Cisco

Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

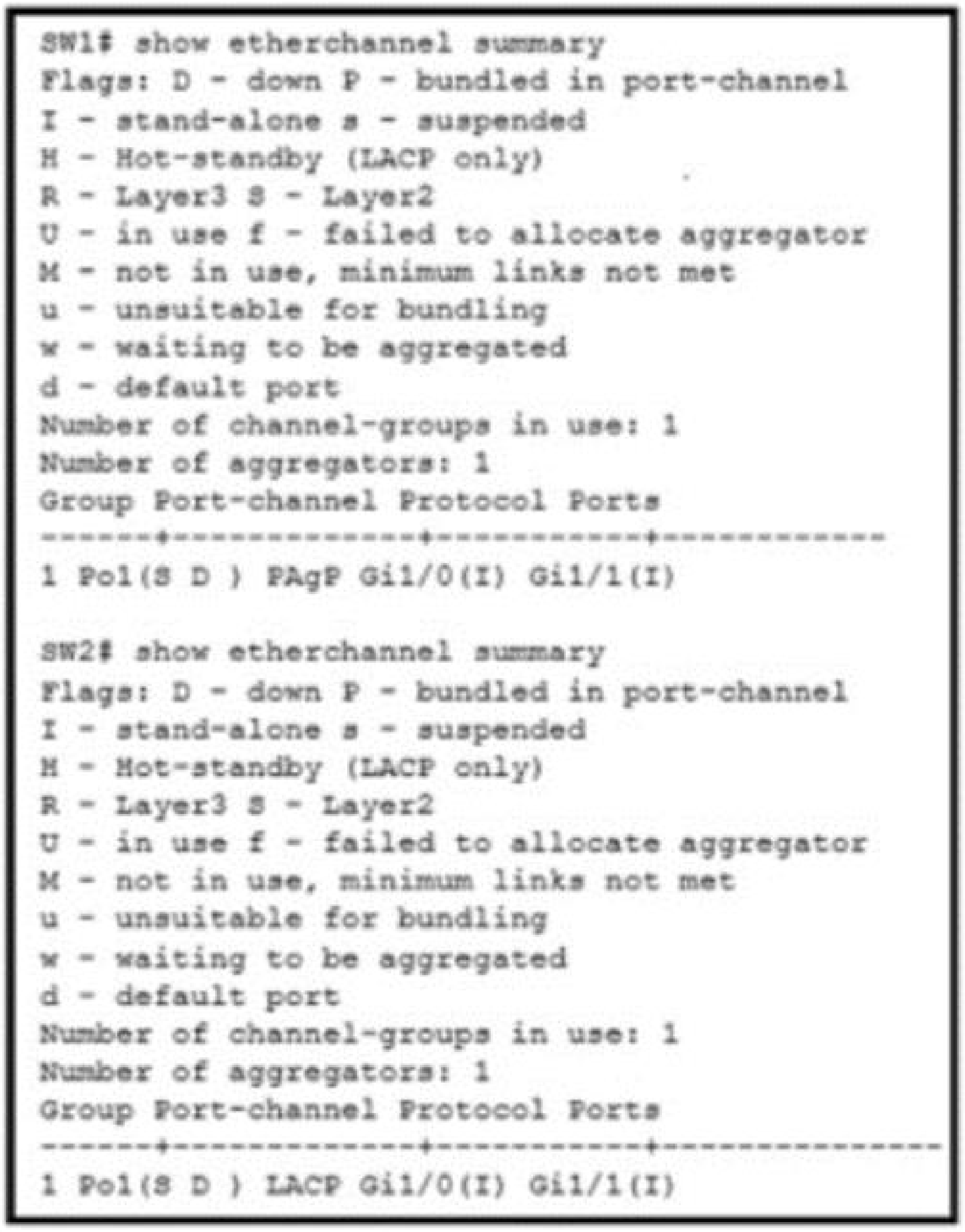
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
- (Topic 4)



```
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)
```

Reler to the exhibit The EtherChannel between SW1 and SW2 is not operational. Which a coon will resolve the issue?

A. Configure channel-group 1 mode active on GVO and G1 1 of SW2.
B. Configure twitchport trunk encapsulation dot1q on SW1 and SW2.
C. Configure channel-group 1 mode active on Gl'O and GM of SW1 .
D. Configure switchport mode dynamic desirable on SW1 and SW2

Answer: C

NEW QUESTION 2
- (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 3
- (Topic 4)
A switch is attached to router R1 on its gig 0/0 interface. Fort security reasons, you want to prevent R1 from sending OSPF hellos to the switch. Which command should be enabled to accomplish this?

A. R1(config-router)#ip ospf hello disable
B. R1(config-router)#ip ospf hello-interval 0
C. R1(config)#passive-interface Gig 0/0
D. R1(config-router)#passive-interface Gig 0/0

Answer: D

NEW QUESTION 4
- (Topic 4)
An engineer must implement a configuration to allow a network administrator to connect to the console port of a router and authenticate over the network. Which

command set should the engineer use?

A. aaa new-modelaaa authentication login default enable
B. aaa new-modelaaa authentication login console local
C. aaa new-model aaa authentication login console group radius
D. aaa new-modelaaa authentication enable default

Answer: B

NEW QUESTION 5
- (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

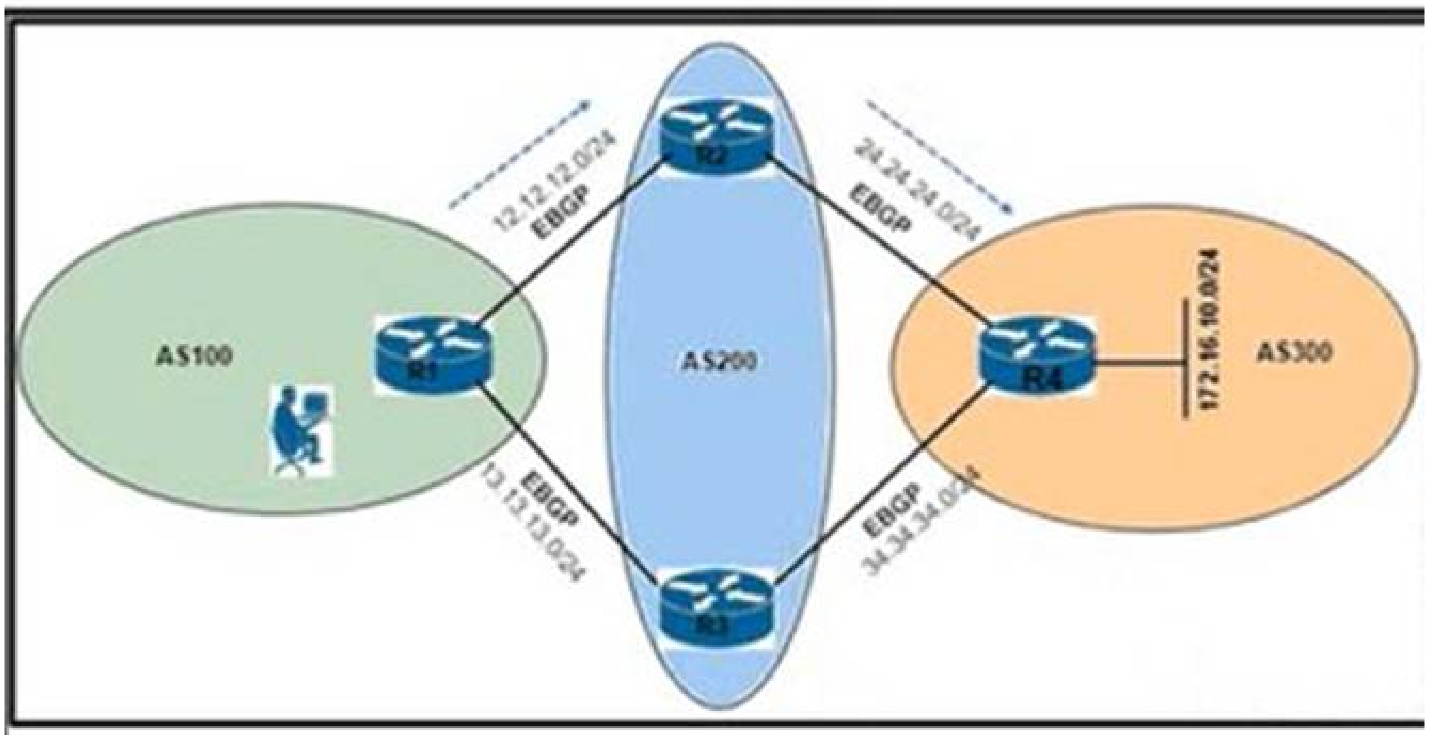
NEW QUESTION 6
- (Topic 4)
A network administrator wants to install new VoIP switches in a small network closet but is concerned about the current heat level of the room. Which of the following should the administrator take into consideration before installing the new equipment?

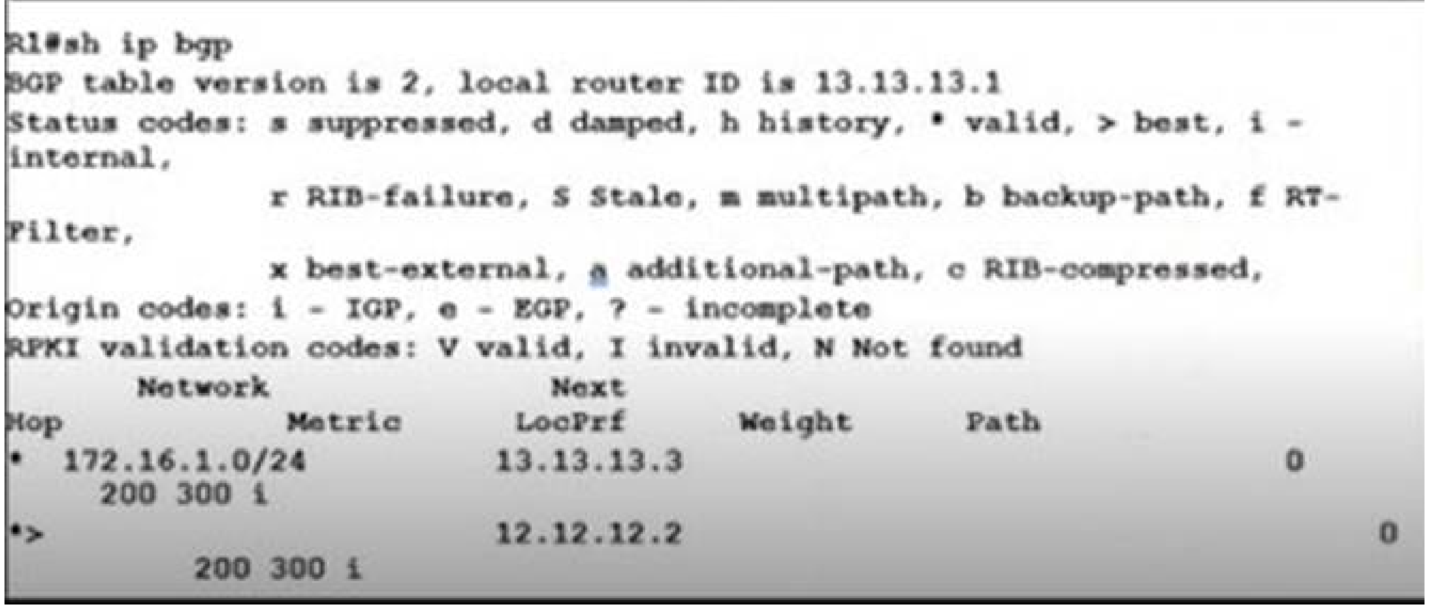
A. The power load of the switches
B. The humidity in the room
C. The fire suppression system
D. The direction of airflow within the switches

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 7
- (Topic 4)

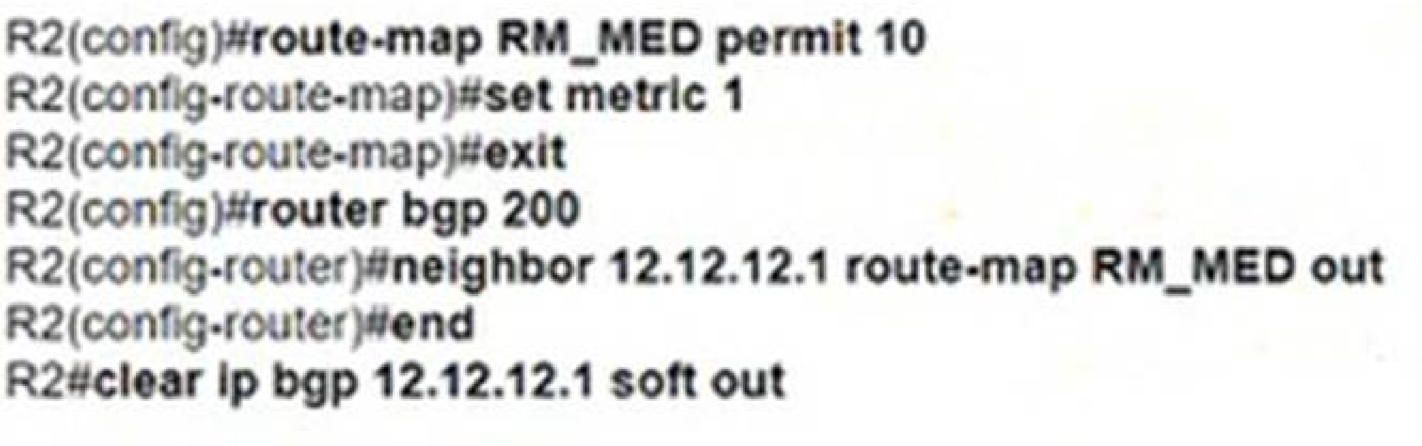




```
R1#sh ip bgp
BGP table version is 2, local router ID is 13.13.13.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin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

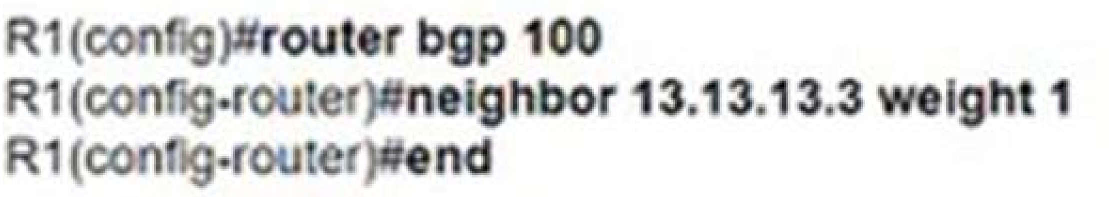
Refer to the exhibit. An engineer is reaching network 172.16.10.0/24 via the R1-R2-R4 path. Which configuration forces the traffic to fake a path of R1-R3-R4?

A)



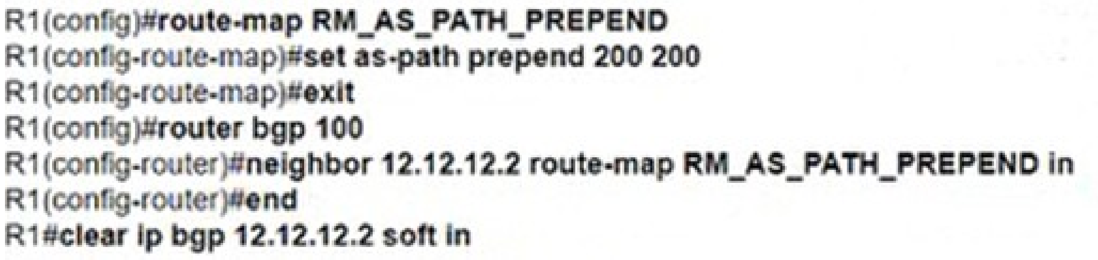
```
R2(config)#route-map RM_MED permit 10
R2(config-route-map)#set metric 1
R2(config-route-map)#exit
R2(config)#router bgp 200
R2(config-router)#neighbor 12.12.12.1 route-map RM_MED out
R2(config-router)#end
R2#clear ip bgp 12.12.12.1 soft out
```

B)



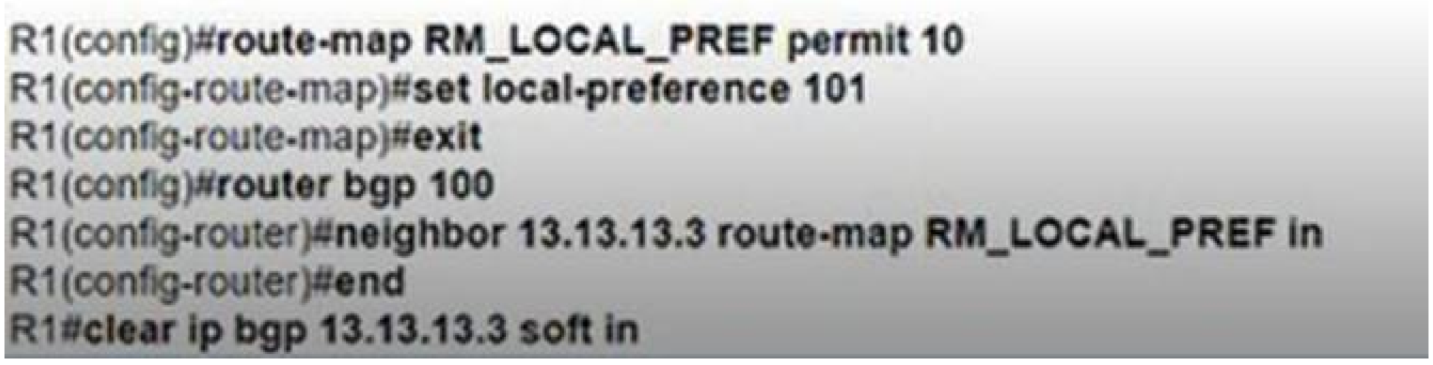
```
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 weight 1
R1(config-router)#end
```

C)



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

D)

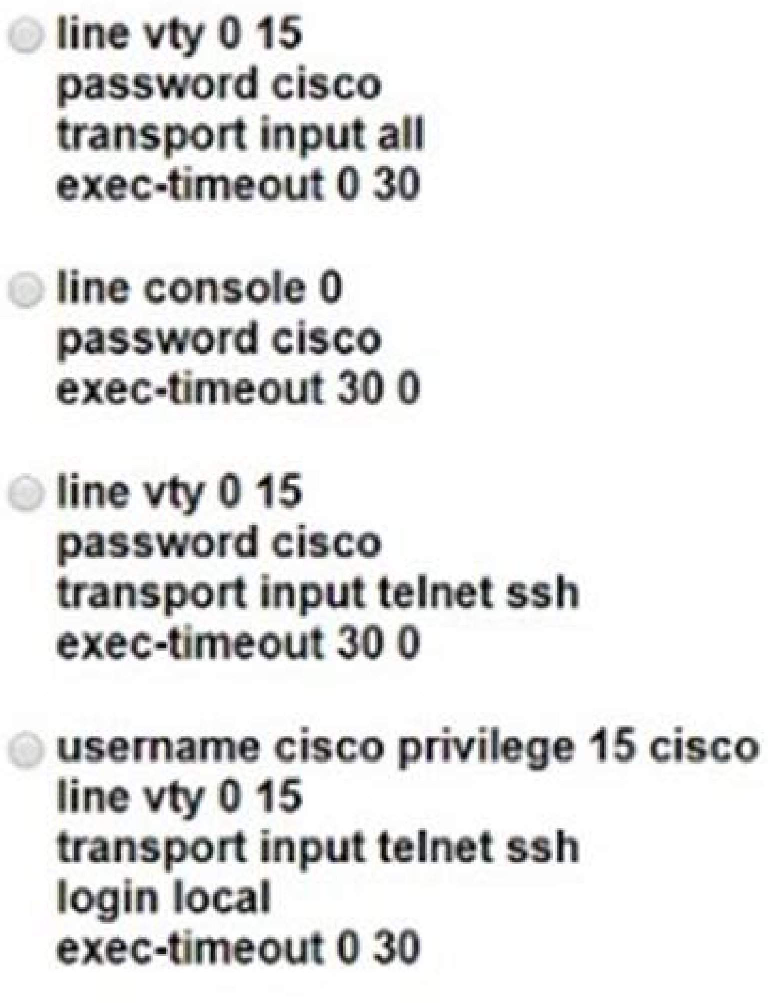


```
R1(config)#route-map RM_LOCAL_PREF permit 10
R1(config-route-map)#set local-preference 101
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 route-map RM_LOCAL_PREF in
R1(config-router)#end
R1#clear ip bgp 13.13.13.3 soft in
```

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

Answer: D

NEW QUESTION 8
- (Topic 4)
A network engineer must configure a switch to allow remote access for all feasible protocols. Only a password must be requested for device authentication and all idle sessions must be terminated in 30 minutes. Which configuration must be applied?



○
```
line vty 0 15
password cisco
transport input all
exec-timeout 0 30
```

○
```
line console 0
password cisco
exec-timeout 30 0
```

○
```
line vty 0 15
password cisco
transport input telnet ssh
exec-timeout 30 0
```

○
```
username cisco privilege 15 cisco
line vty 0 15
transport input telnet ssh
login local
exec-timeout 0 30
```

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

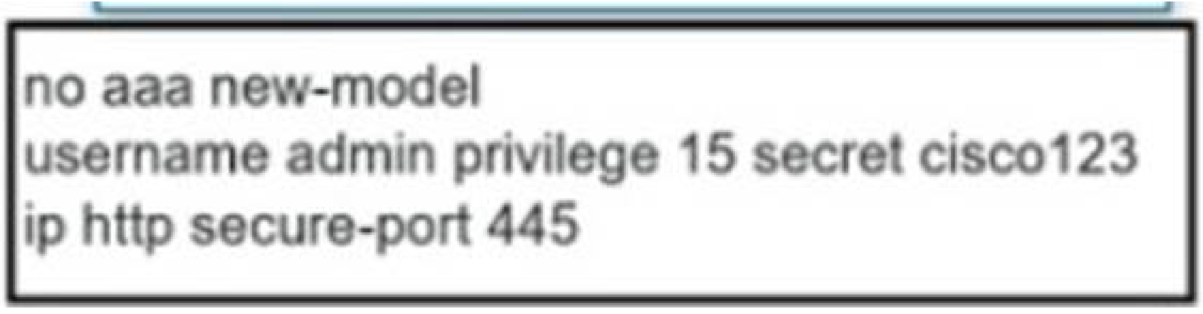
Answer: C

NEW QUESTION 9
- (Topic 4)
Which mechanism can be used to enforce network access authentication against an AAA server if the endpoint does not support the 802.1X supplicant functionality?

A. private VLANs
B. port security
C. MAC Authentication Bypass
D. MACsec

Answer: C

NEW QUESTION 10
- (Topic 4)



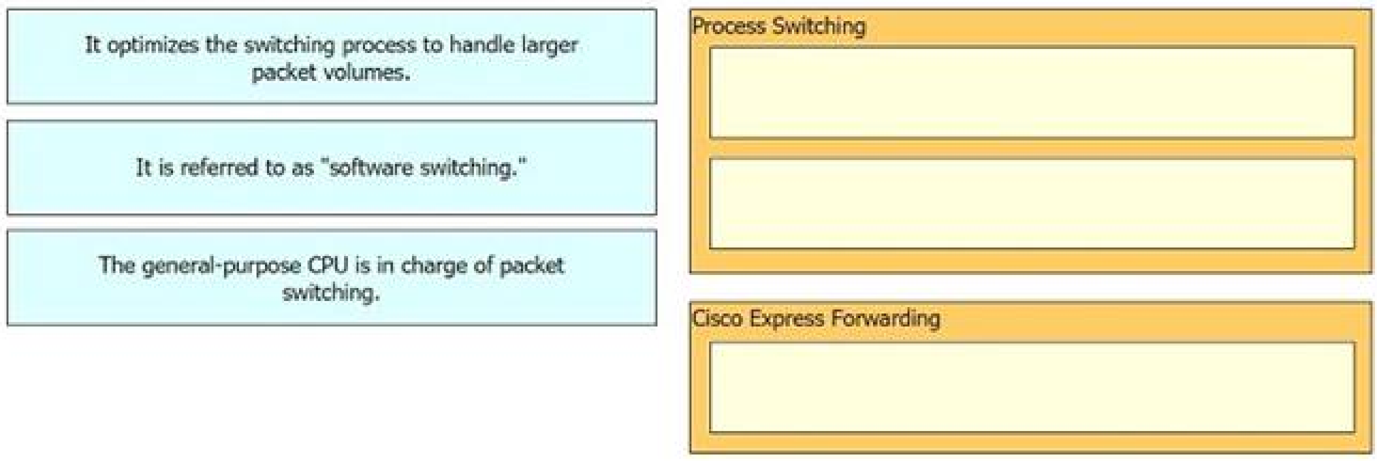
```
no aaa new-model
username admin privilege 15 secret cisco123
ip http secure-port 445
```

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

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

Answer: A

NEW QUESTION 10
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the switching architectures on the right.



It optimizes the switching process to handle larger packet volumes.

It is referred to as "software switching."

The general-purpose CPU is in charge of packet switching.

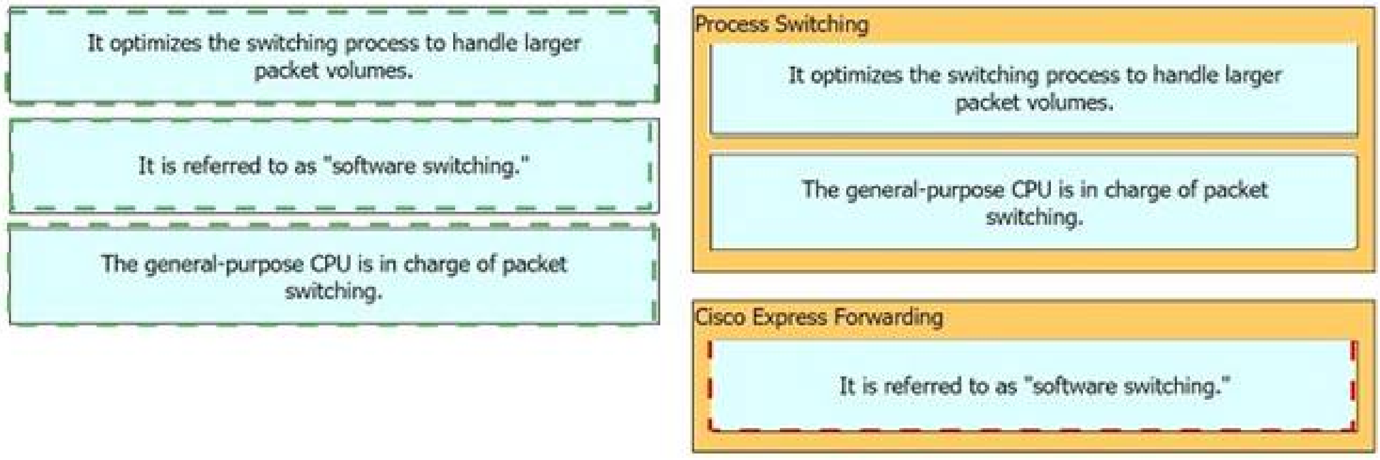
Process Switching

Cisco Express Forwarding

A. Mastered
B. Not Mastered

Answer: A

Explanation:



It optimizes the switching process to handle larger packet volumes.

It is referred to as "software switching."

The general-purpose CPU is in charge of packet switching.

Process Switching

It optimizes the switching process to handle larger packet volumes.

The general-purpose CPU is in charge of packet switching.

Cisco Express Forwarding

It is referred to as "software switching."

NEW QUESTION 14
- (Topic 4)
An engineer must protect the password for the VTY lines against over-the-shoulder attacks. Which configuration should be applied?

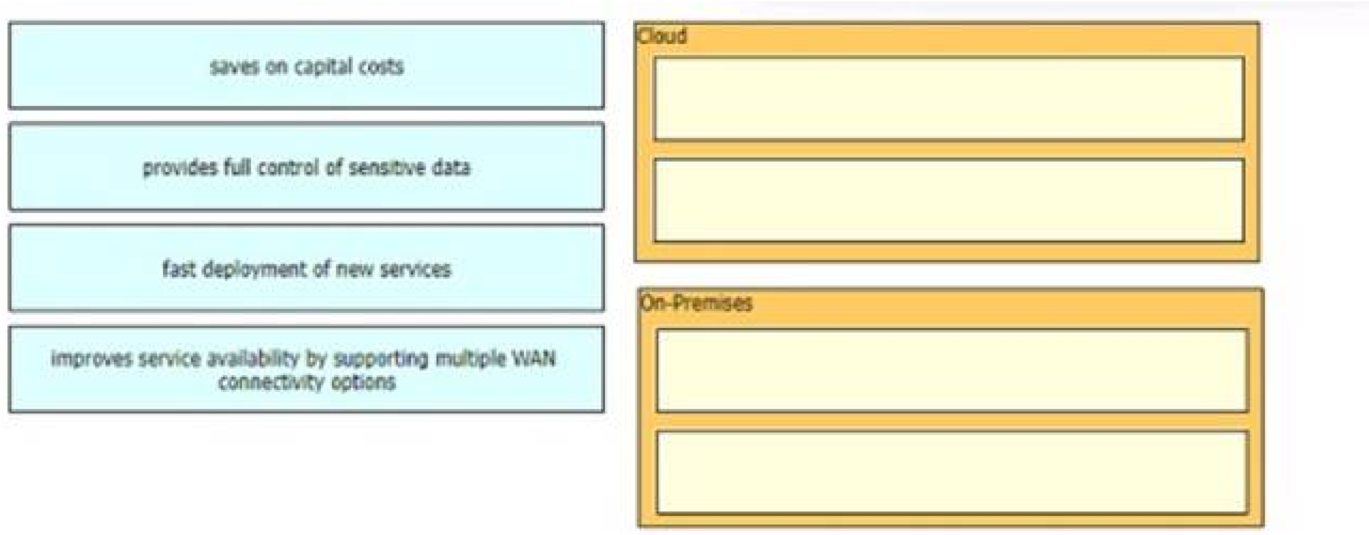
A. service password-encryption
B. username netadmin secret 9 $9$vFpMf8elb4RVV8$seZ/bDA
C. username netadmin secret 7$1$42J36k33008Pyh4QzwXyZ4
D. line vty 0 15 p3ssword XD822j

Answer: A

Explanation:

```
cisco(config)#username test privilege 15 password test777 cisco(config)#do s running-config | include user
username test privilege 15 password 0 test777
cisco(config)#service password-encryption cisco(config)#do s running-config | include user
username test privilege 15 password 7 044F0E151B761B19 cisco(config)#
cisco(config)#do wr
Building configuration... [OK]
cisco(config)#
```

NEW QUESTION 19
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the deployment model on the right.



saves on capital costs

provides full control of sensitive data

fast deployment of new services

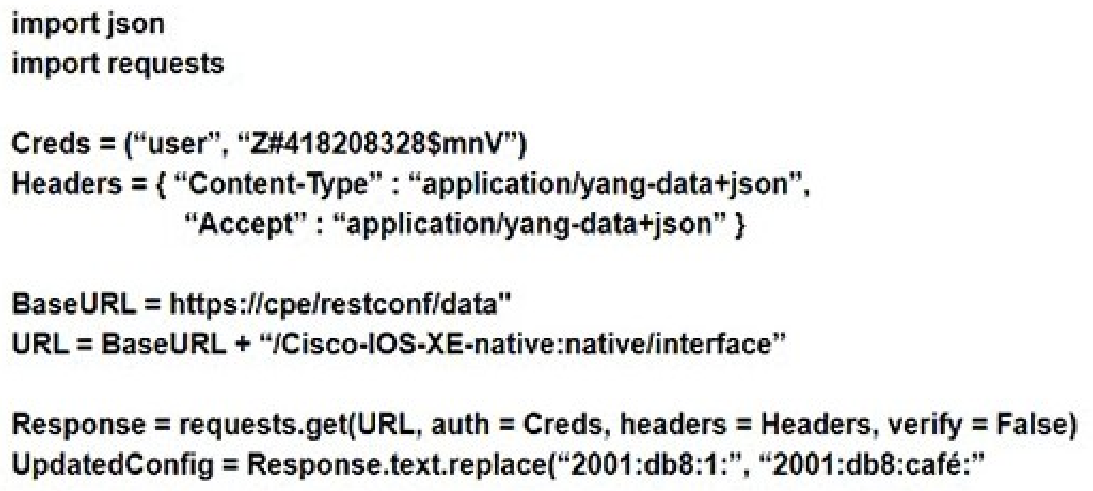
improves service availability by supporting multiple WAN connectivity options

A. Mastered
B. Not Mastered

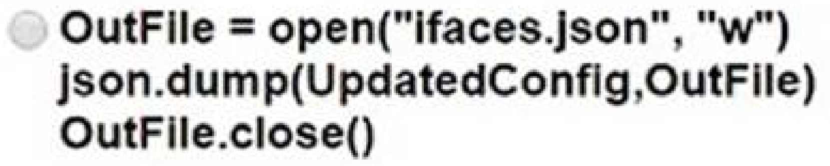
Answer: A

Explanation:
CLOUD1 and 3ON-PREMISES2 and 4

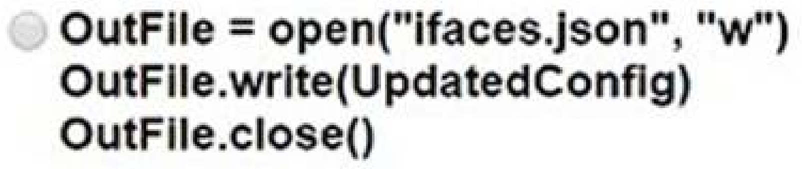
NEW QUESTION 21
- (Topic 4)
Which Python code snippet must be added to the script to store the changed interface configuration to a local JSON-formatted file?



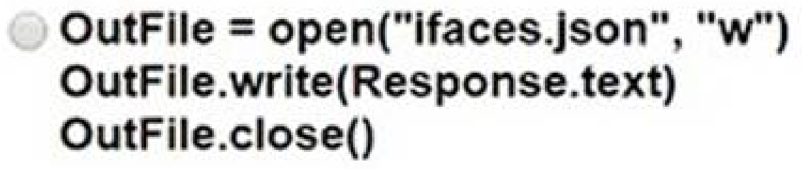
```
import json
import requests

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

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

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



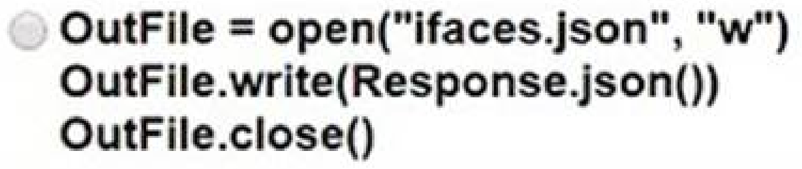
```
○ OutFile = open("ifaces.json", "w")
  json.dump(UpdatedConfig,OutFile)
  OutFile.close()
```



```
○ OutFile = open("ifaces.json", "w")
  OutFile.write(UpdatedConfig)
  OutFile.close()
```



```
○ OutFile = open("ifaces.json", "w")
  OutFile.write(Response.text)
  OutFile.close()
```



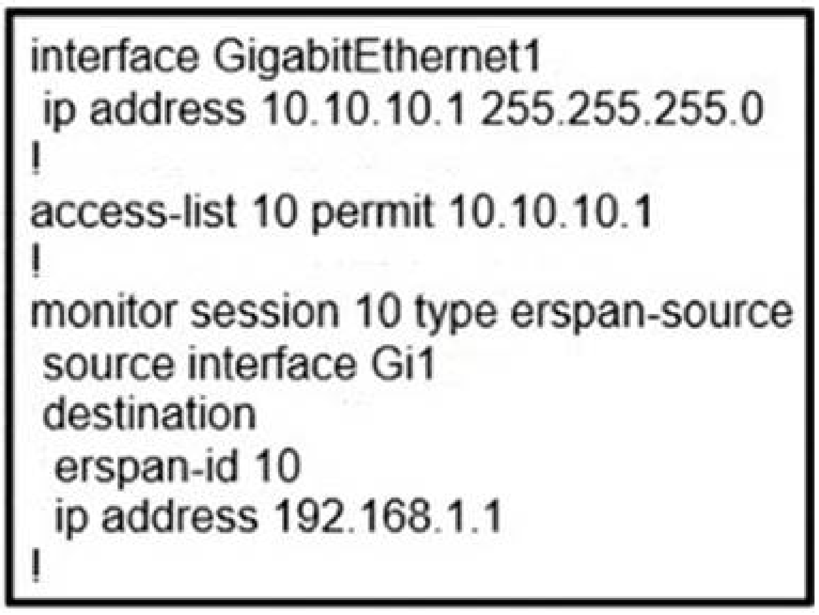
```
○ OutFile = open("ifaces.json", "w")
  OutFile.write(Response.json())
  OutFile.close()
```

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

Answer: B

NEW QUESTION 24

- (Topic 4)



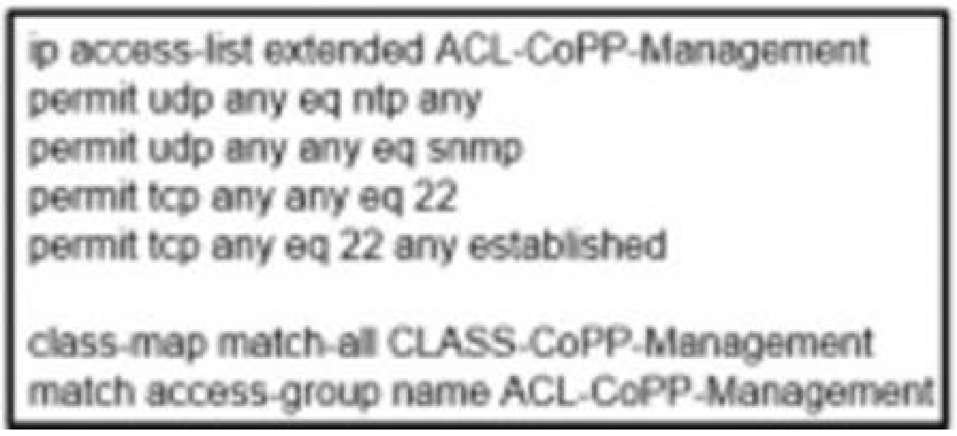
```
interface GigabitEthernet1
 ip address 10.10.10.1 255.255.255.0
!
access-list 10 permit 10.10.10.1
!
monitor session 10 type erspan-source
 source interface Gi1
 destination
  erspan-id 10
  ip address 192.168.1.1
!
```

Refer to the exhibit. Which command filters the ERSPAN session packets only to interface GigabitEthernet1?

A. source ip 10.10.10.1
B. source interface gigabitethernet1 ip 10.10.10.1
C. filter access-group 10
D. destination ip 10.10.10.1

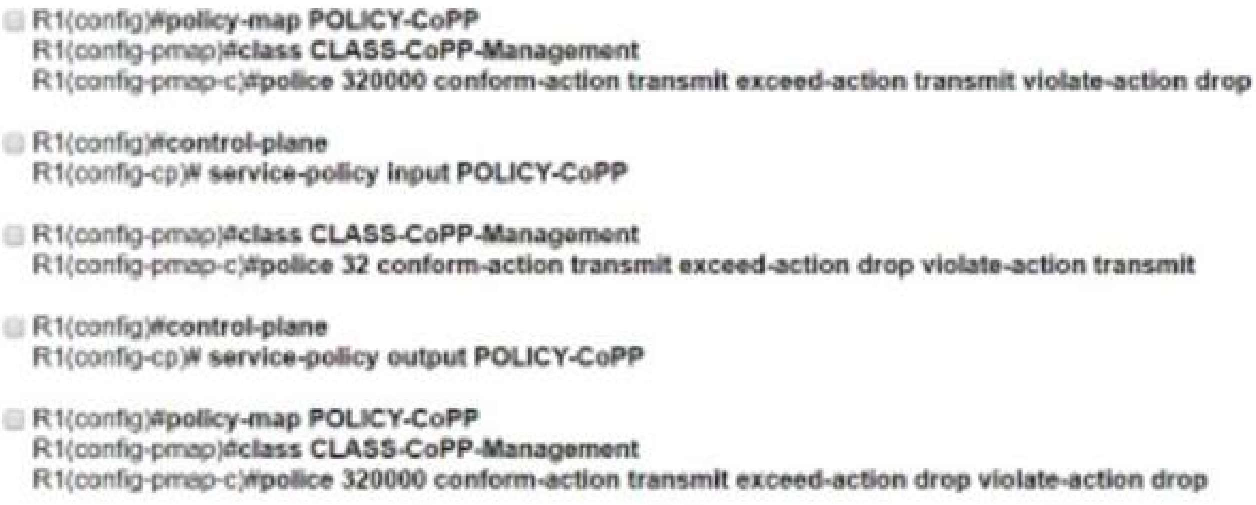
Answer: C

NEW QUESTION 28
- (Topic 4)



```
ip access-list extended ACL-CoPP-Management
permit udp any eq ntp any
permit udp any any eq snmp
permit tcp any any eq 22
permit tcp any eq 22 any established

class-map match-all CLASS-CoPP-Management
match access-group name ACL-CoPP-Management
```

Refer to the exhibit. An engineer must protect the CPU of the router from high rates of NTP, SNMP, and SSH traffic. Which two configurations must be applied to drop these types of traffic when it continuously exceeds 320 kbps? (Choose two)



```
□ R1(config)#policy-map POLICY-CoPP
  R1(config-pmap)#class CLASS-CoPP-Management
  R1(config-pmap-c)#police 320000 conform-action transmit exceed-action transmit violate-action drop

□ R1(config)#control-plane
  R1(config-cp)# service-policy input POLICY-CoPP

□ R1(config-pmap)#class CLASS-CoPP-Management
  R1(config-pmap-c)#police 32 conform-action transmit exceed-action drop violate-action transmit

□ R1(config)#control-plane
  R1(config-cp)# service-policy output POLICY-CoPP

□ R1(config)#policy-map POLICY-CoPP
  R1(config-pmap)#class CLASS-CoPP-Management
  R1(config-pmap-c)#police 320000 conform-action transmit exceed-action drop violate-action drop
```

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

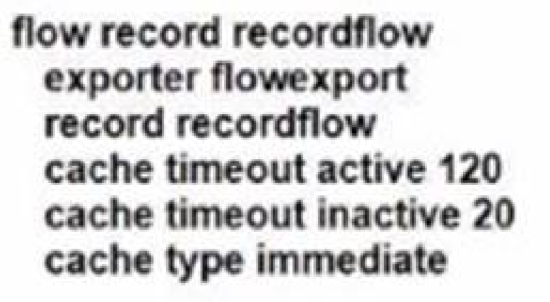
Answer: BE

NEW QUESTION 29
- (Topic 4)
What is the rose of the vSmart controller in a Cisco SD-WN environment?

