

## Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies

<https://www.2passeasy.com/dumps/350-401/>



### 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)

```
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 trunksport trunk encapsulation dot1q on SW1 and SW2.
- C. Configure channel-group 1 mode active on GI'O and GM of SW1 .
- D. Configure switchport mode dynamic desirable on SW1 and SW2

Answer: C

### NEW QUESTION 3

- (Topic 4)

Which two results occur if Cisco DNA center loses connectivity to devices in the SD- ACCESS fabric? (Choose two)

- A. All devices reload after detecting loss of connection to Cisco DNA Center
- B. Already connected users are unaffected, but new users cannot connect
- C. User connectivity is unaffected
- D. Cisco DNA Center is unable to collect monitoring data in Assurance
- E. Users lose connectivity

Answer: CD

### NEW QUESTION 4

- (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 5

- (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 6

- (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?

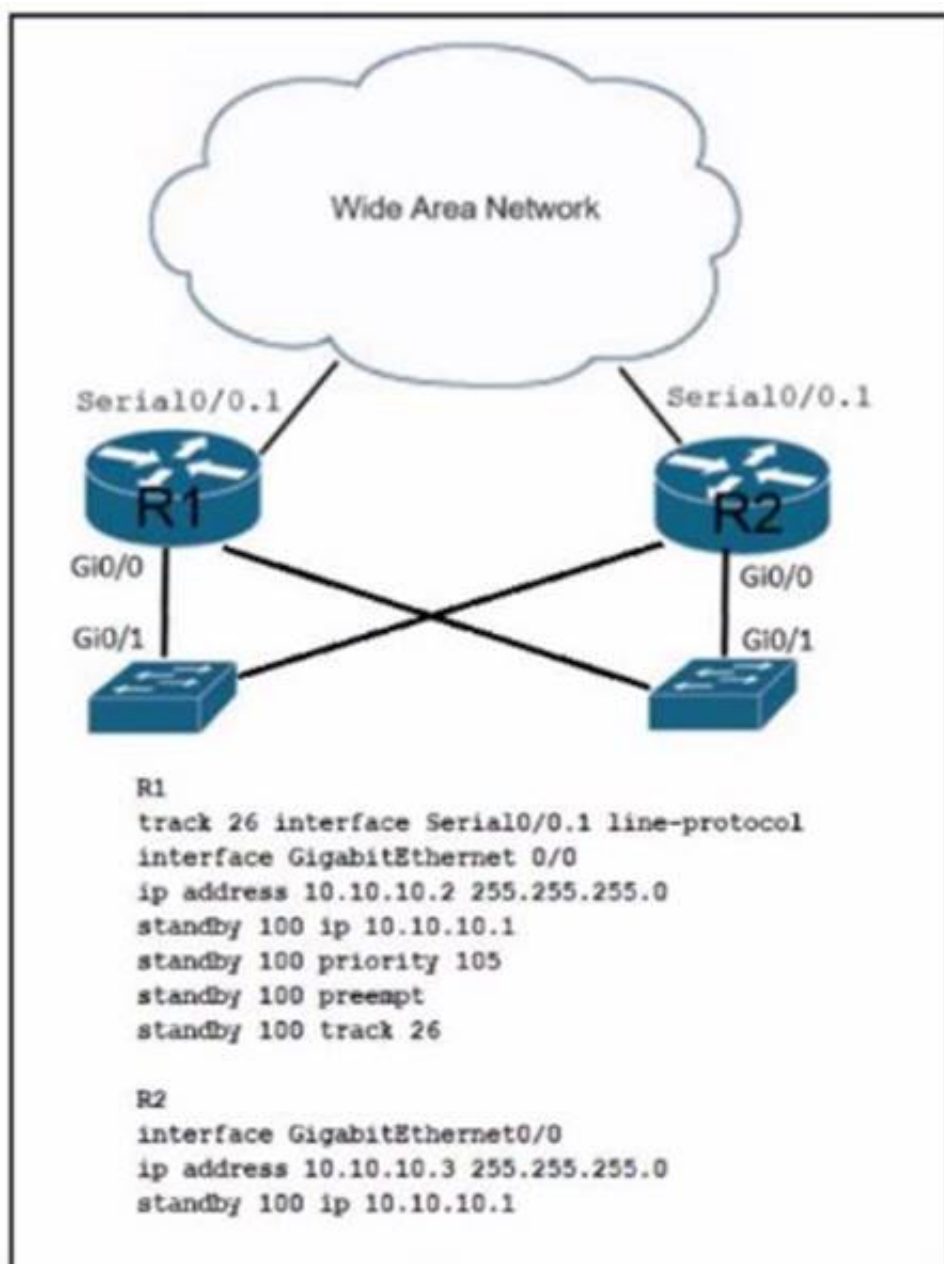
- A. Ethernet over IP
- B. IPsec
- C. Mobility
- D. VPN

**Answer:** A

#### NEW QUESTION 7

- (Topic 4)

Refer to the exhibit.



An engineer must modify the existing configuration so that R2 can take over as the primary router when serial interface 0/0.1 on R1 goes down. Which command must the engineer apply?

- A. R2W standby 100 track 26 decrement 10
- B. R2# standby 100 preempt
- C. R2# track 26 interface SerialWO.1 line-protocol
- D. R2# standby 100 priority 100

Answer: A

#### NEW QUESTION 8

- (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 9

- (Topic 4)

Refer to the exhibit.

Port		13 (FastEthernet1/0/11)		
Hello Time		2 sec	Max Age 20 sec	Forward Delay 15 sec
Bridge ID		32769 (priority 32768 sys-id-ext 1)		
Address		001b.0d8e.e080		
Hello Time		2 sec	Max Age 20 sec	Forward Delay 15 sec
Interface	Role	Sts	Cost	Prio.Nbr Type
FastEthernet1/0/7	Desig	FWD	2	128.9 P2p Bound (PVST)
FastEthernet1/0/10	Desig	FWD	2	128.12 P2p Bound (PVST)
FastEthernet1/0/11	Root	FWD	2	128.13 P2p
FastEthernet1/0/12	Altn	BLK	2	128.14 P2p

DSW1#sh spanning-tree mst				
##### MST1	vlan mapped: 10.20			
Bridge	address	001b.0d8e.e080	priority	32769 (32768 sysid 1)
Root	address	0018.7363.4300	priority	32769 (32768 sysid 1)
	port	FastEthernet1/0/11	cost	2
				ren hops 19
... output omitted				

Which two commands ensure that DSW1 becomes the root bridge for VLAN 10 and 20? (Choose two.)

- A. spanning-tree mst 1 priority 1
- B. spanning-tree mstp vlan 10.20 root primary
- C. spanning-tree mst 1 root primary
- D. spanning-tree mst 1 priority 4096
- E. spanning-tree mst vlan 10.20 priority root

Answer: DE

#### NEW QUESTION 10

- (Topic 4)

Which Python library is used to work with YANG data models via NETCONF?

- A. Postman
- B. requests
- C. ncclient
- D. cURL

Answer: C

#### NEW QUESTION 10

- (Topic 4)

In a Cisco StackWise Virtual environment, which planes are virtually combined in the common logical switch?

- A. control, and forwarding
- B. management and data
- C. control and management
- D. control and data

Answer: C

#### NEW QUESTION 14

- (Topic 4)

Which solution should be used in a high-density wireless environment to increase bandwidth for each user?

- A. Increase antenna size



- B. Increase the mandatory minimum data rate.
- C. Increase the cell size of each AP.
- D. Increase TX power.

**Answer:** B

#### NEW QUESTION 18

- (Topic 4)

How does SSO work with HSRP to minimize network disruptions?

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

**Answer:** D

#### NEW QUESTION 21

- (Topic 4)

When using BFD in a network design, which consideration must be made?

- A. BFD is used with first hop routing protocols to provide subsecond convergence.
- B. BFD is more CPU-intensive than using reduced hold timers with routing protocols.
- C. BFD is used with dynamic routing protocols to provide subsecond convergence.
- D. BFD is used with NSF and graceful to provide subsecond convergence.

**Answer:** C

#### NEW QUESTION 23

- (Topic 1)

What is the function of a VTEP in VXLAN?

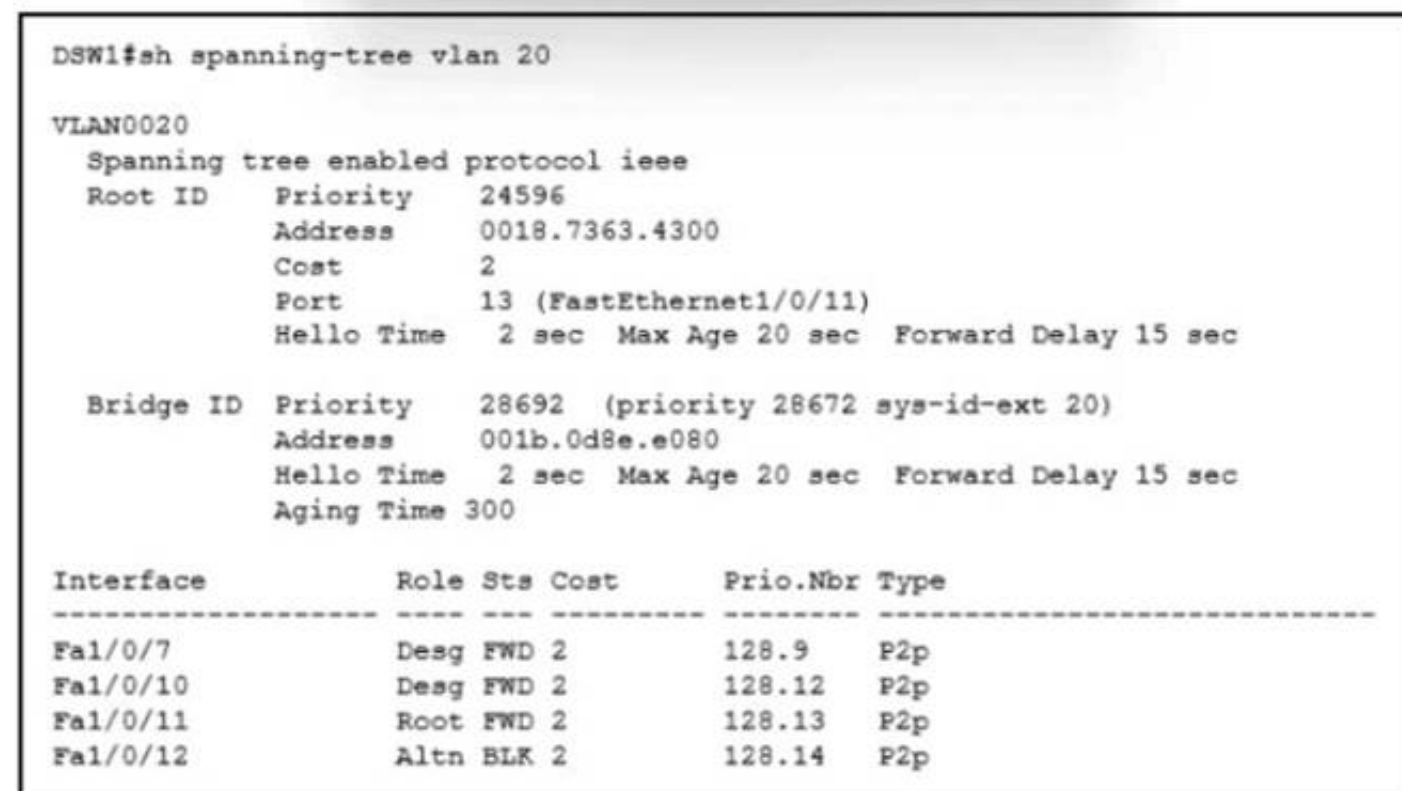
- A. provide the routing underlay and overlay for VXLAN headers
- B. dynamically discover the location of end hosts in a VXLAN fabric
- C. encapsulate and de-encapsulate traffic into and out of the VXLAN fabric
- D. statically point to end host locations of the VXLAN fabric

**Answer:** C

#### NEW QUESTION 28

- (Topic 2)

Refer to the exhibit.



```
DSW1#sh spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol ieee
    Root ID    Priority    24596
              Address    0018.7363.4300
              Cost        2
              Port        13 (FastEthernet1/0/11)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID   Priority    28692 (priority 28672 sys-id-ext 20)
              Address    001b.0d8e.e080
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300

Interface                Role Sts Cost      Prio.Nbr Type
-----
Fa1/0/7                   Desg FWD 2        128.9    P2p
Fa1/0/10                   Desg FWD 2        128.12   P2p
Fa1/0/11                   Root FWD 2        128.13   P2p
Fa1/0/12                   Altn BLK 2        128.14   P2p
```

What does the output confirm about the switch's spanning tree configuration?

- A. The spanning-tree mode stp ieee command was entered on this switch
- B. The spanning-tree operation mode for this switch is IEEE.
- C. The spanning-tree operation mode for this switch is PVST+.
- D. The spanning-tree operation mode for this switch is PVST

**Answer:** C

#### NEW QUESTION 29

- (Topic 2)

What is a characteristic of Cisco StackWise technology?

- A. It uses proprietary cabling
- B. It supports devices that are geographically separated
- C. It combines exactly two devices
- D. It is supported on the Cisco 4500 series.

**Answer:** C

### NEW QUESTION 30

- (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 33

- (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 35

- (Topic 2)

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

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

**Answer:** AB

#### Explanation:

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

### NEW QUESTION 38

- (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 39**

- (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 (= 2<sup>24</sup>) VXLAN segments to coexist within the same infrastructure. This surely solves the small number of traditional VLANs.

**NEW QUESTION 42**

- (Topic 2)

In a Cisco SD-WAN solution, how is the health of a data plane tunnel monitored?

- A. with IP SLA
- B. ARP probing
- C. using BFD
- D. with OMP

**Answer:** C

**NEW QUESTION 44**

- (Topic 2)

What is required for a virtual machine to run?

- A. a Type 1 hypervisor and a host operating system
- B. a hypervisor and physical server hardware
- C. only a Type 1 hypervisor
- D. only a Type 2 hypervisor

**Answer:** B

**NEW QUESTION 49**

- (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

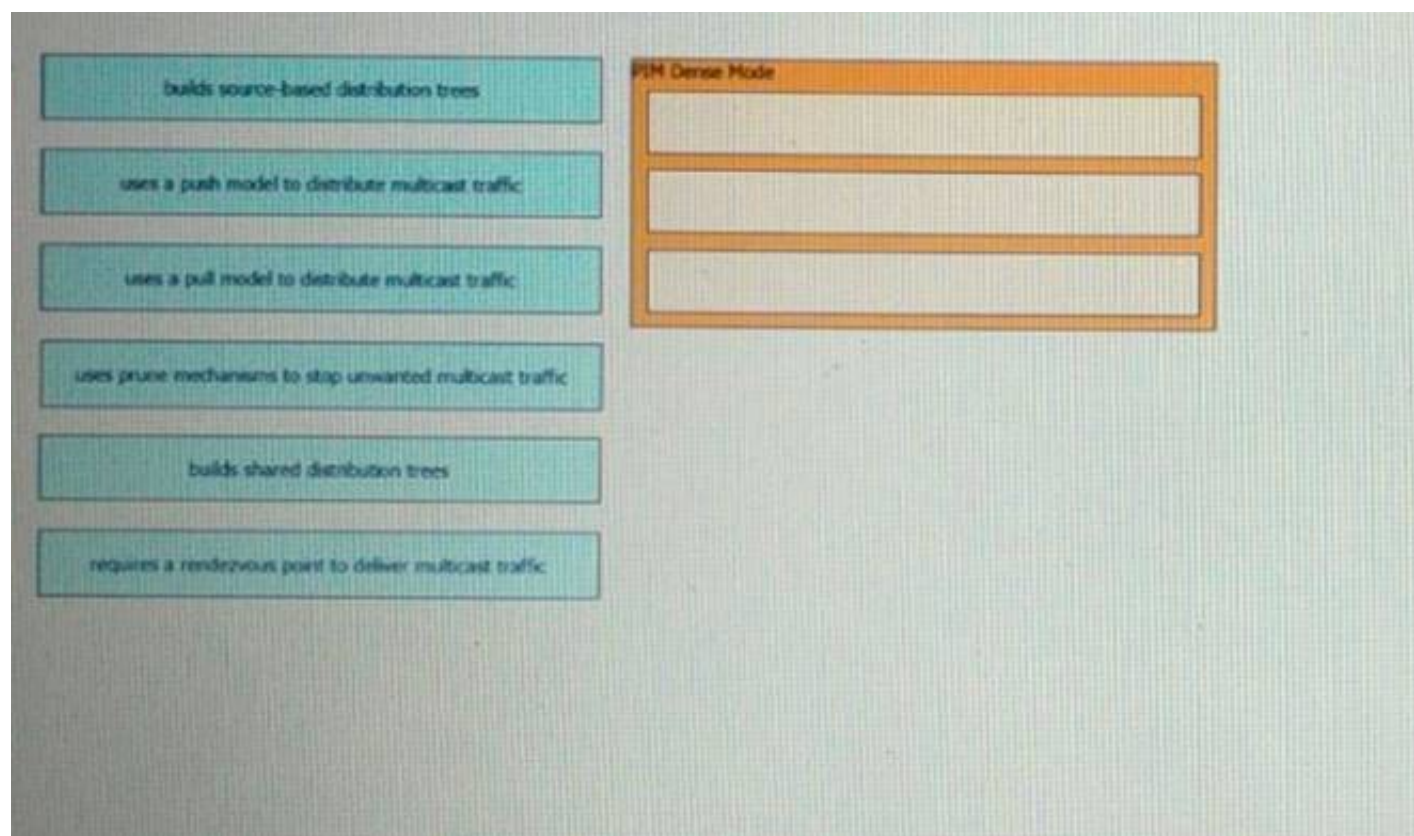
**Explanation:**

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 53**

DRAG DROP - (Topic 2)

Drag and drop characteristics of PIM dense mode from the left to the right.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

PIM-DM supports only source trees – that is, (S,G) entries—and cannot be used to build a shared distribution tree.

**NEW QUESTION 56**

- (Topic 2)

Refer to the exhibit:

```
R1#show running-config interface fa0/0
Building configuration...

Current configuration: 192 bytes
!
interface FastEthernet0/0
 ip address 192.68.3.5 255.255.255.0
 duplex full
 vrrp 1 ip 192.168.3.1
 vrrp 1 priority 110
 vrrp 1 authentication text cisco
 vrrp 1 track 20 decrement 20
end

R1#show running-config | include track 20
track 20 ip route 10.10.1.1 255.255.255.255 reachability
```

```
R2#show running-config interface fa0/0
Building configuration...

Current configuration: 141 bytes
!
interface FastEthernet0/0
 ip address 192.68.3.2 255.255.255.0
 duplex full
 vrrp 1 ip 192.168.3.1
 vrrp 1 authentication text cisco
end
```

An engineer configures VRRP and issues the show commands to verify operation. What does the engineer confirm about VRRP group 1 from the output?

- A. There is no route to 10.10.1.1/32 in R2's routing table



- B. If R1 reboots, R2 becomes the master virtual router until R2 reboots
- C. Communication between VRRP members is encrypted using MD5
- D. R1 is primary if 10.10.1.1/32 is in its routing table

**Answer:** D

#### NEW QUESTION 58

- (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 62

- (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

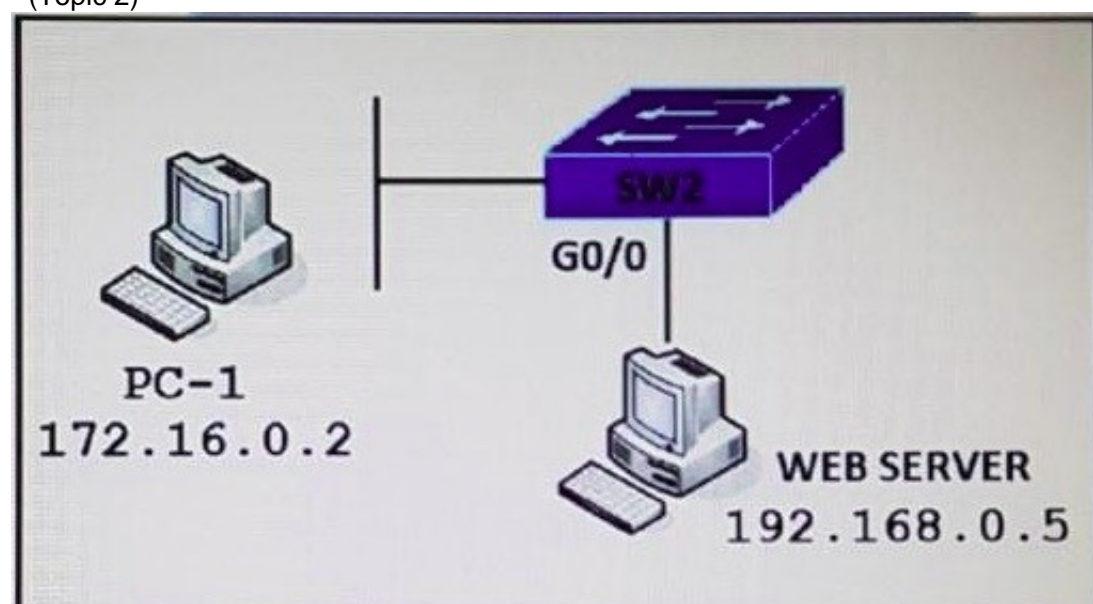
**Answer:** A

#### 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 64

- (Topic 2)



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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 66

- (Topic 2)

Which two actions, when applied in the LAN network segment, will facilitate Layer 3 CAPWAP discovery for lightweight AP? (Choose two.)

- A. Utilize DHCP option 17.
- B. Configure WLC IP address on LAN switch.
- C. Utilize DHCP option 43.
- D. Configure an ip helper-address on the router interface
- E. Enable port security on the switch port

**Answer:** CE

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html>

#### NEW QUESTION 67

- (Topic 2)

Which protocol is used to encrypt control plane traffic between SD-WAN controllers and SD-WAN endpoints?

- A. DTLS
- B. IPsec
- C. PGP
- D. HTTPS

**Answer:** A

#### Explanation:

DTLS protocol is used to encrypt control plane traffic between vSmart (controllers) and other SD-WAN endpoints.

#### NEW QUESTION 72

- (Topic 2)

Refer to the exhibit.

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

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

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

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

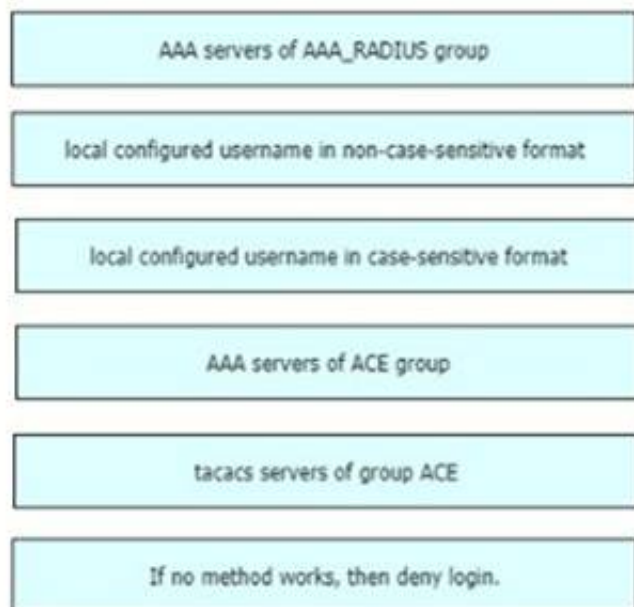
**Answer:** D

#### NEW QUESTION 76

DRAG DROP - (Topic 2)

An engineer creates the configuration below. Drag and drop the authentication methods from the left into the order of priority on the right. Not all options are used.

