

# Cisco

## Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies



**NEW QUESTION 1**

- (Topic 4)

Which access control feature does MAB provide?

- A. user access based on IP address
- B. allows devices to bypass authenticate\*
- C. network access based on the physical address of a device
- D. simultaneous user and device authentication

**Answer:** C

**NEW QUESTION 2**

- (Topic 4)

Which two security features are available when implementing NTP? (Choose two.)

- A. symmetric server passwords
- B. dock offset authentication
- C. broadcast association mode
- D. encrypted authentication mechanism
- E. access list-based restriction scheme

**Answer:** DE

**NEW QUESTION 3**

- (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)
```

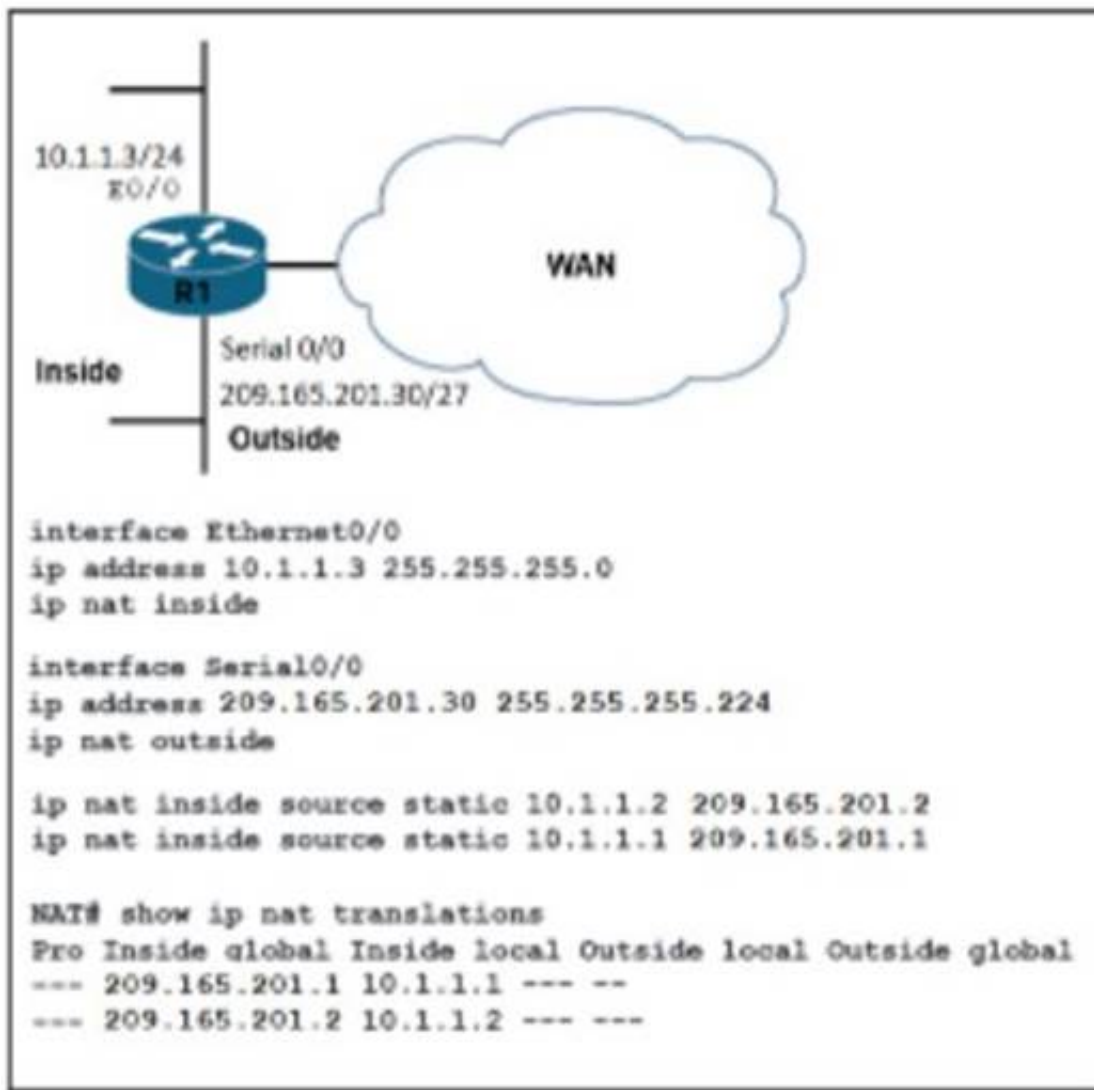
Refer to the exhibit. The EtherChannel between SW1 and SW2 is not operational. Which action will resolve the issue?

- 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 GI'0 and GM of SW1 .
- D. Configure switchport mode dynamic desirable on SW1 and SW2

**Answer:** C

**NEW QUESTION 4**

- (Topic 4)



Refer to the exhibit. What are two results of the NAT configuration? (Choose two.)

- A. Packets with a destination of 200.1.1.1 are translated to 10.1.1.1 or .2. respectively.
- B. A packet that is sent to 200.1.1.1 from 10.1.1.1 is translated to 209.165.201.1 on R1.
- C. R1 looks at the destination IP address of packets entering S0/0 and destined for inside hosts.
- D. R1 processes packets entering E0/0 and S0/0 by examining the source IP address.
- E. R1 is performing NAT for inside addresses and outside address.

**Answer: BC**

#### NEW QUESTION 5

- (Topic 4)

What are two benefits of implementing a traditional WAN instead of an SD-WAN solution? (Choose two.)

- A. comprehensive configuration standardization
- B. lower control plane abstraction
- C. simplify troubleshooting
- D. faster fault detection
- E. lower data plane overhead

**Answer: BD**

#### NEW QUESTION 6

- (Topic 4)

Which Cisco DNA Center application is responsible for group-based access control permissions?

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

**Answer: C**

#### NEW QUESTION 7

- (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 8

- (Topic 4)

A network administrator wants to install new VoIP switches in a small network closet but is concerned about the current heat level of the room. Which of the

following should the administrator take into consideration before installing the new equipment?

- A. The power load of the switches
- B. The humidity in the room
- C. The fire suppression system
- D. The direction of airflow within the switches

**Answer: D**

**Explanation:**

This is because the direction of airflow within the switches can affect the heat level of the room, as the switches can either exhaust or intake hot air from the environment. The network administrator should take into consideration the direction of airflow within the switches before installing the new equipment, and ensure that the switches are aligned in the same direction and have enough space for ventilation. The network administrator should also avoid mixing switches with different airflow directions, as this can create a hot spot and reduce the cooling efficiency. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.1: Implementing Device Hardening.

**NEW QUESTION 9**

- (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?

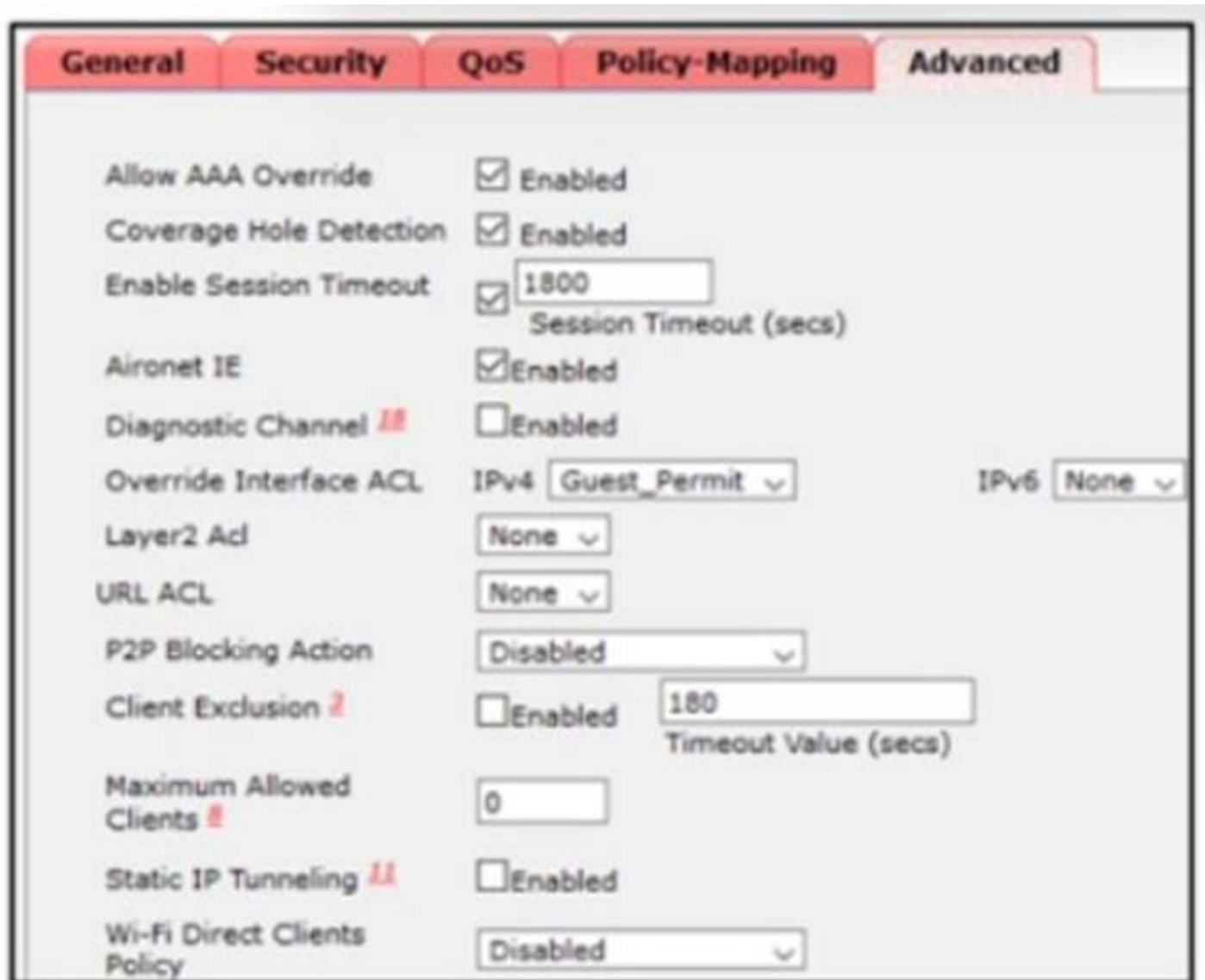
- A. Router(config)# aaa authentication login default local Router(config)# aaa authorization exec default local
- B. Router(config)# aaa authentication login default group tacacs+ local Router(config)# aaa authorization exec default group tacacs+ local
- C. Router(config)# aaa fallback local
- D. Router(config)#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

**Answer: B**

**NEW QUESTION 10**

- (Topic 4)

Refer to the exhibit.



The image shows the Cisco WLAN configuration interface with the Security tab selected. The settings are as follows:

Setting	Value
Allow AAA Override	<input checked="" type="checkbox"/> Enabled
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled
Enable Session Timeout	<input checked="" type="checkbox"/> 1800 Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/> Enabled
Diagnostic Channel	<input type="checkbox"/> Enabled
Override Interface ACL	IPv4: Guest_Permit, IPv6: None
Layer2 Acl	None
URL ACL	None
P2P Blocking Action	Disabled
Client Exclusion	<input type="checkbox"/> Enabled, 180 Timeout Value (secs)
Maximum Allowed Clients	0
Static IP Tunneling	<input type="checkbox"/> Enabled
Wi-Fi Direct Clients Policy	Disabled

An engineer configures a new WLAN that will be used for secure communications; however, wireless clients report that they are able to communicate with each other. Which action resolves this issue?

- A. Enable Client Exclusions.
- B. Disable Aironet IE

- C. Enable Wi-Fi Direct Client Policy
- D. Enable P2P Blocking.

**Answer:** D

#### NEW QUESTION 10

- (Topic 4)

Which tunnel type allows clients to perform a seamless Layer 3 roam between a Cisco AireOS WLC and a Cisco IOS XE WLC?

- A. Ethernet over IP
- B. IPsec
- C. Mobility
- D. VPN

**Answer:** A

#### NEW QUESTION 13

- (Topic 4)

A network engineer must configure a switch to allow remote access for all feasible protocols. Only a password must be requested for device authentication and all idle sessions must be terminated in 30 minutes. Which configuration must be applied?

- ☒ **line vty 0 15  
password cisco  
transport input all  
exec-timeout 0 30**
- ☐ **line console 0  
password cisco  
exec-timeout 30 0**
- ☐ **line vty 0 15  
password cisco  
transport input telnet ssh  
exec-timeout 30 0**
- ☐ **username cisco privilege 15 cisco  
line vty 0 15  
transport input telnet ssh  
login local  
exec-timeout 0 30**

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

**Answer:** C

#### NEW QUESTION 14

- (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 17

- (Topic 4)

Which mechanism can be used to enforce network access authentication against an AAA server if the endpoint does not support the 802.1X supplicant functionality?

- A. private VLANs
- B. port security
- C. MAC Authentication Bypass



D. MACsec

**Answer: C**

**NEW QUESTION 22**

- (Topic 4)



```
no aaa new-model
username admin privilege 15 secret cisco123
ip http secure-port 445
```

Refer to the exhibit Which command must be applied to complete the configuration and enable RESTCONF?

- A. ip http secure-server
- B. ip http server
- C. ip http secure-port 443
- D. ip http client username restconf

**Answer: A**

**NEW QUESTION 24**

- (Topic 4)

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

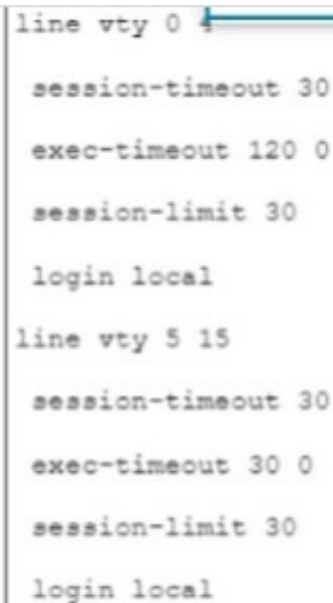
- A. Policy or ACLS are nor required.
- B. There is no requirements to run IEEE 802.1X when TrustSec is enabled on a switch port.
- C. Applications flows between hosts on the LAN to remote destinations can be encrypted.
- D. Policy can be applied on a hop-by-hop basis.

**Answer: C**

**NEW QUESTION 27**

- (Topic 4)

Refer to the exhibit.



```
line vty 0 4
 session-timeout 30
 exec-timeout 120 0
 session-limit 30
 login local
line vty 5 15
 session-timeout 30
 exec-timeout 30 0
 session-limit 30
 login local
```

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

- ☐ access-list 23 permit 10.10.10.0 0.0.0.255  
line vty 0 4  
access-class 23 in  
transport input ssh
- ☐ access-list 23 permit 10.10.10.0 0.0.0.255  
line vty 0 15  
access-class 23 in  
transport input ssh
- ☐ access-list 23 permit 10.10.10.0 0.0.0.255  
line vty 0 15  
access-class 23 out  
transport input all
- ☐ access-list 23 permit 10.10.10.0 255.255.255.0  
line vty 0 15  
access-class 23 in  
transport input ssh

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

Answer: B

#### NEW QUESTION 32

- (Topic 4)

What is a characteristic of para-virtualization?

- A. Para-virtualization allows direct access between the guest OS and the hypervisor.
- B. Para-virtualization allows the host hardware to be directly accessed.
- C. Para-virtualization guest servers are unaware of one another.
- D. Para-virtualization lacks support for containers.

Answer: A

#### NEW QUESTION 33

- (Topic 4)

What is the role of the vSmart controller in a Cisco SD-WN environment?

- A. it performs authentication and authorization
- B. it manages the control plane.
- C. it is the centralized network management system
- D. it manages the data plane

Answer: B

#### NEW QUESTION 37

- (Topic 4)

An engineer is connected to a Cisco router through a Telnet session. Which command must be issued to view the logging messages from the current session as soon as they are generated by the router?

- A. logging buffer
- B. service timestamps log uptime
- C. logging host
- D. terminal monitor

Answer: D

#### NEW QUESTION 40

- (Topic 4)

How does Protocol Independent Multicast function?

- A. In sparse mode, it establishes neighbor adjacencies and sends hello messages at 5- second intervals.
- B. It uses the multicast routing table to perform the multicast forwarding function.
- C. It uses unicast routing information to perform the multicast forwarding function.
- D. It uses broadcast routing information to perform the multicast forwarding function.

**Answer: C**

#### NEW QUESTION 45

- (Topic 4)

<pre> R1#show ip ospf interface Gi0/0 GigabitEthernet0/0 is up, line protocol is up Internet Address 172.20.0.1/24, Area 0, Attached via Network Statement Process ID 1, RouterID 172.20.0.1, Network Type BROADCAST, Cost: 1 Topology-MTID      Cost      Disabled      Shutdown Topology Name 0                  1          no            no Base Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 172.20.0.1, Interface address 172.20.0.1 No backup designated router on this network Timer intervals configured,Hello 10,Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 No Hellos (Passive interface) Supports Link-local Signaling (LLS) Cisco NSF helper support enabled </pre>	<pre> R2#show ip ospf interface Gi0/0 GigabitEthernet0/0 is up, line protocol is up Internet Address 172.20.0.2/24, Area 0, Attached via Network Statement Process ID 1, RouterID 172.20.0.2, Network Type BROADCAST, Cost: 5 Topology-MTID      Cost      Disabled      Shutdown Topology Name 0                  5          no            no Base Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 172.20.0.2, Interface address 172.20.0.2 No backup designated router on this network Timer intervals configured,Hello 10,Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:01 Supports Link-local Signaling (LLS) Cisco NSF helper support enabled IETF NSF helper support enabled </pre>
--	--

Refer to the exhibit. Cisco IOS routers R1 and R2 are interconnected using interface Gi0/0. Which configuration allows R1 and R2 to form an OSPF neighborship on interface Gi0/0?

- ☐ R2(config)#router ospf 1  
R2(config-router)#passive-interface Gi0/0
- ☐ R2(config)#interface Gi0/0  
R2(config-if)#ip ospf cost 1
- ☐ R1(config)#router ospf 1  
R1(config-router)#no passive-interface Gi0/0
- ☐ R1(config)#router ospf 1  
R1(config-if)#network 172.20.0.0 0.0.0.255 area 1

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

**Answer: C**

#### NEW QUESTION 49

- (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.

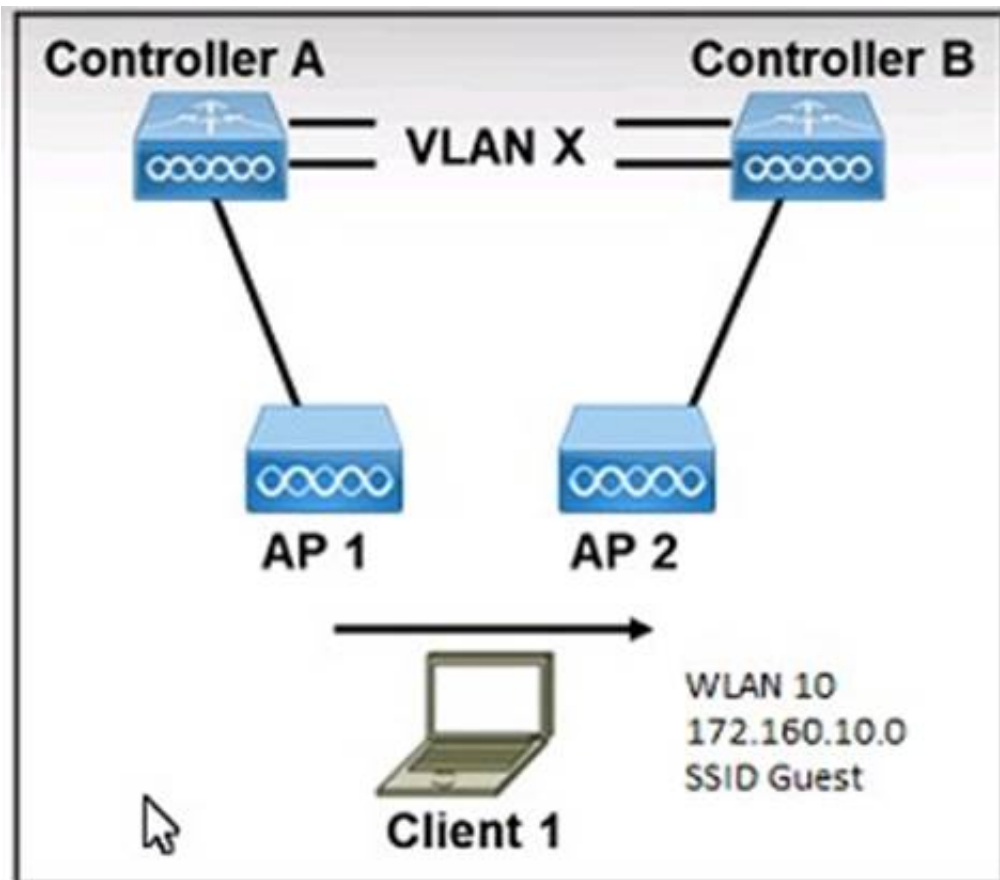
**Answer: B**

#### NEW QUESTION 51

- (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 55

- (Topic 4)

