.",
          "TABLE_package_list": {
            "ROW_package_list": {
              "package_id": 0
            }
          }
        }
      }
    }
  }
}
```

Which HTTP JSON response does the python code output give?

- A. NameError: name 'json' is not defined
- B. KeyError 'kickstart_ver_str'
- C. 7.61
- D. 7.0(3)I7(4)

Answer: D

NEW QUESTION 204

- (Topic 1)

Which statement about TLS is accurate when using RESTCONF to write configurations on network devices?

- A. It requires certificates for authentication
- B. It is provided using NGINX acting as a proxy web server
- C. It is used for HTTP and HTTPS requests
- D. It is not supported on Cisco devices

Answer: B

NEW QUESTION 205

- (Topic 1)

A network engineer is configuring Flexible Netflow and enters these commands
Sampler Netflow1
Mode random one-out-of 100 Interface fastethernet 1/0 Flow-sampler netflow1

Which are two results of implementing this feature instead of traditional Netflow? (Choose two.)

- A. CPU and memory utilization are reduced.
- B. Only the flows of top 100 talkers are exported
- C. The data export flow is more secure.
- D. The number of packets to be analyzed are reduced
- E. The accuracy of the data to be analyzed is improved

Answer: AD

NEW QUESTION 206

DRAG DROP - (Topic 1)

Drag and drop the characteristics from the left onto the protocols they apply to on the right?

uses Dijkstra's Shortest Path First algorithm

uses Diffused Update Algorithm

uses bandwidth, delay, reliability, and load for routing metric

uses an election process

OSPF

EIGRP

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

uses Dijkstra's Shortest Path First algorithm

uses Diffused Update Algorithm

uses bandwidth, delay, reliability, and load for routing metric

uses an election process

OSPF

uses Dijkstra's Shortest Path First algorithm

uses an election process

EIGRP

uses Diffused Update Algorithm

uses bandwidth, delay, reliability, and load for routing metric

NEW QUESTION 210

DRAG DROP - (Topic 1)

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

customizable hardware, purpose-built systems

easy to scale and upgrade

more suitable for companies with specific regulatory or security requirements

resources can be over or underutilized as requirements vary

requires a strong and stable internet connection

built-in, automated data backups and recovery

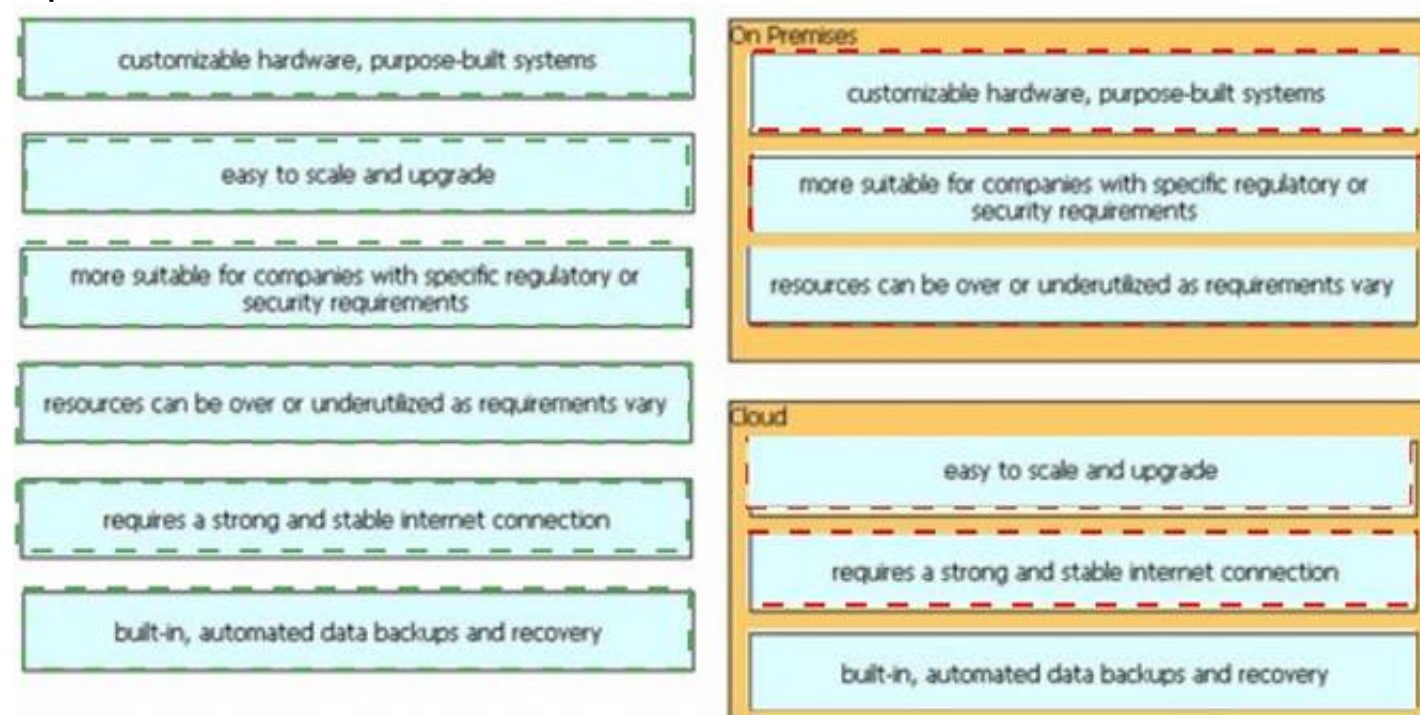
On Premises

Cloud

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 211

- (Topic 1)

What are two characteristics of VXLAN? (Choose two)

- A. It uses VTEPs to encapsulate and decapsulate frames.
- B. It has a 12-bit network identifier
- C. It allows for up to 16 million VXLAN segments
- D. It lacks support for host mobility
- E. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay.

Answer: AC

NEW QUESTION 213

- (Topic 1)

Which device makes the decision for a wireless client to roam?

- A. wireless client
- B. wireless LAN controller
- C. access point
- D. WCS location server

Answer: A

NEW QUESTION 215

- (Topic 1)

What is a fact about Cisco EAP-FAST?

- A. It does not require a RADIUS server certificate.
- B. It requires a client certificate.
- C. It is an IETF standard.
- D. It operates in transparent mode.

Answer: A

NEW QUESTION 218

- (Topic 1)

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

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

Answer: A

NEW QUESTION 223

- (Topic 1)

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

- A. The FIB is derived from the data 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. FIB is a database of routing prefixes, and the RIB is the information used to choose the egress interface for each packet.
- D. The FIB is derived from the control plane, and the RIB is derived from the FIB.
- E. The RIB is derived from the control plane, and the FIB is derived from the RIB.

Answer: BE

NEW QUESTION 227

DRAG DROP - (Topic 1)

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

supports virtual links

can automatically summarize networks at the boundary

requires manual configuration of network summarization

EIGRP

OSPF

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

supports virtual links

can automatically summarize networks at the boundary

requires manual configuration of network summarization

EIGRP

can automatically summarize networks at the boundary

OSPF

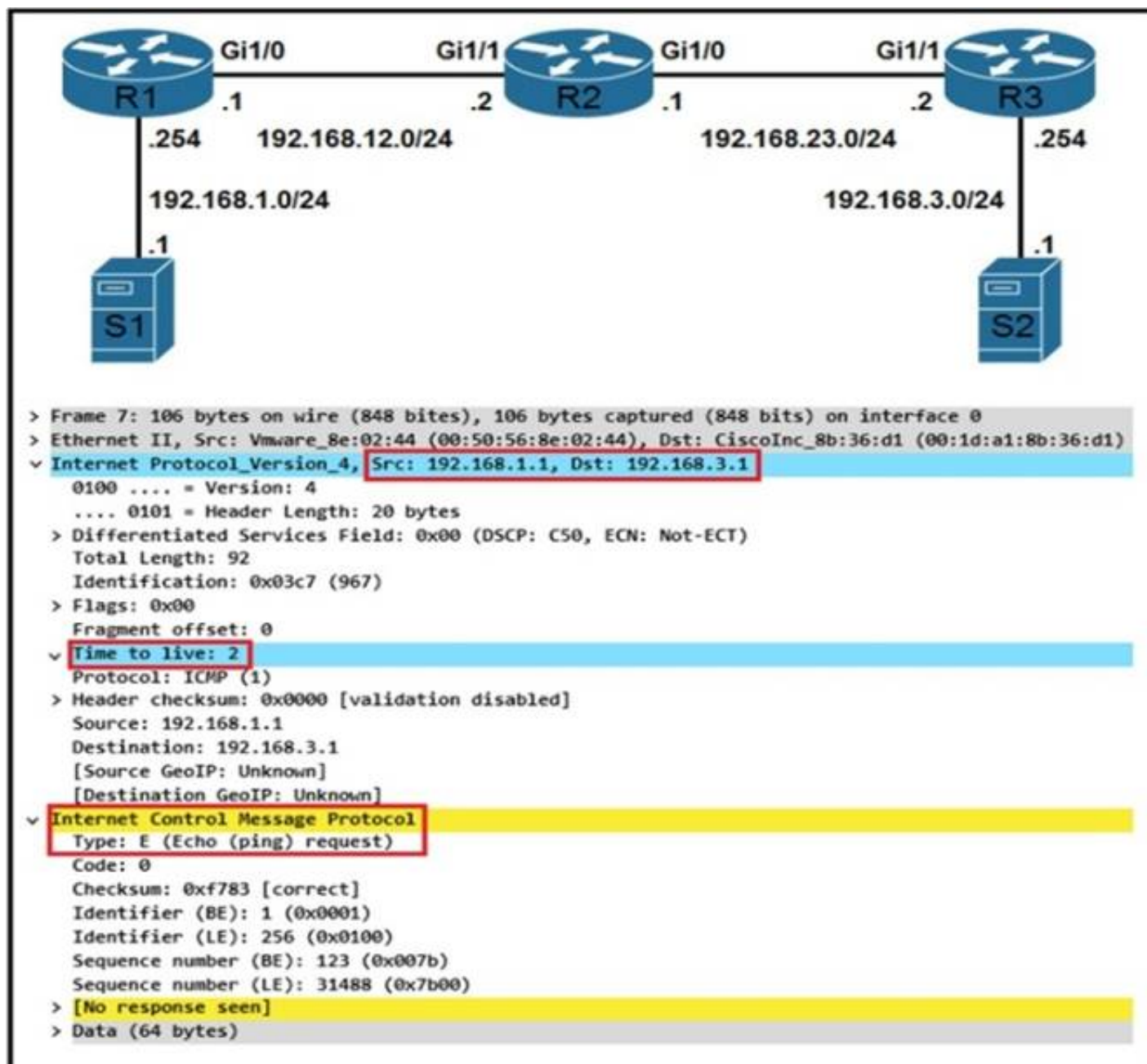
supports virtual links

requires manual configuration of network summarization

NEW QUESTION 232

- (Topic 1)

Refer to the exhibit.



Which troubleshooting a routing issue, an engineer issues a ping from S1 to S2. When two actions from the initial value of the TTL? (Choose two.)

- A. The packet reaches R3, and the TTL expires
- B. R2 replies with a TTL exceeded message
- C. R3 replies with a TTL exceeded message.
- D. The packet reaches R2 and the TTL expires
- E. R1 replies with a TTL exceeded message
- F. The packet reaches R1 and the TTL expires.

Answer: AD

Explanation:

Source MAC in the capture is VMWare, MAC is Cisco. Routers first check the TTL before any further process, subtract 1 at R1. Send to R2, subtract and you have ZERO. Discard packet and reply with ICMP Time Exceeded message from that point, don't even bother checking the Route table for further processing.

NEW QUESTION 236

- (Topic 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
```

An engineer must create a configuration that executes the show run command and then terminates the session when user CCNP logs in. Which configuration change is required?

- A. Add the access-class keyword to the username command
- B. Add the access-class keyword to the aaa authentication command
- C. Add the autocmd keyword to the username command
- D. Add the autocmd keyword to the aaa authentication command

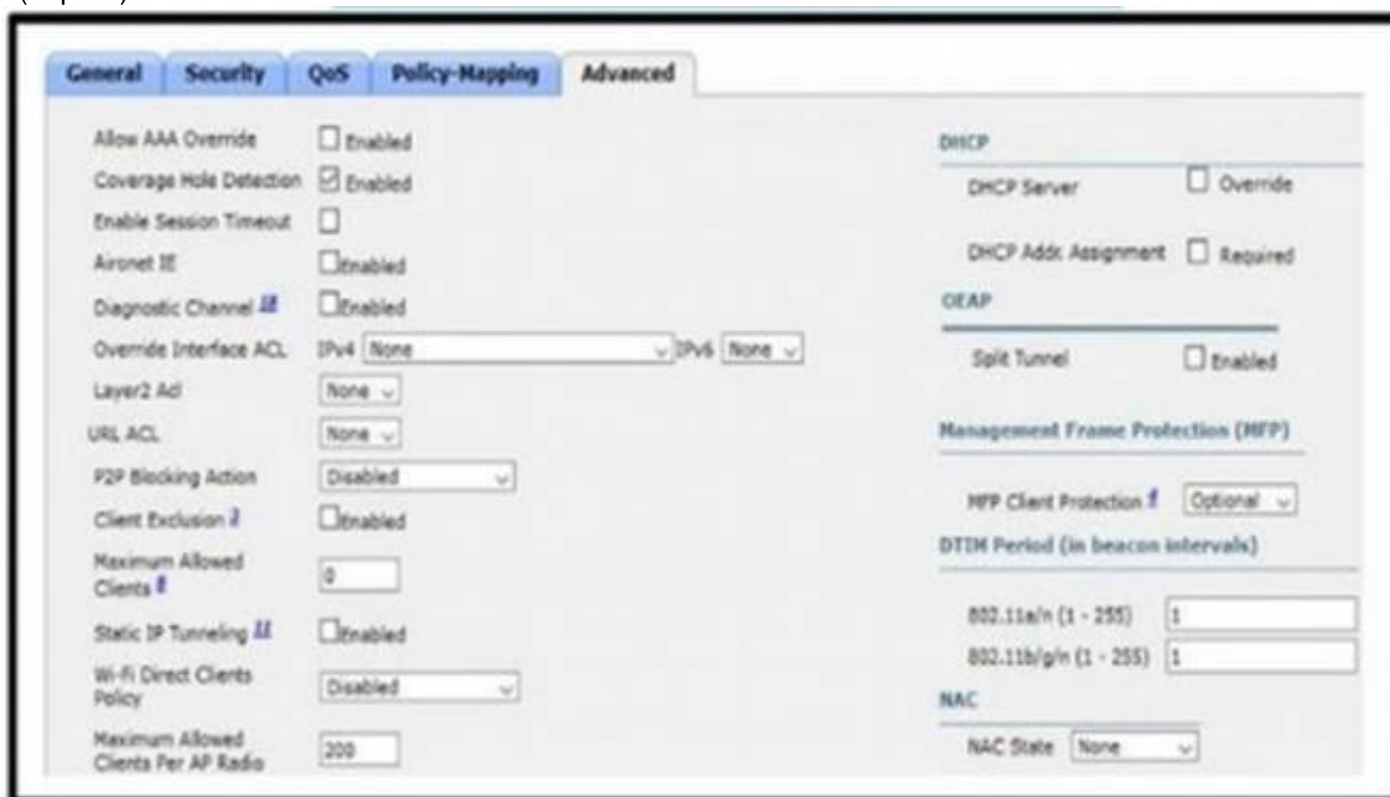
Answer: C

Explanation:

The autocmd 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 autocmd keyword must be the last option on the line. In this specific question, we have to enter this line username CCNP autocmd show running-config.

NEW QUESTION 239

- (Topic 1)



Refer to the exhibit. An engineer has configured Cisco ISE to assign VLANs to clients based on their method of authentication, but this is not working as expected. Which action will resolve this issue?

- A. require a DHCP address assignment
- B. utilize RADIUS profiling
- C. set a NAC state
- D. enable AAA override

Answer: B

NEW QUESTION 243

- (Topic 1)

If the noise floor is -90 dBm and wireless client is receiving a signal of -75 dBm, what is the SNR?

- A. 15
- B. 1.2
- C. -165
- D. .83

Answer: A

NEW QUESTION 246

- (Topic 1)

Which command set configures RSPAN to capture outgoing traffic from VLAN 3 on interface GigabitEthernet 0/3 while ignoring other VLAN traffic on the same interface?

A)

```
monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 3
```

B)

```
monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 1 - 2 , 4 - 4094
```

C)

```
monitor session 2 source interface gigabitethernet0/3 rx
monitor session 2 filter vlan 3
```

D)

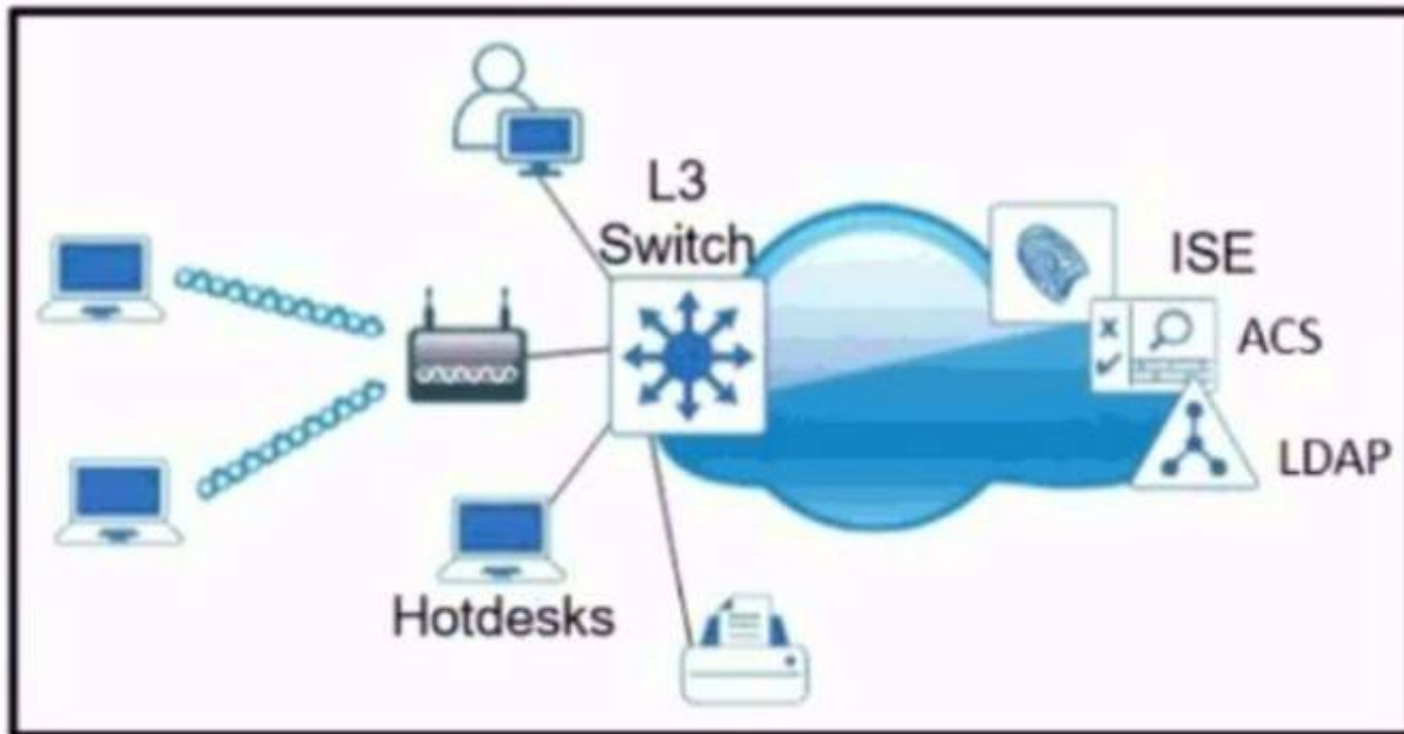
```
monitor session 2 source interface gigabitethernet0/3 rx
monitor session 2 filter vlan 1 - 2 , 4 - 4094
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

NEW QUESTION 247

- (Topic 1)



Refer to the exhibit Which single security feature is recommended to provide Network Access Control in the enterprise?

- A. MAB
- B. 802.1X
- C. WebAuth
- D. port security sticky MAC

Answer: B

NEW QUESTION 251

- (Topic 1)

Where is radio resource management performed in a cisco SD-access wireless solution?

- A. DNA Center
- B. control plane node
- C. wireless controller
- D. Cisco CMX

Answer: C

Explanation:

Fabric wireless controllers manage and control the fabric-mode APs using the same general model as the traditional local-mode controllers which offers the same operational advantages such as mobility control and radio resource management. A significant difference is that client traffic from wireless endpoints is not tunneled from the APs to the wireless controller. Instead, communication from wireless clients is encapsulated in VXLAN by the fabric APs which build a tunnel to their first-hop fabric edge node. Wireless traffic is tunneled to the edge nodes as the edge nodes provide fabric services such as the Layer 3 Anycast Gateway, policy, and traffic enforcement. <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html>

NEW QUESTION 253

- (Topic 1)

```
Switch2#
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/23, putting Fa0/23 in err-disable
state
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/24, putting Fa0/24 in err-disable
state
Switch2#
```

```
Switch1#show etherchannel summary
```

```
!output omitted
```

Group	Port-channel	Protocol	Ports
1	Po2(SD)	LACP	Fa1/0/23(D)

```
Switch2#show etherchannel summary
```

```
!output omitted
```

Group	Port-channel	Protocol	Ports
1	Po1(SD)	-	Fa0/23(D) Fa0/24(D)

Refer to the exhibit. An engineer is configuring an EtherChannel between Switch1 and Switch2 and notices the console message on switch2. Based on the output, which action resolves this issue?

- A. Configure less member ports on Switch2.
- B. Configure the same port channel interface number on both switches
- C. Configure the same EtherChannel protocol on both switches
- D. Configure more member ports on Switch1.

Answer: C

Explanation:

In this case, we are using your EtherChannel without a negotiation protocol on Switch2. 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.

NEW QUESTION 254

- (Topic 1)

Refer to the exhibit.