```
R1#sh run | i aaa
aaa new-model
aaa authentication login default group ACE group AAA_RADIUS local-case
aaa session-id common
R1#
```



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

priority 1: AAA servers of ACE group

priority 2: AAA servers of AAA\_RADIUS group

priority 3: local configured username in case-sensitive format priority 4: If no method works, then deny login

**NEW QUESTION 79**

- (Topic 2)

Which two parameters are examples of a QoS traffic descriptor? (Choose two)

- A. MPLS EXP bits
- B. bandwidth
- C. DSCP
- D. ToS
- E. packet size

**Answer:** AC

**NEW QUESTION 81**

- (Topic 2)

A network monitoring system uses SNMP polling to record the statistics of router interfaces The SNMP queries work as expected until an engineer installs a new interface and reloads the router After this action, all SNMP queries for the router fail What is the cause of this issue?

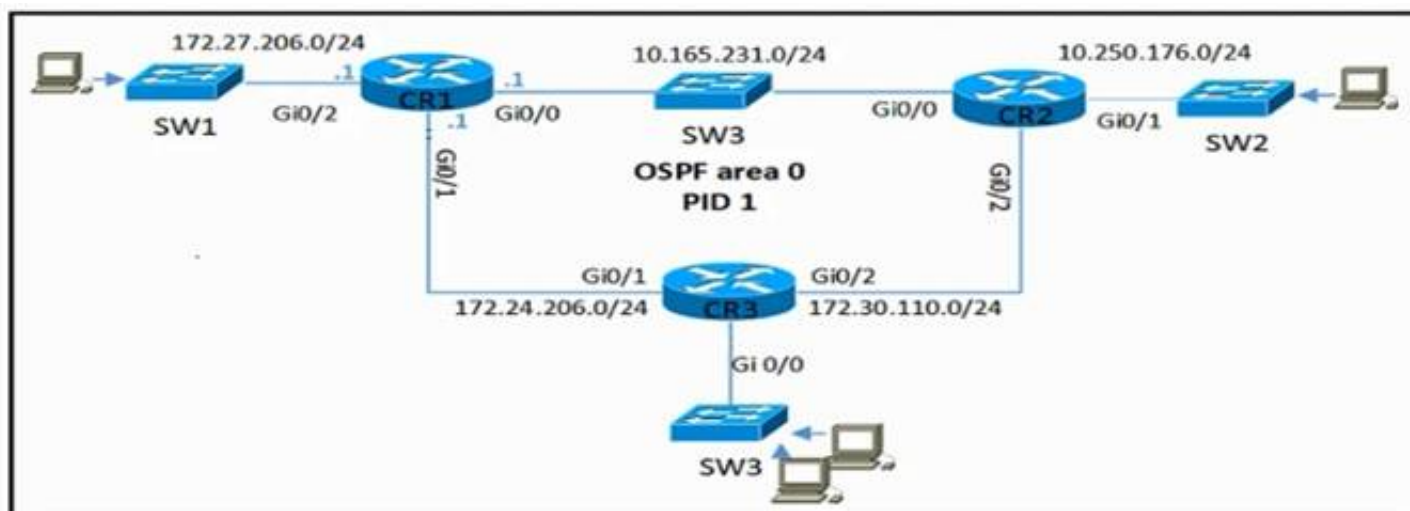
- A. The SNMP community is configured incorrectly
- B. The SNMP interface index changed after reboot.
- C. The SNMP server traps are disabled for the interface index
- D. The SNMP server traps are disabled for the link state.

**Answer:** B

**NEW QUESTION 85**

- (Topic 2)

Refer to the exhibit.



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

A)



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

B)

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

C)

```
interface Gi0/2
ip ospf 1 area 0

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

D)

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

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

**Answer: D****NEW QUESTION 89**

- (Topic 2)

```
Device# configure terminal
Device(config)# netconf ssh acl 1
Device(config)# netconf lock-time 100
Device(config)# netconf max-sessions 1
Device(config)# netconf max-message 10
```

Refer to the exhibit. A network engineer must configure NETCONF. After creating the configuration, the engineer gets output from the command show line, but not from show running-config. Which command completes the configuration?

- ☐ Device(config)# netconf lock-time 500
- ☐ Device(config)# netconf max-message 1000
- ☐ Device(config)# no netconf ssh acl 1
- ☐ Device(config)# netconf max-sessions 100

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

**Answer: C**



#### NEW QUESTION 90

- (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 92

- (Topic 2)

Refer to the exhibit.



Which command set must be added to the configuration to analyze 50 packets out of every 100?

A)

```
interface GigabitEthernet 0/0/0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

B)

```
sampler SAMPLER-1
 no mode random 1-out-of 2
 mode percent 50
```

```
interface GigabitEthernet 0/0/0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

C)

```
flow monitor FLOW-MONITOR-1
 record v4_r1
 sampler SAMPLER-1

interface GigabitEthernet 0/0/0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

D)

```
sampler SAMPLER-1
 mode random 1-out-of 2
 flow FLOW-MONITOR-1

interface GigabitEthernet 0/0/0
 ip flow monitor SAMPLER-1 input
```

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

**Answer:** A

#### NEW QUESTION 96

- (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 100

- (Topic 1)

Which technology provides a secure communication channel for all traffic at Layer 2 of the OSI model?

- A. MACsec
- B. IPsec
- C. SSL
- D. Cisco Trustsec

**Answer:** A

#### Explanation:

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-ofband methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the

#### NEW QUESTION 102

- (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 107

- (Topic 1)

Which two mechanisms are available to secure NTP? (Choose two.)

- A. IP prefix list-based
- B. IPsec
- C. TACACS-based authentication
- D. IP access list-based
- E. Encrypted authentication

**Answer:** DE

#### NEW QUESTION 109

- (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 112

- (Topic 1)

An engineer runs the code against an API of Cisco DNA 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 114

- (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 117

- (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 121

- (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 124

- (Topic 1)

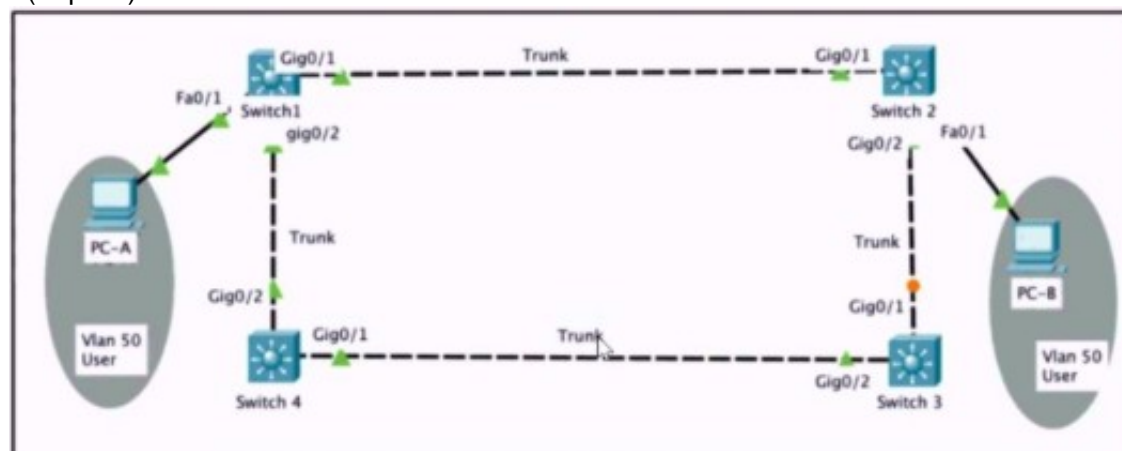
After a redundant route processor failure occurs on a Layer 3 device, which mechanism allows for packets to be forwarded from a neighboring router based on the most recent tables?

- A. BFD
- B. RPVST+
- C. RP failover
- D. NSF

Answer: D

#### NEW QUESTION 125

- (Topic 1)



Refer to the exhibit. Rapid PVST+ is enabled on all switches. Which command set must be configured on switch1 to achieve the following results on port fa0/1?

- When a device is connected, the port transitions immediately to a forwarding state.
- The interface should not send or receive BPDUs.
- If a BPDU is received, it continues operating normally.

A)

```
Switch1(config)# interface f0/1
Switch1(config-if)# spanning-tree portfast
```

B)

```
Switch1(config)# spanning-tree portfast bpduguard default
Switch1(config)# interface f0/1
Switch1(config-if)# spanning-tree portfast
```

C)

```
Switch1(config)# spanning-tree portfast bpduguard default
Switch1(config)# interface f0/1
Switch1(config-if)# spanning-tree portfast
```

D)

```
Switch1(config)# interface f0/1
Switch1(config-if)# spanning-tree portfast
Switch1(config-if)# spanning-tree bpduguard enable
```

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

Answer: D

#### NEW QUESTION 128

- (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 133

- (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 135

- (Topic 1)

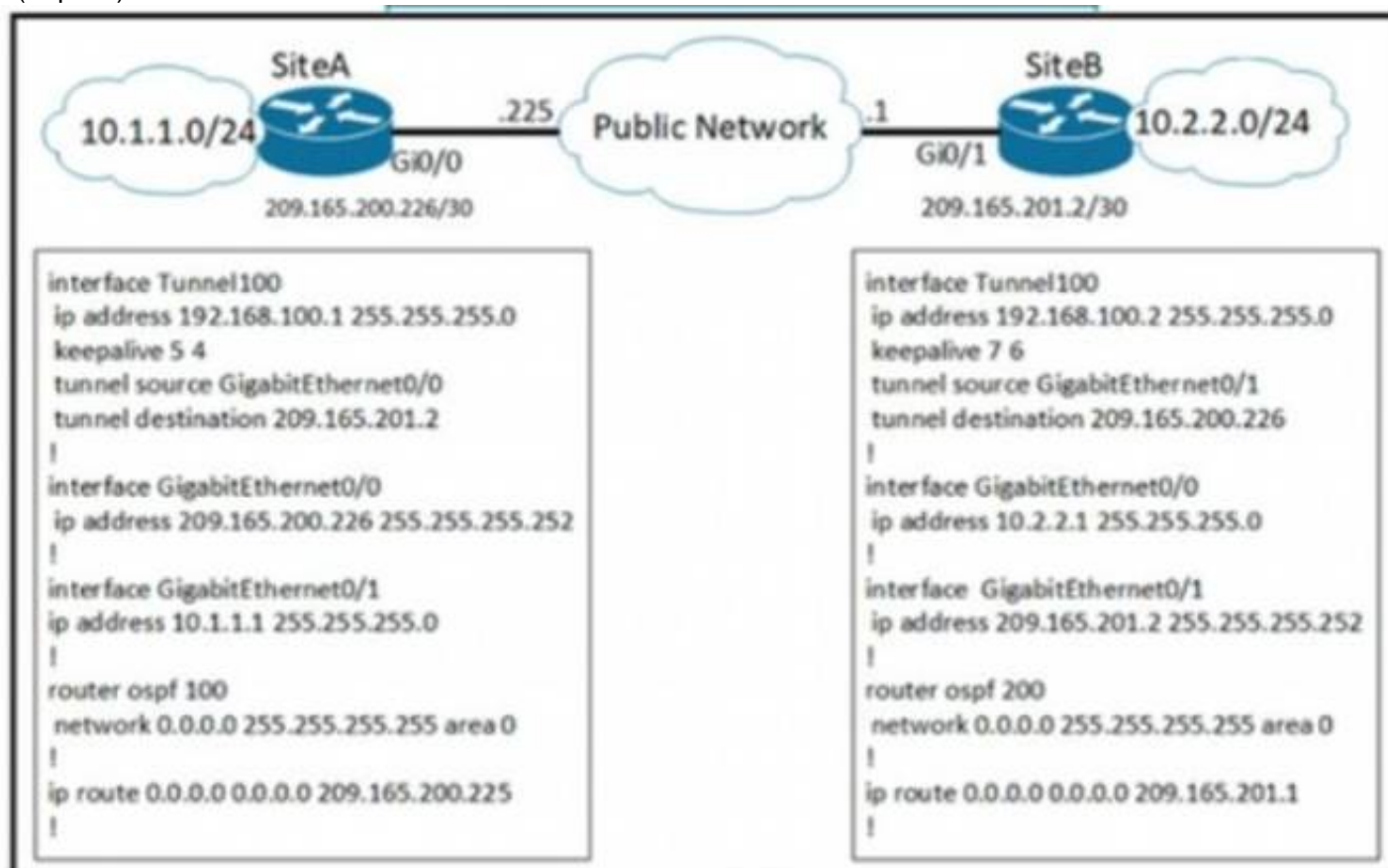
How are the different versions of IGMP compatible?

- A. IGMPv2 is compatible only with IGMPv1.
- B. IGMPv2 is compatible only with IGMPv2.
- C. IGMPv3 is compatible only with IGMPv3.
- D. IGMPv3 is compatible only with IGMPv1

Answer: A

### NEW QUESTION 139

- (Topic 1)



A network engineer configures a new GRE tunnel and enters the show run command. What does the output verify?

- A. The tunnel will be established and work as expected
- B. The tunnel destination will be known via the tunnel interface
- C. The tunnel keepalive is configured incorrectly because they must match on both sites
- D. The default MTU of the tunnel interface is 1500 byte.

Answer: B

NEW QUESTION 142

- (Topic 1)

```
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.2 on FastEthernet0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
%OSPF-6-AREACHG: 10.0.0.1/32 changed from area 0 to area 1
%OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from
backbone area must be virtual-link but not found from 10.0.0.2,
FastEthernet0/0
```

Refer to me exhibit. What is the cause of the log messages?

- A. hello packet mismatch
- B. OSPF area change
- C. MTU mismatch
- D. IP address mismatch

Answer: B

NEW QUESTION 147

- (Topic 1)

A network engineer is configuring Flexible Netflow and enters these commands  
Sampler Netflow1  
Mode random one-out-of 100 Interface fastethernet 1/0 Flow-sampler netflow1  
Which are two results of implementing this feature instead of traditional Netflow? (Choose two.)

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

Answer: AD

NEW QUESTION 150

DRAG DROP - (Topic 1)

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

customizable hardware, purpose-built systems

easy to scale and upgrade

more suitable for companies with specific regulatory or security requirements

resources can be over or underutilized as requirements vary

requires a strong and stable internet connection

built-in, automated data backups and recovery

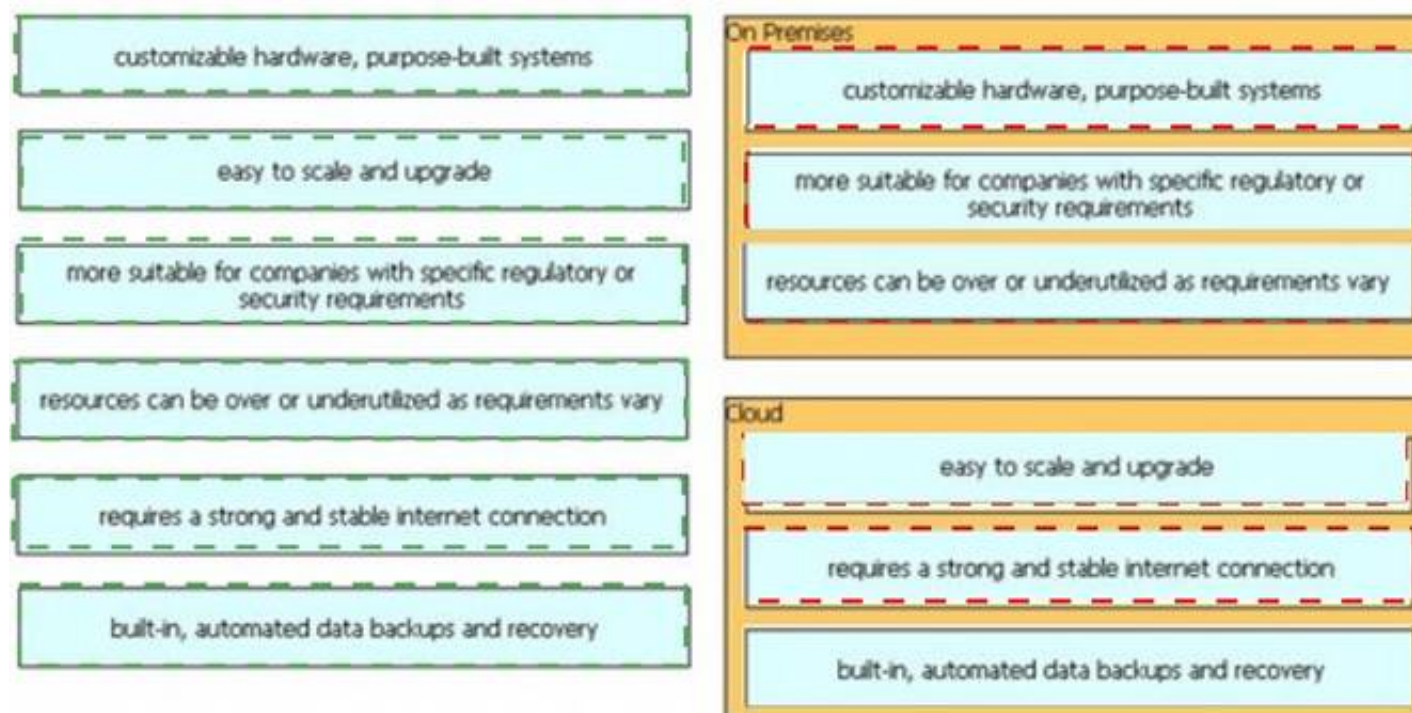
On Premises

Cloud

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



#### NEW QUESTION 152

- (Topic 1)

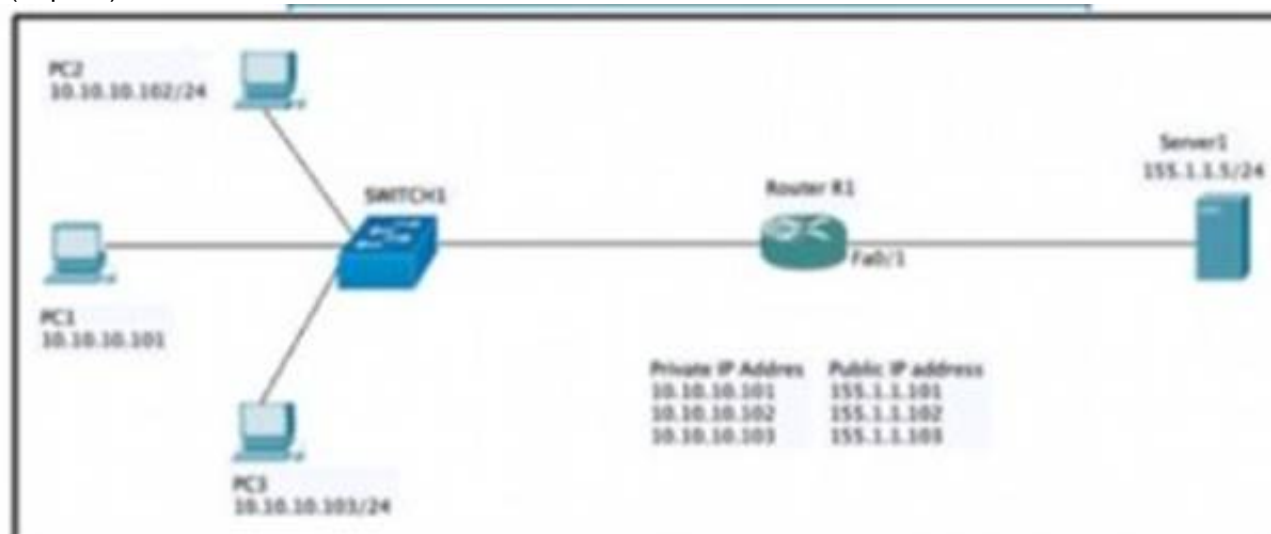
An engineer must provide wireless converge in a square office. The engineer has only one AP and believes that it should be placed it in the middle of the room. Which antenna type should the engineer use?

- A. directional
- B. polarized
- C. Yagi
- D. omnidirectional

Answer: D

#### NEW QUESTION 153

- (Topic 1)



Refer to the exhibit. Which set of commands on router r R1 Allow deterministic translation of private hosts PC1, PC2, and PC3 to addresses in the public space?

A)