```
username cisco privilege 15 noescape secret 5 F7u$9cyE438490035m8TQ$nv&6502x
username cisco autocommand show startup-config
aaa authentication login default local-case enable
aaa authorization exec default local
```

An engineer applies this configuration to router R1. How does R1 respond when the user 'cisco' logs in?

- A. It displays the startup config and then permits the user to execute commands
- B. It places the user into EXEC mode and permits the user to execute any command
- C. It displays the startup config and then terminates the session.
- D. It places the user into EXEC mode but permits the user to execute only the show startup-config command

**Answer:** A

#### NEW QUESTION 59

- (Topic 1)

Which method should an engineer use to deal with a long-standing contention issue between any two VMs on the same host?

- A. Adjust the resource reservation limits
- B. Live migrate the VM to another host
- C. Reset the VM
- D. Reset the host

**Answer:** A

#### NEW QUESTION 60

- (Topic 1)

What is the function of a VTEP in VXLAN?

- A. provide the routing underlay and overlay for VXLAN headers
- B. dynamically discover the location of end hosts in a VXLAN fabric
- C. encapsulate and de-encapsulate traffic into and out of the VXLAN fabric
- D. statically point to end host locations of the VXLAN fabric

**Answer:** C

#### NEW QUESTION 63

- (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](https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/12s_mdnf.html)

**NEW QUESTION 66**

- (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

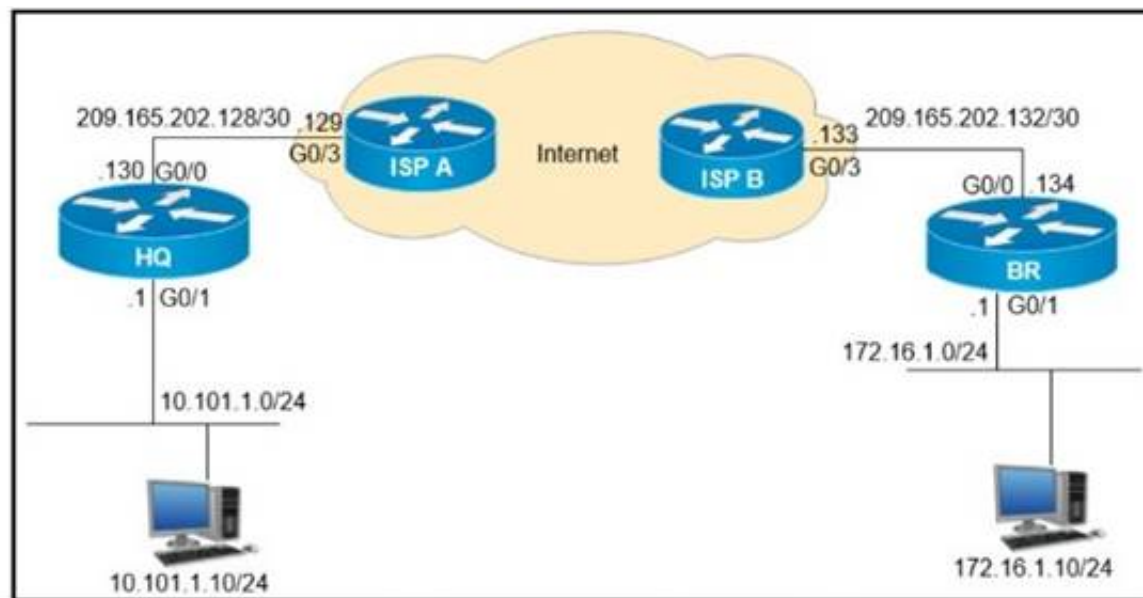
R1#sh run | include username

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 67**

- (Topic 2)

Refer to the exhibit.



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

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

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

**Answer:** A

#### NEW QUESTION 70

- (Topic 2)

Which NGFW mode block flows crossing the firewall?

- A. Passive
- B. Tap
- C. Inline tap
- D. Inline

**Answer:** D

#### Explanation:

Firepower Threat Defense (FTD) provides six interface modes which are: Routed, Switched, Inline Pair, Inline Pair with Tap, Passive, Passive (ERSPAN). When Inline Pair Mode is in use, packets can be blocked since they are processed inline. When you use Inline Pair mode, the packet goes mainly through the FTD Snort engine. When Tap Mode is enabled, a copy of the packet is inspected and dropped internally while the actual traffic goes through FTD unmodified.

#### NEW QUESTION 75

- (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 issues ideally before the users complain or notice connectivity degradation. To address these issues we have created Cisco's Wireless Service Assurance and a new AP mode called "sensor" mode. Cisco's Wireless Service Assurance platform has three components, namely, Wireless Performance Analytics, Real-time Client Troubleshooting, and Proactive Health Assessment. Using a supported AP or dedicated sensor the device can actually function much like a WLAN client would associating and identifying client connectivity issues within the network in real time without requiring an IT or technician to be on site.

Reference:

[https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-5/b\\_Cisco\\_Aironet\\_Sensor\\_Deployment\\_Guide.html.xml](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 79

- (Topic 2)

How cloud deployments differ from on-prem deployments?

- A. Cloud deployments require longer implementation times than on-premises deployments
- B. Cloud deployments are more customizable than on-premises deployments.
- C. Cloud deployments require less frequent upgrades than on-premises deployments.
- D. Cloud deployments have lower upfront costs than on-premises deployments.



Answer: C

### NEW QUESTION 83

- (Topic 2)

```
interface Vlan10
ip vrf forwarding Clients
ip address 192.168.1.1 255.255.255.0
!
interface Vlan20
ip vrf forwarding Servers
ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
ip vrf forwarding Printers
ip address 10.1.1.1 255.255.255.0
-- output omitted for brevity --
router eigrp 1
10.0.0.0
172.16.0.0
192.168.1.0
```

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

A)

```
router eigrp 1
network 10.0.0.0 255.255.255.0
network 172.16.0.0 255.255.255.0
network 192.168.1.0 255.255.255.0
```

B)

```
interface Vlan10
no ip vrf forwarding Clients
!
interface Vlan20
no ip vrf forwarding Servers
!
interface Vlan30
no ip vrf forwarding Printers
```

C)

```
interface Vlan10
no ip vrf forwarding Clients
ip address 192.168.1.2 255.255.255.0
!
interface Vlan20
no ip vrf forwarding Servers
ip address 172.16.1.2 255.255.255.0
!
interface Vlan30
no ip vrf forwarding Printers
ip address 10.1.1.2 255.255.255.0
```

D)

```
router eigrp 1
network 10.0.0.0 255.0.0.0
network 172.16.0.0 255.255.0.0
network 192.168.1.0 255.255.0.0
```

A. Option A



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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 86**

- (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 90**

- (Topic 2)

Refer to the exhibit.



```
enable secret cisco

username cisco privilege 15 secret cisco

aaa new-model
aaa authentication login default group radius local
aaa authorization network default group radius
```

The network administrator must be able to perform configuration changes when all the RADIUS servers are unreachable. Which configuration allows all commands to be authorized if the user has successfully authenticated?

- A. aaa authorization exec default group radius none
- B. aaa authentication login default group radius local none
- C. aaa authorization exec default group radius if-authenticated
- D. aaa authorization exec default group radius

**Answer:** C

**NEW QUESTION 91**

- (Topic 2)

What is the difference between a RIB and a FIB?

- A. The RIB is used to make IP source prefix-based switching decisions
- B. The FIB is where all IP routing information is stored
- C. The RIB maintains a mirror image of the FIB
- D. The FIB is populated based on RIB content

**Answer:** D

**Explanation:**

CEF uses a Forwarding Information Base (FIB) to make IP destination prefix- based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with earlier switching paths such as fast switching and optimum switching.

Note: In order to view the Routing information base (RIB) table, use the “show ip route” command. To view the Forwarding Information Base (FIB), use the “show ip cef” command. RIB is in Control plane while FIB is in Data plane.

**NEW QUESTION 96**

- (Topic 2)

Refer to the exhibit.

```
R1#show run | b router ospf
router ospf 1
network 192.168.10.0 0.0.0.255 area 0

R1#show run | b interface loopback0
interface loopback0
ip address 192.168.10.50 255.255.255.0
```

R2 is the neighboring router of R1. R2 receives an advertisement for network 192.168.10.50/32. Which configuration should be applied for the subnet to be advertised with the original /24 netmask?

A)  
**R1(config)#router ospf 1**  
**R1(config-router)#network 192.168.10.0 255.255.255.0 area 0**

B)  
**R1(config)#interface loopback0**  
**R1(config-if)#ip ospf 1 area 0**

C)  
**R1(config)# interface loopback0**  
**R1(config-if)# ip ospf network point-to-point**

D)  
**R1(config)# interface loopback0**  
**R1(config-if)# ip ospf network non-broadcast**

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

**Answer: C**

#### NEW QUESTION 97

- (Topic 2)

Which outcome is achieved with this Python code?

```
client.connect ( ip, port= 22, username= usr, password= pswd )
stdin, stdout, stderr = client.exec_command ( 'show ip bgp 192.168.101.0 bestpath\n ' )
print (stdout)
```

- A. connects to a Cisco device using SSH and exports the routing table information
- B. displays the output of the show command in a formatted way
- C. connects to a Cisco device using SSH and exports the BGP table for the prefix
- D. connects to a Cisco device using Telnet and exports the routing table information

**Answer: C**

#### NEW QUESTION 101

- (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 103

- (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 105

- (Topic 2)

Which method is used by an AP to join HA controllers and is configured in NVRAM?

- A. stored WLC information
- B. DNS
- C. IP Helper Addresses
- D. Primary/Secondary/Tertiary/Backup

**Answer: A**

#### Explanation:

An AP can be “primed” with up to three controllers—a primary, a secondary, and a tertiary. These are stored in nonvolatile memory so that the AP can remember them after a reboot or power failure.

#### NEW QUESTION 106

- (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 110**

- (Topic 2)

Refer to the exhibit.

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

Current configuration : 95 bytes
!
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel destination 192.168.10.2
end

Router1#show ip int br
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0 192.168.1.1     YES manual up          up
GigabitEthernet0/1 unassigned      YES unset   administratively down down
GigabitEthernet0/2 unassigned      YES unset   administratively down down
GigabitEthernet0/3 unassigned      YES unset   administratively down down
Loopback0          192.168.10.1    YES manual up          up
Tunnel0            172.16.1.1      YES manual up          down
Router1#
```

Which command must be applied to Router 1 to bring the GRE tunnel to an up/up state?

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

**Answer:** B

**NEW QUESTION 113**

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

uses areas to segment a network

summaries can be created in specific parts of the IGP topology

OSPF

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 118**

- (Topic 2)

Which feature does Cisco TrustSec use to provide scalable, secure communication throughout a network?

- A. security group tag ACL assigned to each port on a switch
- B. security group tag number assigned to each port on a network



- C. security group tag number assigned to each user on a switch
- D. security group tag ACL assigned to each router on a network

**Answer: B**

**Explanation:**

Cisco TrustSec uses tags to represent logical group privilege. This tag, called a Security Group Tag (SGT), is used in access policies. The SGT is understood and is used to enforce traffic by Cisco switches, routers and firewalls . Cisco TrustSec is defined in three phases: classification, propagation and enforcement. When users and devices connect to a network, the network assigns a specific security group. This process is called classification. Classification can be based on the results of the authentication or by associating the SGT with an IP, VLAN, or port-profile (-> Answer 'security group tag ACL assigned to each port on a switch' and answer 'security group tag number assigned to each user on a switch' are not correct as they say "assigned ... on a switch" only. Answer 'security group tag ACL assigned to each router on a network' is not correct either as it says "assigned to each router").

**NEW QUESTION 123**

- (Topic 2)

Which action is performed by Link Management Protocol in a Cisco StackWise Virtual domain?

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

**Answer: A**

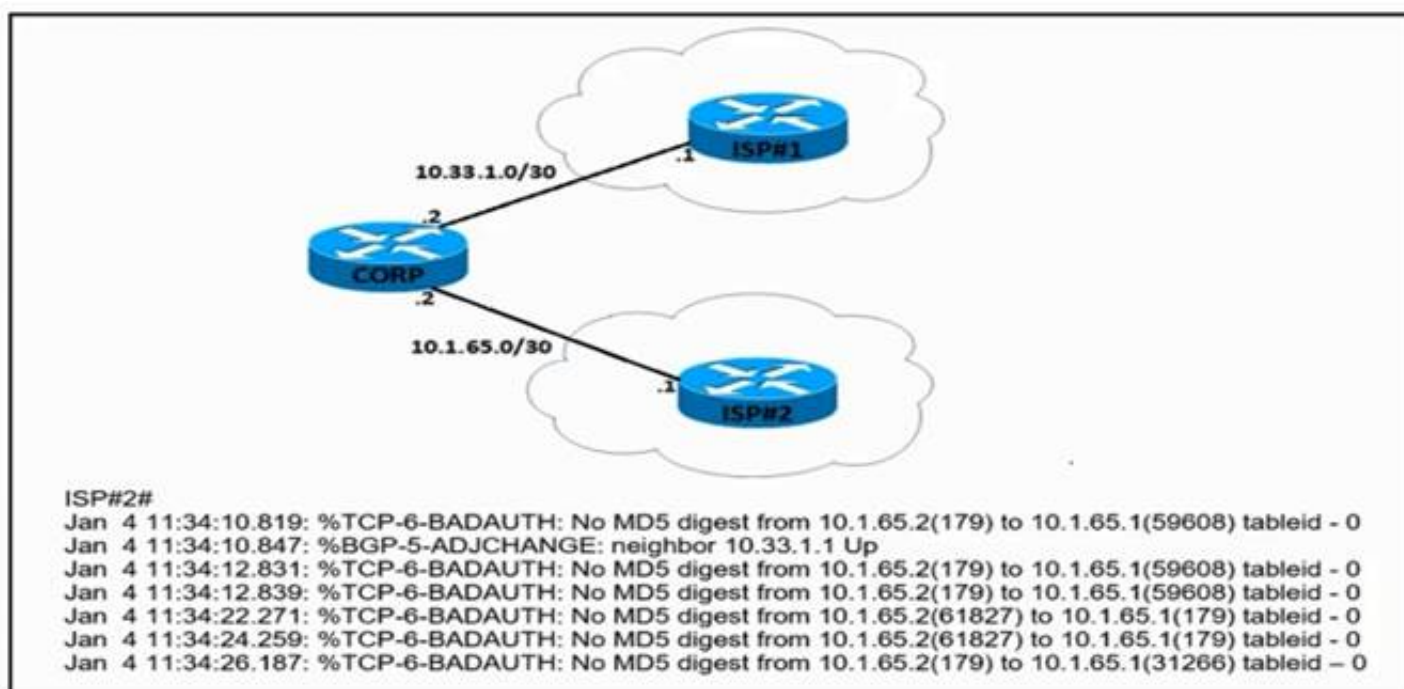
**Explanation:**

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

**NEW QUESTION 126**

- (Topic 2)

Refer to the exhibit.



An engineer attempts to establish BGP peering between router CORP and two ISP routers. What is the root cause for the failure between CORP and ISP#2?

- A. Router ISP#2 is configured to use SHA-1 authentication.
- B. There is a password mismatch between router CORP and router ISP#2.
- C. Router CORP is configured with an extended access control list.
- D. MD5 authorization is configured incorrectly on router ISP#2.

**Answer: B**

**NEW QUESTION 131**

DRAG DROP - (Topic 2)

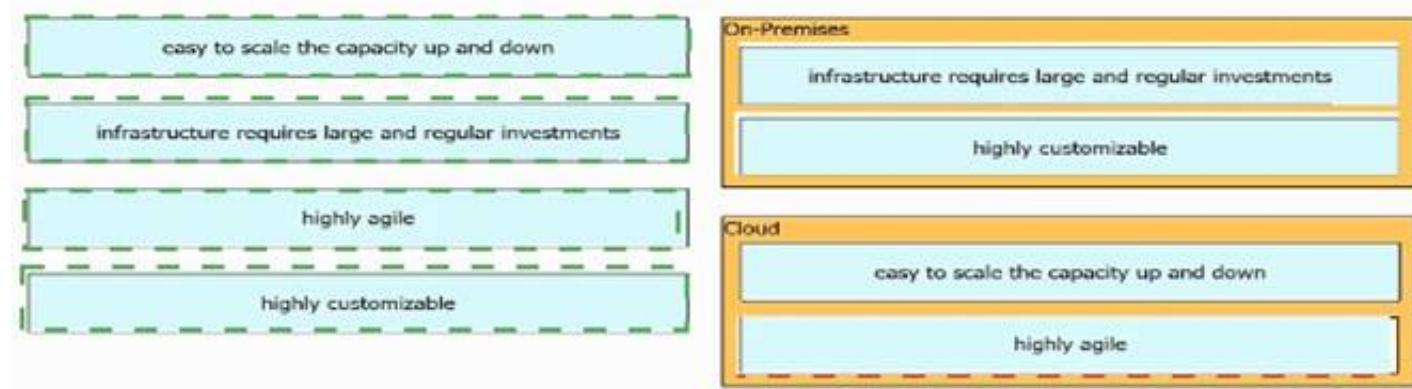
Drag and drop the characteristics from the left onto the infrastructure deployment models they describe on the right.

easy to scale the capacity up and down	On-Premises
infrastructure requires large and regular investments	
highly agile	Cloud
highly customizable	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



#### NEW QUESTION 134

- (Topic 2)

Refer to the exhibit.

```
Switch1# show interfaces trunk
! Output omitted for brevity
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802.1q trunking 10

Port Vlans allowed on trunk
Gi1/0/20 1-4094

Switch2# show interfaces trunk
! Output omitted for brevity
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802.1q trunking 10

Port Vlans allowed on trunk
Gi1/0/20 1-4094
```

The trunk does not work over the back-to-back link between Switch1 interface Giq1/0/20 and Switch2 interface Gig1/0/20. Which configuration fixes the problem?