```
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 network engineer configures a GRE tunnel and enters the show Interface tunnel command. What does the output confirm about the configuration?

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

Answer: C

NEW QUESTION 259

- (Topic 1)

“HTTP/1.1 204 content” is returned when `curl -I -x delete` command is issued. Which situation has occurred?

- A. The object could not be located at the URI path.
- B. The command succeeded in deleting the object
- C. The object was located at the URI, but it could not be deleted.
- D. The URI was invalid

Answer: B

Explanation:

HTTP Status 204 (No Content) indicates that the server has successfully fulfilled the request and that there is no content to send in the response payload body.

NEW QUESTION 263

- (Topic 1)

A customer requests a network design that supports these requirements:

- FHRP redundancy
- multivendor router environment
- IPv4 and IPv6 hosts

Which protocol does the design include?

- A. HSRP version 2
- B. VRRP version 2
- C. GLBP
- D. VRRP version 3

Answer: D

NEW QUESTION 266

- (Topic 1)

What is one benefit of implementing a VSS architecture?

- A. It provides multiple points of management for redundancy and improved support
- B. It uses GLBP to balance traffic between gateways.
- C. It provides a single point of management for improved efficiency.
- D. It uses a single database to manage configuration for multiple switches

Answer: C

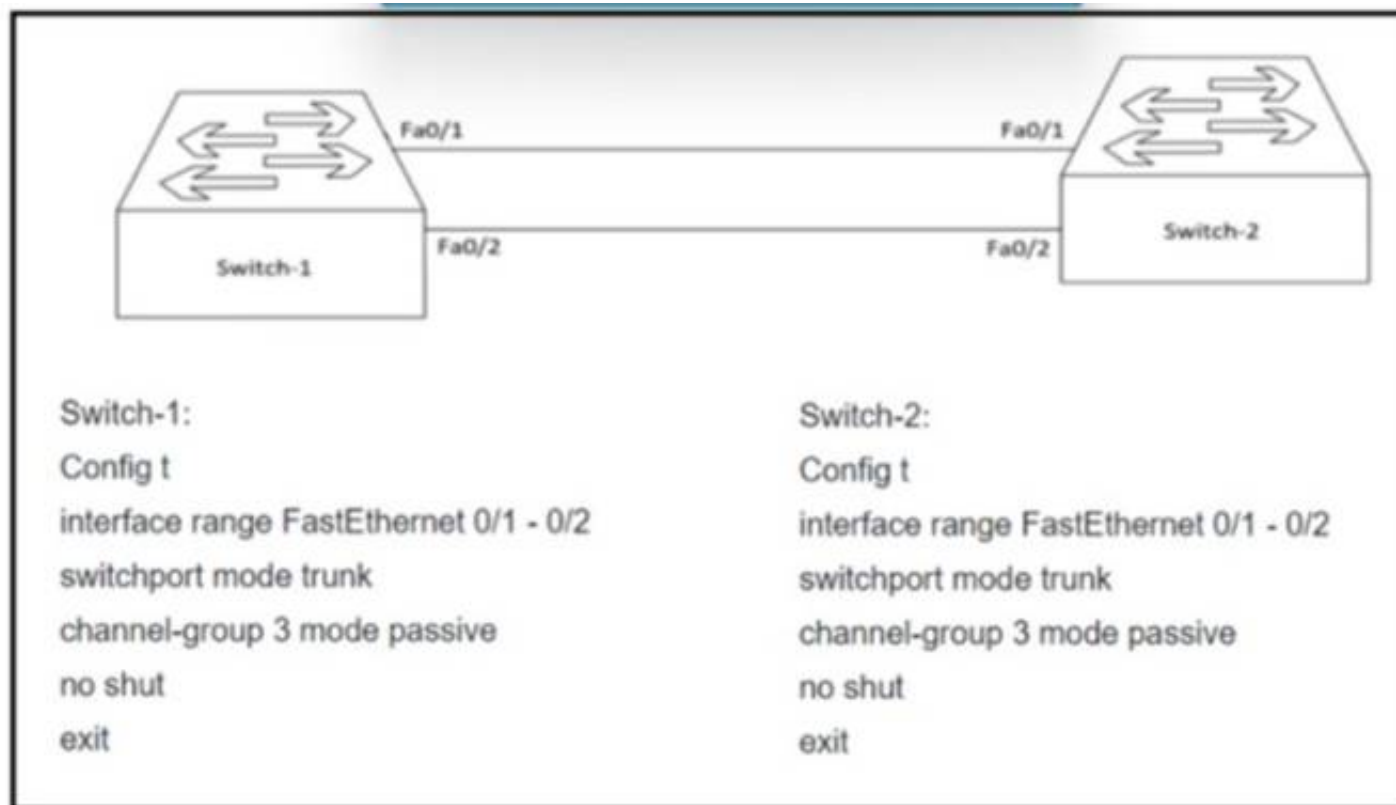
Explanation:

Support Virtual Switching System (VSS) to provide resiliency, and increased operational efficiency with a single point of management; VSS increases operational efficiency by simplifying the network, reducing switch management overhead by at least 50 percent. – Single configuration file and node to manage. Removes the need to configure redundant switches twice with identical policies.

NEW QUESTION 271

- (Topic 4)

Refer to the exhibit.



An LACP port channel is configured between Switch-1 and Switch-2, but It falls to come up. Which action will resolve the issue?

- A. Configure Switch-1 with channel-group mode active
- B. Configure Switch-2 with channel-group mode desirable.
- C. Configure Switch-1 with channel-group mode on.
- D. Configure SwKch-2 with channel-group mode auto

Answer: A

NEW QUESTION 272

DRAG DROP - (Topic 4)

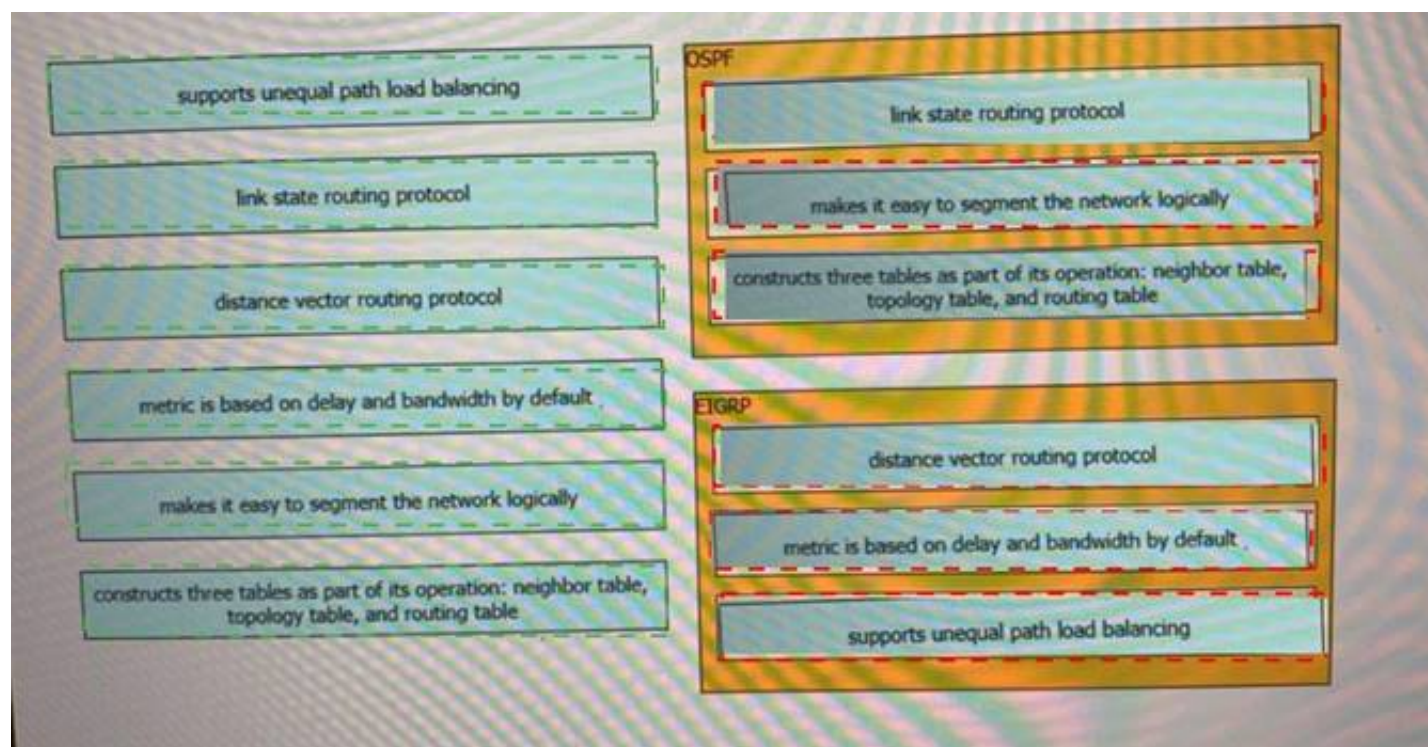
Drag the drop the description from the left onto the routing protocol they describe on the right.

supports unequal path load balancing	OSPF
link state routing protocol	
distance vector routing protocol	
metric is based on delay and bandwidth by default	EIGRP
makes it easy to segment the network logically	
constructs three tables as part of its operation: neighbor table, topology table, and routing table	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 273

- (Topic 4)

Which device, in a LISP routing architecture, receives and de-encapsulates LISP traffic for endpoints within a LISP-capable site?

- A. MR
- B. ETR
- C. OMS
- D. ITR

Answer: B

NEW QUESTION 276

- (Topic 4)

In which way are EIGRP and OSPF similar?

- A. They both support unequal-cost load balancing
- B. They both support MD5 authentication for routing updates.
- C. They have similar CPU usage, scalability, and network convergence times.
- D. They both support autosummarization

Answer: C

NEW QUESTION 278

- (Topic 4)

What is one benefit of implementing a data model language?

- A. accuracy of the operations performed
- B. uses XML style of data formatting
- C. machine-oriented logic and language-facilitated processing.
- D. conceptual representation to simplify interpretation.

Answer: A

NEW QUESTION 281

DRAG DROP - (Topic 4)

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

supports unequal path load balancing

link state routing protocol

distance vector routing protocol

metric is based on delay and bandwidth by default

makes it easy to segment the network logically

constructs three tables as part of its operation: neighbor table, topology table, and routing table

OSPF

EIGRP

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

supports unequal path load balancing

link state routing protocol

distance vector routing protocol

metric is based on delay and bandwidth by default

makes it easy to segment the network logically

constructs three tables as part of its operation: neighbor table, topology table, and routing table

OSPF

link state routing protocol

makes it easy to segment the network logically

constructs three tables as part of its operation: neighbor table, topology table, and routing table

EIGRP

supports unequal path load balancing

distance vector routing protocol

metric is based on delay and bandwidth by default

NEW QUESTION 283

- (Topic 4)
Which of the following protocols has a default administrative distance value of 90?

- A. RIP
- B. EIGRP
- C. OSPF
- D. BGP

Answer: B

Explanation:

This is because EIGRP is an advanced distance vector routing protocol that uses a composite metric to calculate the best path to a destination. EIGRP has a default administrative distance value of 90, which means that it is more trustworthy than RIP (120) or OSPF (110), but less trustworthy than BGP (20). The source of this answer is the Cisco ENCOR v1.1 course, module 4, lesson 4.1: Implementing EIGRP.

NEW QUESTION 286

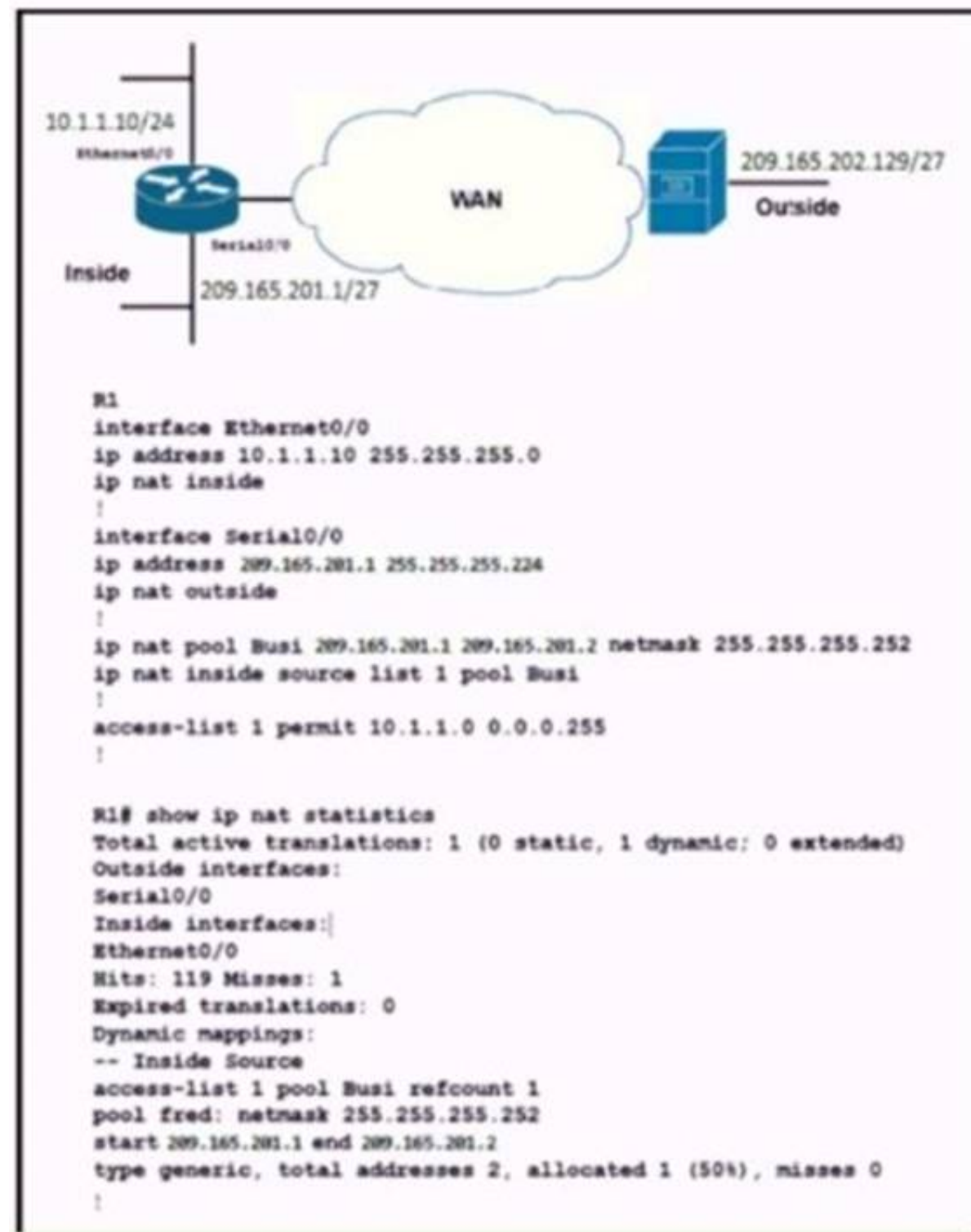
- (Topic 4)
What do Chef and Ansible have in common?

- A. They rely on a declarative approach.
- B. They rely on a procedural approach.
- C. They use YAML as their primary configuration syntax.
- D. They are clientless architectures.

Answer: B

NEW QUESTION 289

- (Topic 4)



Refer to the exhibit. A network engineer configures NAT on R1 and enters the show command to verify the configuration. What does the output confirm?

- A. The first packet triggered NAT to add an entry to the NAT table
- B. R1 is configured with NAT overload parameters.
- C. A Telnet session from 160.1.1.1 to 10.1.1.10 has been initiated.
- D. R1 is configured with NAT overload parameters

Answer: A

NEW QUESTION 292

- (Topic 4)

When a branch location loses connectivity, which Cisco FlexConnect state rejects new users but allows existing users to function normally?

- A. Authentication-Down / Switch-Local
- B. Authentication-Down / Switching-Down
- C. Authentication-Local / Switch-Local
- D. Authentication-Central / Switch-Local

Answer: A

Explanation:

This is because Cisco FlexConnect is a feature that allows wireless access points to operate in standalone mode when they lose connectivity to the wireless LAN controller. Cisco FlexConnect has different states depending on the status of the authentication and switching functions. Authentication-Down means that the access point cannot authenticate new users with the central server, such as a RADIUS server. Switch-Local means that the access point can switch the traffic locally without sending it to the wireless LAN controller. Therefore, Authentication-Down / Switch-Local is the state that rejects new users but allows existing users to function normally. The source of this answer is the Cisco ENCOR v1.1 course, module 7, lesson 7.3: Implementing FlexConnect.

NEW QUESTION 295

- (Topic 4)

When a DNS host record is configured for a new Cisco AireOS WLC, which hostname must be added to allow APs to successfully discover the WLC?

- A. CONTROLLER-CAPWAP-CISCO
- B. CISCO-CONTROLLER-CAPWAP
- C. CAPWAP-CISCO-CONTROLLER
- D. CISCO-CAPWAP-CONTROLLER

Answer: D

NEW QUESTION 299

DRAG DROP - (Topic 4)

An engineer must create a script to append and modify device entries in a JSON-formatted file. The script must work as follows:

? Until interrupted from the keyboard, the script reads in the hostname of a device, its management IP address, operating system type, and CLI remote access protocol.

? After being interrupted, the script displays the entered entries and adds them to

the JSON-formatted file, replacing existing entries whose hostname matches. The contents of the JSON-formatted file are as follows:

```
{
  "examplerouter": {
    "ip": "203.0.113.1",
    "os": "ios-xe",
    "protocol": "ssh"
  },
  ...
}
```

Drag and drop the statements onto the blanks within the code to complete the script. Not all options are used.