```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102
RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103
```

B)



```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102
RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103
```

C)

```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255
RouterR1(config)#ip nat pool POOL 155.1.1.101 155.1.1.103 netmask 255.255.255.0
RouterR1(config)#ip nat inside source list 1 pool POOL
```

D)

```
RouterR1(config)#int f0/0
RouterR1(config-if)#ip nat inside
RouterR1(config-if)#exit
RouterR1(config)#int f0/1
RouterR1(config-if)#ip nat outside
RouterR1(config-if)#exit
RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255
RouterR1(config)#ip nat inside source list 1 interface f0/1 overload
```

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

**Answer:** A

#### NEW QUESTION 156

- (Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 157

- (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 159

- (Topic 1)

Refer to the exhibit.

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

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

- A. event manager applet EEM\_IP\_SLA event track 10 state down
- B. event manager applet EEM\_IP\_SLA event track 10 state unreachable
- C. event manager applet EEM\_IP\_SLA event sla 10 state unreachable
- D. event manager applet EEM\_IP\_SLA event sla 10 state down

**Answer:** A

#### Explanation:

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

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

#### NEW QUESTION 161

DRAG DROP - (Topic 1)

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

DHCP request	Step 1
DHCP offer	Step 2
DHCP discover	Step 3
DHCP ack	Step 4

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

There are four messages sent between the DHCP Client and DHCP Server: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACKNOWLEDGEMENT.

This process is often abbreviated as DORA (for Discover, Offer, Request, Acknowledgement).

#### NEW QUESTION 165

- (Topic 1)

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

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

- D. The FIB is derived from the control plane, and the RIB is derived from the FIB.
- E. The RIB is derived from the control plane, and the FIB is derived from the RIB.

**Answer:** BE

#### NEW QUESTION 166

- (Topic 1)

In a Cisco SD-Access solution, what is the role of the Identity Services Engine?

- A. It is leveraged for dynamic endpoint to group mapping and policy definition.
- B. It provides GUI management and abstraction via apps that share context.
- C. it is used to analyze endpoint to app flows and monitor fabric status.
- D. It manages the LISP EID database.

**Answer:** A

#### NEW QUESTION 169

- (Topic 1)

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

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

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

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

**Answer:** A

#### NEW QUESTION 170

- (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 175

- (Topic 1)

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

A)

```
standby 300 priority 110
standby 300 timers 1 110
```

B)

```
standby version 2
standby 300 priority 110
standby 300 preempt
```

C)

```
standby 300 priority 90
standby 300 preempt
```

D)

```
standby version 2
standby 300 priority 90
standby 300 preempt
```

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

Answer: B

#### NEW QUESTION 180

- (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 183

- (Topic 1)

Under which network conditions is an outbound QoS policy that is applied on a router WAN interface most beneficial?

- A. under interface saturation condition
- B. under network convergence condition
- C. under all network condition
- D. under traffic classification and marking conditions.

Answer: A

#### NEW QUESTION 185

- (Topic 1)

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

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

Answer: B

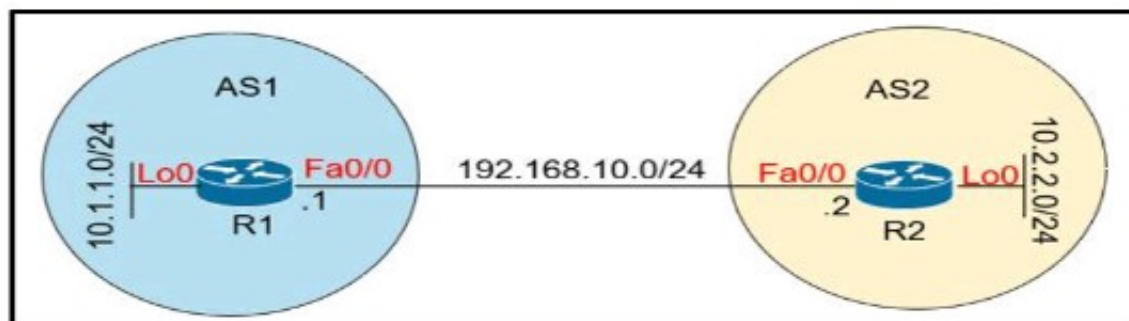
#### Explanation:

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

#### NEW QUESTION 189

- (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.

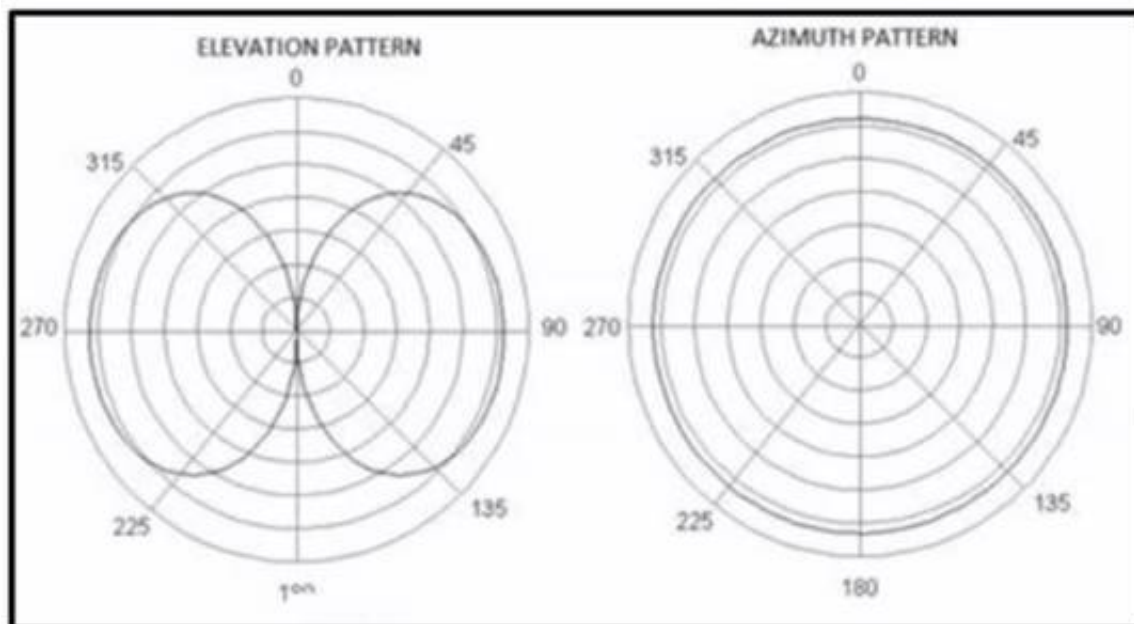
+ Bridge mode: bridge together the WLAN and the wired infrastructure together.

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 191

- (Topic 4)

Refer to the exhibit.



Which antenna emits this radiation pattern?

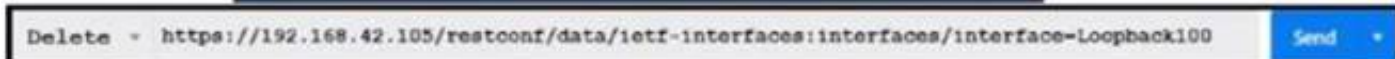
- A. omnidirectional
- B. Yagi
- C. RP-TNC
- D. dish

**Answer:** A

#### NEW QUESTION 194

- (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 198

- (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 199

- (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 204

- (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 206

- (Topic 4)

What is stateful switchover?

- A. mechanism used to prevent routing protocol loops during an RP switchover
- B. mechanism to take control from a failed RP while maintaining connectivity
- C. First Hop Redundancy Protocol for host gateway connectivity
- D. cluster protocol used to facilitate switch failover

**Answer:** D

#### NEW QUESTION 208

- (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 211

- (Topic 4)

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

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

**Answer:** B



#### NEW QUESTION 215

- (Topic 4)

Which of the following protocols has a default administrative distance value of 90?

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

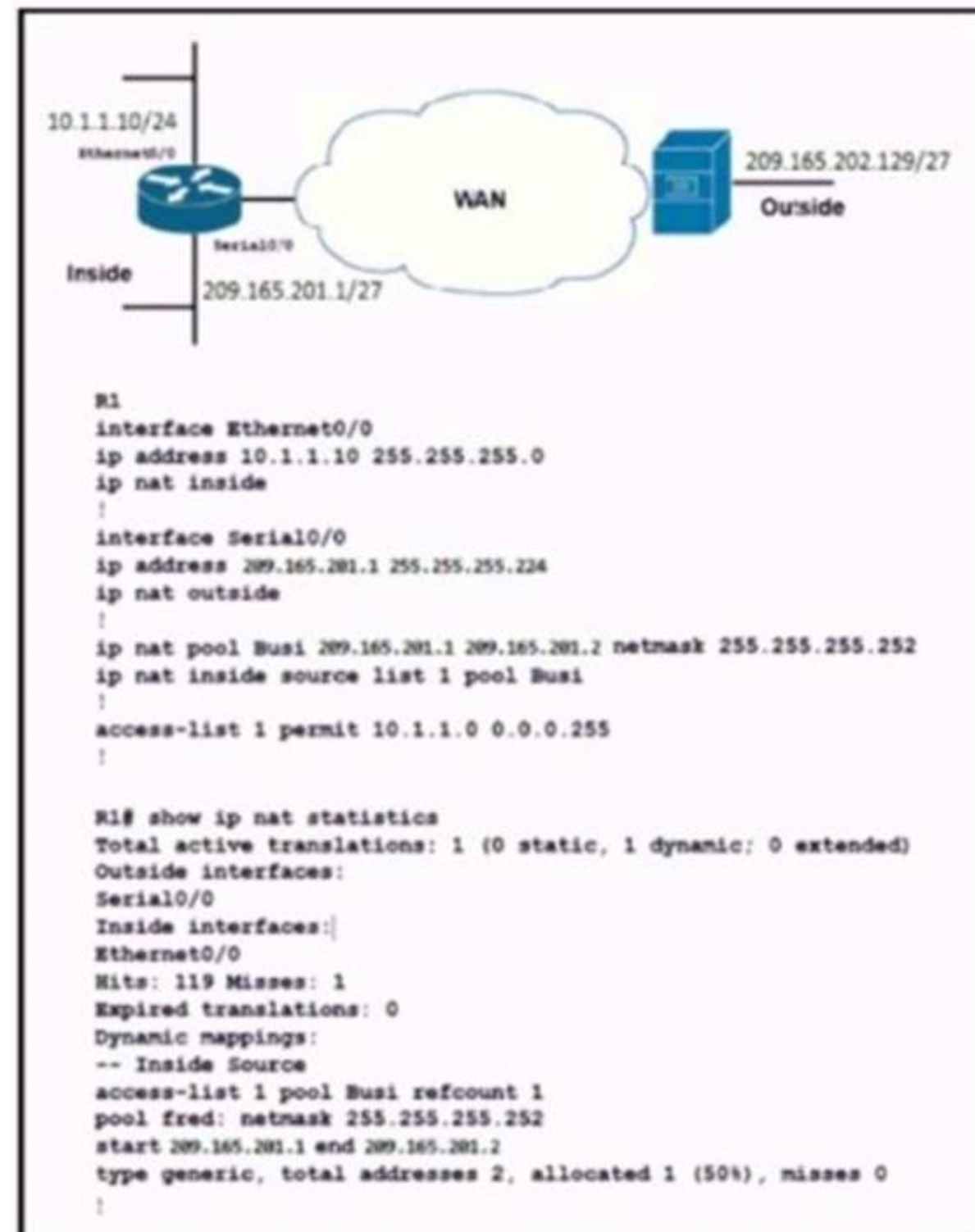
**Answer: B**

#### 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 220

- (Topic 4)



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

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

**Answer: A**

#### NEW QUESTION 221

- (Topic 4)

Which Cisco WLC feature allows a wireless device to perform a Layer 3 roam between two separate controllers without changing the client IP address?

- A. mobile IP
- B. mobility tunnel
- C. LWAPP tunnel
- D. GRE tunnel

**Answer: B**



NEW QUESTION 222

- (Topic 4)

```
<?xml version="1.0"?>
<nc:rpc message-id="101" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <nc:get>
    <nc:filter type="subtree">
      <native xmlns="http://cisco.com/ns/yang/net/ios">
        <interface>
          <GigabitEthernet>
            <name>1</name>
            <ip></ip>
          </GigabitEthernet>
        </interface>
      </native>
    </nc:filter>
  </nc:get>
</nc:rpc>
]]>]]>
```

Refer to the exhibit. The NETCONF object is sent to a Cisco IOS XE switch. What is the purpose of the object?

- A. view the configuration of all GigabitEthernet interfaces.
- B. Discover the IP address of interface GigabitEthernet.
- C. Set the description of interface GigabitEthernet1 to \*1\*.
- D. Remove the IP address from interface GigabitEthernet1.

Answer: A

NEW QUESTION 224

- (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 226

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 231

- (Topic 4)

Why does the vBond orchestrator have a public IP?

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

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

Answer: C

#### NEW QUESTION 233

- (Topic 4)

Refer to the exhibit.

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

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

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

Answer: C

#### Explanation:

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

#### NEW QUESTION 238

- (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 241

- (Topic 4)

Which two methods are used to interconnect two Cisco SD-Access Fabric sites? (Choose two.)

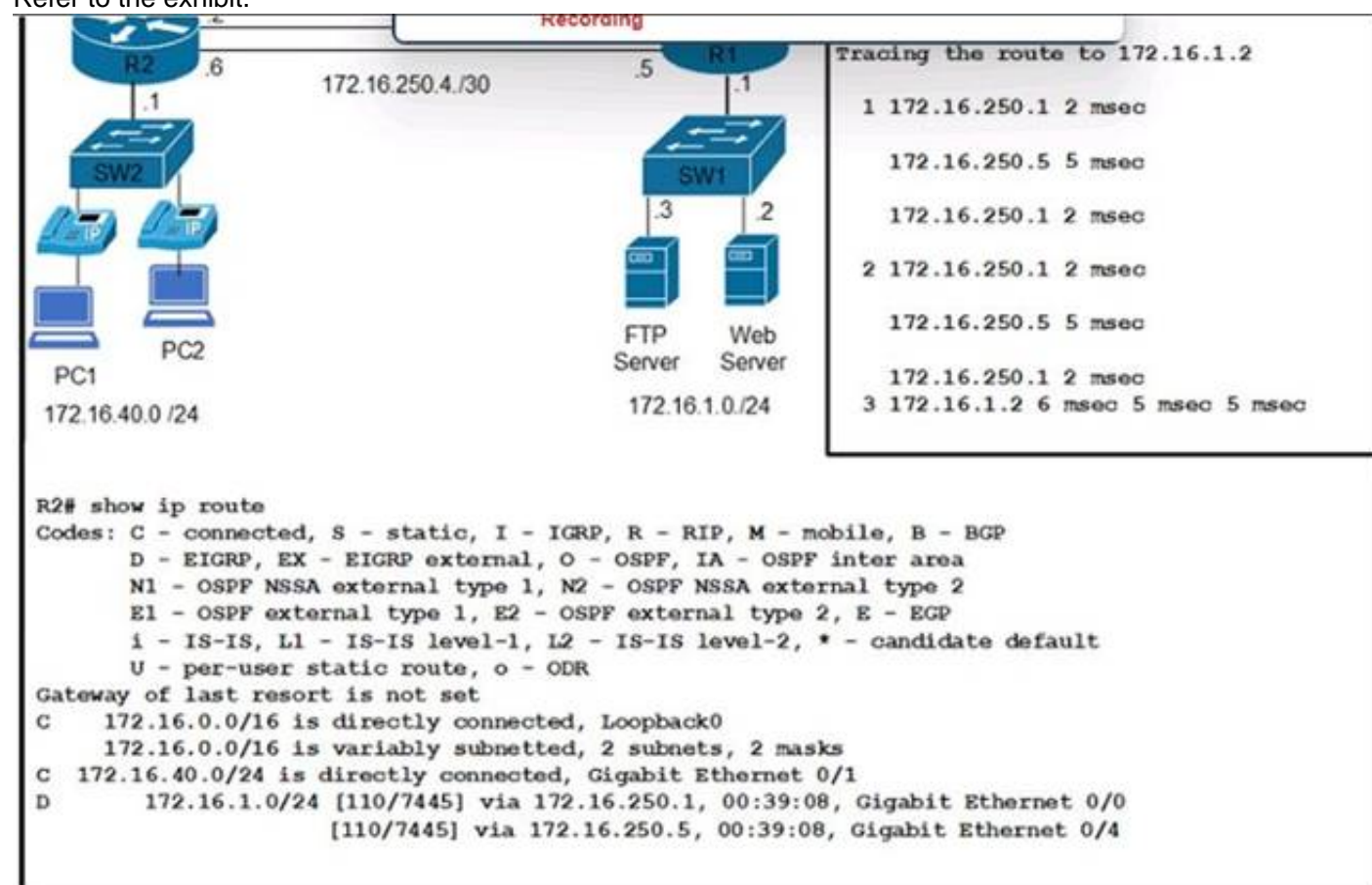
- A. SD-Access transit
- B. fabric interconnect
- C. wireless transit
- D. IP-based transit
- E. SAN transit

Answer: AD

#### NEW QUESTION 243

- (Topic 4)

Refer to the exhibit.



Clients are reporting an issue with the voice traffic from the branch site to the central site. What is the cause of this issue?

- A. The voice traffic is using the link with less available bandwidth.
- B. There is a routing loop on the network.
- C. Traffic is load-balancing over both links, causing packets to arrive out of order.
- D. There is a high delay on the WAN links.

Answer: C

#### Explanation:

Traffic is load-balancing over both links, causing packets to arrive out of order. This can cause voice quality issues, such as jitter and delay. To avoid this problem, voice traffic should be sent over a single path, using a routing protocol that supports unequal-cost load balancing, such as EIGRP. The source of this answer is the Cisco ENCOR v1.1 course, module 4, lesson 4.3: Implementing EIGRP.

#### NEW QUESTION 247

- (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 248

- (Topic 4)

By default, which virtual MAC address does HSRP group 15 use?

- A. 05:5e:ac:07:0c:0f
- B. c0:42:34:03:73:0f
- C. 00:00:0c:07:ac:0f
- D. 05:af:1c:0f:ac:15

**Answer:** C

#### Explanation:

```
interface Ethernet0/0.100 encapsulation dot1Q 100
ip address 10.0.111.1 255.255.255.0
standby 15 ip 10.0.111.254
!
```

cisco(config-subif)#do s stand Ethernet0/0.100 - Group 15  
State is Speak  
Virtual IP address is 10.0.111.254 Active virtual MAC address is unknown  
Local virtual MAC address is 0000.0c07.ac0f (v1 default) Hello time 3 sec, hold time 10 sec  
Next hello sent in 1.200 secs Preemption disabled  
Active router is unknown Standby router is unknown

#### NEW QUESTION 250

- (Topic 4)

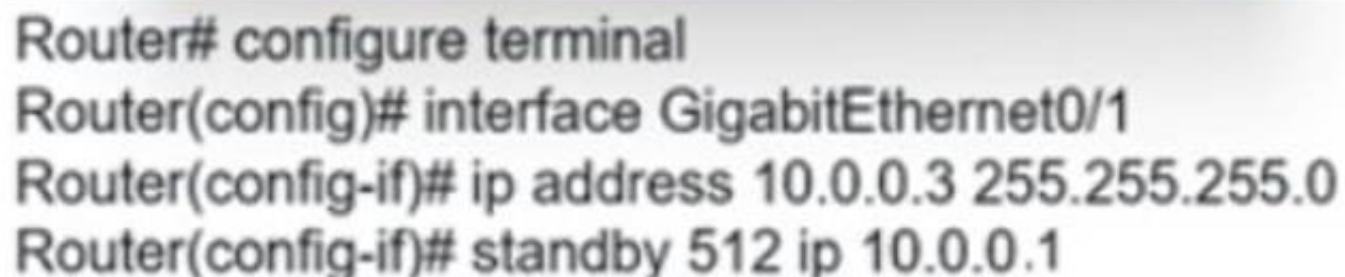
Which unit of measure is used to measure wireless RF SNR?

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

**Answer:** C

#### NEW QUESTION 254

- (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 256

- (Topic 4)

Refer to the exhibit.

```

R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 65001
<output omitted>
Neighbor      V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.50.2   4        65002    10      9        5    0    0 00:04:56    2

R1#show ip bgp 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 2
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  65002
    192.168.50.2 from 192.168.50.2 (172.20.0.2)
      Origin IGP, metric 0, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0

<CONFIGURATION CHANGE MADE>

R1#show ip bgp 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 6
Paths: (1 available, best #1, table default, RIB-failure(17))
  Not advertised to any peer
  Refresh Epoch 1
  65002
    192.168.50.2 from 192.168.50.2 (172.20.0.2)
      Origin IGP, metric 0, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0

```

R1 has a BGP neighborship with a directly connected router on interface Gi0/0. Which command set is applied between the iterations of show ip bgp 2.2.2.2?

- A. R1(config)#router bgp 65001R1(config-router)#neighbor 192.168.50.2 shutdown
- B. R1(config)#router bgp 65002R1(config-router)#neighbor 192.168.50.2 shutdown
- C. R1(config)#no ip route 192.168.50.2 255.255.255.255 Gi0/0
- D. R1(config)#ip route 2.2.2.2 255.255.255.255 192.168.50.2

Answer: D

#### NEW QUESTION 257

- (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 259

- (Topic 4)

What is a benefit of YANG modules?

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

Answer: B

#### NEW QUESTION 263

- (Topic 4)

Refer to the exhibit.