- A)
 

```
Switch1(config)#interface gig1/0/20
Switch1(config-if)#switchport mode dynamic auto
```
- B)
 

```
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic desirable
```
- C)
 

```
Switch1(config)#interface gig1/0/20
Switch1(config-if)#switchport trunk native vlan 1
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport trunk native vlan 1
```
- D)
 

```
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic auto
```

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

Answer: B

#### NEW QUESTION 136

- (Topic 2)

What is a characteristic of Cisco DNA Northbound APIs?

- A. They simplify the management of network infrastructure devices.
- B. They enable automation of network infrastructure based on intent.
- C. They utilize RESTCONF.
- D. They utilize multivendor support APIs.

**Answer: C**

#### NEW QUESTION 141

DRAG DROP - (Topic 2)

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

HTTP basic authentication	public API resource
OAuth	username and password in an encoded string
secure vault	authorization through identity provider

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

HTTP basic authentication	OAuth
OAuth	HTTP basic authentication
secure vault	secure vault

#### NEW QUESTION 145

- (Topic 2)

What Is a Type 2 hypervisor?

- A. installed as an application on an already installed operating system
- B. runs directly on a physical server and includes its own operating system
- C. supports over-allocation of physical resources
- D. also referred to as a "bare metal hypervisor" because it sits directly on the physical server

**Answer: A**

#### NEW QUESTION 150

- (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 154

- (Topic 2)

What is the wireless received signal strength indicator?

- A. The value given to the strength of the wireless signal received compared to the noise level
- B. The value of how strong the wireless signal is leaving the antenna using transmit power, cable loss, and antenna gain
- C. The value of how much wireless signal is lost over a defined amount of distance
- D. The value of how strong a wireless signal is received, measured in dBm

**Answer: D**

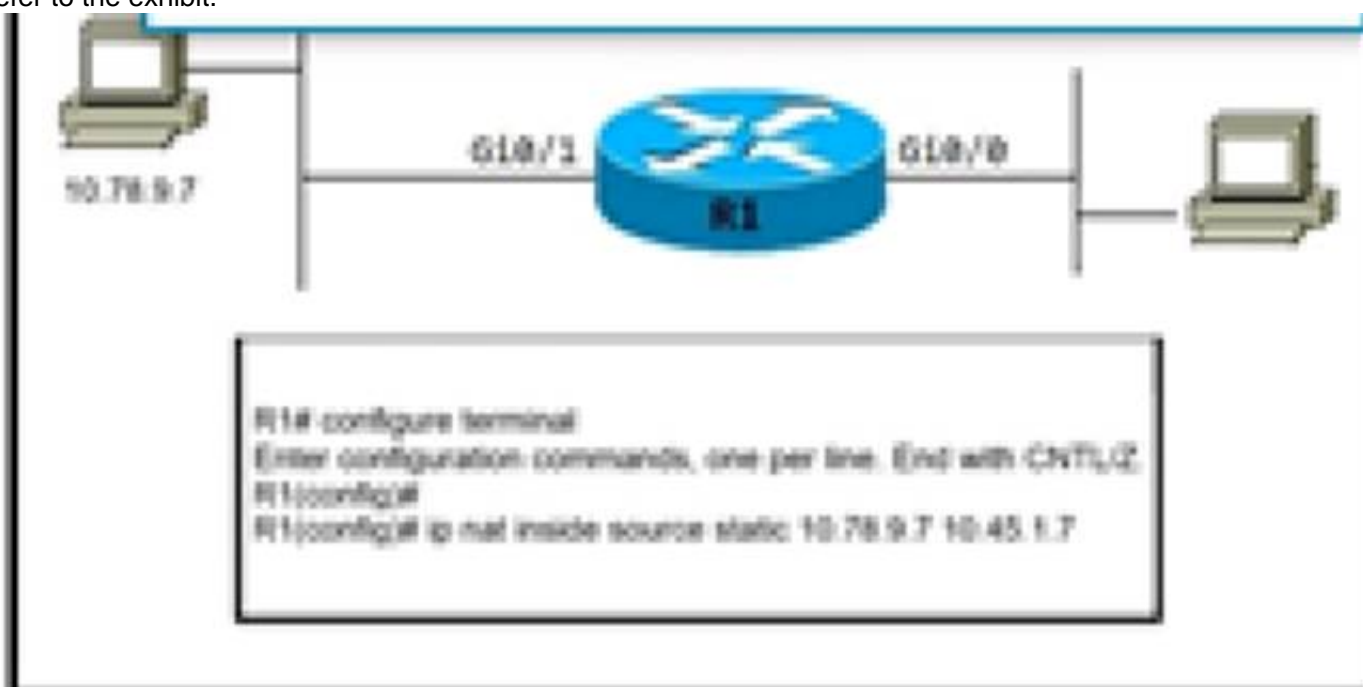
#### Explanation:

RSSI, or "Received Signal Strength Indicator," is a measurement of how well your device can hear a signal from an access point or router. It's a value that is useful for determining if you have enough signal to get a good wireless connection. This value is measured in decibels (dBm) from 0 (zero) to -120 (minus 120). The closer to 0 (zero) the stronger the signal is which means it's better, typically voice networks require a - 65db or better signal level while a data network needs -80db or better.

#### NEW QUESTION 157

- (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 158

- (Topic 2)

Which antenna type should be used for a site-to-site wireless connection?

- A. Omnidirectional
- B. dipole
- C. patch
- D. Yagi

**Answer:** D

**Explanation:**

Yagi Antenna

- Used to communicate in one direction (unidirectional)
- They have a longer range in comparison to Omni Antennas
- Typically only communicate with one other radio, however can talk to multiple
- More common to see used in remote locations

Graphical user interface, text Description automatically generated

#### NEW QUESTION 163

- (Topic 2)

Refer to the exhibit.



Which JSON syntax is derived from this data?

- A)  

```
{["First Name": "Johnny", "Last Name": "Table", "Hobbies": ["Running", "Video games"]], ["First Name": "Billy", "Last Name": "Smith", "Hobbies": ["Napping", "Reading"]]}
```
- B)  

```
{ "Person": [{"First Name": "Johnny", "Last Name": "Table", "Hobbies": "Running", "Video games"}, {"First Name": "Billy", "Last Name": "Smith", "Hobbies": "Napping", "Reading"}]}
```
- C)  

```
{["First Name": "Johnny", "Last Name": "Table", "Hobbies": "Running", "Hobbies": "Video games"], ["First Name": "Billy", "Last Name": "Smith", "Hobbies": "Napping", "Hobbies": "Reading"]}]
```
- D)  

```
{ "Person": [{"First Name": "Johnny", "Last Name": "Table", "Hobbies": ["Running", "Video games"]}, {"First Name": "Billy", "Last Name": "Smith", "Hobbies": ["Napping", "Reading"]}]}]
```

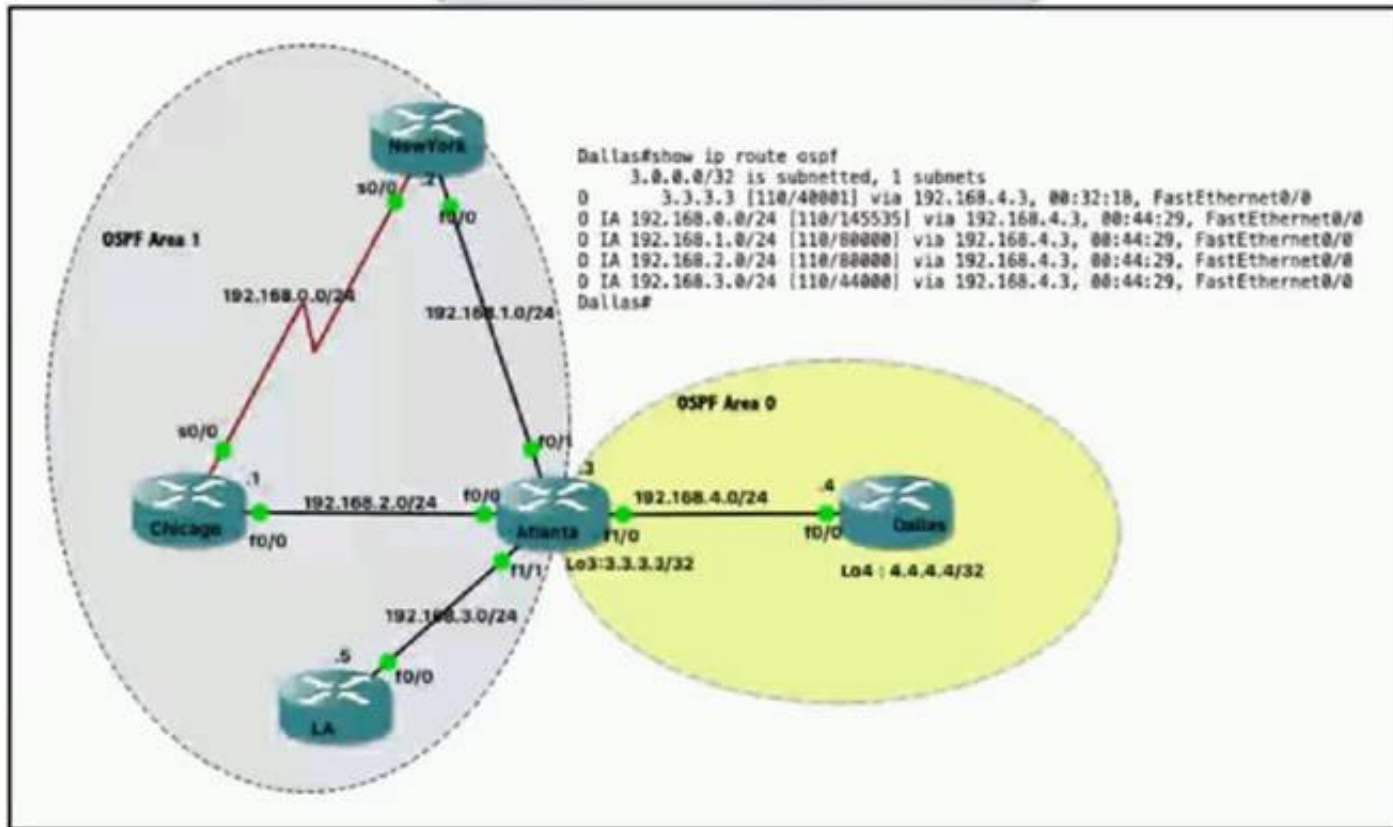
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** D

# NEW QUESTION 164

- (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 167

- (Topic 2)

Which two items are found in YANG data models? (Choose two.)

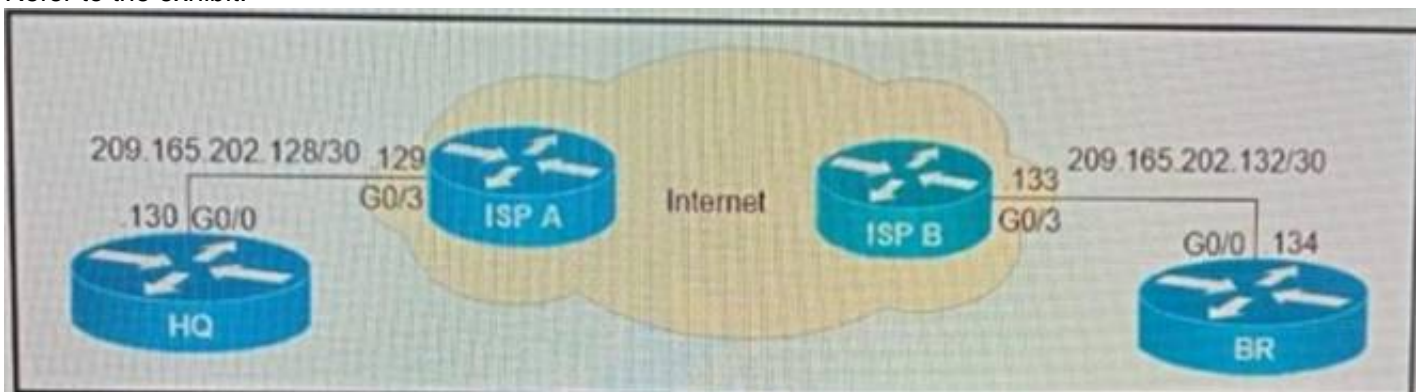
- A. HTTP return codes
- B. rpc statements
- C. JSON schema
- D. container statements
- E. XML schema

**Answer: CE**

# NEW QUESTION 168

- (Topic 2)

Refer to the exhibit.



What is the effect of these commands on the BR and HQ tunnel interfaces?

```
BR(config)#interface tunnel1
BR(config-if)#keepalive 5 3

HQ(config)#interface tunnel1
HQ(config-if)#keepalive 5 3
```

- A. The tunnel line protocol goes down when the keepalive counter reaches 6
- B. The keepalives are sent every 5 seconds and 3 retries
- C. The keepalives are sent every 3 seconds and 5 retries
- D. The tunnel line protocol goes down when the keepalive counter reaches 5

**Answer: B**

#### NEW QUESTION 173

- (Topic 2)

What is the process for moving a virtual machine from one host machine to another with no downtime?

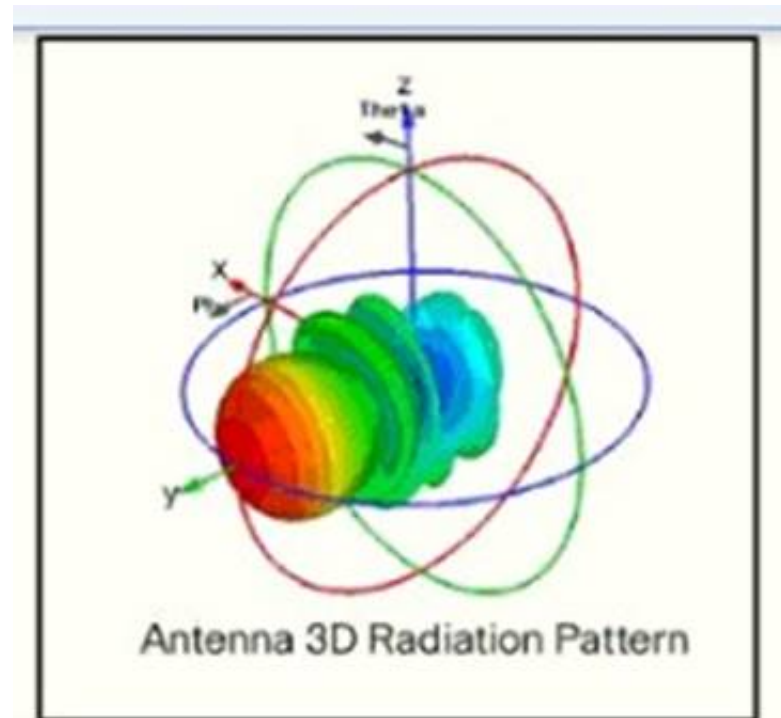
- A. high availability
- B. disaster recovery
- C. live migration
- D. multisite replication

**Answer: C**

#### NEW QUESTION 175

- (Topic 2)

Refer to the exhibit.



Which type of antenna does the radiation pattern represent?

- A. Yagi
- B. multidirectional
- C. directional patch
- D. omnidirectional

**Answer: A**

#### NEW QUESTION 179

- (Topic 2)

Which technology uses network traffic telemetry, contextual information, and file reputation to provide insight into cyber threats?

- A. threat defense
- B. security services
- C. security intelligence
- D. segmentation

**Answer: C**

#### NEW QUESTION 184

- (Topic 2)

Which technology is used as the basis for the cisco sd-access data plane?

- A. IPsec
- B. LISP
- C. VXLAN
- D. 802.1Q

**Answer: C**

#### Explanation:

A virtual network identifier (VNI) is a value that identifies a specific virtual network in the data plane.

#### NEW QUESTION 188

- (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 191

- (Topic 1)

What is the recommended MTU size for a Cisco SD-Access Fabric?

- A. 1500
- B. 9100
- C. 4464
- D. 17914

**Answer:** B

#### NEW QUESTION 192

- (Topic 1)

In cisco SD\_WAN, which protocol is used to measure link quality?

- A. OMP
- B. BFD
- C. RSVP
- D. IPsec

**Answer:** B

#### Explanation:

The BFD (Bidirectional Forwarding Detection) is a protocol that detects link failures as part of the Cisco SD-WAN (Viptela) high availability solution, is enabled by default on all vEdge routers, and you cannot disable it.

#### NEW QUESTION 194

- (Topic 1)

Which JSON syntax is valid?

A)

```
{"switch": "name": "dist1", "interfaces": ["gig1", "gig2", "gig3"]}
```

B)

```
{'switch': ('name': 'dist1', 'interfaces': ['gig1', 'gig2', 'gig3'])}
```

C)

```
{"switch": {"name": "dist1", "interfaces": ["gig1", "gig2", "gig3"]}}
```

D)

```
{/switch/: {/name/: "dist1", /interfaces/: ["gig1", "gig2", "gig3"]}}
```

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

**Answer:** C

#### Explanation:

This JSON can be written as follows:

```
{
'switch': { 'name': 'dist1',
'interfaces': ['gig1', 'gig2', 'gig3']
}
}
```

#### NEW QUESTION 198

- (Topic 1)

An engineer runs the code against an API of Cisco DMA Center, and the platform returns this output What does the response indicate?



```
import requests
import sys
import urllib3

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

def main():
    device_uri = "https://192.168.1.1/dna/system/api/v1/auth/token"
    http_result = requests.get(device_uri, auth=("root", "test398586070!"))
    print(http_result)
    if http_result.status_code != requests.codes.ok:
        print("Call failed! Review get_token() . ")
        sys.exit()
    print(http_result.json()["Token"])

if __name__ == "__main__":
    sys.exit(main())
```

#### Output

```
$ python get_token.py
<Response [405]>
Call failed! Review get_token ().
```

- A. The authentication credentials are incorrect
- B. The URI string is incorrect.
- C. The Cisco DNA Center API port is incorrect
- D. The HTTP method is incorrect

**Answer:** D

#### Explanation:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Status>

#### NEW QUESTION 199

- (Topic 1)

What is a consideration when designing a Cisco SD-Access underlay network?

- A. End user subnets and endpoints are part of the underlay network.
- B. The underlay switches provide endpoint physical connectivity for users.
- C. Static routing is a requirement,
- D. It must support IPv4 and IPv6 underlay networks

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 203

- (Topic 1)

In a wireless Cisco SD-Access deployment, which roaming method is used when a user moves from one access point to another on a different access switch using a single WLC?

- A. Layer 3
- B. inter-xTR
- C. auto anchor
- D. fast roam

**Answer:** B

#### Explanation:

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

From Cisco's guide, under SDA roaming - When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter- xTR, like a highway. Intra is within intra is between. Like interstate highways. That's how I remember. [https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b\\_wl\\_16\\_10\\_cg/mobility.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/mobility.html)

#### NEW QUESTION 208

- (Topic 1)

How is Layer 3 roaming accomplished in a unified wireless deployment?

- A. An EoIP tunnel is created between the client and the anchor controller to provide seamless connectivity as the client is associated with the new AP.
- B. The client entry on the original controller is passed to the database on the new controller.
- C. The new controller assigns an IP address from the new subnet to the client
- D. The client database on the original controller is updated the anchor entry, and the new controller database is updated with the foreign entry.

**Answer:** D

**NEW QUESTION 210**

- (Topic 1)

Which features does Cisco EDR use to provide threat detection and response protection?