ChangedDevices = {}

try:

Name = input('\n\nDevice name: ')

IP = input('Address: ')

OS = input('Operating system: ')

Proto = input('CLI access protocol: ')

ChangedDevices.update({Name: {"ip": IP,

"os": OS, "protocol": Proto}})

(KeyboardInterrupt, EOFError):

pass

print("\n\n==> Entered device entries <==")

print(json.dumps(ChangedDevices, indent=4))

("devicesData.json", "r+")

Devices = json.load(File)

Devices.update(ChangedDevices)

File.seek(0)

json.dump(Devices, File, indent=4)

while True:

except

import json

File.open()

File.close()

File = open

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:


```
import json
ChangedDevices = {}
try:
    while True:
        Name = input('\n\nDevice name: ')
        IP = input('Address: ')
        OS = input('Operating system: ')
        Proto = input('CLI access protocol: ')
        ChangedDevices.update({Name: {"ip": IP,
        "os": OS, "protocol": Proto}})
        File.close() (KeyboardInterrupt, EOFError):
        pass

    print("\n\n==> Entered device entries <==")
    print(json.dumps(ChangedDevices, indent=4))
    File.open() ("devicesData.json", "r+")
    Devices = json.load(File)
    Devices.update(ChangedDevices)
    File.seek(0)
    json.dump(Devices, File, indent=4)
    File = open
```

NEW QUESTION 301

- (Topic 4)

An engineer receives a report that an application exhibits poor performance. On the switch where the server is connected, this syslog message is visible:
SW_MATM4-MACFLAP_N0HF: Host 0054.3831.8253 in vlan 14 is flapping between port GUAM and port Gi1/0/2.
What is causing the problem?

- A. wrong SFP+ and cable connected between the server and the switch
- B. undesirable load-balancing configuration on the switch
- C. failed NIC on the server
- D. invalid port channel configuration on the switch

Answer: B

NEW QUESTION 303

- (Topic 4)

```
monitor session 11 type erspan-source
source interface GigabitEthernet3
destination
erspan-id 12
ip address 10.10.10.10
origin ip address 10.100.10.10
```

Refer to the exhibit. Which command set completes the ERSPAN session configuration?

- ☐ monitor session 12 type erspan-destination
destination interface GigabitEthernet4
source
erspan-id 12
ip address 10.10.10.10
- ☐ monitor session 11 type erspan-destination
destination interface GigabitEthernet4
source
erspan-id 12
ip address 10.100.10.10
- ☐ monitor session 11 type erspan-destination
destination interface GigabitEthernet4
source
erspan-id 11
ip address 10.10.10.10
- ☐ monitor session 12 type erspan-destination
destination interface GigabitEthernet4
source
erspan-id 11
ip address 10.10.10.10

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

NEW QUESTION 304

DRAG DROP - (Topic 4)

Drag and drop the code snippets from the bottom onto the blanks in the Python script to print the device model to the screen and write JSON data to a file Not all options are used

```
import json

data = {
    "measurement": "ifHCInOctets",
    "maxDataPoints": 30,
    "policy": "default",
    "params": None,
    "devices": [
        {"model": "Cisco Nexus 3550", "ipv4": '172.16.16.249'}
    ]
}

[ ] (data["devices"][0]["model"])

with [ ] ("data.json", " [ ] ") as file:
    json. [ ] (data, file, indent=4)
```

dumps

print

dump

open

r

w

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```
import json

data = {
    "measurement": "ifHCInOctets",
    "maxDataPoints": 30,
    "policy": "default",
    "params": None,
    "devices": [
        {"model": "Cisco Nexus 3550", "ipv4": '172.16.16.249'}
    ]
}

dump (data["devices"][0]["model"])
with open ("data.json", " r ") as file:
    json. print (data, file, indent=4)
```

NEW QUESTION 309

- (Topic 4)

Which two functions is an edge node responsible for? (Choose two.)

- A. provides multiple entry and exit points for fabric traffic
- B. provides the default exit point for fabric traffic
- C. provides the default entry point for fabric traffic
- D. provides a host database that maps endpoint IDs to a current location
- E. authenticates endpoints

Answer: AD

NEW QUESTION 311

- (Topic 4)

An engineer must configure GigabitEthernet 0/0 for VRRP group 65. The router must assume the primary role when it has the highest priority in the group. Which command set must be applied?

A)

```
interface GigabitEthernet0/0
ip address 10.10.10.1 255.255.255.0
vrrp 65 ip 10.10.10.1
standby 65 priority 100
standby 65 preempt
```

B)

```
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.255.0
standby 65 ip 10.10.10.1
standby 65 track 1 decrement 10
standby 65 preempt
```

C)

```
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.255.0
vrrp 65 ip 10.20.20.1
vrrp 65 track 1 decrement 100
vrrp 65 preempt
vrrp 65 authentication $2#442619822
```

D)


```
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.255.0
vrrp 65 ip 10.10.10.1
vrrp 65 priority 110
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 312

- (Topic 4)

Why does the vBond orchestrator have a public IP?

to enable vBond to team the public IP of WAN Edge devices that are behind NAT gateways or in private address space

- A. to facilitate downloading and distribution of operational and security patches
- B. to allow for global reachability from all WAN Edges in the Cisco SD-WAN and
- C. to facilitate NAT traversal to provide access
- D. to Cisco Smart Licensing servers for license enablement

Answer: C

NEW QUESTION 315

- (Topic 4)

Which two pieces of information are necessary to compute SNR? (Choose two.)

- A. transmit power
- B. noise floor
- C. EIRP
- D. antenna gain
- E. RSSI

Answer: BE

NEW QUESTION 318

- (Topic 4)

Which signal strength and noise values meet the minimum SNR for voice networks?

- A. signal strength -67 dBm, noise 91 dBm
- B. signal strength -69 dBm, noise 94 dBm
- C. signal strength -68 dBm, noise 89 dBm
- D. signal strength -66 dBm, noise 90 dBm

Answer: A

NEW QUESTION 322

- (Topic 4)

A network engineer wants to configure console access to a router without using AAA so that the privileged exec mode is entered directly after a user provides the correct login credentials. Which action achieves this goal?

- A. Configure login authentication privileged on line con 0.
- B. Configure a local username with privilege level 15.
- C. Configure privilege level 15 on line con 0.
- D. Configure a RADIUS or TACACS+ server and use it to send the privilege level.

Answer: C

NEW QUESTION 325

- (Topic 4)

A company hires a network architect to design a new OTT wireless solution within a Cisco

SD-Access Fabric wired network. The architect wants to register access points to the WLC to centrally switch the traffic. Which AP mode must the design include?

- A. Bridge
- B. Fabric
- C. FlexConnect
- D. local

Answer: D

NEW QUESTION 327

- (Topic 4)

Refer to the exhibit.

```
aaa new-model
aaa authentication login default group tacacs+ local
!
tacacs server prod
address ipv4 10.10.10.23
key cisco123
!
ip tacacs source-interface Gig 0/0
```

Which configuration must be applied for the TACACS+ server to grant access-level rights to remote users?

- A. R1(config)# aaa authentication login enable
- B. R1(config)# aaa authorization exec default local if-authenticated
- C. R1(config)# aaa authorization exec default group tacacs+
- D. R1(config)# aaa accounting commands 15 default start-stop group tacacs+

Answer: C

Explanation:

The aaa authorization exec default group tacacs+ command enables TACACS+ exec authorization, which allows the TACACS+ server to grant access-level rights to remote users. Exec authorization determines whether the user can access the privileged EXEC mode or remain in user EXEC mode after authentication. The TACACS+ server can also assign a privilege level to the user based on the configuration of the server. The default keyword specifies that this is the default method list for exec authorization. The group tacacs+ keyword specifies that the TACACS+ server group defined by the tacacs server command is used for authorization. Reference: TACACS+ Configuration Guide - Configuring TACACS [Cisco Cloud Services Router 1000V Series] - Cisco

NEW QUESTION 329

- (Topic 4)

```
Router#sh access-list
Extended IP access list 100
 10 permit tcp any any eq telnet
Extended IP access list 101
 10 permit tcp any any eq 22
```

Refer to the exhibit. Which configuration set implements Control plane Policing for SSH and Telnet?

- ☒ Router(config)#class-map match-all class-control
 - Router(config-cmap)#match access-group 100
 - Router(config-cmap)#match access-group 101
 - Router(config)#policy-map CoPP
 - Router(config-pmap)#class class-control
 - Router(config-pmap-c)#police 1000000 conform-action transmit
 - Router(config)#control-plane
 - Router(config-cp)#service-policy output CoPP
- ☐ Router(config)#class-map type inspect match-all
 - Router(config-cmap)#match access-group 100
 - Router(config-cmap)#match access-group 101
 - Router(config)#policy-map CoPP
 - Router(config-pmap)#class class-control
 - Router(config-pmap-c)#police 1000000 conform-action transmit
 - Router(config)#control-plane
 - Router(config-cp)#service-policy output CoPP

- ☐ Router(config)#class-map class-telnet
Router(config-cmap)#match access-group 100
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP

Router(config-pmap)#class class-telnet-ssh
Router(config-pmap-c)#police 1000000 conform-action transmit
Router(config)#control-plane
Router(config-cp)#service-policy input CoPP
- ☒ Router(config)#class-map match-any class-control
Router(config-cmap)#match access-group 100
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP

Router(config-pmap)#class class-control
Router(config-pmap-c)#police 1000000 conform-action transmit
Router(config)#control-plane
Router(config-cp)#service-policy input CoPP

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 332

- (Topic 4)

```
list = [1, 2, 3, 4]
list[3] = 10
print(list)
```

Refer to the exhibit. What is the value of the variable list after the code is run?

- A. [1, 2, 10]
- B. [1, 2, 3, 10]
- C. [1, 2, 10, 4]
- D. [1, 10, 10, 10]

Answer: B

NEW QUESTION 337

- (Topic 4)

If AP power level is increased from 25 mW to 100 mW. what is the power difference in dBm?

- A. 6 dBm
- B. 14 dBm
- C. 17 dBm
- D. 20 dBm

Answer: D

NEW QUESTION 341

- (Topic 4)

In Cisco DNA Center, what is the integration API?

- A. southbound consumer-facing RESTful AP
- B. which enables network discovery and configuration management
- C. westbound interface, which allows the exchange of data to be used by ITS
- D. IPAM and reporting
- E. an interface between the controller and the network devices, which enables network discovery and configuration management
- F. northbound consumer-facing RESTful API, which enables network discovery and configuration management

Answer: B

NEW QUESTION 345

DRAG DROP - (Topic 4)

Drag and drop the code snippets from the bottom onto the blanks in the code to construct a request that configures a deny rule on an access list?

```
{
  "ip": {
    "access-list": {
      "ios-acl:extended": {
        "ios-acl:name": "ato",
        "ios-acl:": {
          "ios-acl:sequence": "111111",
          "ios-acl:ace-rule": {
            "ios-acl:action": "",
            "ios-acl:protocol": "",
            "ios-acl:any": "",
            "ios-acl:": ""
          }
        }
      }
    }
  }
}
```

deny

access-list-seq-rule

dst-any

ip

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```
{
  "ip": {
    "access-list": {
      "ios-acl:extended": {
        "ios-acl:name": "ato",
        "ios-acl:dst-any": {
          "ios-acl:sequence": "111111",
          "ios-acl:ace-rule": {
            "ios-acl:action": "deny",
            "ios-acl:protocol": "ip",
            "ios-acl:any": "",
            "ios-acl:access-list-seq-rule": ""
          }
        }
      }
    }
  }
}
```

deny

access-list-seq-rule

dst-any

ip

NEW QUESTION 348

- (Topic 4)

Which JSON script is properly formatted?

A)

```
[
  "Session":{
    "title":"Writing 201",
    "grade":"11",
    "location":"Maine",
  }
]
```

B)

```
{
  "river": [
    {
      "name":"Mississippi",
      "state":"Louisiana",
      "ranking":"13"
    }
  ]
}
```

C)

```
"paint":[
  {
    "type":"indoor",
    "color":"white",
    "sheen":"satin"
  }]
}
```

D)

```
{
  "file":
  [
    "name":"File_4616,
    "location":"User_files",
    "bytes":"13070",
  ]
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Option A is the properly formatted JSON script. JSON (JavaScript Object Notation) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client, so it can be displayed on a web page, or vice versa). The JSON syntax rules are as follows¹²:

? Data is in name/value pairs, separated by commas. A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value: "name": "value".

? Curly braces hold objects. An object can contain multiple name/value pairs: {"name": "value", "name": "value", ...}.

? Square brackets hold arrays. An array can contain multiple values, separated by commas: ["value", "value", ...].

? Values can be strings (in double quotes), numbers, booleans (true or false), null, objects, or arrays.

Option A follows these rules and is a valid JSON script. It defines an object with four name/value pairs: "name", "age", "hobbies", and "address". The value of "name" is a string, the value of "age" is a number, the value of "hobbies" is an array of strings, and the value of "address" is another object with two name/value pairs: "city" and "country". The object is enclosed in curly braces and the name/value pairs are separated by commas.

Option B is not a valid JSON script because it uses single quotes instead of double quotes for the field names and string values. JSON requires double quotes for strings¹².

Option C is not a valid JSON script because it does not use commas to separate the name/value pairs. JSON requires commas to separate the data elements within an object or an array¹².

Option D is not a valid JSON script because it uses a semicolon instead of a colon to separate the field name and the value. JSON requires a colon to separate the name and the value in a name/value pair¹². References: 1: JSON Introduction, 2: JSON Syntax

NEW QUESTION 351

- (Topic 4)

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip address 10.0.0.3 255.255.255.0
Router(config-if)# standby 512 ip 10.0.0.1
```

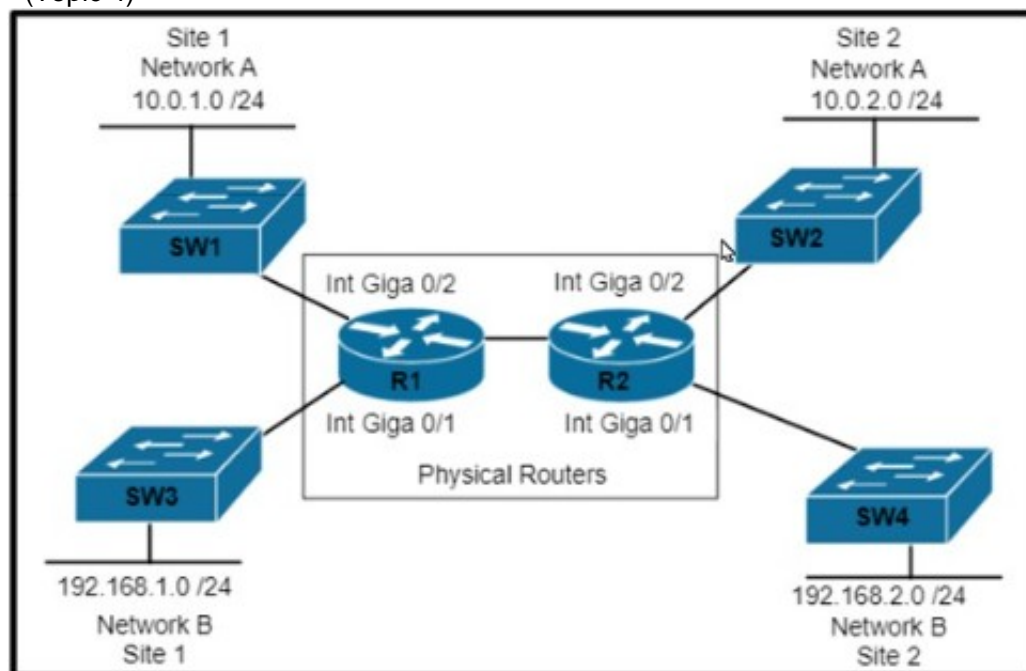
Refer to the exhibit. An engineer attempts to configure standby group 512 on interface GigabitEthernet0/1, but the configuration is not accepted. Which command resolves this problem?

- A. standby version 2
- B. standby 512 preempt
- C. standby redirects
- D. standby 512 priority 100

Answer: A

NEW QUESTION 354

- (Topic 4)



Refer to the exhibit. Which set of commands is required to configure and verify the VRF for Site 1 Network A on router R1?

- ☐ R1#ip routing
R1#(config)#ip vrf 100
!
R1(config)#interface Gi0/2
R1(config-if)#ip address 10.0.1.1 255.255.255.0

R1#show ip route
- ☐ R1#ip routing
R1#(config)#ip vrf 100
R1#(config-vrf)#rd 100:1
R1#(config-vrf)# address family ipv4
!
R1(config)#interface Gi0/2
R1(config-if)#ip address 10.0.1.1 255.255.255.0

R1#show ip route
- ☐ R1#ip routing
R1#(config)#ip vrf 100
!
R1(config)#interface Gi0/2
R1(config-if)#ip address 10.0.1.1 255.255.255.0

R1#show ip vrf
- ☐ R1#ip routing
R1#(config)#ip vrf 100
!
R1(config)#interface Gi0/2
R1(config-if)#ip vrf forwarding 100
R1(config-if)#ip address 10.0.1.1 255.255.255.0

R1#show ip vrf

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 358

- (Topic 4)

```
>tracert www.crmABC.com
Tracing route to www.crmABC.com [192.168.100.1]
 0  3ms    5ms    3ms    10.10.10.1
 1  4ms    6ms    4ms    10.100.100.1
 2  4ms    6ms    4ms    10.100.200.1

 4  4ms    6ms    4ms    10.100.100.1
 5  4ms    6ms    4ms    10.100.200.1
 6  4ms    6ms    4ms    10.100.100.1
 7  4ms    6ms    4ms    10.100.200.1
<output truncated>
```

Refer to the exhibit Users cannot reach the web server at 192.168.100.1. What is the root cause for the failure?

- A. The server is attempting to load balance between links 10.100.100.1 and 10.100.200.1.
- B. The server is out of service.
- C. There is a loop in the path to the server.
- D. The gateway cannot translate the server domain name.

Answer: C

NEW QUESTION 361

- (Topic 4)

```
line vty 0 4
  exec-timeout 120 0
  login local

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

Refer to the exhibit. An engineer must update the existing configuration to achieve these results:

- Only administrators from the 192.168.1.0/24 subnet can access the vty lines.

* Access to the vty lines using clear-text protocols is prohibited. Which command set should be applied?