```
R2#
*May 27 15:33:59.642: OSPF-1 ADJ Gi1: Send DBD to 192.168.201.137 seq 0xDE7 opt 0x52 flag 0x7 len 32
*May 27 15:33:59.642: OSPF-1 ADJ Gi1: Retransmitting DBD to 192.168.201.137 [15]
*May 27 15:33:59.645: OSPF-1 ADJ Gi1: Rcv DBD from 192.168.201.137 seq 0xDE7 opt 0x52 flag 0x2 len 112 mtu 9100 state EXSTART
```

The OSPF neighborship fails between two routers. What is the cause of this issue?

- A. The OSPF router ID is missing on this router.
- B. The OSPF process is stopped on the neighbor router.
- C. There is an MTU mismatch between the two routers.
- D. The OSPF router ID is missing on the neighbor router.

**Answer: C**

**Explanation:**

```
cisco_R2(config-subif)#do debug ip ospf adj OSPF adjacency debugging is on
cisco_R2(config-subif)#ip mtu 1111 <<<<<<<<<<<<<<< cisco_R2(config-subif)#
cisco_R2(config-subif)# cisco_R2(config-subif)#do clear ip ospf
!!!debug shows this: cisco_R2(config-subif)#
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Rcv DBD from 6.6.6.6 seq 0x19FD opt 0x52
flag 0x7 len 32 mtu 1500 state EXSTART <<<<<<<<<<<
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Nbr 6.6.6.6 has larger interface MTU
<<<<<<<<<
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Rcv DBD from 6.6.6.6 seq 0x26B opt 0x52
flag 0x2 len 112 mtu 1500 state EXSTART
*Dec 23 13:02:27.164: OSPF-1 ADJ Et0/0.10: Nbr 6.6.6.6 has larger interface MTU
*Dec 23 13:02:27.395: OSPF-1 ADJ Et0/0.10: Rcv DBD from 6.6.6.6 seq 0x26B opt 0x52
flag 0x2 len 112 mtu 1500 state EXSTART
```

**NEW QUESTION 268**

- (Topic 4)

A company's office has publicly accessible meeting rooms equipped with network ports. A recent audit revealed that visitors were able to access the corporate network by plugging personal laptops into open network ports. Which of the following should the company implement to prevent this in the future?

- A. URL filters
- B. VPN
- C. ACLs
- D. NAC

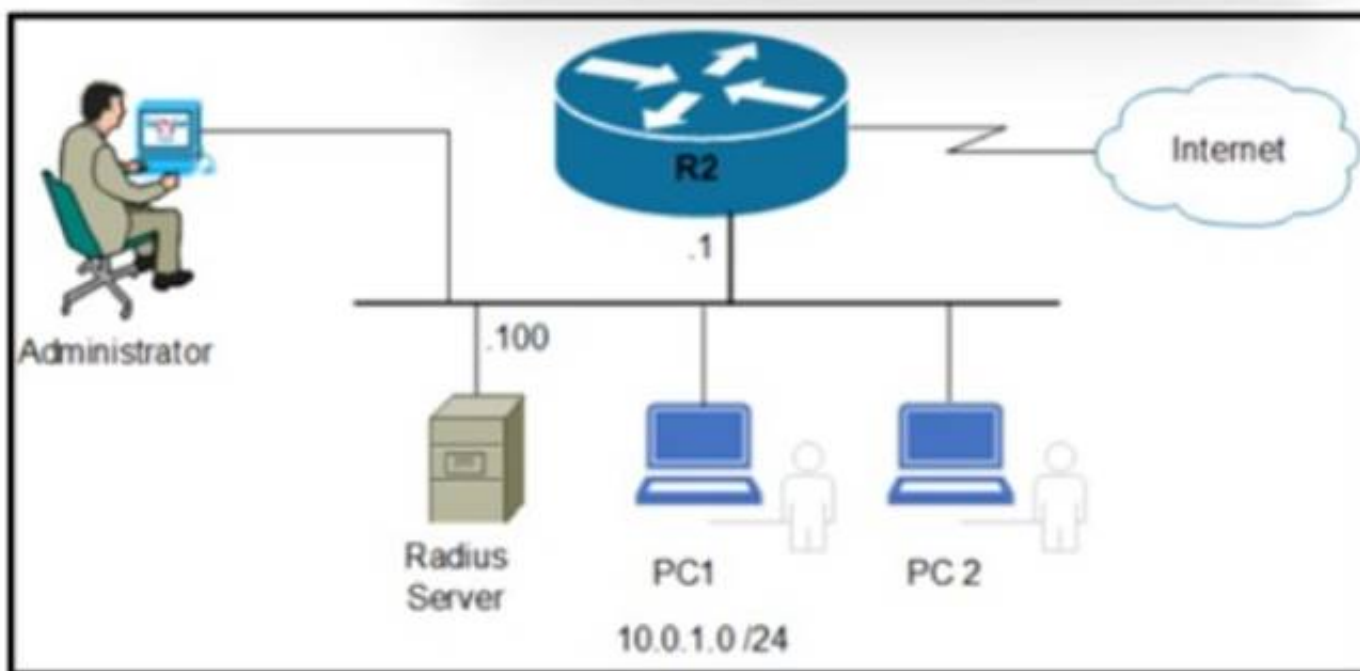
**Answer: D**

**Explanation:**

This is because NAC stands for network access control, which is a security mechanism that allows or denies access to a network based on the identity and compliance of the device. NAC can prevent unauthorized visitors from accessing the corporate network by plugging personal laptops into open network ports, as NAC can enforce policies such as authentication, authorization, posture assessment, and remediation. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.4: Implementing Network Access Control.

## NEW QUESTION 269

- (Topic 4)



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

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

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

Answer: C

#### NEW QUESTION 274

- (Topic 4)

Which JSON script is properly formatted?

A)

```
[ "Lodging":
  {
    "type":B&B,
    "location":Oceanfront,
    "contact":946-230-7462
  }
]
```

B)

```
{
  "frames": [
    {
      "type":"premium",
      "material":"wood",
      "shape":"square"
    }
  ]
}
```

C)

```
[
  {
    "subject": {
      [
        "title":"Sewing"
        "listing":"elective"
        "session":"Summer"
      ]
    }
  ]
]
```

D)

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

- 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 277

DRAG DROP - (Topic 4)

Drag and drop the characteristics from the left onto the switching mechanisms they describe on the right.

The forwarding table is created in advance.

The router processor is involved with every forwarding decision.

All forwarding decisions are made in software.

All packets are switched using hardware.

Cisco Express Forwarding

Process Switching

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The forwarding table is created in advance.

The router processor is involved with every forwarding decision.

All forwarding decisions are made in software.

All packets are switched using hardware.

Cisco Express Forwarding

The forwarding table is created in advance.

All forwarding decisions are made in software.

Process Switching

The router processor is involved with every forwarding decision.

All packets are switched using hardware.



#### NEW QUESTION 282

- (Topic 4)

Users have reported an issue connecting to a server over the network. A workstation was recently added to the network and configured with a shared USB printer. Which of the following is most likely causing the issue?

- A. The switch is oversubscribed and cannot handle the additional throughput.
- B. The printer is tying up the server with DHCP discover messages.
- C. The web server's back end was designed for only single-threaded applications.
- D. The workstation was configured with a static IP that is the same as the server.

**Answer: D**

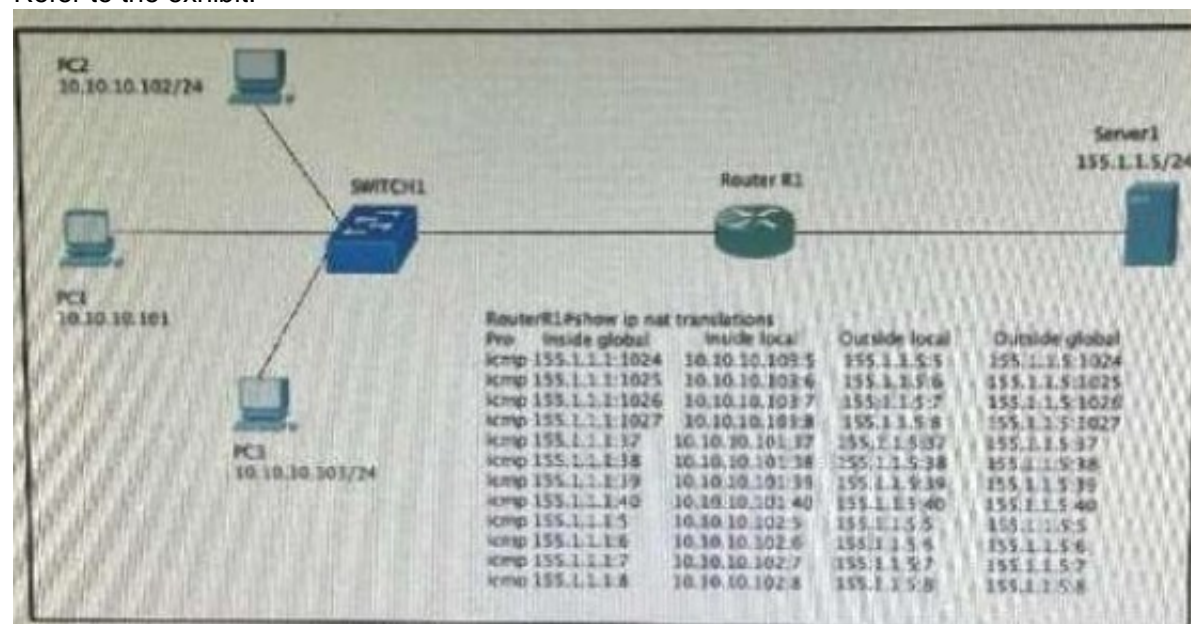
#### Explanation:

The workstation was configured with a static IP that is the same as the server. This is because if two devices on the same network have the same IP address, they will cause an IP address conflict, which will prevent them from communicating with other devices on the network. The users who were moved to different desks may have been assigned static IP addresses that were not updated after the move, and they may have accidentally used the same IP address as the server. The source of this answer is the Cisco ENCOR v1.1 course, module 3, lesson 3.1: Implementing IPv4 and IPv6 Addressing.

#### NEW QUESTION 285

- (Topic 4)

Refer to the exhibit.



Hosts PC1 PC2 and PC3 must access resources on Serve 1. An engineer configures NAT on Router R1 1e enable the communication and enters the show command to verify operation Which IP address is used by the hosts when they communicate globally to Server1?

- A. 155.1.1.1
- B. random addresses in the 155.1.1.0/24 range
- C. their own address in the 10.10.10.0/24 rance
- D. 155.1.1.5

**Answer: A**

#### NEW QUESTION 286

- (Topic 4)

Which method ensures the confidentiality ot 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 290

- (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 292

- (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**

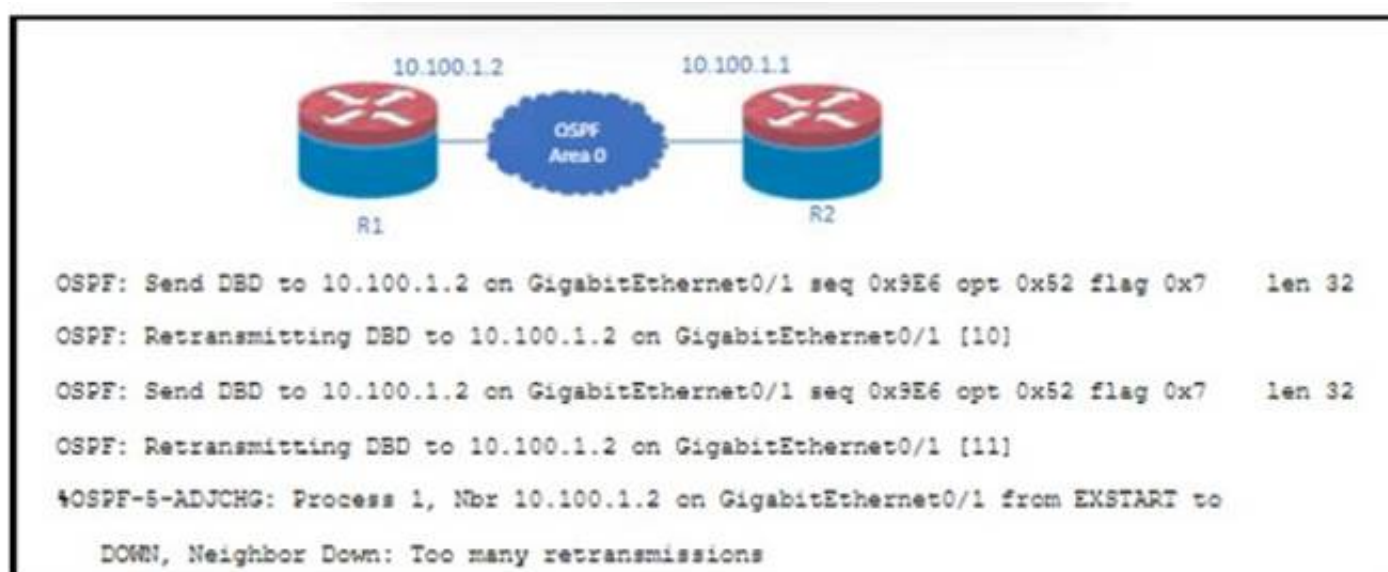
**Explanation:**

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 294**

- (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 298**

- (Topic 4)

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

- A. Cisco Express Forwarding switching uses adjacency tables built by the CDP protocol, and process switching uses the routing table.

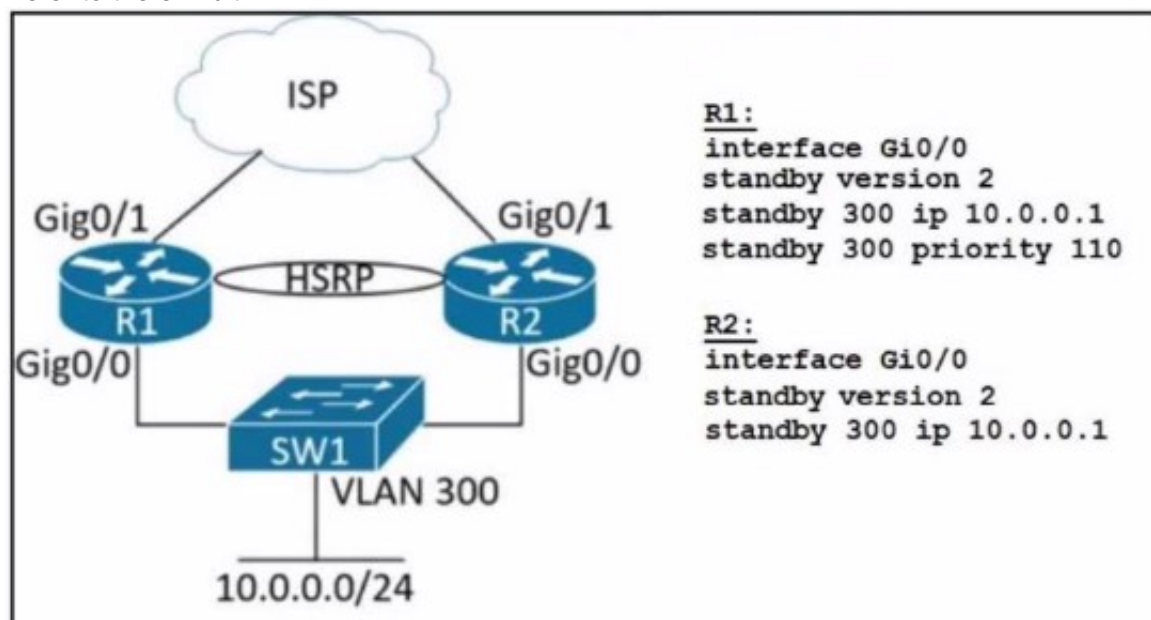
- B. Cisco Express Forwarding switching uses dedicated hardware processors, and process switching uses the main processor.  
 C. Cisco Express Forwarding switching saves memory by storing adjacency tables in dedicated memory on the line cards, and process switching stores all tables in the main memory.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

Answer: C

#### NEW QUESTION 302

- (Topic 4)

Refer to the exhibit.



Refer to the exhibit. An engineer must implement HSRP between two WAN routers. In the event R1 fails and then regains operational status, it must allow 100 seconds for the routing protocol to converge before preemption takes effect. Which configuration is required?

A)

**R1:**  
 interface Gi0/0  
 standby 300 preempt

**R2:**  
 interface Gi0/0  
 standby 300 delay sync 100

B)

**R1:**  
 interface Gi0/0  
 standby 300 preempt

**R2:**  
 interface Gi0/0  
 standby 300 delay minimum 100

C)

**R1:**  
 interface Gi0/0  
 standby 300 preempt  
 standby 300 delay minimum 100

D)

**R2:**  
 interface Gi0/0  
 standby 300 preempt  
 standby 300 delay sync 100

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

Answer: B

Explanation:



Option B is the correct configuration to implement HSRP between two WAN routers with the given requirement. The configuration steps are as follows<sup>12</sup>:

? Define the HSRP group number and the virtual IP address for the group using the standby <group> ip <address> command. In this case, the group number is 300 and the virtual IP address is 10.10.10.1: standby 300 ip 10.10.10.1.

? Configure HSRP preemption and preemption delay using the standby <group> preempt [delay [minimum] <seconds>] command. Preemption allows a router with higher priority to take over the active role from a router with lower priority.

Preemption delay is the time that a router waits before taking over the active role in the HSRP group. In this case, the preemption delay is 100 seconds, which means that R1 will wait for 100 seconds before preempting R2 after R1 regains operational status: standby 300 preempt delay minimum 100.

? Configure the HSRP priority for the router using the standby <group> priority <value> command. The priority determines which router is the active router and which router is the standby router. The higher the priority, the more likely the router is to become the active router. In this case, R1 has a priority of 200 and R2 has a priority of 100, which means that R1 is the preferred active router and R2 is the standby router: standby 300 priority 200 on R1 and standby 300 priority 100 on R2.

Option A is incorrect because it does not configure HSRP preemption and preemption delay, which are required by the question. Without preemption, R2 will remain the active router even if R1 has a higher priority and regains operational status. Without preemption delay, R1 will attempt to preempt R2 immediately, which may cause routing instability<sup>12</sup>.

Option C is incorrect because it configures HSRP preemption delay with the reload keyword, which means that the delay period applies only to the first interface-up event after the router has reloaded. This does not meet the requirement of the question, which states that the delay period should apply to any interface-up event after R1 fails and then regains operational status<sup>12</sup>.

Option D is incorrect because it configures HSRP preemption delay with the sync keyword, which means that the delay period applies only to the first interface-up event after the router has reloaded, and only if such an event occurs within 360 seconds from reload. This does not meet the requirement of the question, which states that the delay period should apply to any interface-up event after R1 fails and then regains operational status, and without any time limit<sup>12</sup>. References: 1: Configuring HSRP, 2: HSRP Configuration Guide

### NEW QUESTION 305

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
!
```