- A. containment, threat intelligence, and machine learning
- B. firewalling and intrusion prevention
- C. container-based agents
- D. cloud analysis and endpoint firewall controls

**Answer:** B

**NEW QUESTION 215**

- (Topic 1)

Which design principle states that a user has no access by default to any resource, and unless a resource is explicitly granted, it should be denied?

- A. least privilege
- B. fail-safe defaults
- C. economy of mechanism
- D. complete mediation

**Answer:** B

**NEW QUESTION 216**

- (Topic 1)

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

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

**Answer:** C

**NEW QUESTION 217**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_VXLAN\\_Configuration\\_Guide\\_7x/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_VXLAN\\_Configuration\\_Guide\\_7x\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x_chapter_010.html)

**NEW QUESTION 219**

- (Topic 1)

After a redundant route processor failure occurs on a Layer 3 device, which mechanism allows for packets to be forwarded from a neighboring router based on the most recent tables?

- A. BFD
- B. RIPv2
- C. RP failover
- D. NSF

**Answer:** D

**NEW QUESTION 221**

- (Topic 1)

Which entity is a Type 1 hypervisor?

- A. Oracle VM VirtualBox
- B. VMware server
- C. Citrix XenServer
- D. Microsoft Virtual PC

**Answer:** C

NEW QUESTION 225

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 230

- (Topic 1)

Which congestion queuing method on Cisco IOS based routers uses four static queues?

- A. Priority
- B. custom
- C. weighted fair
- D. low latency

Answer: A

NEW QUESTION 235

- (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 Vlan10ip 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 Customer1ip 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 Vlan10ip route 172.16.1.0 255.255.255.0 Vlan20

Answer: A

#### NEW QUESTION 238

DRAG DROP - (Topic 1)

Drag and drop the threat defense solutions from the left onto their descriptions on the right.

Umbrella	provides malware protection on endpoints
AMP4E	provides IPS/IDS capabilities
FTD	performs security analytics by collecting network flows
StealthWatch	protects against email threat vector
ESA	provides DNS protection

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Umbrella	AMP4E
AMP4E	FTD
FTD	StealthWatch
StealthWatch	ESA
ESA	Umbrella

#### NEW QUESTION 242



DRAG DROP - (Topic 1)  
Drag and drop the characteristics from the left onto the orchestration tools they describe on the right.

utilizes a pull model

utilizes a push model

multimaster architecture

primary/secondary architecture

Ansible

Puppet

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Ansible

utilizes a push model

primary/secondary architecture

Puppet

utilizes a pull model

multimaster architecture

NEW QUESTION 245

DRAG DROP - (Topic 1)  
Drag and drop the Qos mechanisms from the left to the correct descriptions on the right

service policy

policy map

DSCP

mechanism to create a scheduler for packets prior to forwarding

mechanism to apply a QoS policy to an interface

portion of the IP header used to classify packets

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

service policy

policy map

DSCP

policy map

service policy

DSCP

NEW QUESTION 249

- (Topic 1)

When configuration WPA2 Enterprise on a WLAN, which additional security component configuration is required?

- A. NTP server
- B. PKI server
- C. RADIUS server
- D. TACACS server

**Answer: C**

#### NEW QUESTION 254

- (Topic 1)

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

Refer to the exhibit. What is the effect of this configuration?

- A. When users attempt to connect to vty lines 0 through 4, the device will authenticate them against TACACS+ if local authentication fails
- B. The device will authenticate all users connecting to vty lines 0 through 4 against TACACS+
- C. The device will allow users at 192.168.0.202 to connect to vty lines 0 through 4 using the password ciscotestkey
- D. The device will allow only users at 192.166.0.202 to connect to vty lines 0 through 4

**Answer: B**

#### NEW QUESTION 257

- (Topic 1)

Which protocol does REST API rely on to secure the communication channel?

- A. TCP
- B. HTTPS
- C. SSH
- D. HTTP

**Answer: B**

#### Explanation:

The REST API accepts and returns HTTP (not enabled by default) or HTTPS messages that contain JavaScript Object Notation (JSON) or Extensible Markup Language (XML) documents. You can use any programming language to generate the messages and the JSON or XML documents that contain the API methods or Managed Object (MO) descriptions.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest\\_cfg/2\\_1\\_x/b\\_Cisco\\_APIC\\_REST\\_API\\_Configuration\\_Guide/b\\_Cisco\\_APIC\\_REST\\_API\\_Configuration\\_Guide\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Configuration_Guide_chapter_01.html)

#### NEW QUESTION 262

- (Topic 1)

When is an external antenna used inside a building?

- A. only when using Mobility Express
- B. when it provides the required coverage
- C. only when using 2.4 GHz
- D. only when using 5 GHz

**Answer: B**

#### NEW QUESTION 264

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:

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

customizable hardware, purpose-built systems

more suitable for companies with specific regulatory or security requirements

resources can be over or underutilized as requirements vary

Cloud

easy to scale and upgrade

requires a strong and stable internet connection

built-in, automated data backups and recovery

NEW QUESTION 269

- (Topic 1)  
Refer to the exhibit.

```
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 ) FAgP Gi0/0(I) Gi0/1(I)

SW3# show etherchannel summary
Flags: D - down F - 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 Gi0/0(I) Gi0/1(I)
```

Which action resolves the EtherChannel issue between SW2 and SW3?

- A. Configure switchport mode trunk on SW2.
- B. Configure switchport nonegotiate on SW3
- C. Configure channel-group 1 mode desirable on both interfaces.
- D. Configure channel-group 1 mode active on both interfaces.

**Answer:** D

#### NEW QUESTION 270

- (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 271

- (Topic 1)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 272

- (Topic 1)





Refer to the exhibit. An engineer attempts to configure a trunk between switch sw1 and switch SW2 using DTP, but the trunk does not form. Which command should the engineer apply to switch SW2 to resolve this issue?

- A. switchport mode dynamic desirable
- B. switchport nonegotiate
- C. no switchport
- D. switchport mode access

**Answer:** A

#### NEW QUESTION 276

- (Topic 1)

How is 802.11 traffic handled in a fabric-enabled SSID?

- A. centrally switched back to WLC where the user traffic is mapped to a VXLAN on the WLC
- B. converted by the AP into 802.3 and encapsulated into VXLAN
- C. centrally switched back to WLC where the user traffic is mapped to a VLAN on the WLC
- D. converted by the AP into 802.3 and encapsulated into a VLAN

**Answer:** B

#### NEW QUESTION 281

- (Topic 1)

What is a characteristic of a virtual machine?

- A. It must be aware of other virtual machines, in order to allocate physical resources for them
- B. It is deployable without a hypervisor to host it
- C. It must run the same operating system as its host
- D. It relies on hypervisors to allocate computing resources for it

**Answer:** D

#### NEW QUESTION 286

- (Topic 1)

What is the function of the LISP map resolver?

- A. to send traffic to non-LISP sites when connected to a service provider that does not accept nonroutable EIDs as packet sources
- B. to connect a site to the LISP-capable part of a core network publish the EID-to-RLOC mappings for the site, and respond to map-request messages
- C. to decapsulate map-request messages from ITRs and forward the messages to the MS.
- D. to advertise routable non-LISP traffic from one address family to LISP sites in a different address family

**Answer:** C

#### Explanation:

Map resolver (MR): The MR performs the following functions: Receives MAP requests, which are encapsulated by ITRs. Provides a service interface to the ALT router, de-encapsulates MAP requests, and forwards on the ALT topology.

#### NEW QUESTION 287

- (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 289

- (Topic 1)

What is one fact about Cisco SD-Access wireless network deployments?

- A. The access point is part of the fabric underlay
- B. The WLC is part of the fabric underlay

- C. The access point is part the fabric overlay
- D. The wireless client is part of the fabric overlay

**Answer: C**

#### NEW QUESTION 292

- (Topic 1)

```
R2#show standby
FastEthernet1/0 - Group 50
  State is Active
    2 state changes, last state change 00:04:02
  Virtual IP address is 10.10.1.1
  Active virtual MAC address is 0000.0c07.ac32 (MAC In Use)
  Local virtual MAC address is 0000.0c07.ac32 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.504 secs
  Preemption enabled, delay reload 90 secs
  Active router is local
  Standby router is unknown
  Priority 200 (configured 200)
  Track interface FastEthernet0/0 state Up decrement 20
  Group name is "hsrp-Fal/0-50" (default)
R2#
%IP-4-DUPADDR: Duplicate address 10.10.1.1 on FastEthernet1/0, sourced by 0000.0c07.ac28
R2#
```

Refer to the exhibit. An engineer configures a new HSRP group. While reviewing the HSRP status, the engineer sees the logging message generated on R2. Which is the cause of the message?

- A. The same virtual IP address has been configured for two HSRP groups
- B. The HSRP configuration has caused a spanning-tree loop
- C. The HSRP configuration has caused a routing loop
- D. A PC is on the network using the IP address 10.10.1.1

**Answer: A**

#### NEW QUESTION 296

- (Topic 1)

Refer to the exhibit.

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

An engineer must modify the access control list EGRESS to allow all IP traffic from subnet 10.1.10.0/24 to 10.1.2.0/24. The access control list is applied in the outbound direction on router interface GigabitEthernet 0/1. Which configuration commands can the engineer use to allow this traffic without disrupting existing traffic flows?

A)  
**config t**  
**ip access-list extended EGRESS**  
**permit ip 10.1.10.0 255.255.255.0 10.1.2.0 255.255.255.0**

B)  
**config t**  
**ip access-list extended EGRESS**  
**5 permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255**

C)  
**config t**  
**ip access-list extended EGRESS2**  
**permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255**  
**permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255**  
**deny ip any any**  
**!**  
**interface g0/1**  
**no ip access-group EGRESS out**  
**ip access-group EGRESS2 out**

D)  
**config t**  
**ip access-list extended EGRESS**  
**permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255**

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

**Answer:** B

#### NEW QUESTION 297

- (Topic 1)

Refer to the exhibit.

```
Extended IP access list EGRESS
10 permit ip 10.0.0.0 0.0.0.255 any
!
<Output Omitted>
!
interface GigabitEthernet0/0
ip address 209.165.200.225 255.255.255.0
ip access-group EGRESS out
duplex auto
speed auto
media-type rj45
!
```

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

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

**Answer:** A

#### NEW QUESTION 298

- (Topic 1)

```
ip vrf BLUE
rd 1:1
!
interface Vlan100
description GLOBAL_INTERFACE
ip address 10.10.1.254 255.255.255.0
!
access-list 101 permit ip 10.10.5.0 0.0.0.255 10.10.1.0
255.255.255.0
!
route-map VRF_TO_GLOBAL permit 10
match ip address 101
set global
!
interface Vlan500
description VRF_BLUE
ip vrf forwarding BLUE
ip address 10.10.5.254 255.255.255.0
ip policy route-map VRF_TO_GLOBAL
```

Refer to the exhibit. An engineer attempts to create a configuration to allow the Blue VRF to leak into the global routing table, but the configuration does not function as expected. Which action resolves this issue?

- A. Change the access-list destination mask to a wildcard.
- B. Change the source network that is specified in access-list 101.
- C. Change the route-map configuration to VRF\_BLUE.
- D. Change the access-list number in the route map

**Answer:** A

#### NEW QUESTION 299

- (Topic 1)

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

- A. MTU
- B. Window size



- C. MRU
- D. MSS

**Answer:** D

**Explanation:**

The TCP Maximum Segment Size (TCP MSS) defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. This TCP/IP datagram might be fragmented at the IP layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. Contrary to popular belief, the MSS value is not negotiated between hosts. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host. TCP MSS takes care of fragmentation at the two endpoints of a TCP connection, but it does not handle the case where there is a smaller MTU link in the middle between these two endpoints. PMTUD was developed in order to avoid fragmentation in the path between the endpoints. It is

**NEW QUESTION 303**

- (Topic 1)

A customer has recently implemented a new wireless infrastructure using WLC-5520 at a site directly next to a large commercial airport. Users report that they intermittently lose Wi-Fi connectivity, and troubleshooting reveals it is due to frequent channel changes. Which two actions fix this issue? (Choose two)

- A. Remove UNII-2 and Extended UNII-2 channels from the 5 GHz channel list
- B. Restore the DCA default settings because this automatically avoids channel interference.
- C. Configure channels on the UNII-2 and the Extended UNII-2 sub-bands of the 5 GHz band only
- D. Enable DFS channels because they are immune to radar interference.
- E. Disable DFS channels to prevent interference with Doppler radar

**Answer:** AE

**NEW QUESTION 304**

- (Topic 1)

"HTTP/1.1 204 content" is returned when the 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 306**

- (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 308**

- (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:**

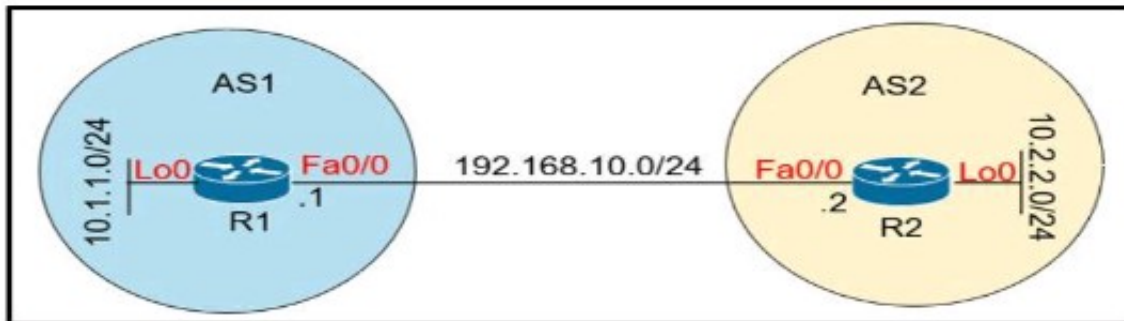
Support Virtual Switching System (VSS) to provide resiliency, and increased operational efficiency with a single point of management; VSS increases operational efficiency by simplifying the network, reducing switch

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 311

- (Topic 1)

Refer to the exhibit.



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

A)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0
```

```
R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

B)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0
```

```
R2(config)#router bgp 2
R2(config-router)#neighbor 10.1.1.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

C)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.0.0.0 mask 255.0.0.0
```

```
R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.0.0.0 mask 255.0.0.0
```

D)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#neighbor 10.2.2.2 update-source lo0
R1(config-router)#network 10.1.1.0 mask 255.255.255.0
```

```
R2(config)#router bgp 2
R2(config-router)#neighbor 10.1.1.1 remote-as 1
R2(config-router)#neighbor 10.1.1.1 update-source lo0
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

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

**Answer:** A

#### Explanation:

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

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



+ the command “neighbor 10.1.1.1 ebgp-multihop 2” on R1 and “neighbor 10.2.2.2 ebgpmultihop 2” on R1. This command increases the TTL value to 2 so that BGP updates can reach the BGP neighbor which is two hops away.

+ Answer 'R1 (config) #router bgp 1  
R1 (config-router) #neighbor 192.168.10.2 remote-as 2  
R1 (config-router) #network 10.1.1.0 mask 255.255.255.0 R2 (config) #router bgp 2  
R2 (config-router) #neighbor 192.168.10.1 remote-as 1  
R2 (config-router) #network 10.2.2.0 mask 255.255.255.0

Quick Wireless Summary

Cisco Access Points (APs) can operate in one of two modes: autonomous or lightweight

+ Autonomous: self-sufficient and standalone. Used for small wireless networks.

+ Lightweight: A Cisco lightweight AP (LAP) has to join a Wireless LAN Controller (WLC) to function. LAP and WLC communicate with each other via a logical pair of CAPWAP tunnels.

– Control and Provisioning for Wireless Access Point (CAPWAP) is an IETF standard for control messaging for setup, authentication and operations between APs and WLCs. CAPWAP is similar to LWAPP except the following differences:

+CAPWAP uses Datagram Transport Layer Security (DTLS) for authentication and encryption to protect traffic between APs and controllers. LWAPP uses AES.

+ CAPWAP has a dynamic maximum transmission unit (MTU) discovery mechanism.

+ CAPWAP runs on UDP ports 5246 (control messages) and 5247 (data messages) An LAP operates in one of six different modes:

+ Local mode (default mode): measures noise floor and interference, and scans for intrusion detection (IDS) events every 180 seconds on unused channels

+ FlexConnect, formerly known as Hybrid Remote Edge AP (H-REAP), mode: allows data traffic to be switched locally and not go back to the controller. The FlexConnect AP can perform standalone client authentication and switch VLAN traffic locally even when it's disconnected to the WLC (Local Switched). FlexConnect AP can also tunnel (via CAPWAP) both user wireless data and control traffic to a centralized WLC (Central Switched).

+ Monitor mode: does not handle data traffic between clients and the infrastructure. It acts like a sensor for location-based services (LBS), rogue AP detection, and IDS

+ Rogue detector mode: monitor for rogue APs. It does not handle data at all.

+ Sniffer mode: run as a sniffer and captures and forwards all the packets on a particular channel to a remote machine where you can use protocol analysis tool (Wireshark, Airopeek, etc) to review the packets and diagnose issues. Strictly used for troubleshooting purposes.

+ Bridge mode: bridge together the WLAN and the wired infrastructure together.

Mobility Express is the ability to use an access point (AP) as a controller instead of a real WLAN controller. But this solution is only suitable for small to midsize, or multi-site branch locations where you might not want to invest in a dedicated WLC. A Mobility Express WLC can support up to 100 Aps

#### NEW QUESTION 314

- (Topic 4)

A network administrator is designing a new network for a company that has frequent power spikes. The company wants to ensure that employees can the best solution for the administrator to recommend?

- A. Generator
- B. Cold site
- C. Redundant power supplies
- D. Uninterruptible power supply

**Answer: D**

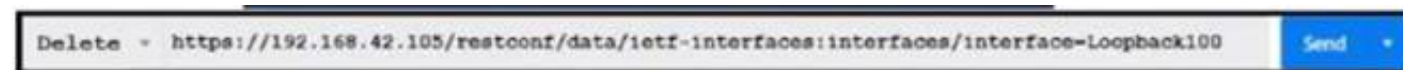
#### Explanation:

This is because an uninterruptible power supply (UPS) is a device that provides backup power to a network device or a computer in case of a power outage or a power spike. A UPS can prevent data loss, corruption, or damage to the device by providing a smooth and continuous power supply. A UPS can also protect the device from power surges, brownouts, or voltage fluctuations. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.1: Implementing Device Hardening.

#### NEW QUESTION 316

- (Topic 4)

Refer to the exhibit.



What does the response "204 No Content mean for the REST API request?

- A. Interface toopback 100 is not removed from the configuration.
- B. Interface toopback 100 is not found in the configuration.
- C. Interface toopback 100 is removed from the configuration.
- D. The DELETE method is not supported.

**Answer: C**

#### Explanation:

This is because the response “204 No Content” means that the REST API request was successful, but there is no content to return. The request was a DELETE method, which is used to remove a resource from the server. The resource in this case was the interface loopback 100, which was deleted from the configuration of the device. The source of this answer is the Cisco ENCOR v1.1 course, module 8, lesson 8.4: Implementing REST API.

#### NEW QUESTION 321

- (Topic 4)

An engineer is configuring RADIUS-Based Authentication with EAP MS-CHAPv2 is configured on a client device. Which outer method protocol must be configured on the ISE to support this authentication type?

- A. EAP-TLS



- B. PEAP
- C. LDAP
- D. EAP-FAST

**Answer:** D

#### NEW QUESTION 325

- (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 330

- (Topic 4)

An engineer applies this EEM applet to a router:

```
event manager applet Test
event timer watchdog time 600
action 1.0 cli command "enable"
action 2.0 cli command "term exec prompt timestamp"
action 3.0 cli command "term length 0"
action 4.0 cli command "show ip arp | in 0005.4210.0049"
action 5.0 regexp ".*(ARPA).*" $_cli_result
action 6.0 if $_regexp_result eq 1
action 7.0 syslog msg $_cli_result
action 8.0 end
```

What does the applet accomplish?

- A. It generates a syslog message every 600 seconds on the status of the specified MAC address.
- B. It checks the MAC address table every 600 seconds to see if the specified address has been learned.
- C. It compares syslog output to the MAC address table every 600 seconds and generates an event when there is a match.
- D. It compares syslog output to the MAC address table every 600 seconds and generates an event when no match is found.

**Answer:** B

#### NEW QUESTION 331

- (Topic 4)

Which two methods are used by an AP that is trying to discover a wireless LAN controller? (Choose two.)

- A. Cisco Discovery Protocol neighbour
- B. broadcasting on the local subnet
- C. DNS lookup cisco-DNA-PRIMARY.localdomain
- D. DHCP Option 43
- E. querying other APs

**Answer:** BD

#### NEW QUESTION 335

- (Topic 4)

What does the statement `print(format(0.8, '.0%'))` display?

- A. 80%
- B. 8%
- C. .08%
- D. 8.8%

**Answer:** B

#### NEW QUESTION 340

- (Topic 4)

What is one being of implementing a data modeltag 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 342

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 347

- (Topic 4)

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

```
{
  "response": [{
    "family": "Routers",
    "macAddress": "00:c8:8b:80:bb:00",
    "hostname": "BorderA",
    "role": "BORDER ROUTER",
    "lastUpdateTime": 1577420167054,
    "serialNumber": "FXS8799Q1SE",
    "softwareVersion": "16.3.2",
    "upTime": "5 days, 9:22:32:17",
    "lastUpdated": "2021-03-05 23:30:37"
  ]
}]
```

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

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

**Answer:** C

#### NEW QUESTION 348

- (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 349

- (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 f 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 351

- (Topic 4)

Refer to the exhibit.