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

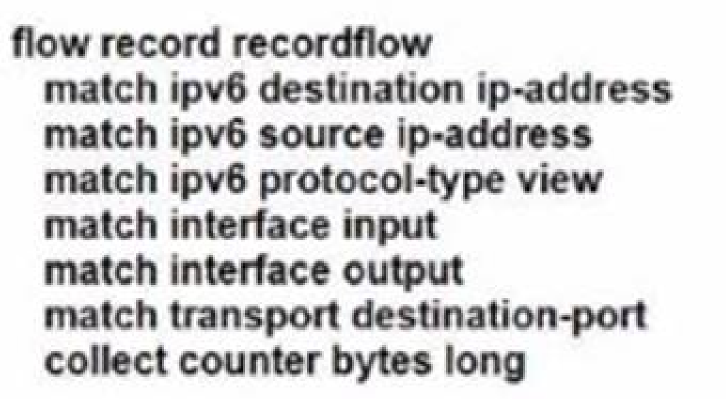
Answer: B

NEW QUESTION 32
- (Topic 4)
An engineer must use flexible NetFlow on a group of switches. To prevent overloading of the flow collector, if the flow is idle for 20 seconds, the flow sample should be exported. Which command set should be applied?
A)



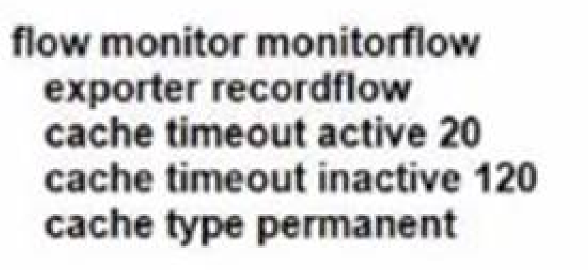
```
flow record recordflow
  exporter flowexport
  record recordflow
  cache timeout active 120
  cache timeout inactive 20
  cache type immediate
```

B)



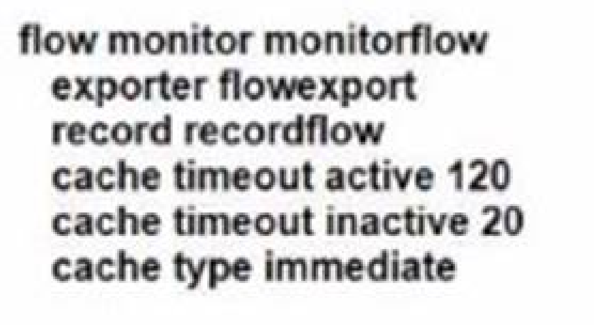
```
flow record recordflow
  match ipv6 destination ip-address
  match ipv6 source ip-address
  match ipv6 protocol-type view
  match interface input
  match interface output
  match transport destination-port
  collect counter bytes long
```

C)



```
flow monitor monitorflow
  exporter recordflow
  cache timeout active 20
  cache timeout inactive 120
  cache type permanent
```

D)



```
flow monitor monitorflow
  exporter flowexport
  record recordflow
  cache timeout active 120
  cache timeout inactive 20
  cache type immediate
```

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

Answer: C

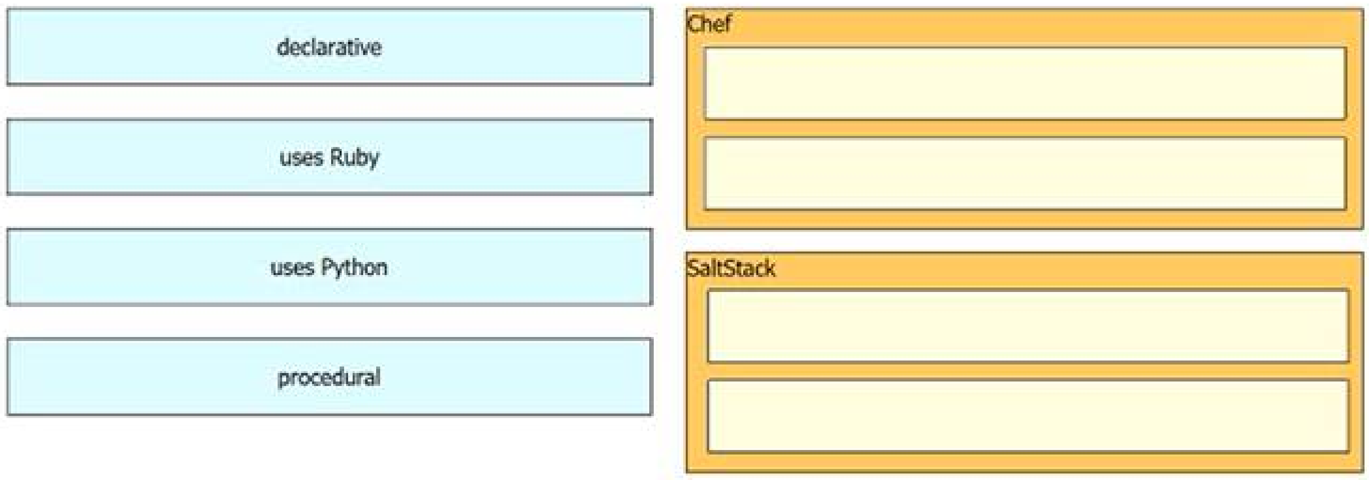
Explanation:
Option C is the correct set of commands to apply flexible NetFlow on a group of switches with the given requirement. The configuration steps are as follows12:
? Define a flow record that specifies the fields to be collected and exported for the flows. In this case, the flow record is named FNF-RECORD and it collects the source and destination IP addresses, the input and output interfaces, the transport protocol, and the source and destination port numbers: flow record FNF-RECORD and match ipv4 source address, match ipv4 destination address, match interface input, match interface output, match transport protocol, match transport source-port, match transport destination-port.
? Define a flow exporter that specifies the destination and transport protocol for sending the flow data. In this case, the flow exporter is named FNF- EXPORTER and it uses UDP port 9996 to send the flow data to the IP address 10.10.10.10: flow exporter FNF-EXPORTER and destination 10.10.10.10, transport udp 9996.
? Define a flow monitor that applies the flow record and the flow exporter to the monitored traffic. In this case, the flow monitor is named FNF-MONITOR and it uses the flow record FNF-RECORD and the flow exporter FNF-EXPORTER. It also sets the cache timeout for inactive flows to 20 seconds, which means that the flow sample will be exported if the flow is idle for 20 seconds: flow monitor FNF-
MONITOR and record FNF-RECORD, exporter FNF-EXPORTER, cache timeout inactive 20.
? Apply the flow monitor to the interfaces that need to be monitored. In this case, the flow monitor FNF-MONITOR is applied to the input and output direction of the interface GigabitEthernet0/1: interface GigabitEthernet0/1 and ip flow monitor FNF-MONITOR input, ip flow monitor FNF-MONITOR output.
Option A is incorrect because it does not set the cache timeout for inactive flows to 20 seconds, which is required by the question. The default cache timeout for inactive flows is 15 seconds1.
Option B is incorrect because it does not apply the flow monitor to the output direction of the interface, which is required to capture both incoming and outgoing traffic on the interface1.
Option D is incorrect because it does not use a flow record to specify the fields to be collected and exported for the flows, which is required to customize the flow data according to the user’s needs1. References: 1: Configuring Flexible NetFlow, 2: Flexible NetFlow Configuration Guide

NEW QUESTION 33
- (Topic 4)
A wireless administrator must create a new web authentication corporate SSID that will be using ISE as the external RADIUS server. The guest VLAN must be specified after the authentication completes. Which action must be performed to allow the ISE server to specify the guest VLAN?

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

Answer: C

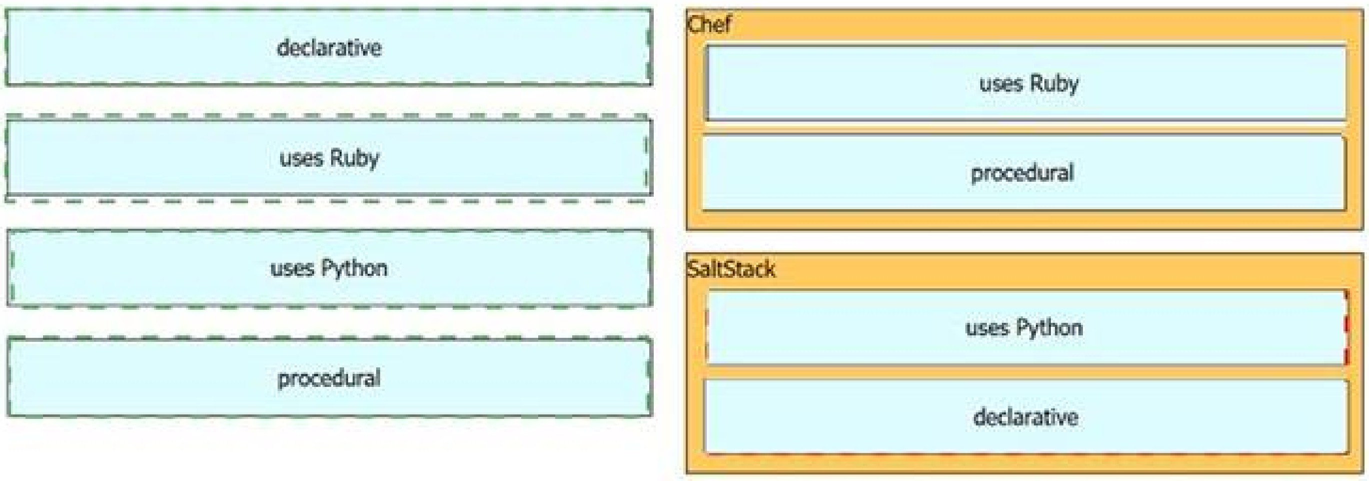
NEW QUESTION 36
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 39
- (Topic 4)
When does a Cisco StackWise primary switch lose its role?

A. when a stack member fails
B. when the stack primary is reset
C. when a switch with a higher priority is added to the stack
D. when the priority value of a stack member is changed to a higher value

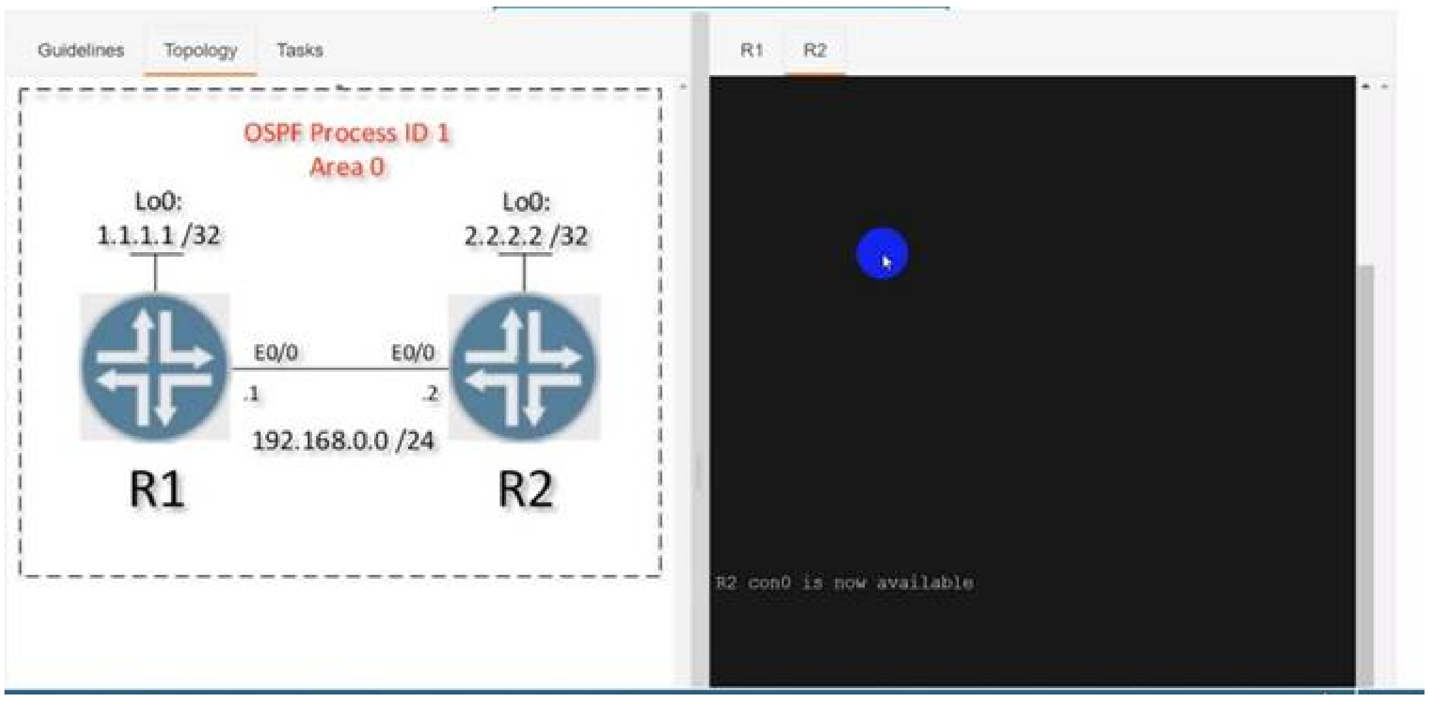
Answer: C

NEW QUESTION 42
- (Topic 4)
Which solution should be used in a high-density wireless environment to increase bandwidth for each user?

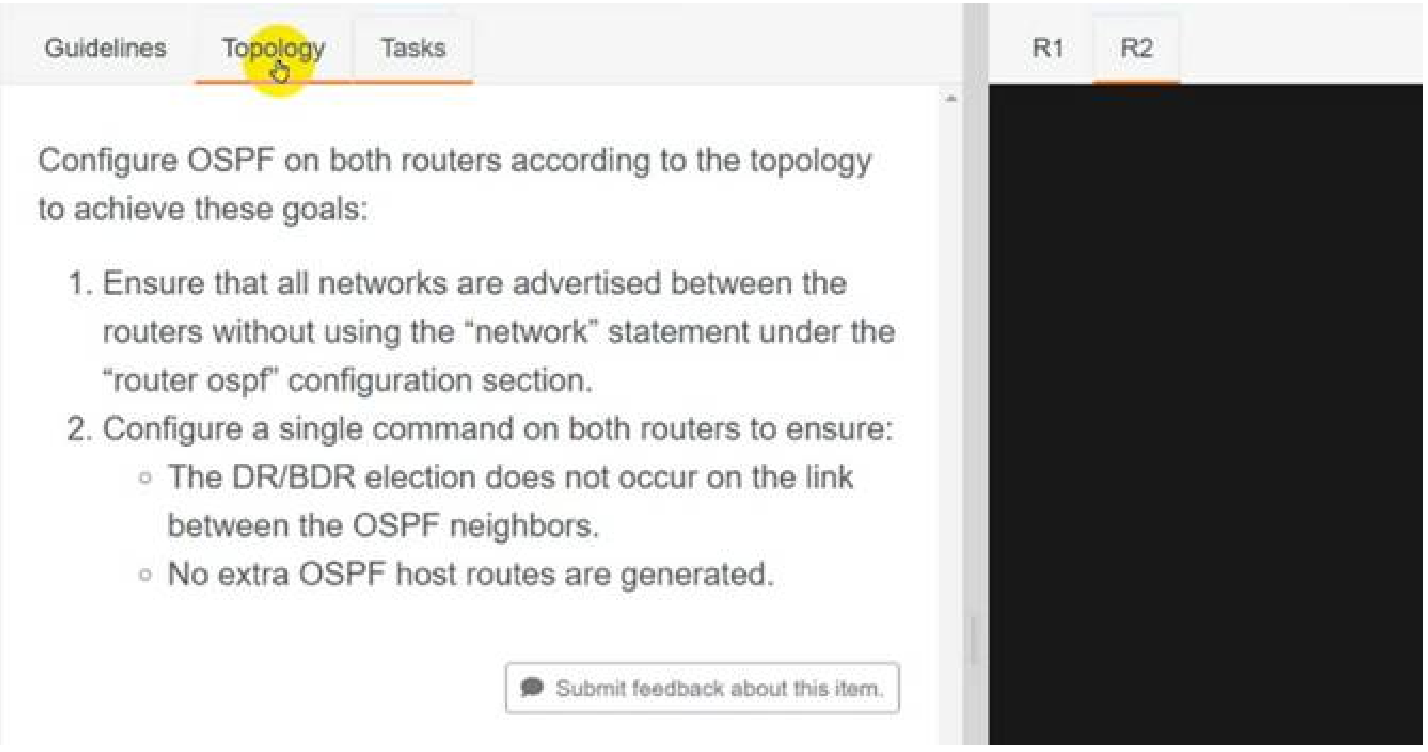
A. Increase antenna size
B. Increase the mandatory minimum data rate.
C. Increase the cell size of each AP.
D. Increase TX power.

Answer: B

NEW QUESTION 45
SIMULATION - (Topic 4)
Simulation 04



```
R2 con0 is now available
```



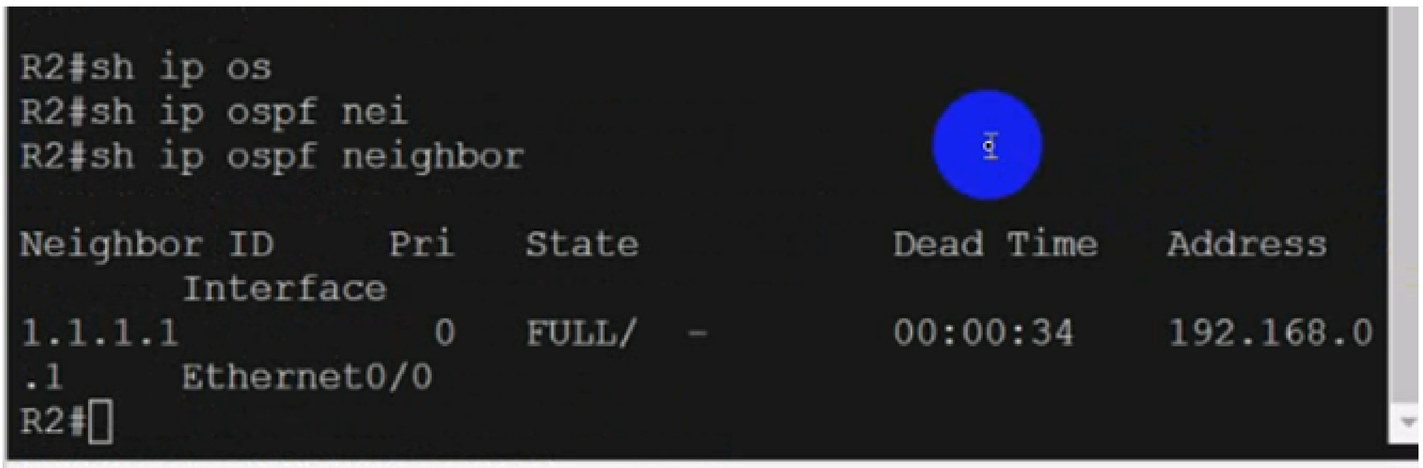
Configure OSPF on both routers according to the topology to achieve these goals:

1. Ensure that all networks are advertised between the routers without using the “network” statement under the “router ospf” configuration section.
2. Configure a single command on both routers to ensure:
   - The DR/BDR election does not occur on the link between the OSPF neighbors.
   - No extra OSPF host routes are generated.

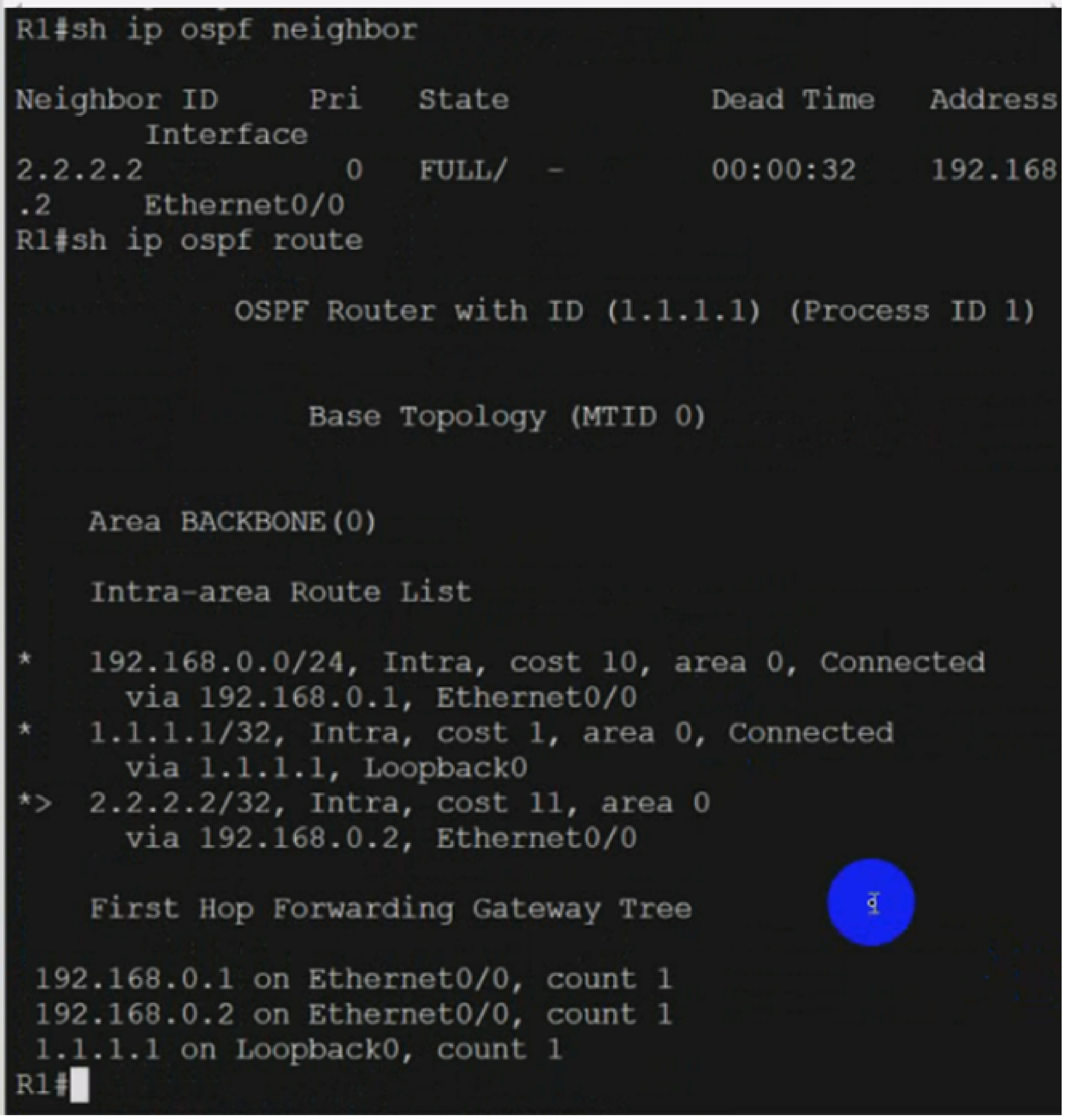
A. Mastered
B. Not Mastered

Answer: A

Explanation:
R1
Router ospf 1 Int loop0
Ip ospf 1 area 0 Int et0/0
Ip ospf 1 area 0
Ip ospf network point-to-point Copy run start
R2
Router ospf 1 Int loop0
Ip ospf 1 area 0 Int et0/0
Ip ospf 1 area 0
Ip ospf network point-to-point Copy run start
Verification:-



```
R2#sh ip os
R2#sh ip ospf nei
R2#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
        Interface
1.1.1.1           0   FULL/  -        00:00:34    192.168.0
.1      Ethernet0/0
R2#
```



```
R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
        Interface
2.2.2.2           0   FULL/  -        00:00:32    192.168
.2      Ethernet0/0
R1#sh ip ospf route

            OSPF Router with ID (1.1.1.1) (Process ID 1)


                Base Topology (MTID 0)


    Area BACKBONE(0)

    Intra-area Route List

*   192.168.0.0/24, Intra, cost 10, area 0, Connected
      via 192.168.0.1, Ethernet0/0
*   1.1.1.1/32, Intra, cost 1, area 0, Connected
      via 1.1.1.1, Loopback0
*>  2.2.2.2/32, Intra, cost 11, area 0
      via 192.168.0.2, Ethernet0/0

    First Hop Forwarding Gateway Tree

 192.168.0.1 on Ethernet0/0, count 1
 192.168.0.2 on Ethernet0/0, count 1
 1.1.1.1 on Loopback0, count 1
R1#
```

NEW QUESTION 50
- (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, white the routing protocol reconverges.
D. It enables HSRP to failover to the standby RP on the same device.

Answer: D

NEW QUESTION 54
- (Topic 4)
Where in Cisco DNA Center is documentation of each API call, organized by its functional area?

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

Answer: A

Explanation:

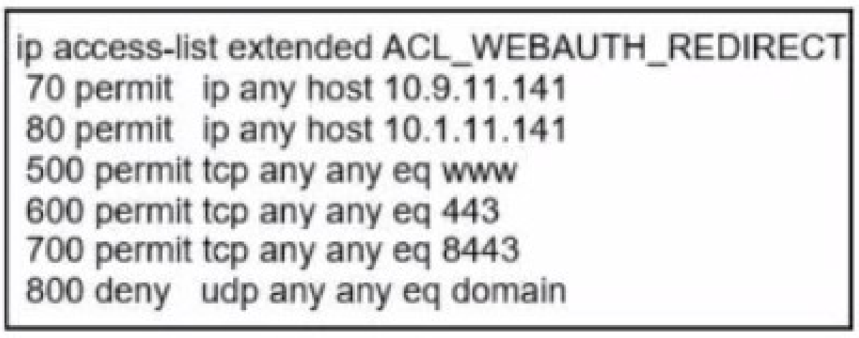
https://developer.cisco.com/docs/dna-center/#!api-quick-start/cisco-dna-center-platform-api-overview

NEW QUESTION 57

- (Topic 4)

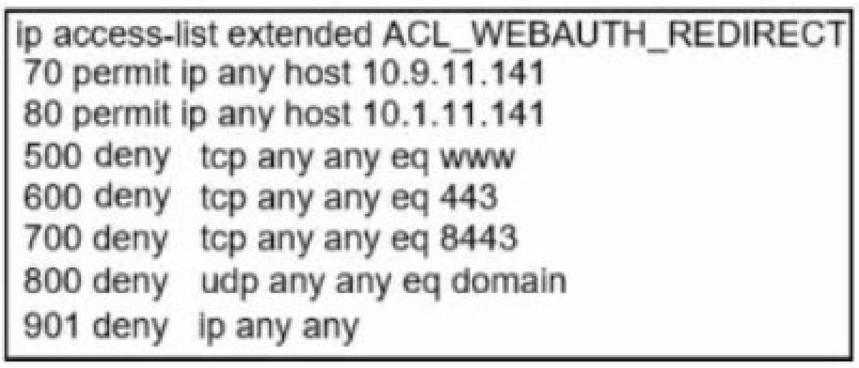
An engineer must construct an access list tot a Cisco Catalyst 9800 Series WLC that will - edirect wireless guest users to a splash page that is hosted on a Cisco ISE server. The Cisco ISE servers are hosted at 10.9.11.141 and 10.1.11.141. Which access list meets the requirements?

A)



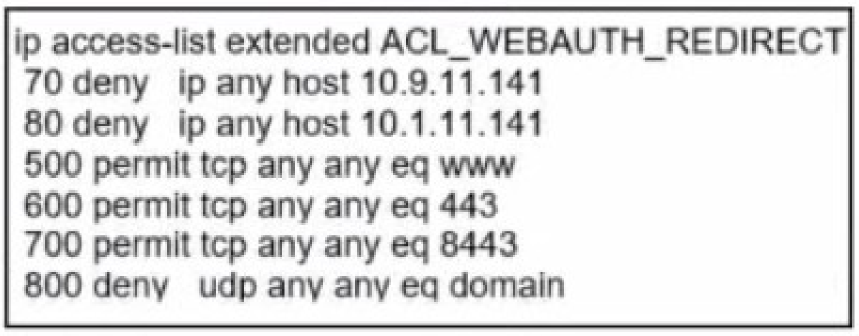
```
ip access-list extended ACL_WEBAUTH_REDIRECT
 70 permit   ip any host 10.9.11.141
 80 permit   ip any host 10.1.11.141
 500 permit tcp any any eq www
 600 permit tcp any any eq 443
 700 permit tcp any any eq 8443
 800 deny   udp any any eq domain
```

B)



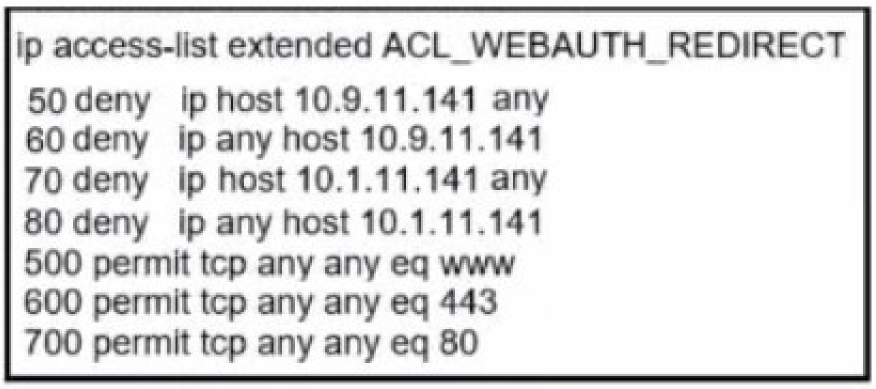
```
ip access-list extended ACL_WEBAUTH_REDIRECT
 70 permit ip any host 10.9.11.141
 80 permit ip any host 10.1.11.141
 500 deny   tcp any any eq www
 600 deny   tcp any any eq 443
 700 deny   tcp any any eq 8443
 800 deny   udp any any eq domain
 901 deny   ip any any
```

C)



```
ip access-list extended ACL_WEBAUTH_REDIRECT
 70 deny   ip any host 10.9.11.141
 80 deny   ip any host 10.1.11.141
 500 permit tcp any any eq www
 600 permit tcp any any eq 443
 700 permit tcp any any eq 8443
 800 deny   udp any any eq domain
```

D)



```
ip access-list extended ACL_WEBAUTH_REDIRECT
 50 deny   ip host 10.9.11.141 any
 60 deny   ip any host 10.9.11.141
 70 deny   ip host 10.1.11.141 any
 80 deny   ip any host 10.1.11.141
 500 permit tcp any any eq www
 600 permit tcp any any eq 443
 700 permit tcp any any eq 80
```

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

Answer: D

Explanation:
Option D is the correct access list to redirect wireless guest users to a splash page that is hosted on a Cisco ISE server. The configuration steps are as follows12:
? Define an extended access list that permits TCP traffic from any source to the Cisco ISE servers on port 80 (HTTP) and port 443 (HTTPS). In this case, the access list is named ACL_WEBAUTH_REDIRECT and it allows any host to connect to the IP addresses 10.9.11.141 and 10.1.11.141 on port 80 and port 443: ip access-list extended ACL_WEBAUTH_REDIRECT and permit tcp any host 10.9.11.141 eq 80, permit tcp any host 10.9.11.141 eq 443, permit tcp any host 10.1.11.141 eq 80, permit tcp any host 10.1.11.141 eq 443.
? Apply the access list to the guest WLAN using the ip access-group command. This command filters the traffic on the interface based on the access list. In this case, the access list ACL_WEBAUTH_REDIRECT is applied to the guest WLAN interface in the inbound direction, which means that only the traffic that matches the access list can enter the interface: interface wlan-guest and ip access-group ACL_WEBAUTH_REDIRECT in.
Option A is incorrect because it does not permit TCP traffic to the Cisco ISE servers on port 80, which is required for HTTP redirection. Without this, the guest users will not be able to see the splash page on their web browsers12.
Option B is incorrect because it does not permit TCP traffic to the Cisco ISE servers on port 443, which is required for HTTPS redirection. Without this, the guest users will not be able to see the splash page on their web browsers if they use HTTPS12.
Option C is incorrect because it permits TCP traffic from any source to any destination on port 80 and port 443, which is too broad and may allow unwanted traffic to enter the guest WLAN interface. This may compromise the security and performance of the guest network12. References: 1: Configuring Web Authentication, 2: ISE and Catalyst 9800 Series Integration Guide

NEW QUESTION 58

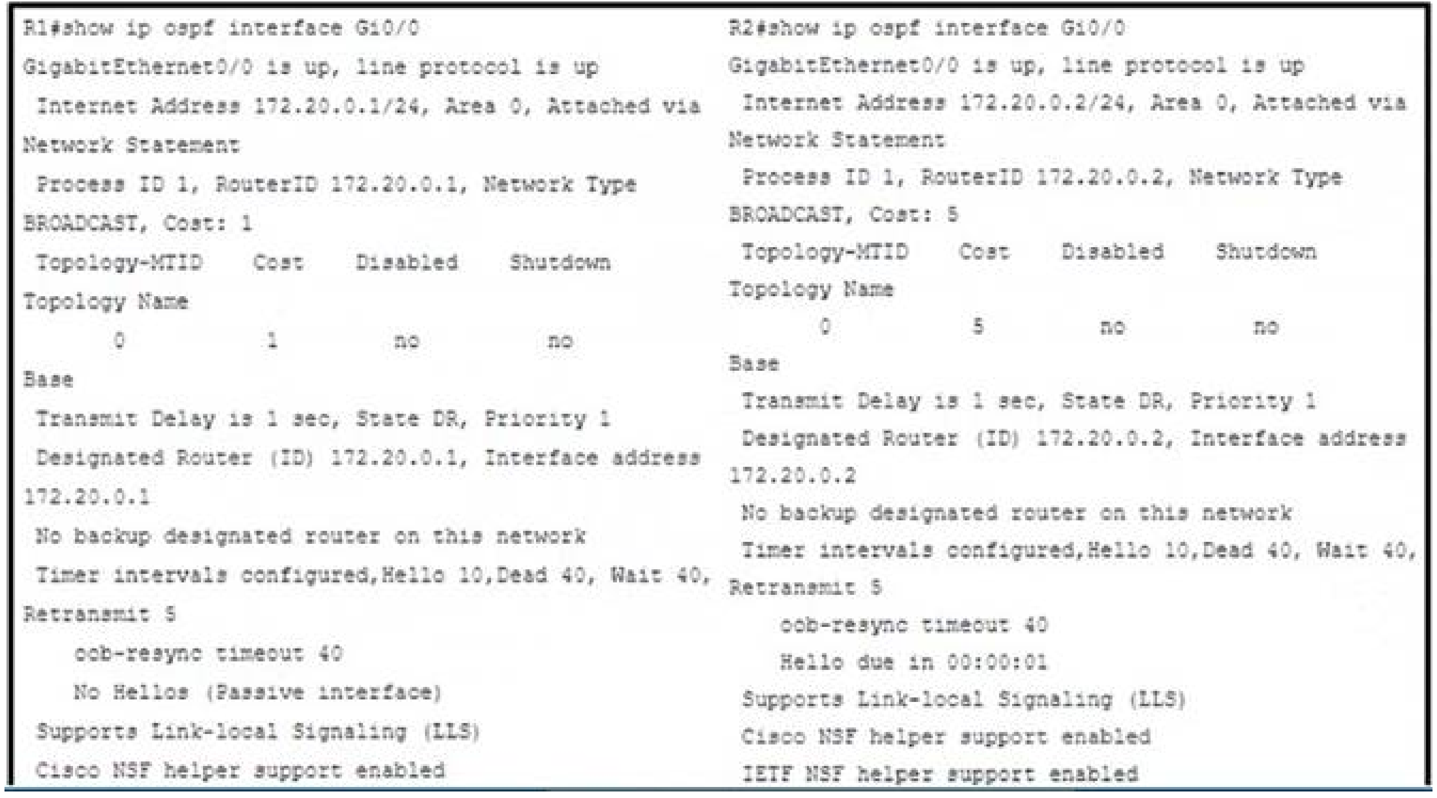
- (Topic 4)

How does Protocol Independent Multicast function?

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

Answer: C

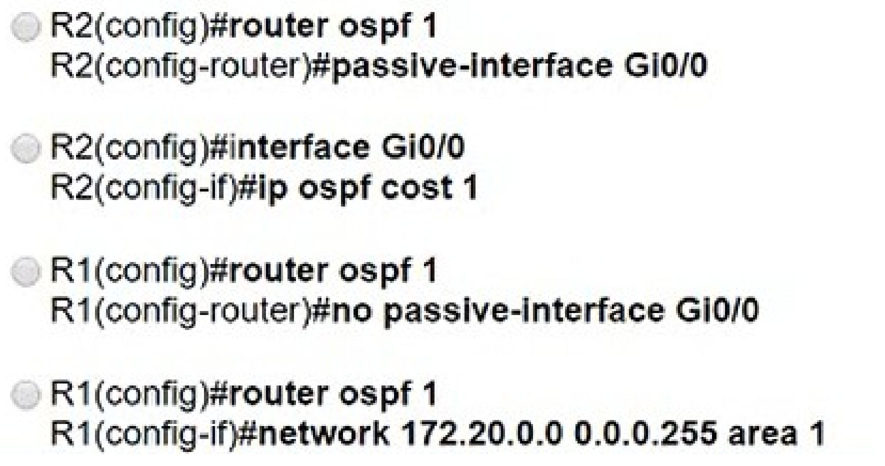
NEW QUESTION 61
- (Topic 4)



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

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

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



○ R2(config)#**router ospf 1**
R2(config-router)#**passive-interface Gi0/0**

○ R2(config)#**interface Gi0/0**
R2(config-if)#**ip ospf cost 1**

○ R1(config)#**router ospf 1**
R1(config-router)#**no passive-interface Gi0/0**

○ R1(config)#**router ospf 1**
R1(config-if)#**network 172.20.0.0 0.0.0.255 area 1**

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

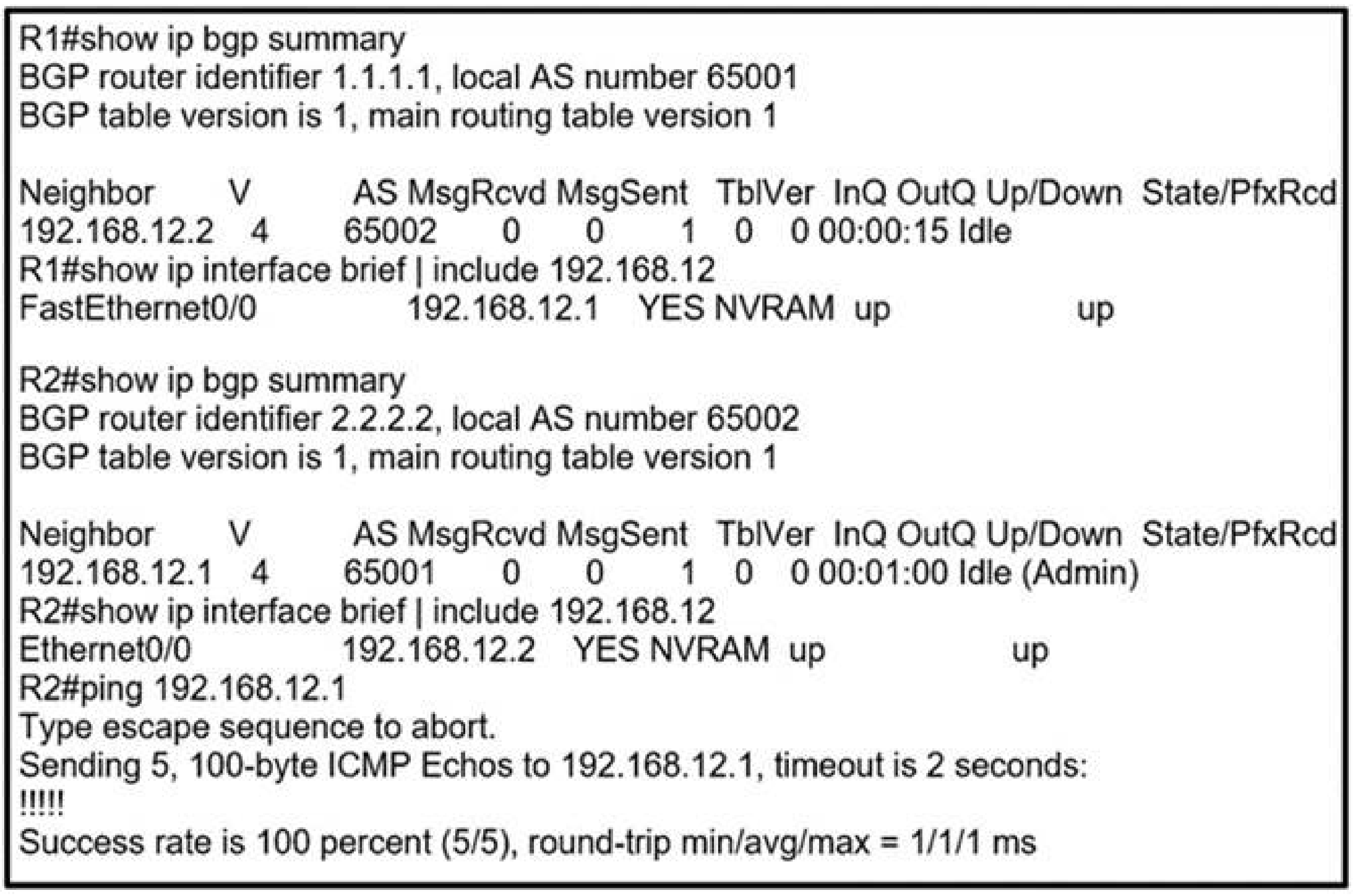
Answer: C

NEW QUESTION 62
- (Topic 4)
An engineer must configure a new WLAN that allows a user to enter a passphrase and provides forward secrecy as a security measure. Which Layer 2 WLAN configuration is required on the Cisco WLC?