DISTRO-SW2

*Passing Certification Exams Made Easy*



```

!
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 aes2
56-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes2
56-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 308

- (Topic 4)

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

Refer to the exhibit What does this Python script do?

- enters the RAOIUS username for a specific IP address
- writes the username for a specific IP address into a light database
- enters the TACACS\* username for a specific IP address
- reads the username for a specific IP address from a light database

Answer: B

### NEW QUESTION 311

- (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 314

- (Topic 4)

What is a characteristic of a Type 2 hypervisor?

- A. It eliminates the need for an underlying operating system.
- B. Its main task is to manage hardware resources between different operating systems
- C. Problems in the base operating system can affect the entire system.
- D. It is completely independent of the operating system

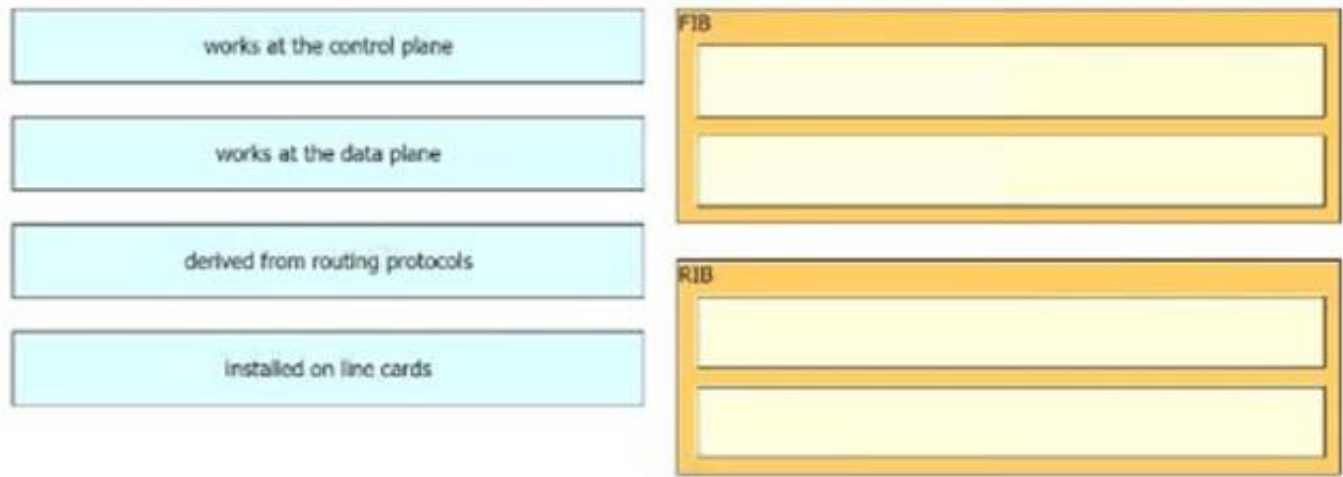
**Answer:** C

#### NEW QUESTION 315

DRAG DROP - (Topic 4)

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

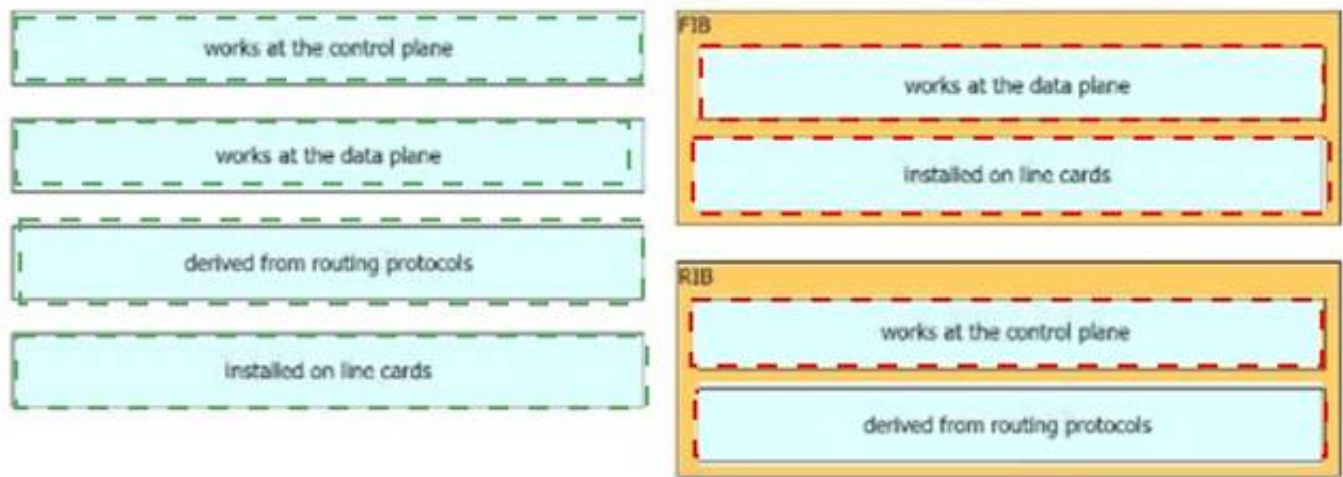




- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 318

- (Topic 2)  
What does the Cisco DNA Center use to enable the delivery of applications through a network and to yield analytics for innovation?

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

Answer: C

Explanation:

The Cisco DNA Center open platform for intent-based networking provides 360- degree extensibility across multiple components, including:  
+ Intent-based APIs leverage the controller to enable business and IT applications to deliver intent to the network and to reap network analytics and insights for IT and business innovation. These enable APIs that allow Cisco DNA Center to receive input from a variety of sources, both internal to IT and from line-of-business applications, related to application policy, provisioning, software image management, and assurance.  
...  
Reference: <https://www.cisco.com/c/en/us/products/collateral/cloud-systemsmanagement/dna-center/nb-06-dna-cent-plat-sol-over-cte-en.html>

NEW QUESTION 322

- (Topic 2)  
Refer to the exhibit.

|                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>R1 key chain cisco123 key 1 key-string cisco123!  Ethernet0/0 - Group 10 State is Active   8 state changes, last state change 00:02:49 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a</pre> | <pre>R2 key chain cisco123 key 1 key-string cisco123!  Ethernet0/0 - Group 10 State is Active   17 state changes, last state change 00:02:17 Virtual IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a</pre> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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

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

**Answer:** A

**Explanation:**

The virtual MAC address is 0000.0c07.acXX (XX is the hexadecimal group number) so it is using HSRPv1.  
 Note: HSRP Version 2 uses a new MAC address which ranges from 0000.0c9f.f000 to 0000.0c9f.ffff.

**NEW QUESTION 324**

- (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:

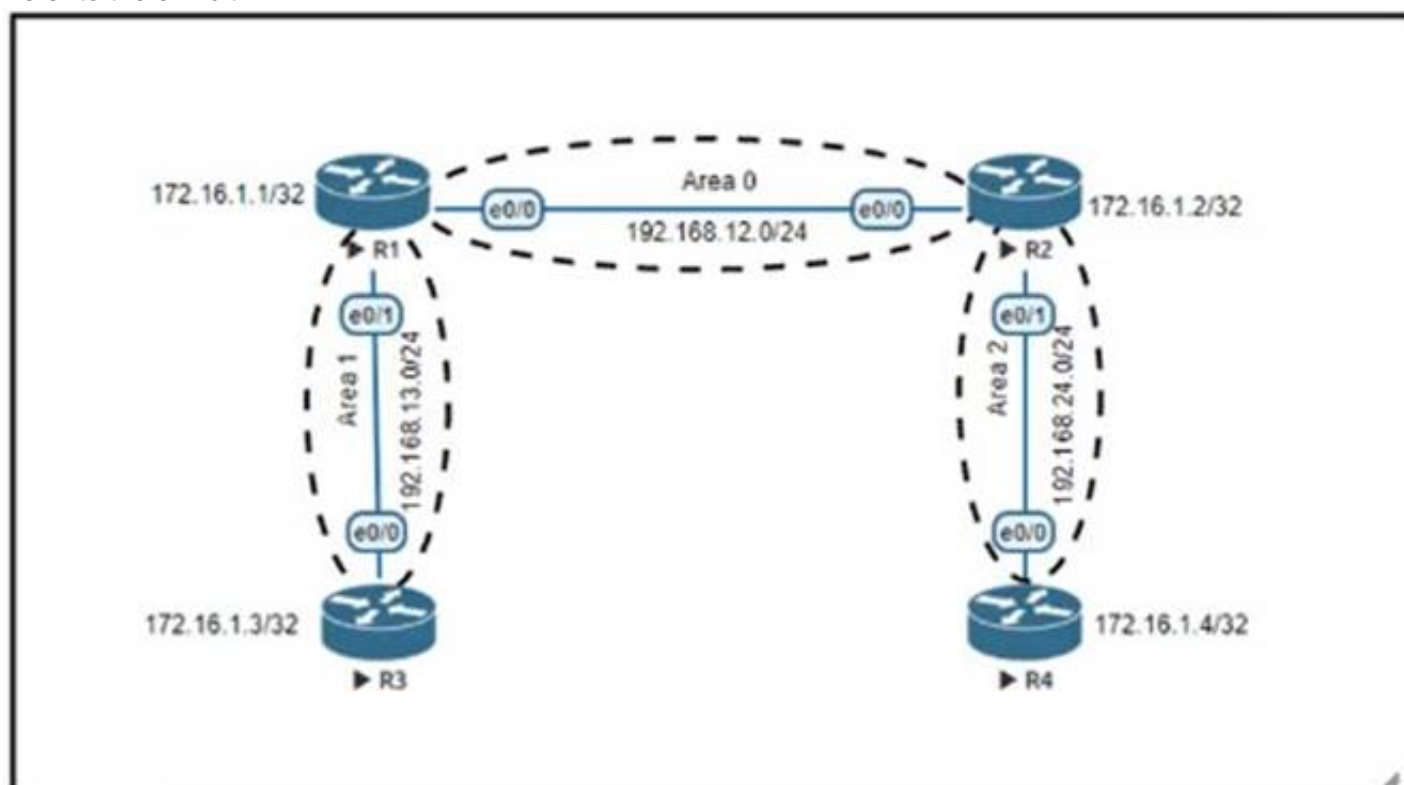
- + Broadcast and Non-Broadcast (adjust hello/dead timers)
- + Point-to-Point and Point-to-Multipoint (adjust hello/dead timers)

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 328**

- (Topic 2)

Refer to the exhibit.



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

- On R1  
 ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32  
 ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32  
  
 router ospf 200  
 area 1 filter-list prefix INTO-AREA1 out
- On R3  
 ip access-list standard R4\_L0  
 deny host 172.16.1.4  
 permit any  
  
 router ospf 200  
 distribute-list R4\_L0 in
- On R1  
 ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32  
 ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32  
  
 router ospf 200  
 area 1 filter-list prefix INTO-AREA1 in
- On R3  
 ip prefix-list INTO-AREA1 seq 5 deny 172.16.1.4/32  
 ip prefix-list INTO-AREA1 seq 10 permit 0.0.0.0/0 le 32  
  
 router ospf 200  
 area 1 filter-list prefix INTO-AREA1 in

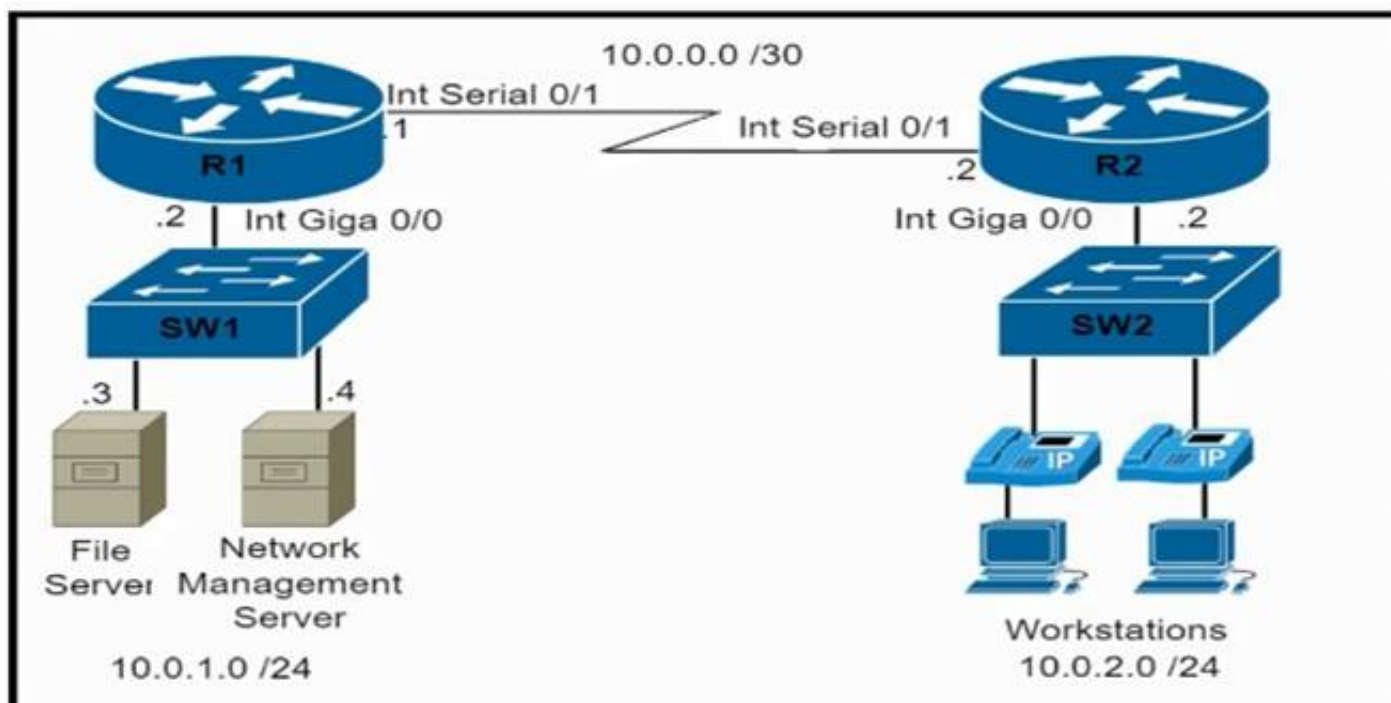
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

#### NEW QUESTION 329

- (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 332

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 335

- (Topic 2)

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

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

Answer: C

#### NEW QUESTION 340

- (Topic 4)

Refer to the exhibit.

|                                     |              |                                     |          |                       |                      |
|-------------------------------------|--------------|-------------------------------------|----------|-----------------------|----------------------|
| DSW1#sh spanning-tree               |              |                                     |          |                       |                      |
| MST1                                |              |                                     |          |                       |                      |
| Spanning tree enabled protocol mstp |              |                                     |          |                       |                      |
| Root ID                             | Priority     | 32769                               |          |                       |                      |
|                                     | Address      | 001b.7363.4300                      |          |                       |                      |
|                                     | Cost         | 2                                   |          |                       |                      |
|                                     | Port         | 13 (FastEthernet1/0/11)             |          |                       |                      |
|                                     | Hello Time   | 2 sec                               | Max Age  | 20 sec                | Forward Delay 15 sec |
|                                     |              |                                     |          |                       |                      |
| Bridge ID                           | Priority     | 32769 (priority 32768 sys-id-ext 1) |          |                       |                      |
|                                     | Address      | 001b.0d8e.e080                      |          |                       |                      |
|                                     | Hello Time   | 2 sec                               | Max Age  | 20 sec                | Forward Delay 15 sec |
|                                     |              |                                     |          |                       |                      |
| Interface                           | Role         | Sts                                 | Cost     | Prio.Nbr              | Type                 |
| -----                               |              |                                     |          |                       |                      |
| Fa1/0/7                             | Desg         | FWD                                 | 2        | 128.9                 | P2p Bound(PVST)      |
| Fa1/0/10                            | Desg         | FWD                                 | 2        | 128.12                | P2p Bound(PVST)      |
| Fa1/0/11                            | Root         | FWD                                 | 2        | 128.13                | P2p                  |
| Fa1/0/12                            | Altn         | BLK                                 | 2        | 128.14                | P2p                  |
|                                     |              |                                     |          |                       |                      |
| DSW1#sh spanning-tree mst           |              |                                     |          |                       |                      |
| ##### MST1                          |              |                                     |          |                       |                      |
|                                     | vlan mapped: | 10,20                               |          |                       |                      |
| Bridge                              | address      | 001b.0d8e.e080                      | priority | 32769 (32768 sysid 1) |                      |
| Root                                | address      | 001b.7363.4300                      | priority | 32769 (32768 sysid 1) |                      |
|                                     | port         | Fa1/0/11                            | cost     | 2                     | rem hops 19          |
|                                     |              |                                     |          |                       |                      |
|                                     |              |                                     |          |                       |                      |
| ... output omitted                  |              |                                     |          |                       |                      |
|                                     |              |                                     |          |                       |                      |

Which two commands ensure that DSW1 becomes root bridge for VLAN 10 and 20?

- A. spanning-tree mst 1 priority 1
- B. spanning-tree mst 1 root primary
- C. spanning-tree mstp vlan 10,20 root primary
- D. spanning-tree mst vlan 10,20 priority root
- E. spanning-tree mst 1 priority 4096

Answer: BE

#### NEW QUESTION 345

- (Topic 4)

Refer to the exhibit.

```
SW1#show cdp neighbors | include Local|0/1
Device ID    Local Intrfce  Holdtime    Capability Platform Port ID
SW2          Fas 0/1       131         R S WS-C3750- Fas 0/1

SW1#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On

SW2#show cdp neighbors | include Local|0/1
Device ID    Local Intrfce  Holdtime    Capability Platform Port ID
SW1          Fas 0/1       142         R S WS-C3750- Fas 0/1

SW2#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
```

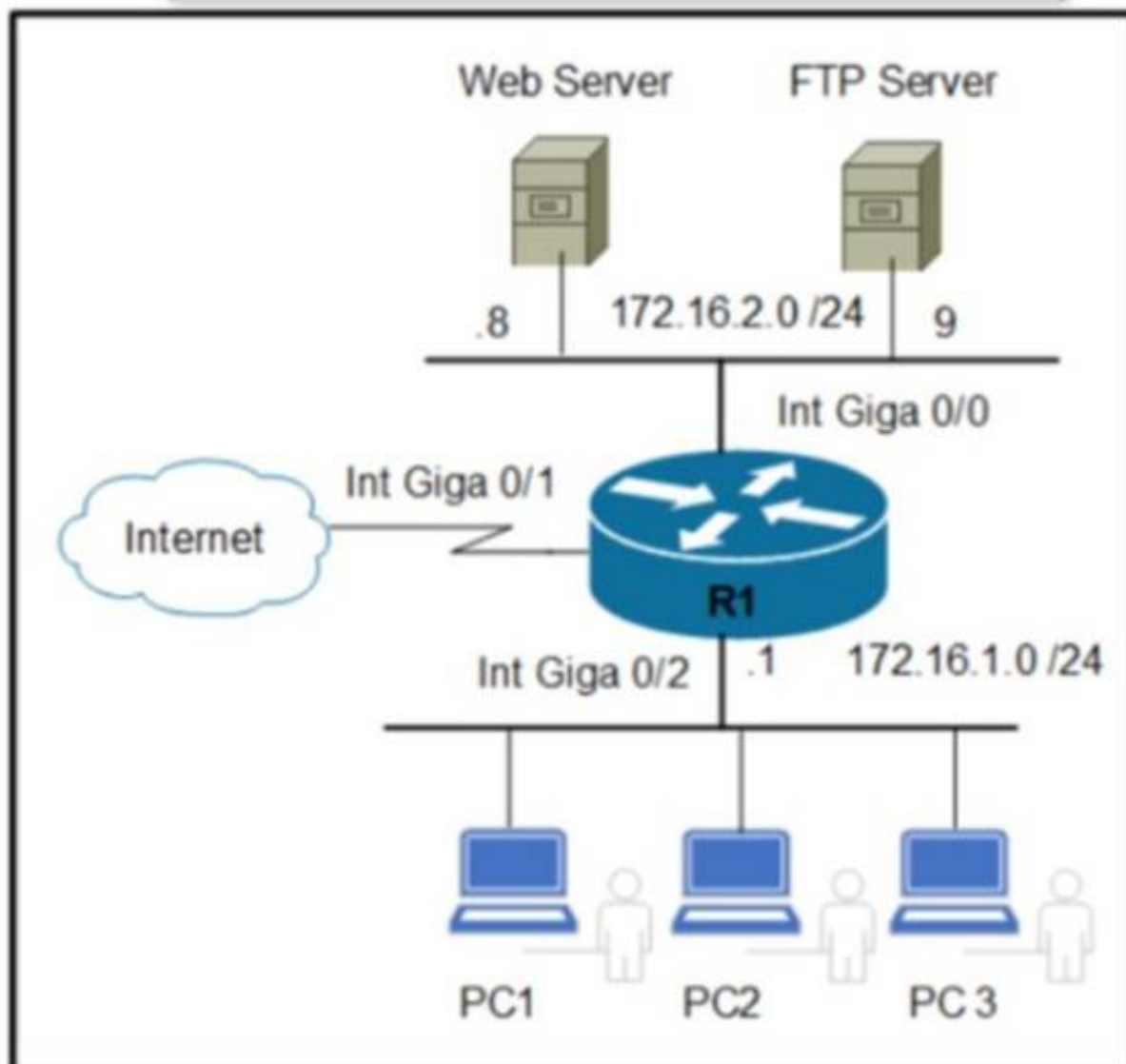
An engineer configures a trunk between SW1 and SW2 but tagged packets are not passing. Which action fixes the issue?

- A. Configure SW1 with dynamic auto mode on interface FastEthernet0/1.
- B. Configure the native VLAN to be the same VLAN on both switches on interface FastEthernet0/1.
- C. Configure SW2 with encapsulation dot1q on interface FastEthernet0/1.
- D. Configure FastEthernet0/1 on both switches for static trunking.

Answer: C

#### NEW QUESTION 346

- (Topic 4)



Refer to the exhibit. An engineer must allow the FTP traffic from users on 172.16.1.0 /24 to 172.16.2.0 /24 and block all other traffic. Which configuration must be applied?