```
v= json.loads(requests.get("http://10.66.77.88:3000/version").text)[0]['ver']
c= json.loads(requests.get("http://10.66.77.88:3000/version").text)[1]['cnt']
bp= []
for i in range (int(c)):
    bp.append(json.loads(requests.get("http://10.66.77.88:3000/badip").text)[1]['ip'])
```

What is achieved by this Python script?

- A. It counts JSON data from a website.
- B. It loads JSON data into an HTTP request.
- C. It reads JSON data into a formatted list.
- D. It converts JSON data to an HTML document.

**Answer:** B

#### NEW QUESTION 353



- (Topic 4)

Which authorization framework gives third-party applications limited access to HTTP services?

- A. IPsec
- B. Basic Auth
- C. GRE
- D. OAuth 2.0

**Answer: D**

#### NEW QUESTION 355

- (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 356

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)
```

dumps

print

dump

open

r

w

#### NEW QUESTION 357

- (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 362

- (Topic 4)

How is traffic classified when using Cisco TrustSec technology?

- A. with the VLAN  
B. with the MAC address  
C. with the IP address  
D. with the security group tag

**Answer:** D

**NEW QUESTION 364**

- (Topic 4)

A customer deploys a new wireless network to perform location-based services using Cisco DNA Spaces. The customer has a single WLC located on-premises in a secure data center. The security team does not want to expose the WLC to the public Internet. Which solution allows the customer to securely send RSSI updates to Cisco DNA Spaces?

- A. Implement Cisco Mobility Services Engine
- B. Replace the WLC with a cloud-based controller.
- C. Perform tethering with Cisco DNA Center.
- D. Deploy a Cisco DNA Spaces connector as a VM.

**Answer:** D

**NEW QUESTION 366**

- (Topic 4)

What is a characteristics of Cisco SD-WAN?

- A. operates over DTLS/TLS authenticated and secured tunnels
- B. requires manual secure tunnel configuration
- C. uses unique per-device feature templates
- D. uses control connections between routers

**Answer:** A

**NEW QUESTION 371**

- (Topic 4)

Which two actions provide controlled Layer 2 network connectivity between virtual machines running on the same hypervisor? (Choose two.)

- A. Use a single trunk link to an external Layer2 switch.
- B. Use a virtual switch provided by the hypervisor.
- C. Use a virtual switch running as a separate virtual machine.
- D. Use a single routed link to an external router on stick.
- E. Use VXLAN fabric after installing VXLAN tunneling drivers on the virtual machines.

**Answer:** BC

**Explanation:**

Source 1: [https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-1000v-switch-vmware-vsphere/at\\_a\\_glance\\_c45-532467.pdf](https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-1000v-switch-vmware-vsphere/at_a_glance_c45-532467.pdf)

Source 2: [https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/sw/vm\\_fex/vmware/gui/config\\_guide/2-1/b\\_GUI\\_VMware\\_VM-FEX\\_UCSM\\_Configuration\\_Guide\\_2\\_1/b\\_GUI\\_VMware\\_VM-FEX\\_UCSM\\_Configuration\\_Guide\\_2\\_1\\_chapter\\_0110.pdf](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/vm_fex/vmware/gui/config_guide/2-1/b_GUI_VMware_VM-FEX_UCSM_Configuration_Guide_2_1/b_GUI_VMware_VM-FEX_UCSM_Configuration_Guide_2_1_chapter_0110.pdf)

**NEW QUESTION 374**

- (Topic 4)

What is a benefit of using segmentation with TrustSec?

- A. Packets sent between endpoints on a LAN are encrypted using symmetric key cryptography.
- B. Firewall rules are streamlined by using business-level profiles.
- C. Integrity checks prevent data from being modified in transit.
- D. Security group tags enable network segmentation.

**Answer:** B

**NEW QUESTION 378**

- (Topic 4)

Why does the vBond orchestrator have a public IP?

to enable vBond to learn 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 381**

- (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 386

- (Topic 4)

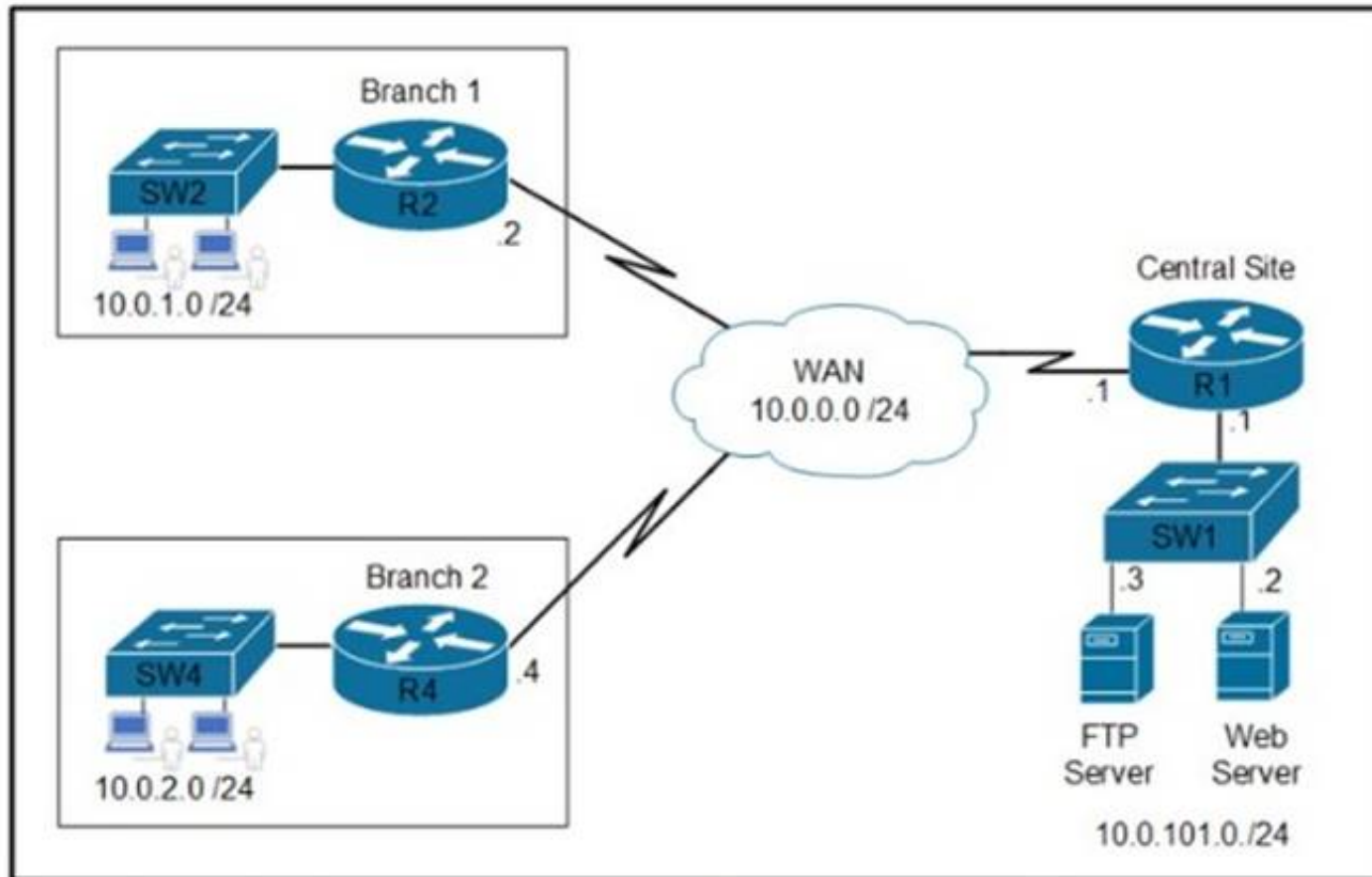
Which solution simplifies management of secure access to network resources?

- A. RFC 3580-based solution to enable authenticated access leveraging RADIUS and AV pairs
- B. TrustSec to logically group internal user environments and assign policies
- C. 802.1AE to secure communication in the network domain
- D. ISE to automate network access control leveraging RADIUS AV pairs

**Answer: B**

#### NEW QUESTION 387

- (Topic 4)



Refer to the exhibit Which two commands are required on route» R1 to block FTP and allow all other traffic from the Branch 2 network' (Choose two)

- ☐ `access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data`  
`access-list 101 permit ip any any`
- ☐ `access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp`  
`access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data`  
`access-list 101 permit ip any any`
- ☐ `interface GigabitEthernet0/0`  
`ip address 10.0.0.1 255.255.255.252`  
`ip access-group 101 out`
- ☐ `interface GigabitEthernet0/0`  
`ip address 10.0.101.1 255.255.255.252`  
`ip access-group 101 in`
- ☐ `access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp`  
`access-list 101 permit ip any any`

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

**Answer: BC**

#### NEW QUESTION 390

- (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?

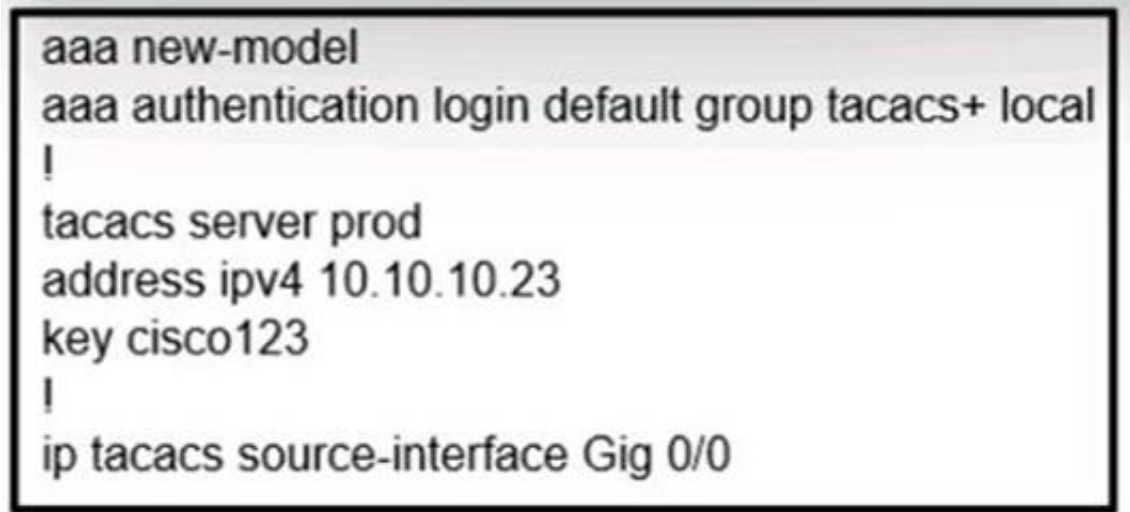
- A. Configure login authentication privileged on line con 0.
- B. Configure a local username with privilege level 15.
- C. Configure privilege level 15 on line con 0.
- D. Configure a RADIUS or TACACS+ server and use it to send the privilege level.

Answer: C

NEW QUESTION 395

- (Topic 4)

Refer to the exhibit.



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+

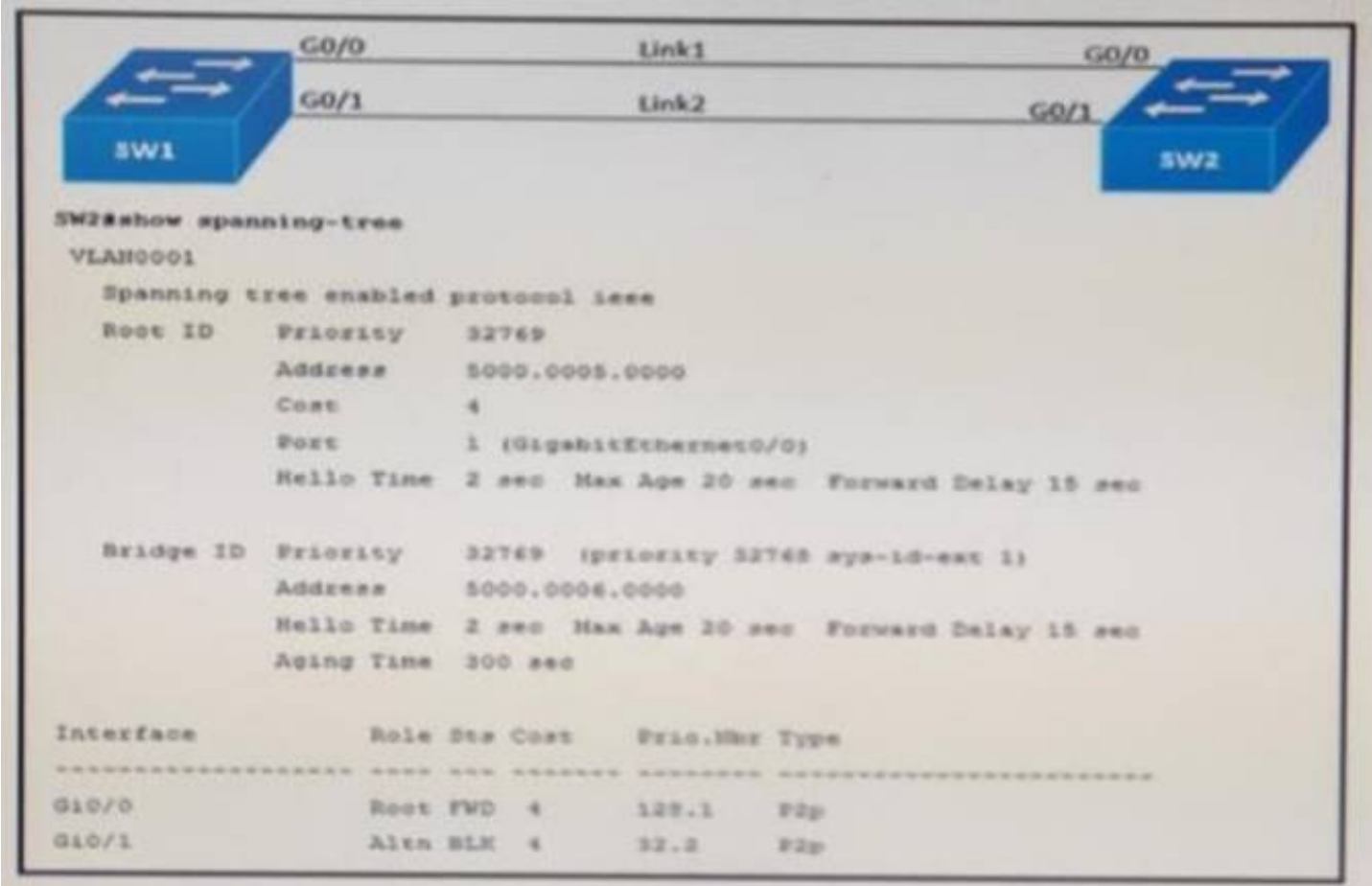
Answer: C

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 396

- (Topic 4)



Refer to the exhibit. Link 1 uses a copper connection and link 2 uses a fiber connection. The fiber port must be the primary port for all forwarding. The output of the show spanning- tree command on SW2 shows that the fiber port is blocked by Spanning Tree. After entering the spanning-tree port-priority 32 command on G0/1 on SW2, the port remains blocked. Which command should be entered on the ports connected to Link 2 is resolve the issue?

- A. Enter spanning-tree port-priority 64 on SW2
- B. Enter spanning-tree port-priority 224 on SW1.
- C. Enter spanning-tree port-priority 4 on SW2.
- D. Enter spanning-tree port-priority 32 on SW1.

Answer: D

NEW QUESTION 397

- (Topic 4)

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

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

**Answer: B**

**Explanation:**

This is because the Design workflow in Cisco DNA Center allows the engineer to create a new network infrastructure by defining the physical network device hierarchy based on the location of the devices. The location hierarchy consists of four levels: global, area, building, and floor. The engineer can add, edit, or delete locations and assign devices to them. The location hierarchy helps to organize the network devices and apply policies and settings based on the location. The source of this answer is the Cisco ENCOR v1.1 course, module 8, lesson 8.6: Implementing Network Design Processes.

**NEW QUESTION 402**

- (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 405

- (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 409

- (Topic 4)

```
Request URL: https://www.cisco.com/libs/granite/csrf/token.json
Request Method: GET
Status Code: 403
Remote Address: 23.207.65.173:443
Referrer Policy: strict-origin-when-cross-origin
```

Refer to the exhibit. Why was the response code generated?

- A. The resource was unreachable
- B. Access was denied based on the user permissions.
- C. The resource is no longer available on the server.
- D. There is a conflict in the current state of the resource.

**Answer: B**

#### NEW QUESTION 412

- (Topic 4)

Refer to the exhibit.

```
interface Ethernet0/0

ipaddress 10.1.1.1 255.255.255.252

ip natoutside

!

interface Ethernet0/0

ipaddress 10.10.10.1 255.255.255.0

ip natinside

!

ip nat inside source static 10.10.10.10 10.0.3.10
```

Which address type is 10.10.10.10 configured for?

- A. inside global
- B. outside local
- C. outside global
- D. inside local

**Answer:** D

#### NEW QUESTION 415

- (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 416

- (Topic 4)

In a wireless network environment, what is calculated using the numerical values of the transmitter power level, cable loss, and antenna gain?

- A. RSSI
- B. dBI
- C. SNR
- D. EIRP

**Answer:** B

#### NEW QUESTION 421

- (Topic 4)

In the Cisco DNA Center Image Repository, what is a golden image?

- A. The latest software image that is available for a specific device type
- B. The Cisco recommended software image for a specific device type.
- C. A software image that is compatible with multiple device types.
- D. A software image that meets the compliance requirements of the organization.