A. WPA2 Personal
B. WPA3 Enterprise
C. WPA3 Personal
D. WPA2 Enterprise

Answer: C

NEW QUESTION 66
- (Topic 4)



```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 65001
BGP table version is 1, main routing table version 1

Neighbor       V        AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.2   4      65002       0       0        1    0    0 00:00:15 Idle
R1#show ip interface brief | include 192.168.12
FastEthernet0/0            192.168.12.1    YES NVRAM  up                 up

R2#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 65002
BGP table version is 1, main routing table version 1

Neighbor       V        AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.1   4      65001       0       0        1    0    0 00:01:00 Idle (Admin)
R2#show ip interface brief | include 192.168.12
Ethernet0/0            192.168.12.2    YES NVRAM  up                 up
R2#ping 192.168.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Refer to the exhibit. R1 and R2 are directly connected, but the BGP session does not establish. Which action must be taken to build an eBGP session?

A. Configure ip route 1.1.1.1 0.0.0.0 192.168.12.1 on R2.
B. Configure neighbor 192.168.12.1 activate under R2 BGP process.
C. Configure neighbor 2.2.2.2 remote-as 65002 under R1 BGP process.
D. Configure no neighbor 192.168.12.1 shutdown under R2 BGP process.

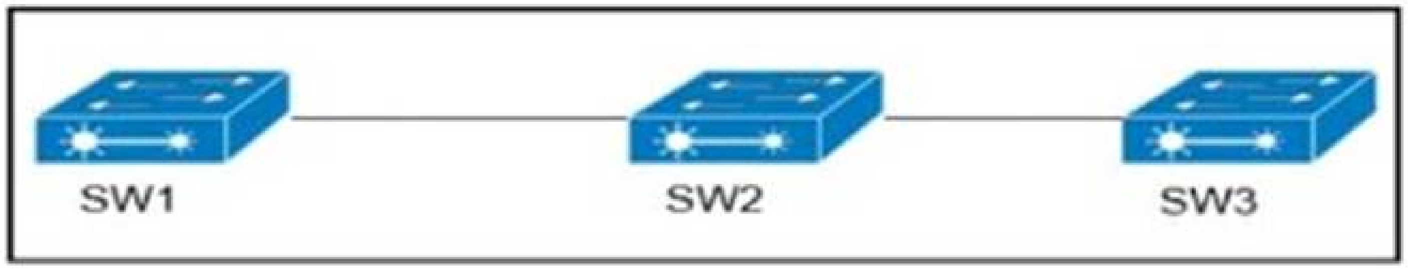
Answer: D

NEW QUESTION 69
- (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 74
- (Topic 1)
Refer to exhibit.



VLANs 50 and 60 exist on the trunk links between all switches All access ports on SW3 are configured for VLAN 50 and SW1 is the VTP server Which command ensures that SW3 receives frames only from VLAN 50?

A. SW1 (config)#vtp pruning
B. SW3(config)#vtp mode transparent
C. SW2(config)=vtp pruning
D. SW1 (config >»vtp mode transparent

Answer: A

Explanation:
SW3 does not have VLAN 60 so it should not receive traffic for this VLAN (sent from SW2). Therefore we should configure VTP Pruning on SW3 so that SW2 does not forward VLAN 60 traffic to SW3. Also notice that we need to configure pruning on SW1 (the VTP Server), not SW2.

NEW QUESTION 77
- (Topic 1)
What is used to perform OoS packet classification?

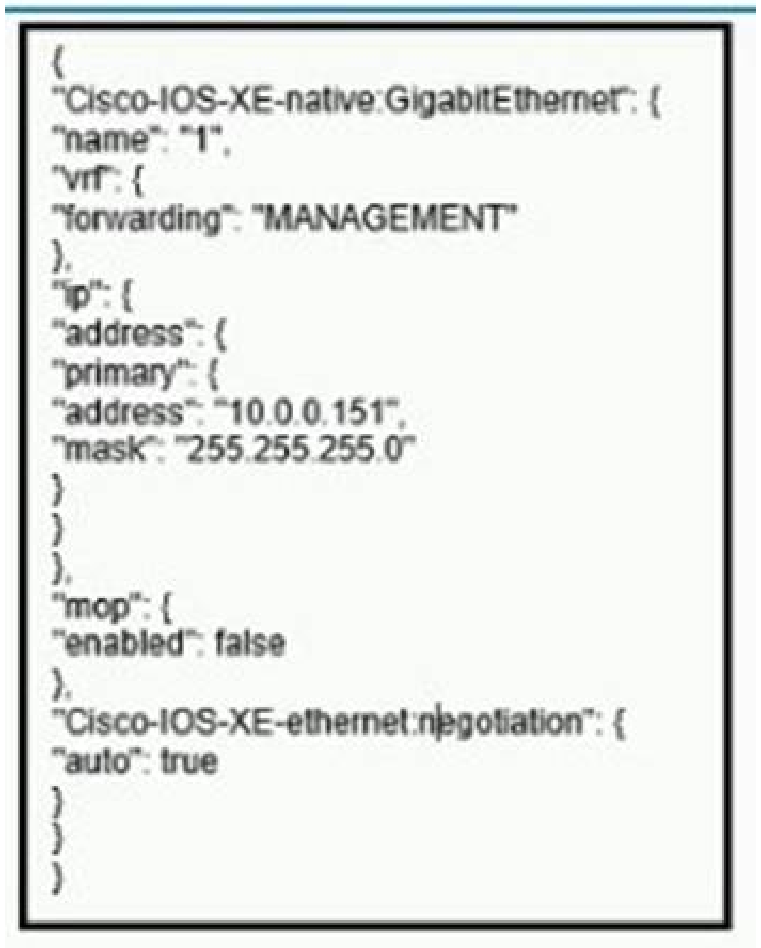
A. the Options field in the Layer 3 header
B. the Type field in the Layer 2 frame

C. the Flags field in the Layer 3 header
D. the TOS field in the Layer 3 header

Answer: D

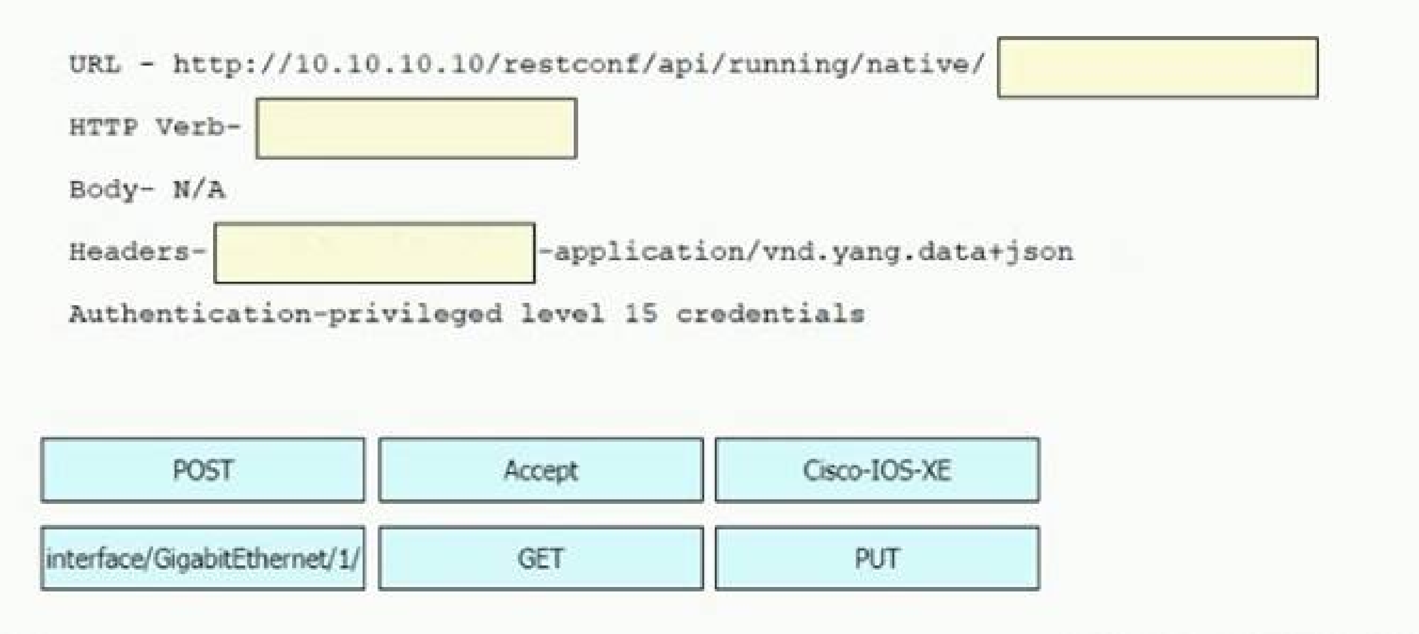
Explanation:
Type of service, when we talk about PACKET, means layer 3

NEW QUESTION 82
DRAG DROP - (Topic 1)



```
{
"Cisco-IOS-XE-native:GigabitEthernet": {
"name": "1",
"vrf": {
"forwarding": "MANAGEMENT"
},
"ip": {
"address": {
"primary": {
"address": "10.0.0.151",
"mask": "255.255.255.0"
}
}
},
"mop": {
"enabled": false
},
"Cisco-IOS-XE-ethernet:negotiation": {
"auto": true
}
}
}
```

Refer to the exhibit Drag and drop the snippets into the RESTCONF request to form the request that returns this response Not all options are used

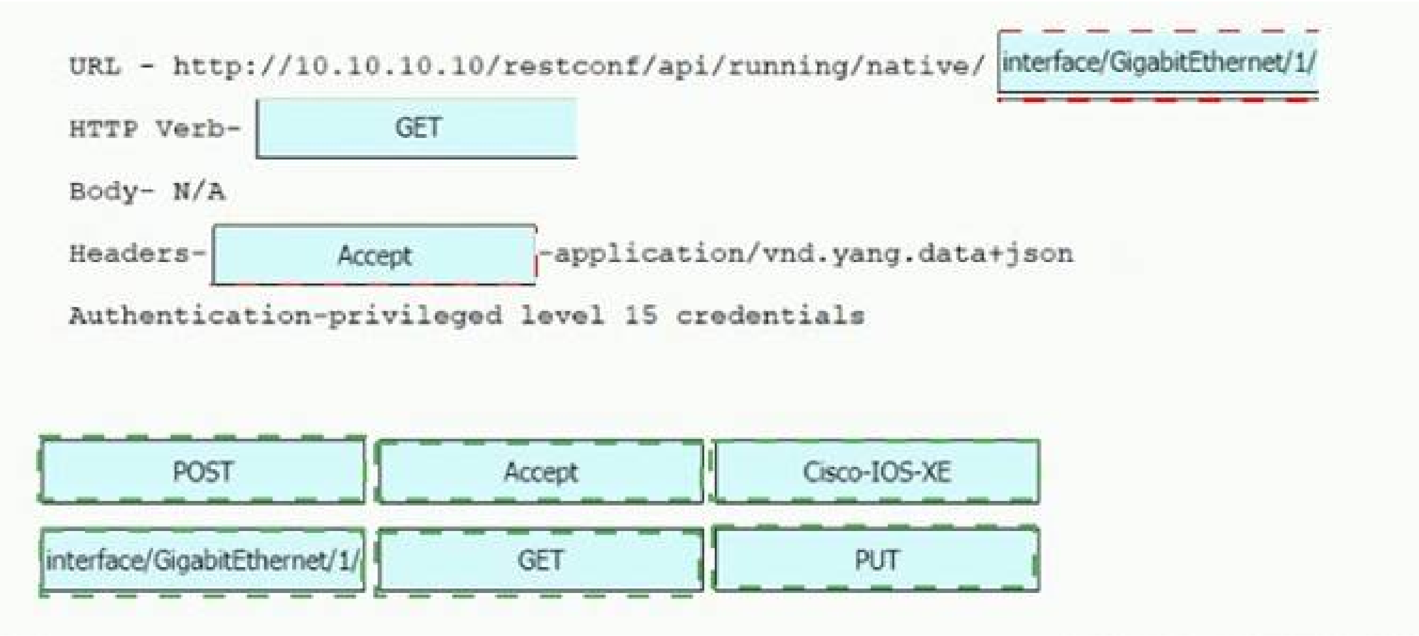


```
URL - http://10.10.10.10/restconf/api/running/native/
HTTP Verb-
Body- N/A
Headers- -application/vnd.yang.data+json
Authentication-privileged level 15 credentials
```

A. Mastered
B. Not Mastered

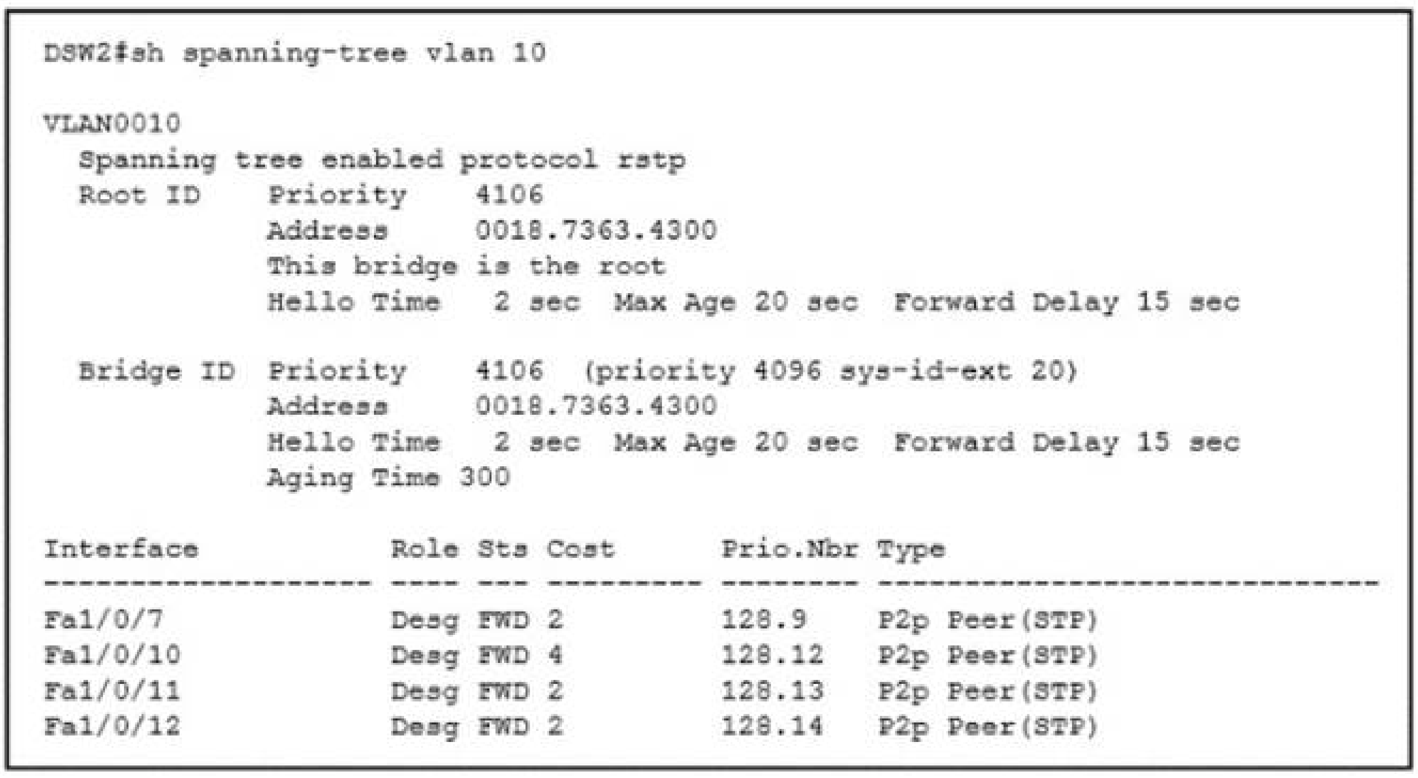
Answer: A

Explanation:



```
URL - http://10.10.10.10/restconf/api/running/native/ interface/GigabitEthernet/1/

HTTP Verb- GET

Body- N/A

Headers- Accept -application/vnd.yang.data+json

Authentication-privileged level 15 credentials
```

NEW QUESTION 85
- (Topic 2)
Refer to the exhibit.



```
DSW2#sh spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    4106
             Address     0018.7363.4300
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4106  (priority 4096 sys-id-ext 20)
             Address     0018.7363.4300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- -----------------------------
Fa1/0/7             Desg FWD 2         128.9    P2p Peer(STP)
Fa1/0/10            Desg FWD 4         128.12   P2p Peer(STP)
Fa1/0/11            Desg FWD 2         128.13   P2p Peer(STP)
Fa1/0/12            Desg FWD 2         128.14   P2p Peer(STP)
```

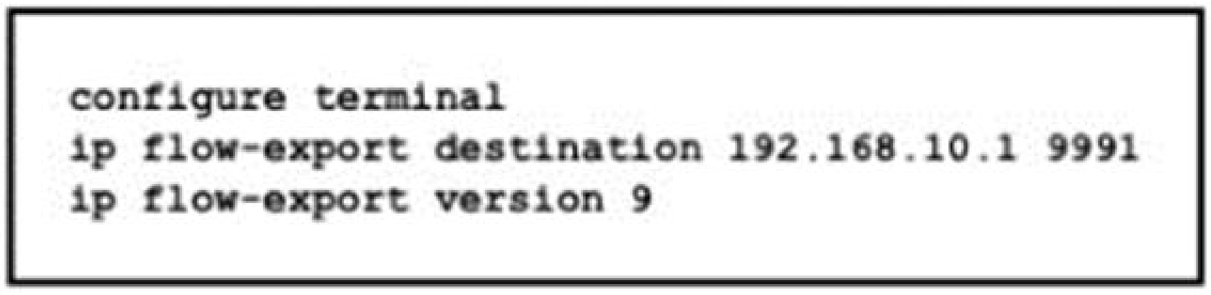
What is the result when a switch that is running PVST+ is added to this network?

A. DSW2 operates in Rapid PVST+ and the new switch operates in PVST+
B. Both switches operate in the PVST+ mode
C. Spanning tree is disabled automatically on the network
D. Both switches operate in the Rapid PVST+ mode.

Answer: A

Explanation:
From the output we see DSW2 is running in RSTP mode (in fact Rapid PVST+ mode as Cisco does not support RSTP alone). When a new switch running PVST+ mode is added to the topology, they keep running the old STP instances as RSTP (in fact Rapid PVST+) is compatible with PVST+.

NEW QUESTION 89
- (Topic 2)
Refer to the exhibit.



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

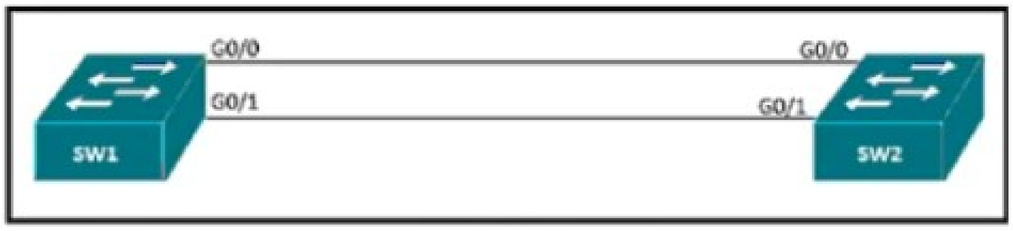
What is required to configure a second export destination for IP address 192.168.10.1?

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

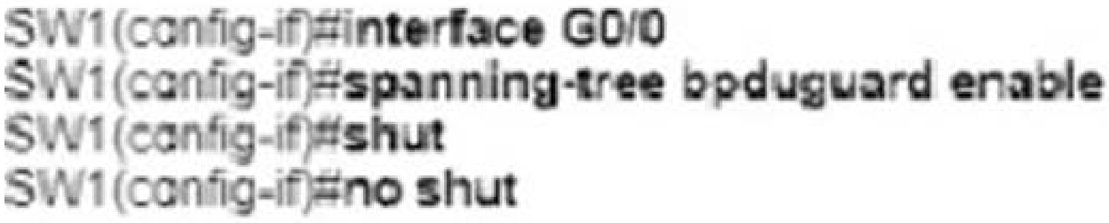
Answer: B

Explanation:
To configure multiple NetFlow export destinations to a router, use the following commands in global configuration mode:
Step 1: Router(config)# ip flow-export destination ip-address udp-port
Step 2: Router(config)# ip flow-export destination ip-address udp-port
The following example enables the exporting of information in NetFlow cache entries: ip flow-export destination 10.42.42.1 9991 ip flow-export destination 10.0.101.254 1999
Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/12s_mdnf.html

NEW QUESTION 91
- (Topic 2)
Refer to the exhibit.

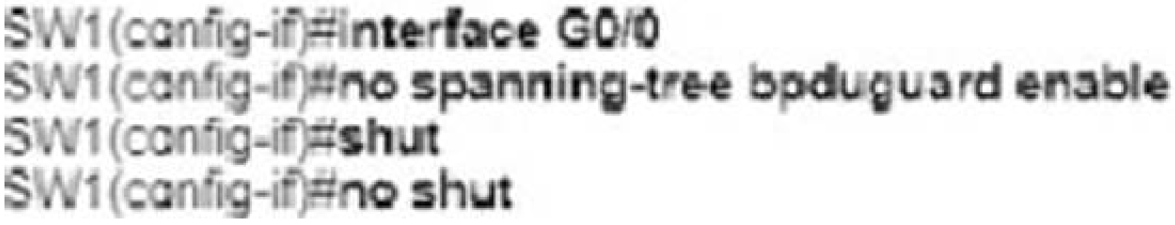


An engineer reconfigures the pot-channel between SW1 and SW2 from an access port to a trunk and immediately notices this error in SW1's log.
Which command set resolves this error?
A)



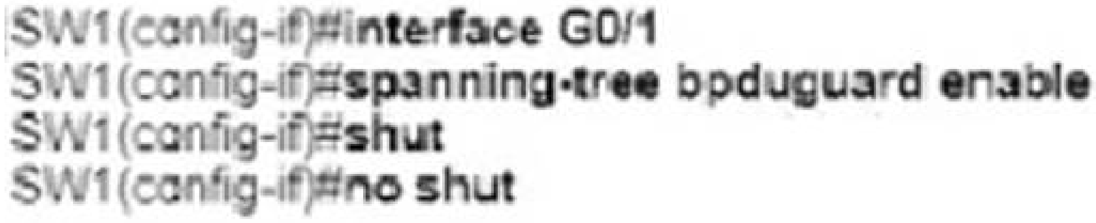
```
SW1(config-if)#interface G0/0
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

B)



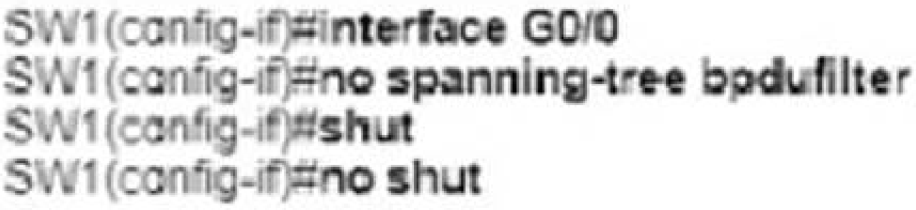
```
SW1(config-if)#interface G0/0
SW1(config-if)#no spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

C)



```
SW1(config-if)#interface G0/1
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

D)



```
SW1(config-if)#interface G0/0
SW1(config-if)#no spanning-tree bpdufilter
SW1(config-if)#shut
SW1(config-if)#no shut
```

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

Answer: B

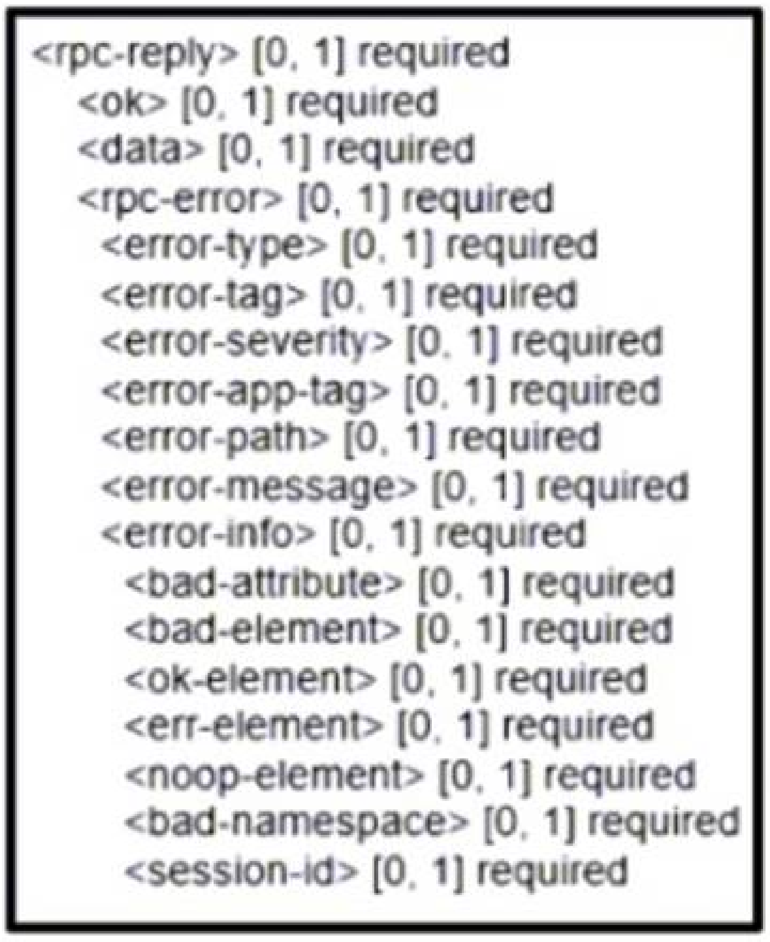
NEW QUESTION 96
- (Topic 2)
Which NGFW mode block flows crossing the firewall?

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 97
- (Topic 2)



```
<rpc-reply> [0, 1] required
   <ok> [0, 1] required
   <data> [0, 1] required
   <rpc-error> [0, 1] required
     <error-type> [0, 1] required
     <error-tag> [0, 1] required
     <error-severity> [0, 1] required
     <error-app-tag> [0, 1] required
     <error-path> [0, 1] required
     <error-message> [0, 1] required
     <error-info> [0, 1] required
       <bad-attribute> [0, 1] required
       <bad-element> [0, 1] required
       <ok-element> [0, 1] required
       <err-element> [0, 1] required
       <noop-element> [0, 1] required
       <bad-namespace> [0, 1] required
       <session-id> [0, 1] required
```

Refer to the exhibit. Which command is required to verify NETCONF capability reply messages?

A. show netconf | section rpc-reply
B. show netconf rpc-reply
C. show netconf xml rpc-reply
D. show netconf schema | section rpc-reply

Answer: D

NEW QUESTION 100
- (Topic 2)
AN engineer is implementing a route map to support redistribution within BGP. The route map must configured to permit all unmatched routes. Which action must the engineer perform to complete this task?

A. Include a permit statement as the first entry
B. Include at least one explicit deny statement
C. Remove the implicit deny entry
D. Include a permit statement as the last entry

Answer: D

NEW QUESTION 103
- (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

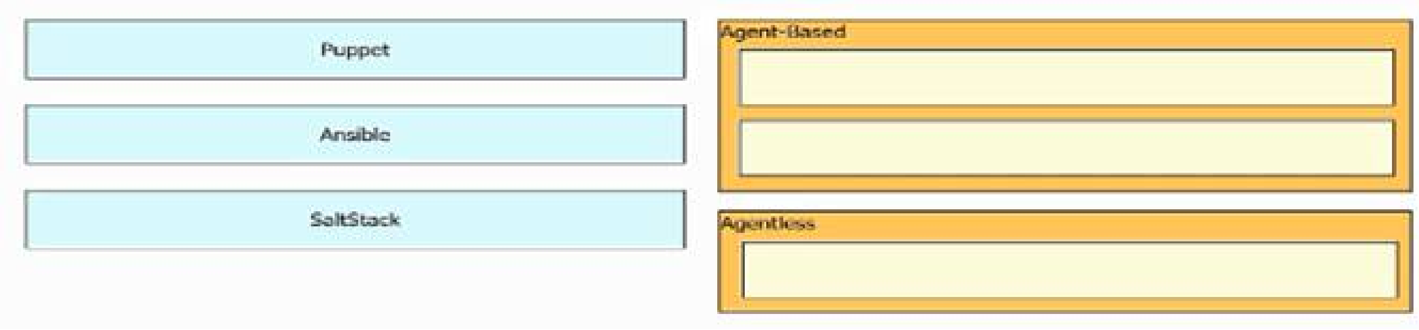
Explanation:
OMP is the control protocol that is used to exchange routing, policy, and management information between Cisco vSmart Controllers and Cisco IOS XE SD-WAN devices in the overlay network. These devices automatically initiate OMP peering sessions between themselves, and the two IP end points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

NEW QUESTION 108
- (Topic 2)
How cloud deployments differ from on-prem deployments?

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

Answer: C

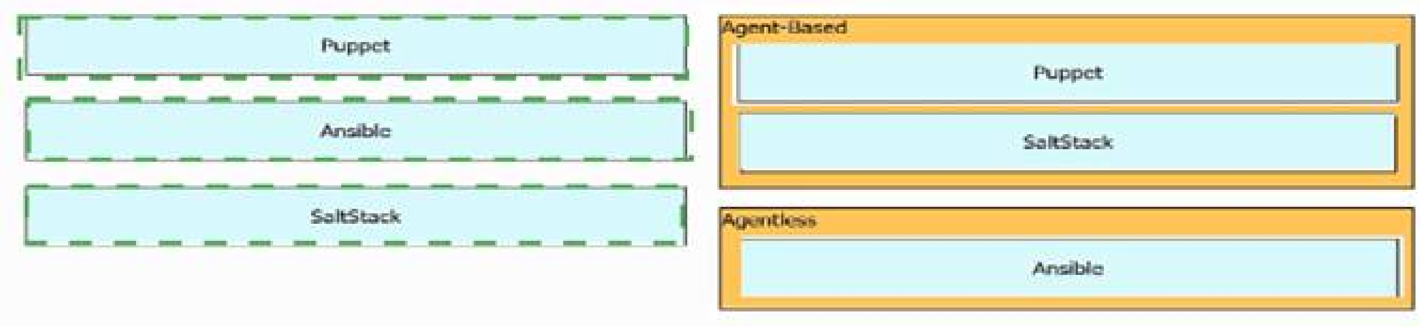
NEW QUESTION 113
DRAG DROP - (Topic 2)
Drag and drop the tools from the left onto the agent types on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 118
- (Topic 2)
Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

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

Answer: D

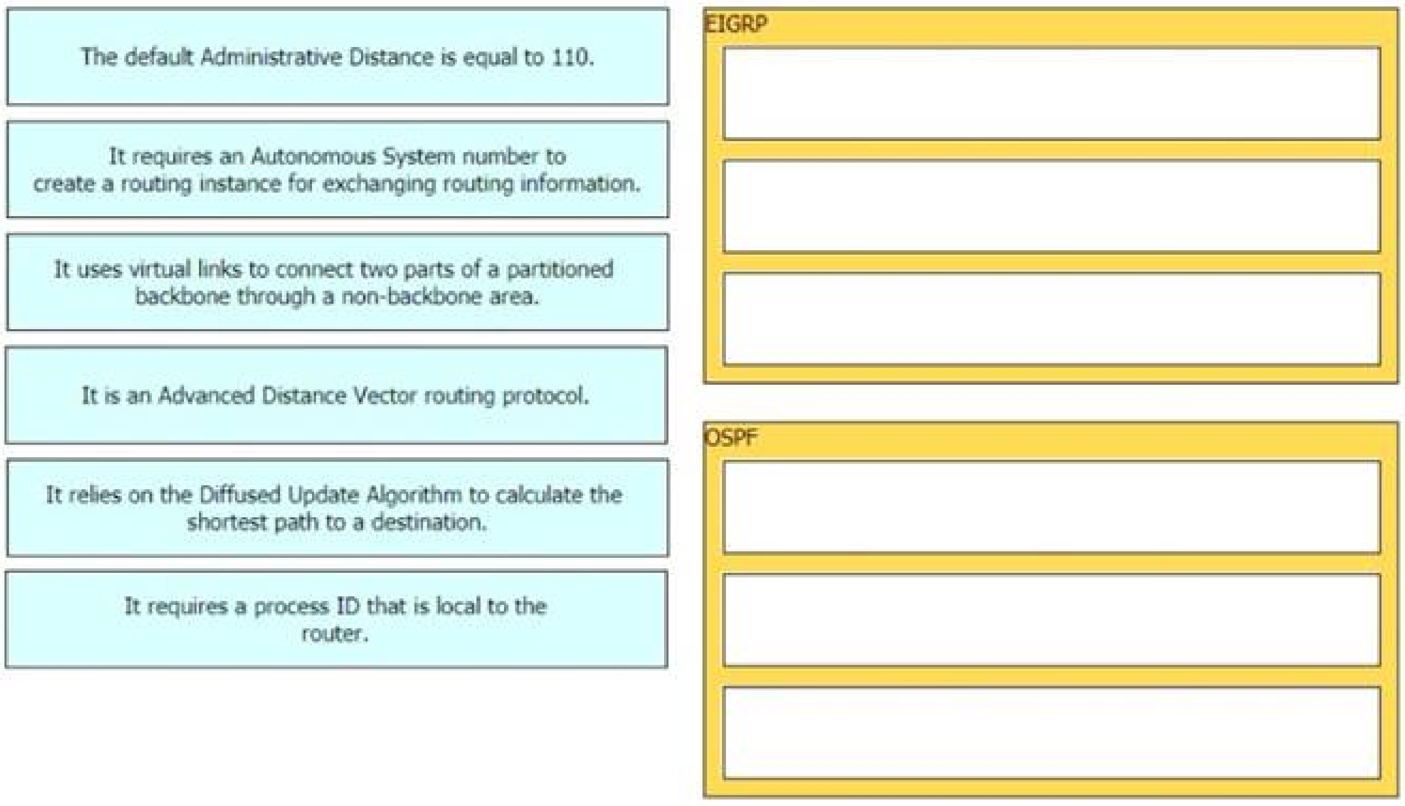
Explanation:
VXLAN has a 24-bit VXLAN network identifier (VNI), which allows for up to 16 million (= 224) VXLAN segments to coexist within the same infrastructure. This surely solve the small number of traditional VLANs.

NEW QUESTION 119
- (Topic 2)
When are multicast RPs required?

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

Answer: D

NEW QUESTION 122
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the routing protocols they describe on the right.



The default Administrative Distance is equal to 110.

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

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

It is an Advanced Distance Vector routing protocol.

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

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

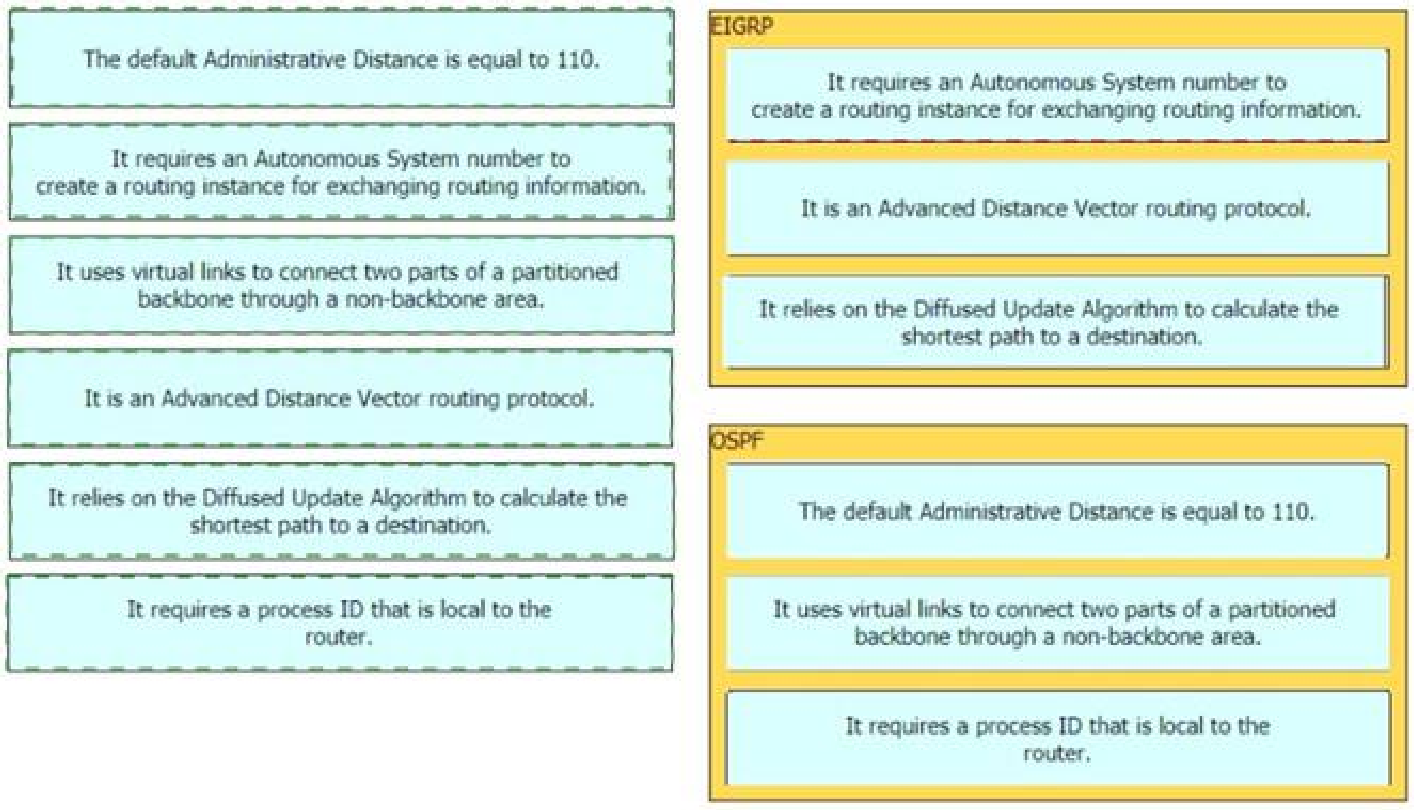
EIGRP

OSPF

A. Mastered
B. Not Mastered

Answer: A

Explanation:



The default Administrative Distance is equal to 110.

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

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

It is an Advanced Distance Vector routing protocol.

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

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

EIGRP

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

It is an Advanced Distance Vector routing protocol.

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

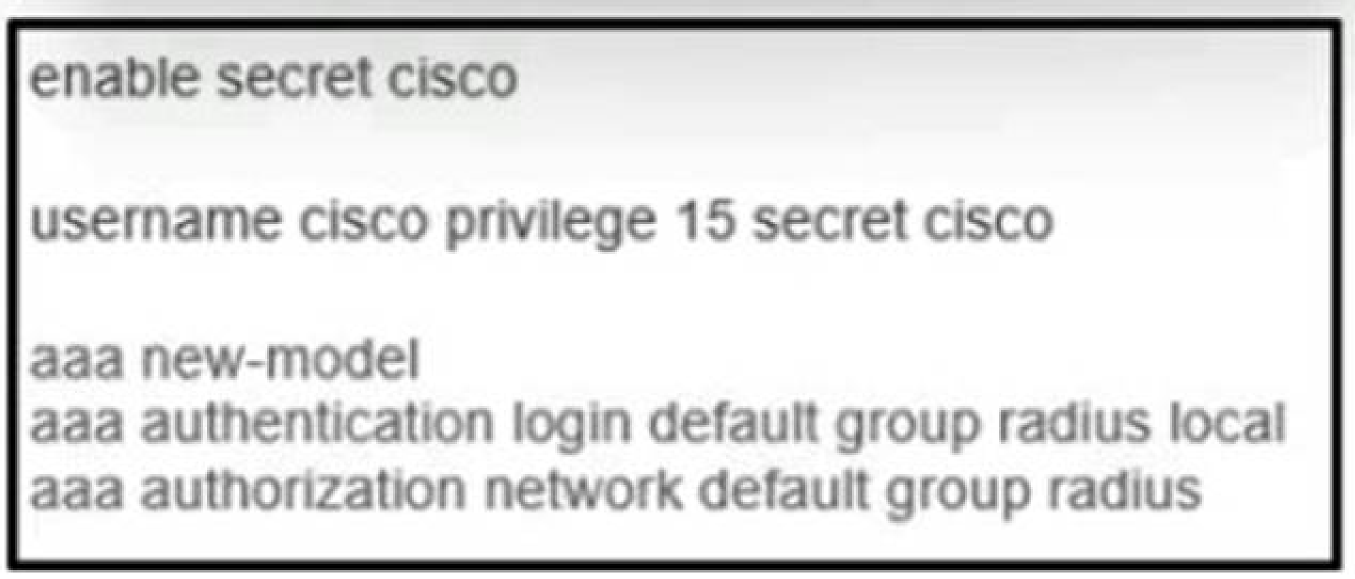
OSPF

The default Administrative Distance is equal to 110.

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

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

NEW QUESTION 127
- (Topic 2)
Refer to the exhibit.



```
enable secret cisco

username cisco privilege 15 secret cisco

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

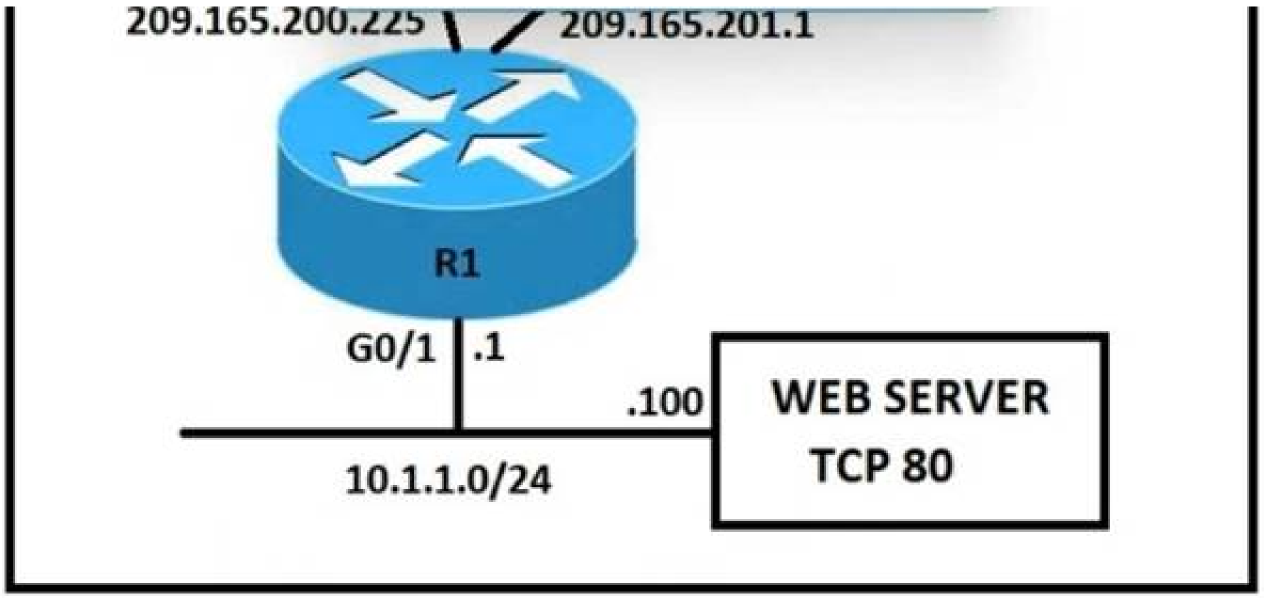
The network administrator must be able to perform configuration changes when all the RADIUS servers are unreachable. Which configuration allows all commands to be authorized if the user has successfully authenticated?

A. aaa authorization exec default group radius none
B. aaa authentication login default group radius local none

C. aaa authorization exec default group radius if-authenticated
D. aaa authorization exec default group radius

Answer: C

NEW QUESTION 129
- (Topic 2)
Refer to the exhibit.

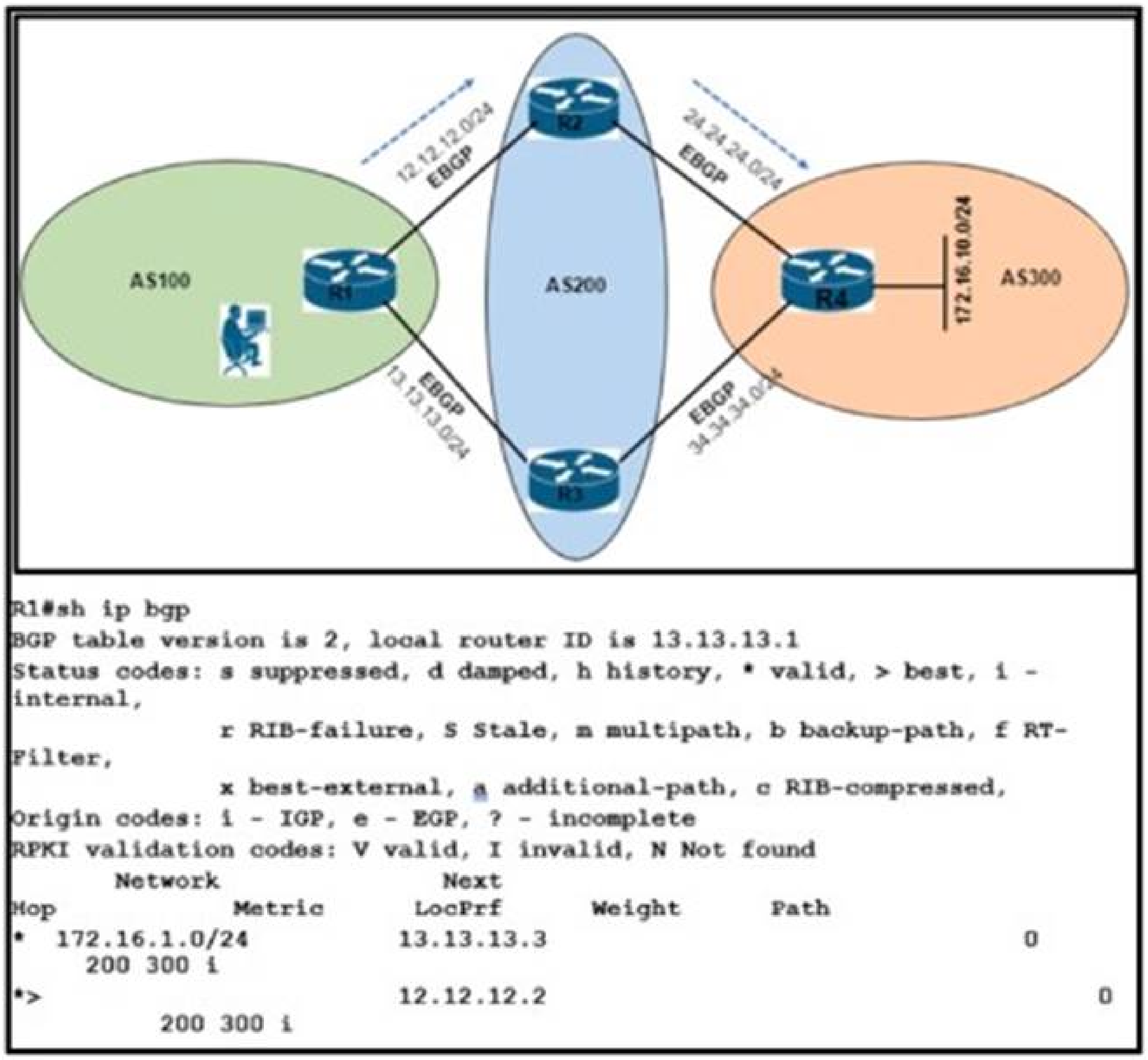


An engineer must configure static NAT on R1 lo allow users HTTP access to the web server on TCP port 80. The web server must be reachable through ISP 1 and ISP 2. Which command set should be applied to R1 to fulfill these requirements?

A. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 extendableip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 extendable
B. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80
C. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80ip nat inside source static tcp 10.1.1.100 8080 209.165.201.1 8080
D. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 no-aliasip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 no-alias

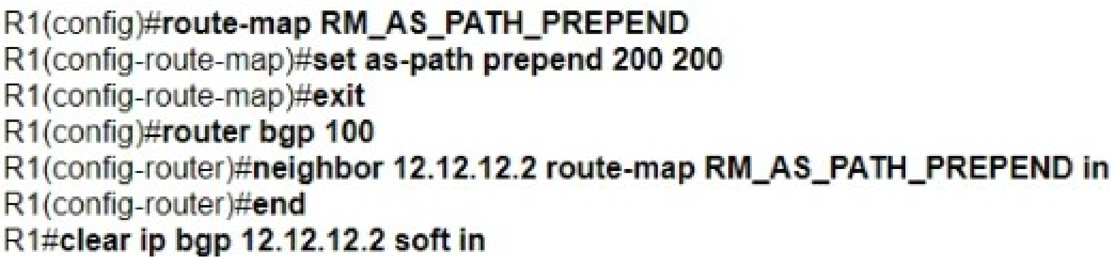
Answer: B

NEW QUESTION 130
- (Topic 2)
Refer to the exhibit.



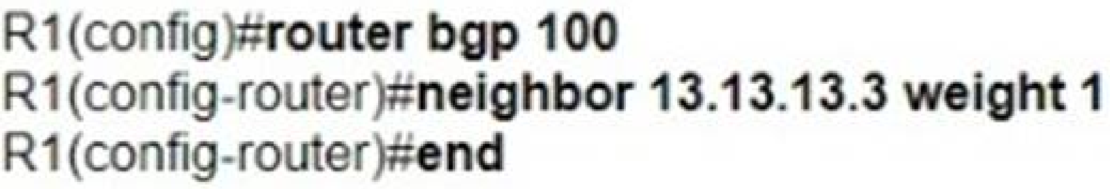
```
R1#sh ip bgp
BGP table version is 2, local router ID is 13.13.13.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin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