A)

```
access-list 1 permit 192.168.1.0 255.255.255.0
line vty 0 15
 access-class 1 in
 transport input telnet rlogin
```

B)

```
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 15
access-class 1 in
line vty 0 15
access-class 1 in
transport input none
```

C)

```
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 15
access-class 1 in
transport input ssh
```

D)

```
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 15
access-class 1 in
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

Option B is the correct command set to update the existing configuration to achieve the desired results. The configuration steps are as follows¹²:

? Define a standard access list that permits only the administrators from the 192.168.1.0/24 subnet to access the vty lines. In this case, the access list is named ADMIN and it allows any host with an IP address in the range of 192.168.1.1 to 192.168.1.254 to access the vty lines: ip access-list standard ADMIN and permit 192.168.1.0 0.0.0.255.

? Apply the access list to the vty lines using the access-class command. This command restricts incoming and outgoing connections between a particular vty and the addresses in the access list. In this case, the access list ADMIN is applied to the vty lines 0 to 15 in the inbound direction, which means that only the hosts that match the access list can initiate a connection to the vty lines: line vty 0 15 and access-class ADMIN in.

? Disable the clear-text protocols such as Telnet for the vty lines using the transport input command. This command specifies which protocols are allowed for incoming connections. In this case, only SSH is allowed for the vty lines, which is a secure protocol that encrypts the data between the client and the server: transport input ssh.

Option A is incorrect because it does not apply the access list to the vty lines, which is required to restrict the access to the administrators from the 192.168.1.0/24 subnet. Without the access-class command, any host can attempt to connect to the vty lines¹².

Option C is incorrect because it does not disable the clear-text protocols for the vty lines, which is required to prohibit the access to the vty lines using unsecure protocols. Without the transport input ssh command, both Telnet and SSH are allowed for the vty lines by default¹².

Option D is incorrect because it uses an extended access list instead of a standard access list, which is not recommended for controlling access to the vty lines. An extended access list requires more configuration and processing than a standard access list, and it cannot be applied directly to the vty lines. It has to be applied to each interface that can be used to access the vty lines, which increases the complexity and the possibility of errors¹². References: 1: Controlling Access to a Virtual Terminal Line, 2: Configuring Secure Shell

NEW QUESTION 365

- (Topic 4)

```
!
interface FastEthernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
!
interface FastEthernet0/2
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
access-list 10 permit 10.10.10.0 0.0.0.255
!
```

Refer to the exhibit. Which command allows hosts that are connected to FastEthernet0/2 to access the Internet?

- A. ip nat inside source list 10 interface FastEthernet0/1 overload
- B. ip nat inside source list 10 interface FastEthernet0/2 overload
- C. ip nat outside source list 10 interface FastEthernet0/2 overload

D. ip nat outside source static 209.165.200.225 10.10.10.0 overload

Answer: A

NEW QUESTION 368

- (Topic 4)

What is a benefit of YANG modules?

- A. tightly coupled models with encoding to improve performance
- B. easier multivendor interoperability provided by common or industry models
- C. avoidance of ecosystem fragmentation by having fixed that cannot be changed
- D. single protocol and model couple to simplify maintenance and supported

Answer: B

NEW QUESTION 370

- (Topic 4)

Which configuration enables a device to be configured via NETCONF over SSHv2?

A)

```
hostname Device
!
username admin password 0 admin
!
ip domain-name cisco.com
crypto key generate rsa modulus 2048
ip ssh version 2
!
netconf-yang
!
line vty 0 15
login local
```

B)

```
hostname Device
!
aaa new-model
!
username cisco privilege 15 password cisco
!
ip domain-name cisco.com
crypto key generate rsa modulus 2048
ip ssh version 2
!
aaa authentication login default local
aaa authorization exec default local
!
netconf-yang
netconf ssh
```

C)


```
hostname Device
!
aaa new-model
!
username admin privilege 15 password 0 admin
!
ip domain-name cisco.com
crypto key generate rsa modulus 2048
ip ssh version 2
!
netconf-yang
```

D)

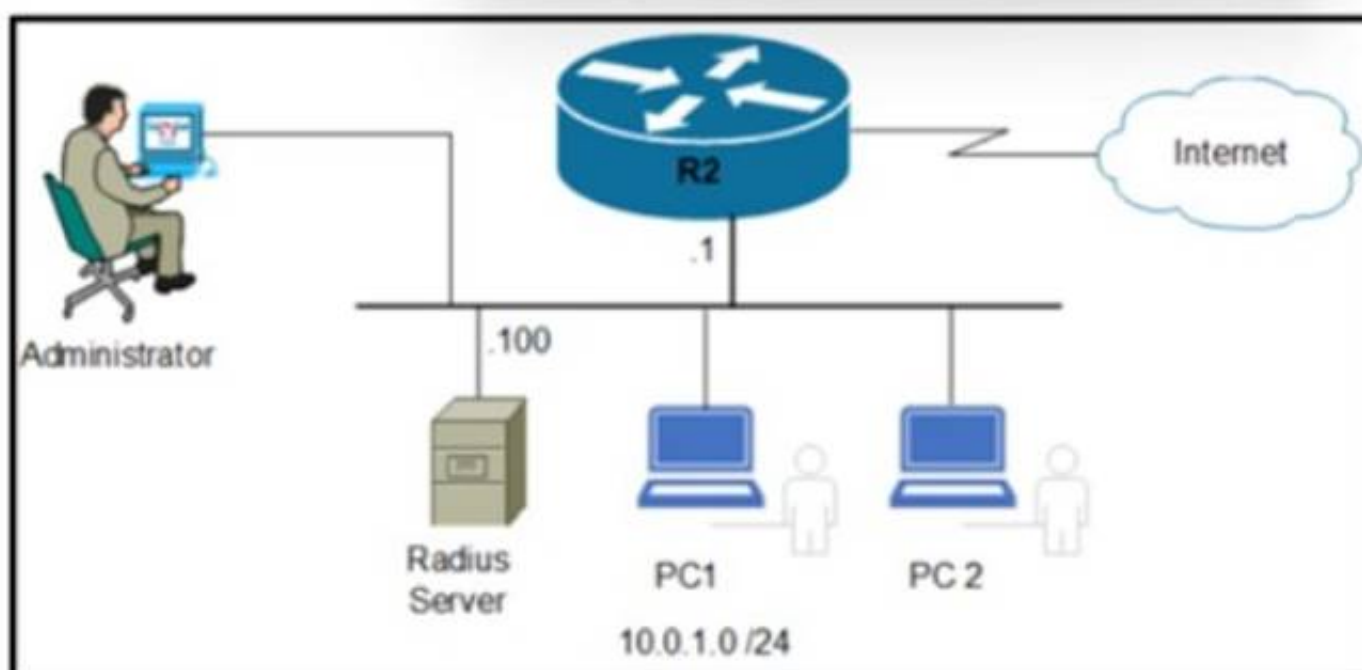
```
hostname Device
!
username cisco1 privilege 15 password 0 cisco1
!
ip domain-name cisco.com
crypto key generate rsa modulus 2048
ip ssh version 2
!
netconf ssh
!
line vty 0 15
login local
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 373

- (Topic 4)



Refer to the exhibit. An engineer must save the configuration of router R2 using the NETCONF protocol. Which script must be used?

- ☐ `<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
 <cisco-ia:reset xmlns:cisco-ia="http://cisco.com/yang/cisco-ia">
 <cisco-ia:reinitialize>true</cisco-ia:reinitialize>
 </cisco-ia:reset>
</rpc>`
- ☐ `<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
 <get>
 <filter type="subtree">
 <ncm:netconf-state xmlns:ncm="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">
 <ncm:capabilities/>
 </ncm:netconf-state>
 </filter>
 </get>
</rpc>`
- ☐ `<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
 <cisco-ia:save-config xmlns:cisco-ia="http://cisco.com/yang/cisco-ia"/>
</rpc>`
- ☐ `<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
 <cisco-ia:sync-from xmlns:cisco-ia="http://cisco.com/yang/cisco-ia"></cisco-ia:sync-from>
</rpc>`

- A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

NEW QUESTION 374

- (Topic 4)

Which technology enables a redundant supervisor engine to take over when the primary supervisor engine fails?

- A. NSF
B. graceful restart
C. SSO
D. FHRP

Answer: C

NEW QUESTION 376

- (Topic 4)

Refer to the exhibit.

```
R1#show policy-map control-plane
Control Plane

Service-policy input: CoPP

Class-map: telnet_copp (match-all)
  33 packets, 1998 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group 100
  police:
    cir 8000 bps, bc 1500 bytes
    conformed 33 packets, 1998 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 0 bps, exceed 0 bps

Class-map: class-default (match-any)
  59 packets, 5516 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
R1#sh access-lists 100
Extended IP access list 100
  10 deny tcp host 10.0.0.5 any eq 22 (13 matches)
  20 permit tcp any any eq 22 (2 matches)
  30 deny tcp host 10.0.0.5 any eq telnet (18 matches)
  40 permit tcp any any eq telnet (31 matches)
R1#
```

Which result is achieved by the CoPP configuration?

- A. Traffic that matches entry 10 of ACL 100 is always allowed.
B. Class-default traffic is dropped.
C. Traffic that matches entry 10 of ACL 100 is always allowed with a limited CIR.

D. Traffic that matches entry 10 of ACL 100 is always dropped.

Answer: C

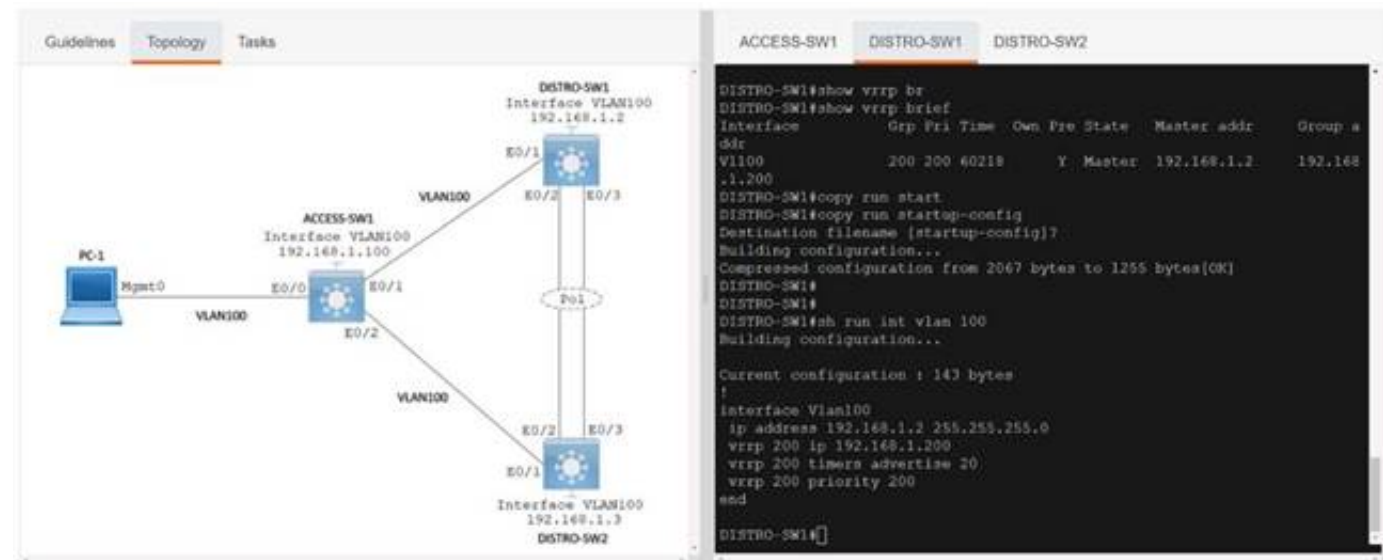
Explanation:

This is because the CoPP configuration shown in the exhibit applies a service policy to the control plane of the router, which is responsible for processing the routing protocols, management protocols, and other control traffic. The service policy uses a class map that matches the access list 100, which permits the traffic with the source IP address 10.1.1.1. The service policy also uses a policy map that sets the committed information rate (CIR) for the matched traffic to 64 kbps, which means that the traffic is guaranteed to have a minimum bandwidth of 64 kbps. The policy map also sets the exceed action to drop, which means that any traffic that exceeds the CIR will be dropped. Therefore, the traffic that matches entry 10 of ACL 100 is always allowed with a limited CIR, and any excess traffic is dropped. The source of this answer is the Cisco ENCOR v1.1 course, module 6, lesson 6.3: Implementing QoS.

NEW QUESTION 380

SIMULATION - (Topic 4)

Simulation 10

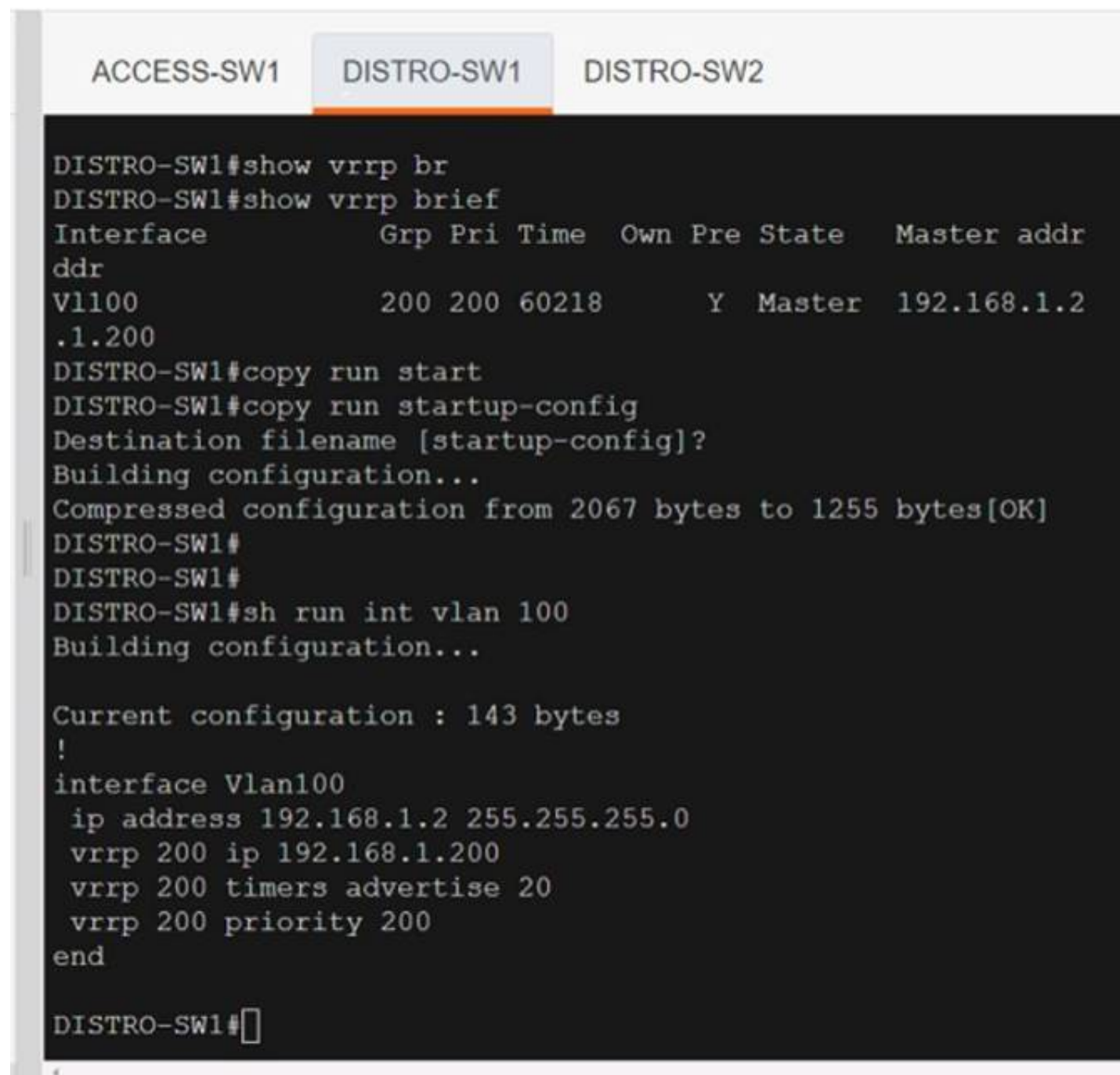


The image shows a network simulation interface with two main panes. The left pane, titled 'Topology', displays a network diagram. It includes a PC-1 connected to a switch labeled 'ACCESS-SW1' (Interface VLAN100, 192.168.1.100). This switch is connected to two distribution switches, 'DISTRO-SW1' (Interface VLAN100, 192.168.1.2) and 'DISTRO-SW2' (Interface VLAN100, 192.168.1.3). The right pane shows the configuration for 'DISTRO-SW1'. It displays the output of 'show vrrp br' and 'show vrrp brief' commands, showing VRRP group 200 on interface Vlan100 with IP 192.168.1.200 as the master. Below this, it shows the configuration of the VRRP group using 'copy run start' and 'copy run startup-config', followed by 'sh run int vlan 100' to display the current configuration for interface Vlan100, which includes IP address, VRRP group, timers, and priority.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



The image shows a network simulation interface with three tabs: 'ACCESS-SW1', 'DISTRO-SW1', and 'DISTRO-SW2'. The 'DISTRO-SW1' tab is selected, showing a terminal window with the following commands and output:

```
DISTRO-SW1#show vrrp br
DISTRO-SW1#show vrrp brief
Interface          Grp Pri Time  Own Pre State  Master addr
ddr
Vl100              200 200 60218      Y  Master  192.168.1.2
.1.200
DISTRO-SW1#copy run start
DISTRO-SW1#copy run startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2067 bytes to 1255 bytes[OK]
DISTRO-SW1#
DISTRO-SW1#
DISTRO-SW1#sh run int vlan 100
Building configuration...

Current configuration : 143 bytes
!
interface Vlan100
 ip address 192.168.1.2 255.255.255.0
 vrrp 200 ip 192.168.1.200
 vrrp 200 timers advertise 20
 vrrp 200 priority 200
end
DISTRO-SW1#
```


ACCESS-SW1 DISTRO-SW1 DISTRO-SW2

```
Building configuration...

Current configuration : 90 bytes
!
interface Vlan100
 ip address 192.168.1.3 255.255.255.0
 vrrp 200 ip 192.168.1.200
end
DISTRO-SW1#show vrrp brief
Interface          Grp Pri Time   Own Pre State   Master addr   Group a
ddr
Vl100              200 200 60218      Y  Master 192.168.1.2   192.168
.1.200
DISTRO-SW1#
```

NEW QUESTION 383

- (Topic 4)

What function does VXLAN perform in a Cisco SD-Access deployment?

- A. data plane forwarding
- B. control plane forwarding
- C. systems management and orchestration
- D. policy plane forwarding

Answer: A

Explanation:

This is because VXLAN is a network virtualization technology that encapsulates Layer 2 frames in UDP headers and allows them to be transported over Layer 3 networks. VXLAN is used in Cisco SD-Access to create virtual networks that span across multiple physical locations and devices. VXLAN performs the data plane forwarding function, which is responsible for moving packets from one point to another based on the destination address. The source of this answer is the Cisco ENCOR v1.1 course, module 9, lesson 9.2: Implementing VXLAN.

NEW QUESTION 388

- (Topic 4)

Refer to the exhibit.

Edit WLAN

Layer 2 Security Mode

WPA + WPA2

MAC Filtering

☐

Protected Management Frame

PMF

Disabled

WPA Parameters

WPA Policy

☐

WPA2 Policy

☒

GTK Randomize

☐

OSEN Policy

☐

WPA2 Encryption

☒ AES(CCMP128)

☐ CCMP256

☐ GCMP128

☐ GCMP256

Auth Key Mgmt

☐ 802.1x

☐ PSK

☐ CCKM

☐ FT + 802.1x

☐ FT + PSK

☐ 802.1x-SHA256

☐ PSK-SHA256

Lobby Admin Access

☐

Fast Transition

Disabled

Over the DS

☐

Reassociation Timeout

20

MPSK Configuration

MPSK

☐

Which action must be taken to configure a WLAN for WPA2-AES with PSK and allow only 802.11r-capable clients to connect?

- A. Change Fast Transition to Adaptive Enabled and enable FT * PSK
- B. Enable Fast Transition and FT + PSK.
- C. Enable Fast Transition and PSK
- D. Enable PSK and FT + PSK.

Answer: A

Explanation:

This is because Fast Transition (FT) is a feature that allows 802.11r-capable clients to roam faster between access points by reducing the authentication and key exchange time. FT can be configured in two modes: adaptive and over-the-DS. Adaptive mode is recommended for mixed environments where both 802.11r-capable and non-capable clients are present, as it allows the access point to negotiate the FT mode with the client. Over-the-DS mode is only suitable for environments where all clients are 802.11r-capable, as it requires the access point to communicate with the previous access point over the distribution system. FT + PSK is a security option that enables FT with pre-shared key (PSK) authentication, which is a simple and common method of securing wireless networks. WPA2-AES is an encryption standard that provides strong security and privacy for wireless networks. The source of this answer is the Cisco ENCOR v1.1 course, module 7, lesson 7.2: Implementing WPA2 and WPA3.

NEW QUESTION 390

- (Topic 4)

Refer to the exhibit.

```
event manager applet CONFIG_BACKUP
action 1.0 cli command "enable"
action 3.0 cli command "end"
action 4.0 cli command "exit"

write_backup.tcl
set output [exec "copy run backup"]
set fd [open "flash:/backup.txt" "w"]
puts $fd $output
close $fd

ios_config "file prompt quiet" "end"
copy flash:/backup.txt tftp://10.1.1.23/backup.txt
ios_config "no file prompt quiet" "end"
file delete -force "flash:/backup.txt"
```

Which statement is needed to complete the EEM applet and use the Tel script to store the backup file?