**Answer:** B

#### NEW QUESTION 423

- (Topic 4)

Which unit of measure is used to measure wireless RF SNR?

- A. mW
- B. bBm
- C. dB
- D. dBi

**Answer:** C

#### NEW QUESTION 427

- (Topic 4)

Refer to the exhibit.

```
count = 8
while count > 4 :
    print(count)
    count -= 1
```

What is output by this code?

- A. 8 7 6 5
- B. -4 -5 -6 -7
- C. -1 -2-3-4
- D. 4 5 6 7

**Answer:** A

#### NEW QUESTION 429

- (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 follows<sup>12</sup>:

? 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 strings<sup>12</sup>.

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 array<sup>12</sup>.

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 pair<sup>12</sup>. References: 1: JSON Introduction, 2: JSON Syntax

**NEW QUESTION 434**

- (Topic 4)

A company recently rearranged some users' workspaces and moved several users to different desks. The network administrator receives a report that all of the users who were moved are having connectivity issues. Which of the following is the most likely reason?

- A. Ports are error disabled.
- B. Ports are administratively down.
- C. Ports are having an MDIX issue.
- D. Ports are trunk ports.

**Answer:** A

**Explanation:**

This is because ports can become error disabled when they detect certain errors or violations on the network, such as a loop, a security breach, or a duplex mismatch. When a port is error disabled, it shuts down and stops forwarding traffic until it is manually re-enabled by the administrator. The users who were moved to different desks may have plugged their devices into ports that were configured with different settings or security policies than their original ports, and this may have triggered the error disable state. The source of this answer is the Cisco ENCOR v1.1 course, module 3, lesson 3.3: Implementing EtherChannel.

**NEW QUESTION 438**

- (Topic 4)

In which two ways does the routing protocol OSPF differ from EIGRP? (Choose two.)

- A. OSPF supports an unlimited number of hop
- B. EIGRP supports a maximum of 255 hops.
- C. OSPF provides shorter convergence time than EIGRP.
- D. OSPF is distance vector protoco
- E. EIGRP is a link-state protocol.
- F. OSPF supports only equal-cost load balancin
- G. EIGRP supports unequal-cost load balancing.
- H. OSPF supports unequal-cost load balancin
- I. EIGRP supports only equal-cost load balancing.

**Answer:** AD

**NEW QUESTION 439**

- (Topic 4)

A customer has a wireless network deployed within a multi-tenant building. The network provides client access, location-based services, and is monitored using Cisco DNA Center. The security department wants to locate and track malicious devices based on threat signatures. Which feature is required for this solution?

- A. Cisco aWIPS policies on the WLC
- B. Cisco aWIPS policies on Cisco DNA Center
- C. malicious rogue rules on the WLC
- D. malicious rogue rules on Cisco DNA Center

**Answer:** B

**NEW QUESTION 443**

- (Topic 4)

Which QoS feature uses the IP Precedence bits in the ToS field of the IP packet header to partition traffic into different priority levels?

- A. marking
- B. shaping
- C. policing
- D. classification

**Answer:** D

**NEW QUESTION 445**

- (Topic 4)

A customer has a pair of Cisco 5520 WLCs set up in an SSO cluster to manage all APs. Guest traffic is anchored to a Cisco 3504 WLC located in a DMZ. Which action is needed to ensure that the EoIP tunnel remains in an UP state in the event of failover on the SSO cluster?

- A. Configure back-to-back connectivity on the RP ports.
- B. Enable default gateway reachability check.
- C. Use the same mobility domain on all WLCs.
- D. Use the mobility MAC when the mobility peer is configured.

**Answer: B**

**NEW QUESTION 448**

- (Topic 4)

Refer to the exhibit.

```
R2(config)#event manager applet script_1
R2(config-applet)#action 1 cli command "enable"
R2(config-applet)#action 2 cli command "config t"
R2(config-applet)#action 3 cli command "interface ge0/0"
R2(config-applet)#action 4 cli command "ip add 172.16.1.1 255.255.255.0"
R2(config-applet)#action 5 cli command "no sh"
R2(config-applet)#action 6 cli command "end"
R2(config-applet)#exit
```

An engineer must create a manually triggered EEM applet to enable the R2 router interface and assign an IP address to it. What is required to complete this configuration?

- A. R2(config-applet)# event oir
- B. R2(config-applet)#action 4 cli command "ip add 172.16.1.1 0.0.0.255"
- C. R2(config)# event manager session cli username
- D. R2(config-applet)# event none sync yes

**Answer: D**

**NEW QUESTION 453**

- (Topic 4)

Which element is unique to a Type 2 hypervisor?

- A. memory
- B. VM OS
- C. host OS
- D. host hardware

**Answer: C**

**NEW QUESTION 455**

- (Topic 4)

Which two methods are used to assign security group tags to the user in a Cisco Trust Sec architecture? (Choose two )

- A. modular QoS
- B. policy routing
- C. web authentication
- D. DHCP
- E. IEEE 802.1x

**Answer: CE**

**NEW QUESTION 460**

- (Topic 4)

A VoIP phone is plugged in to a port but cannot receive calls. Which of the following needs to be done on the port to address the issue?

- A. Trunk all VLANs on the port.
- B. Configure the native VLAN.
- C. Tag the traffic to voice VLAN.
- D. Disable VLANs.

**Answer: C**

**Explanation:**

This is because the voice VLAN is a special VLAN that is used to separate the voice traffic from the data traffic on a switch port. The voice VLAN allows the VoIP phone to communicate with the voice server and receive calls. The voice VLAN is usually configured with a higher priority than the data VLAN to ensure the quality of service for the voice traffic. The voice VLAN is tagged with a VLAN ID that is different from the data VLAN ID. The switch port must be configured to tag the

traffic to the voice VLAN, either manually or automatically using protocols such as CDP or LLDP. The source of this answer is the Cisco ENCOR v1.1 course, module 3, lesson 3.2: Implementing VLANs and Trunks.

#### NEW QUESTION 461

- (Topic 4)

A firewall address of 192.168.1.101 can be pinged from a router but, when running a traceroute to it, this output is received

```

1  *  *  *
2  *  *  *
3  *  *  *
4  *  *  *
5  *  *  *
6  *  *  *
7  *  *  *
8  *  *  *
9  *  *  *
10 *  *  *
```

What is the cause of this issue?

- A. The firewall blocks ICMP traceroute traffic.
- B. The firewall rule that allows ICMP traffic does not function correctly
- C. The firewall blocks ICMP traffic.
- D. The firewall blocks UDP traffic

**Answer: D**

#### NEW QUESTION 465

- (Topic 4)

What is one characteristic of VXLAN?

- A. It supports a maximum of 4096 VLANs.
- B. It supports multitenant segments.
- C. It uses STP to prevent loops in the underlay network.
- D. It uses the Layer 2 header to transfer packets through the network underlay.

**Answer: B**

#### NEW QUESTION 469

- (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?

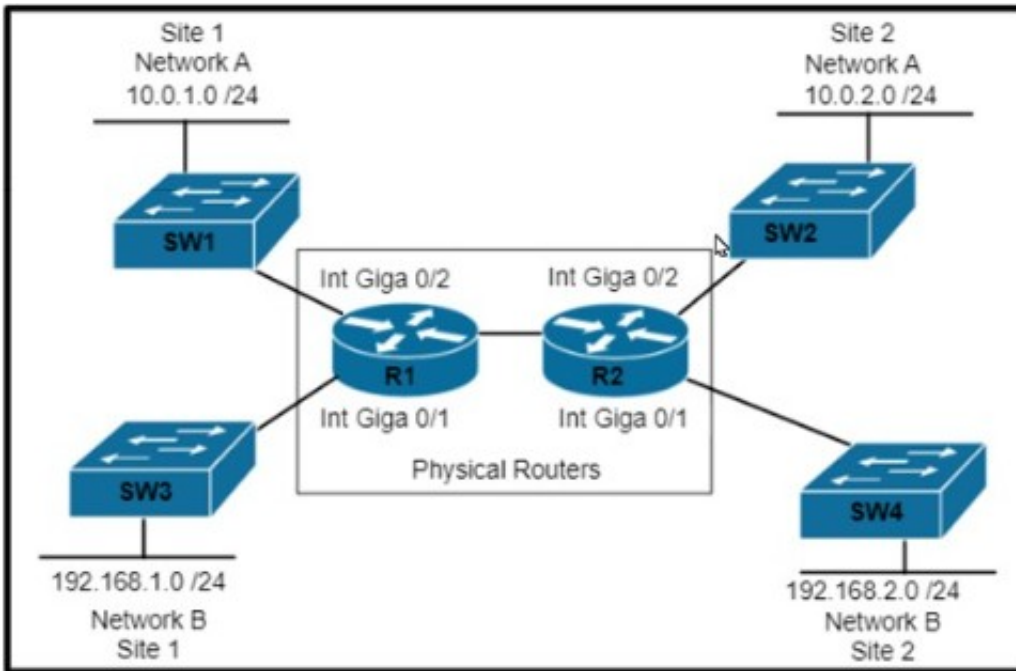
- A. standby version 2
- B. standby 512 preempt
- C. standby redirects
- D. standby 512 priority 100

**Answer: A**

#### NEW QUESTION 473

- (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 477

- (Topic 4)

An engineer must configure Interface and sensor monitoring on a router. The NMS server is located in a trusted zone with IP address 10.15.2.19. Communication between the router and the NMS server must be encrypted and password-protected using the most secure algorithms. Access must be allowed only for the NMS server and with the minimum permission levels needed. Which configuration must the engineer apply?

A)

```
ip access-list standard nms
 permit 10.15.2.19 255.255.255.255

snmp-server view ro cisco included

snmp-server view ro ifEntry included

snmp-server group nms v3 priv read ro access nms
snmp-server user user1 nms v3 auth 3des Password1 pri aes 192 Password123
```

B)

```
ip access-list standard nms
 permit 10.15.2.19 0.0.0.0

snmp-server view rw iso included

snmp-server view rw ifEntry included

snmp-server group nms v3 auth write rw access nms
snmp-server user user1 nms v3 auth des Password1 pri des Password123
```

C)

```
ip access-list extended nms
 permit 1 host 10.15.2.19 any

snmp-server view ro internet included

snmp-server view ro ifEntry included

snmp-server group nms v3 priv notify ro access nms
snmp-server user user1 nms v3 encrypted auth md5 Password1 pri 3des Password123
```

D)

```
ip access-list standard nms
 permit 10.15.2.19 0.0.0.0

snmp-server view ro iso included
```

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

**Answer:** A

**Explanation:**

Option A is the correct configuration to apply interface and sensor monitoring on a router with the given requirements. This option uses SNMPv3, which is the most secure version of SNMP that supports encryption and authentication. The configuration steps are as follows<sup>12</sup>:

? Create an access list named nms that permits only the NMS server with IP address 10.15.2.19 to access the router: ip access-list standard nms and permit 10.15.2.19 0.0.0.0.

? Create a view named rw that includes all the SNMP objects: snmp-server view rw included.

? Create a group named nms that uses SNMPv3 with privacy (encryption) and authentication, and assigns the view rw and the access list nms to the group: snmp-server group nms v3 priv read rw access nms.

? Create a user named nms that belongs to the group nms and uses DES for authentication and AES for encryption, with the passwords despass and aespass respectively: snmp-server user nms nms v3 auth des despass priv aes 192 aespass.

Option B is incorrect because it does not use encryption for SNMP communication, which is required by the question. The noauth keyword in the snmp-server group command means that no authentication or encryption is used, which makes the SNMP packets vulnerable to eavesdropping and tampering<sup>1</sup>.

Option C is incorrect because it does not use the most secure algorithms for SNMP communication, which is required by the question. The md5 and des keywords in the snmp-server user command mean that MD5 and DES are used for authentication and encryption respectively, which are considered weak and outdated algorithms. AES and SHA are recommended instead<sup>1</sup>.

Option D is incorrect because it does not restrict the access to the NMS server only, which is required by the question. The snmp-server community command creates a community string that acts as a password for SNMP access, but it does not specify an access list to limit the source IP addresses that can use the community string. Therefore, any device that knows the community string can access the router via SNMP<sup>1</sup>. References: 1: Configuring SNMPv3, 2: SNMP Configuration Guide, Cisco IOS XE Gibraltar 16.12.x

**NEW QUESTION 481**

- (Topic 4)

Refer to the exhibit.

```
vlan 222
  remote-span
!
vlan 223
  remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

What happens to access interfaces where VLAN 222 is assigned?

- A. STP BPDU guard is enabled
- B. A description "RSPAN" is added.
- C. They are placed into an inactive state.
- D. They cannot provide PoE.

**Answer: C**

**Explanation:**

This is because the exhibit shows the configuration of a remote SPAN (RSPAN) VLAN, which is a special VLAN that is used to transport mirrored traffic from one switch to another switch over a trunk link. The RSPAN VLAN is configured with the remote- span option, which indicates that the VLAN is dedicated for RSPAN use only. The access interfaces where the RSPAN VLAN is assigned are placed into an inactive state, which means that they cannot forward any traffic other than the mirrored traffic. The source of this answer is the Cisco ENCOR v1.1 course, module 6, lesson 6.2: Implementing SPAN, RSPAN, and ERSPAN.

**NEW QUESTION 485**

- (Topic 4)

Refer to the exhibit.

```
client.load_system_host_keys()
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
client.connect(ip, port= 22, username= usr, password= pswd)
stdin, stdout, stderr = client.exec_command(t + '\n')
time.sleep(3)
print(t)
for u in stdout:
    print(u)
client.close()
```

Which action results from executing the Python script?

- A. display the output of a command that is entered on that device in a single line
- B. SSH to the IP address that is manually entered on that device
- C. display the output of a command that is entered on that device
- D. display the unformatted output of a command that is entered on that device

**Answer: A**

**NEW QUESTION 488**

- (Topic 4)



```
>tracert www.crmABC.com
Tracing route to www.crmABC.com [192.168.100.1]
 0  0ms  0ms  0ms  10.10.10.1
 1  3ms  5ms  3ms  10.10.10.1
 2  4ms  6ms  4ms  10.100.100.1
 3  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 492

- (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 follows<sup>12</sup>:

? 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 lines<sup>12</sup>.

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 default<sup>12</sup>.

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 errors<sup>12</sup>. References: 1: Controlling Access to a Virtual Terminal Line, 2: Configuring Secure Shell

**NEW QUESTION 495**

- (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 500**

- (Topic 4)

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

- A. The router with the shortest uptime
- B. The router with the lowest IP address
- C. The router with the highest IP address

D. The router with the longest uptime

**Answer:** B

#### NEW QUESTION 503

- (Topic 4)

What does a YANG model provide?

- A. standardized data structure independent of the transport protocols
- B. creation of transport protocols and their interaction with the OS
- C. user access to interact directly with the CLI of the device to receive or modify network configurations
- D. standardized data structure that can be used only with NETCONF or RESTCONF transport protocols

**Answer:** D

#### NEW QUESTION 505

- (Topic 4)

What does the Cisco DNA Center Authentication API provide?

- A. list of global issues that are logged in Cisco DNA Center
- B. access token to make calls to Cisco DNA Center
- C. list of VLAN names
- D. dent health status

**Answer:** B

#### NEW QUESTION 506

- (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:

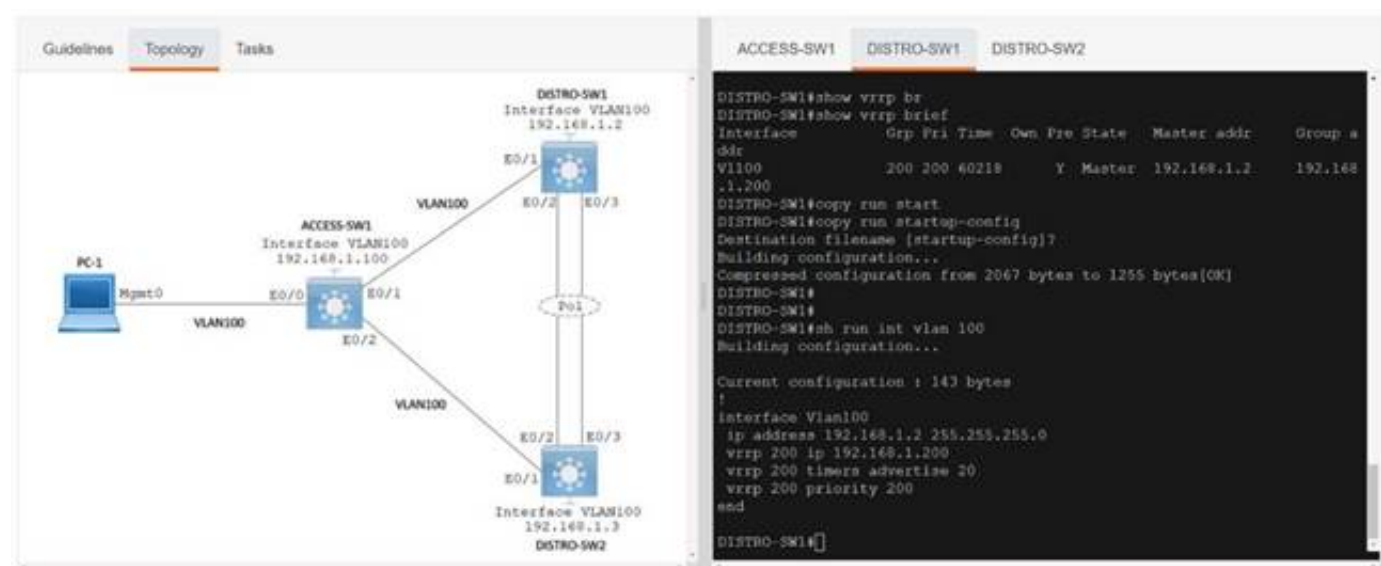
This is because the CoPP configuration shown in the exhibit applies a service policy to the control plane of the router, which is responsible for processing the routing protocols, management protocols, and other control traffic. The service policy uses a class map that matches the access list 100, which 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 511

SIMULATION - (Topic 4)