```
A)
R1(config)# access-list 120 deny any any
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21
R1(config)#interface giga 0/0
R1(config-if)#ip access-group 120 out
```

B)



```
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 in
```

C)

```
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 20
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 in
```

D)

```
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)# access-list 120 permit udp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 out
```

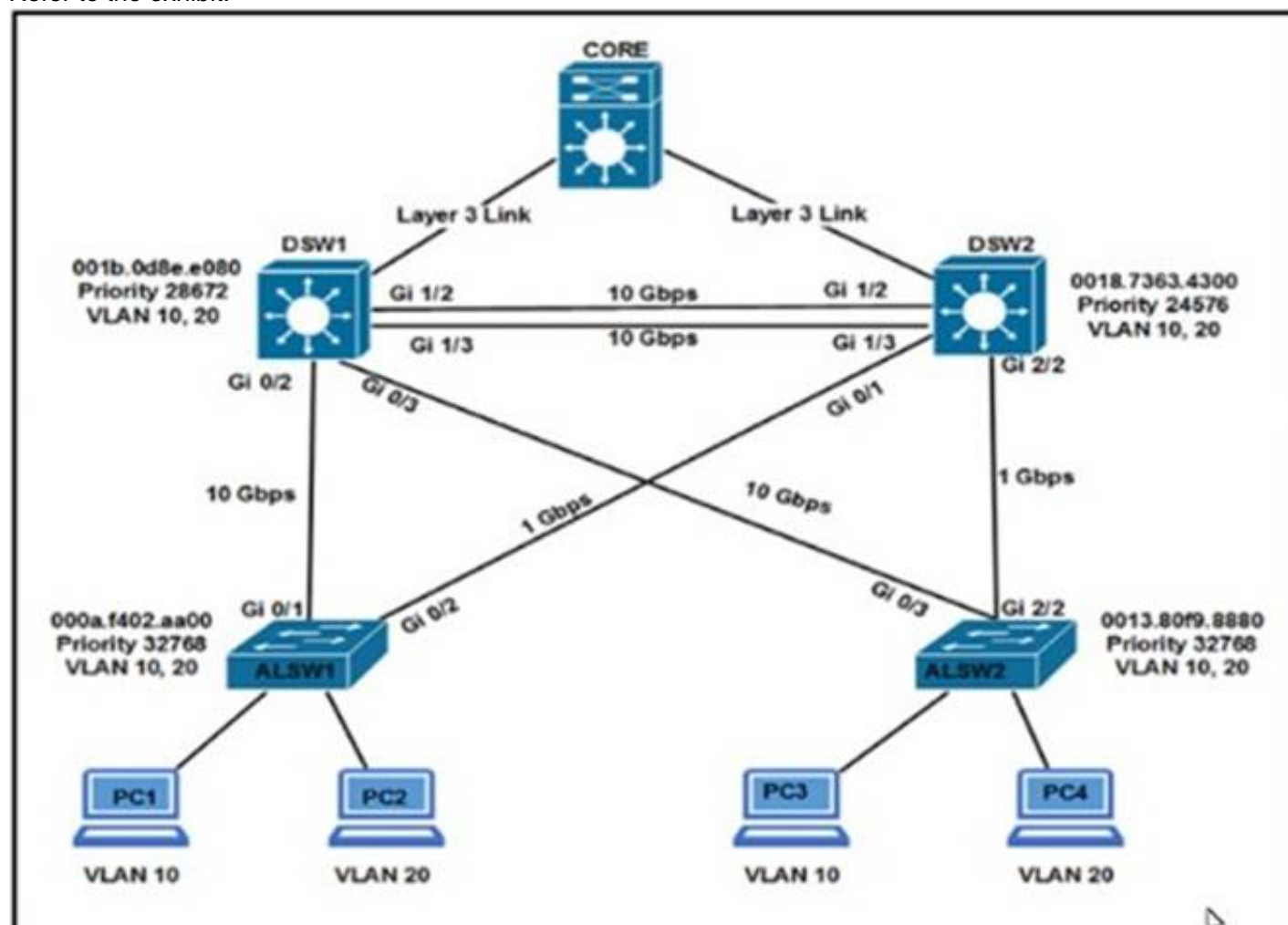
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

#### NEW QUESTION 348

- (Topic 4)

Refer to the exhibit.



Assuming all links are functional, which path does PC1 take to reach DSW1?

- A. PC1 goes from ALSW1 to DSW2 to CORE to DSW1.
- B. PC1 goes from ALSW1 to DSW2 to DSW1.
- C. PC1 goes from ALSW1 to DSW1.
- D. PC1 goes from ALSW1 to DSW2 to ALSW2 to DSW1.

Answer: B

#### NEW QUESTION 353

- (Topic 4)

When a wired client connects to an edge switch in a Cisco SD-Access fabric, which component decides whether the client has access to the network?

- A. control-plane node
- B. edge node
- C. Identity services Engine
- D. RADIUS server

Answer: C

#### NEW QUESTION 355

- (Topic 4)

Which hypervisor requires a host OS to run and is not allowed to directly access the hosts hardware and resources?

- A. native
- B. bare metal
- C. type 1
- D. type 2

**Answer:** D

#### NEW QUESTION 356

- (Topic 4)

```
Router A
Interface GigabitEthernet 1/0
ip address 192.168.0.1 255.255.255.0
vrrp priority 120

Router B
Interface GigabitEthernet 1/0
ip address 192.168.0.200 255.255.255.0
vrrp priority 100

Router C
Interface GigabitEthernet 1/0
ip address 192.168.0.3 255.255.255.0
vrrp priority 130

Router D
Interface GigabitEthernet 1/0
ip address 192.168.0.4 255.255.255.0
vrrp priority 90
```

Refer to the exhibit. Which router is elected as the VRRP primary virtual router?

- A. Router B
- B. Router D
- C. Router C
- D. Router A

**Answer:** C

#### NEW QUESTION 357

- (Topic 4)

Which of the following are examples of Type 2 hypervisors? (Choose three.)

- A. VMware ESXi
- B. Oracle VirtualBox
- C. Oracle Solaris Zones
- D. Microsoft Hyper-V
- E. Microsoft Virtual PC

**Answer:** BCE

#### NEW QUESTION 361

- (Topic 4)

What is a characteristics of VXLAN?

- A. It extends Layer 2 and Layer 3 overlay networks over a Layer 2 underlay.
- B. It has a 12-byt packet header.
- C. It frame encapsulation is performed by MAC-In-UDP
- D. It uses TCP for transport

**Answer:** C

#### NEW QUESTION 363

- (Topic 4)

Which two actions, when applied in the LAN network segment, will facilitate Layer 3 CAPWAP discovery for lightweight AP? Choose two.)

- A. Enable port security on the switch port.
- B. Configure an IP helper-address on the router interface.

- C. Utilize DHCP option 17.
- D. Configure WLC IP address LAN switch.
- E. Utilize DHCP option 43.

**Answer:** AE

#### NEW QUESTION 364

- (Topic 4)

How do OSPF and EIGRP compare?

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

**Answer:** D

#### NEW QUESTION 369

DRAG DROP - (Topic 3)

Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

|                               |           |
|-------------------------------|-----------|
| declarative                   | Chef      |
| communicates using knife tool |           |
| communicates through SSH      | SaltStack |
| procedural                    |           |

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Chef  
 Communicates using knife tool Procedural  
 SaltStack  
 Communicates through SSH Declarative

#### NEW QUESTION 371

- (Topic 3)

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

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

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

**Answer:** D

#### NEW QUESTION 373

DRAG DROP - (Topic 3)

Drag and drop the LISP components on the left to their descriptions on the right. Not all options are used.

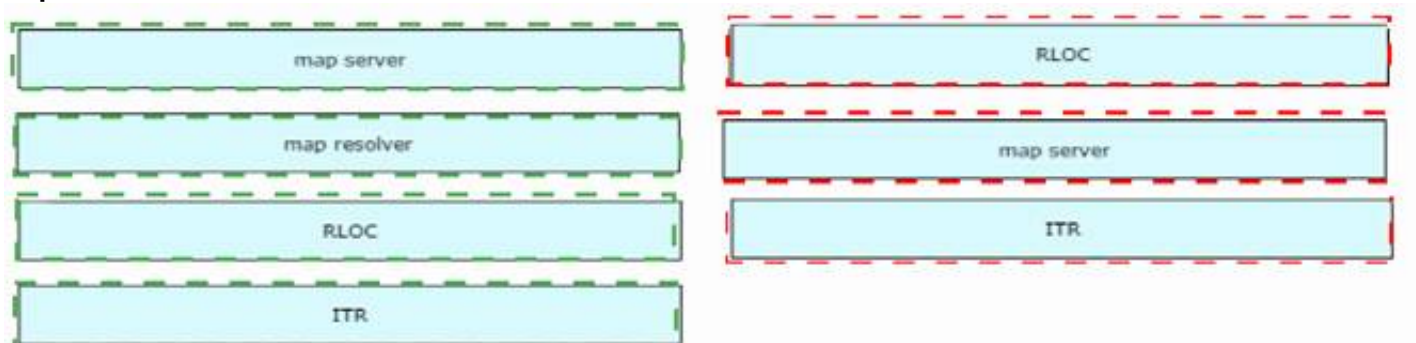
map server	IPv4 or IPv6 address of an egress tunnel router that is Internet facing or network core facing
map resolver	receives map-request messages from ITR and searches for the appropriate ETR by consulting mapping database
RLOC	encapsulates LISP packets coming from inside of the LISP site to destinations outside of the site
ITR	



- A. Mastered
- B. Not Mastered

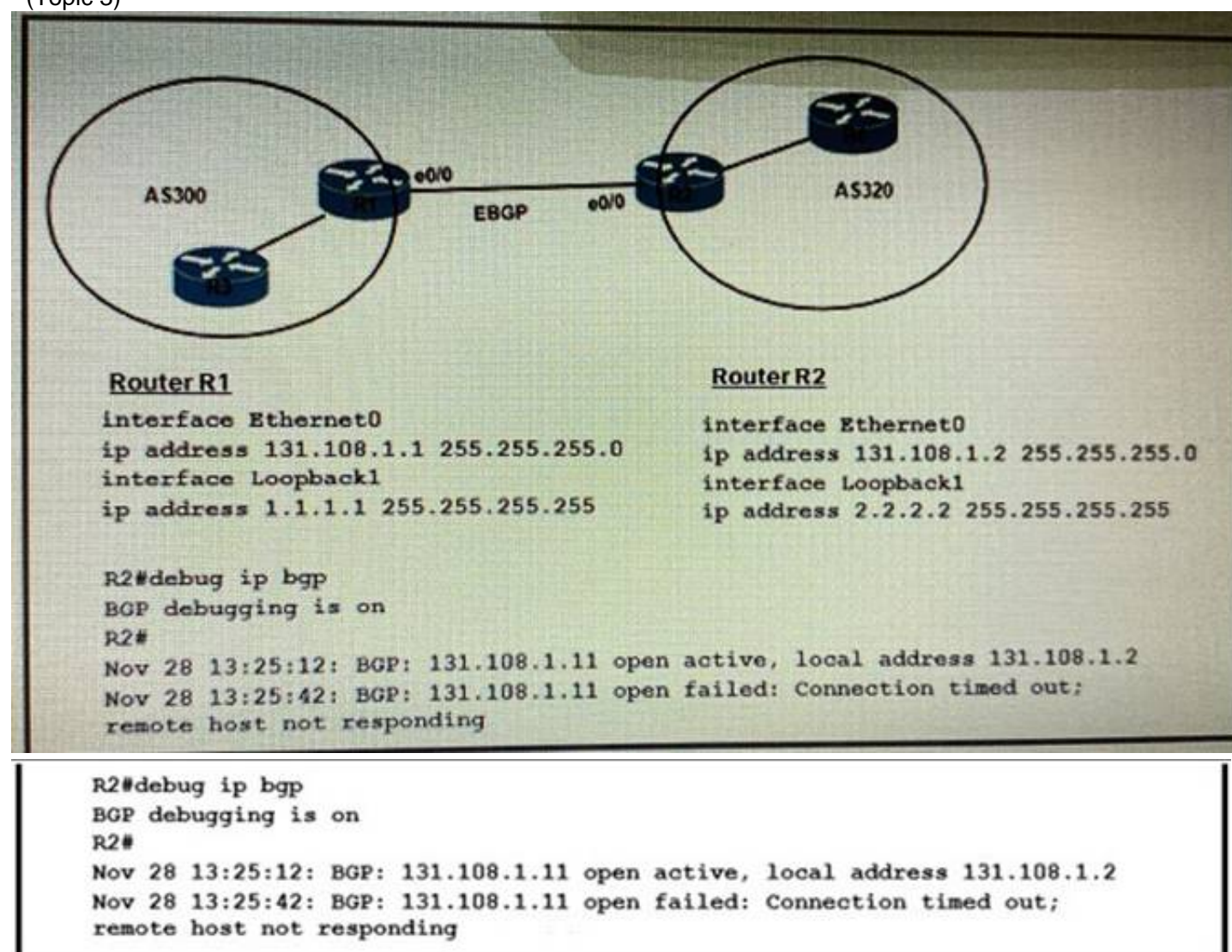
Answer: A

Explanation:

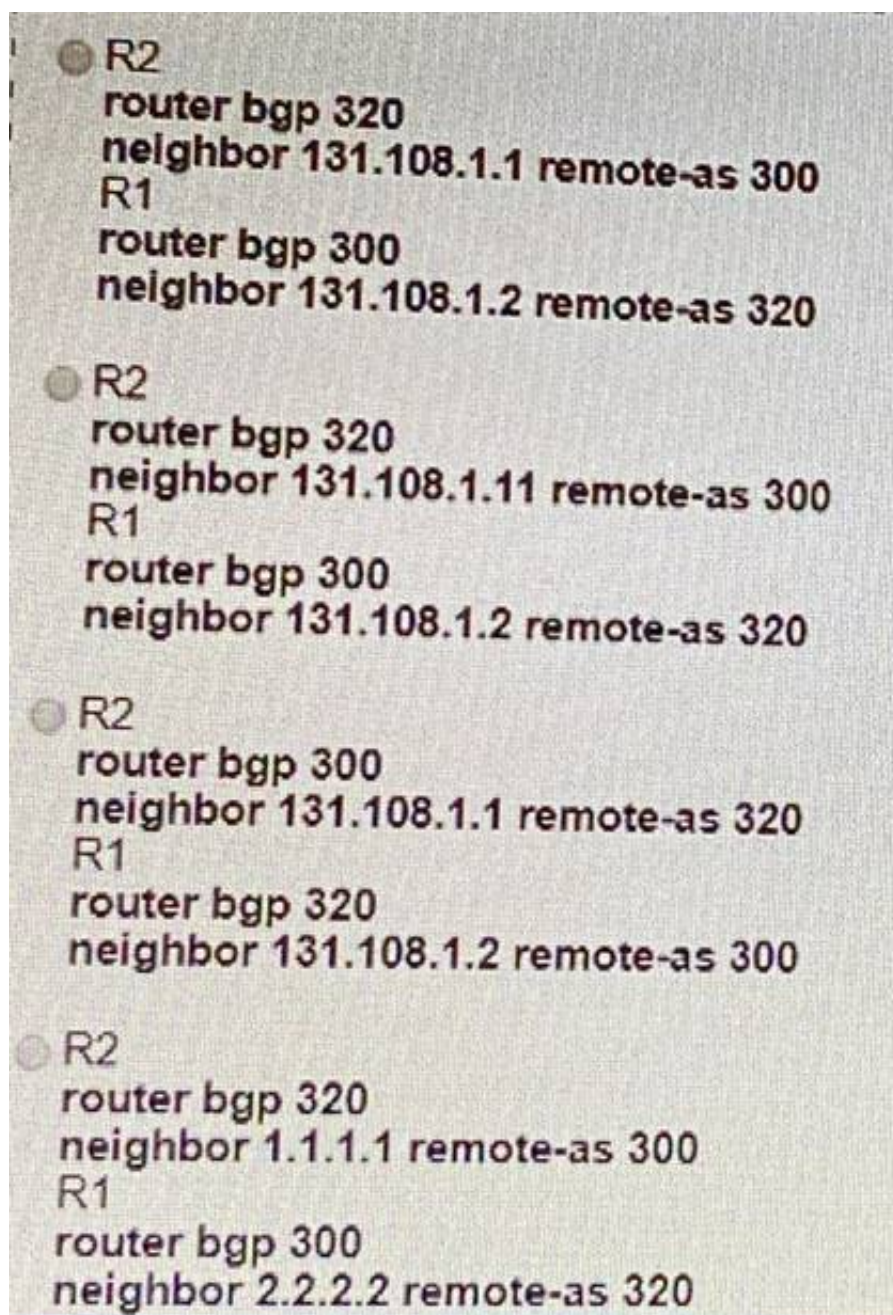


#### NEW QUESTION 375

- (Topic 3)



Refer to the exhibit. Which configuration must be implemented to establish EBGP peering between R1 and R2?



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

**Answer:** A

#### NEW QUESTION 380

- (Topic 3)

Which type of tunnel is required between two WLCs to enable Intercontroller roaming?

- A. mobility
- B. LWAPP
- C. CAPWAP
- D. IPsec

**Answer:** A

#### NEW QUESTION 382

- (Topic 3)

A system must validate access rights to all its resources and must not rely on a cached permission matrix. If the access level to a given resource is revoked but is not reflected in the permission matrix, the security is violated. Which term refers to this REST security design principle?

- A. economy of mechanism
- B. complete mediation
- C. separation of privilege
- D. least common mechanism

**Answer:** B

#### Explanation:

A system should validate access rights to all its resources to ensure that they are allowed and should not rely on the cached permission matrix. If the access level to a given resource is being revoked, but that is not being reflected in the permission matrix, it would be violating security.

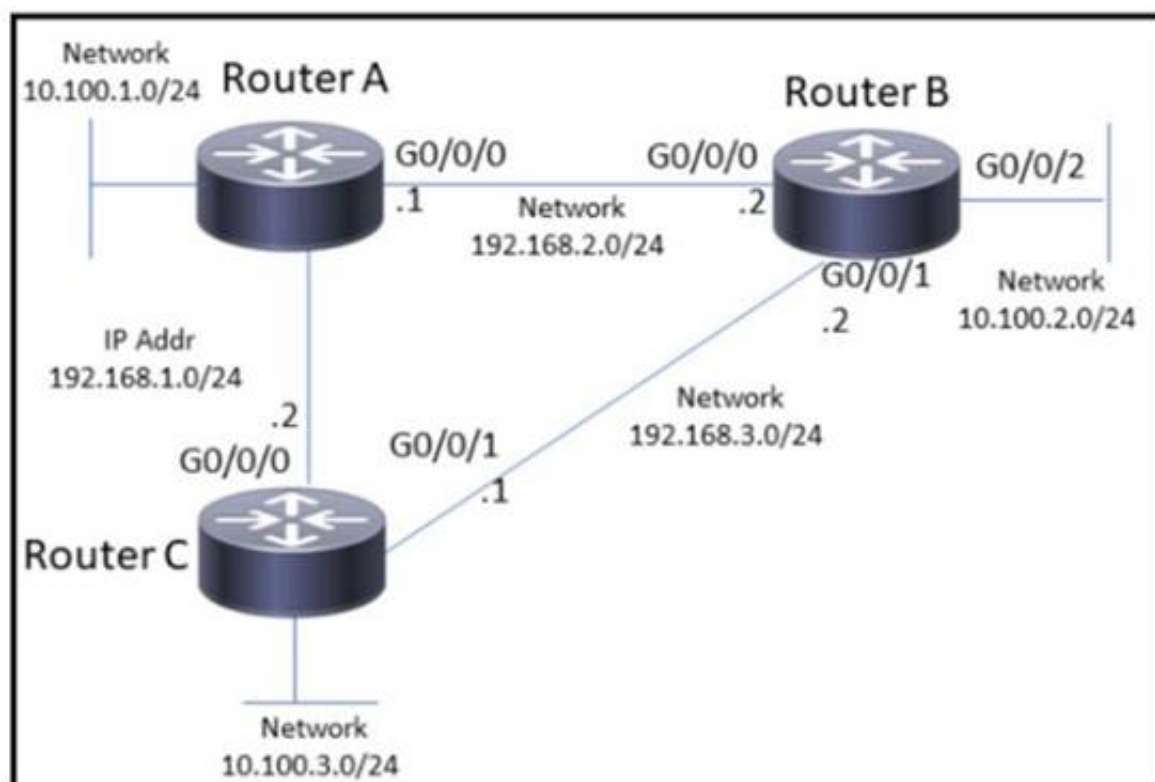
<https://medium.com/strike-sh/rest-security-design-principles-434bd6ee57ea>

#### NEW QUESTION 383

- (Topic 3)

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





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

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

Answer: C

#### NEW QUESTION 386

- (Topic 3)

Which Cisco FlexConnect state allows wireless users that are connected to the network to continue working after the connection to the WLC has been lost?

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

Answer: C

#### Explanation:

Operation Modes

There are two modes of operation for the FlexConnect AP.

? Connected mode: The WLC is reachable. In this mode the FlexConnect AP has CAPWAP connectivity with its WLC.

? Standalone mode: The WLC is unreachable. The FlexConnect has lost or failed to establish CAPWAP connectivity with its WLC. A WAN-link outage between a branch and its central site is a example of such a mode of operation.

FlexConnect States

A FlexConnect WLAN, depending on its configuration and network connectivity, is classified as being in one of the following defined states.

? Authentication-Central/Switch-Central: This state represents a WLAN that uses a centralized authentication method such as 802.1X, VPN, or web. User traffic is sent to the WLC via CAPWAP (Central switching). This state is supported only when FlexConnect is in connected mode.

? Authentication Down/Switching Down: Central switched WLANs no longer beacon or respond to probe requests when the FlexConnect AP is in standalone mode. Existing clients are disassociated.

? Authentication-Central/Switch-Local: This state represents a WLAN that uses centralized authentication, but user traffic is switched locally. This state is supported only when the FlexConnect AP is in connected mode.



? Authentication-Down/Switch-Local: A WLAN that requires central authentication rejects new users. Existing authenticated users continue to be switched locally until session time-out if configured. The WLAN continues to beacon and respond to probes until there are no more existing users associated to the WLAN. This state occurs as a result of the AP going into standalone mode.

? Authentication-local/switch-local: This state represents a WLAN that uses open, static WEP, shared, or WPA2 PSK security methods. User traffic is switched locally. These are the only security methods supported locally if a FlexConnect goes into standalone mode. The WLAN continues to beacon and respond to probes. Existing users remain connected and new user associations are accepted. If the AP is in connected mode, authentication information for these security types is forwarded to the WLC.

#### NEW QUESTION 387

DRAG DROP - (Topic 3)

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 391

- (Topic 3)

Which IPv4 packet field carries the QoS IP classification marking?

- A. ID
- B. TTL
- C. FCS
- D. ToS

**Answer:** D

**Explanation:**

The classification is carried in the IP packet header, using 6 bits from the deprecated IP type of service (ToS) field to carry the classification (class) information. Classification can also be carried in the Layer 2 frame.

#### NEW QUESTION 396

DRAG DROP - (Topic 3)

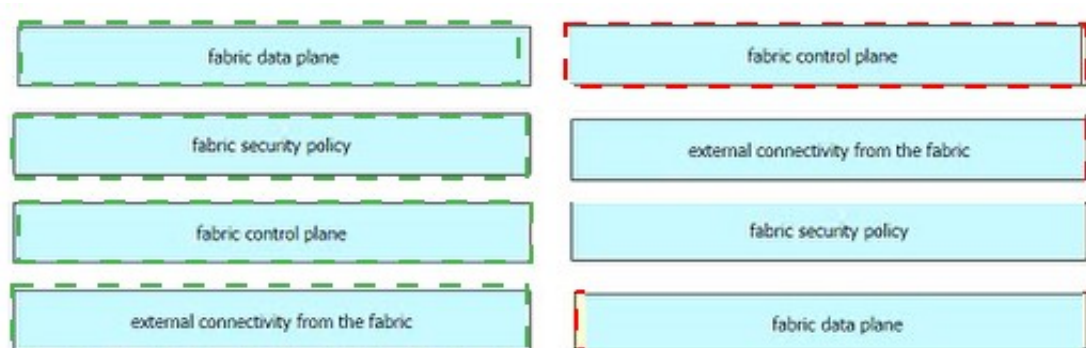
Drag and drop the Cisco SD-Access solution areas from the left onto the protocols they use on the right.

fabric data plane	LISP
fabric security policy	BGP
fabric control plane	CTS
external connectivity from the fabric	VXLAN

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 398

- (Topic 3)

What is used to validate the authenticity of the client and is sent in HTTP requests as a JSON object?

- A. SSH
- B. HTTPS
- C. JWT
- D. TLS

Answer: C

#### NEW QUESTION 403

- (Topic 3)

Which Python snippet should be used to store the devices data structure in a JSON file?