- A. action 2.0 cli command "write_backup.tcl tcl"
- B. action 2.0 cli command "flash:write_backup.tcl"
- C. action 2.0 cli command "write_backup.tcl"
- D. action 2.0 cli command "telsh flash:write_backup.tcl"

Answer: B

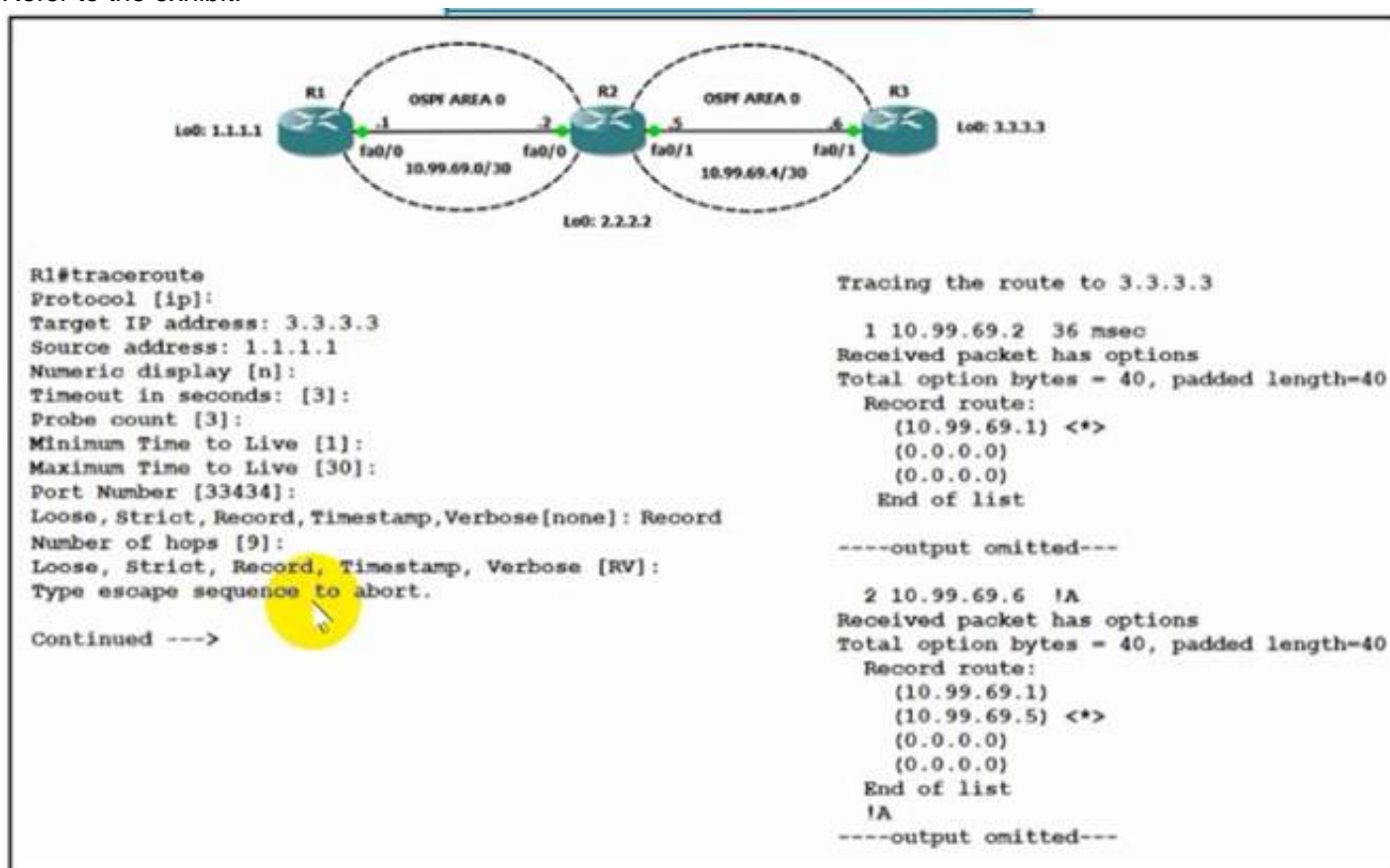
Explanation:

This is because the EEM applet needs to specify the full path of the Tcl script that is stored in the flash memory of the device. The script name is write_backup.tcl and it is used to backup the running configuration to a remote server. The source of this answer is the Cisco ENCOR v1.1 course, module 8, lesson 8.3: Implementing Embedded Event Manager.

NEW QUESTION 392

- (Topic 4)

Refer to the exhibit.



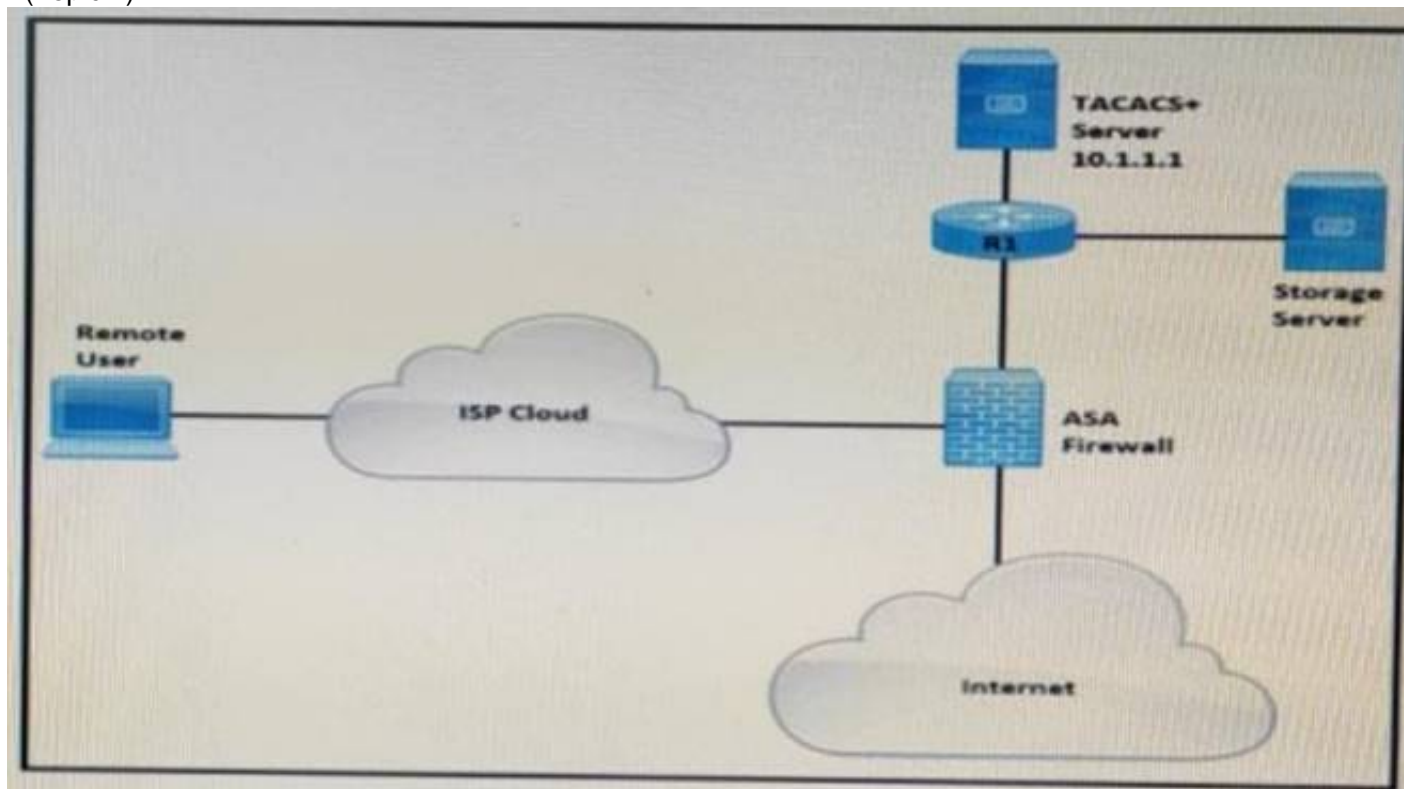
The traceroute fails from R1 to R3. What is the cause of the failure?

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

Answer: C

NEW QUESTION 394

- (Topic 4)



Refer to the exhibit Remote users cannot access the Internet but can upload files to the storage server Which configuration must be applied to allow Internet access?

- A)
- ```
ciscoasa (config)# access-list MAIL_AUTH extended permit tcp any any eq www
ciscoasa (config)# aaa authentication listener http inside redirect
```
- B)
- ```
ciscoasa(config)# access-list MAIL_AUTH extended permit tcp any any eq http
ciscoasa(config)# aaa authentication listener http inside port 43
```
- C)
- ```
ciscoasa(config)# access-list HTTP_AUTH extended permit udp any any eq http
ciscoasa(config)# aaa authentication listener http outside port 43
```
- D)
- ```
ciscoasa(config)# access-list MAIL_AUTH extended permit udp any any eq http
ciscoasa(config)# aaa authentication listener http outside redirect
```

- A. Option A
 B. Option B
 C. Option C
 D. Option D

Answer: A

NEW QUESTION 395

- (Topic 4)

How does Cisco Express Forwarding switching differ from process switching on Cisco devices?

- A. Cisco Express Forwarding switching uses adjacency tables built by the CDP protocol, and process switching uses the routing table.
 B. Cisco Express Forwarding switching uses dedicated hardware processors, and process switching uses the main processor.
 C. Cisco Express Forwarding switching saves memory by storing adjacency tables in dedicated memory on the line cards, and process switching stores all tables in the main memory.
 D. Cisco Express Forwarding switching uses a proprietary protocol based on IS-IS for MAC address lookup, and process switching uses the MAC address table.

Answer: C

NEW QUESTION 398

- (Topic 4)

```

import sqlite3
a= sqlite3.connect('/home/sdwan-lab/user.sqlite3')
b= a.cursor()
c= "select user from monitor_branch where loopbackip='"+ str(ip[i]) + "'"
d= b.execute(c)
e= b.fetchall()
usr= str(e[0])
usr= usr.replace("'", "")
usr= usr.replace(",)", ",")
  
```

Refer to the exhibit What does this Python script do?

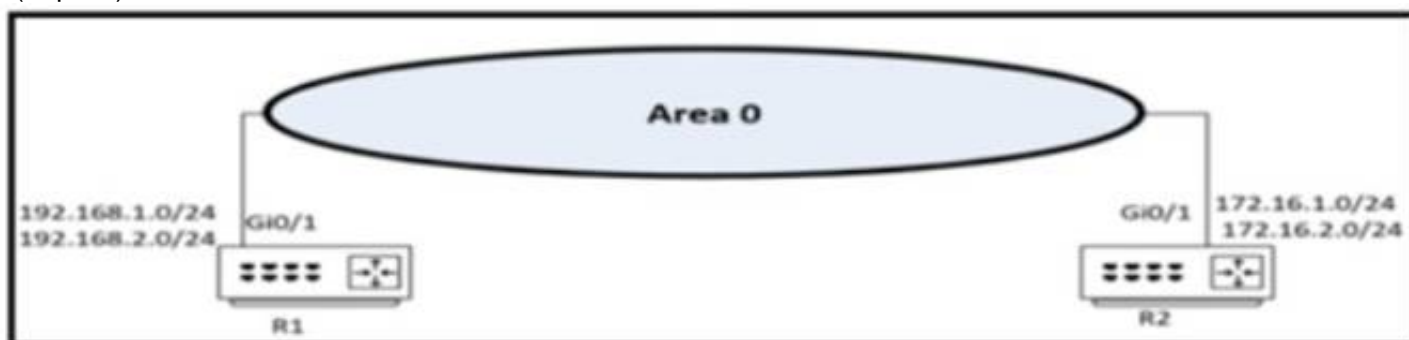
- A. enters the RAOIUS username for a specific IP address

- B. writes the username for a specific IP address into a light database
- C. enters the TACACS* username for a specific IP address
- D. reads the username for a specific IP address from a light database

Answer: B

NEW QUESTION 401

- (Topic 4)



Refer to the exhibit. Which two configurations enable R1 and R2 to advertise routes into OSPF? (Choose two)

A)

```
R2
router ospf 0
network 172.16.1.0 255.255.255.0 area 0
network 172.16.2.0 255.255.255.0 area 0
```

B)

```
R2
router ospf 0
network 172.16.1.0 0.0.0.255 area 0
network 172.16.2.0 255.255.255.0 area 0
```

C)

```
R1
router ospf 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
```

D)

```
R2
router ospf 0
network 172.16.1.0 0.0.0.255 area 0
network 172.16.2.0 0.0.0.255 area 0
```

E)

```
R1
router ospf 0
network 192.168.1.0 255.255.255.0 area 0
network 192.168.2.0 255.255.255.0 area 0
```

- A. Option A
- B. Option B
- C. Option C
- D. Option DE) Option E

Answer: CD

NEW QUESTION 403

- (Topic 4)

```

1 def main():
2     vlans = {'vlan10':'192.168.1.0',
3             'vlan20':'192.168.2.0',
4             'vlan30':'192.168.3.0' }
5     vlans_key(vlans)
6
7 def vlans_key(vlans):
8     for key in vlans.keys():
9         print(str(key) + ' ' + str(vlans[key]))
10
11 if __name__ == '__main__':
12     main()

```

Refer to the exhibit. What is printed to the console when this script is run?

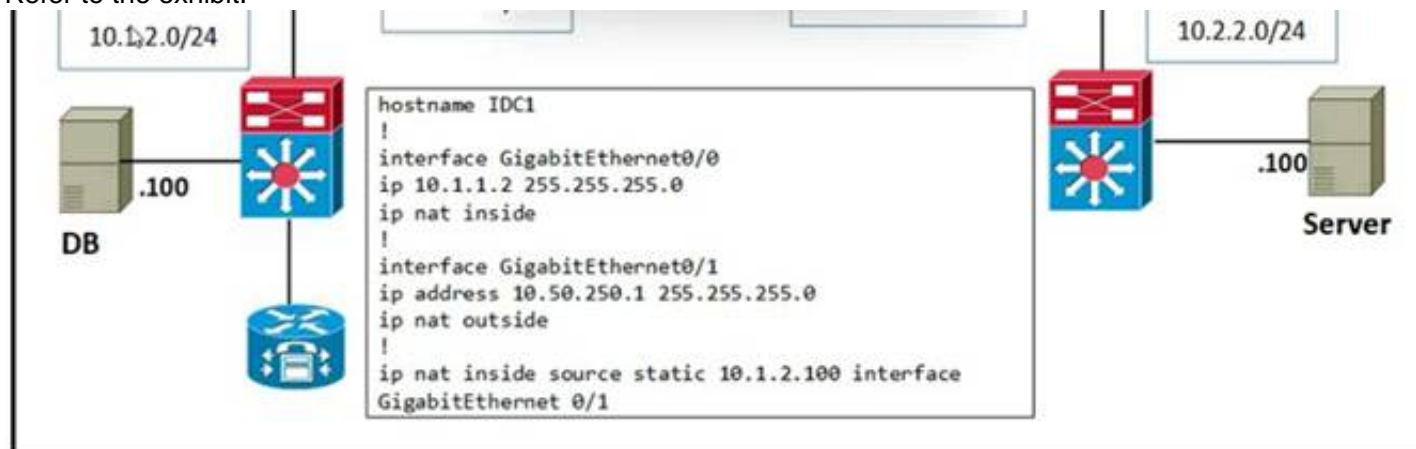
- A. a key-value pair in tuple type
- B. a key-value pair in list type
- C. a key-value pair in string type
- D. an error

Answer: C

NEW QUESTION 407

- (Topic 4)

Refer to the exhibit.



The server in DC2 is expecting traffic from the database in DC1 to use the source network of 10.50.250.0/24. The server sends the initial request. The inside global IP is configured for 10.50.250.1. What is the result of this configuration?

- A. Only the server can initiate communication.
- B. The server and the database cannot communicate.
- C. The server and the database can initiate communication.
- D. Only the database can initiate communication

Answer: C

NEW QUESTION 410

- (Topic 2)

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

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

Answer: A

Explanation:

The following different OSPF types are compatible with each other:

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

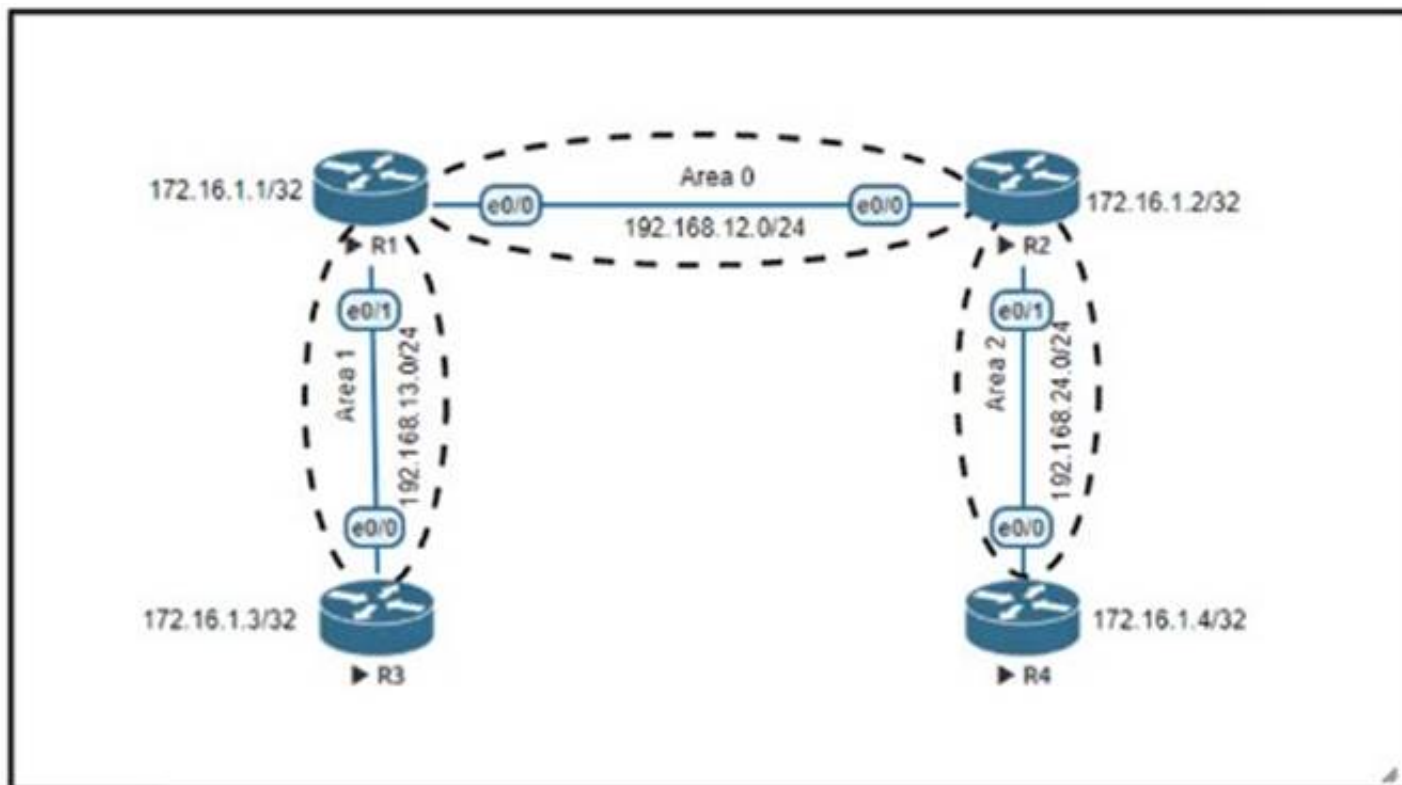
+ Point-to-Point and Point-to-Multipoint (adjust hello/dead timers)

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

NEW QUESTION 414

- (Topic 2)

Refer to the exhibit.



An engineer must create a configuration that prevents R3 from receiving the LSA about 172.16.1.4/32. Which configuration set achieves this goal?

- ☐ On R1
ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32
ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32

router ospf 200
area 1 filter-list prefix INTO-AREA1 out
- ☐ On R3
ip access-list standard R4_L0
deny host 172.16.1.4
permit any

router ospf 200
distribute-list R4_L0 in
- ☐ On R1
ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32
ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32

router ospf 200
area 1 filter-list prefix INTO-AREA1 in
- ☐ On R3
ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32
ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32

router ospf 200
area 1 filter-list prefix INTO-AREA1 in

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 418

- (Topic 2)

A network engineer configures a WLAN controller with increased security for web access. There is IP connectivity with the WLAN controller, but the engineer cannot start a management session from a web browser. Which action resolves the issued

- A. Disable JavaScript on the web browser
- B. Disable Adobe Flash Player
- C. Use a browser that supports 128-bit or larger ciphers.
- D. Use a private or incognito session.