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



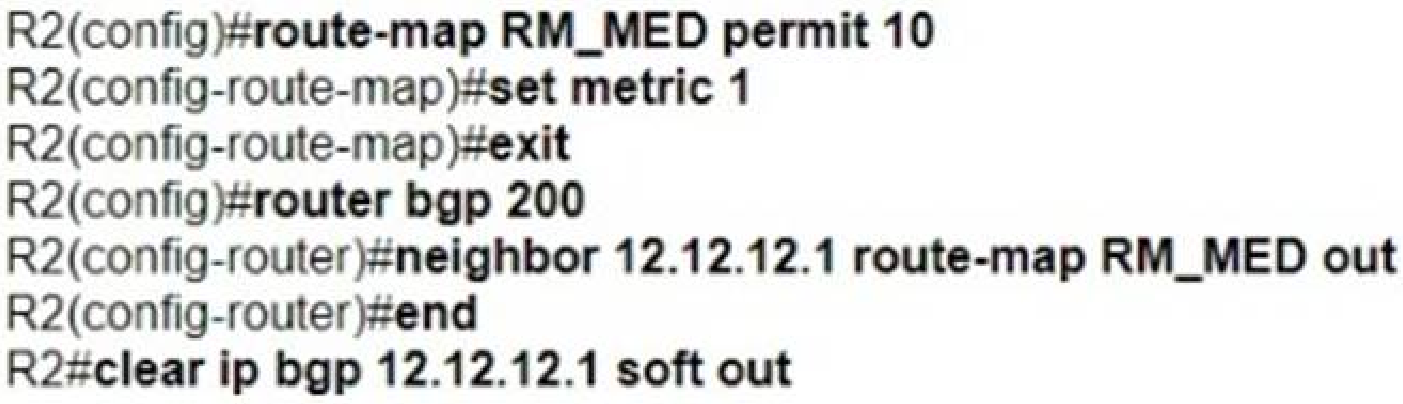
```
R1(config)#route-map RM_AS_PATH_PREPEND
R1(config-route-map)#set as-path prepend 200 200
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 12.12.12.2 route-map RM_AS_PATH_PREPEND in
R1(config-router)#end
R1#clear ip bgp 12.12.12.2 soft in
```

B)



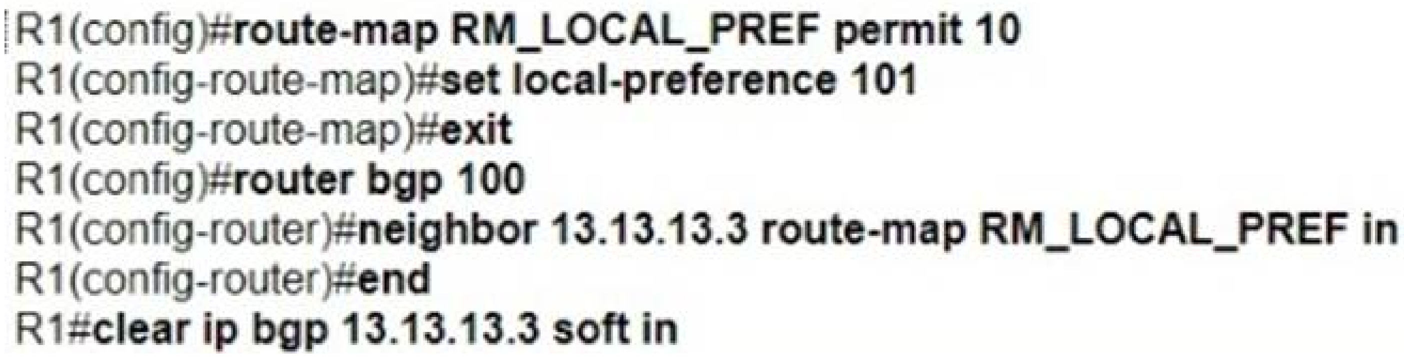
```
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 weight 1
R1(config-router)#end
```

C)



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

D)



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

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

Answer: D

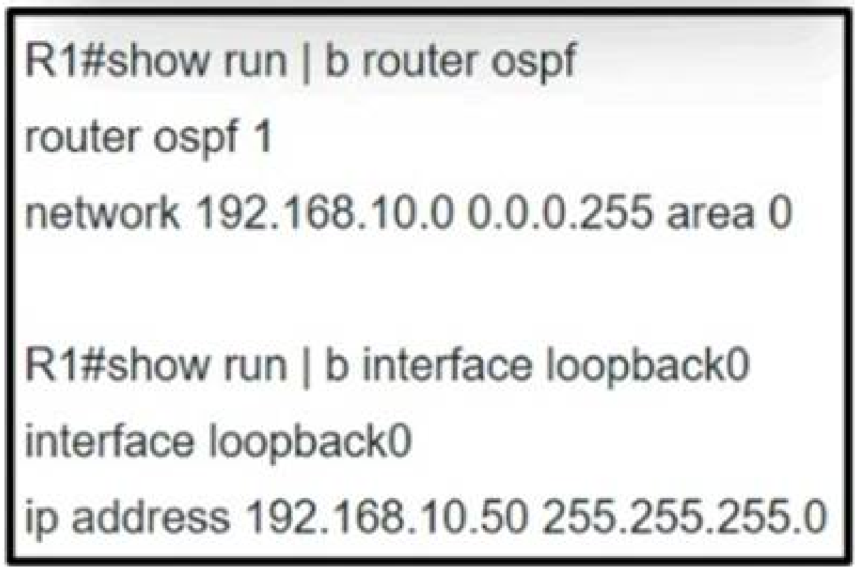
NEW QUESTION 133
- (Topic 2)
Which threat defence mechanism, when deployed at the network perimeter, protects against zero-day attacks?

A. intrusion prevention
B. stateful inspection
C. sandbox
D. SSL decryption

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html“File analysis and sandboxing: Secure Malware Analytics’ highly secure environment helps you execute, analyze, and test malware behavior to discover previously unknown ZERO-DAY threats. The integration of Secure Malware Analytics’ sandboxing technology into Malware Defense results in more dynamic analysis checked against a larger set of behavioral indicators. “

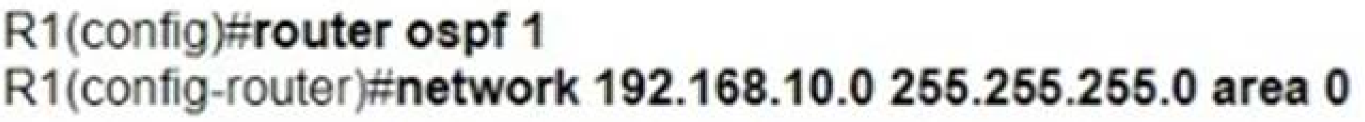
NEW QUESTION 137
- (Topic 2)
Refer to the exhibit.



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

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

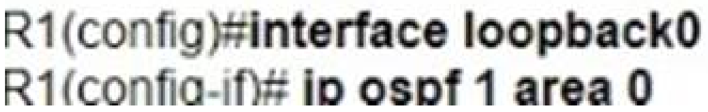
R2 is the neighboring router of R1. R2 receives an advertisement for network 192 168.10.50/32. Which configuration should be applied for the subnet to be advertised with the original /24 netmask?

A)



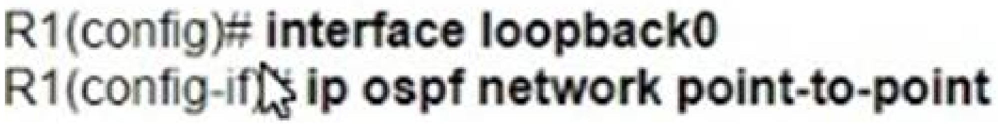
```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 255.255.255.0 area 0
```

B)



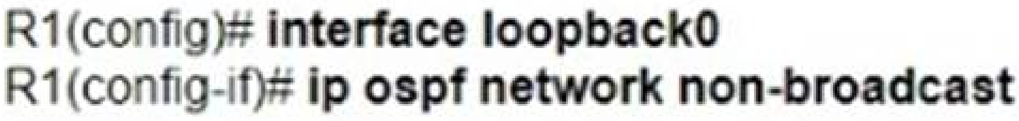
```
R1(config)#interface loopback0
R1(config-if)# ip ospf 1 area 0
```

C)



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

D)



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

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

Answer: C

NEW QUESTION 140
- (Topic 2)
A customer wants to provide wireless access to contractors using a guest portal on Cisco ISE. The portal Is also used by employees A solution is implemented, but contractors receive a certificate error when they attempt to access the portal Employees can access the portal without any errors. Which change must be implemented to allow the contractors and employees to access the portal?

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

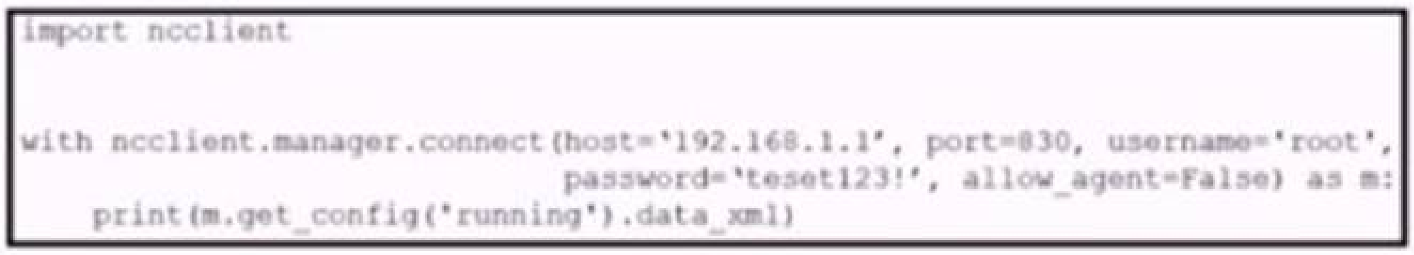
Answer: C

NEW QUESTION 143
- (Topic 2)
Which element enables communication between guest VMs within a virtualized environment?

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

Answer: B

NEW QUESTION 146
- (Topic 2)
Refer to the exhibit.



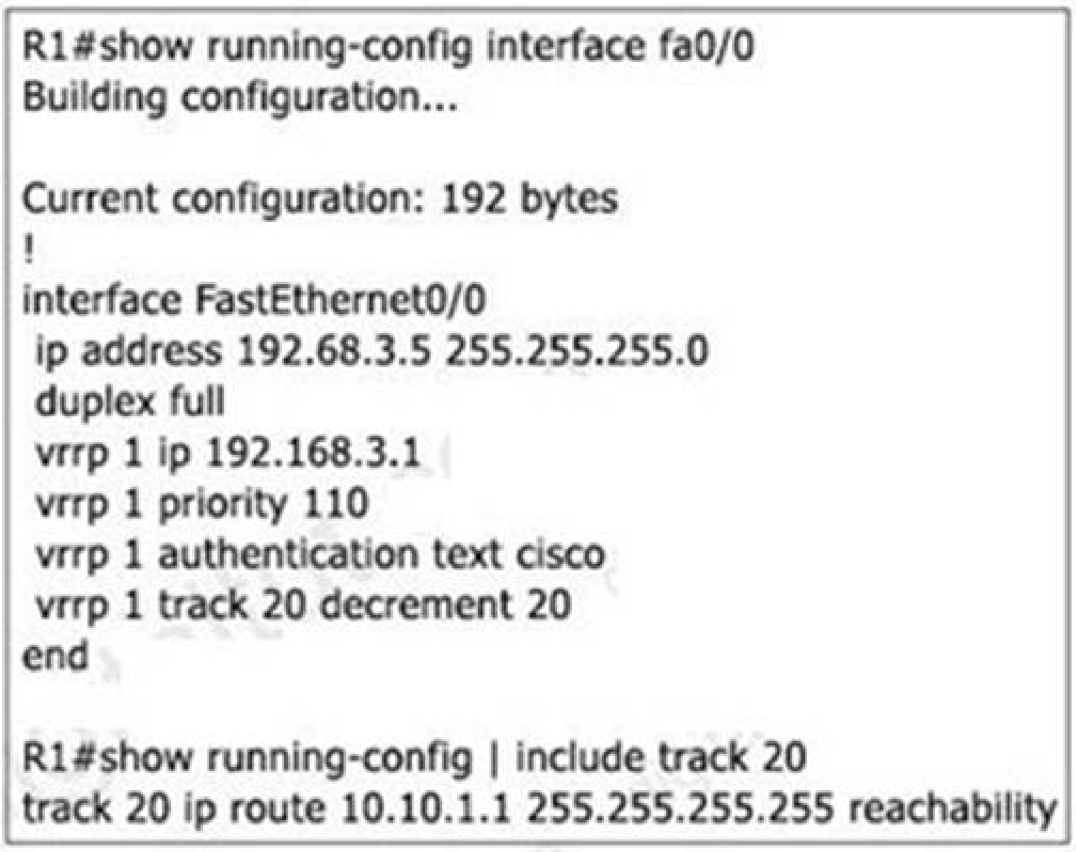
```
import ncclient

with ncclient.manager.connect(host='192.168.1.1', port=830, username='root',
                             password='teset123!', allow_agent=False) as m:
    print(m.get_config('running').data_xml)
```

After running the code in the exhibit. Which step reduces the amount of data that NETCONF server returns to the NETCONF client, to only the interface's configuration?

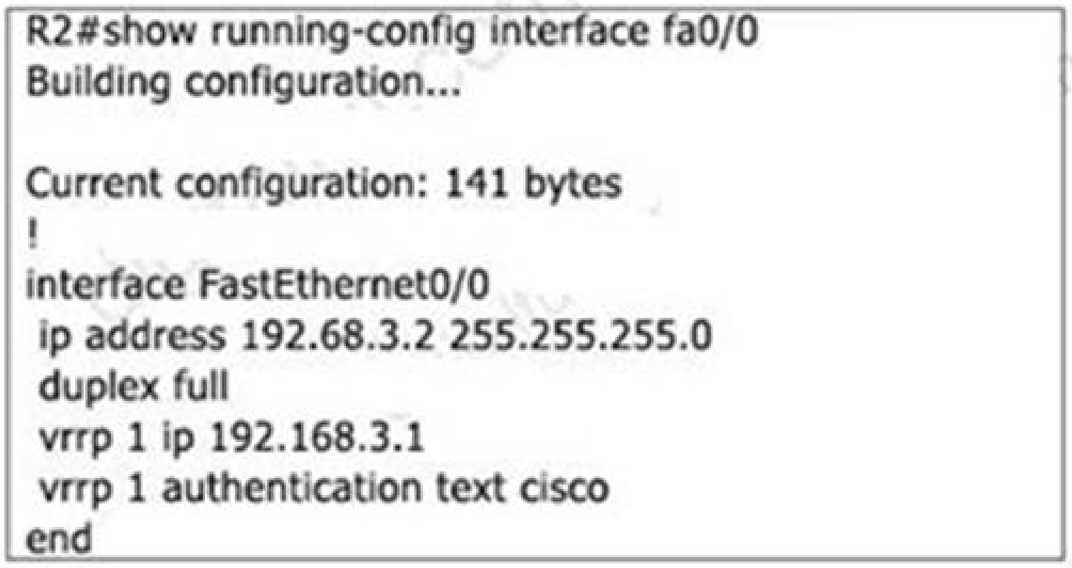
A. Create an XML filter as a string and pass it to get_config() method as an argument
B. Use the txml library to parse the data returned by the NETCONF server for the interface's configuration
C. Create a JSON filter as a string and pass it to the get_config() method as an argument
D. Use the JSON library to parse the data returned by the NETCONF server for the interface's configuration

Answer: D

NEW QUESTION 151
- (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 153
- (Topic 2)
How is a data modeling language used?

A. To enable data lo be easily structured, grouped, validated, and replicated
B. To represent finite and well-defined network elements that cannot be changed
C. To model the flows of unstructured data within the infrastructure
D. To provide human readability to scripting languages

Answer: A

NEW QUESTION 157
- (Topic 2)
Which feature does Cisco TrustSec use to provide scalable, secure communication throughout a network?

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

Answer: B

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

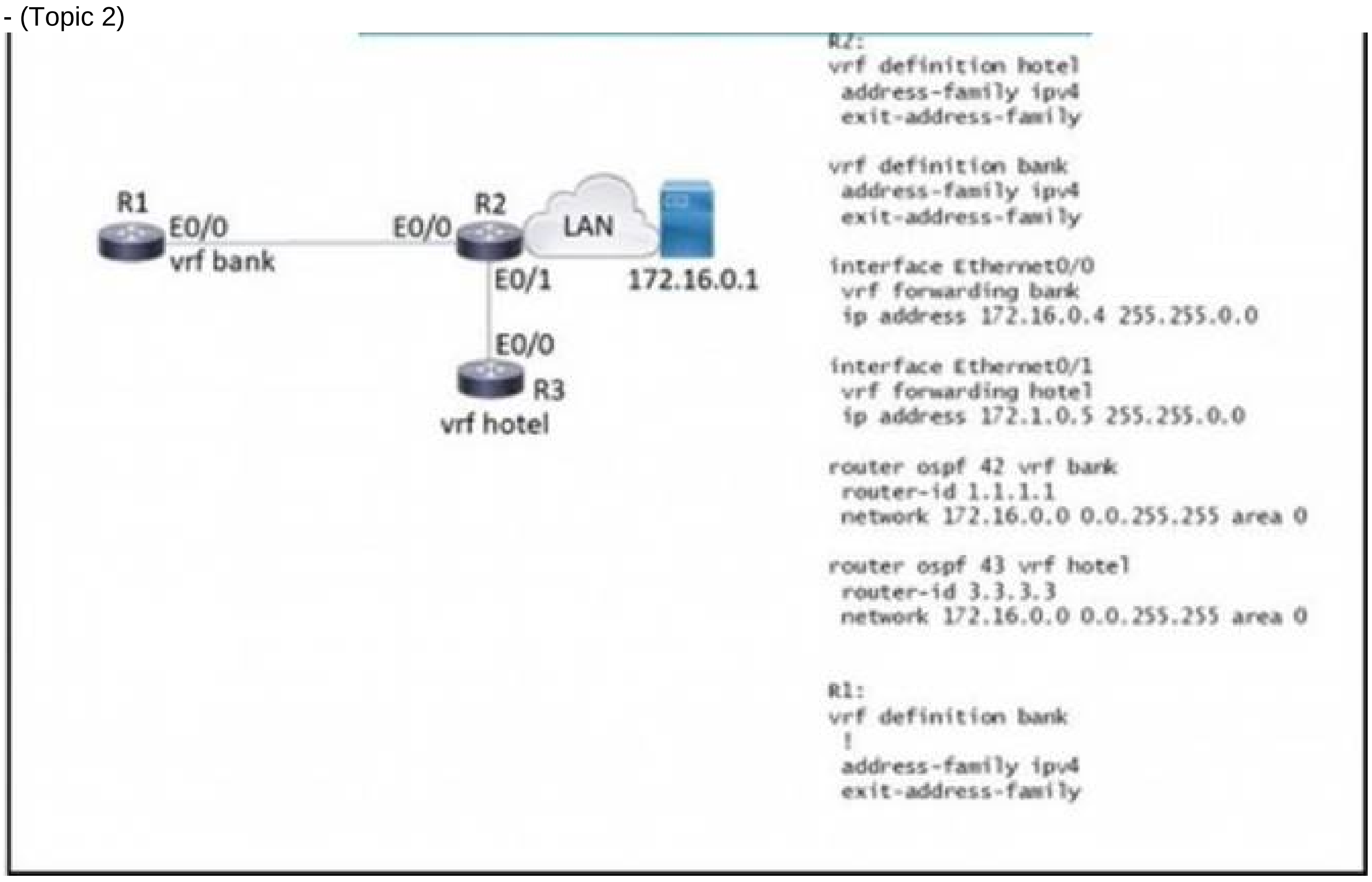
NEW QUESTION 162
- (Topic 2)
Which action is performed by Link Management Protocol in a Cisco StackWise Virtual domain?

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

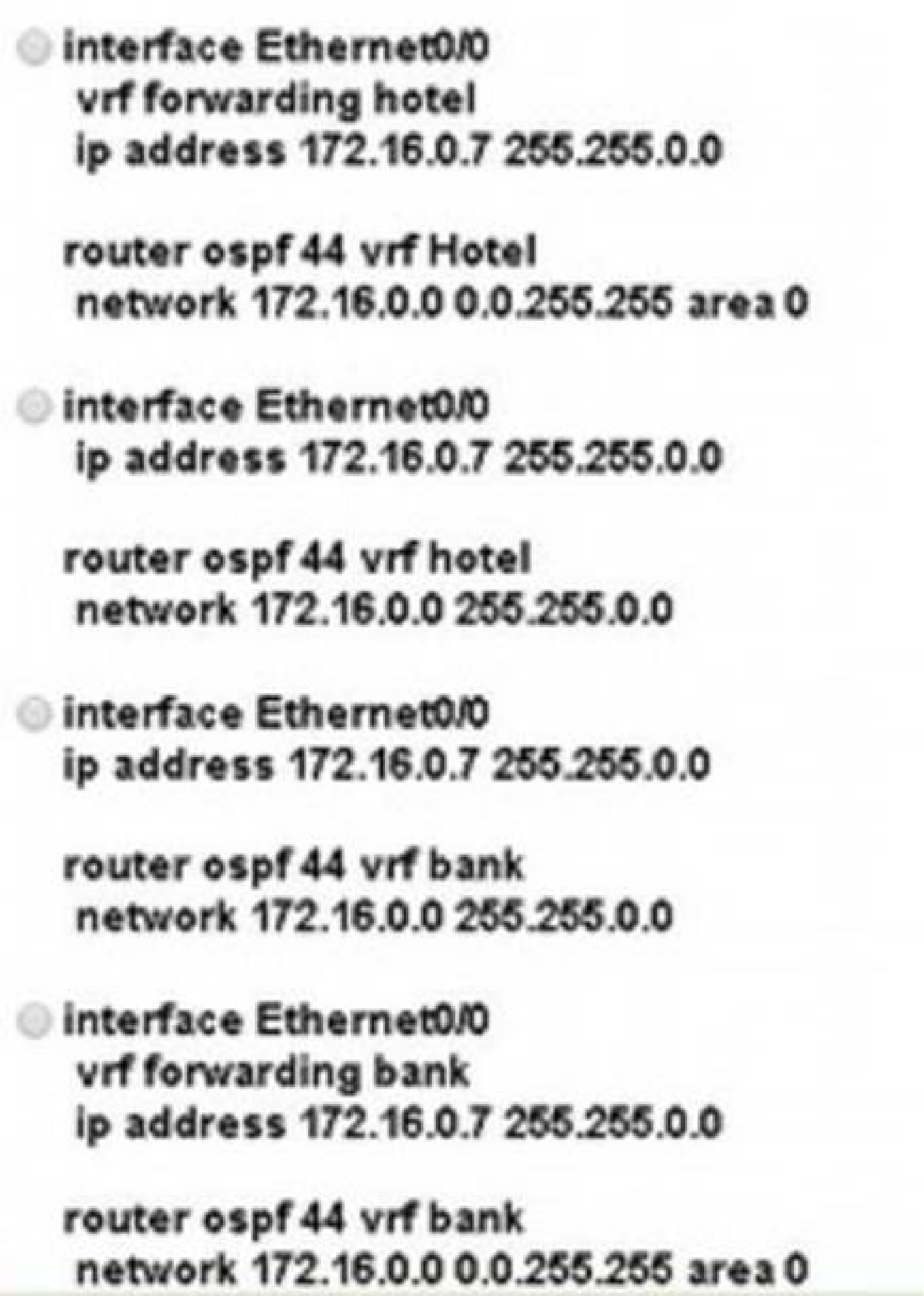
Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb- 06-cat-9k-stack-wp-cte-en.html

NEW QUESTION 163
- (Topic 2)



```
R2:
vrf definition hotel
 address-family ipv4
 exit-address-family

vrf definition bank
 address-family ipv4
 exit-address-family

interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.4 255.255.0.0

interface Ethernet0/1
 vrf forwarding hotel
 ip address 172.1.0.5 255.255.0.0

router ospf 42 vrf bank
 router-id 1.1.1.1
 network 172.16.0.0 0.0.255.255 area 0

router ospf 43 vrf hotel
 router-id 3.3.3.3
 network 172.16.0.0 0.0.255.255 area 0


R1:
vrf definition bank
 !
 address-family ipv4
 exit-address-family
```

Refer to the exhibit. Which configuration must be applied to R1 to enable R1 to reach the server at 172.16.0.1?

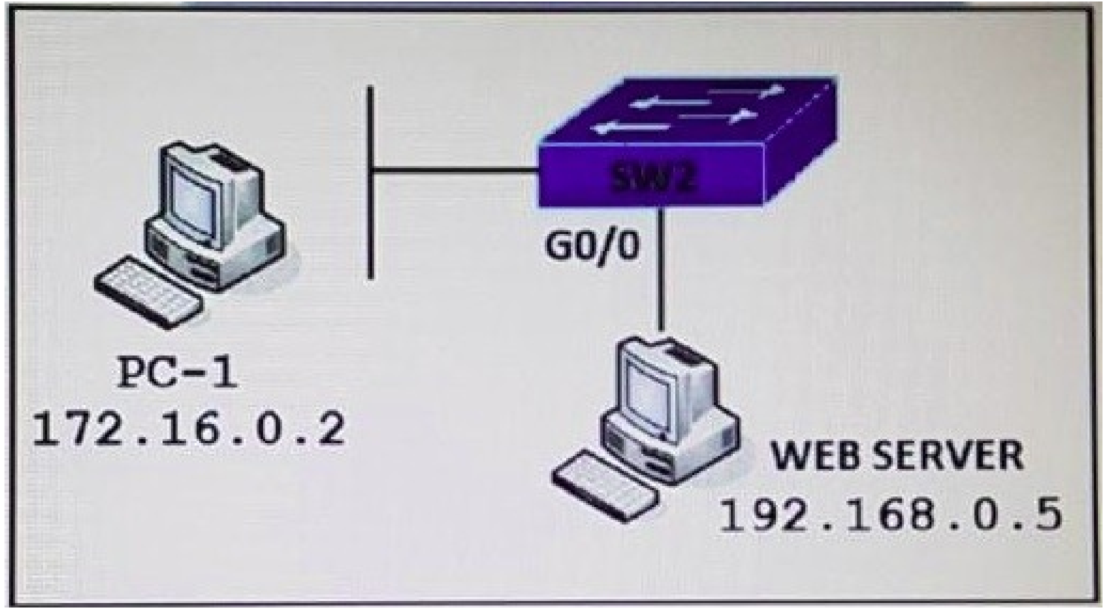


```
○ interface Ethernet0/0
   vrf forwarding hotel
   ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf Hotel
   network 172.16.0.0 0.0.255.255 area 0

○ interface Ethernet0/0
   ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf hotel
   network 172.16.0.0 255.255.0.0

○ interface Ethernet0/0
  ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf bank
   network 172.16.0.0 255.255.0.0

○ interface Ethernet0/0
   vrf forwarding bank
   ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf bank
   network 172.16.0.0 0.0.255.255 area 0
```

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

Answer: D

NEW QUESTION 165
- (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 169
- (Topic 2)

What is the structure of a JSON web token?

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

Answer: A

Explanation:
JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA.
JSON Web Tokens are composed of three parts, separated by a dot (.): Header, Payload, Signature. Therefore, a JWT typically looks like the following:
xxxxx.yyyyy.zzzzz
The header typically consists of two parts: the type of the token, which is JWT, and the signing algorithm being used, such as HMAC SHA256 or RSA.
The second part of the token is the payload, which contains the claims. Claims are statements about an entity (typically, the user) and additional data.
To create the signature part you have to take the encoded header, the encoded payload, a secret, the algorithm specified in the header, and sign that. Reference: https://jwt.io/introduction/

NEW QUESTION 170
- (Topic 2)
What is a characteristic of Cisco DNA Northbound APIs?

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

Answer: C

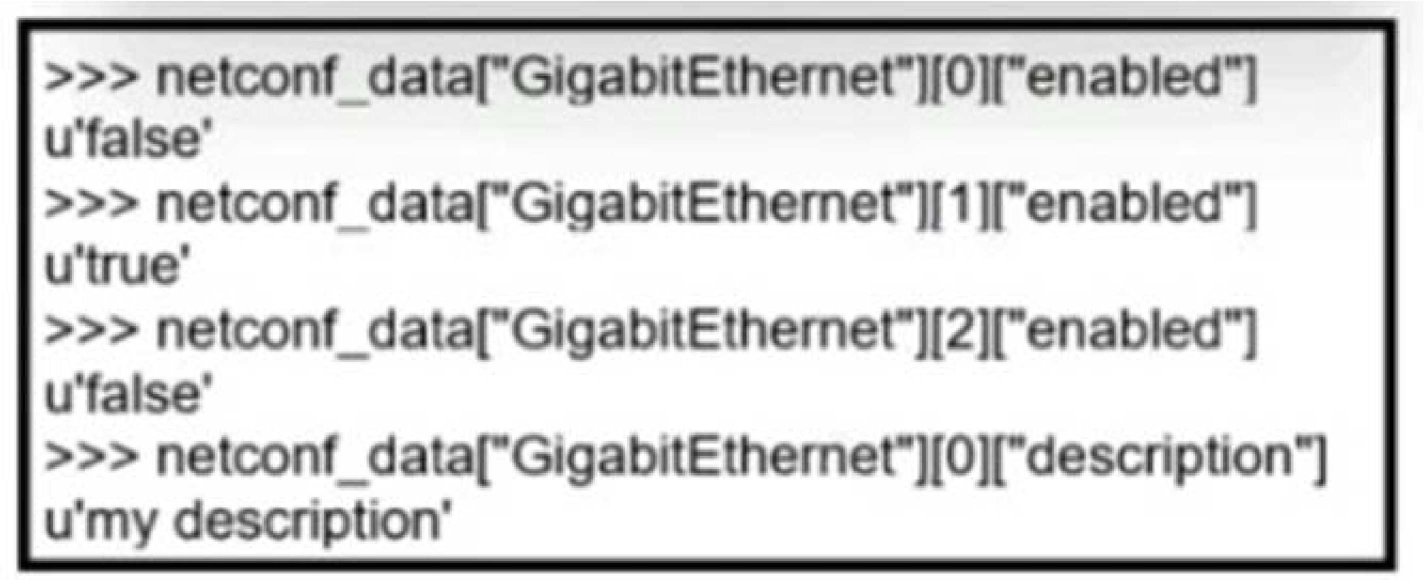
NEW QUESTION 172
- (Topic 2)
Which protocol is used to encrypt control plane traffic between SD-WAN controllers and SD-WAN endpoints?

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

Answer: A

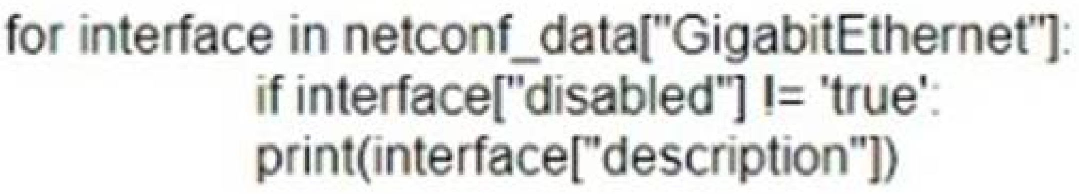
Explanation:
DTLS protocol is used to encrypt control plane traffic between vSmart (controllers) and other SD-WAN endpoints.

NEW QUESTION 173
- (Topic 2)
Refer to the exhibit.



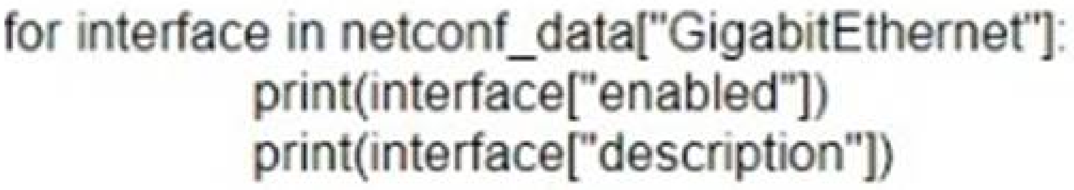
```
>>> netconf_data["GigabitEthernet"][0]["enabled"]
u'false'
>>> netconf_data["GigabitEthernet"][1]["enabled"]
u'true'
>>> netconf_data["GigabitEthernet"][2]["enabled"]
u'false'
>>> netconf_data["GigabitEthernet"][0]["description"]
u'my description'
```

Which Python code snippet prints the descriptions of disabled interfaces only?
A)



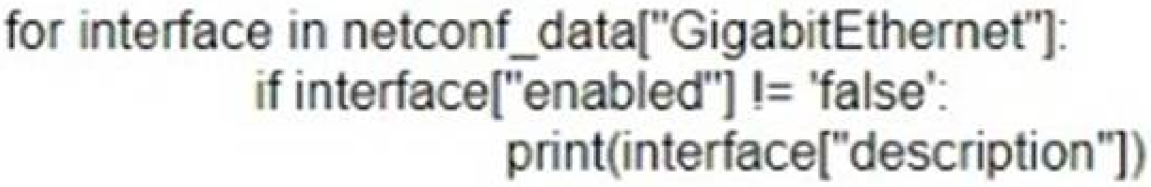
```
for interface in netconf_data["GigabitEthernet"]:
            if interface["disabled"] != 'true':
            print(interface["description"])
```

B)



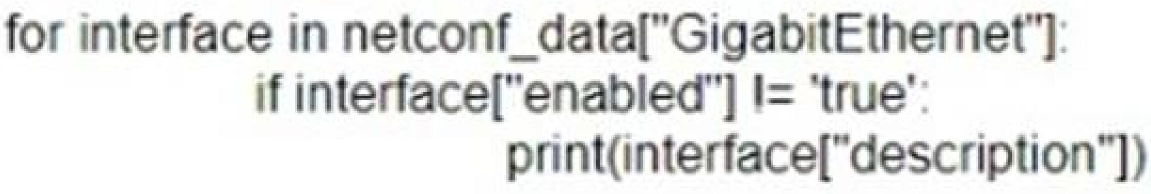
```
for interface in netconf_data["GigabitEthernet"]:
            print(interface["enabled"])
            print(interface["description"])
```

C)



```
for interface in netconf_data["GigabitEthernet"]:
            if interface["enabled"] != 'false':
                        print(interface["description"])
```

D)



```
for interface in netconf_data["GigabitEthernet"]:
            if interface["enabled"] != 'true':
                        print(interface["description"])
```

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

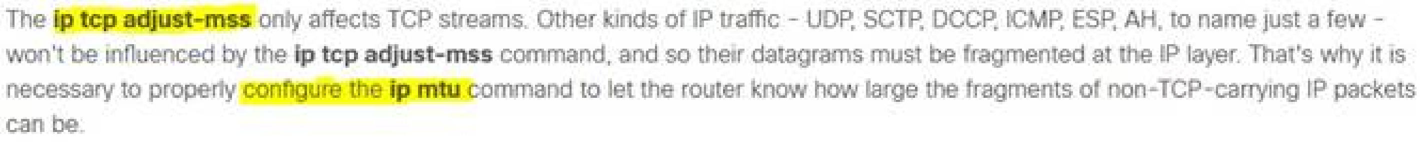
Answer: D

NEW QUESTION 175
- (Topic 2)
Which two GRE features are configured to prevent fragmentation? (Choose two.)

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

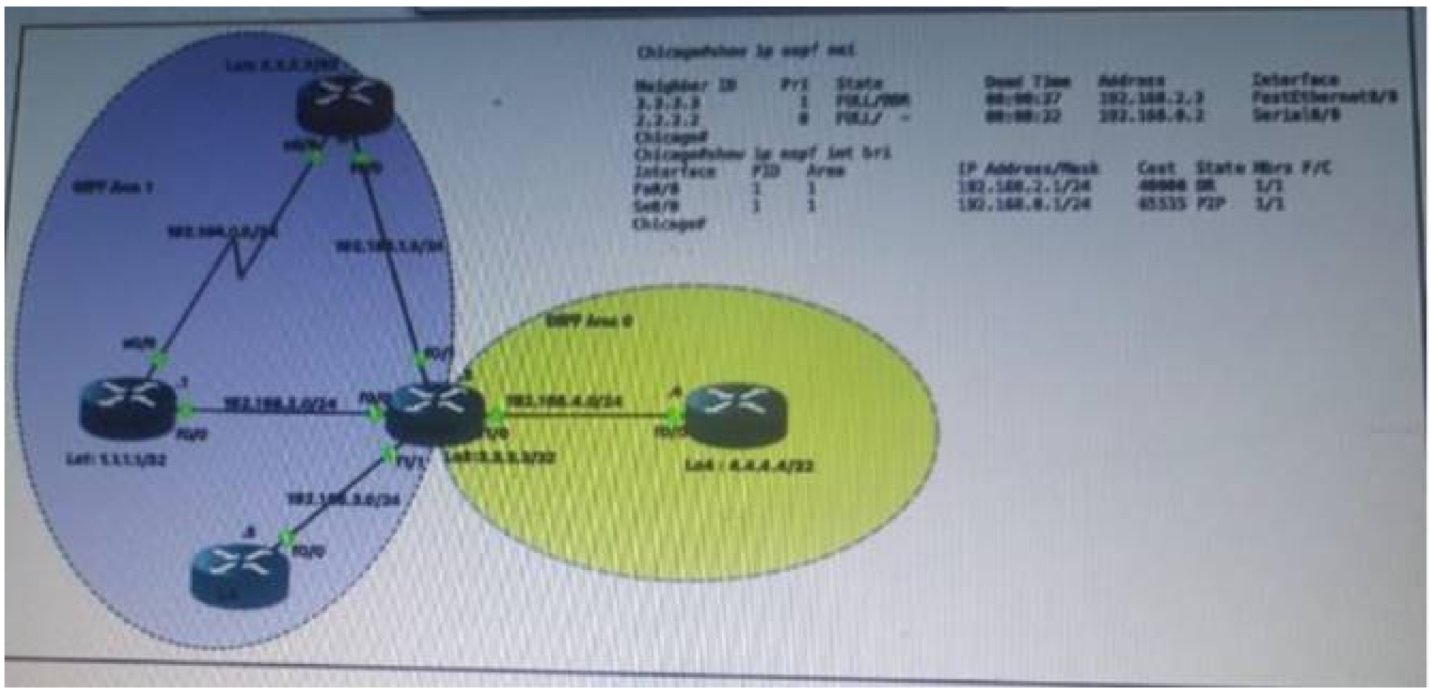
Answer: AE

Explanation:



The **ip tcp adjust-mss** only affects TCP streams. Other kinds of IP traffic - UDP, SCTP, DCCP, ICMP, ESP, AH, to name just a few - won't be influenced by the **ip tcp adjust-mss** command, and so their datagrams must be fragmented at the IP layer. That's why it is necessary to properly configure the **ip mtu** command to let the router know how large the fragments of non-TCP-carrying IP packets can be.

NEW QUESTION 177
- (Topic 2)
Refer the exhibit.



```
Chicago#show ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   FULL/BDR        00:00:37    192.168.2.3     FastEthernet0/0
2.2.2.2           0   FULL/  -        00:00:32    192.168.0.2     Serial0/0
Chicago#
Chicago#show ip ospf int bri
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Fa0/0        1     1               192.168.2.1/24     40000 DR    1/1
Se0/0        1     1               192.168.0.1/24     65535 P2P   1/1
Chicago#
```

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

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

Answer: B

NEW QUESTION 178
- (Topic 2)
What is the wireless received signal strength indicator?

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

Answer: D

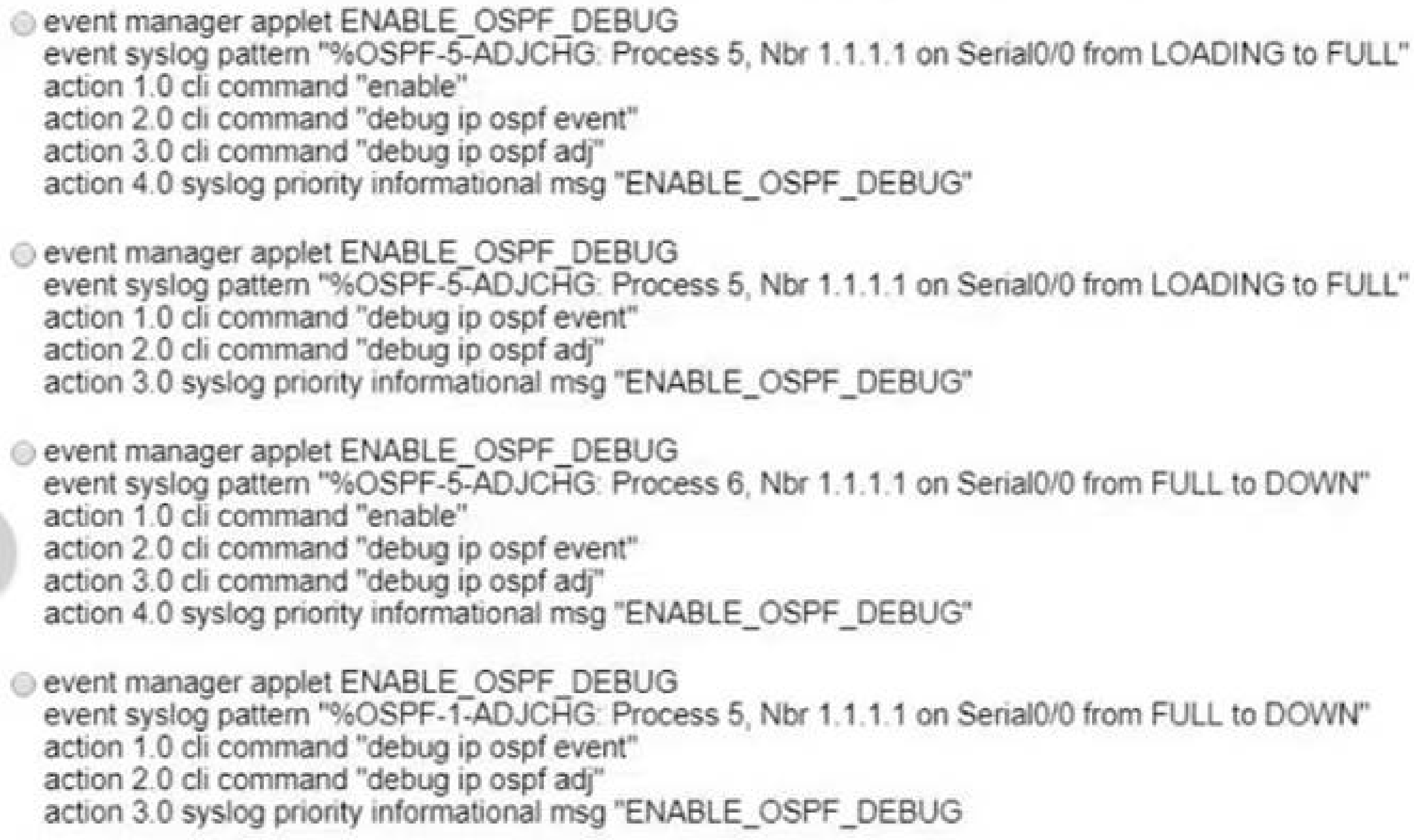
Explanation:
RSSI, or “Received Signal Strength Indicator,” is a measurement of how well your device can hear a signal from an access point or router. It’s a value that is useful for determining if you have enough signal to get a good wireless connection.
This value is measured in decibels (dBm) from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

NEW QUESTION 181
- (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 183
- (Topic 2)
An engineer must create an EEM script to enable OSPF debugging in the event the OSPF neighborship goes down. Which script must the engineer apply?