```
import json
Devices = {'Switches': [{'name': 'AccSw1',
                          'ip': '2001:db8:4166:8961:5::1'},
                     {'name': 'AccSw2',
                          'ip': '2001:db8:12b1:31a7:fffe::2'}],
          'Routers': [{'name': 'CE1', 'ip': '2001:db8:31ac:a97a:8::1'},
                     {'name': 'CE2', 'ip': '2001:db8:7ac8:9ab7::2'}
                    ]
}
```

A)

```
with open("devices.json", "w") as OutFile:
    json.dumps(Devices)
```

B)

```
OutFile = open("devices.json", "w")
OutFile.write(str(Devices))
OutFile.close()
```

C)

```
OutFile = open("devices.json", "w")
json.dump(Devices, OutFile)
OutFile.close()
```

D)

```
with open("devices.json", "w") as OutFile:
    Devices = json.load(OutFile)
```

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

Answer: A

#### NEW QUESTION 407

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 411**

- (Topic 3)

What is one main REST security design principle?

- A. separation of privilege
- B. password hashing
- C. confidential algorithms
- D. OAuth

**Answer:** A

**Explanation:**

Separation of Privilege: Granting permissions to an entity should not be purely based on a single condition, a combination of conditions based on the type of resource is a better idea.

<https://restfulapi.net/security-essentials/#:~:text=REST%20Security%20Design%20Principles&text=Least%20Privilege%3A%20An%20entity%20should,when%20no%20longer%20in%20use.>

**NEW QUESTION 416**

- (Topic 3)

```
Router#show access-lists
Extended IP access list 100
 10 permit ip 192.168.0.0 0.0.255.255 any
 20 permit ip 172.16.0.0 0.0.15.255 any
```

Refer to the exhibit. Which command set must be added to permit and log all traffic that comes from 172.20.10.1 in interface GigabitEthernet0/1 without impacting the functionality of the access list?

- ☐ Router(config)#no access-list 100 permit ip 172.16.0.0 0.0.15.255 any  
Router(config)#access-list 100 permit ip 172.16.0.0 0.0.15.255 any log  
Router(config)#interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in
- ☐ Router(config)#access-list 100 seq 5 permit ip host 172.20.10.1 any log  
Router(config)#Interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in
- ☐ Router(config)#ip access-list extended 100  
Router(config-ext-nacl)#5 permit ip 172.20.10.0 0.0.0.255 any log  
Router(config)#interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in
- ☐ Router(config)#access-list 100 permit ip host 172.20.10.1 any log  
Router(config)#Interface GigabitEthernet0/1  
Router(config-if)#access-group 100 in

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

**Answer:** B

**NEW QUESTION 418**

- (Topic 3)

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



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

Answer: C

#### NEW QUESTION 419

DRAG DROP - (Topic 3)

Drag and drop the automation characteristics from the left onto the appropriate tools on the right.

provides intent-based networking feedback loop

agent or agentless automation platform

agentless automation platform

assesses the impact of changes before applied

**Ansible**

**Puppet**

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

provides intent-based networking feedback loop

agent or agentless automation platform

agentless automation platform

assesses the impact of changes before applied

**Ansible**

agentless automation platform

provides intent-based networking feedback loop

**Puppet**

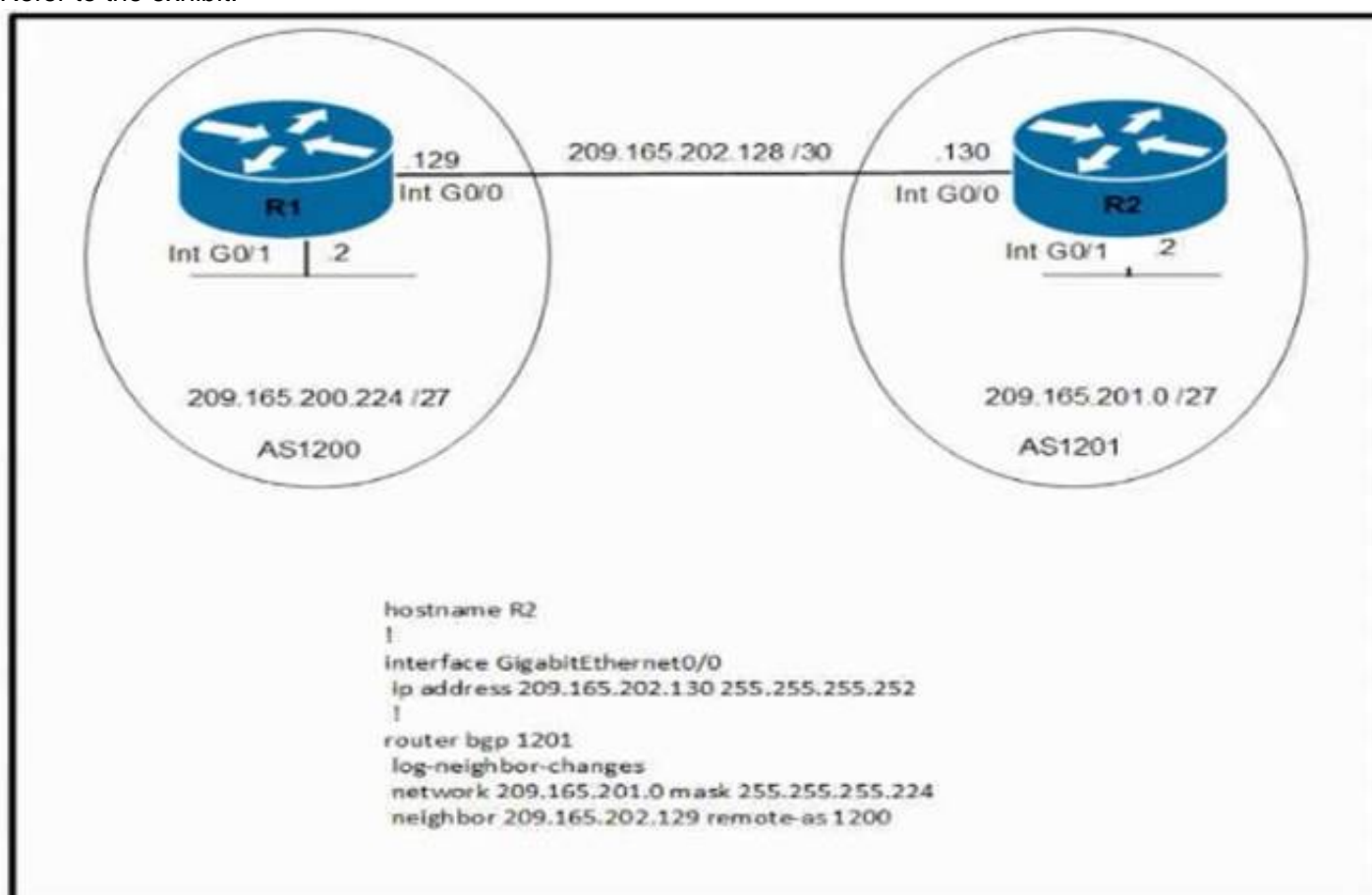
agent or agentless automation platform

assesses the impact of changes before applied

#### NEW QUESTION 423

- (Topic 3)

Refer to the exhibit.



Which command set must be applied on R1 to establish a BGP neighborship with R2 and to allow communication from R1 to reach the networks?

A)

```

router bgp 1200
network 209.165.201.0 mask 255.255.255.224
neighbor 209.165.202.130 remote-as 1201
  
```

B)

```
router bgp 1200
network 209.165.200.224 mask 255.255.255.224
neighbor 209.165.201.2 remote-as 1200
```

C)

```
router bgp 1200
network 209.165.200.224 mask 255.255.255.224
neighbor 209.165.202.130 remote-as 1201
```

D)

```
router bgp 1200
network 209.165.200.224 mask 255.255.255.224
```

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

**Answer:** A

#### NEW QUESTION 427

- (Topic 3)

```
event manager applet config-alert
event cli pattern "write mem.*" sync yes
```

Refer to the exhibit. Which EEM script generates a critical-level syslog message and saves a copy of the running configuration to the bootflash when an administrator saves the running configuration to the startup configuration?

- ☐ action 1.0 cli command copy running-config bootflash:/current\_config.txt  
 action 2.0 syslog msg "Configuration saved and copied to bootflash"
- ☐ action 1.0 cli command "enable"  
 action 2.0 cli command "configure terminal"  
 action 3.0 cli command "file prompt quiet"  
 action 4.0 cli command "end"  
 action 5.0 cli command copy running-config bootflash:/current\_config.txt  
 action 6.0 cli command "configure terminal"  
 action 7.0 cli command "no file prompt quiet"  
 action 8.0 syslog priority critical msg "Configuration saved and copied to bootflash"
- ☐ action 1.0 cli command "enable"  
 action 2.0 cli command "file prompt quiet"  
 action 3.0 cli command copy running-config bootflash:/current\_config.txt  
 action 4.0 cli command "no file prompt quiet"  
 action 5.0 syslog priority critical msg "Configuration saved and copied to bootflash"
- ☐ action 1.0 cli command copy running-config bootflash:/current\_config.txt  
 action 2.0 syslog priority critical msg "Configuration saved and copied to bootflash"

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

**Answer:** B

#### NEW QUESTION 431

- (Topic 3)

Refer to the exhibit.



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

Service-policy input: CoPP

Class-map: class-telnet (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: access-group 100
 police:
   cir 100000 bps, bc 3125 bytes
   conformed 0 packets, 0 bytes; actions:
     transmit
   exceeded 0 packets, 0 bytes; actions:
     drop
   conformed 0 bps, exceed 0 bps

Class-map: class-default (match-any)
 56 packets, 9874 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: any

Router#show access-list 100
Extended IP access list 100
 10 permit tcp any any eq telnet
```

Which commands are required to allow SSH connection to the router?

- A)
- ```
Router(config)#access-list 100 permit udp any any eq 22
Router(config)#access-list 101 permit tcp any any eq 22
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP
Router(config-pmap)#police 100000 conform-action transmit
```
- B)
- ```
Router(config)#access-list 100 permit tcp any eq 22 any
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 10
Router(config)#policy-map CoPP
Router(config-pmap)#class class-ssh
Router(config-pmap-c)#police 100000 conform-action transmit
```
- C)
- ```
Router(config)#access-list 10 permit tcp any eq 22 any
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 10
Router(config)#policy-map CoPP
Router(config-pmap)#class class-ssh
Router(config-pmap-c)#police 100000 conform-action transmit
```
- D)



```
Router(config)#access-list 100 permit tcp any any eq 22
Router(config)#access-list 101 permit tcp any any eq 22
Router(config)#class-map class-ssh
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP
Router(config-pmap)#class class-ssh
Router(config-pmap-c)#police 100000 conform-action transmit
```

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

Answer: D

#### NEW QUESTION 432

- (Topic 3)

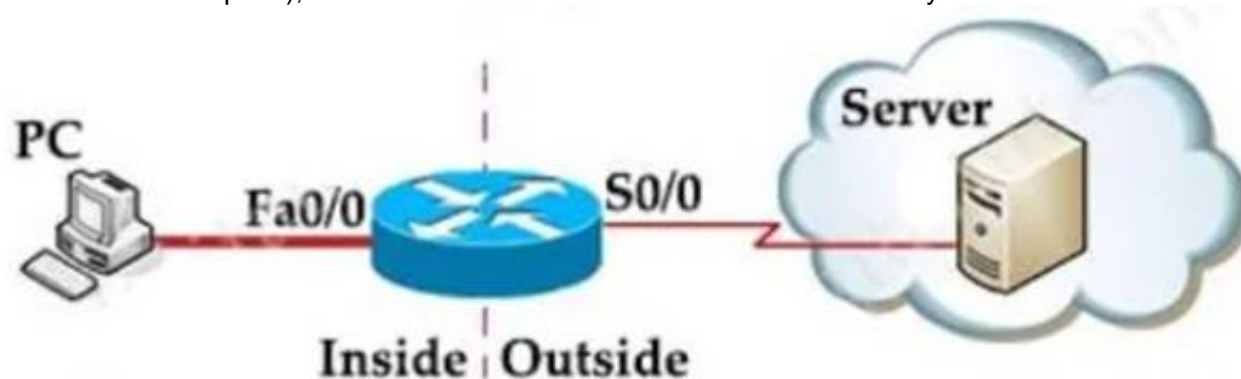
An engineer must configure an ACL that permits packets which include an ACK in the TCP header Which entry must be included in the ACL?

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

Answer: D

#### Explanation:

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



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

```
access-list 100 permit tcp any any established
access-list 101 permit tcp any any eq telnet
```

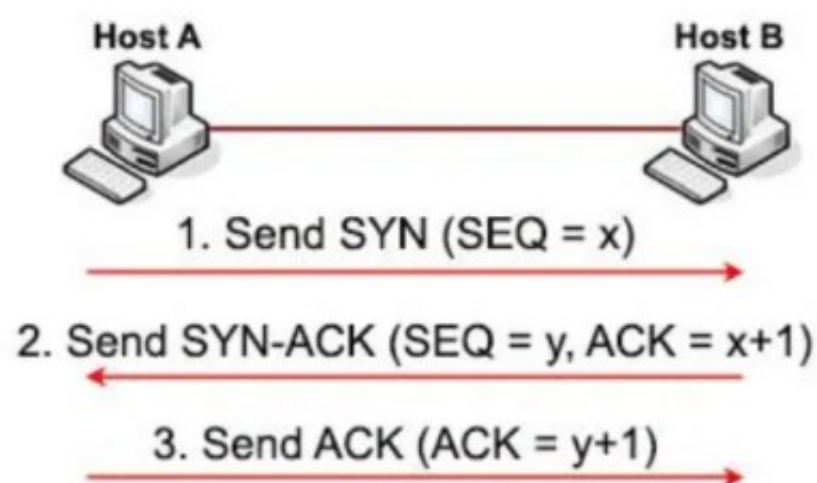
!

interface S0/0

ip access-group 100 in ip access-group 101 out

Note: Suppose host A wants to start communicating with host B using TCP. Before they can send real data, a three-way handshake must be established first.

Let's see how this process takes place:



\* 1. First host A will send a SYN message (a TCP segment with SYN flag set to 1, SYN is short for SYNchronize) to indicate it wants to setup a connection with host B. This message includes a sequence (SEQ) number for tracking purpose. This sequence number can be any 32-bit number (range from 0 to 232) so we use "x" to represent it.

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

+ SYN sequence number (let's called it "y") is a random number and does not have any relationship with Host A's SYN SEQ number.

+ ACK number is the next number of Host A's SYN sequence number it received, so we represent it with "x+1". It means I received your part. Now send me the next part (x + 1)".

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

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

#### NEW QUESTION 435

- (Topic 3)

Which two Cisco SD-WAN components exchange OMP information?

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

**Answer:** BC

#### NEW QUESTION 440

DRAG DROP - (Topic 3)

Drag and drop the characteristics from the left onto the technology types on the right.

|   |                          |
|---|--------------------------|
| This type of technology provides automation across multiple technologies and domains. | Configuration Management |
| This type of technology enables consistent configuration of infrastructure resources. |                          |
| Puppet is used for this type of technology.   | Orchestration            |
| Ansible is used for this type of technology.  |                          |

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Orchestration

Orchestration means arranging or coordinating multiple systems. It's also used to mean "running the same tasks on a bunch of servers at once, but not necessarily all of them." Configuration Management

Config Management is part of provisioning. Basically, that's using a tool like Chef, Puppet or Ansible to configure our server. "Provisioning" often implies it's the first time we do it. Config management usually happens repeatedly.

Configuration management (CM) is a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life Configuration management is all about bringing consistency in the infrastructure.

Configuration Orchestration vs Configuration Management

The first thing that should be clarified is the difference between "configuration orchestration" and "configuration management" tools, both of which are considered IaC tools and are included on this list.

Configuration orchestration tools, which include Terraform and AWS CloudFormation, are designed to automate the deployment of servers and other infrastructure. Configuration management tools like Chef, Puppet, and the others on this list help configure the software and systems on this infrastructure that has already been provisioned.

#### NEW QUESTION 444

- (Topic 3)

What is the purpose of an RP in PIM?

- A. send join messages toward a multicast source SPT
- B. ensure the shortest path from the multicast source to the receiver
- C. receive IGMP joins from multicast receivers
- D. secure the communication channel between the multicast sender and receiver

**Answer:** A

#### NEW QUESTION 447

- (Topic 3)

Refer to the exhibit.

```
enable secret cisco

aaa new-model

tacacs server ise-1
address 10.1.1.1
key cisco123!

tacacs server ISE-2
address 10.2.2.1
key cisco123!

aaa group server tacacs+ ISE-Servers
server name ise-1
server name ise-2
```

A network engineer must configure the router to use the ISE-Servers group for authentication. If both ISE servers are unavailable, the local username database must be used. If no usernames are defined in the configuration, then the enable password must be the last resort to log in. Which configuration must be applied to achieve this result?

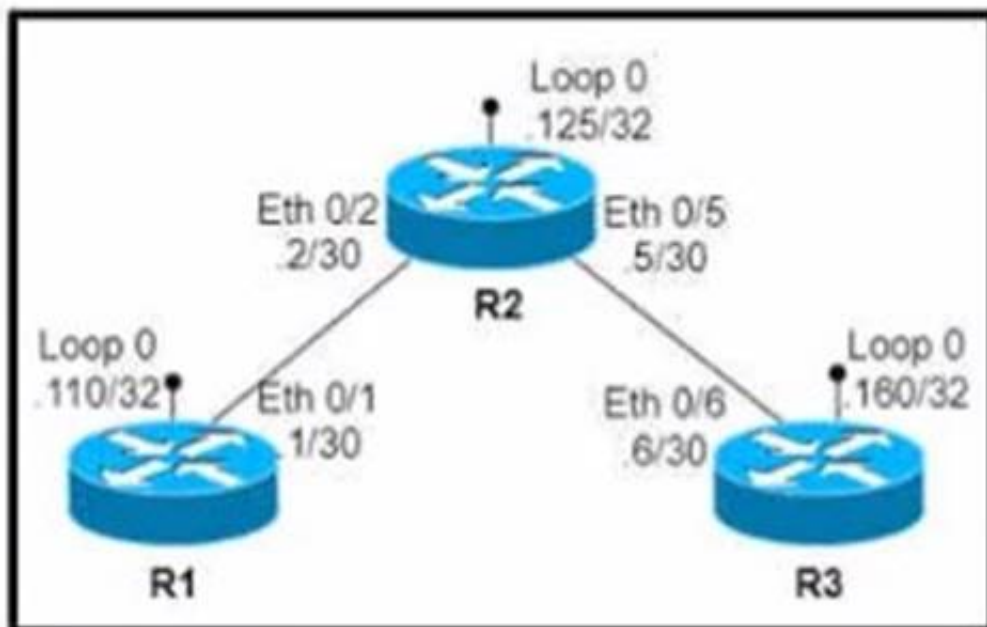
- A. aaa authentication login default group ISE-Servers local enable
- B. aaa authentication login default group enable local ISE-Servers
- C. aaa authorization exec default group ISE-Servers local enable
- D. aaa authentication login error-enableaaa authentication login default group enable local ISE-Servers

**Answer: A**

#### NEW QUESTION 449

- (Topic 3)

Refer to the exhibit.



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

A)

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

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

B)



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

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

C)

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

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

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

D)

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

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

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

**Answer:** D

#### NEW QUESTION 451

- (Topic 3)

What is one benefit of adopting a data modeling language?

- A. augmenting management process using vendor centric actions around models
- B. refactoring vendor and platform specific configurations with widely compatible configurations
- C. augmenting the use of management protocols like SNMP for status subscriptions
- D. deploying machine-friendly codes to manage a high number of devices

**Answer:** B

#### NEW QUESTION 455

- (Topic 3)

What is the calculation that is used to measure the radiated power of a signal after it has gone through the radio, antenna cable, and antenna?

- A. EIRP
- B. mW
- C. dBm
- D. dBi

**Answer:** A

#### NEW QUESTION 459

- (Topic 3)

Which definition describes JWT in regard to REST API security?