Answer: C

NEW QUESTION 419

- (Topic 2)

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

commands incorrectly? (Choose two.)

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

Answer: CD

NEW QUESTION 420

- (Topic 2)

What is YANG used for?

- A. scraping data via CLI
- B. processing SNMP read-only polls
- C. describing data models
- D. providing a transport for network configuration data between client and server

Answer: C

NEW QUESTION 423

- (Topic 2)

What are two benefits of implementing a Cisco SD-WAN architecture? (Choose two)

- A. It provides resilient and effective traffic flow using MPLS.
- B. It improves endpoint protection by integrating embedded and cloud security features.
- C. It allows configuration of application-aware policies with real time enforcement.
- D. It simplifies endpoint provisioning through standalone router management
- E. It enforces a singl
- F. scalabl
- G. hub-and-spoke topology.

Answer: CD

Explanation:

The top SD-WAN benefits are:

- + Increased bandwidth at a lower cost
- + Centralized management across branch networks
- + Full visibility into the network
- + Providing organizations with more connection type options and vendor selection when building a network.

Reference: <https://www.sdxcentral.com/networking/sd-wan/definitions/sd-wan-technology/>

-> We can provision endpoints (vEdges) through a centralized router vManage -> Answer D is correct.

Answer A is not correct as we can use different kind of connections on SD-WAN: MPLS, LTE, 4G, xDSL, Internet connections...

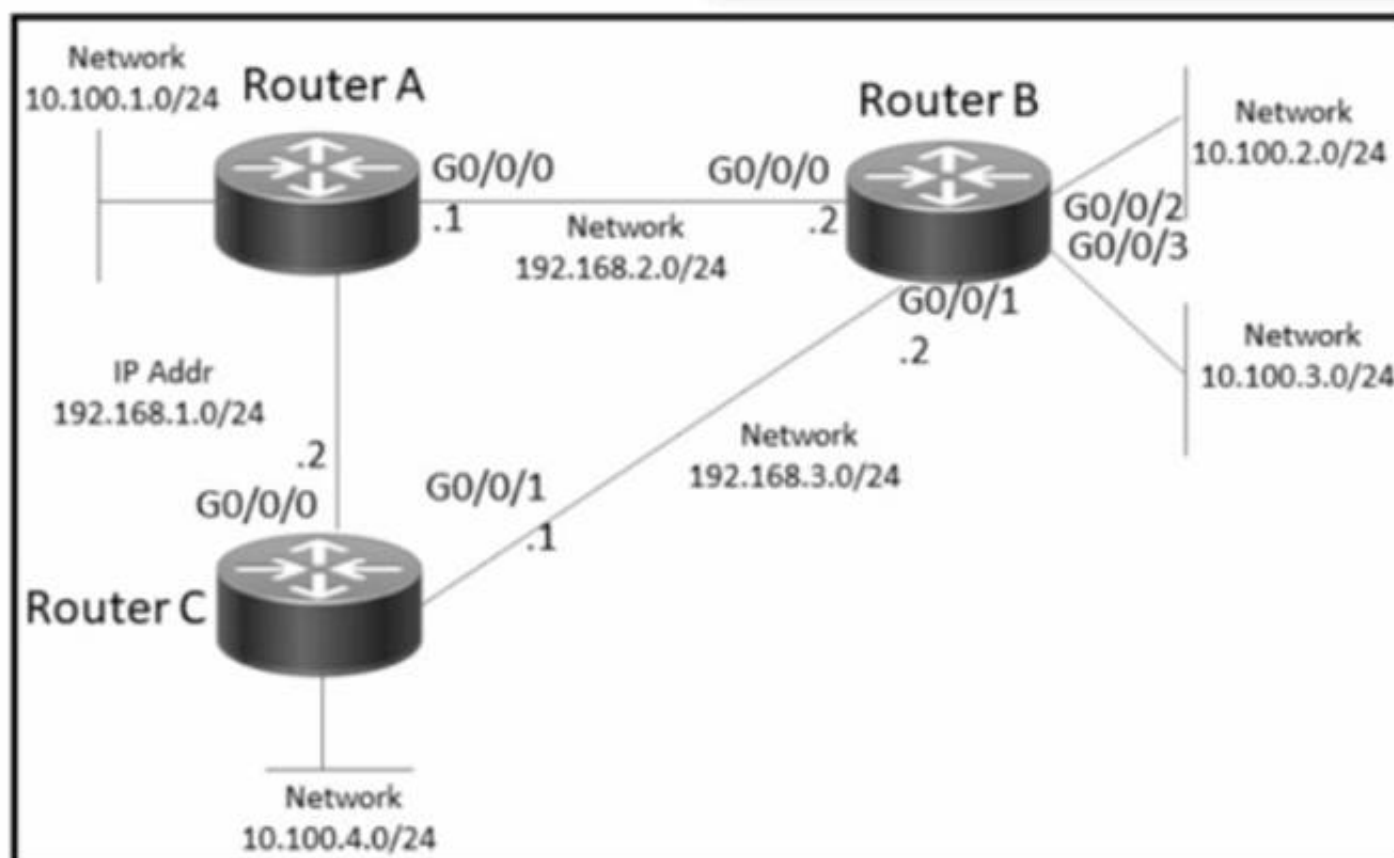
Application-Aware Routing policy is configured in vManage as a centralized data policy that maps the service- side application(s) to specific SLA requirements.

The centralized policies provisioned in vSmart controller is pushed to relevant WAN Edge devices for enforcement. The defined policy consists of match- action pairs, where the match statement defines the application-list or the type of traffic to match, and the action statement defines the SLA action the WAN Edge devices must enforce for the specified traffic.

Reference: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan- application-awarerouting-deploy-guide.html>

NEW QUESTION 428

- (Topic 4)



Refer to the exhibit. A network administrator must configure router B to allow traffic only from network 10.100.2.0 to networks outside of router 0. Which configuration must be applied?

A)
RouterB(config)# access-list 101 permit ip 10.100.3.0 0.0.0.255 any
RouterB(config)# access-list 101 deny any
RouterB(config)# int g0/0/0
RouterB(config-if)# ip access-group 101 out
RouterB(config)# int g0/0/1
RouterB(config-if)# ip access-group 101 out

B)
RouterB(config)# access-list 101 permit ip 10.100.2.0 0.0.0.255 any
RouterB(config)# access-list 101 deny any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in

C)
RouterB(config)# access-list 101 permit ip 10.100.2.0 0.0.0.255 any
RouterB(config)# access-list 101 deny any
RouterB(config)# int g0/0/0
RouterB(config-if)# ip access-group 101 out

D)
RouterB(config)# access-list 101 permit ip 10.100.2.0 0.0.0.255 any
RouterB(config)# int g0/0/0
RouterB(config-if)# ip access-group 101 out
RouterB(config)# int g0/0/1
RouterB(config-if)# ip access-group 101 out

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 432

- (Topic 4)

Why would an architect use an OSPF virtual link?

- A. to allow a stub area to transit another stub area
- B. to connect two networks that have overlapping private IP address space
- C. to merge two existing Area 0s through a nonbackbone
- D. to connect a nonbackbone area to Area 0 through another nonbackbone area

Answer: D

Explanation:

A virtual link is a logical connection between two OSPF routers that belong to different areas but share a common border with a transit area. A virtual link allows an OSPF router to participate in the backbone area (Area 0) even if it is not physically connected to it. This way, the OSPF network can maintain connectivity and routing consistency across all areas. A virtual link is configured between the OSPF router IDs of the two routers that need to be connected to the backbone area¹²³.

Option A is incorrect because a stub area is an area that does not receive external routes from other autonomous systems or other OSPF areas. A stub area can only transit traffic to and from the backbone area, and it cannot be used as a transit area for a virtual link¹². Option B is incorrect because a virtual link does not change the IP address space of the networks that it connects. A virtual link is transparent to the IP layer and only affects the OSPF routing protocol. To connect two networks that have overlapping private IP address space, other solutions such as NAT or VPN are required¹².

Option C is incorrect because a virtual link cannot merge two existing Area 0s through a nonbackbone area. A virtual link can only extend an existing Area 0 through a nonbackbone area. If there are two separate Area 0s in an OSPF network, they cannot be merged by a virtual link, and the network is considered to be partitioned. A partitioned network can cause routing loops and inconsistencies, and it should be avoided¹². References: 1: Configure OSPF Connection in a Virtual Link

Environment, 2: How to configure OSPF Virtual Link, 3: Understand OSPF Areas and Virtual Links

NEW QUESTION 434

DRAG DROP - (Topic 4)

Drag and drop the snippets onto the blanks within the code to construct a script that brings up the failover Ethernet port if the primary port goes down and also shuts down the failover port when the primary returns to service. Not all options are used.


```

event manager applet SRV-1-Up
event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9, changed state to [ ]"
action 1.0 cli command "enable"
action 2.0 cli command "configure terminal"
action 3.0 cli command "Interface GigabitEthernet3/0/10"
action 4.0 cli command "no shutdown"
action 5.0 cli command "end"
event manager applet SRV-1-Down
event syslog pattern "Line protocol on Interface [ ] , changed state to up"
action 1.0 cli command "enable"
action 2.0 cli command "configure terminal"
action 3.0 cli command "Interface GigabitEthernet3/0/10"
action 4.0 cli command "[ ]"
action 5.0 cli command "end"

```

Shutdown

Up

GigabitEthernet3/0/10

No shutdown

Down

GigabitEthernet4/0/9

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

```

event manager applet SRV-1-Up
event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9, changed state to [Down]"
action 1.0 cli command "enable"
action 2.0 cli command "configure terminal"
action 3.0 cli command "Interface GigabitEthernet3/0/10"
action 4.0 cli command "no shutdown"
action 5.0 cli command "end"
event manager applet SRV-1-Down
event syslog pattern "Line protocol on Interface [GigabitEthernet4/0/9] , changed state to up"
action 1.0 cli command "enable"
action 2.0 cli command "configure terminal"
action 3.0 cli command "Interface GigabitEthernet3/0/10"
action 4.0 cli command "[Shutdown]"
action 5.0 cli command "end"

```

Shutdown

Up

GigabitEthernet3/0/10

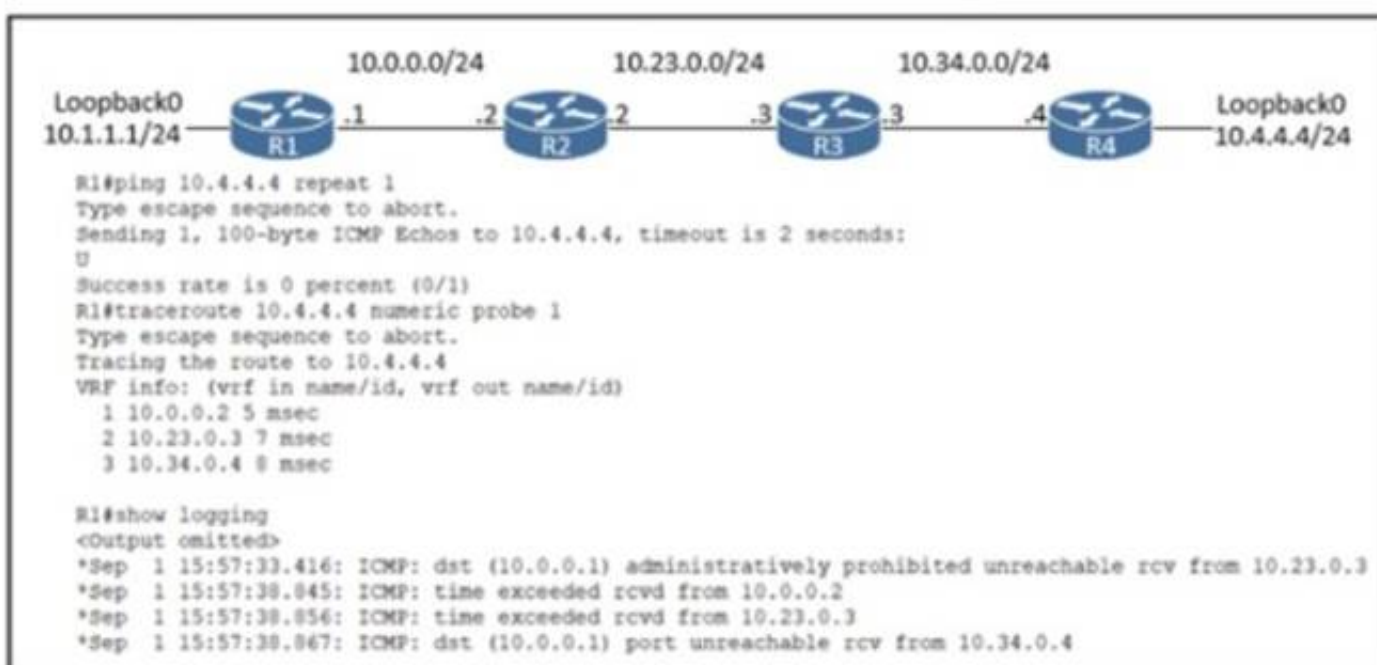
No shutdown

Down

GigabitEthernet4/0/9

NEW QUESTION 439

- (Topic 4)



Refer to the exhibit. What is the cause of the communication failure between R1 and R4?

- A. R1 is configured with the no ip unreachable command.
 B. R2 is denying ICMP
 C. R4 is denying ICMP.
 D. R3 is denying ICMP.

Answer: A

NEW QUESTION 440

- (Topic 4)

Refer to the exhibit.

```
R1#show access-list 100
Extended IP access list 100
 10 deny ip any any
 20 permit ip 192.168.0.0 0.0.255.255 any
 30 permit ip any 192.168.0.0 0.0.255.255
```

Extended access-list 100 is configured on interface GigabitEthernet 0/0 in an inbound direction, but it does not have the expected behavior of allowing only packets to or from 192.168.0.0/16. Which command set properly configures the access list?

- A. R1(config)#no access-list 100 seq 10 R1(config)#access-list 100 seq 40 deny ip any any
- B. R1(config)#ip access-list extended 100 R1(config-ext-nacl)#no 10
- C. R1(config)#no access-list 100 deny ip any any
- D. R1(config)#ip access-list extended 100 R1(config-ext-nacl)#5 permit to any any

Answer: A

NEW QUESTION 443

- (Topic 4)

What are two characteristics of Cisco SD-Access elements? (Choose two.)

- A. The border node is required for communication between fabric and nonfabric devices.
- B. Traffic within the fabric always goes through the control plane node.
- C. Fabric endpoints are connected directly to the border node.
- D. The control plane node has the full RLOC-to-EID mapping database.
- E. The border node has the full RLOC-to-EID mapping database.

Answer: AD

NEW QUESTION 447

- (Topic 4)

In a campus network design, what are two benefits of using BFD for failure detection? (Choose two.)

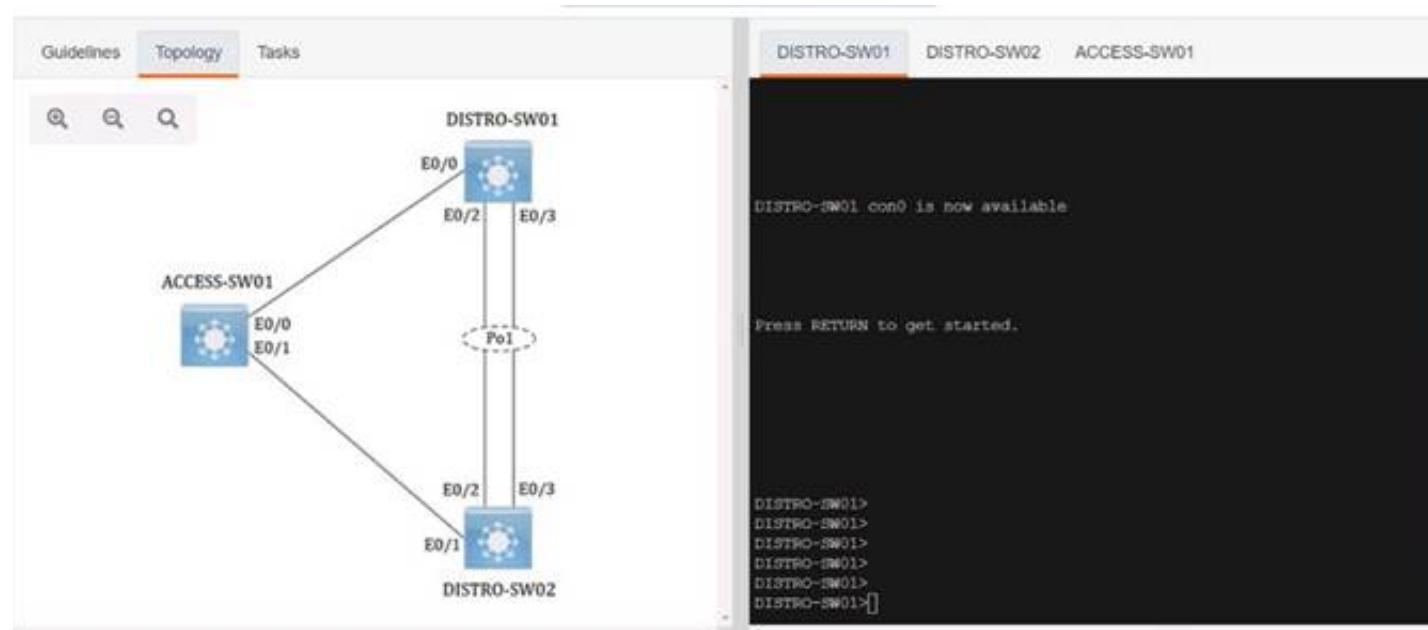
- A. BFD provides path failure detection in less than a second.
- B. BFD is an efficient way to reduce memory and CPU usage.
- C. BFD provides fault tolerance by enabling multiple routers to appear as a single virtual router.
- D. BFD speeds up routing convergence time.
- E. BFD enables network peers to continue forwarding packets in the event of a restart.

Answer: AB

NEW QUESTION 449

SIMULATION - (Topic 4)

Simulation 06



Guidelines
Topology
Tasks

The operations team started configuring network devices for a new site. Complete the configurations to achieve these goals:

1. Ensure that port channel Po1 between DISTRO-SW01 and DISTRO-SW02 is operational using the LACP protocol. Configuration changes for this task must be made on DISTRO-SW01.
2. Ensure that traffic on VLAN 10 is carried as untagged traffic between DISTRO-SW01 and DISTRO-SW02.
3. Complete the Rapid-PVST+ configuration on DISTRO-SW2 by ensuring it is the secondary root switch for all VLANs in the range of 1 to 1005.

[Submit feedback about this item](#)

DISTRO-SW01
DISTRO-SW02
ACCESS-SW01

DISTRO-SW01 con0 is now available

Press RETURN to get started.

DISTRO-SW01>
DISTRO-SW01>
DISTRO-SW01>
DISTRO-SW01>

```

DISTRO-SW01#config t
Enter configuration commands, one per line. End with CNTL/Z.
DISTRO-SW01(config)#int et0/0
DISTRO-SW01(config-if)#no chan
DISTRO-SW01(config-if)#no channel-gr
DISTRO-SW01(config-if)#no channel-group 1 mo
DISTRO-SW01(config-if)#no channel-group 1 mode passi
DISTRO-SW01(config-if)#no channel-group 1 mode passive
DISTRO-SW01(config-if)#
*Jan  4 10:02:14.924: %LINEPROTO-5-UPDOWN: Line protocol on Interface
hernet0/0, changed state to up
DISTRO-SW01(config-if)#shut
DISTRO-SW01(config-if)#no shut
DISTRO-SW01(config-if)#

```

```

DISTRO-SW01(config)#int ra
DISTRO-SW01(config)#int range et0/2 - 3
DISTRO-SW01(config-if-range)#chan
DISTRO-SW01(config-if-range)#channel-gr
DISTRO-SW01(config-if-range)#channel-group 1 mod
DISTRO-SW01(config-if-range)#channel-group 1 mode ac
DISTRO-SW01(config-if-range)#channel-group 1 mode active
DISTRO-SW01(config-if-range)#shut
*Jan  4 10:06:10.920: %LINEPROTO-5-UPDOWN: Line protocol on Interface Et
hernet0/2, changed state to up
*Jan  4 10:06:10.920: %LINEPROTO-5-UPDOWN: Line protocol on Interface Et
hernet0/3, changed state to up
DISTRO-SW01(config-if-range)#shut
DISTRO-SW01(config-if-range)#no shut
DISTRO-SW01(config-if-range)#

```

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Distro-Switch1
 Int et0/0
 No Channel-group 1 mode passive
 Int range et0/2-3
 No Channel-group 1 mode passive Channel-group 1 mode active Shut
 No shut
 Int port 1
 Switchport trunk native vlan 10 Copy run start
 Distro-Switch2
 Int port 1
 Switchport trunk native vlan 10 Copy run start
 Distro-Switch2
 Spanning-tree vlan 1-1005 root secondary Copy run start

NEW QUESTION 454

- (Topic 4)
How do OSPF and EIGRP compare?