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

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

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

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

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

Answer: C

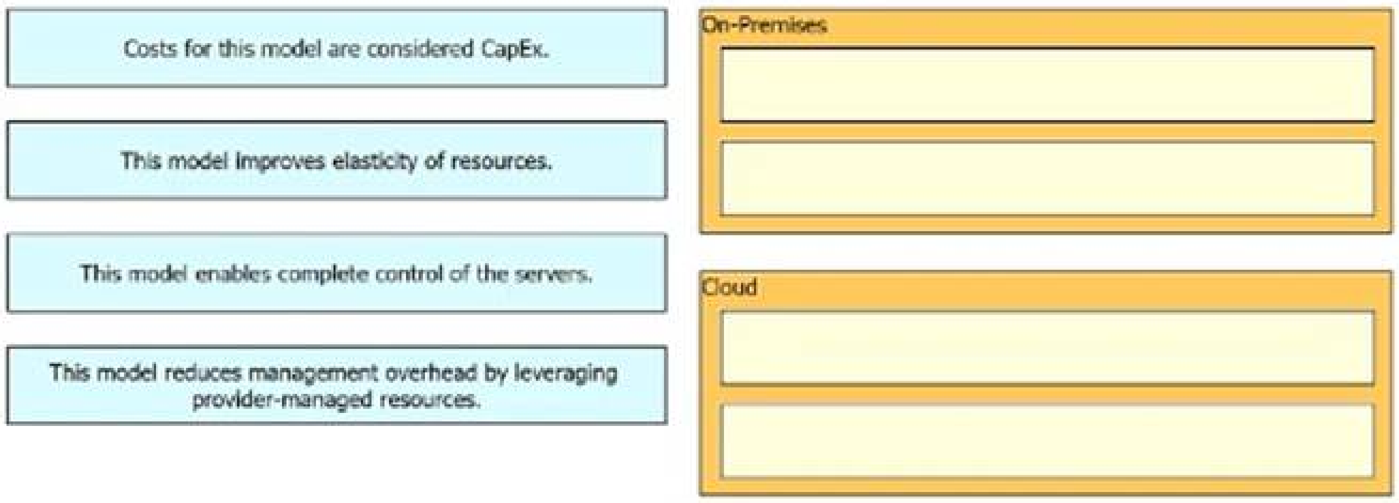
NEW QUESTION 186
- (Topic 2)
What NTP Stratum level is a server that is connected directly to an authoritative time source?

A. Stratum 0
B. Stratum 1
C. Stratum 14
D. Stratum 15

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/bsm/16-6-1/b-bsm-xe-16-6-1-asr920/bsm-timecalendar- set.html

NEW QUESTION 191
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the infrastructure deployment models on the right.



Costs for this model are considered CapEx.

This model improves elasticity of resources.

This model enables complete control of the servers.

This model reduces management overhead by leveraging provider-managed resources.

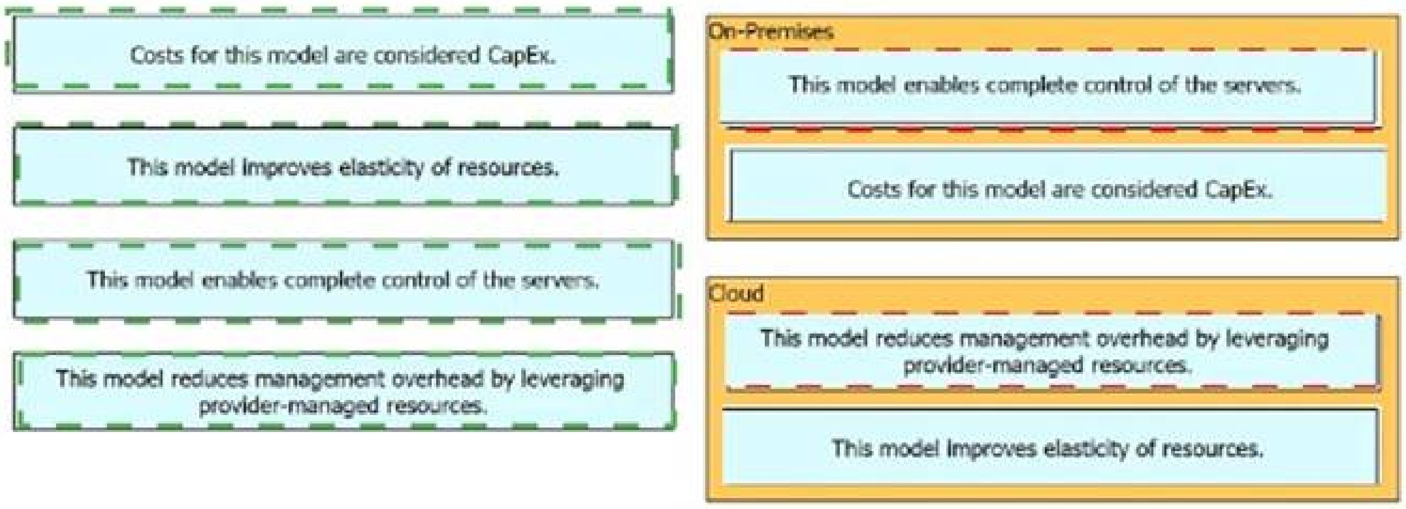
On-Premises

Cloud

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Costs for this model are considered CapEx.

This model improves elasticity of resources.

This model enables complete control of the servers.

This model reduces management overhead by leveraging provider-managed resources.

On-Premises

This model enables complete control of the servers.

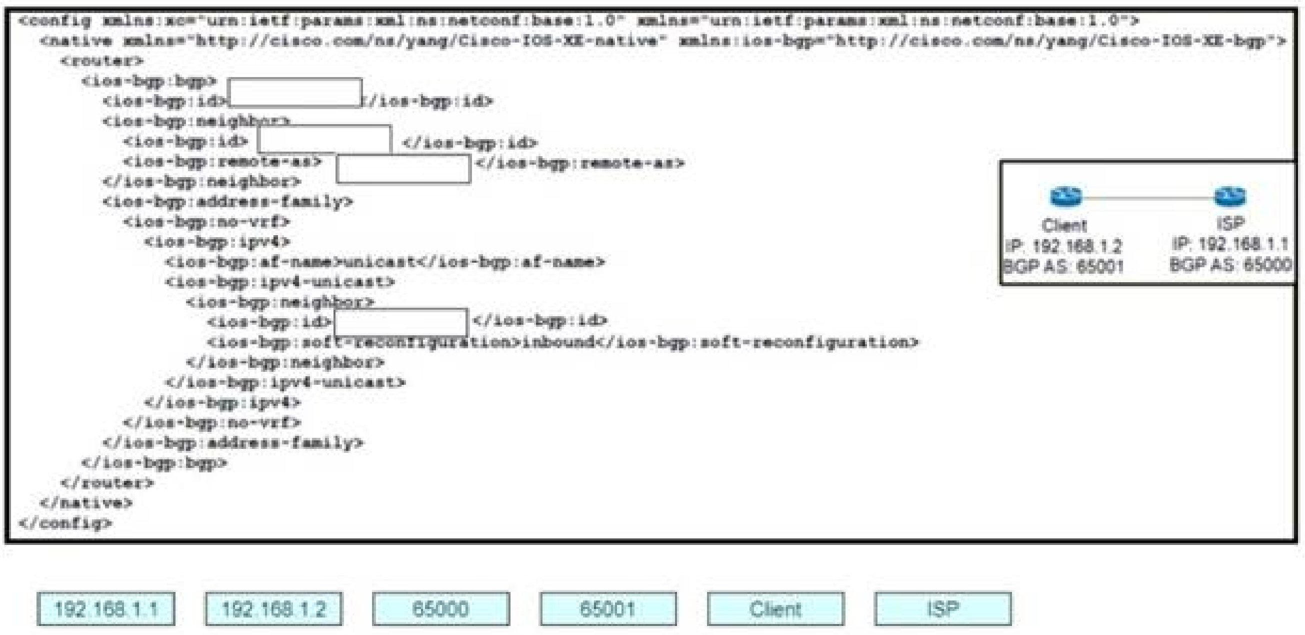
Costs for this model are considered CapEx.

Cloud

This model reduces management overhead by leveraging provider-managed resources.

This model improves elasticity of resources.

NEW QUESTION 194
DRAG DROP - (Topic 2)
Drag and drop the snippets onto the blanks within the code to construct a script that configures BGP according to the topology. Not all options are used, and some options may be used twice.



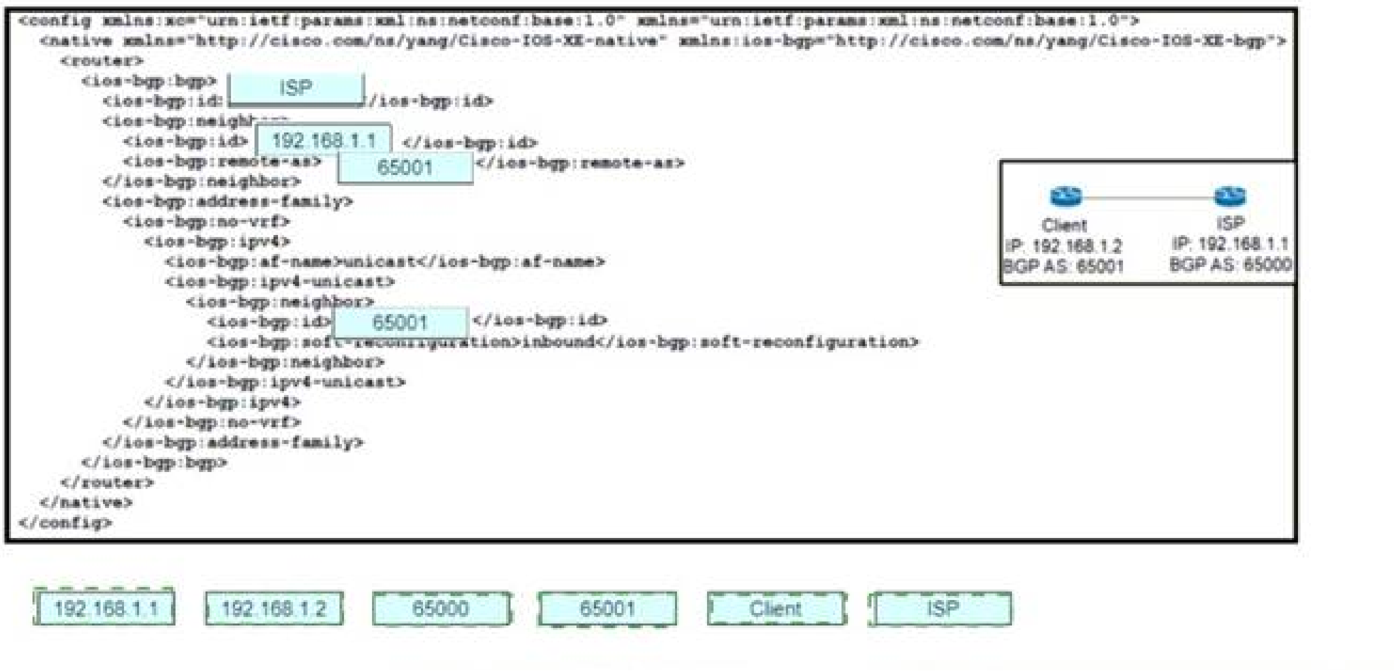
```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>
        <ios-bgp:id>            </ios-bgp:id>
        <ios-bgp:neighbor>
          <ios-bgp:id>            </ios-bgp:id>
          <ios-bgp:remote-as>            </ios-bgp:remote-as>
        </ios-bgp:neighbor>
        <ios-bgp:address-family>
          <ios-bgp:no-vrf>
            <ios-bgp:ipv4>
              <ios-bgp:af-name>unicast</ios-bgp:af-name>
              <ios-bgp:ipv4-unicast>
                <ios-bgp:neighbor>
                  <ios-bgp:id>            </ios-bgp:id>
                  <ios-bgp:soft-reconfiguration>inbound</ios-bgp:soft-reconfiguration>
                </ios-bgp:neighbor>
              </ios-bgp:ipv4-unicast>
            </ios-bgp:ipv4>
          </ios-bgp:no-vrf>
        </ios-bgp:address-family>
      </ios-bgp:bgp>
    </router>
  </native>
</config>
```

192.168.1.1 | 192.168.1.2 | 65000 | 65001 | Client | ISP

A. Mastered
B. Not Mastered

Answer: A

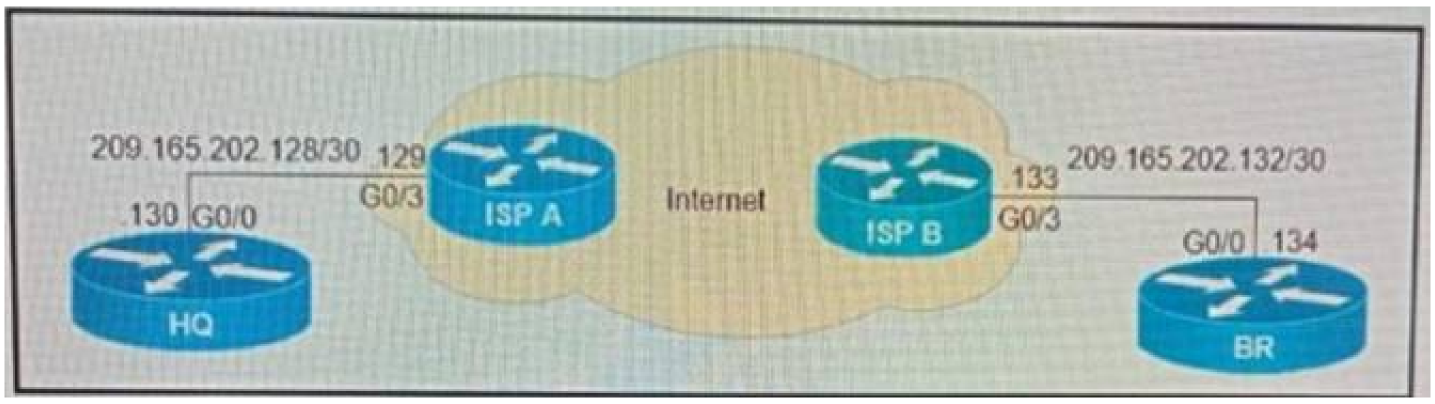
Explanation:



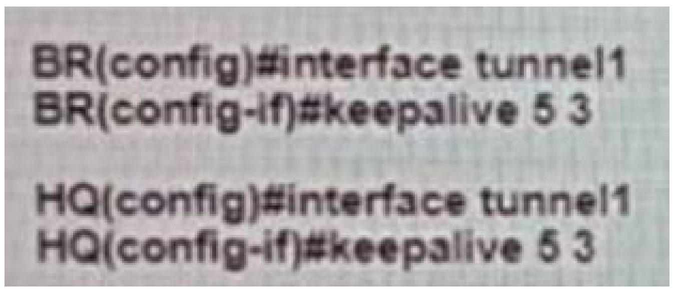
```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp> ISP
        <ios-bgp:id: </ios-bgp:id>
        <ios-bgp:neighb
          <ios-bgp:id> 192.168.1.1 </ios-bgp:id>
          <ios-bgp:remote-as> 65001 </ios-bgp:remote-as>
        </ios-bgp:neighbor>
        <ios-bgp:address-family>
          <ios-bgp:no-vrf>
            <ios-bgp:ipv4>
              <ios-bgp:af-name>unicast</ios-bgp:af-name>
              <ios-bgp:ipv4-unicast>
                <ios-bgp:neighbor>
                  <ios-bgp:id> 65001 </ios-bgp:id>
                  <ios-bgp:soft-reconfiguration>inbound</ios-bgp:soft-reconfiguration>
                </ios-bgp:neighbor>
              </ios-bgp:ipv4-unicast>
            </ios-bgp:ipv4>
          </ios-bgp:no-vrf>
        </ios-bgp:address-family>
      </ios-bgp:bgp>
    </router>
  </native>
</config>
```

192.168.1.1 | 192.168.1.2 | 65000 | 65001 | Client | ISP

NEW QUESTION 199
- (Topic 2)
Refer to the exhibit.



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



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

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

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

Answer: B

NEW QUESTION 201
- (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

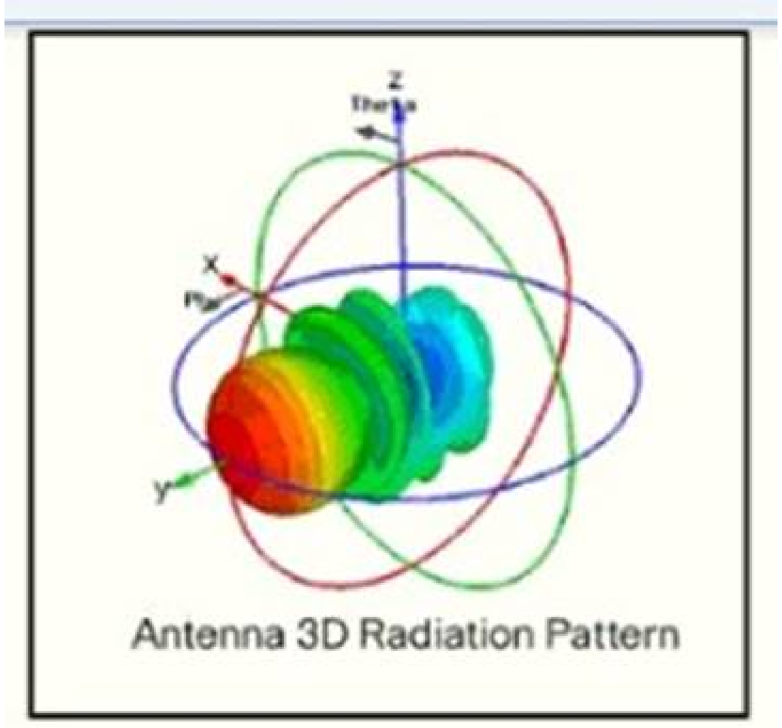
NEW QUESTION 203
- (Topic 2)
What is the responsibility of a secondary WLC?

A. It shares the traffic load of the LAPs with the primary controller.
B. It avoids congestion on the primary controller by sharing the registration load on the LAPs.
C. It registers the LAPs if the primary controller fails.
D. It enables Layer 2 and Layer 3 roaming between Itself and the primary controller.

Answer: C

NEW QUESTION 206
- (Topic 2)

Refer to the exhibit.



Which type of antenna does the radiation pattern represent?

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

Answer: A

NEW QUESTION 210
- (Topic 2)
Which technology is used as the basis for the cisco sd-access data plane?

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

Answer: C

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

NEW QUESTION 213
- (Topic 1)
Which component of the Cisco Cyber Threat Defense solution provides user and flow context analysis?

A. Cisco Firepower and FireSIGHT
B. Cisco Stealth watch system
C. Advanced Malware Protection
D. Cisco Web Security Appliance

Answer: B

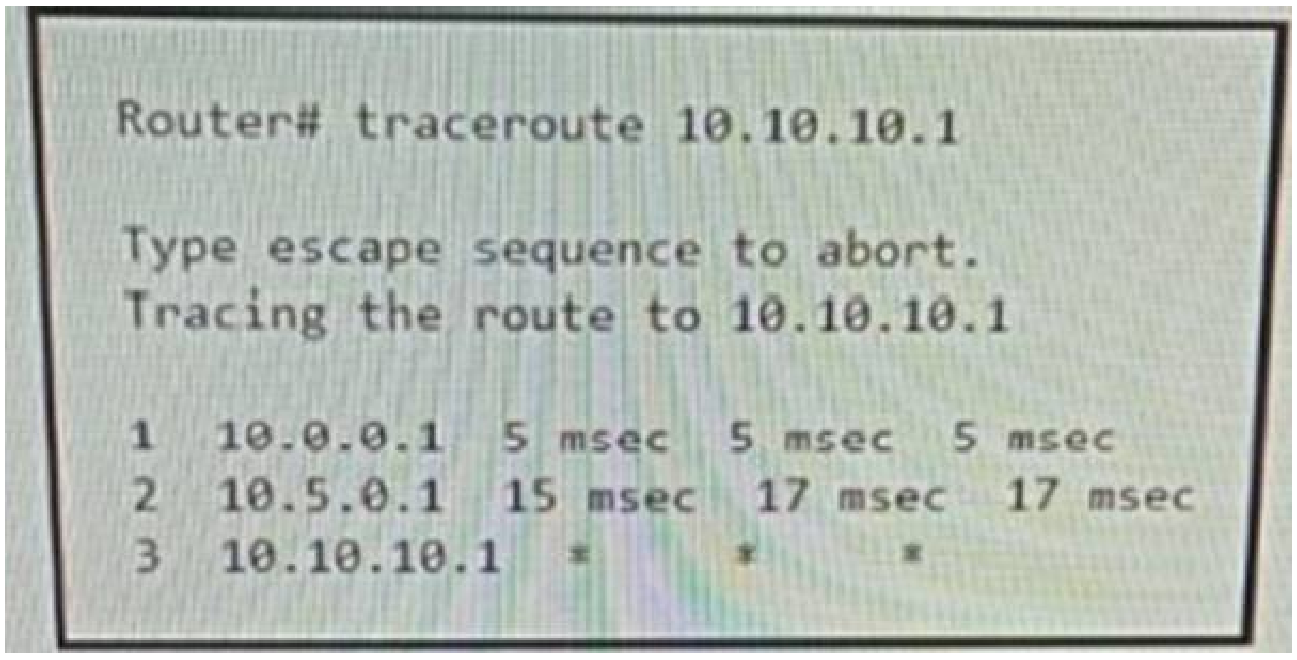
NEW QUESTION 217
- (Topic 1)
In cisco SD_WAN, which protocol is used to measure link quality?

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

Answer: B

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

NEW QUESTION 221
- (Topic 1)
Refer to the exhibit.



```
Router# traceroute 10.10.10.1

Type escape sequence to abort.
Tracing the route to 10.10.10.1

1  10.0.0.1   5 msec   5 msec   5 msec
2  10.5.0.1   15 msec  17 msec  17 msec
3  10.10.10.1   *        *        *
```

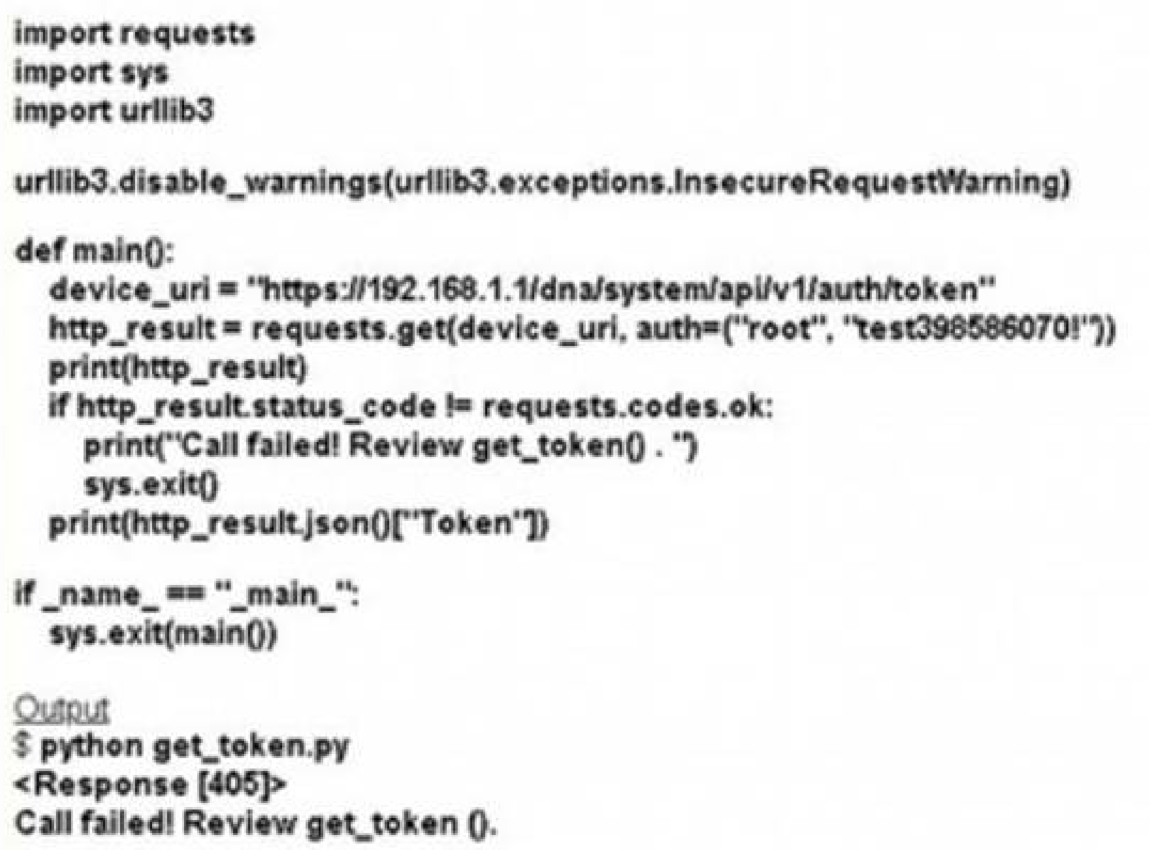
An engineer is troubleshooting a connectivity issue and executes a traceoute. What does the result confirm?

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

Answer: D

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

NEW QUESTION 223
- (Topic 1)
An engineer runs the code against an API of Cisco DMA Center, and the platform returns this output What does the response indicate?



```
import requests
import sys
import urllib3

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

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

if _name_ == "_main_":
   sys.exit(main())

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

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

Answer: D

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

NEW QUESTION 226
- (Topic 1)
What is a consideration when designing a Cisco SD-Access underlay network?

A. End user subnets and endpoints are part of the underlay network.
B. The underlay switches provide endpoint physical connectivity for users.

C. Static routing is a requirement,
D. It must support IPv4 and IPv6 underlay networks

Answer: B

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

NEW QUESTION 230
- (Topic 1)
How is Layer 3 roaming accomplished in a unified wireless deployment?

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

Answer: D

NEW QUESTION 232
- (Topic 1)
which entity is a Type 1 hypervisor?

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

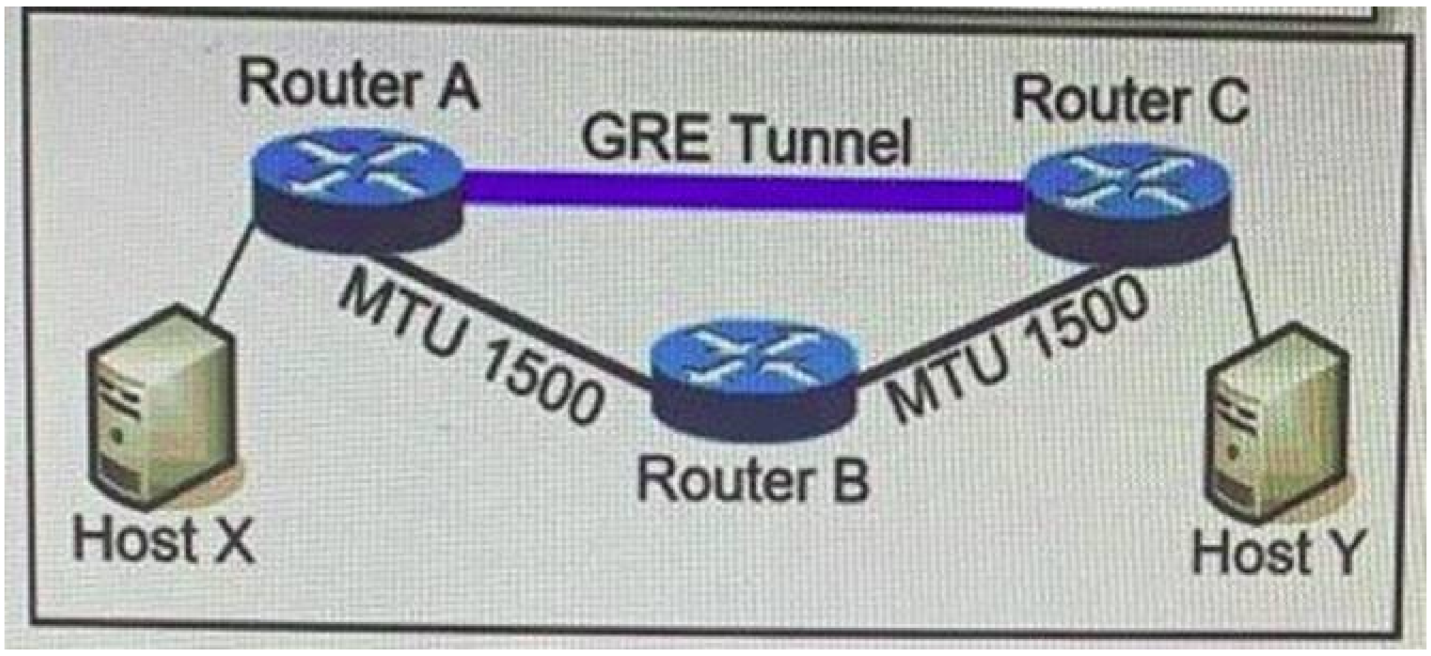
Answer: C

NEW QUESTION 234
- (Topic 1)
What is the centralized control policy in a Cisco SD-WAN deployment?

A. list of ordered statements that define user access policies
B. set of statements that defines how routing is performed
C. set of rules that governs nodes authentication within the cloud
D. list of enabled services for all nodes within the cloud

Answer: B

NEW QUESTION 236
- (Topic 1)
Refer to Exhibit.

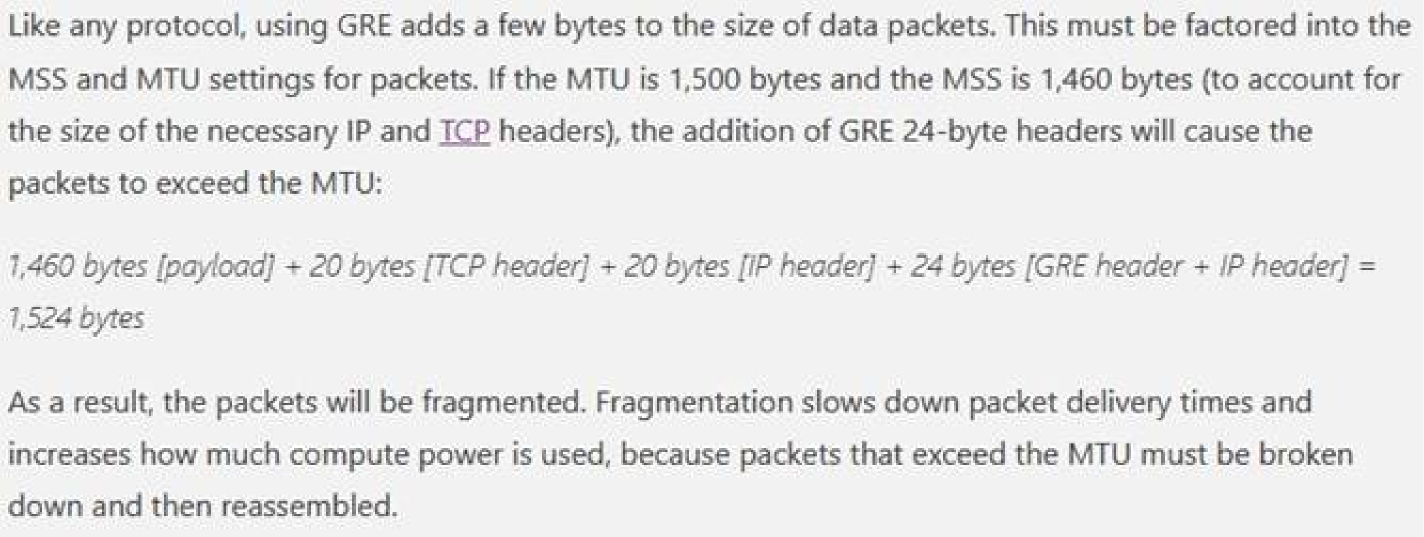


MTU has been configured on the underlying physical topology, and no MTU command has been configured on the tunnel interfaces. What happens when a 1500-byte IPv4 packet traverses the GRE tunnel from host X to host Y, assuming the DF bit is cleared?

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

Answer: D

Explanation:

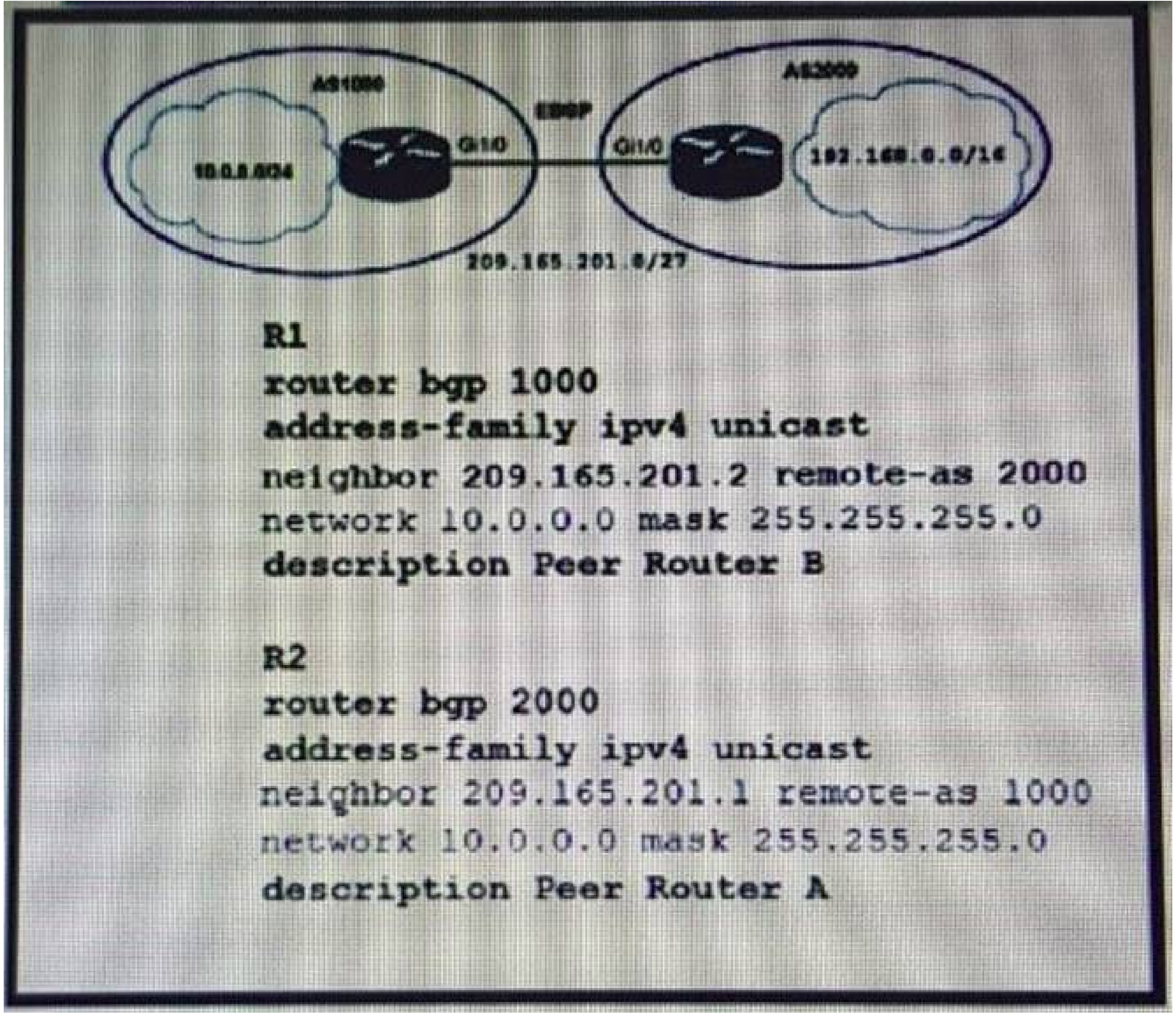


Like any protocol, using GRE adds a few bytes to the size of data packets. This must be factored into the MSS and MTU settings for packets. If the MTU is 1,500 bytes and the MSS is 1,460 bytes (to account for the size of the necessary IP and TCP headers), the addition of GRE 24-byte headers will cause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

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

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

NEW QUESTION 238
- (Topic 1)



```
R1
router bgp 1000
address-family ipv4 unicast
neighbor 209.165.201.2 remote-as 2000
network 10.0.0.0 mask 255.255.255.0
description Peer Router B

R2
router bgp 2000
address-family ipv4 unicast
neighbor 209.165.201.1 remote-as 1000
network 10.0.0.0 mask 255.255.255.0
description Peer Router A
```

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

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

Answer: BC

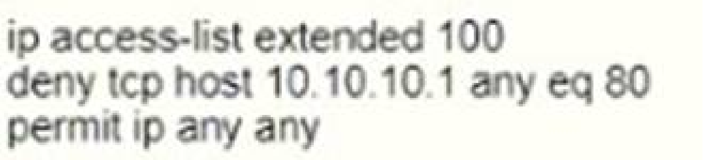
NEW QUESTION 242
- (Topic 1)
How are the different versions of IGMP compatible?

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

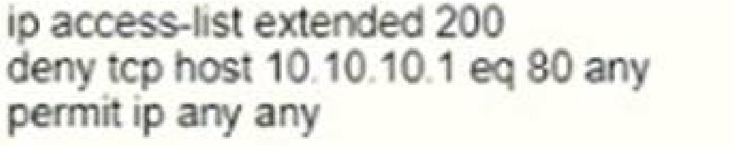
NEW QUESTION 247
- (Topic 1)
Which outbound access list, applied to the WAN interface of a router, permits all traffic except for http traffic sourced from the workstation with IP address 10.10.10.1?

A)



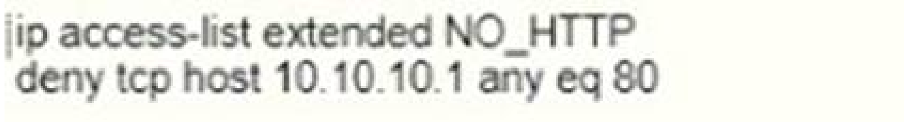
```
ip access-list extended 100
deny tcp host 10.10.10.1 any eq 80
permit ip any any
```

B)



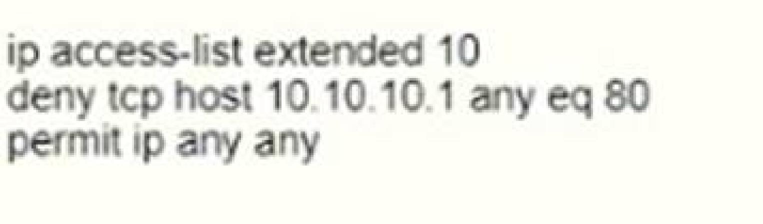
```
ip access-list extended 200
deny tcp host 10.10.10.1 eq 80 any
permit ip any any
```

C)



```
ip access-list extended NO_HTTP
deny tcp host 10.10.10.1 any eq 80
```

D)

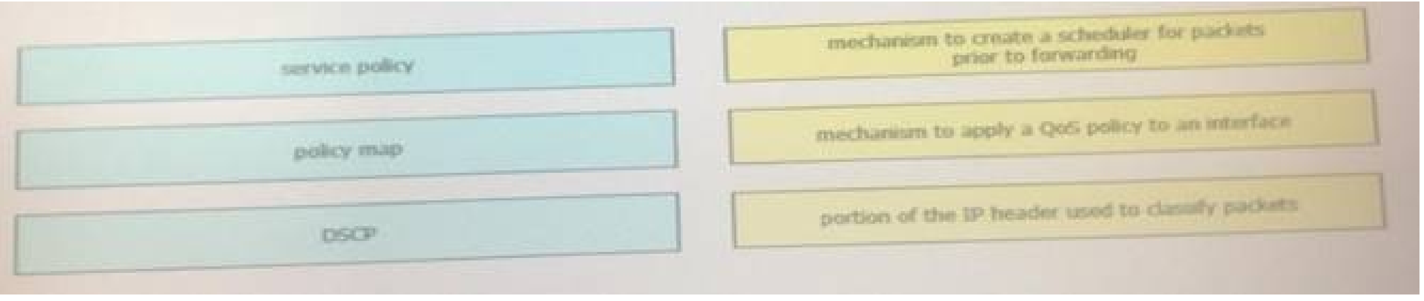


```
ip access-list extended 10
deny tcp host 10.10.10.1 any eq 80
permit ip any any
```

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

Answer: A

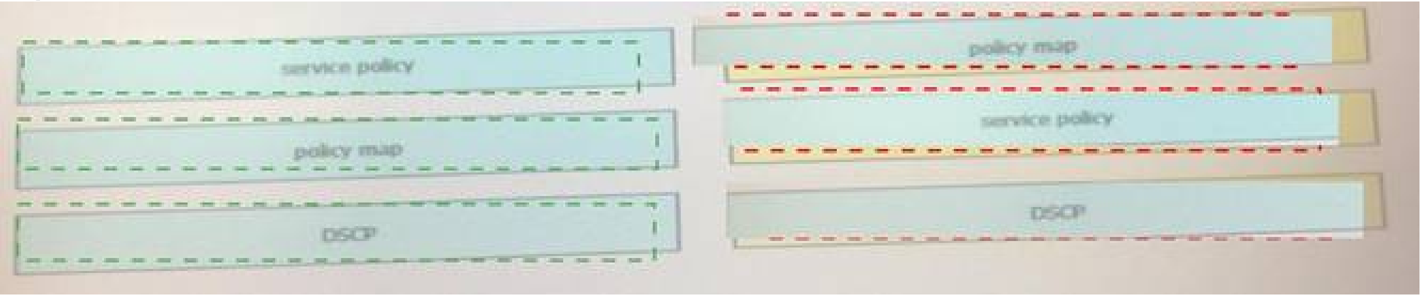
NEW QUESTION 252
DRAG DROP - (Topic 1)
Drag and drop the Qos mechanisms from the left to the correct descriptions on the right


service policy
policy map
DSCP
mechanism to create a scheduler for packets prior to forwarding
mechanism to apply a QoS policy to an interface
portion of the IP header used to classify packets

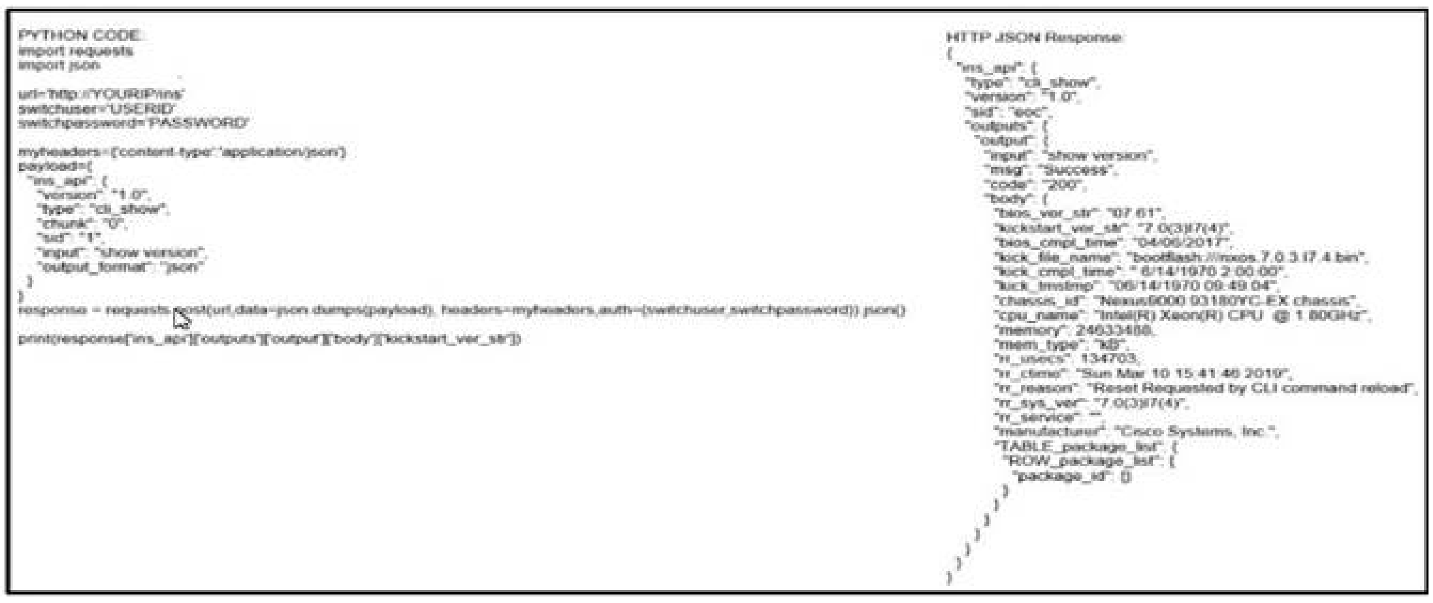
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 257
- (Topic 1)
Refer to the exhibit.