- A. an encrypted JSON token that is used for authentication
- B. an encrypted JSON token that is used for authorization
- C. an encoded JSON token that is used to securely exchange information
- D. an encoded JSON token that is used for authentication

**Answer:** D

#### Explanation:

JWT: JSON Web Tokens are an open and standard (RFC 7519) way for you to represent your user's identity securely during a two-party interaction. That is to say, when two systems exchange data you can use a JSON Web Token to identify your user without having to send private credentials on every request.

#### NEW QUESTION 463

- (Topic 3)

An engineer must configure an EXEC authorization list that first checks a AAA server then a local username. If both methods fail, the user is denied. Which configuration should be applied?

- A. aaa authorization exec default local group tacacs+
- B. aaa authorization exec default local group radius none
- C. aaa authorization exec default group radius local none
- D. aaa authorization exec default group radius local

**Answer:** D

#### NEW QUESTION 464

- (Topic 3)

Which benefit is realized by implementing SSO?

- A. IP first-hop redundancy
- B. communication between different nodes for cluster setup
- C. physical link redundancy
- D. minimal network downtime following an RP switchover

**Answer:** D

#### NEW QUESTION 469

- (Topic 3)

- A. S2 is configured as LAC
- B. Change the channel group mode to passive
- C. S2 is configured with PAg
- D. Change the channel group mode to active.
- E. S1 is configured with LAC
- F. Change the channel group mode to on
- G. S1 is configured as PAg
- H. Change the channel group mode to desirable

**Answer:** B

#### NEW QUESTION 472

- (Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 475

- (Topic 2)

A customer transitions a wired environment to a Cisco SD-Access solution. The customer does not want to integrate the wireless network with the fabric. Which wireless deployment approach enables the two systems to coexist and meets the customer requirement?

- A. Deploy the APs in autonomous mode
- B. Deploy the wireless network over the top of the fabric
- C. Deploy a separate network for the wireless environment
- D. Implement a Cisco DNA Center to manage the two networks

**Answer: B**

#### NEW QUESTION 476

- (Topic 2)

Refer to the exhibit.

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

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

A)

```
SW2(config-if)# standby version 2
SW2(config-if)# standby 1000 ip 10.23.87.1
SW2(config-if)# standby 1000 priority 95
SW2(config-if)# standby 1000 preempt
SW2(config-if)# standby 1000 track gigabitEthernet0/0
```

B)

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

C)

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

D)

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

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

**Answer: C**

#### NEW QUESTION 479

- (Topic 2)

How must network management traffic be treated when defining QoS policies?

- A. as delay-sensitive traffic in a low latency queue
- B. using minimal bandwidth guarantee
- C. using the same marking as IP routing
- D. as best effort

**Answer: A**

#### Explanation:

Low latency queuing (LLQ) adds a priority queue to CBWFQ from which delay-sensitive traffic, such as voice traffic, can be transmitted ahead of packets in other queues.

By configuring the quality of service (QoS), you can provide preferential treatment to specific types of traffic at the expense of other traffic types. Without QoS, the device offers best-effort service for each packet, regardless of the packet contents or size. The device sends the packets without any assurance of reliability, delay bounds, or throughput.

The following are specific features provided by QoS:

- ? Low latency
- ? Bandwidth guarantee
- ? Buffering capabilities and dropping disciplines
- ? Traffic policing
- ? Enables the changing of the attribute of the frame or packet header



- ? Relative services
- ? Modular QoS Command-Line Interface
- ? Supported QoS Features for Wired Access
- ? Hierarchical QoS

#### NEW QUESTION 480

- (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?

- ☐ R1#sh run | include aaa  
aaa new-model  
aaa authentication login default group tacacs+  
aaa session-id common  
  
R1#sh run | section vty  
line vty 0 4  
transport input none  
R1#
- ☐ 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 02050D480809  
  
R1#sh run | include username  
R1#
- ☐ 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#
- ☐ R1#sh run | include aaa  
aaa new-model  
aaa authentication login VTY group tacacs+ none  
aaa session-id common  
  
R1#sh run | section vty  
line vty 0 4  
password 7 02050D480809  
  
R1#sh run | include username  
R1#

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

Answer: B

#### NEW QUESTION 485

- (Topic 2)

An engineer must configure the strongest password authentication to locally authenticate on a router. Which configuration must be used?

- ☐ username netadmin secret 5 \$1\$b1Ju\$kZbBS1Pyh4QzwXyZ1kSZ2
- ☐ username netadmin secret \$1\$b1Ju\$k404850110QzwXyZ1kSZ2
- ☐ line Console 0  
password \$1\$b1Ju\$
- ☐ username netadmin secret 9 \$9\$vFpMf8elb4RVV8\$seZ/bDAx1uV

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

**Answer:** D

**Explanation:**

Scrypt is safer than MD5, so answer A is wrong and answer D is correct  
R1(config)#username user secret ?  
0 Specifies an UNENCRYPTED secret will follow  
5 Specifies a MD5 HASHED secret will follow  
8 Specifies a PBKDF2 HASHED secret will follow  
9 Specifies a SCRYPT HASHED secret will follow  
<0-9> Encryption types not explicitly specified  
LINE The UNENCRYPTED (cleartext) user secret  
LINE The UNENCRYPTED (cleartext) user secret  
Reference: <https://community.cisco.com/t5/networking-documents/understanding-the-differences-between-the-cisco-password-secret/ta-p/3163238>

**NEW QUESTION 489**

- (Topic 2)

A client device roams between wireless LAN controllers that are mobility peers, Both controllers have dynamic interface on the same client VLAN which type of roam is described?

- A. intra-VLAN
- B. inter-controller
- C. intra-controller
- D. inter-subnet

**Answer:** B

**NEW QUESTION 492**

- (Topic 2)

How does the EIGRP metric differ from the OSPF metric?

- A. The EIGRP metric is calculated based on bandwidth onl
- B. The OSPF metric is calculated on delay only.
- C. The EIGRP metric is calculated based on delay onl
- D. The OSPF metric is calculated on bandwidth and delay.
- E. The EIGRP metric Is calculated based on bandwidth and dela
- F. The OSPF metric is calculated on bandwidth only.
- G. The EIGRP metric Is calculated based on hop count and bandwidt
- H. The OSPF metric is calculated on bandwidth and delay.

**Answer:** C

**Explanation:**

By default, EIGRP metric is calculated: metric = bandwidth + delay

While OSPF is calculated by:

OSPF metric = Reference bandwidth / Interface bandwidth in bps

(Or Cisco uses 100Mbps (108) bandwidth as reference bandwidth. With this bandwidth, our equation would be:

Cost = 108/interface bandwidth in bps)

**NEW QUESTION 496**

- (Topic 2)

An engineer configures a WLAN with fast transition enabled Some legacy clients fail to connect to this WLAN Which feature allows the legacy clients to connect while still allowing other clients to use fast transition based on then OLTIs?

- A. over the DS
- B. adaptive R
- C. 802.11V
- D. 802.11k

**Answer:** B

**NEW QUESTION 500**

- (Topic 2)

Which deployment option of Cisco NGFW provides scalability?

- A. tap

- B. clustering
- C. inline tap
- D. high availability

**Answer:** B

**Explanation:**

Clustering lets you group multiple Firepower Threat Defense (FTD) units together as a single logical device. Clustering is only supported for the FTD device on the Firepower 9300 and the Firepower 4100 series. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.}

**NEW QUESTION 501**

- (Topic 2)

Refer to the exhibit.

```
Vlan503 - Group 1
  State is Active
    1 state change, last state change 32w6d
  Virtual IP address is 10.0.3.241
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (vl default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.064 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.3.242, priority 100 (expires in 10.624 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl503-1" (default)
```

Which two facts does the device output confirm? (Choose two.)

- A. The device sends unicast messages to its peers
- B. The device's HSRP group uses the virtual IP address 10.0.3.242
- C. The standby device is configured with the default HSRP priority.
- D. The device is using the default HSRP hello timer
- E. The device is configured with the default HSRP priority

**Answer:** CD

**NEW QUESTION 505**

- (Topic 2)

An engineer must enable a login authentication method that allows a user to log in by using local authentication if all other defined authentication methods fail. Which configuration should be applied?

- A. aaa authentication login CONSOLE group radius local-case enable aaa
- B. authentication login CONSOLE group radius local enable none
- C. aaa authentication login CONSOLE group radius local enable
- D. aaa authentication login CONSOLE group tacacs+ local enable

**Answer:** D

**NEW QUESTION 506**

- (Topic 1)

Which two methods are used to reduce the AP coverage area? (Choose two)

- A. Reduce channel width from 40 MHz to 20 MHz
- B. Disable 2.4 GHz and use only 5 GHz.
- C. Reduce AP transmit power.
- D. Increase minimum mandatory data rate
- E. Enable Fastlane

**Answer:** CD

**NEW QUESTION 509**

- (Topic 1)

What is a characteristic of a next-generation firewall?

- A. only required at the network perimeter
- B. required in each layer of the network
- C. filters traffic using Layer 3 and Layer 4 information only
- D. provides intrusion prevention

**Answer:** D

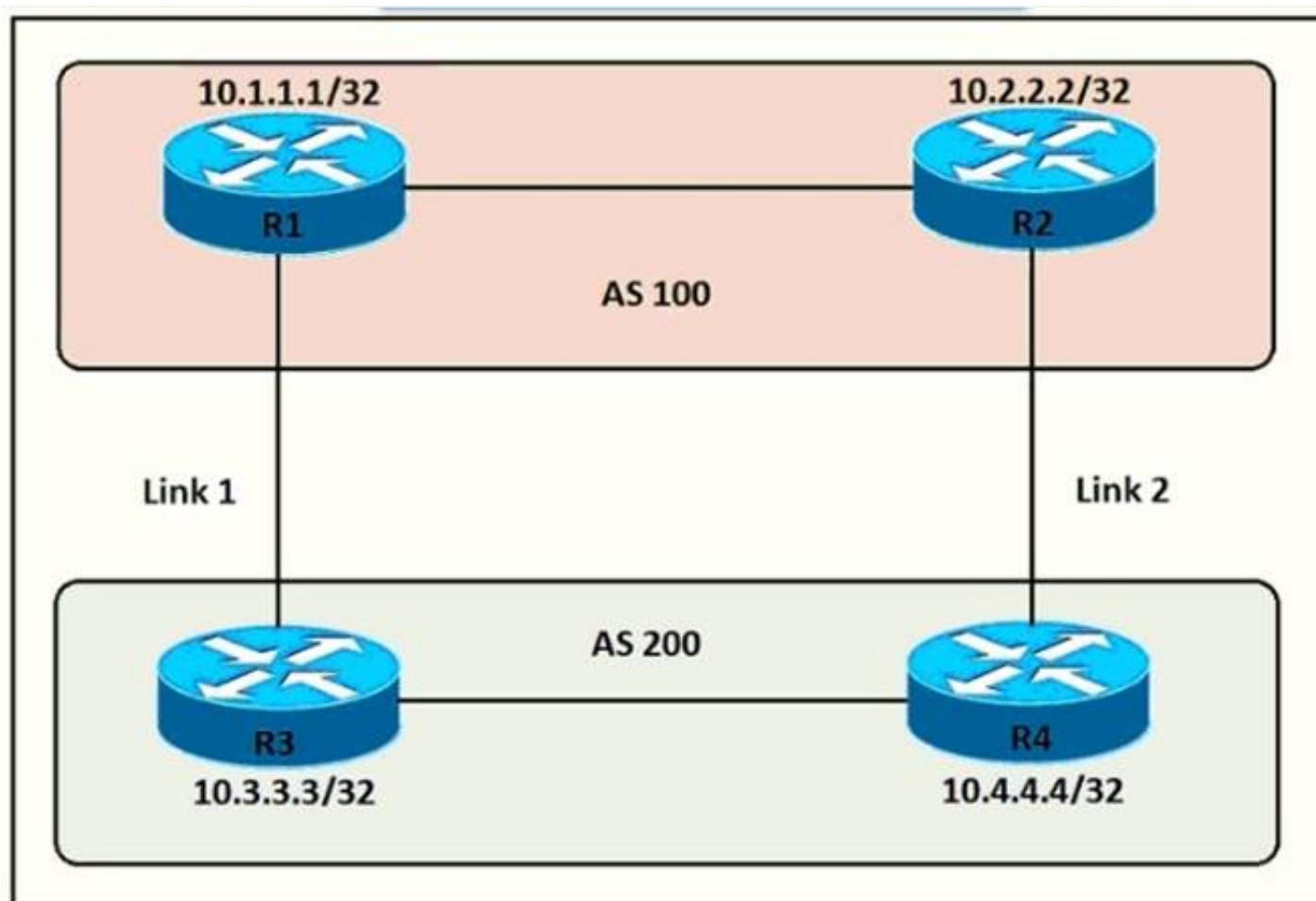
**Explanation:**

The feature set for NGFWs build upon traditional firewall features by including critical security functions like intrusion prevention, VPN, and anti-virus, and even encrypted web traffic inspection to help prevent packets containing malicious content from entering the network

**NEW QUESTION 511**



- (Topic 1)  
Refer to the exhibit.



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

- ☐ R3(config)#route-map PREPEND permit 10  
R3(config-route-map)#set as-path prepend 200 200 200  
  
R3(config)#router bgp 200  
R3(config-router)#neighbor 10.1.1.1 route-map PREPEND out
- ☐ R4(config)#route-map PREPEND permit 10  
R4(config-route-map)#set as-path prepend 100 100 100  
  
R4(config)#router bgp 200  
R4(config-router)#neighbor 10.2.2.2 route-map PREPEND in
- ☐ R3(config)#route-map PREPEND permit 10  
R3(config-route-map)#set as-path prepend 100 100 100  
  
R3(config)#router bgp 200  
R3(config-router)#neighbor 10.1.1.1 route-map PREPEND in
- ☐ R4(config)#route-map PREPEND permit 10  
R4(config-route-map)#set as-path prepend 200 200 200  
  
R4(config)#router bgp 200  
R4(config-router)#neighbor 10.2.2.2 route-map PREPEND out

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 512**

- (Topic 1)

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

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

Answer: A

#### NEW QUESTION 517

- (Topic 1)

Refer to the exhibit.

```

SW2# show run interface gigabitethernet 0/0
Building configuration...
Current configuration : 151 bytes
!
interface GigabitEthernet0/0
switchport trunk encapsulation isl
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
end

SW3# show run interface gigabitethernet 0/1
Building configuration...
Current configuration : 151 bytes
!
interface GigabitEthernet0/1
switchport trunk encapsulation isl
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
end
    
```

The EtherChannel between SW2 and SW3 is not operational which action resolves this issue?

- A. Configure the channel-group mode on SW2 Gi0/1 and Gi0/1 to on.
- B. Configure the channel-group mode on SW3 Gi0/1 to active
- C. Configure the mode on SW2 Gi0/0 to trunk
- D. Configure the mode on SW2 Gi0/1 to access.

Answer: B

#### NEW QUESTION 518

- (Topic 1)

```

<?xml version="1.0" encoding="utf-8"?>
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
    
```

Refer to the exhibit. What does the error message relay to the administrator who is trying to configure a Cisco IOS device?

- A. A NETCONF request was made for a data model that does not exist.
- B. The device received a valid NETCONF request and serviced it without error.
- C. A NETCONF message with valid content based on the YANG data models was made, but the request failed.
- D. The NETCONF running datastore is currently locked.

Answer: A

Explanation:

### 3. Missing Data Model RPC Error Reply Message

If a request is made for a data model that doesn't exist on the Catalyst 3 response. This is expected behavior.



**Tip:** Use the NETCONF capabilities functionality to determine which

```

<?xml version="1.0" encoding="utf-8"?>
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
    
```

Reference: <https://www.cisco.com/c/en/us/support/docs/storage-networking/management/200933-YANG-NETCONF-Configuration-Validation.html>

#### NEW QUESTION 520

- (Topic 1)

Which exhibit displays a valid JSON file?

☐ {  
 "hostname": "edge\_router\_1"  
 "interfaces": {  
 "GigabitEthernet1/1"  
 "GigabitEthernet1/2"  
 "GigabitEthernet1/3"  
 }  
}

☐ {  
 "hostname": "edge\_router\_1",  
 "interfaces": {  
 "GigabitEthernet1/1",  
 "GigabitEthernet1/2",  
 "GigabitEthernet1/3",  
 },  
}

☐ {  
 "hostname": "edge\_router\_1"  
 "interfaces": [  
 "GigabitEthernet1/1"  
 "GigabitEthernet1/2"  
 "GigabitEthernet1/3"  
 ]  
}

☒ {  
 "hostname": "edge\_router\_1",  
 "interfaces": [  
 "GigabitEthernet1/1",  
 "GigabitEthernet1/2",  
 "GigabitEthernet1/3"  
 ]  
}

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

**Answer:** D

#### NEW QUESTION 522

- (Topic 1)

In an SD-Access solution what is the role of a fabric edge node?

- A. to connect external Layer 3- network to the SD-Access fabric
- B. to connect wired endpoint to the SD-Access fabric
- C. to advertise fabric IP address space to external network
- D. to connect the fusion router to the SD-Access fabric

**Answer:** B

#### Explanation:

+ Fabric edge node: This fabric device (for example, access or distribution layer device) connects

#### NEW QUESTION 527

- (Topic 1)



Refer to the exhibit. An engineer is investigating why guest users are able to access other guest user devices when the users are connected to the customer guest WLAN. What action resolves this issue?

- A. implement MFP client protection
- B. implement split tunneling
- C. implement P2P blocking
- D. implement Wi-Fi direct policy

**Answer: C**

**Explanation:**

This control determines whether the Wireless LAN Controller is configured to prevent clients connected to the same Wireless Local Area Controller from communicating with each other.

Wireless Client Isolation prevents wireless clients from communicating with each other over the RF. Packets that arrive on the wireless interface are forwarded only out the wired interface of an Access Point. One wireless client could potentially compromise another client sharing the same wireless network.

**NEW QUESTION 529**

- (Topic 1)

Refer to the exhibit.

```
Router#show ip ospf interface
GigabitEthernet0/1.40 is up, line protocol is up
  Internet Address 10.3.5.254/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
    0          1      no      no      Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 10.3.5.254
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
  No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 172.16.30.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
    0          1      no      no      Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 172.16.30.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
  No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 172.16.11.29/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
    0          1      no      no      Base
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 172.16.11.27, Interface address 172.16.11.27
  Backup Designated router (ID) 172.16.11.30, Interface address 172.16.11.30
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
  Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
```

A network engineer configures OSPF and reviews the router configuration. Which interface or interface or interface are able to establish OSPF adjacency?

- A. GigabitEthernet0/1 and GigabitEthernet0/1.40
- B. only GigabitEthernet0/1
- C. only GigabitEthernet0/0
- D. Gigabit Ethernet0/0 and GigabitEthernet0/1

**Answer:** C

#### NEW QUESTION 534

- (Topic 1)

Which AP mode allows an engineer to scan configured channels for rogue access points?

- A. sniffer
- B. monitor
- C. bridge
- D. local

**Answer:** B

#### NEW QUESTION 535

DRAG DROP - (Topic 1)

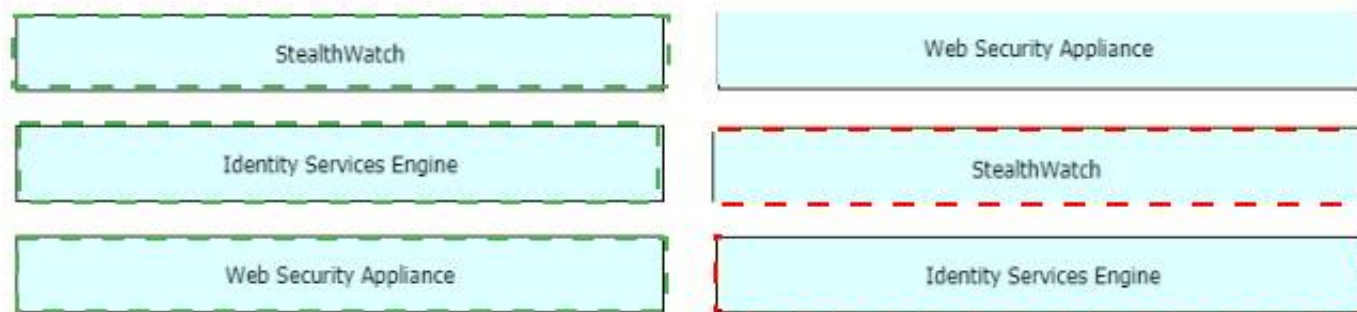
Drag and drop the solutions that comprise Cisco Cyber Threat Defense from the left onto the objectives they accomplish on the right.

|                          |   |
|--------------------------|---|
| StealthWatch             | detects suspicious web activity                 |
| Identity Services Engine | analyzes network behavior and detects anomalies |
| Web Security Appliance   | uses pxGrid to remediate security threats       |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 539**

- (Topic 1)

An engineer is concerned with the deployment of new application that is sensitive to inter- packet delay variance. Which command configures the router to be the destination of jitter measurements?

- A. Router(config)# ip sla responder udp-connect 172.29.139.134 5000
- B. Router(config)# ip sla responder tcp-connect 172.29.139.134 5000
- C. Router(config)# ip sla responder udp-echo 172.29.139.134 5000
- D. Router(config)# ip sla responder tcp-echo 172.29.139.134 5000

**Answer: C**

**Explanation:**

Reference:UDP Jitter measures the delay, delay variation (jitter), corruption, misordering and packet loss by generating periodic UDP traffic. This operation always requires IP SLA responder. The command to enable UDP Jitter Operation is “ip sla responder udp-echo {destination-ip-address} [destination-port]

**NEW QUESTION 542**

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 350-401 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 350-401 Product From:

<https://www.2passeasy.com/dumps/350-401/>

## Money Back Guarantee

### 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 FirstTry
- \* 350-401 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year