Simulation 10

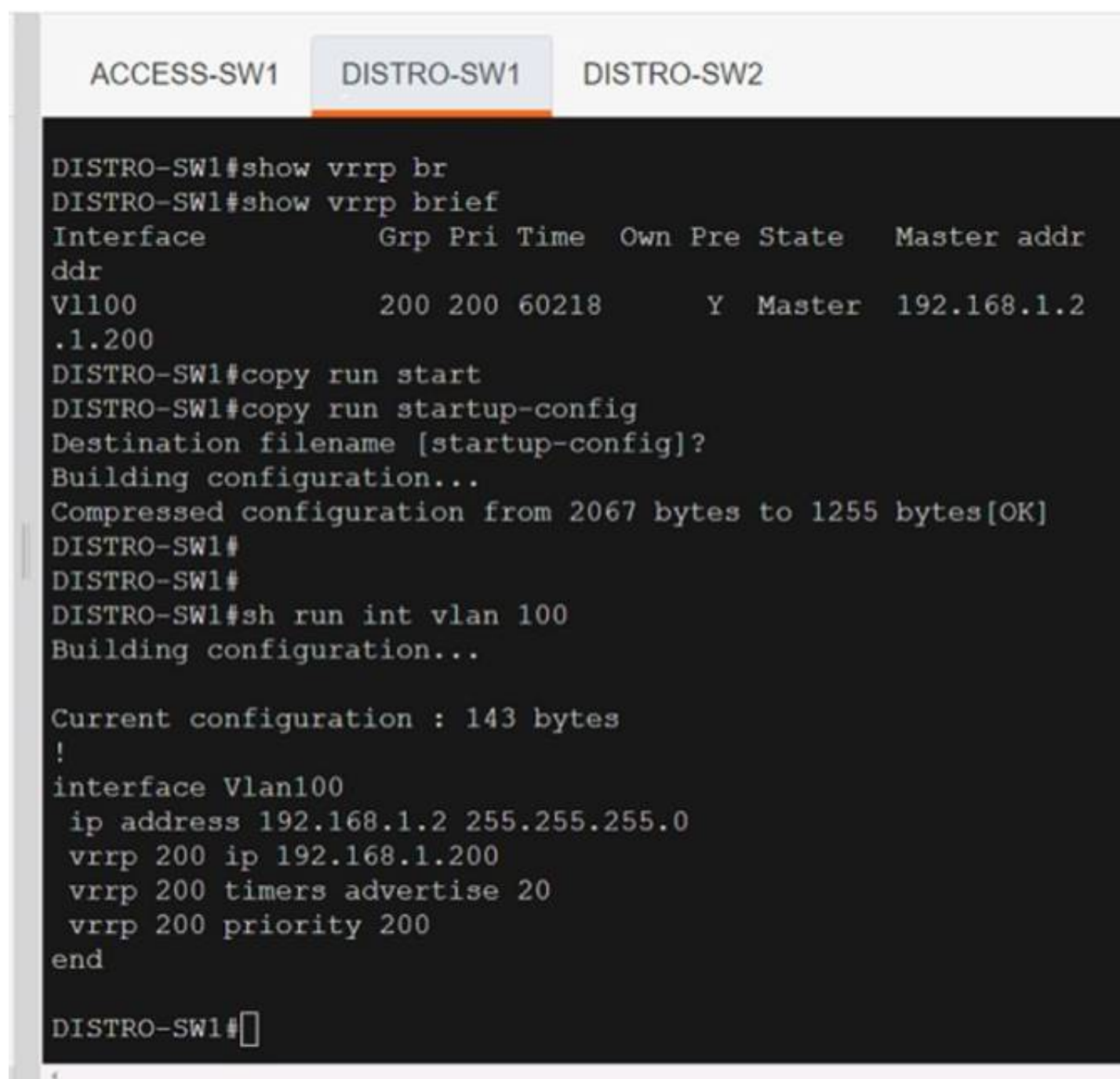


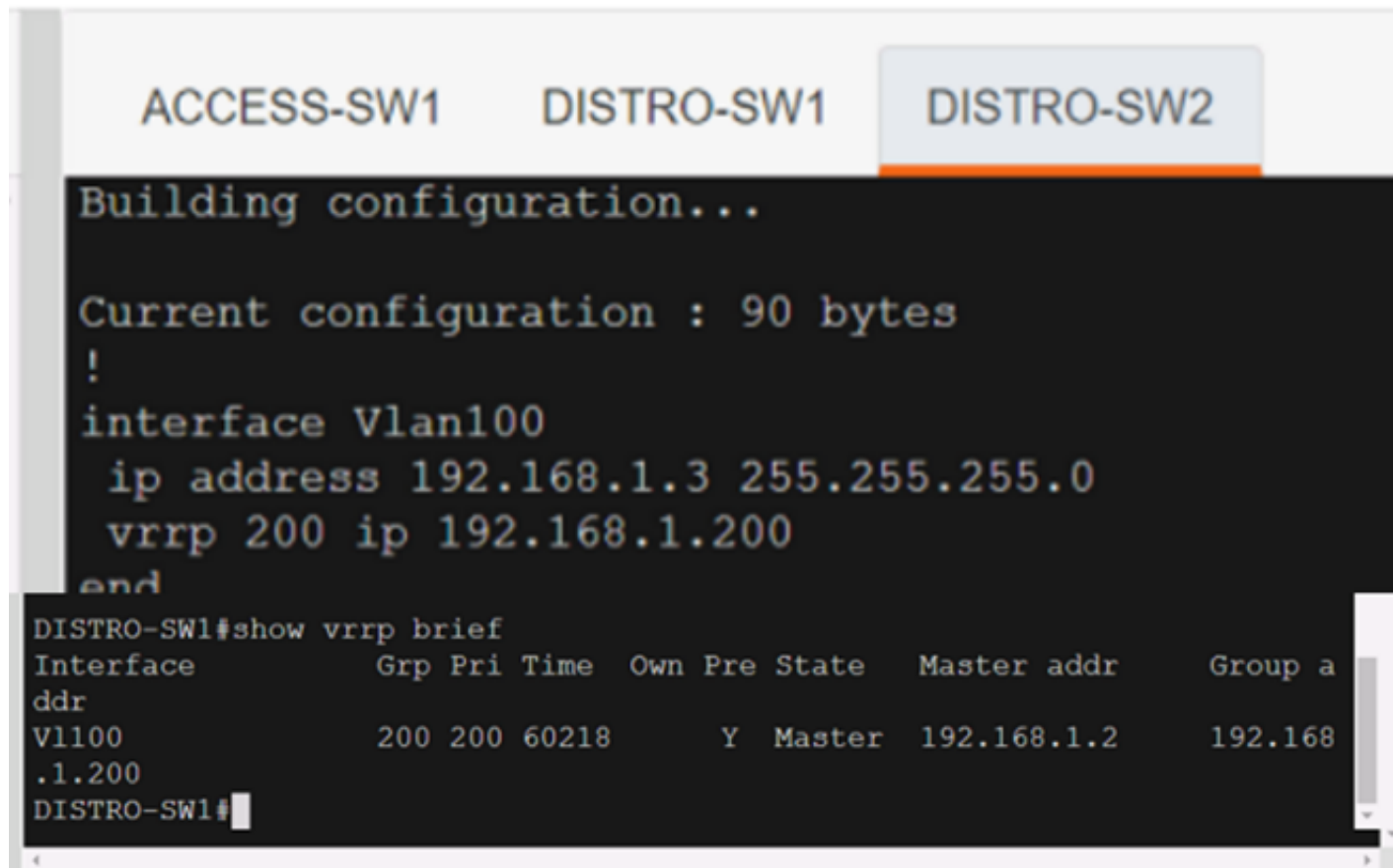


- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**





```

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 514

- (Topic 4)

What is a characteristic of the Cisco DNA Center Template Editor feature?

- A. It facilitates software upgrades to network devices from a central point.
- B. It facilitates a vulnerability assessment of the network devices.
- C. It provides a high-level overview of the health of every network device.
- D. It uses a predefined configuration through parameterized elements or variables.

**Answer: D**

#### Explanation:

This is because the Cisco DNA Center Template Editor feature is a tool that allows the network administrator to create and deploy configuration templates to multiple network devices. The configuration templates use parameterized elements or variables, which are placeholders for values that can be customized for each device. For example, a variable can represent the hostname, IP address, or interface number of a device. The parameterized elements or variables can be defined manually or automatically using the Cisco DNA Center inventory. The source of this answer is the Cisco ENCOR v1.1 course, module 8, lesson 8.5: Implementing Network Configuration Management.

#### NEW QUESTION 519

- (Topic 4)

Refer to the exhibit. What is the result of this Python code?

- A. 1
- B. 7
- C. 7.5

**Answer: D**

#### Explanation:

The Python code in the exhibit defines a function called average that takes two parameters a and b and returns the arithmetic mean of them. The function is then called with the arguments 5 and 10, which are assigned to a and b respectively. The function returns  $(5 + 10) / 2$ , which is 7.5. Therefore, the result of the Python code is 7.5. References: Python Functions, Python Arithmetic Operators

#### NEW QUESTION 521

- (Topic 4)

Which method ensures the confidentiality of data exchanged over a REST API?

- A. Use the POST method instead of URL-encoded GET to pass parameters.
- B. Encode sensitive data using Base64 encoding.
- C. Deploy digest-based authentication to protect the access to the API.
- D. Use TLS to secure the underlying HTTP session.

**Answer: B**

#### NEW QUESTION 522

- (Topic 4)

Which technology reduces the implementation of STP and leverages both unicast and multicast?

- A. VSS
- B. VXLAN
- C. VPC

D. VLAN

**Answer:** B

**NEW QUESTION 524**

- (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 527**

DRAG DROP - (Topic 4)

An engineer plans to use Python to convert text files that contain device information to JSON. Drag and drop the code snippets from the bottom onto the blanks in the code to construct the request. Not all options are used.



```

import json
input_file = 'raw-data.txt'
dictionary_1 = {}
fields = ['Device_type', 'IP_Address', 'IOS_type', 'Username', 'Password']

l = 1
for line in text:
    description = list(line.strip().split(None, 4))
    print(description)
    Device_Number = 'Device' + str(l)
    i = 0
    dictionary_2 = {}
    while i < len(fields):
        dictionary_2[fields[i]] = description[i]
        i = i + 1
    dictionary_1[Device_Number] = dictionary_2
    l = l + 1

json.dump(dictionary_1, out_file, indent=4)

```

raw-data.txt

```

{
  "Device1": {
    "Device_type": "switch",
    "IOS_type": "ios",
    "IP_Address": "10.1.1.1",
    "Username": "user1",
    "Password": "pass1"
  },
  "Device2": {
    "Device_type": "router",
    "IOS_type": "ios-xr",
    "IP_Address": "10.1.1.2",
    "Username": "user2",
    "Password": "pass2"
  },
  "Device3": {
    "Device_type": "nexus-9k",
    "IOS_type": "nx-os",
    "IP_Address": "10.1.1.3",
    "Username": "user3",
    "Password": "pass3"
  }
}

```

Output of Python Code

```

switch ios 10.1.1.1 user1 pass1
router ios-xr 10.1.1.2 user2 pass2
nexus-9k nx-os 10.1.1.3 user3 pass3

```

out\_file.close()

out\_file = open ("Json-Output.json", "w")

with open(raw-data) as text:

with open(input\_file) as text:

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

```

import json
input_file = 'raw-data.txt'
dictionary_1 = {}
fields = ['Device_type', 'IP_Address', 'IOS_type', 'Username', 'Password']

with open(input_file) as text:
    l = 1
    for line in text:
        description = list(line.strip().split(None, 4))
        print(description)
        Device_Number = 'Device' + str(l)
        i = 0
        dictionary_2 = {}
        while i < len(fields):
            dictionary_2[fields[i]] = description[i]
            i = i + 1
        dictionary_1[Device_Number] = dictionary_2
        l = l + 1

out_file = open ("Json-Output.json", "w")
json.dump(dictionary_1, out_file, indent=4)
out_file.close()

```

raw-data.txt

```

{
  "Device1": {
    "Device_type": "switch",
    "IOS_type": "ios",
    "IP_Address": "10.1.1.1",
    "Username": "user1",
    "Password": "pass1"
  },
  "Device2": {
    "Device_type": "router",
    "IOS_type": "ios-xr",
    "IP_Address": "10.1.1.2",
    "Username": "user2",
    "Password": "pass2"
  },
  "Device3": {
    "Device_type": "nexus-9k",
    "IOS_type": "nx-os",
    "IP_Address": "10.1.1.3",
    "Username": "user3",
    "Password": "pass3"
  }
}

```

Output of Python Code

```

switch ios 10.1.1.1 user1 pass1
router ios-xr 10.1.1.2 user2 pass2
nexus-9k nx-os 10.1.1.3 user3 pass3

```

out\_file.close()

out\_file = open ("Json-Output.json", "w")

with open(raw-data) as text:

with open(input\_file) as text:

#### NEW QUESTION 530

- (Topic 4)

Which two new security capabilities are introduced by using a next-generation firewall at the Internet edge? (Choose two.)

- A. DVPN  
 B. NAT  
 C. stateful packet inspection  
 D. application-level inspection  
 E. integrated intrusion prevention

Answer: DE

#### NEW QUESTION 534

- (Topic 4)

Which A record type should be configured for access points to resolve the IP address of a wireless LAN controller using DNS?

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

**Answer: D**

#### NEW QUESTION 538

- (Topic 4)

Refer to the exhibit.

```

1  Status Code: 200
2  Body:
3  {
4      "response": [
5          {
6              "memorySize": "3735302144",
7              "family": "Wireless Controller",
8              "role": "ACCESS",
9              "description": "Cisco Controller Wireless Version:8.5.140.0",
10             "roleSource": "AUTO",
11             "lastUpdated": "2021-09-10 13:48:02",
12             "deviceSupportLevel": "Supported",
13             "softwareType": "Cisco Controller",
14             "softwareVersion": "8.5.140.0",
15             "macAddress": "ac:4a:56:6c:7c:00",
16             "collectionInterval": "Global Default",
17             "inventoryStatusDetail": "<status><general code=\\\"SUCCESS\\\"/></status>",
18             "serialNumber": "FOL25040021",
19             "lastUpdateTime": 1631281682276,
20             "hostname": "c3504.abc.inc",
21             "tagCount": "0",
22
23             ***Output omitted***
24
25             "lineCardId": "",
26             "managedAtleastOnce": true,
27             "location": null,
28             "type": "Cisco 3504 Wireless LAN Controller",
29             "managementState": "Managed",
30             "instanceUuid": "6b741b27-f7e7-4470-b6fc-d5168cc59502",
31             "instanceTenantId": "5e8e896e4d4add00ca2b6487",
32             "id": "6b741b27-f7e7-4470-b6fc-d5168cc59502"
33         }
34     ],
35     "version": "1.0"
36 }

```

Which HTTP request produced the REST API response that was returned by Cisco DNA Center?

- A. fetch /network-device?macAddress=ac:4a:56:6c:7c:00
- B. POST/network-device?macAddress=ac:4a:56:6c:7c:00
- C. GET/network-device?macAddress=ac:4a:56:6c:7c:00

**Answer: C**

#### Explanation:

This is because the REST API response shows the details of a network device with the specified MAC address. The GET method is used to retrieve information from the Cisco DNA Center server. The network-device resource is used to access the network device inventory. The macAddress parameter is used to filter the results by the MAC address of the device. The source of this answer is the Cisco ENCOR v1.1 course, module 8, lesson 8.4: Implementing REST API.

#### NEW QUESTION 539

- (Topic 4)

Which function is performed by vSmart in the Cisco SD-WAN architecture?

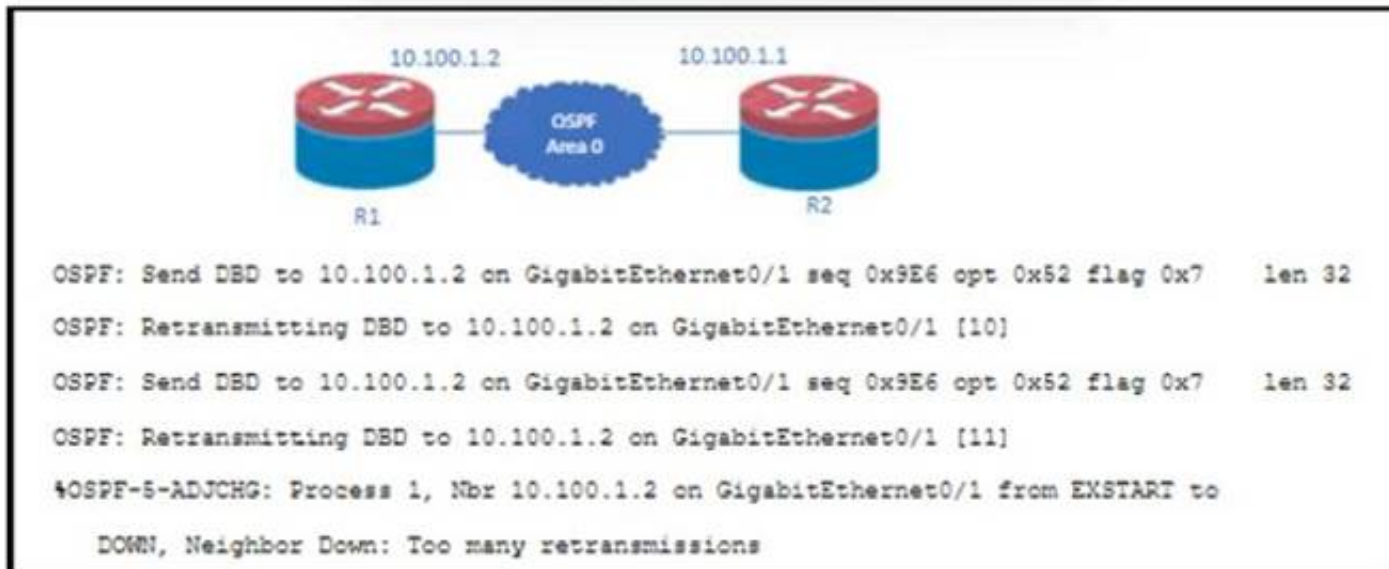
- A. distribution of IPsec keys
- B. Redistribution between OMP and other routing protocols
- C. facilitation of NAT detection and traversal
- D. execution of localized policies

**Answer: B**

#### NEW QUESTION 542

- (Topic 4)

Refer to the exhibit.



Why does OSPF fail to establish an adjacency between R1 and R2?

- A. authentication mismatch
- B. interface MTU mismatch
- C. area mismatch
- D. timers mismatch

**Answer: B**

### NEW QUESTION 543

SIMULATION - (Topic 4)

Simulation 02

Configure HSRP between DISTRO-SW1 and DISTRO-SW2 on VLAN 100 for hosts connected to ACCESS-SW1 to achieve these goals:

- \* 1. Configure group number 1 using the virtual IP address of 192.168.1.1/24.
- \* 2. Configure DISTRO-SW1 as the active router using a priority value of 110 and DISTRO-SW2 as the standby router.
- \* 3. Ensure that DISTRO-SW2 will take over the active role when DISTRO-SW1 goes down, and when DISTRO-SW1 recovers, it automatically resumes the active role.

Comment

---

Guidelines Topology Tasks

Configure HSRP between DISTRO-SW1 and DISTRO-SW2 on VLAN100 for hosts connected to ACCESS-SW1 to achieve these goals:

1. Configure group number 1 using the virtual IP address of 192.168.1.1 /24.
2. Configure DISTRO-SW1 as the active router using a priority value of 110 and DISTRO-SW2 as the standby router.
3. Ensure that DISTRO-SW2 will take over the active role when DISTRO-SW1 goes down, and when DISTRO-SW1 recovers, it automatically resumes the active role.

DISTRO-SW1 DISTRO-SW2

DISTRO-SW1>

Guidelines Topology Tasks

DISTRO-SW1 DISTRO-SW2

DISTRO-SW1>



```
DISTRO-SW1#sh run
DISTRO-SW1#sh running-config
Building configuration...