```
PYTHON CODE:
import requests
import json

url='http://YOURIP/ins'
switchuser='USERID'
switchpassword='PASSWORD'

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

print(response['ins_api']['outputs']['output']['body']['kickstart_ver_str'])
```

```
HTTP JSON Response:
{
  "ins_api": {
    "type": "cli_show",
    "version": "1.0",
    "sid": "eoc",
    "outputs": {
      "output": {
        "input": "show version",
        "msg": "Success",
        "code": "200",
        "body": {
          "bios_ver_str": "07.61",
          "kickstart_ver_str": "7.0(3)I7(4)",
          "bios_cmpl_time": "04/06/2017",
          "kick_file_name": "bootflash:///nxos.7.0.3.I7.4.bin",
          "kick_cmpl_time": " 6/14/1970 2:00:00",
          "kick_tmstmp": "06/14/1970 09:49:04",
          "chassis_id": "Nexus9000 93180YC-EX chassis",
          "cpu_name": "Intel(R) Xeon(R) CPU  @ 1.80GHz",
          "memory": 24633488,
          "mem_type": "kB",
          "rr_usecs": 134703,
          "rr_ctime": "Sun Mar 10 15:41:46 2019",
          "rr_reason": "Reset Requested by CLI command reload",
          "rr_sys_ver": "7.0(3)I7(4)",
          "rr_service": "",
          "manufacturer": "Cisco Systems, Inc.",
          "TABLE_package_list": {
            "ROW_package_list": {
              "package_id": {}
            }
          }
        }
      }
    }
  }
}
```

Which HTTP JSON response does the python code output give?

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

Answer: D

NEW QUESTION 259
- (Topic 1)
When configuration WPA2 Enterprise on a WLAN, which additional security component configuration is required?

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

Answer: C

NEW QUESTION 260
- (Topic 1)
Which statement about TLS is accurate when using RESTCONF to write configurations on network devices?

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

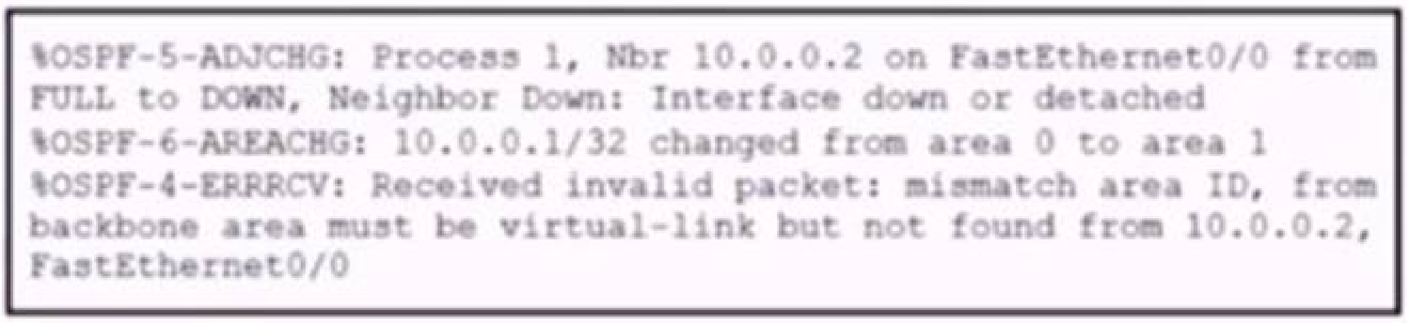
Answer: B

NEW QUESTION 264
- (Topic 1)
Which two network problems Indicate a need to implement QoS in a campus network? (Choose two.)

A. port flapping
B. excess jitter
C. misrouted network packets
D. duplicate IP addresses
E. bandwidth-related packet loss

Answer: BE

NEW QUESTION 267
- (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

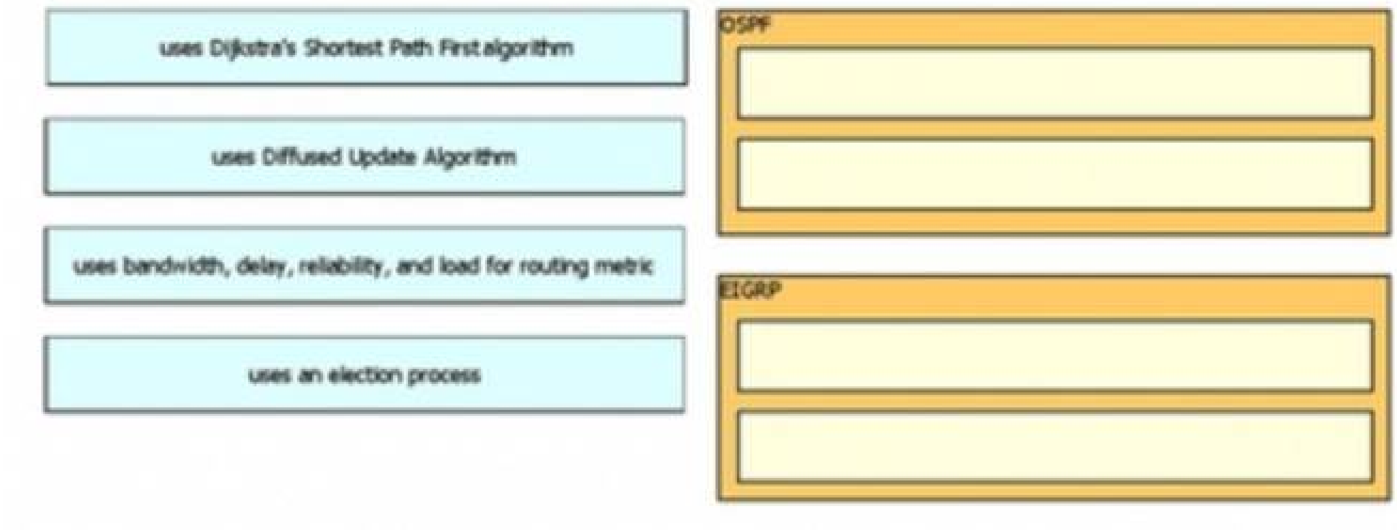
Answer: B

NEW QUESTION 269
- (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 270
DRAG DROP - (Topic 1)
Drag and drop the characteristics from the left onto the protocols they apply to on the right?



uses Dijkstra's Shortest Path First algorithm

uses Diffused Update Algorithm

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

uses an election process

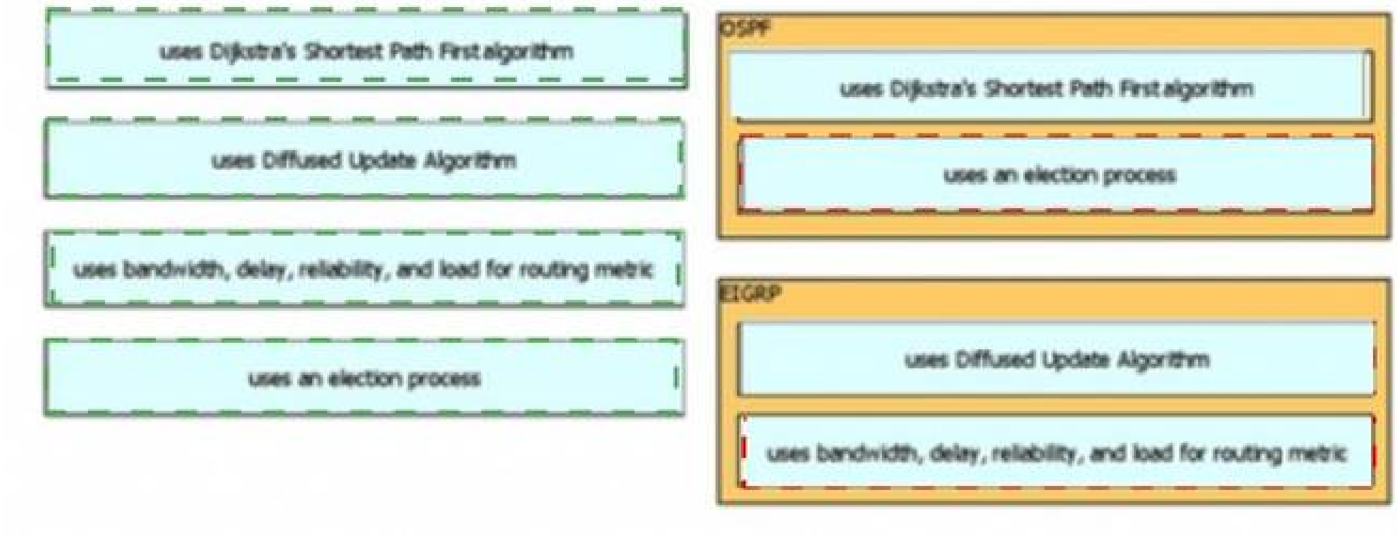
OSPF

EIGRP

A. Mastered
B. Not Mastered

Answer: A

Explanation:



uses Dijkstra's Shortest Path First algorithm

uses Diffused Update Algorithm

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

uses an election process

OSPF

uses Dijkstra's Shortest Path First algorithm

uses an election process

EIGRP

uses Diffused Update Algorithm

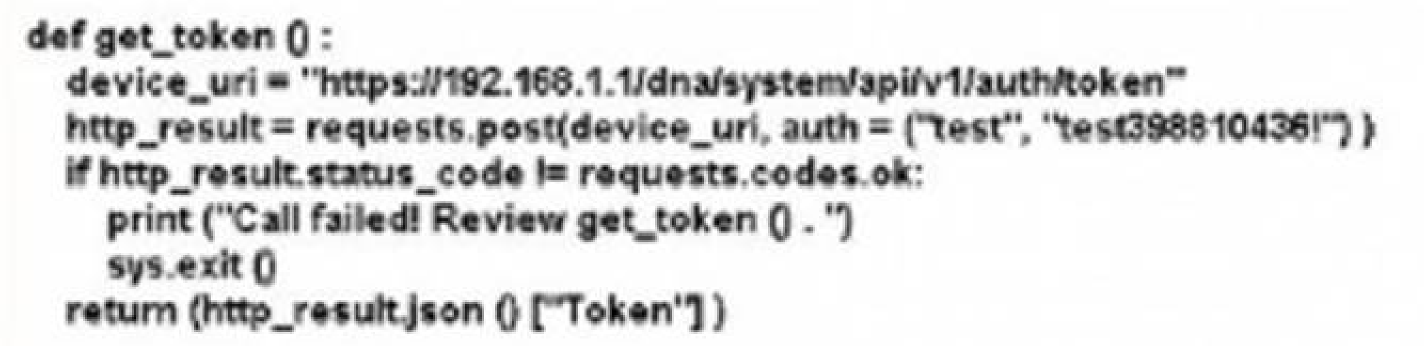
uses bandwidth, delay, reliability, and load for routing metric

NEW QUESTION 274
- (Topic 1)
When is an external antenna used inside a building?

A. only when using Mobility Express
B. when it provides the required coverage
C. only when using 2 4 GHz
D. only when using 5 GHz

Answer: B

NEW QUESTION 279
- (Topic 1)
Which HTTP code must be returned to prevent the script form exiting?



```
def get_token () :
    device_uri = "https://192.168.1.1/dna/system/api/v1/auth/token"
    http_result = requests.post(device_uri, auth = ("test", "test398810436!") )
    if http_result.status_code != requests.codes.ok:
        print ("Call failed! Review get_token () . ")
        sys.exit ()
    return (http_result.json () ["Token"] )
```

A. 200
B. 201
C. 300
D. 301

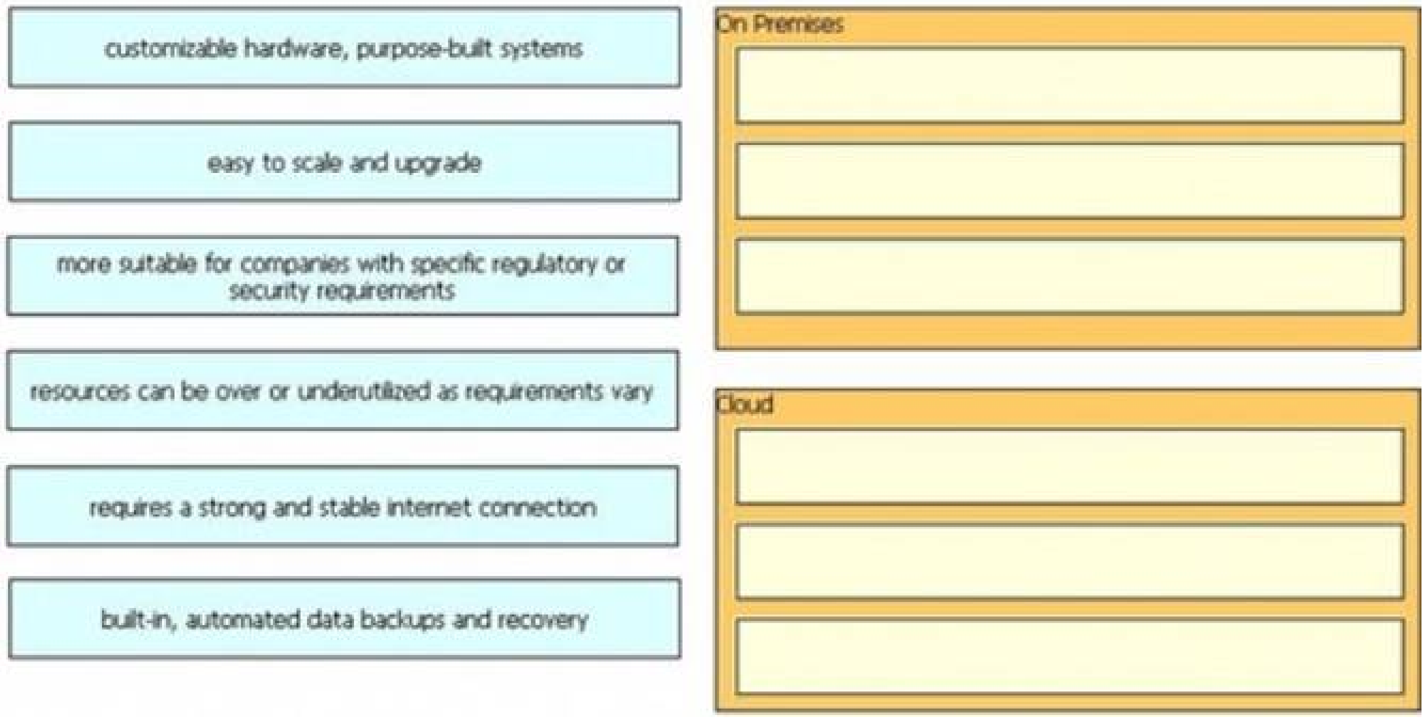
Answer: A

NEW QUESTION 283
- (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 287
DRAG DROP - (Topic 1)
Drag and drop the characteristics from the left onto the appropriate infrastructure deployment types on the right.



customizable hardware, purpose-built systems

easy to scale and upgrade

more suitable for companies with specific regulatory or security requirements

resources can be over or underutilized as requirements vary

requires a strong and stable internet connection

built-in, automated data backups and recovery

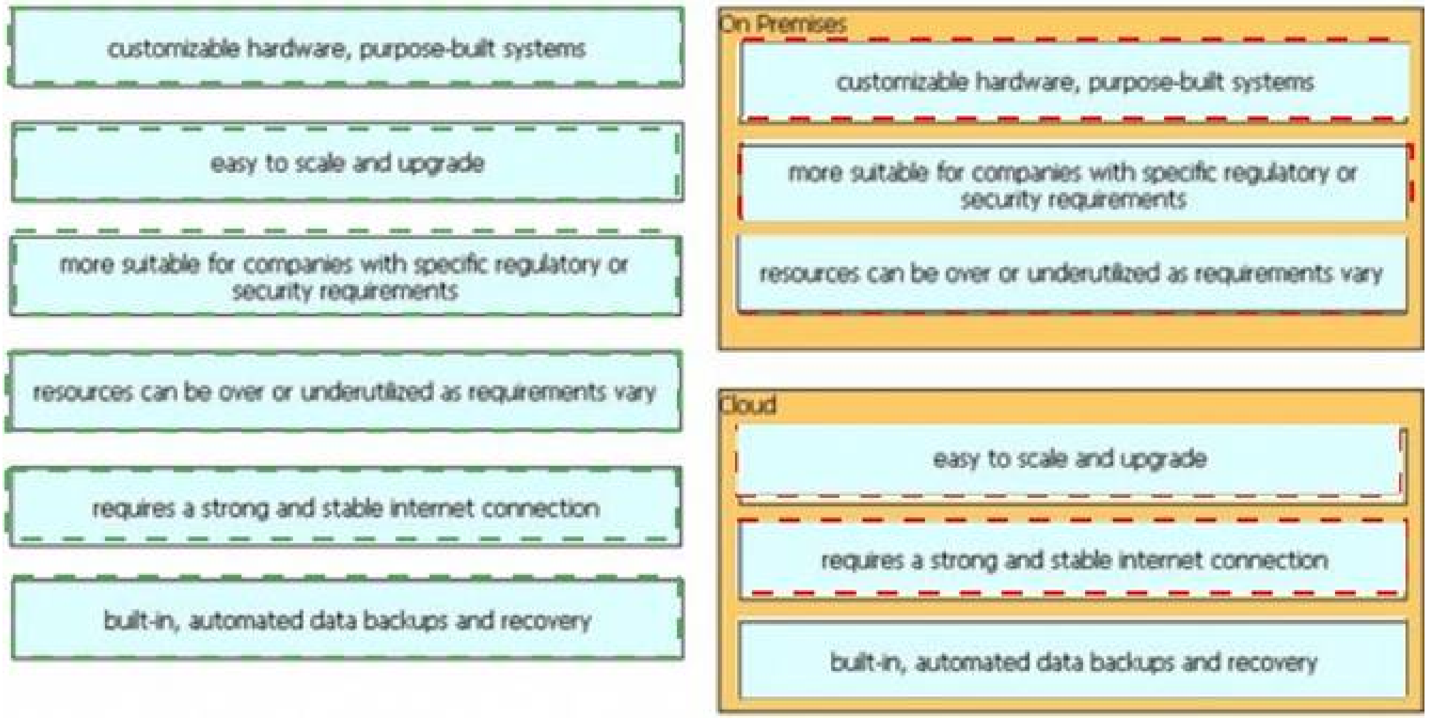
On Premises

Cloud

A. Mastered
B. Not Mastered

Answer: A

Explanation:



customizable hardware, purpose-built systems

easy to scale and upgrade

more suitable for companies with specific regulatory or security requirements

resources can be over or underutilized as requirements vary

requires a strong and stable internet connection

built-in, automated data backups and recovery

On Premises

customizable hardware, purpose-built systems

more suitable for companies with specific regulatory or security requirements

resources can be over or underutilized as requirements vary

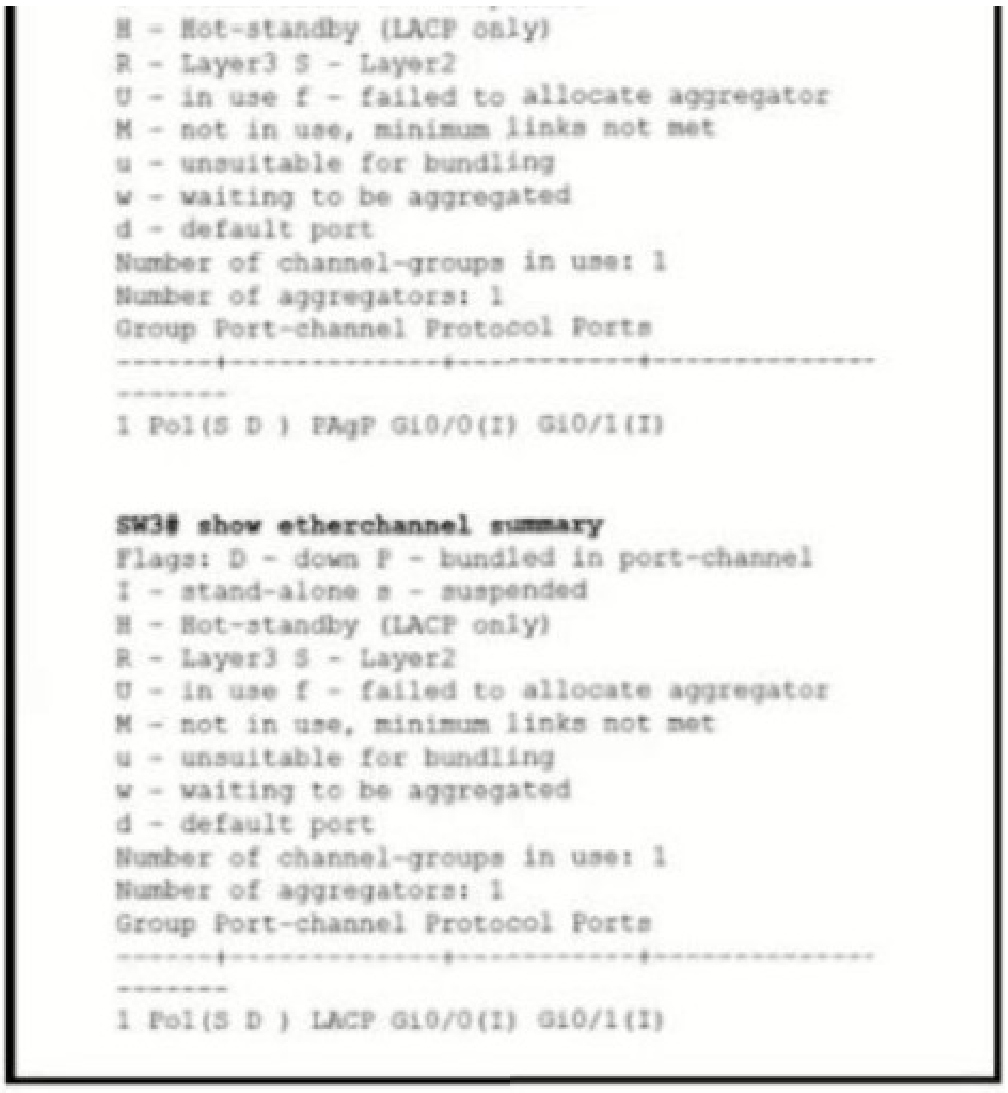
Cloud

easy to scale and upgrade

requires a strong and stable internet connection

built-in, automated data backups and recovery

NEW QUESTION 291
- (Topic 1)
Refer to the exhibit.



```
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+--------------
-------
1 Pol(S D ) PAgP Gi0/0(I) Gi0/1(I)


SW3# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+--------------
-------
1 Pol(S D ) LACP Gi0/0(I) Gi0/1(I)
```

Which action resolves the EtherChannel issue between SW2 and SW3?

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

Answer: D

NEW QUESTION 292
- (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

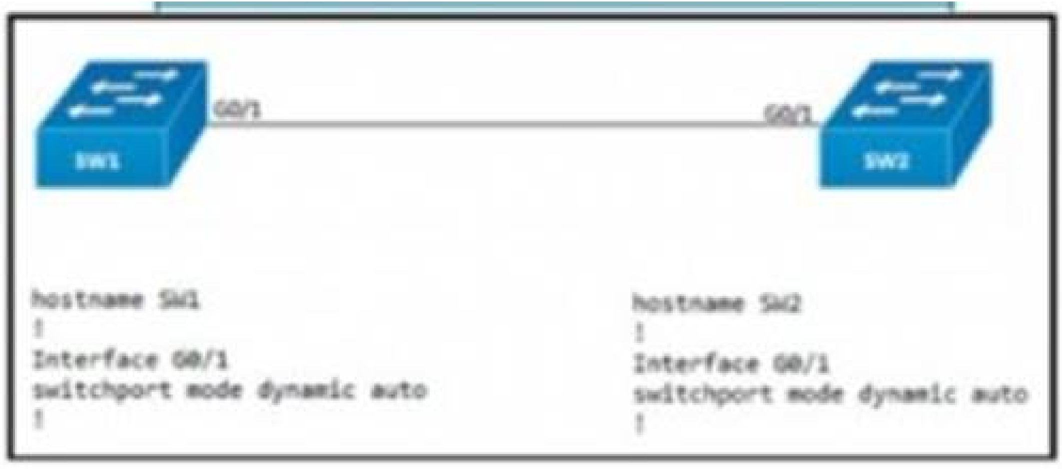
NEW QUESTION 296

- (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 though 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 297
- (Topic 1)



```
hostname SW1
!
Interface G0/1
switchport mode dynamic auto
!
```

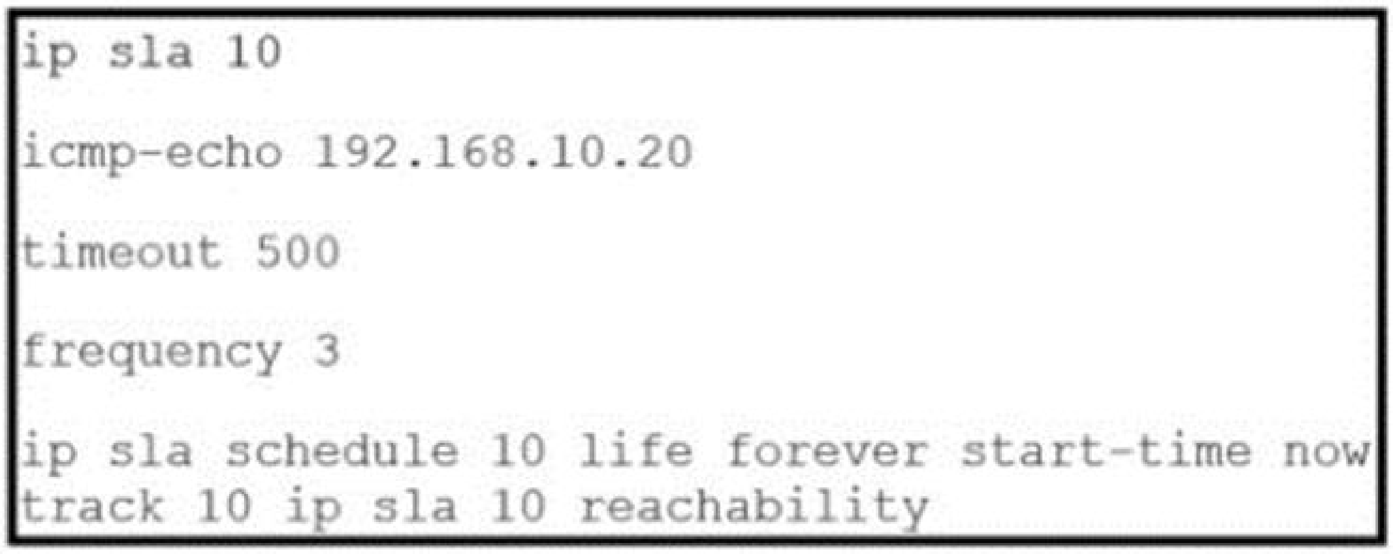
```
hostname SW2
!
Interface G0/1
switchport mode dynamic auto
!
```

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 298
- (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
```

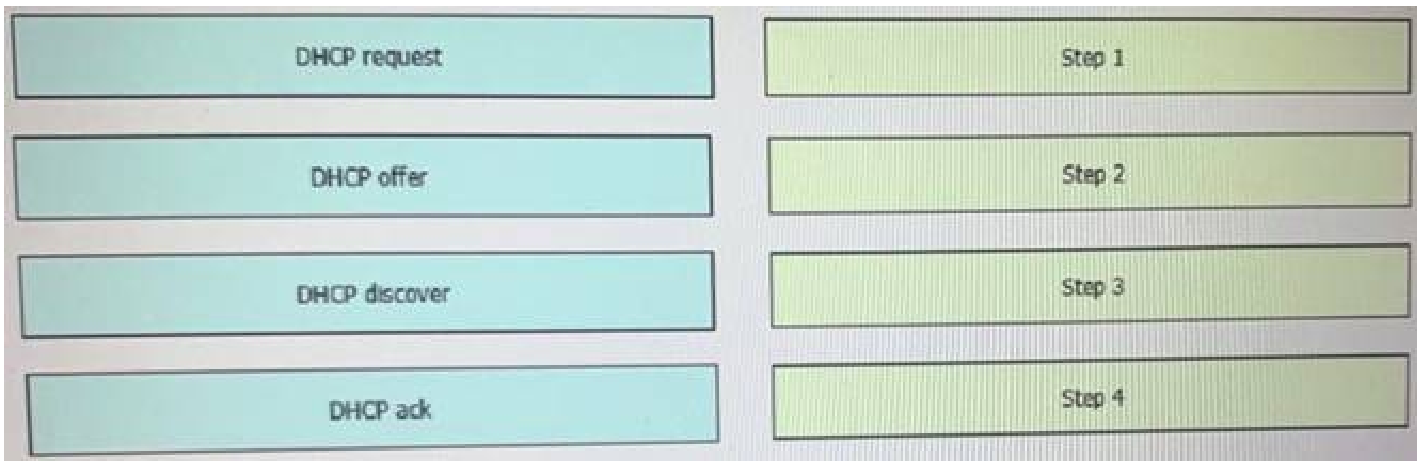
The IP SLA is configured in a router. An engineer must configure an EEM applet to shut down the interface and bring it back up when there is a problem with the IP SLA. Which configuration should the engineer use?

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 302
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

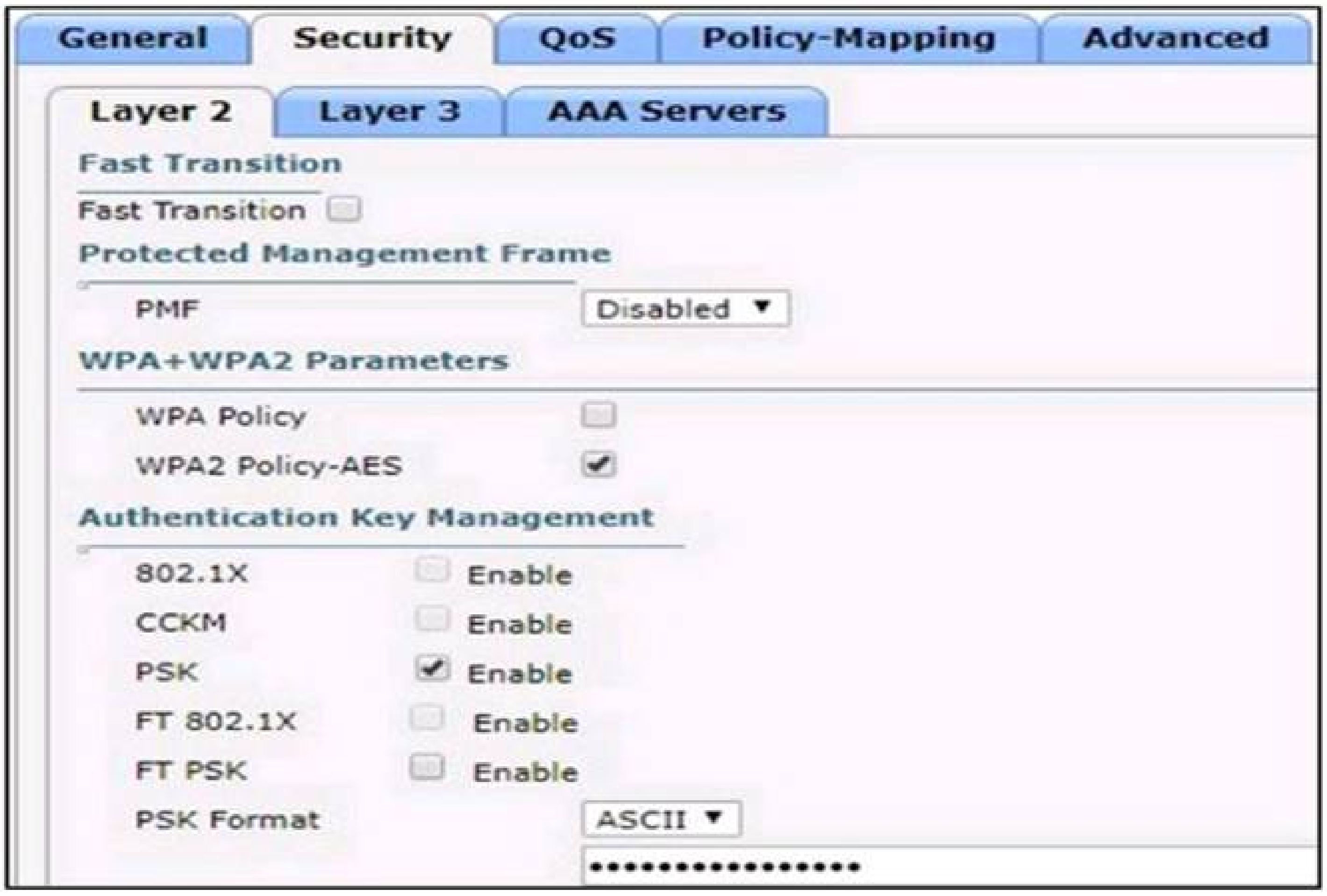
Explanation:
There are four messages sent between the DHCP Client and DHCP Server: DHCPD ISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACKNOWLEDGEMENT.
This process is often abbreviated as DORA (for Discover, Offer, Request, Acknowledgement).

NEW QUESTION 304
- (Topic 1)
How is 802.11 traffic handled in a fabric-enabled SSID?

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

Answer: B

NEW QUESTION 309
- (Topic 1)
Refer to the exhibit.



Fast Transition
Fast Transition □
Protected Management Frame
PMF Disabled ▼
WPA+WPA2 Parameters
WPA Policy □
WPA2 Policy-AES ☑
Authentication Key Management
802.1X □ Enable
CCKM □ Enable
PSK ☑ Enable
FT 802.1X □ Enable
FT PSK □ Enable
PSK Format ASCII ▼
••••••••••••••••

Based on the configuration in this WLAN security setting, Which method can a client use to authenticate to the network?

A. text string
B. username and password
C. certificate
D. RADIUS token

Answer: A

NEW QUESTION 312
- (Topic 1)
What is a characteristic of a virtual machine?

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

Answer: D

NEW QUESTION 316
- (Topic 1)
Which controller is capable of acting as a STUN server during the onboarding process of Edge devices?

A. vBond
B. vSmart
C. vManage
D. PNP server

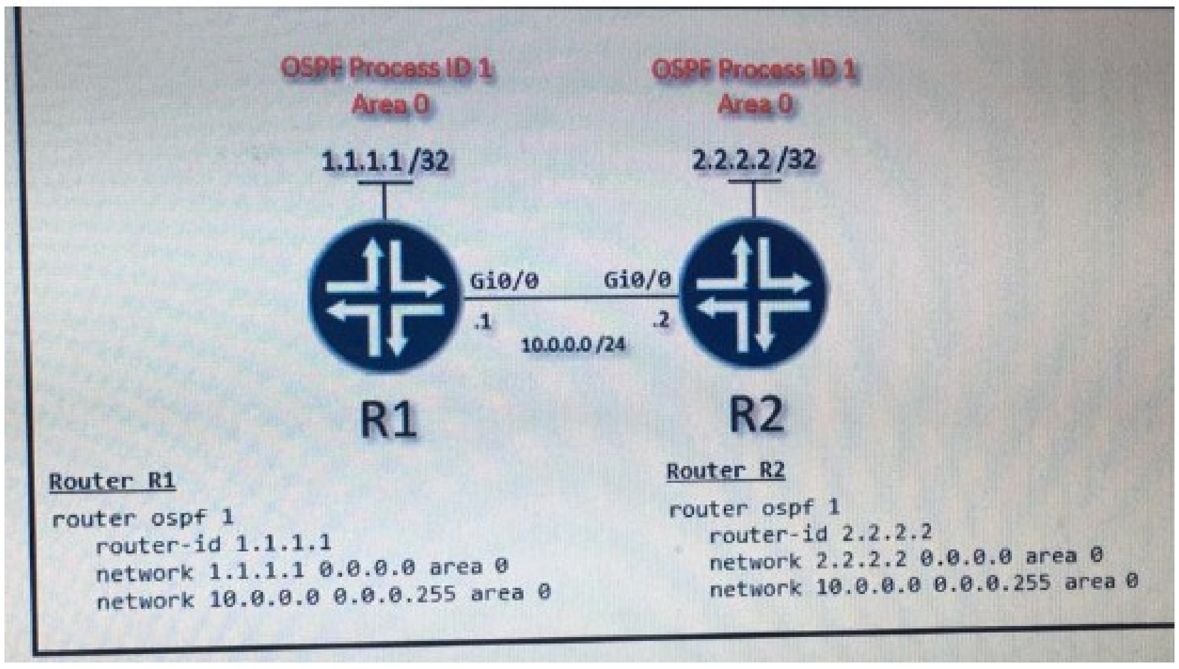
Answer: A

NEW QUESTION 321
- (Topic 1)
What are two benefits of virtual switching when compared to hardware switching? (Choose two.)

A. increased MTU size
B. hardware independence
C. VM-level isolation
D. increased flexibility
E. extended 802.1Q VLAN range

Answer: CD

NEW QUESTION 326
- (Topic 1)
Refer to the exhibit.



Router R1

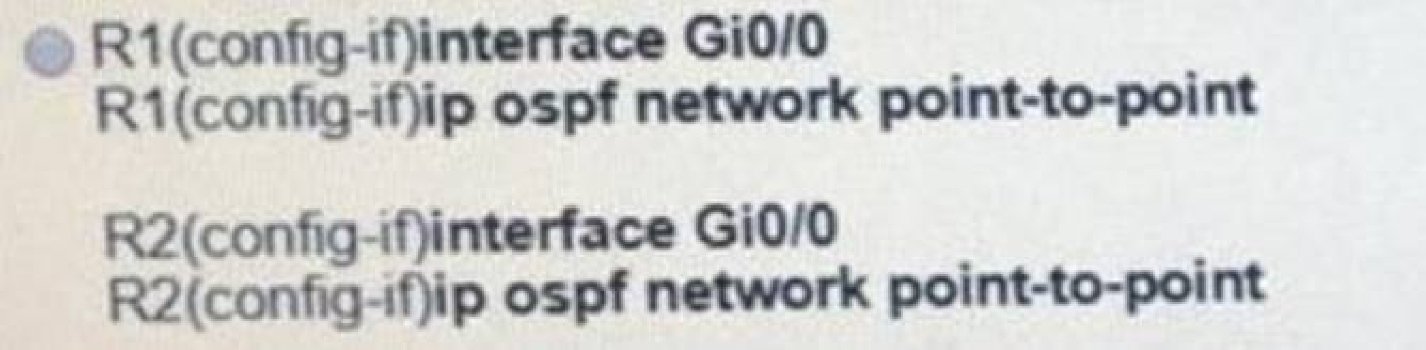
```
router ospf 1
   router-id 1.1.1.1
   network 1.1.1.1 0.0.0.0 area 0
   network 10.0.0.0 0.0.0.255 area 0
```

Router R2

```
router ospf 1
   router-id 2.2.2.2
   network 2.2.2.2 0.0.0.0 area 0
   network 10.0.0.0 0.0.0.255 area 0
```

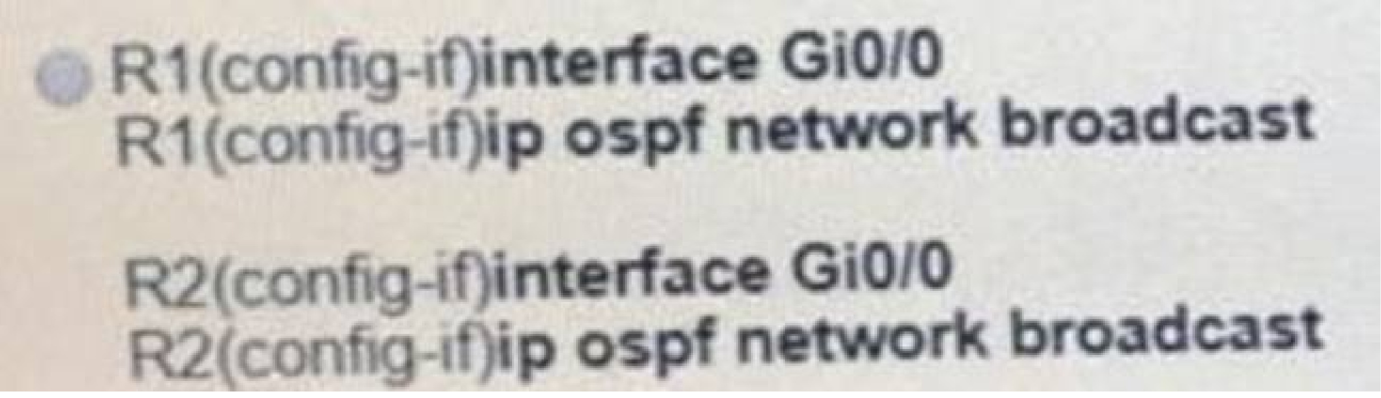
A network engineer is configuring OSPF between router R1 and router R2. The engineer must ensure that a DR/BDR election does not occur on the Gigabit Ethernet interfaces in area 0. Which configuration set accomplishes this goal?