- A. OSPF and EIGRP use the same administrative distance.
- B. Both OSPF and EIGRP use the concept of areas.
- C. EIGRP shows all known routes, and OSPF shows successor and feasible successor routes.
- D. EIGRP shows successor and feasible successor routes, and OSPF shows all known routes.

Answer: D

NEW QUESTION 457

- (Topic 4)
A wireless network engineer must configure a WPA2+WPA3 policy with the Personal security type. Which action meets this requirement?

- A. Configure the GCMP256 encryption cipher.
- B. Configure the CCMP256 encryption cipher.
- C. Configure the CCMP128 encryption cipher.
- D. Configure the GCMP128 encryption cipher.

Answer: A

Explanation:

This is because the GCMP256 cipher is the only one that supports both WPA2 and WPA3 with the Personal security type. The GCMP256 cipher provides stronger encryption and authentication than the CCMP ciphers, which are only compatible with WPA2. The source of this answer is the Cisco ENCOR v1.1 course, module 7, lesson 7.2: Implementing WPA2 and WPA3.

NEW QUESTION 462

DRAG DROP - (Topic 4)

Drag and drop the snippets onto the blanks within the code to create an EEM script that adds an entry to a locally stored text file with a timestamp when a configuration change is made. Not all options are used.

```
event manager applet CONF_CHANGE
[ ] "SYS-5-CONFIG_I"

action 1.0 cli command [ ]

action 2.0 cli command "show clock [ ] :ConfSave.txt"

action 3.0 syslog Priority informational msg "Configuration changed"
```

event cli pattern	"enable"	event syslog pattern
"config t"	append flash	flash

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```
event manager applet CONF_CHANGE
event syslog pattern "SYS-5-CONFIG_I"
action 1.0 cli command "enable"
action 2.0 cli command "show clock | append flash :ConfSave.txt"
action 3.0 syslog Priority informational msg "Configuration changed"
```

event cli pattern "enable" event syslog pattern
 "config t" | append flash flash

NEW QUESTION 467

- (Topic 4)

Refer to the exhibit.

```
router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
router#

12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05: ICMP type=0, code=0
12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05: ICMP type=0, code=0
12:11:05: IP: s=1.1.1.1 (Serial1/0), d=10.1.1.1 (Serial3/0),
g=10.1.1.1, len 100, forward
12:11:05: ICMP type=0, code=0
```

A network engineer issues the debug command while troubleshooting a network issue. What does the output confirm?

- A. ACL100 is tracking ICMP traffic from 1.1.1.1 destined for 10.1.1.1.
- B. ACL100 is tracking all traffic from 10.1.1.1 destined far 1.1.
- C. ACL100 is tracking ICMP traffic from 10.1.1.1 destined for 11.1.1
- D. ACL100 is tracking ICMP traffic from Serial 1/0 destined for Serial3/0.

Answer: A

NEW QUESTION 469

- (Topic 3)

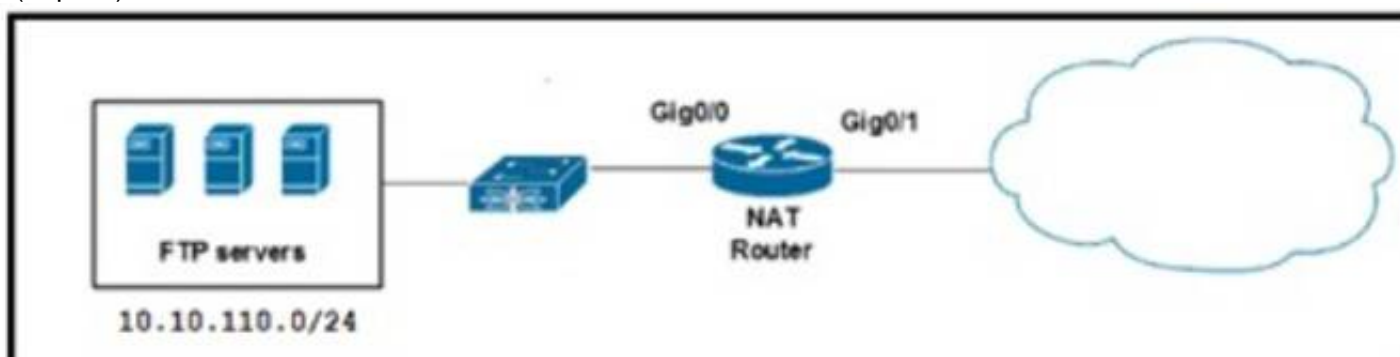
Which two Cisco SD-Access components provide communication between traditional network elements and controller layer? (choose two)

- A. network data platform
- B. network underlay
- C. fabric overlay
- D. network control platform
- E. partner ecosystem

Answer: BC

NEW QUESTION 470

- (Topic 3)



Refer to the exhibit. A network engineer must load balance traffic that comes from the NAT Router and is destined to 10.10.110.10, to several FTP servers. Which two commands sets should be applied? (Choose two).

- A)
- ```
interface gig0/0
ip address 10.10.110.1 255.255.255.0
ip nat inside
Interface gig0/1
ip address 172.16.1.1 255.255.255.252
ip nat outside
```
- B)
- ```
ip nat pool ftp-pool 10.10.110.2 10.10.110.9 netmask 255.255.255.0
access-list 23 permit 10.10.110.10
ip nat inside destination-list 23 pool ftp-pool
```
- C)
- ```
ip nat pool ftp-pool 10.10.110.2 10.10.110.9 netmask 255.255.255.0 type rotary
access-list 23 permit 10.10.110.10
ip nat inside destination-list 23 pool ftp-pool
```
- D)
- ```
ip nat pool ftp-pool 10.10.110.2 10.10.110.9 netmask 255.255.255.0 type rotary
access-list 23 permit 10.10.110.10
ip nat outside destination-list 23 pool ftp-pool
```
- E)
- ```
interface gig0/0
ip address 10.10.110.1 255.255.255.0
ip nat outside
Interface gig0/1
ip address 172.16.1.1 255.255.255.252
ip nat inside
```

- A. Option A  
B. Option B  
C. Option C  
D. Option D  
E. Option E

**Answer:** AC

#### NEW QUESTION 471

- (Topic 3)

```
<interface>
 <Loopback>
 <name>100</name>
 <enabled>true</enabled>
 </Loopback>
</interface>
```

Refer to the exhibit. What is achieved by this code?

- A. It unshuts the loopback interface  
B. It renames the loopback interface  
C. It deletes the loopback interface  
D. It displays the loopback interface

**Answer:** D

#### NEW QUESTION 474

- (Topic 3)

An engineer must configure a new loopback Interface on a router and advertise the interface as a fa4 in OSPF. Which command set accomplishes this task?

- A)
- ```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf 100 area 0
```
- B)


```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf network point-to-point
R2(config-if)# ip ospf 100 area 0
```

C)

```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf network point-to-multipoint
R2(config-if)# router ospf 100
R2(config-router)# network 172.22.2.0 0.0.0.255 area 0
```

D)

```
R2(config)# Interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf network broadcast
R2(config-if)# ip ospf 100 area 0
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

? Step 1. Create the loopback interface using the interface loopback number global configuration command.

? Step 2. Add a description. Although optional, it is a necessary component for documenting a network.

? Step 3. Configure the IP address.

For example, the following commands configure a loopback interface of the R1 router shown in (shown earlier in the chapter):

R1# configure terminal

R1(config)# interface loopback 0

R1(config-if)# ip address 10.0.0.1 255.255.255.0

R1(config-if)# exit

R1(config)#

NEW QUESTION 479

- (Topic 3)

Which two features does the Cisco SD-Access architecture add to a traditional campus network? (Choose two.)

- A. software-defined segmentation
- B. private VLANs
- C. SD-WAN
- D. modular QoS
- E. identity services

Answer: AE

Explanation:

<https://www.aspiretransforms.com/2018/06/06/insider-guide-cisco-sd-access/>

NEW QUESTION 483

- (Topic 3)

Which two solutions are used for backing up a Cisco DNA Center Assurance database? (Choose two)

- A. NFS share
- B. non-linux server
- C. local server
- D. remote server
- E. bare metal server

Answer: AE

Explanation:

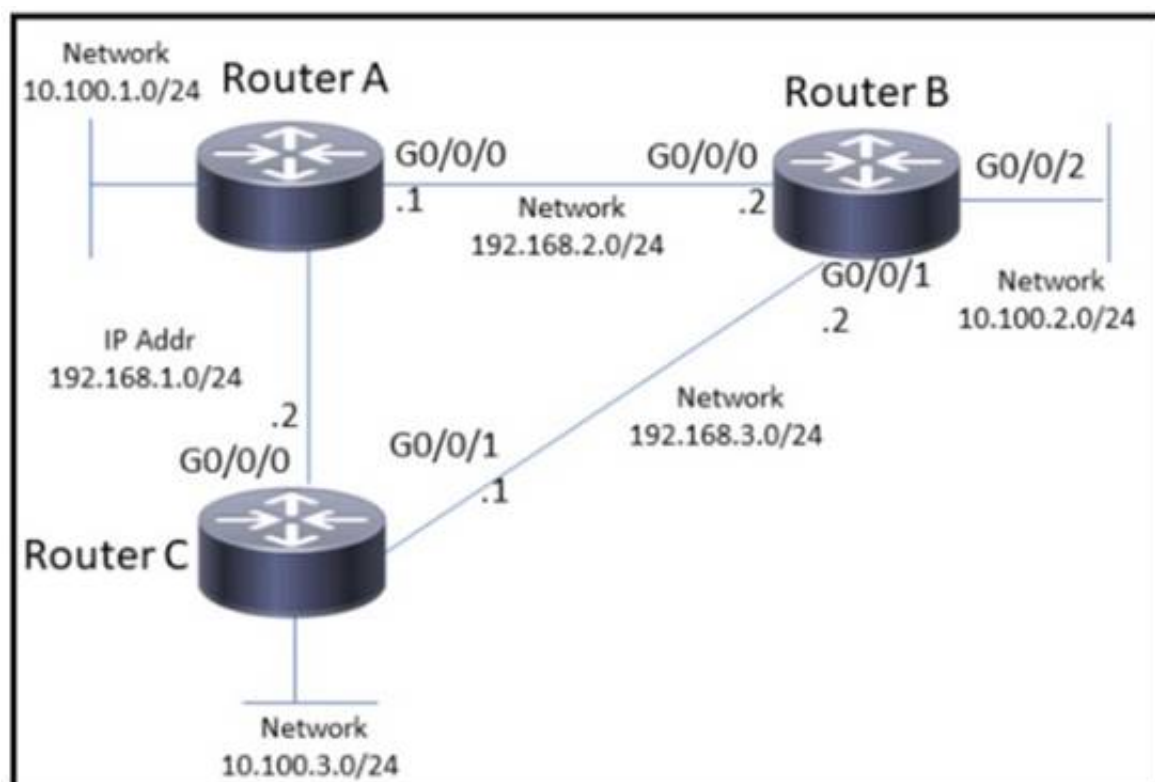
Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name. To support Assurance data backups, the server must be a Linux-based NFS server that meets the following requirements:– Support NFS v4 and NFS v3.– Cisco DNA Center stores backup copies of Assurance data on an external NFS device and automation data on an external remote sync (rsync) target location.– The remote share for backing up an Assurance database (NDP) must be an NFS share.

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/admin_guide/b_cisco_dna_center_admin_guide_2_1_2/b_cisco_dna_center_admin_guide_2_1_1_chapter_0110.html

NEW QUESTION 487

- (Topic 3)

Refer to the exhibit. A network engineer must block Telnet traffic from hosts in the range of 10.100.2.248 to 10.100.2.255 to the network 10.100.3.0 and permit everything else. Which configuration must the engineer apply?



- A)
- ```
RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 22
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```
- B)
- ```
RouterB(config)# access-list 101 deny icmp 10.100.2.0 0.0.0.248 10.100.2.0 0.0.0.248
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```
- C)
- ```
RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 23
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```
- D)
- ```
RouterB(config)# access-list 101 permit tcp 10.100.2.0 0.0.0.252 10.100.3.0 0.0.0.255
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

- A. Option A
 B. Option B
 C. Option C
 D. Option D

Answer: C

NEW QUESTION 490

- (Topic 3)

What is a characteristics of traffic policing?

- A. lacks support for marking or remarking
 B. must be applied only to outgoing traffic
 C. can be applied in both traffic directions
 D. queues out-of-profile packets until the buffer is full

Answer: D

NEW QUESTION 493

- (Topic 3)

Which resource is able to be shared among virtual machines deployed on the same physical server?

- A. applications
 B. disk
 C. VM configuration file
 D. operating system

Answer: B

NEW QUESTION 497

- (Topic 3)

```
R1#show ip interface brief | include 192.168.12
FastEthernet0/0  192.168.12.1  YES manual up      up

R1#ping vrf CUST-A 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1#show ip arp 192.168.12.2
R1#
```

Refer to the exhibit. A network engineer checks connectivity between two routers. The engineer can ping the remote endpoint but cannot see an ARP entry. Why is there no ARP entry?

- A. The ping command must be executed in the global routing table.
- B. Interface FastEthernet0/0 is configured in VRF CUST-A, so the ARP entry is also in that VRF.
- C. When VRFs are used
- D. ARP protocol must be enabled in each VRF.
- E. When VRFs are used
- F. ARP protocol is disabled in the global routing table.

Answer: B

NEW QUESTION 499

- (Topic 3)

Refer to the exhibit.

```
Router# show running-config
! lines omitted for brevity

username cisco password 0 cisco

aaa authentication login group1 group radius line
aaa authentication login group2 group radius local
aaa authentication login group3 group radius none

line con 0
password 0 cisco123
login authentication group1
line aux 0
login authentication group3
line vty 0 4
password 0 test123
login authentication group2
```

A network engineer must log in to the router via the console, but the RADIUS servers are not reachable. Which credentials allow console access?

- A. the username "cisco" and the password "Cisco"
- B. no username and only the password "test123"
- C. no username and only the password "cisco123"
- D. the username "cisco" and the password "cisco123"

Answer: D

NEW QUESTION 503

- (Topic 3)


```
switch1(config)# interface GigabitEthernet 1/1
switch1(config-if)# switchport mode trunk
switch1(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-90
switch1(config)# exit
switch1(config)# monitor session 1 source vlan 10
switch1(config)# monitor session 1 destination remote vlan 70

switch2(config)# interface GigabitEthernet 1/1
switch2(config-if)# switchport mode trunk
switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,80-90
switch2(config)# exit
switch2(config)# monitor session 2 source remote vlan 70
switch2(config)# monitor session 2 destination interface GigabitEthernet1/1
```

Refer to the exhibit. A network administrator configured RSPAN to troubleshoot an issue between switch1 and switch2. The switches are connected using interface GigabitEthernet 1/1. An external packet capture device is connected is switch2 interface GigabitEthernet 1/2. Which two commands must be added to complete this configuration? (Choose two)

- ☐ switch2(config)# monitor session 1 source remote vlan 70
switch2(config)# monitor session 1 destination interface GigabitEthernet1/2
- ☐ switch2(config)# monitor session 1 source remote vlan 70
switch2(config)# monitor session 1 destination interface GigabitEthernet1/1
- ☐ switch1(config)# interface GigabitEthernet 1/1
switch1(config-if)# switchport mode access
switch1(config-if)# switchport access vlan 10

switch2(config)# interface GigabitEthernet 1/1
switch2(config-if)# switchport mode access
switch2(config-if)# switchport access vlan 10
- ☐ switch2(config)# monitor session 2 destination vlan 10
- ☐ switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-80

- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

Answer: AE

NEW QUESTION 504

- (Topic 3)

What is one characteristic of the Cisco SD-Access control plane?

- A. It is based on VXLAN technology.
- B. Each router processes every possible destination and route
- C. It allows host mobility only in the wireless network.
- D. It stores remote routes in a centralized database server

Answer: D

Explanation:

A control plane node maintains a host tracking database (HTDB), and also uses Locator/ID Separation Protocol (LISP) to provide a map server, populating the HTDB from fabric edge registration messages; and a map resolver to respond to queries from edge devices requesting location information about destination nodes.

NEW QUESTION 509

- (Topic 3)

Refer to the exhibit.

```
import json
from requests import get

Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

Devices = open("devices.txt", "r")

for Device in Devices.readlines():
    Hostname, IP, Login, Pass = Device.strip().split(",")
    URL = f"https://{IP}/restconf/data/Cisco-IOS-XE-native:native"
    Creds = (Login, Pass)
    response = get(URL, auth = Creds, headers = Headers, verify = False)
```

How should the script be completed so that each device configuration is saved into a JSON-formatted file under the device name?

A)

Insert after the for loop:

```
with open(f'{Hostname}.json', "w") as OutFile:
    OutFile.write(Response)
```

B)

Insert after the for loop:

```
with open(f'{Hostname}.json', "w") as OutFile:
    OutFile.write(json.dumps(Response.text))
```

C)

Append to the body of the for loop:

```
with open(f'{Hostname}.json', "w") as OutFile:
    OutFile.write(Response.text)
```

D)

Insert immediately before the for loop:

```
with open(f'{Hostname}.json', "w") as OutFile:
    OutFile.write(json.load(Devices))
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

NEW QUESTION 511

- (Topic 3)

What is a characteristic of the overlay network in the Cisco SD-Access architecture?

- A. It uses a traditional routed access design to provide performance and high availability to the network.
- B. It consists of a group of physical routers and switches that are used to maintain the network.
- C. It provides isolation among the virtual networks and independence from the physical network.
- D. It provides multicast support to enable Layer 2 Flooding capability in the underlay network.

Answer: C

NEW QUESTION 512

- (Topic 3)

How do EIGRP metrics compare to OSPF metrics?

- A. EIGRP metrics are based on a combination of bandwidth and packet loss, and OSPF metrics are based on interface bandwidth.
- B. EIGRP uses the Dijkstra algorithm, and OSPF uses The DUAL algorithm
- C. The EIGRP administrative distance for external routes is 170. and the OSPF administrative distance for external routes is undefined
- D. The EIGRP administrative distance for external routes is 170. and the OSPF administrative distance for external routes is 110

Answer: A

NEW QUESTION 517

- (Topic 3)

Refer to the exhibit.

```
switch > enable
switch # configure terminal
switch(config)# interface GigabitEthernet 1/10
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vian 10,20,30
switch(config-if)# exit
switch (config)# monitor session 1 type erspan-source
switch(config-mon-erspan-src)# description source1
switch(config-mon-erspan-src)# source vian 10
switch(config-mon-erspan-src)# source vian 20
switch(config-mon-erspan-src)# filter vian 30
switch(config-mon-erspan-src)# destination
switch(config-mon-erspan-src-dst)# erspan-id 100
switch(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
switch(config-mon-erspan-src-dst)# ip prec 5
switch(config-mon-erspan-src-dst)# ip ttl 32
switch(config-mon-erspan-src-dst)# mtu 1500
switch(config-mon-erspan-src-dst)# ip address 10.10.0.1
switch(config-mon-erspan-src-dst)# vrf 1
switch(config-mon-erspan-src-dst)# no shutdown
switch(config-mon-erspan-src-dst)# end
```

An engineer configures the trunk and proceeds to configure an ESPAN session to monitor VLANs 10, 20, and 30. Which command must be added to complete this configuration?

- A. Device(config.mon.erspan.stc)# no filter vian 30
- B. Device(config.mon.erspan.src-dst)# no vrf 1
- C. Device(config.mon.erspan.src-dst)# erspan id 6
- D. Device(config.mon.erspan.Src-dst)# mtu 1460

Answer: A

NEW QUESTION 520

- (Topic 3)

Refer to the exhibit.