Current configuration : 1661 bytes
!
! Last configuration change at 02:15:58 PST Fri May 20 2022
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname DISTRO-SW1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!
```

```
!
hostname DISTRO-SW1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!
!
!
!
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.2
ip dhcp excluded-address 192.168.1.3
ip dhcp excluded-address 192.168.1.100
!
ip dhcp pool CISCO123
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
!
ip cef
no ip igmp snooping
no ipv6 cef
!
```

```
!
interface Port channel1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
!
interface Ethernet0/0
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
 channel-group 1 mode active
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
 channel-group 1 mode active
!
interface Vlan100
 ip address 192.168.1.2 255.255.255.0
!
```

```
!
interface Vlan100
  ip address 192.168.1.2.255.255.255.0
  !
  ip forward-protocol nd
  !
  no ip http server
  no ip http secure-server
  !
  ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
  ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
  !
  !
  !
  !
  !
  !
  control-plane
  !
  !
  line con 0
    logging synchronous
  line aux 0
  line vty 0 4
    login
```

DISTRO-SW2

```
no ipv6 cef
!!
!!
!!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
!
interface Ethernet0/0
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
!
```

```
!  
interface Ethernet0/1  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 100  
  switchport mode trunk  
!  
interface Ethernet0/2  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 100  
  switchport mode trunk  
  channel-group 1 mode passive  
!  
interface Ethernet0/3  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 100  
  switchport mode trunk  
  channel-group 1 mode passive  
!  
interface Vlan100  
  ip address 192.168.1.3 255.255.255.0  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr  
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr  
!  
!
```

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

DISTRO-SW1

Sw1

int vlan 100

standby 1 ip 192.168.1.1

standby 1 priority 110

standby 1 preempt copy run start

DISTRO-SW2 SW2

int vlan 100

standby 1 ip 192.168.1.1

standby 1 preempt

copy run start

OR

MINOR CHANGE IN ABOVE HSRP SCENERIO



Implement GLBP between DISTRO-SW1 and DISTRO-SW2 on VLAN100 for hosts connected to ACCESS-SW1 to achieve these goals:

1. Configure group 1 using the virtual IP address of 192.168.1.254.
2. Configure DISTRO-SW1 as the AVG using a priority value of 110.
3. If DISTRO-SW1 suffers a failure and recovers, ensure that it automatically resumes the AVG role after waiting for a minimum of 15 seconds.

Description automatically generated

Check the IP address 1.254 check the minimum 15 seconds solution get change.

DISTRO-SW1

Sw1

int vlan 100

glbp 1 ip 192.168.1.254

glbp 1 priority 110

glbp 1 timers 5 15

glbp 1 preempt

copy run start

DISTRO-SW2 SW2

int vlan 100

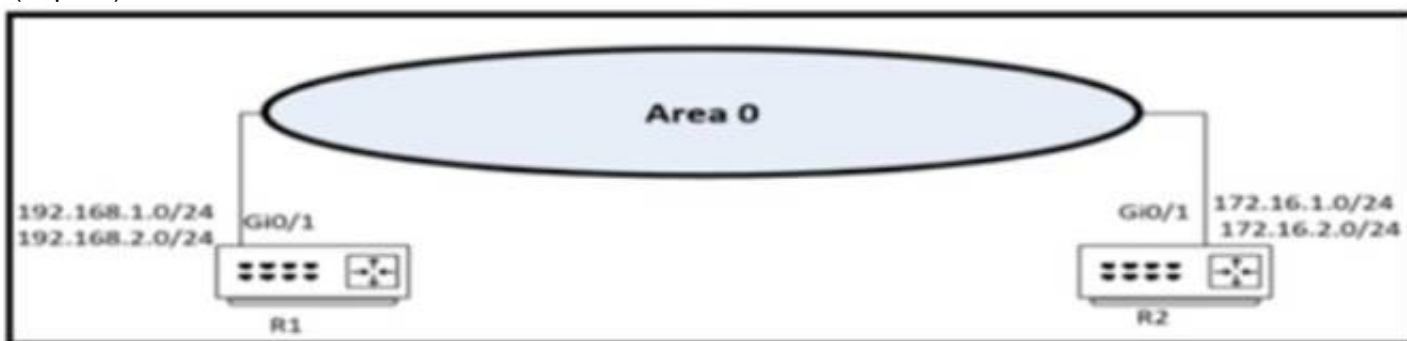
glbp 1 ip 192.168.1.254

glbp 1 timers 5 15

glbp 1 preempt copy run start

#### NEW QUESTION 545

- (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 546

DRAG DROP - (Topic 4)

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

ETR	network infrastructure component that learns of EID-prefix mapping entries from an ETR
map server	IPv4 or IPv6 address of an endpoint within a LISP site.
EID	de-encapsulates LISP packets coming from outside of the LISP site to destinations inside of the site

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

ETR	map server
map server	EID
EID	ETR

NEW QUESTION 551

DRAG DROP - (Topic 4)

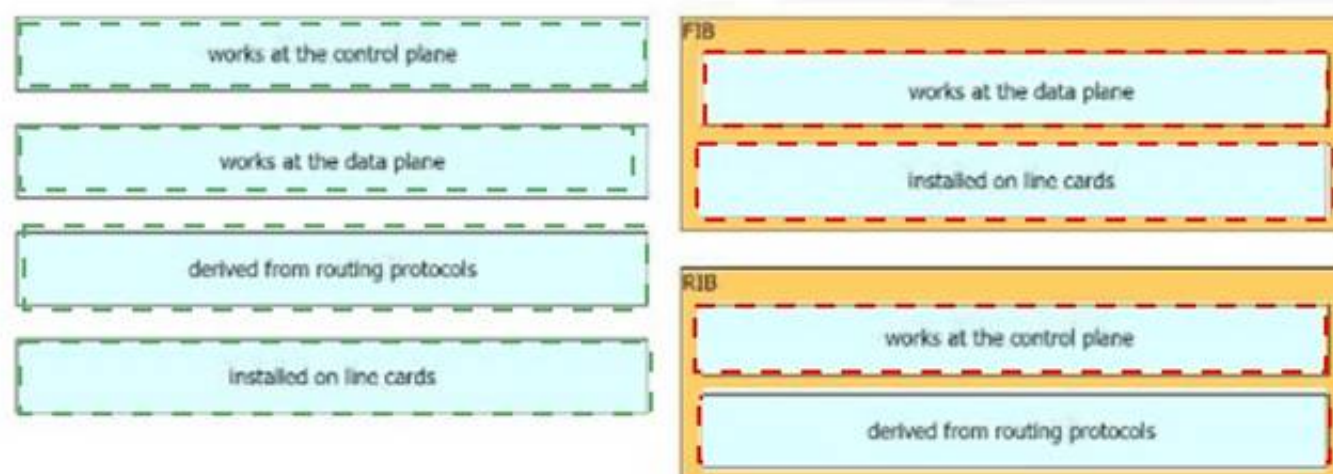
Drag and drop the characteristics from the left onto the architectures on the right.



- A. Mastered
- B. Not Mastered

Answer: A

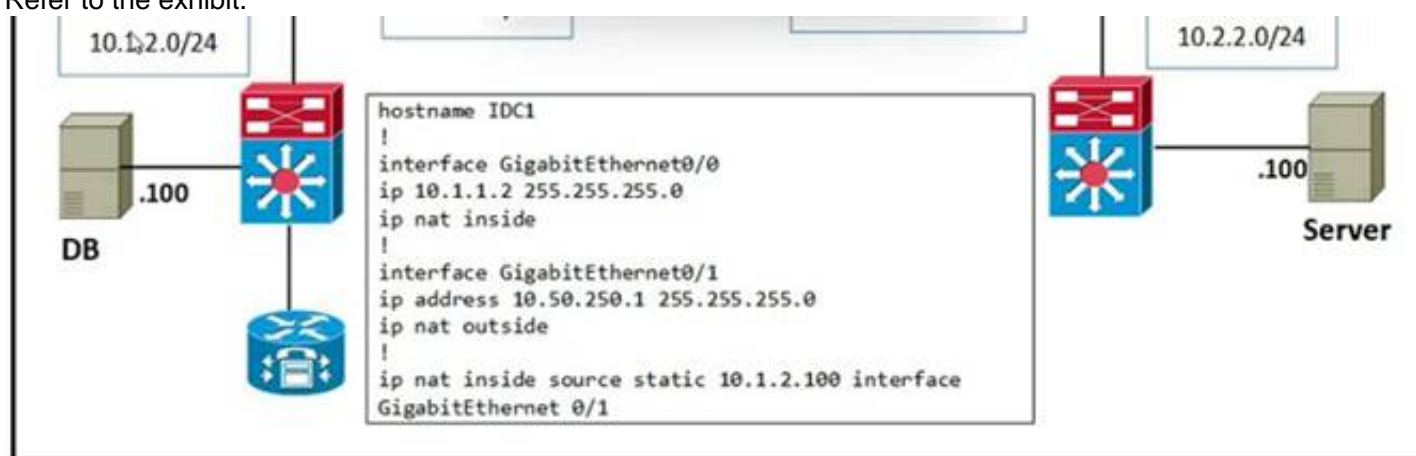
Explanation:



#### NEW QUESTION 553

- (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 555

- (Topic 2)

What occurs when a high bandwidth multicast stream is sent over an MVPN using Cisco hardware?

- A. The traffic uses the default MDT to transmit the data only if it is a (S,G) multicast route entry
- B. A data MDT is created to if it is a (\*, G) multicast route entries
- C. A data and default MDT are created to flood the multicast stream out of all PIM-SM neighbors.
- D. A data MDT is created to allow for the best transmission through the core for (S, G) multicast route entries.

Answer: D



#### NEW QUESTION 557

- (Topic 2)

Which new enhancement was implemented in Wi-Fi 6?

- A. Wi-Fi Protected Access 3
- B. 4096 Quadrature Amplitude Modulation Mode
- C. Channel bonding
- D. Uplink and Downlink Orthogonal Frequency Division Multiple Access

**Answer: D**

#### NEW QUESTION 560

- (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)

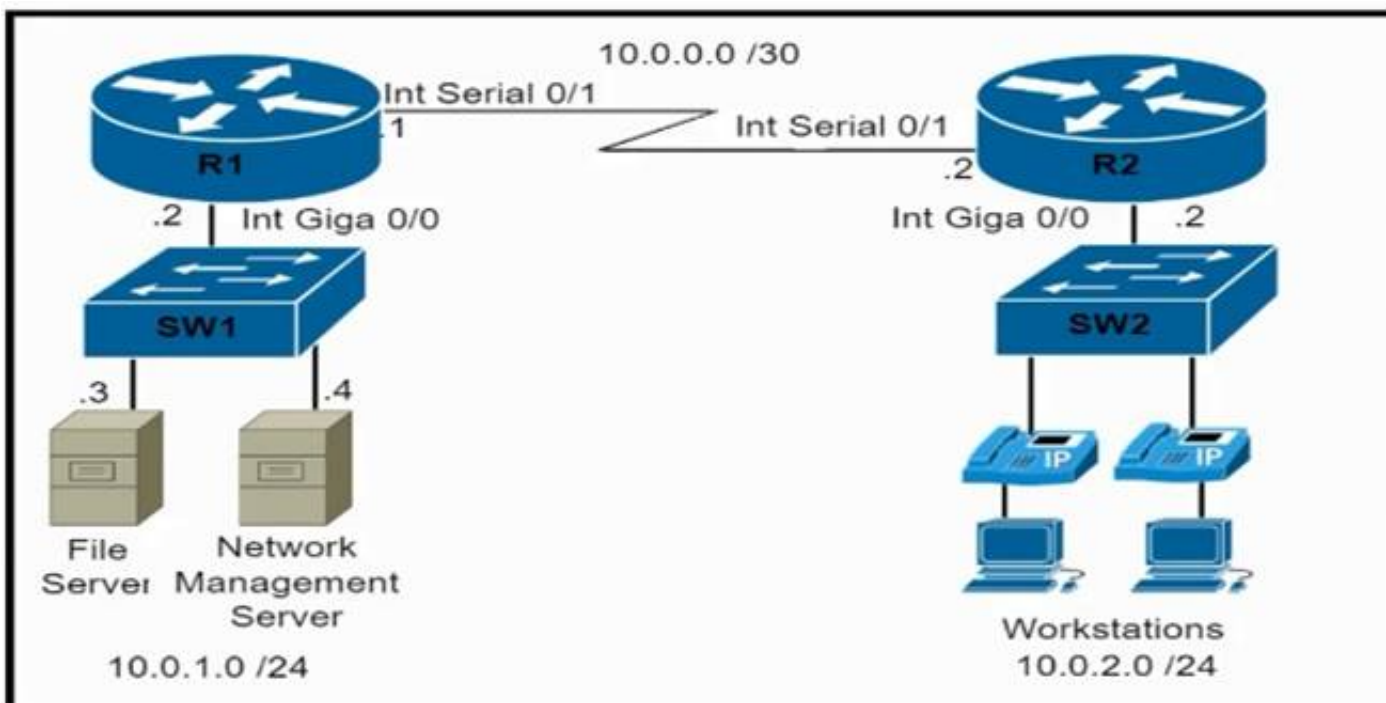
+ Point-to-Point and Point-to-Multipoint (adjust hello/dead timers)

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 562

- (Topic 2)

Refer to the exhibit.



An engineer must configure and validate a CoPP policy that allows the network management server to monitor router R1 via SNMP while protecting the control plane. Which two commands or command sets must be used? (Choose two.)

- ☒ **show policy-map control-plane**
- ☐ **show quality-of-service-profile**
- ☐ **access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp**
- class-map match-all CoPP-management**  
**match access-group 150**
- policy-map CoPP-policy**  
**class CoPP-management**  
**police 8000 conform-action transmit exceed-action transmit**  
**violate-action transmit**
- control-plane**  
**Service-policy input CoPP-policy**
- ☐ **show ip interface brief**

```

❑ show ip interface brief

❑ access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp
access-list 150 permit udp 10.0.1.4 0.0.0.0 eq snmp host 10.0.1.2

class-map match-all CoPP-management
match access-group 150

policy-map CoPP-policy
class CoPP-management
  police 8000 conform-action transmit exceed-action transmit
  violate-action drop

control-plane
  Service-policy input CoPP-policy
  
```

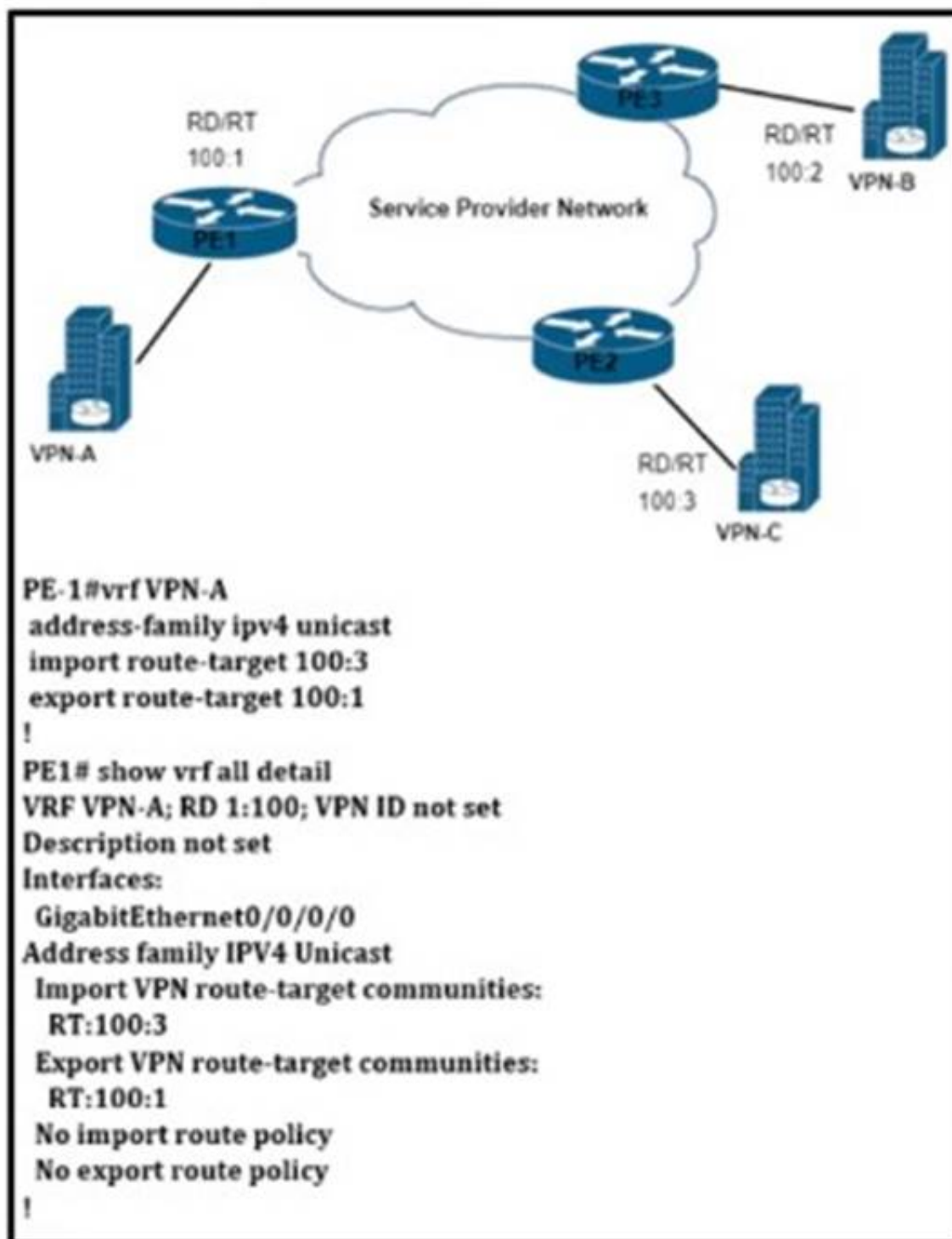
- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E
- F. Option F

**Answer:** AF

#### NEW QUESTION 563

- (Topic 2)

Refer to the exhibit.



VPN-A sends point-to-point traffic to VPN-B and receives traffic only from VPN-C VPN-B sends point-to-point traffic to VPN-C and receives traffic only from VPN-A  
 Which configuration is applied?

A)

PE-2  
vrf VPN-B  
address-family ipv4 unicast  
import route-target 100:1  
export route-target 100:2

B)

PE-3  
vrf VPN-B  
address-family ipv4 unicast  
import route-target 100:1  
export route-target 100:2

C)

PE-2  
vrf VPN-B  
address-family ipv4 unicast  
import route-target 100:1  
export route-target 100:2

D)

PE-3  
vrf VPN-B  
address-family ipv4 unicas  
import route-target 100:2  
export route-target 100:2

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

Answer: B

NEW QUESTION 568

DRAG DROP - (Topic 2)

An engineer is working with the Cisco DNA Center API Drag and drop the methods from the left onto the actions that they are used for on the right.

GET	remove an element using the API
POST	update an element
DELETE	extract information from the API
PUT	create an element

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



GET	DELETE
POST	PUT
DELETE	GET
PUT	POST

#### NEW QUESTION 569

- (Topic 2)

```
RP/0/0/CPU0:R2#debug isis adjacencies
RP/0/0/CPU0:Apr 2 20:57:00.421 : isis[1010]: RECV P2P IIH (L2)
from GigabitEthernet0/0/0/0 SNPA fa16.3ebe.a7bc: System ID R2,
Holdtime 30, length 1429
RP/0/0/CPU0:Apr 2 20:57:01.761 : isis[1010]: SEND P2P IIH (L1)
on GigabitEthernet0/0/0/0: Holdtime 30s, Length 41
```

Refer to the exhibit. A network operator is attempting to configure an IS-IS adjacency between two routers, but the adjacency cannot be established. To troubleshoot the problem, the operator collects this debugging output. Which interfaces are misconfigured on these routers?

- A. The peer router interface is configured as Level 1 only, and the R2 interface is configured as Level 2 only
- B. The R2 interface is configured as Level 1 only, and the Peer router interface is configured as Level 2 only
- C. The R2 interface is configured as point-to-point, and the peer router interface is configured as multipoint.
- D. The peer router interface is configured as point-as-point, and the R2 interface is configured as multipoint.

**Answer: C**

#### NEW QUESTION 572

- (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 573

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 350-401 Practice Exam Features:

- \* 350-401 Questions and Answers Updated Frequently
- \* 350-401 Practice Questions Verified by Expert Senior Certified Staff
- \* 350-401 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 350-401 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 350-401 Practice Test Here](#)**