A)



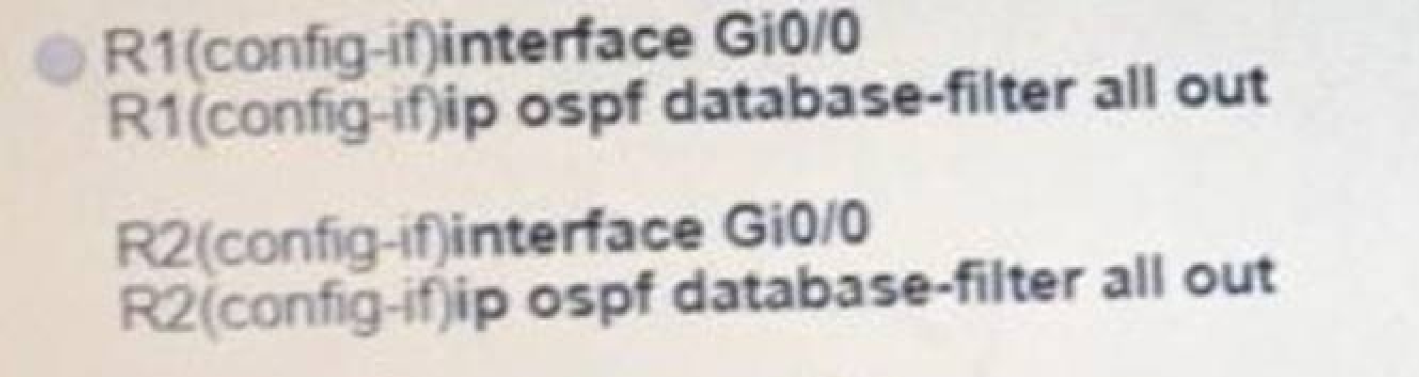
```
○ R1(config-if)interface Gi0/0
  R1(config-if)ip ospf network point-to-point

  R2(config-if)interface Gi0/0
  R2(config-if)ip ospf network point-to-point
```

B)



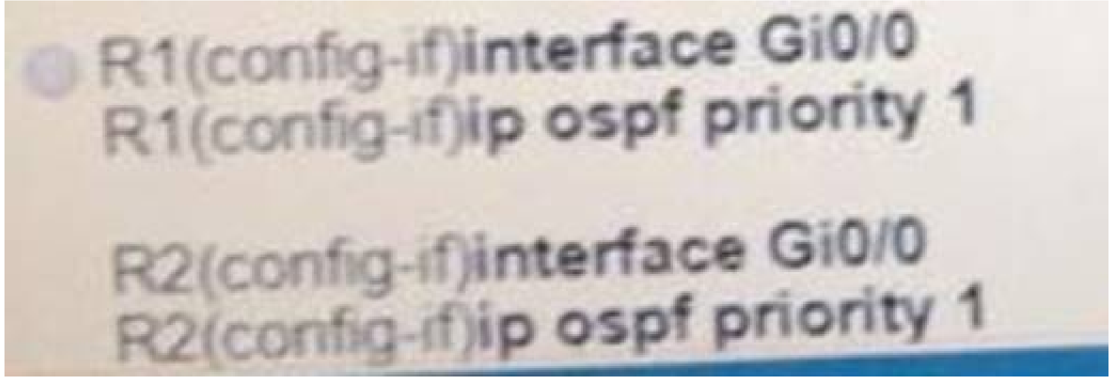
```
○ R1(config-if)interface Gi0/0
  R1(config-if)ip ospf network broadcast

  R2(config-if)interface Gi0/0
  R2(config-if)ip ospf network broadcast
```

C)



```
R1(config-if)interface Gi0/0
R1(config-if)ip ospf database-filter all out

R2(config-if)interface Gi0/0
R2(config-if)ip ospf database-filter all out
```

D)



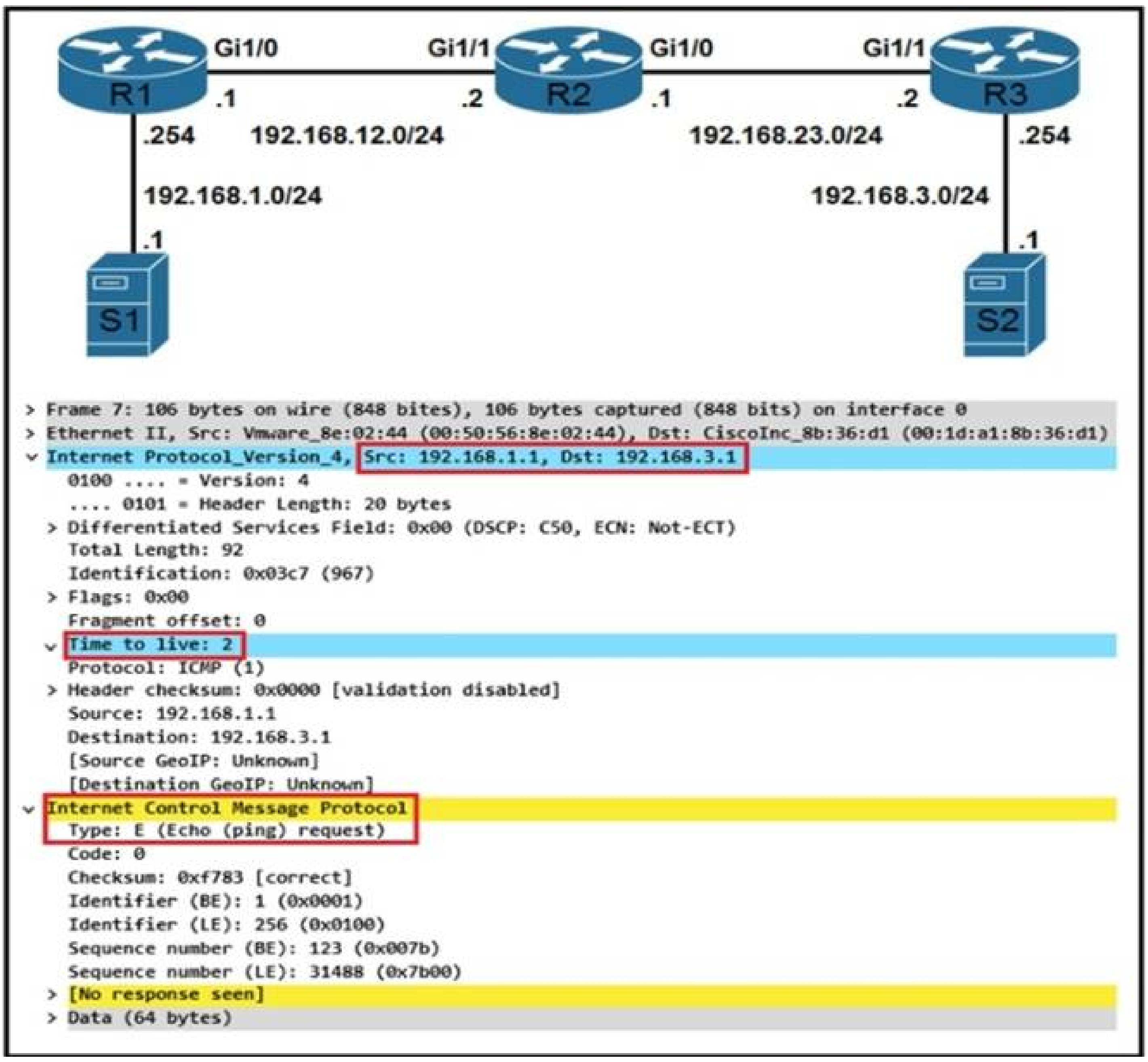
```
R1(config-if)interface Gi0/0
R1(config-if)ip ospf priority 1

R2(config-if)interface Gi0/0
R2(config-if)ip ospf priority 1
```

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

Answer: A

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

NEW QUESTION 331
- (Topic 1)
Refer to the exhibit.



```
> Frame 7: 106 bytes on wire (848 bites), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Vmware_8e:02:44 (00:50:56:8e:02:44), Dst: CiscoInc_8b:36:d1 (00:1d:a1:8b:36:d1)
v Internet Protocol_Version_4, Src: 192.168.1.1, Dst: 192.168.3.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x00 (DSCP: C50, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x03c7 (967)
  > Flags: 0x00
    Fragment offset: 0
  v Time to live: 2
    Protocol: ICMP (1)
  > Header checksum: 0x0000 [validation disabled]
    Source: 192.168.1.1
    Destination: 192.168.3.1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Internet Control Message Protocol
    Type: E (Echo (ping) request)
    Code: 0
    Checksum: 0xf783 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 123 (0x007b)
    Sequence number (LE): 31488 (0x7b00)
  > [No response seen]
  > Data (64 bytes)
```

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

A. The packet reaches R3, and the TTL expires
B. R2 replies with a TTL exceeded message
C. R3 replies with a TTL exceeded message.

D. The packet reaches R2 and the TTL expires
E. R1 replies with a TTL exceeded message
F. The packet reaches R1 and the TTL expires.

Answer: AD

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

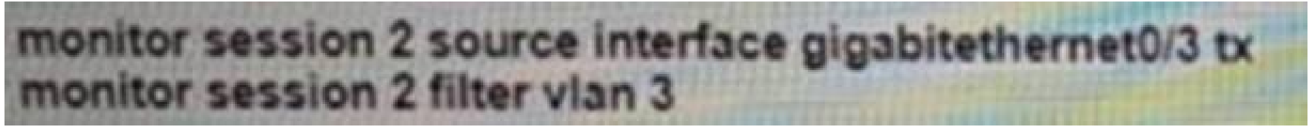
NEW QUESTION 333
- (Topic 1)
Which two threats does AMP4E have the ability to block? (Choose two.)

A. DDoS
B. ransomware
C. Microsoft Word macro attack
D. SQL injection
E. email phishing

Answer: BC

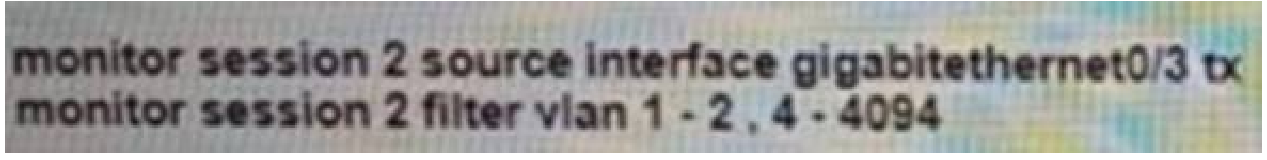
Explanation:
https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/c11-742008-00-cisco-amp-for-endpoints-wp-v2a.pdf

NEW QUESTION 335
- (Topic 1)
Which command set configures RSPAN to capture outgoing traffic from VLAN 3 on interface GigabitEthernet 0/3 while ignoring other VLAN traffic on the same interface?
A)



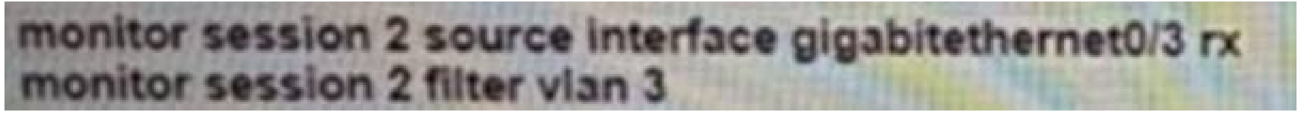
```
monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 3
```

B)



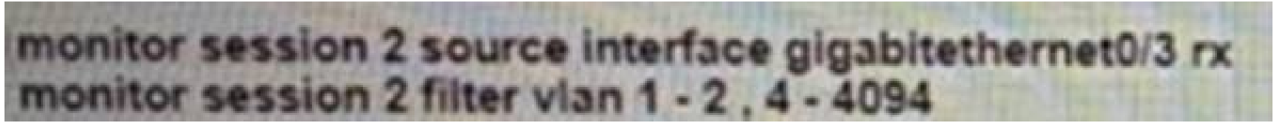
```
monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 1 - 2 , 4 - 4094
```

C)



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

D)



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

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

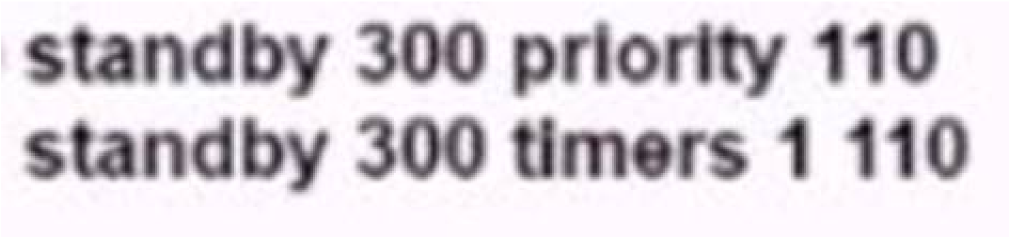
Answer: A

NEW QUESTION 338
- (Topic 1)
What is a benefit of a virtual machine when compared with a physical server?

A. Multiple virtual servers can be deployed on the same physical server without having to buy additional hardware.
B. Virtual machines increase server processing performance.
C. The CPU and RAM resources on a virtual machine cannot be affected by other virtual machines.
D. Deploying a virtual machine is technically less complex than deploying a physical server.

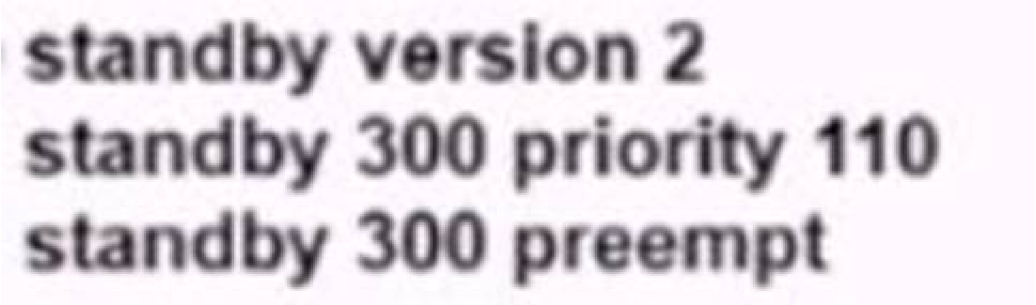
Answer: A

NEW QUESTION 342
- (Topic 1)
An engineer must configure HSRP group 300 on a Cisco IOS router. When the router is functional, it must be the must be the active HSRP router. The peer router has been configured using the default priority value. Which command set is required?
A)



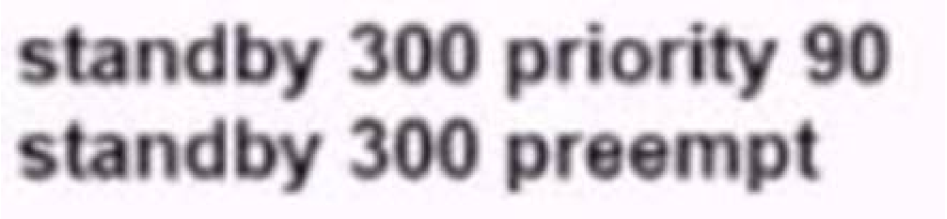
```
standby 300 priority 110
standby 300 timers 1 110
```

B)



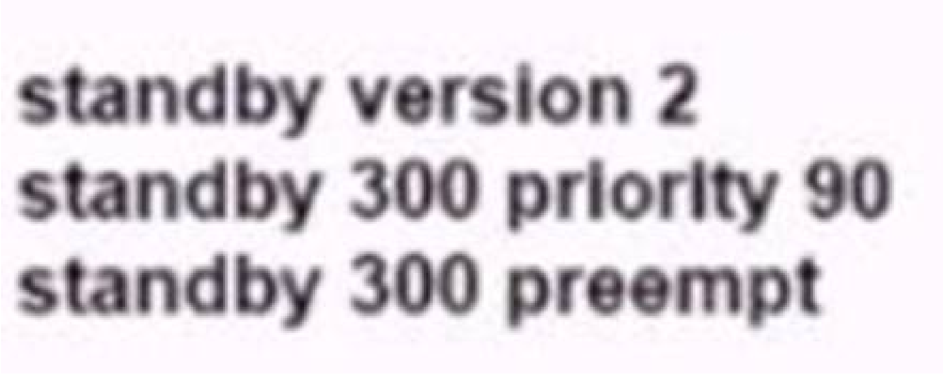
```
standby version 2
standby 300 priority 110
standby 300 preempt
```

C)



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

D)

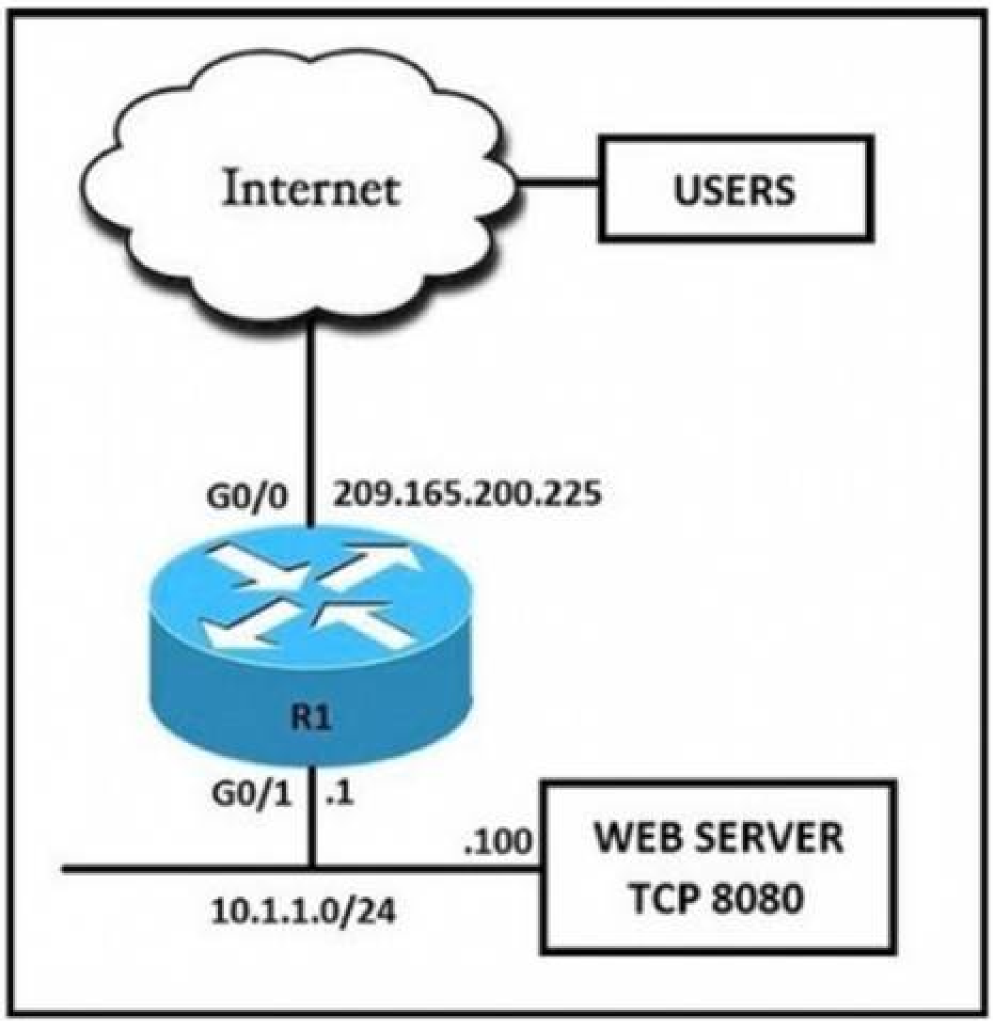


```
standby version 2
standby 300 priority 90
standby 300 preempt
```

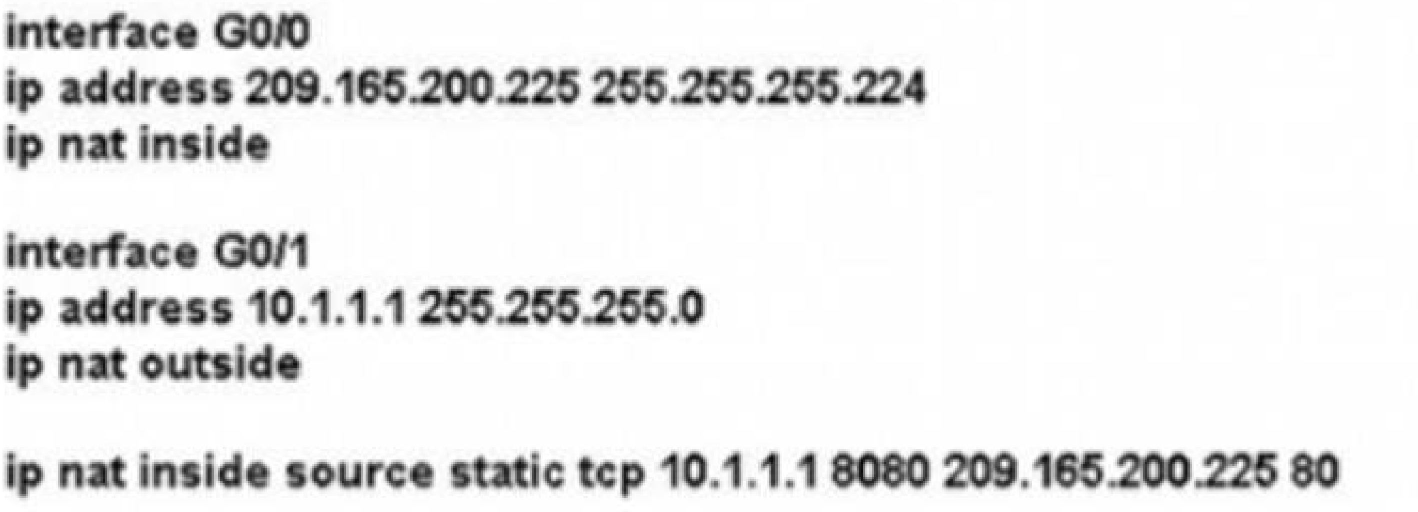
A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 347
- (Topic 1)

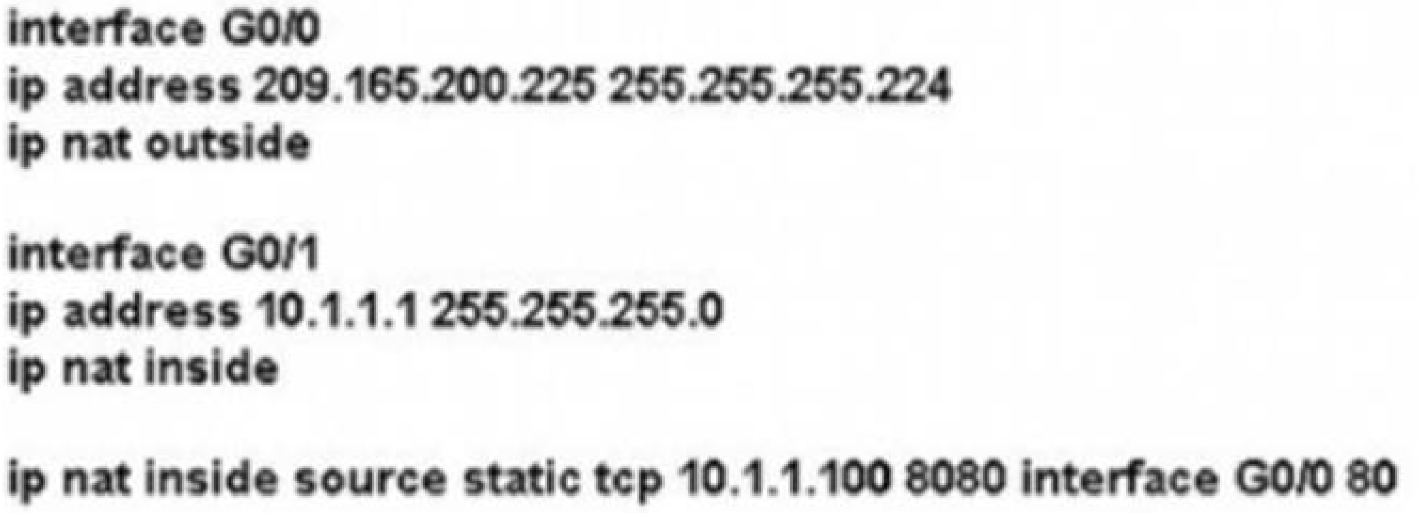


Refer to the exhibit. External users require HTTP connectivity to an internal company web server that is listening on TCP port 8080. Which command set accomplishes this requirement?
A)



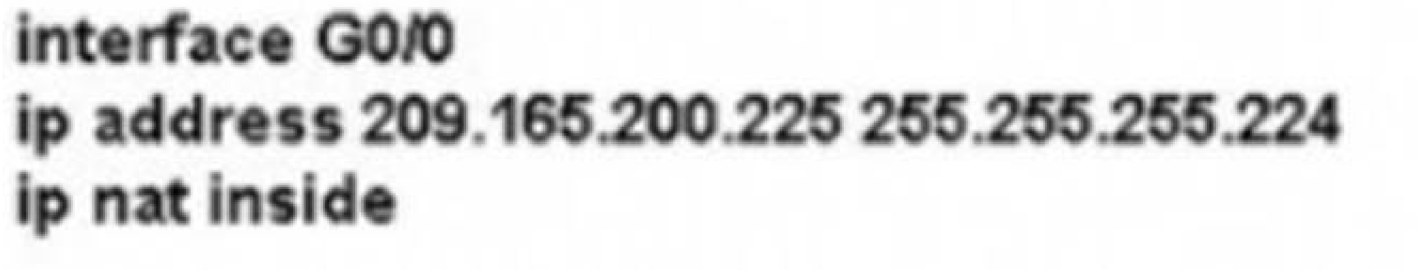
```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat outside

ip nat inside source static tcp 10.1.1.1 8080 209.165.200.225 80
```

B)



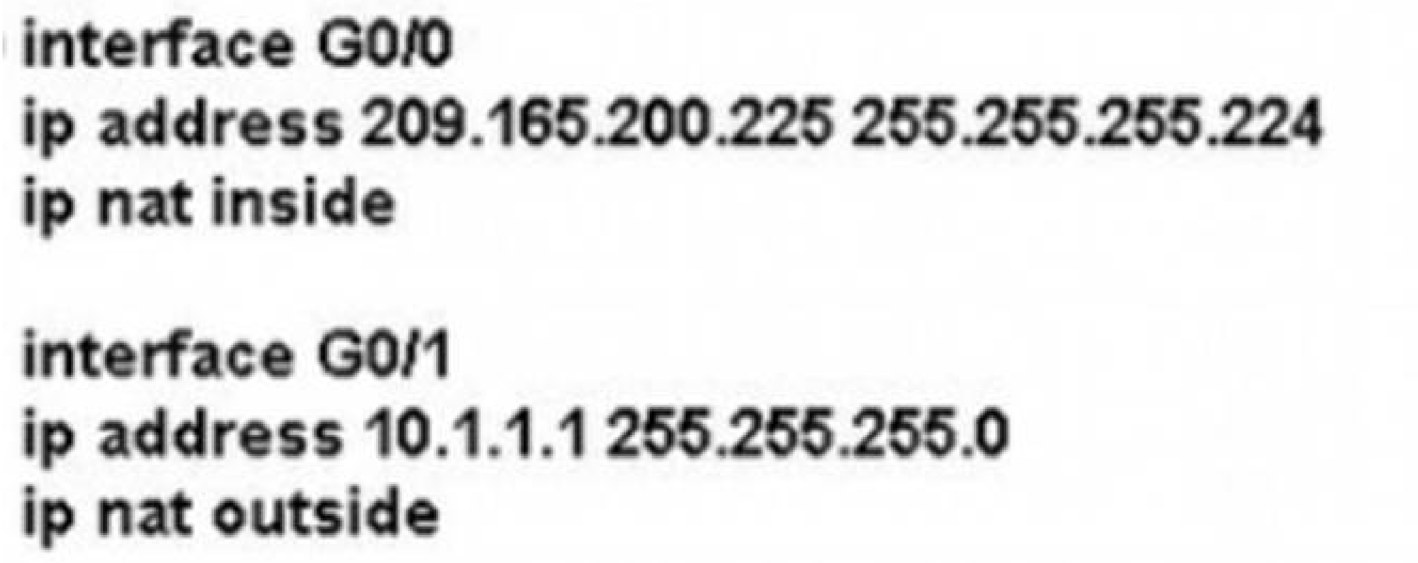
```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat outside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat inside

ip nat inside source static tcp 10.1.1.100 8080 interface G0/0 80
```

C)



```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside
```

D)

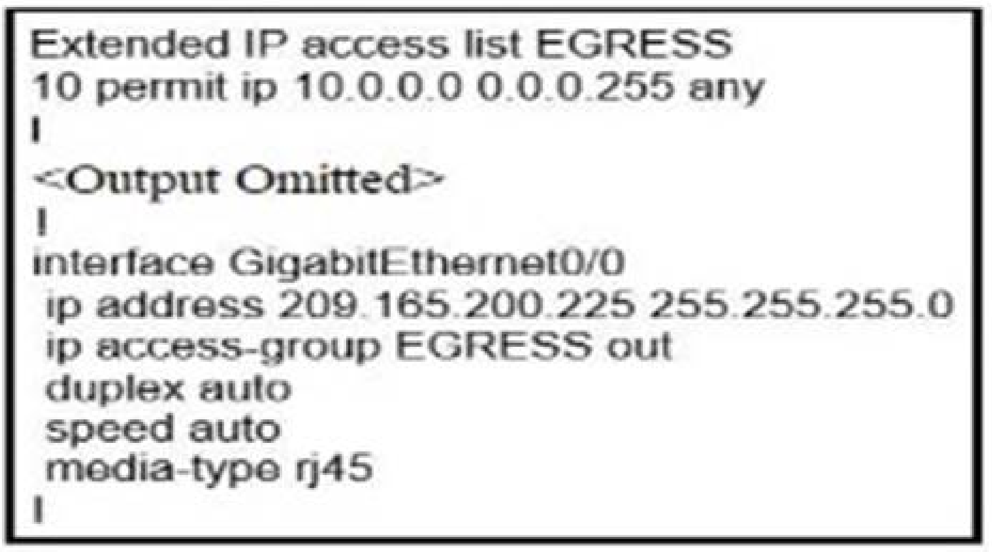


```
interface G0/0
ip address 209.165.200.225 255.255.255.224
ip nat inside

interface G0/1
ip address 10.1.1.1 255.255.255.0
ip nat outside
```

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

Answer: B

NEW QUESTION 351
- (Topic 1)
Refer to the exhibit.



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

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

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

Answer: A

NEW QUESTION 353
- (Topic 1)
Where is radio resource management performed in a cisco SD-access wireless solution?

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

Answer: C

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

NEW QUESTION 354
- (Topic 1)
How does an on-premises infrastructure compare to a cloud infrastructure?

A. On-premises can increase compute power faster than cloud
B. On-premises requires less power and cooling resources than cloud
C. On-premises offers faster deployment than cloud
D. On-premises offers lower latency for physically adjacent systems than cloud.

Answer: D

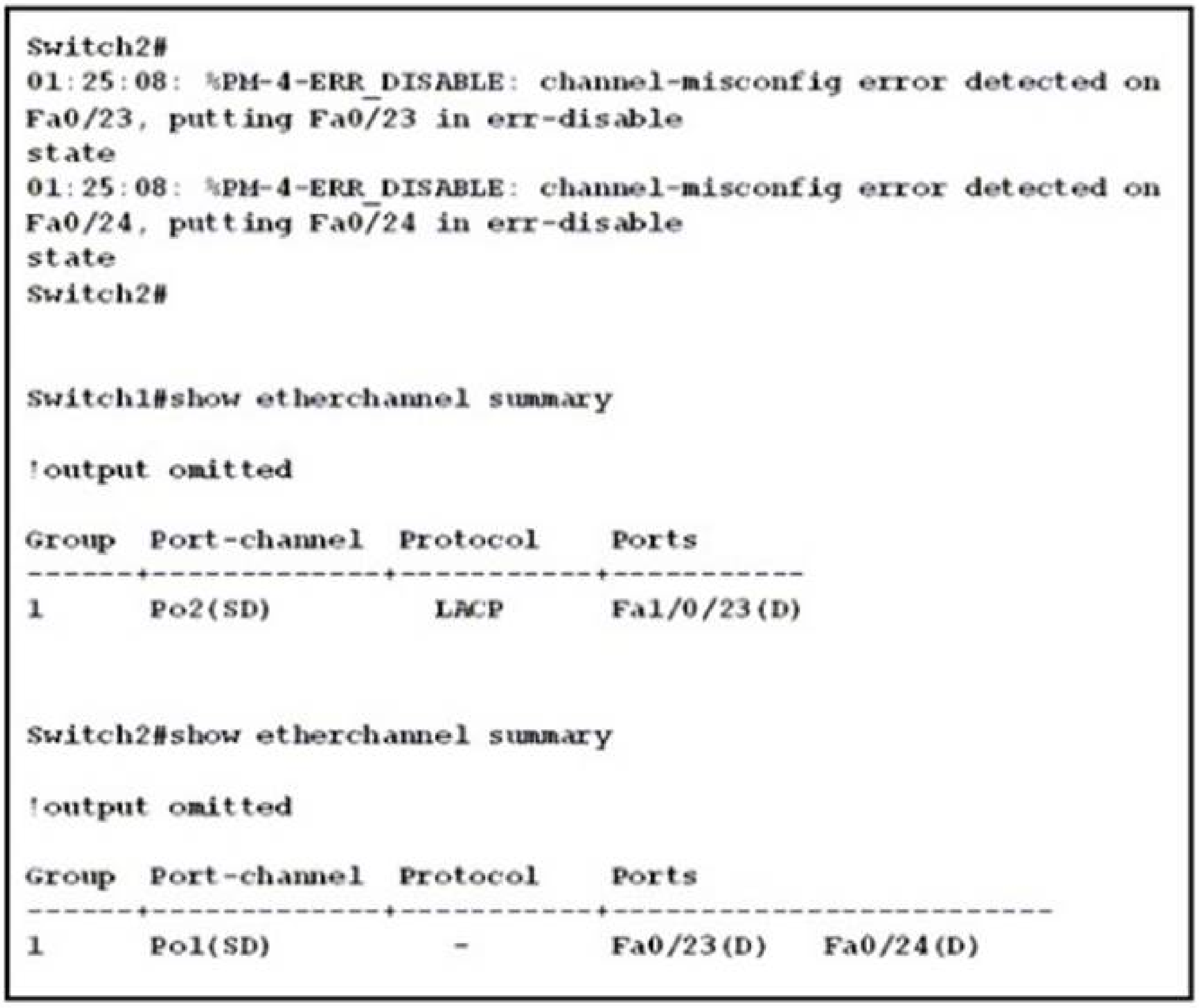
NEW QUESTION 357
- (Topic 1)
Which TCP setting is tuned to minimize the risk of fragmentation on a GRE/IP tunnel?

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 359
- (Topic 1)



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


Switch1#show etherchannel summary

!output omitted

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


Switch2#show etherchannel summary

!output omitted

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

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

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

Answer: C

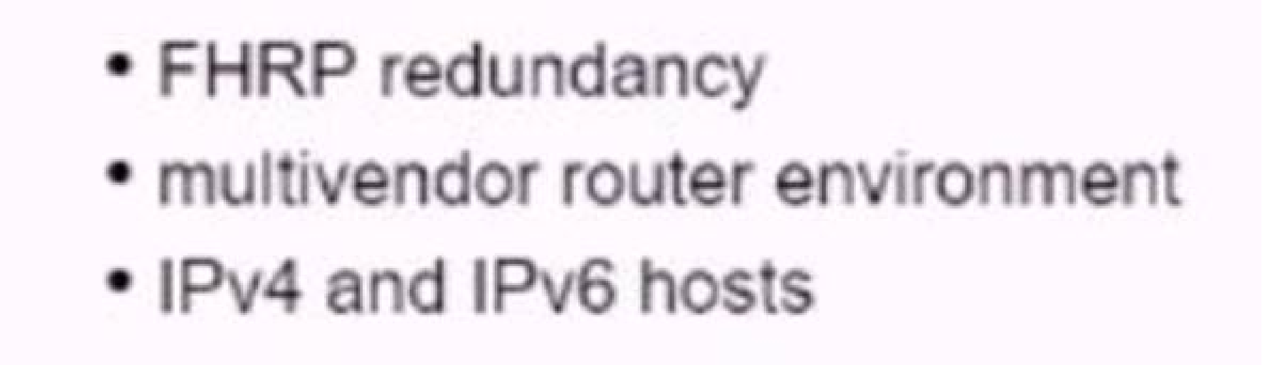
Explanation:
In this case, we are using your EtherChannel without a negotiation protocol on Switch2. As a result, if the opposite switch is not also configured for EtherChannel operation on the respective ports, there is a danger of a switching loop. The EtherChannel Misconfiguration Guard tries to prevent that loop from occuring by disabling all the ports bundled in the EtherChannel.

NEW QUESTION 361
- (Topic 1)
A customer has recently implemented a new wireless infrastructure using WLC-5520 at a site directly next to a large commercial airport. Users report that they intermittently lose WI- FI connectivity, and troubleshooting reveals it is due to frequent channel changes. Which two actions fix this issue? (Choose two)

A. Remove UNII-2 and Extended UNII-2 channels from the 5 Ghz channel list
B. Restore the DCA default settings because this automatically avoids channel interference.
C. Configure channels on the UNIk2 and the Extended UNII-2 sub-bands of the 5 Ghzband only
D. Enable DFS channels because they are immune to radar interference.
E. Disable DFS channels to prevent interference with Doppler radar

Answer: AE

NEW QUESTION 365
- (Topic 1)
A customer requests a network design that supports these requirements:



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

Which protocol does the design include?

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

Answer: D

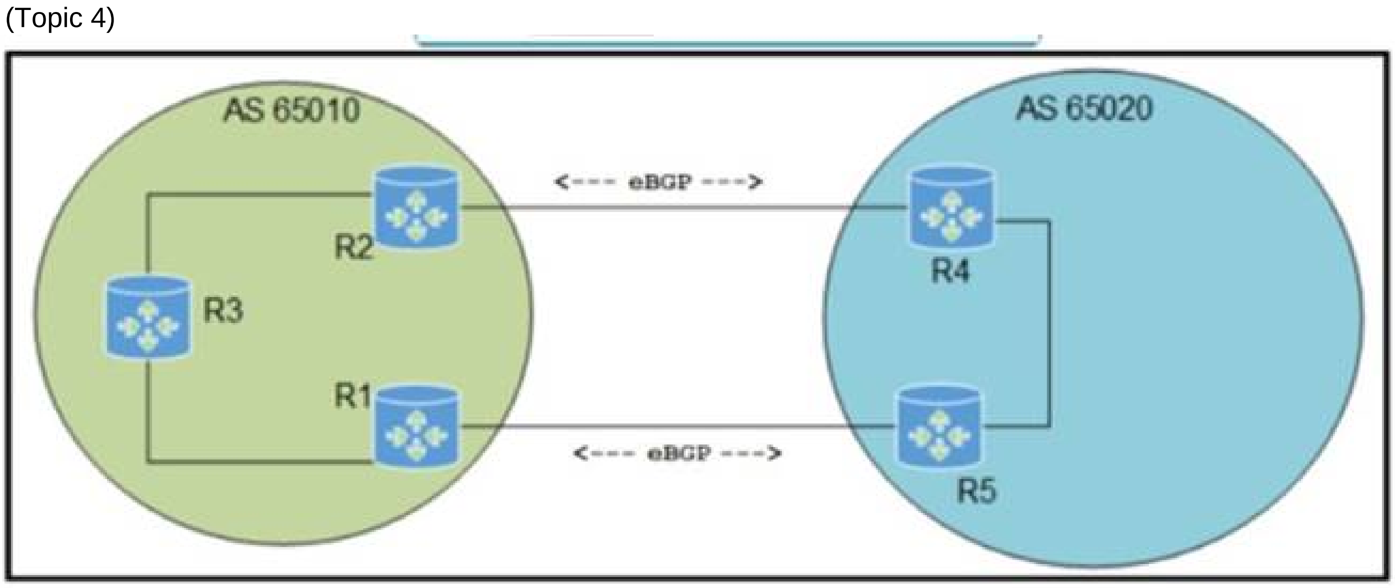
NEW QUESTION 368
- (Topic 1)
What is one benefit of implementing a VSS architecture?

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

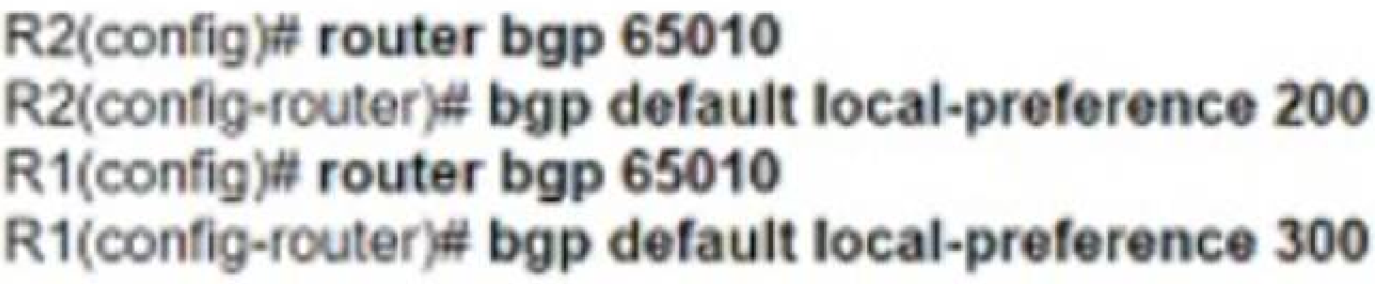
Answer: C

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

NEW QUESTION 369
- (Topic 4)

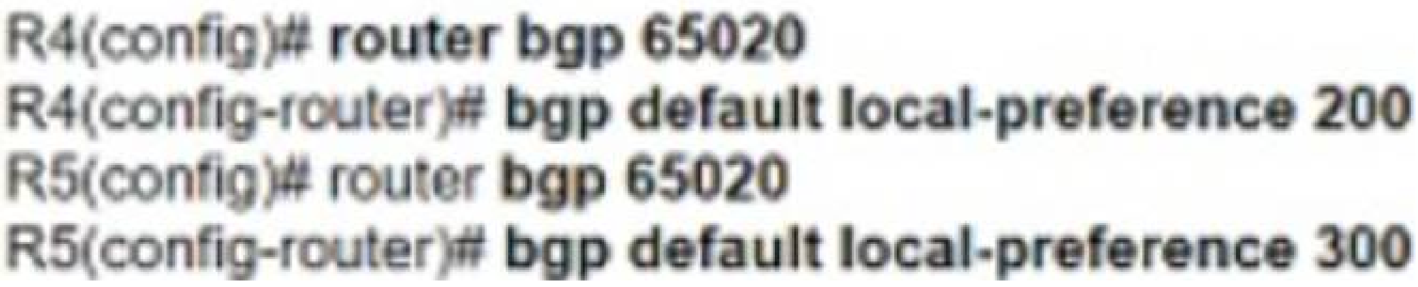


Refer to the exhibit. Which configuration must be applied to ensure that the preferred path for traffic from AS 65010 toward AS 65020 uses the R2 to R4 path?
A)



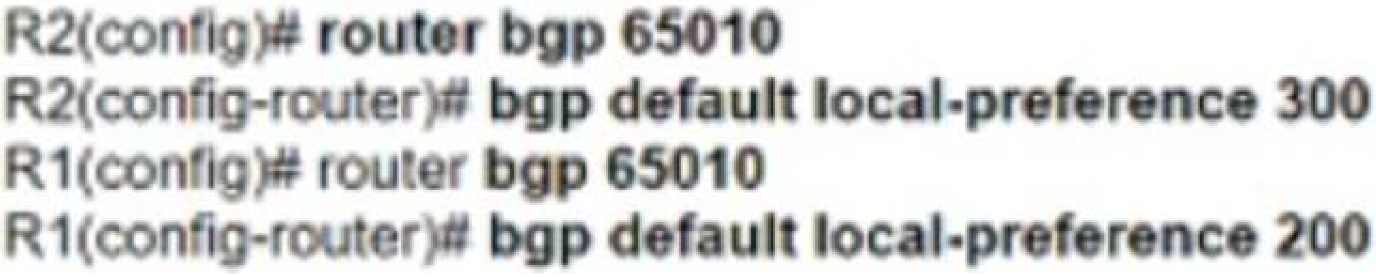
```
R2(config)# router bgp 65010
R2(config-router)# bgp default local-preference 200
R1(config)# router bgp 65010
R1(config-router)# bgp default local-preference 300
```

B)



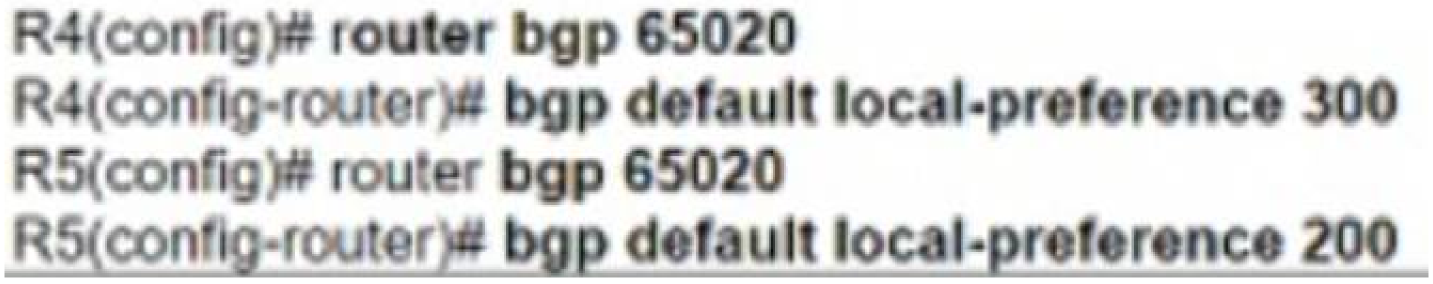
```
R4(config)# router bgp 65020
R4(config-router)# bgp default local-preference 200
R5(config)# router bgp 65020
R5(config-router)# bgp default local-preference 300
```

C)



```
R2(config)# router bgp 65010
R2(config-router)# bgp default local-preference 300
R1(config)# router bgp 65010
R1(config-router)# bgp default local-preference 200
```

D)



```
R4(config)# router bgp 65020
R4(config-router)# bgp default local-preference 300
R5(config)# router bgp 65020
R5(config-router)# bgp default local-preference 200
```

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

Answer: C

NEW QUESTION 372
- (Topic 4)
Which configuration protects the password for the VTY lines against over-the-shoulder attacks?

A. username admin secret 7 6j809j23kpp43883500N7%e$
B. service password-encryption
C. line vty 04 password $25$FpM7182!
D. line vty 0 15password $25$FpM71f82!