```
access-list 1 permit 10.1.1.0 0.0.0.31
ip nat pool CISCO 209.165.201.1 209.165.201.30 netmask 255.255.255.224
ip nat inside source list 1 pool CISCO
```

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

- A. Inside source addresses are translated to the 209.165.201.0/27 subnet.
- B. It establishes a one-to-one NAT translation.
- C. The 10.1.1.0/27 subnet is assigned as the inside global address range.
- D. The 209.165.201.0/27 subnet is assigned as the outside local address range.
- E. The 10.1.1.0/27 subnet is assigned as the inside local addresses.

Answer: AE

NEW QUESTION 522

- (Topic 3)

Which two Cisco SD-WAN components exchange OMP information?

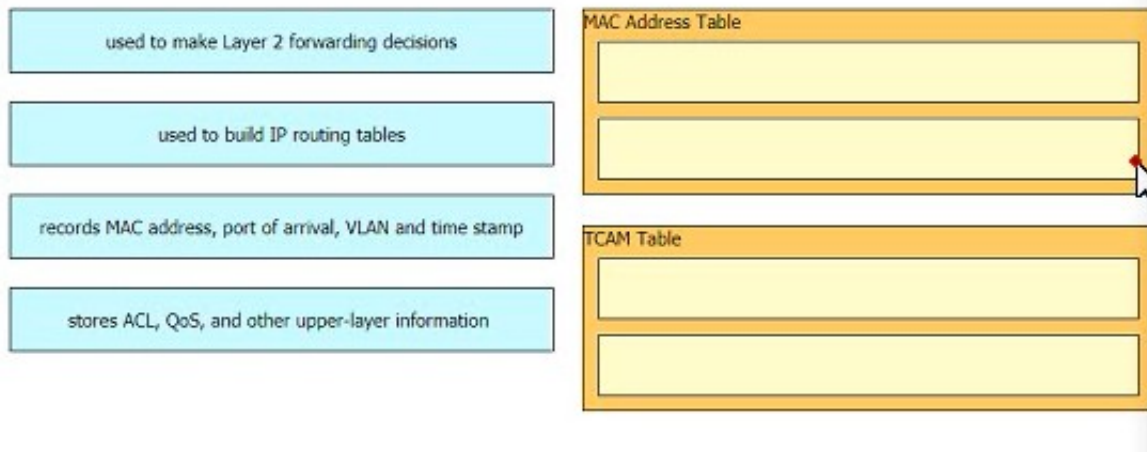
- A. vAnalytics
- B. vSmart
- C. WAN Edge
- D. vBond
- E. vManage

Answer: BC

NEW QUESTION 524

DRAG DROP - (Topic 3)

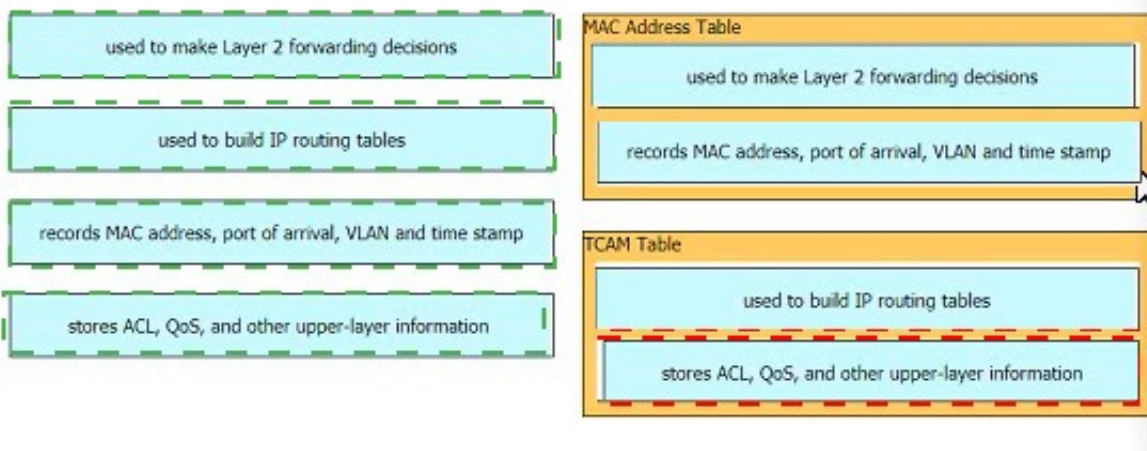
Drag and drop the characteristics from the left to the table types on the right.



- A. Mastered
- B. Not Mastered

Answer: A

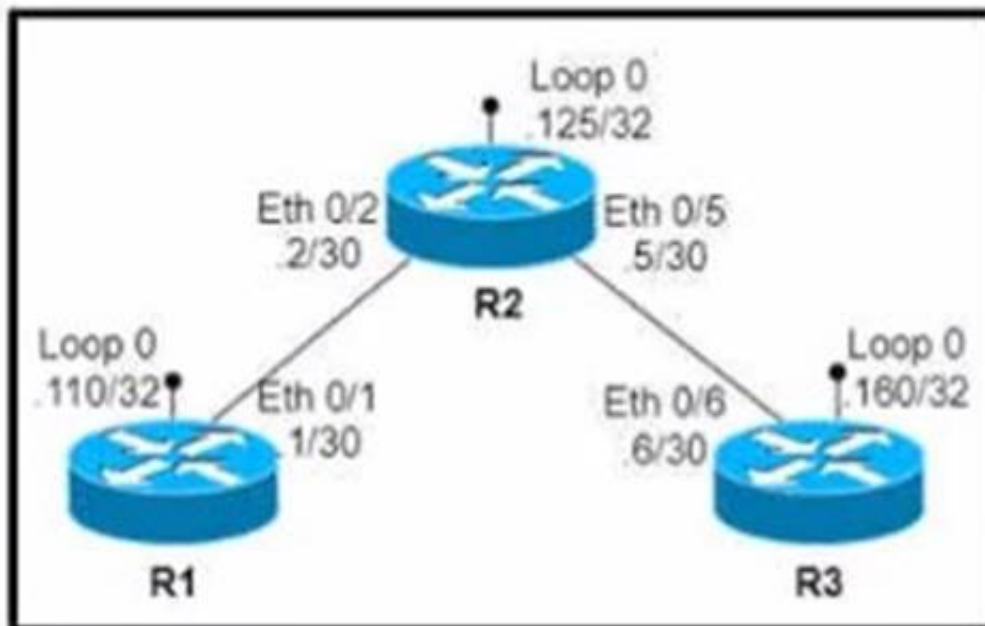
Explanation:



NEW QUESTION 526

- (Topic 3)

Refer to the exhibit.



An engineer configures routing between all routers and must build a configuration to connect R1 to R3 via a GRE tunnel Which configuration must be applied?

A)

```
R1
interface Tunnel1
ip address 1.1.1.13 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.110
```

```
R3
interface Tunnel1
ip address 1.1.1.31 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.160
```

B)

R1
interface Tunnel1
ip address 1.1.1.13 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.110

R3
interface Tunnel1
ip address 1.1.1.31 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.125

C)

R1
interface Tunnel2
ip address 1.1.1.12 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.125

R2
interface Tunnel1
ip address 1.1.1.125 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.110
interface Tunnel3
ip address 1.1.1.125 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.160

R3
interface Tunnel2
ip address 1.1.1.32 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.125

D)

R1
interface Tunnel1
ip address 1.1.1.13 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.160

R3
interface Tunnel1
ip address 1.1.1.31 255.255.255.0
tunnel source Loopback0
tunnel destination x.y.z.110

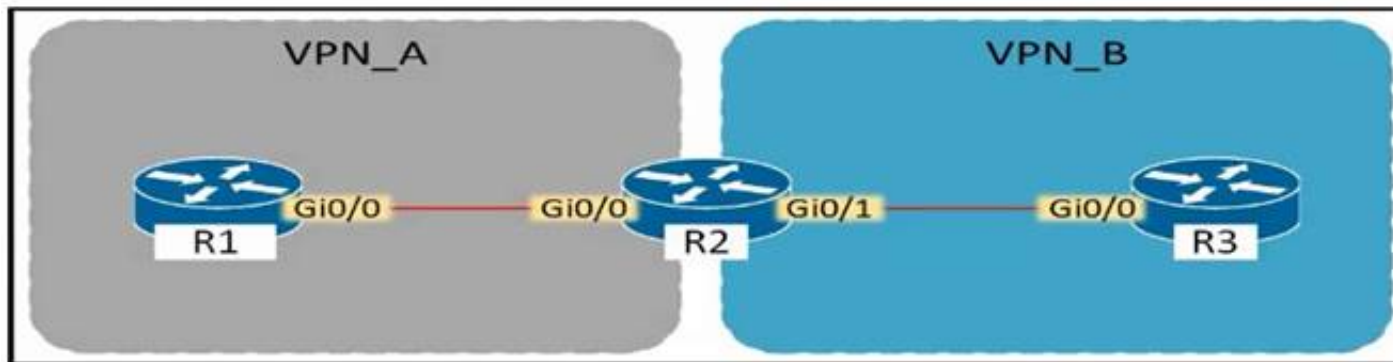
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 527

- (Topic 3)

Refer to The exhibit.



Assuming that R1 is a CE router, which VRF is assigned to Gi0/0 on R1?

- A. VRF VFN_A
- B. VRF VPN_B
- C. management VRF
- D. default VRF

Answer: D

NEW QUESTION 528

- (Topic 2)

Which cisco DNA center application is responsible for group-based access control permissions?

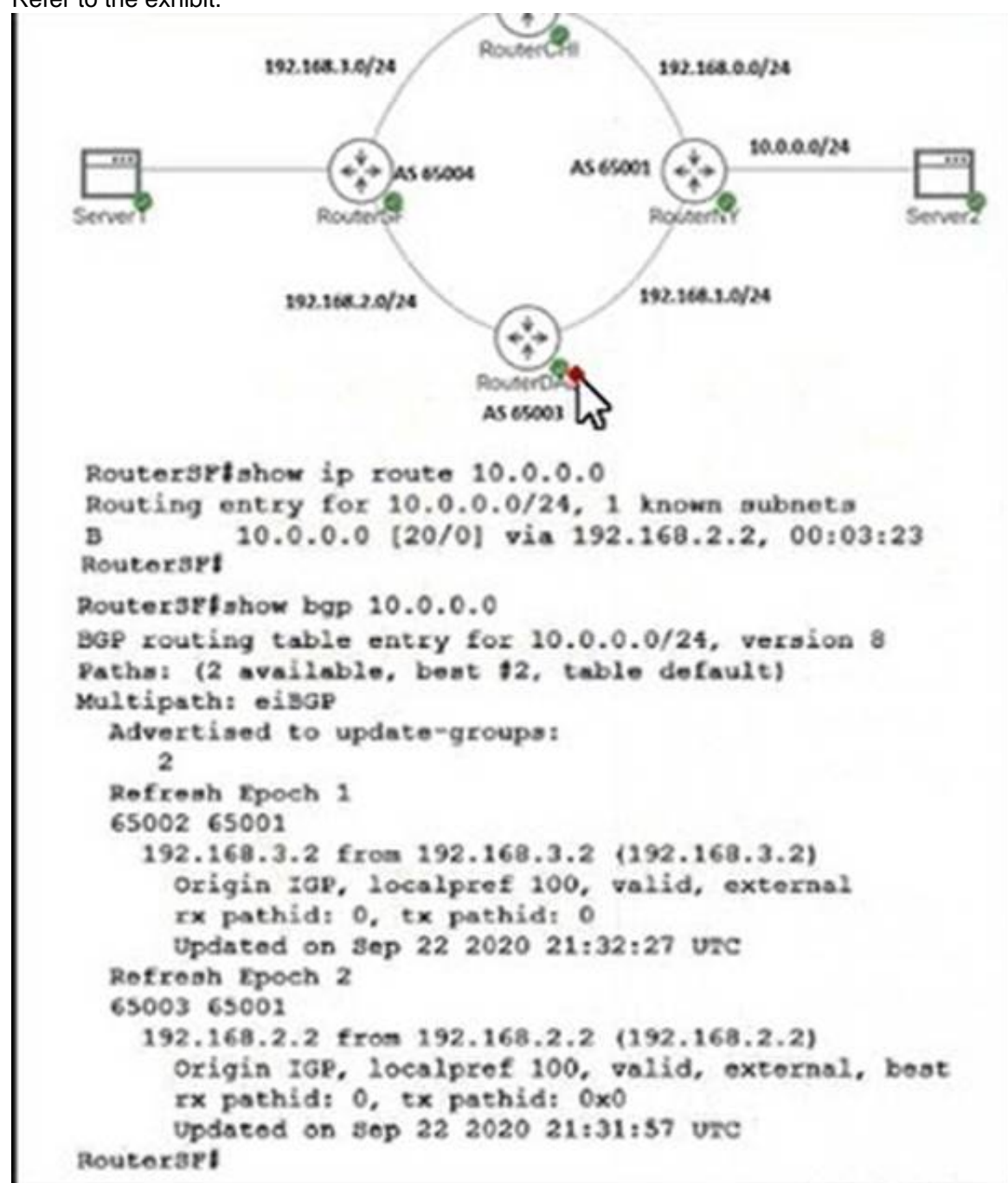
- A. Design
- B. Provision
- C. Assurance
- D. Policy

Answer: D

NEW QUESTION 532

- (Topic 3)

Refer to the exhibit.



After configuring the BGP network, an engineer verifies that the path between Servers and Server2 is functional. Why did RouterSF choose the route from RouterDAL instead of the route from RouterCHI?

- A. The Router-ID for Router DAL is lower than the Router-ID for RouterCHI.
- B. The route from RouterDAL has a lower MED.
- C. BGP is not running on RouterCHI.
- D. There is a static route in RouterSF for 10.0.0.0/24.

Answer: A

NEW QUESTION 534

- (Topic 2)

How does Cisco Trustsec enable more flexible access controls for dynamic networking environments and data centers?

- A. uses flexible NetFlow
- B. assigns a VLAN to the endpoint
- C. classifies traffic based on the contextual identity of the endpoint rather than its IP address
- D. classifies traffic based on advanced application recognition

Answer: C

NEW QUESTION 538

- (Topic 2)

A network engineer is enabling HTTPS access to the core switch, which requires a certificate to be installed on the switch signed by the corporate certificate authority. Which configuration commands are required to issue a certificate signing request from the core switch?

A)
Core-Switch(config)#crypto pki enroll Core-Switch
Core-Switch(config)#ip http secure-trustpoint Core-Switch

B)
Core-Switch(config)#crypto pki trustpoint Core-Switch
Core-Switch(ca-trustpoint)#enrollment terminal
Core-Switch(config)#crypto pki enroll Core-Switch

C)
Core-Switch(config)#crypto pki trustpoint Core-Switch
Core-Switch(ca-trustpoint)#enrollment terminal
Core-Switch(config)#ip http secure-trustpoint Core-Switch

D)
Core-Switch(config)#ip http secure-trustpoint Core-Switch
Core-Switch(config)#crypto pki enroll Core-Switch

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/convert/sec_pki_xe_3s_book/sec_cert_enroll_pki_xe.html

NEW QUESTION 539

- (Topic 2)

In a Cisco SD-Access solution, which protocol is used by an extended node to connect to a single edge node?

- A. VXLAN
- B. IS-IS
- C. 802.1Q
- D. CTS

Answer: C

Explanation:

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

NEW QUESTION 544

- (Topic 2)

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

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

Answer: A

NEW QUESTION 546

- (Topic 2)
Refer to the exhibit.

```
SW2(config)# track 1000 interface gigabitEthernet 0/0 line-protocol
SW2(config-track)# exit
SW2(config)# interface vlan 1000
SW2(config-if)# ip address 10.23.87.3 255.255.255.0
```

An engineer must configure HSRP for VLAN 1000 on SW2. The secondary switch must immediately take over the role of active router If the interlink with the primary switch fails. Which command set completes this task?
A)

```
SW2(config-if)# standby version 2
SW2(config-if)# standby 1000 ip 10.23.87.1
SW2(config-if)# standby 1000 priority 95
SW2(config-if)# standby 1000 preempt
SW2(config-if)# standby 1000 track gigabitethernet0/0
```

B)

```
SW2(config-if)# standby 1000 ip 10.23.87.1
SW2(config-if)# standby 1000 priority 95
SW2(config-if)# standby 1000 preempt
SW2(config-if)# standby 1000 track 1000
```

C)

```
SW2(config-if)# standby version 2
SW2(config-if)# standby 1000 ip 10.23.87.1
SW2(config-if)# standby 1000 priority 95
SW2(config-if)# standby 1000 preempt
SW2(config-if)# standby 1000 track 1000
```

D)

```
SW2(config-if)# standby version 2
SW2(config-if)# standby 1000 ip 10.23.87.1
SW2(config-if)# standby 1000 priority 95
SW2(config-if)# standby 1000 track 1000
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 547

- (Topic 2)
Refer to the exhibit.

| TYPE | PROT | SID | IP | ID | PRIVATE IP | PROXY | STATE | UPTIME | PUKE |
|------------|------|-------------|-----|------|----------------|-------|-------|--------|------|
| PUBLIC IP | | | | PORT | LOCAL COLOR | | | | ID |
| ----- | | | | | | | | | |
| vsmart | dtls | 4.4.4.70 | 100 | 1 | 192.168.100.80 | | | | |
| 12446 | | 10.10.20.70 | | | 12446 default | No | up | | |
| 0:02:24:09 | 0 | | | | | | | | |
| vbond | dtls | 0.0.0.0 | 0 | 0 | 192.168.100.81 | | | | |
| 12346 | | 10.10.20.80 | | | 12346 default | - | up | | |
| 0:02:24:10 | 0 | | | | | | | | |
| vmanage | dtls | 4.4.4.90 | 100 | 0 | 192.168.100.82 | | | | |
| 12446 | | 10.10.20.90 | | | 12446 default | | | | |

POST

https://192.168.100.80:8443/_security_check

Send

Save

Params

Authorization

Headers (1)

Body

Pre-request Script

Tests

Cookies

Code

Comments (0)

none

form-data

x-www-form-urlencoded

raw

binary

| KEY | VALUE | DESCRIPTION | ... | Bulk Edit |
|---|-------|-------------|-----|-----------|
| <input checked="" type="checkbox"/> _Username | admin | | | |
| <input checked="" type="checkbox"/> _password | admin | | | |
| Key | Value | Description | | |

Could not get any response

There was an error connecting to https://192.168.100.80:8443/_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. use basic authentication
- B. change the port to 12446
- C. target 192 168 100 82 in the URI
- D. restart the vsmart host

Answer: B

Explanation:

he first figure is the output of the “show control connections” command. From this figure we learned that the 192.168.100.82 so we need to connect to this IP address (not 192.168.100.80).

NEW QUESTION 550

- (Topic 2)

What are two common sources of interference for Wi-Fi networks? (Choose two.)

- A. rogue AP
- B. conventional oven
- C. fire alarm
- D. LED lights
- E. radar

Answer: AE

NEW QUESTION 555

- (Topic 2)

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 AMP deployment with the Malicious Activity Protection engine enabled.
- B. Use Cisco AMP deployment with the Exploit Prevention engine enabled.
- C. Use Cisco Firepower and block traffic to TOR networks.
- D. Use Cisco Firepower with Intrusion Policy and snort rules blocking SMB exploitation.

Answer: B

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/ampfor-endpoints/white-paper-c11-740980.pdf>

NEW QUESTION 560

.....

Relate Links

100% Pass Your 350-401 Exam with ExamBible Prep Materials

<https://www.exambible.com/350-401-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>