Answer: B

NEW QUESTION 377
- (Topic 4)
What is a client who is running 802.1x for authentication reffered to as?

A. supplicant
B. NAC device
C. authenticator
D. policy enforcement point

Answer: A

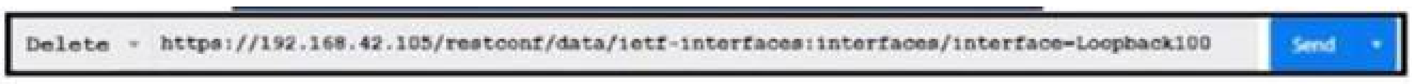
NEW QUESTION 381
- (Topic 4)
Which of the following security methods uses physical characteristics of a person to authorize access to a location?

A. Access control vestibule
B. Palm scanner
C. PIN pad
D. Digital card reader
E. Photo ID

Answer: B

Explanation:
This is because a palm scanner is a type of biometric security method that uses the physical characteristics of a person’s palm, such as the shape, size, and vein patterns, to authorize access to a location. A palm scanner is more reliable and secure than other methods, such as a PIN pad or a digital card reader, which can be easily stolen, lost, or shared. A palm scanner is also more hygienic and convenient than other biometric methods, such as a fingerprint scanner or a facial recognition system, which can be affected by dirt, oil, or lighting conditions. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.2: Implementing Device Access Control.

NEW QUESTION 384
- (Topic 4)
Refer to the exhibit.



Delete https://192.168.42.105/restconf/data/ietf-interfaces:interfaces/interface=Loopback100

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 389
- (Topic 4)
Which two features are available only in next-generation firewalls? (Choose two.)

A. virtual private network
B. deep packet inspection
C. stateful inspection
D. application awareness
E. packet filtering

Answer: CD

NEW QUESTION 393
- (Topic 4)
Which there application has the ability to make REST calls against Cisco DNA Center?

A. API Explorer
B. REST Explorer
C. Postman
D. Mozilla

Answer: C

NEW QUESTION 397
- (Topic 4)
In which way are EIGRP and OSPF similar?

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

Answer: C

NEW QUESTION 398
- (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 faitover

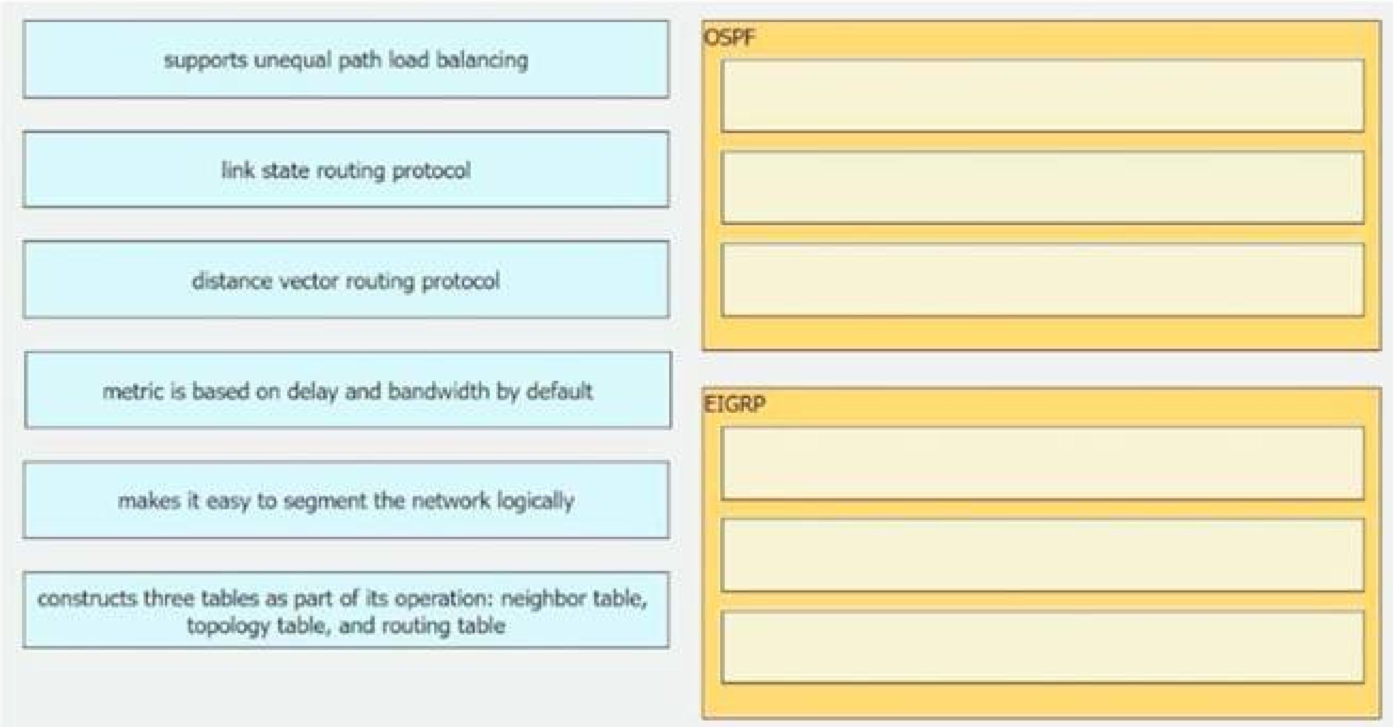
Answer: D

NEW QUESTION 399
- (Topic 4)
What is one being of implementing a data modetag language?

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

Answer: A

NEW QUESTION 403
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the routing protocol they describe on the right



supports unequal path load balancing

link state routing protocol

distance vector routing protocol

metric is based on delay and bandwidth by default

makes it easy to segment the network logically

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

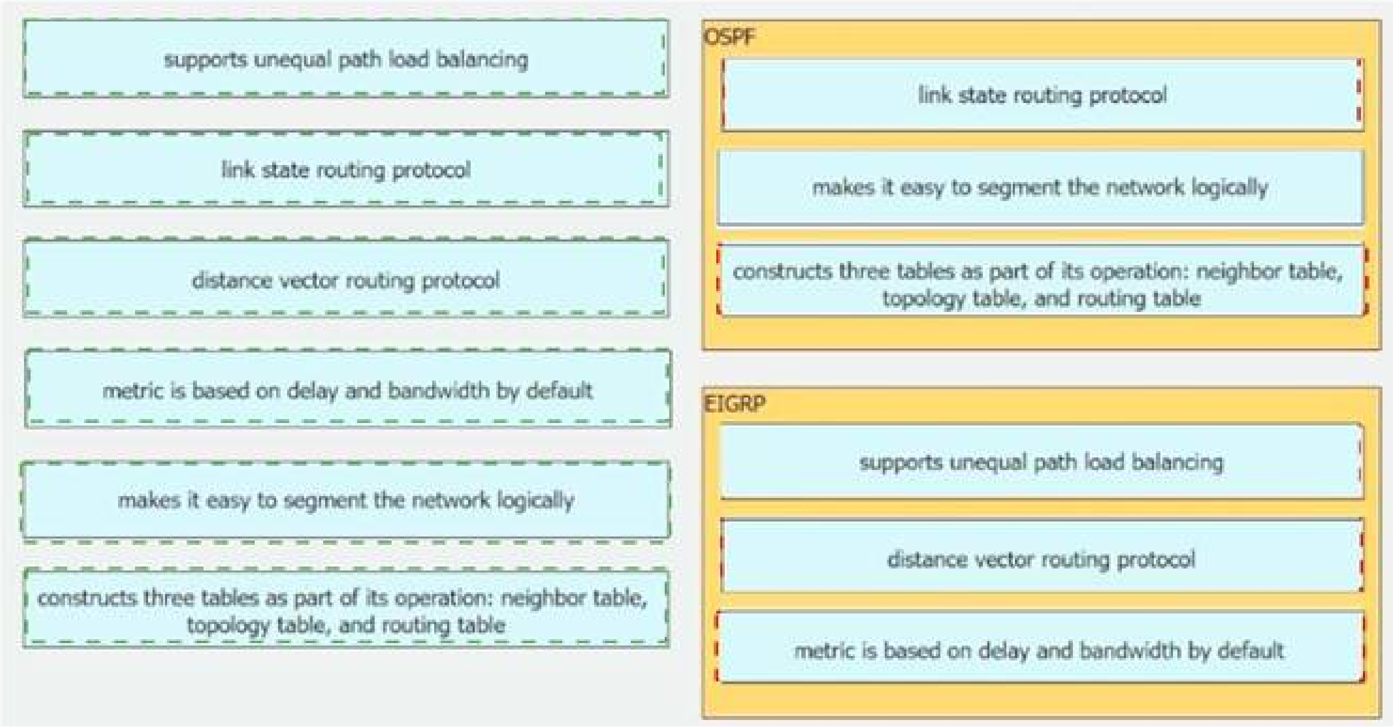
OSPF

EIGRP

A. Mastered
B. Not Mastered

Answer: A

Explanation:



supports unequal path load balancing

link state routing protocol

distance vector routing protocol

metric is based on delay and bandwidth by default

makes it easy to segment the network logically

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

OSPF

link state routing protocol

makes it easy to segment the network logically

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

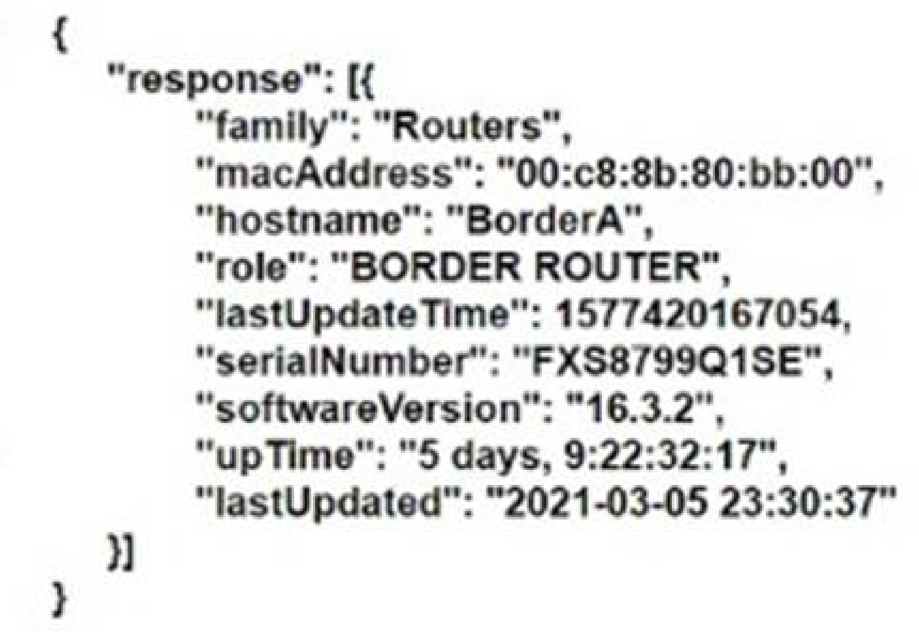
EIGRP

supports unequal path load balancing

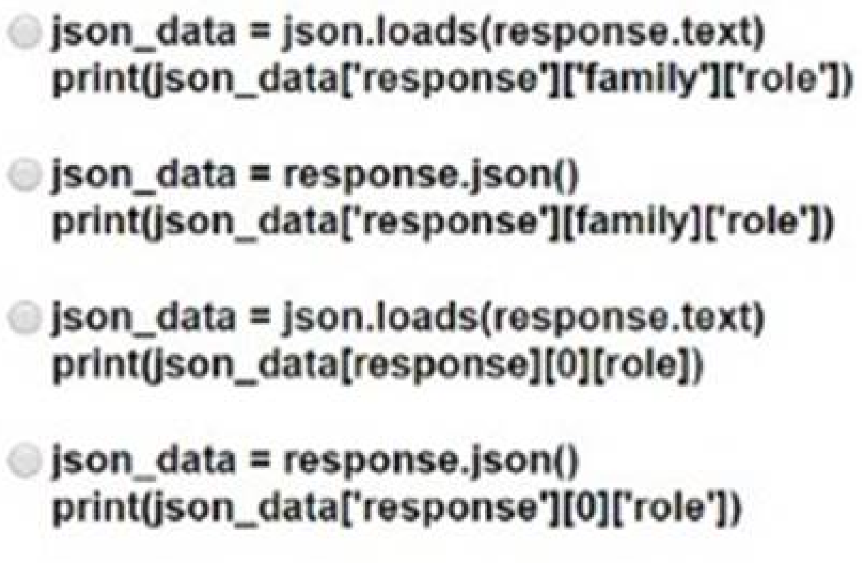
distance vector routing protocol

metric is based on delay and bandwidth by default

NEW QUESTION 407
- (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

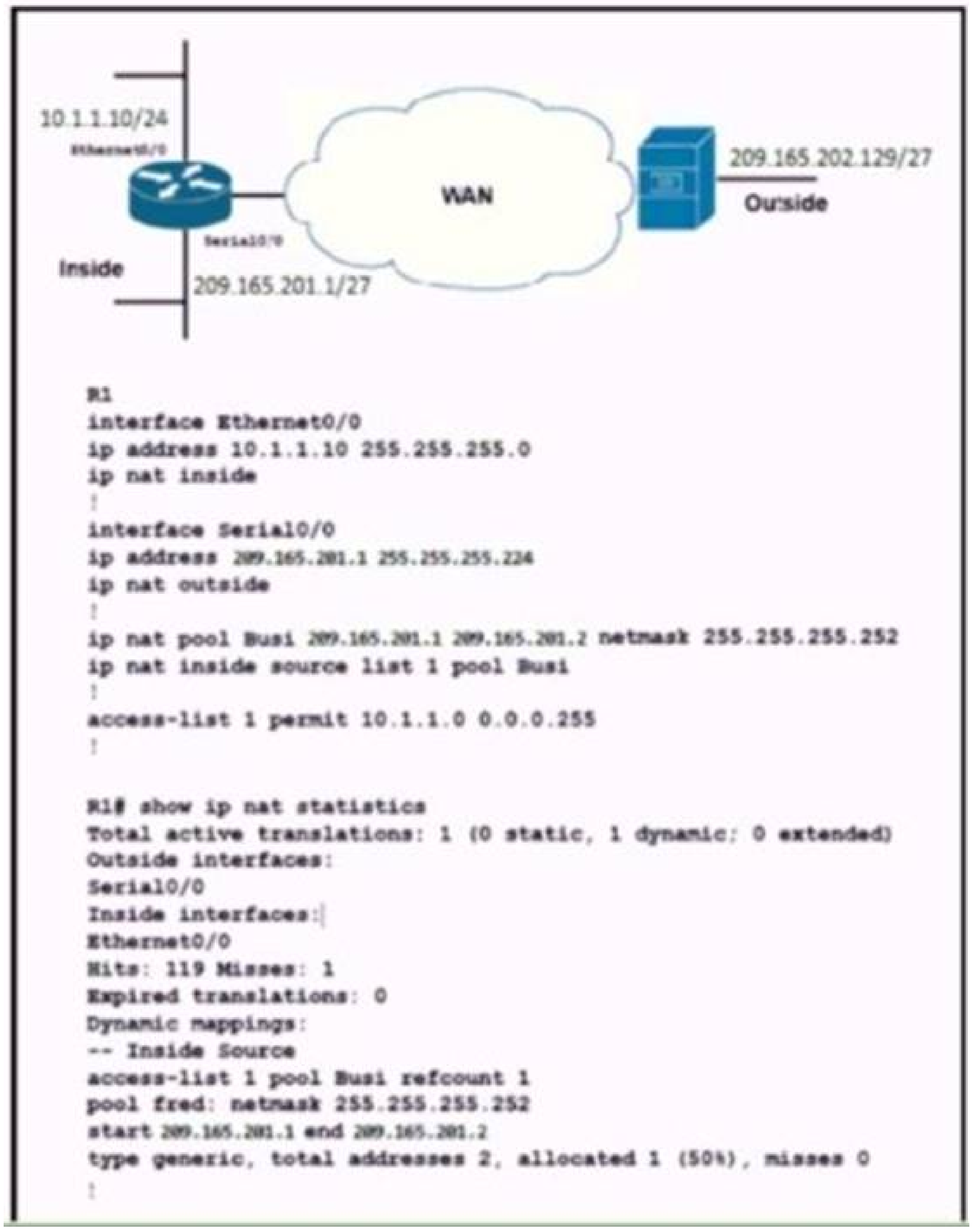
NEW QUESTION 410
- (Topic 4)
What mechanism does PIM use to forward multicast traffic?

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

Answer: A

Explanation:
PIM sparse mode uses a pull model to deliver multicast traffic. This means that multicast traffic is only forwarded to routers that have explicitly requested it, using join messages. This reduces the amount of unnecessary traffic on the network and allows for efficient use of bandwidth. The source of this answer is the Cisco ENCOR v1.1 course, module 5, lesson 5.2: Implementing PIM Sparse Mode.

NEW QUESTION 413
- (Topic 4)



```
R1
interface Ethernet0/0
ip address 10.1.1.10 255.255.255.0
ip nat inside
!
interface Serial0/0
ip address 209.165.201.1 255.255.255.224
ip nat outside
!
ip nat pool Busi 209.165.201.1 209.165.201.2 netmask 255.255.255.252
ip nat inside source list 1 pool Busi
!
access-list 1 permit 10.1.1.0 0.0.0.255
!

R1# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 0 extended)
Outside interfaces:
Serial0/0
Inside interfaces:
Ethernet0/0
Hits: 119 Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool Busi refcount 1
pool fred: netmask 255.255.255.252
start 209.165.201.1 end 209.165.201.2
type generic, total addresses 2, allocated 1 (50%), misses 0
!
```

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

A. The first pocket 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 a configured win PAT overload parameters

Answer: A

NEW QUESTION 417
- (Topic 4)
When a branch location loses connectivity, which Cisco FlexConnect state rejects new users but allows existing users to function normally?

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

Answer: A

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

NEW QUESTION 420
- (Topic 4)
What is a characteristics of traffic shaping?

A. can be applied in both traffic direction
B. queues out-of-profile packets until the buffer is full
C. drops out-of-profile packets
D. causes TCP retransmits when packet are dropped

Answer: B

NEW QUESTION 421
- (Topic 4)
When a DNS host record is configured for a new Cisco AireOS WLC, which hostname must be added to allow APs to successfully discover the WLC?

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

Answer: D

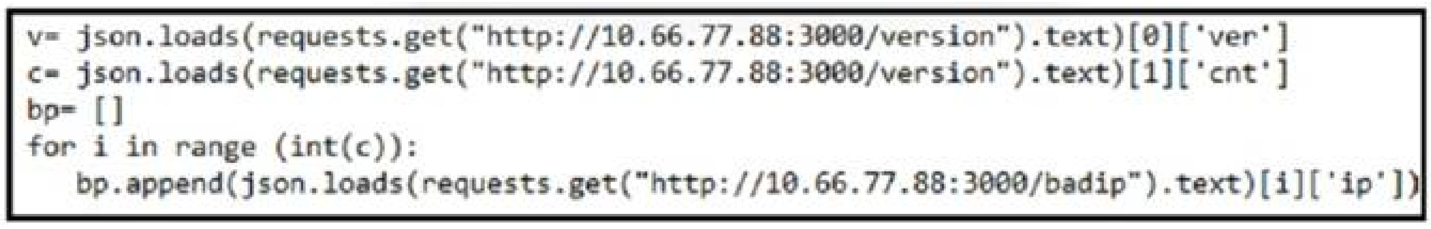
NEW QUESTION 423
- (Topic 4)
What is the recommended minimum SNR for Voice applications for networks?

A. 15
B. 20
C. 25
D. 10

Answer: C

Explanation:
https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength#:~:text=Generally%2C%20a%20signal%20with%20an,networks%20that%20use%20voice%20applications.

NEW QUESTION 425
- (Topic 4)
Refer to the exhibit.



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

What is achieved by this Python script?

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

Answer: B

NEW QUESTION 428
- (Topic 4)
Which authorization framework gives third-party applications limited access to HTTP services?

A. iPsec
B. Basic Auth
C. GRE
D. OAuth 2.0

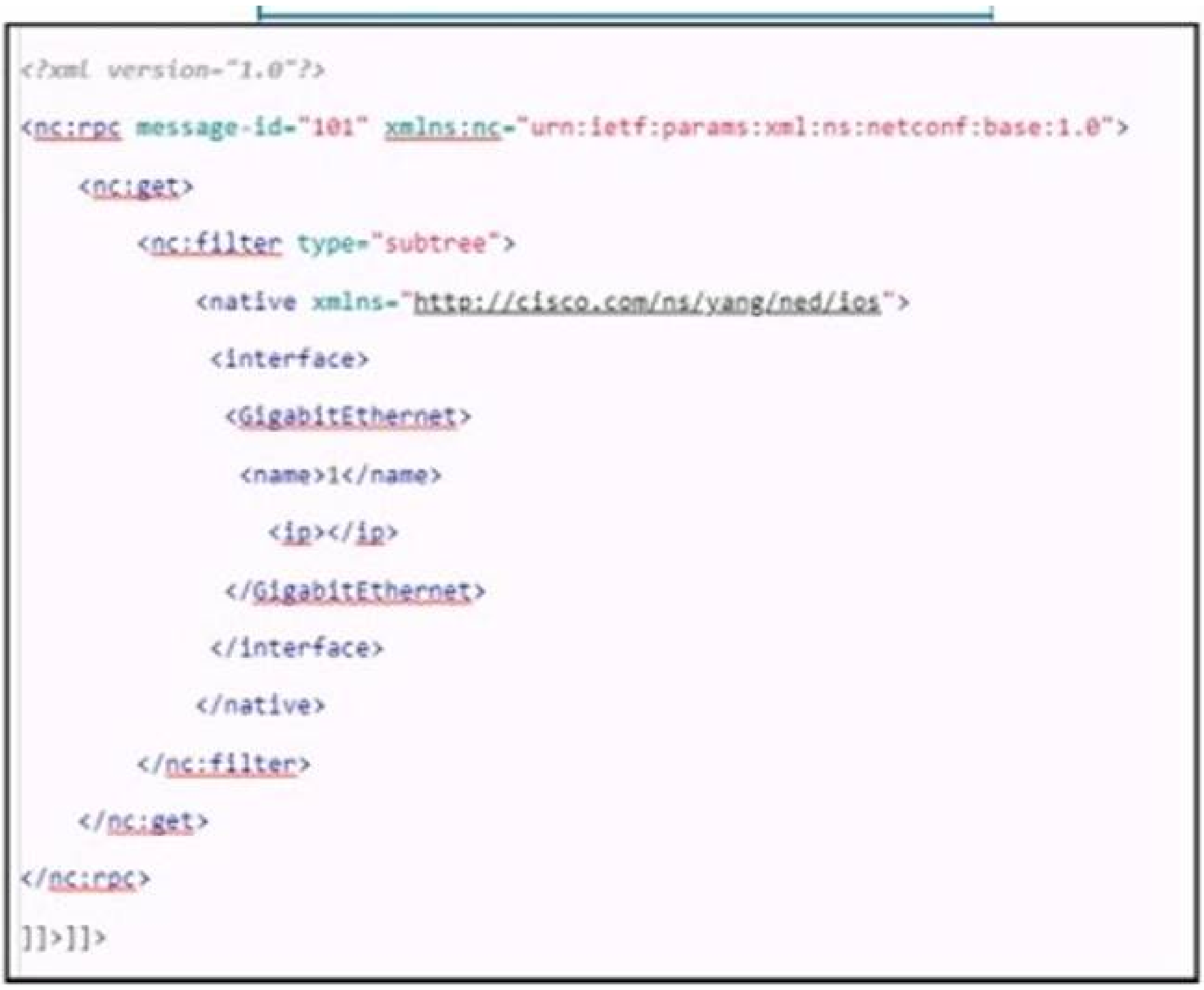
Answer: D

NEW QUESTION 431
- (Topic 4)
An engineer receives a report that an application exhibits poor performance. On the switch where the server is connected, this syslog message is visible: SW_MATM4-MACFLAP_N0HF: Host 0054.3831.8253 in vlan 14 is flapping between port GUAM and port Gi1/0/2.
What is causing the problem?

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

Answer: B

NEW QUESTION 436
- (Topic 4)



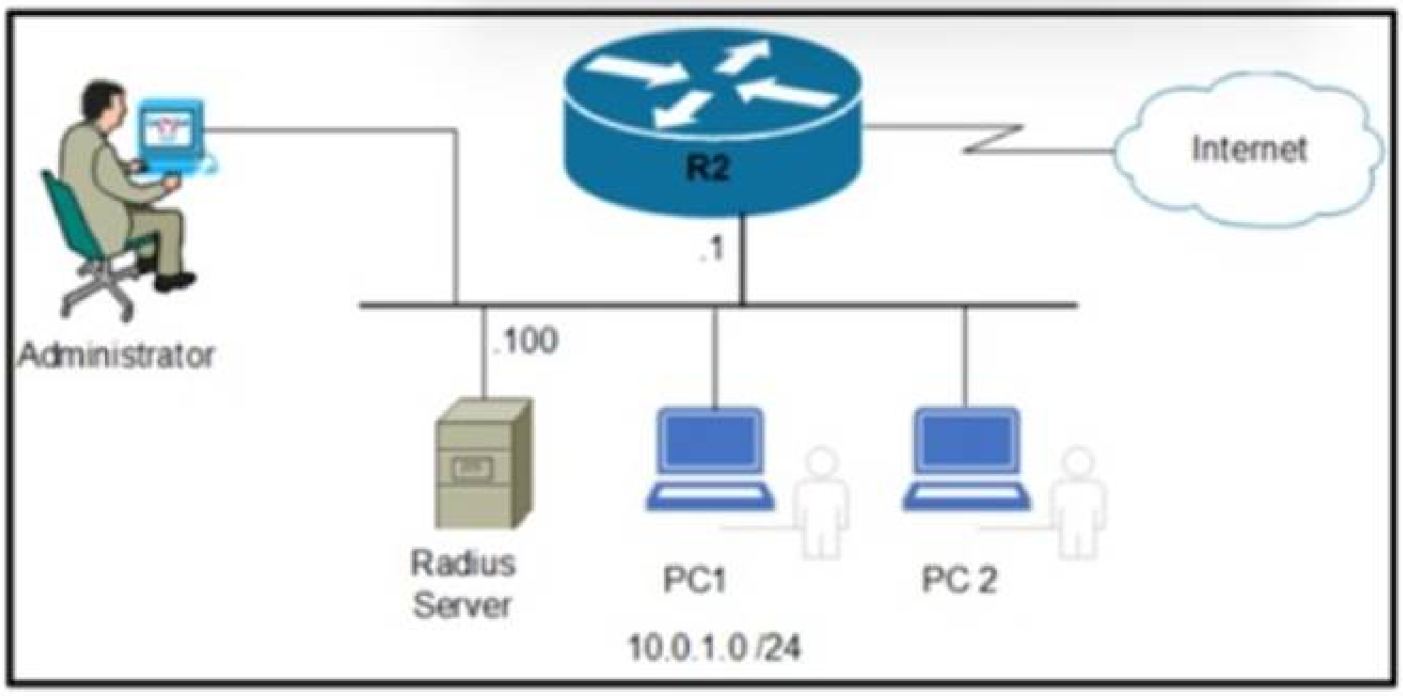
```
<?xml version="1.0"?>
<nc:rpc message-id="101" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
    <nc:get>
        <nc:filter type="subtree">
            <native xmlns="http://cisco.com/ns/yang/ned/ios">
             <interface>
              <GigabitEthernet>
               <name>1</name>
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

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

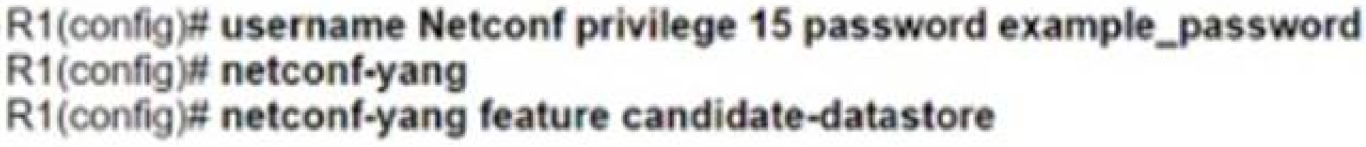
A. view the configuration of all GigabitEthernet interfaces.
B. Discover the IP address of interface GigabitEthernet.
C. Set the description of interface GigabitEthernet1 to *1*.
D. Remove the IP address from interface GigabitEthernet1.

Answer: A

NEW QUESTION 438
- (Topic 4)

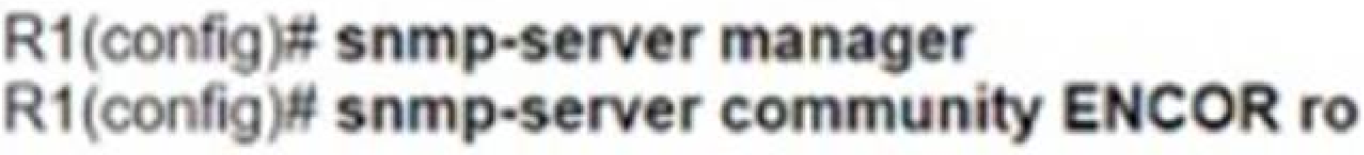


Refer to the exhibit. Which command set enables router R2 to be configured via NETCONF?
A)



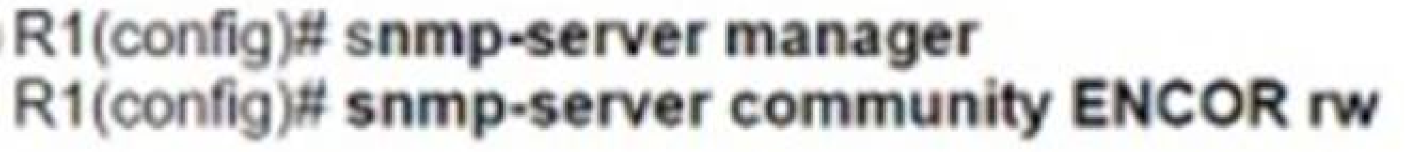
```
R1(config)# username Netconf privilege 15 password example_password
R1(config)# netconf-yang
R1(config)# netconf-yang feature candidate-datastore
```

B)



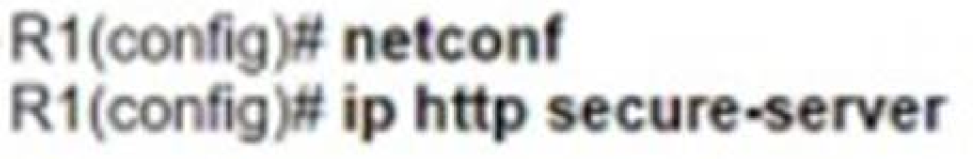
```
R1(config)# snmp-server manager
R1(config)# snmp-server community ENCOR ro
```

C)



```
R1(config)# snmp-server manager
R1(config)# snmp-server community ENCOR rw
```

D)



```
R1(config)# netconf
R1(config)# ip http secure-server
```

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

Answer: A

NEW QUESTION 441
- (Topic 4)
Which two functions is an edge node responsible for? (Choose two.)

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

Answer: AD

NEW QUESTION 445
- (Topic 4)
A script contains the statement "while loop != 999:" Which value terminates the loop?

A. A value equal to 999.
B. A value less than or equal to 999.
C. A value not equal to 999.
D. A value greater than or equal to 999.

Answer: A

NEW QUESTION 450
- (Topic 4)
A customer deploys a new wireless network to perform location-based services using Cisco DNA Spaces The customer has a single WLC located on-premises in a secure data center. The security team does not want to expose the WLC to the public Internet. Which solution allows the customer to securely send RSSI updates to Cisco DNA Spaces?

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

Answer: D

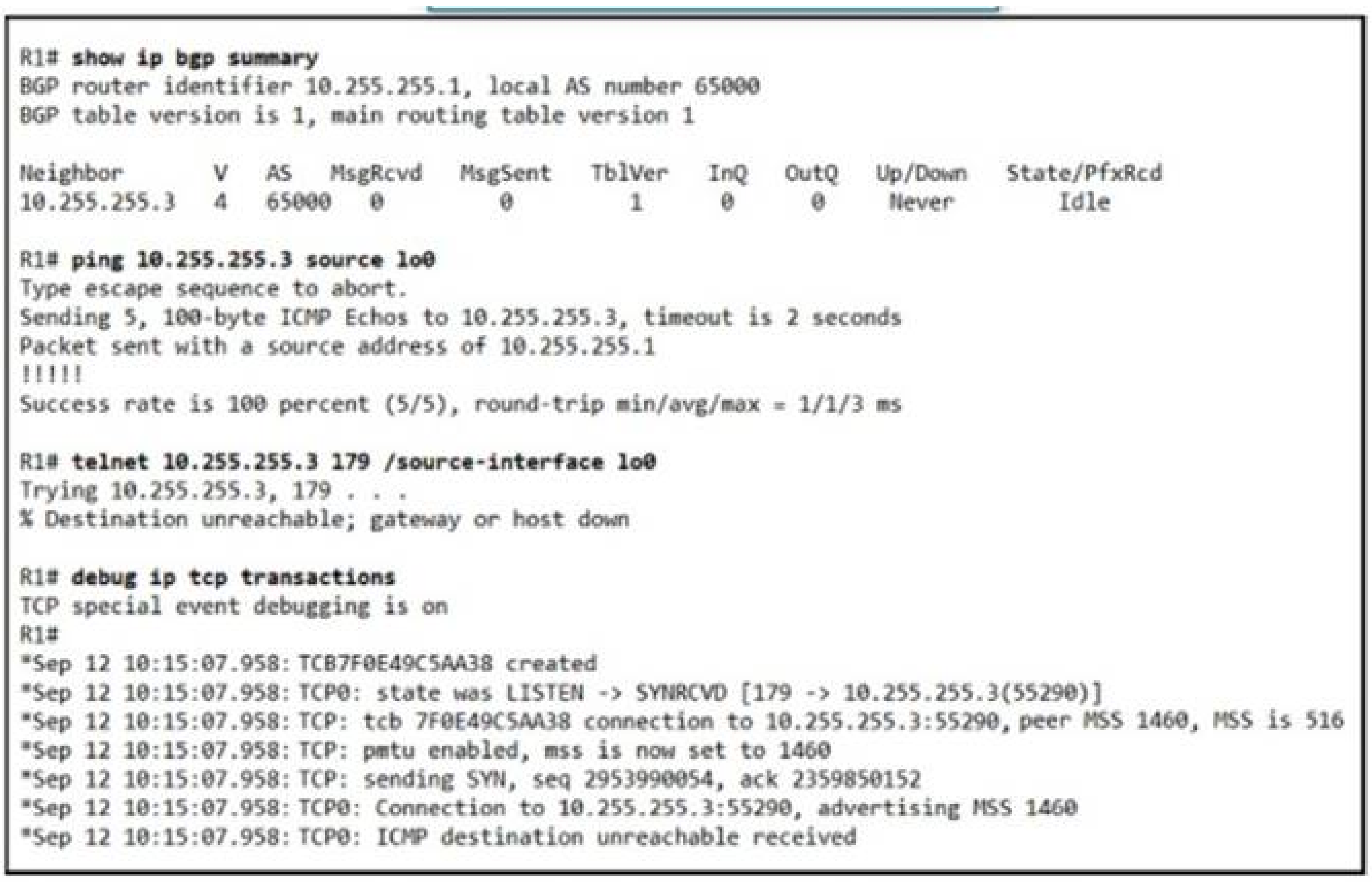
NEW QUESTION 451
- (Topic 4)
Witch two actions provide controlled Layer 2 network connectivity between virtual machines running on the same hypervisor? (Choose two.)

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

Answer: BC

Explanation:
Source 1: https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-1000v-switch-vmware-vsphere/at_a_glance_c45-532467.pdf
Source 2: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/vm_fex/vmware/gui/confi g_guide/2-1/b_GUI_VMware_VM-FEX_UCSM_Configuration_Guide_2_1/b_GUI_VMware_VM- FEX_UCSM_Configuration_Guide_2_1_chapter_0110.pdf

NEW QUESTION 455
- (Topic 4)



```
R1# show ip bgp summary
BGP router identifier 10.255.255.1, local AS number 65000
BGP table version is 1, main routing table version 1

Neighbor        V   AS    MsgRcvd   MsgSent   TblVer   InQ   OutQ   Up/Down   State/PfxRcd
10.255.255.3    4   65000   0          0         1       0     0     Never        Idle

R1# ping 10.255.255.3 source lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.255.255.3, timeout is 2 seconds
Packet sent with a source address of 10.255.255.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

R1# telnet 10.255.255.3 179 /source-interface lo0
Trying 10.255.255.3, 179 . . .
% Destination unreachable; gateway or host down

R1# debug ip tcp transactions
TCP special event debugging is on
R1#
*Sep 12 10:15:07.958: TCB7F0E49C5AA38 created
*Sep 12 10:15:07.958: TCP0: state was LISTEN -> SYNRCVD [179 -> 10.255.255.3(55290)]
*Sep 12 10:15:07.958: TCP: tcb 7F0E49C5AA38 connection to 10.255.255.3:55290, peer MSS 1460, MSS is 516
*Sep 12 10:15:07.958: TCP: pmtu enabled, mss is now set to 1460
*Sep 12 10:15:07.958: TCP: sending SYN, seq 2953990054, ack 2359850152
*Sep 12 10:15:07.958: TCP0: Connection to 10.255.255.3:55290, advertising MSS 1460
*Sep 12 10:15:07.958: TCP0: ICMP destination unreachable received
```

Refer to the exhibit An engineer is troubleshooting a newly configured BGP peering that does not establish What is the reason for the failure?

A. BGP peer 10 255 255 3 is not configured for peenng wth R1
B. Mandatory BOP parameters between R1 and 10 255 255 3 are mismatched
C. A firewall is blocking access to TCP port 179 on the BGP peer 10 255 255.3
D. Both BGP pern are configured for passive TCP transport

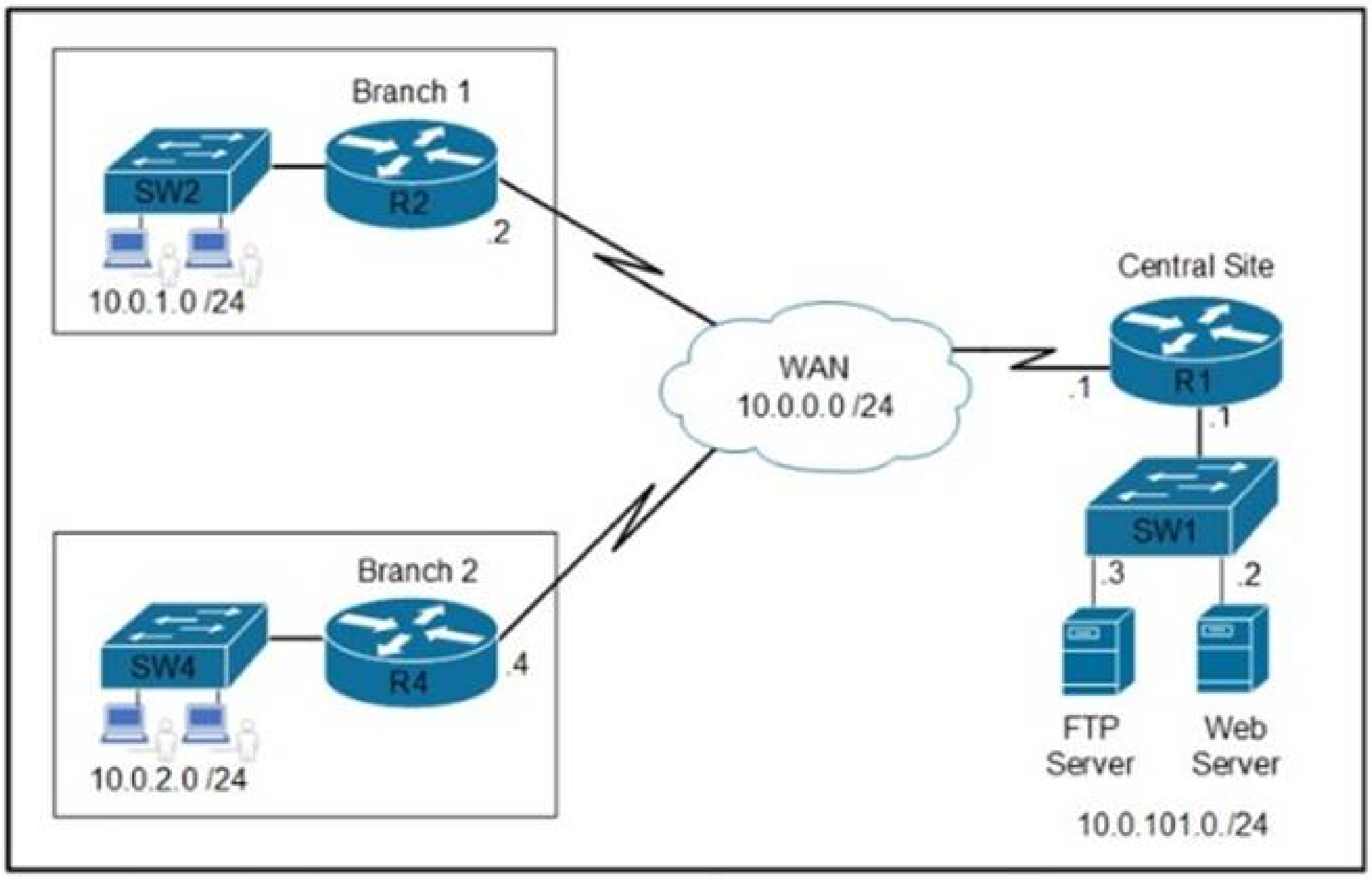
Answer: A

NEW QUESTION 460
- (Topic 4)
Which solution simplifies management ot secure access to network resources?

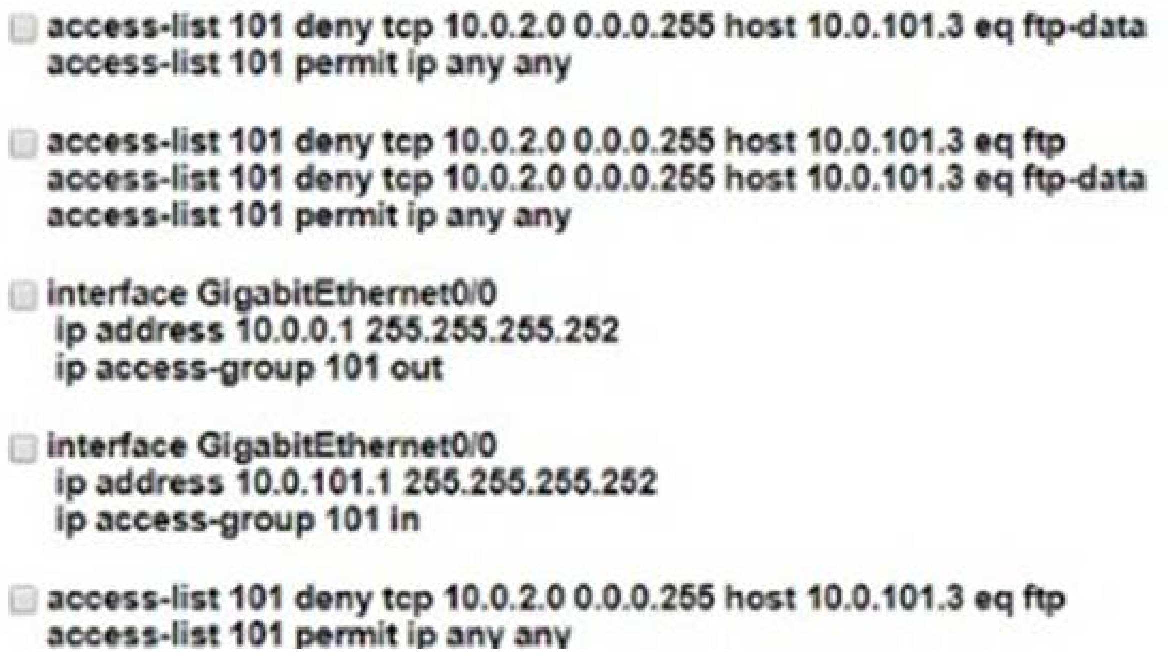
A. RFC 3580-based solution to enable authenticated access leveraging RADIUS and AV pairs
B. TrustSec to logically group internal user environments and assign policies
C. 802.1AE to secure communication in the network domain
D. ISE to automate network access control leveraging RADIUS AV pairs

Answer: B

NEW QUESTION 462
- (Topic 4)



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

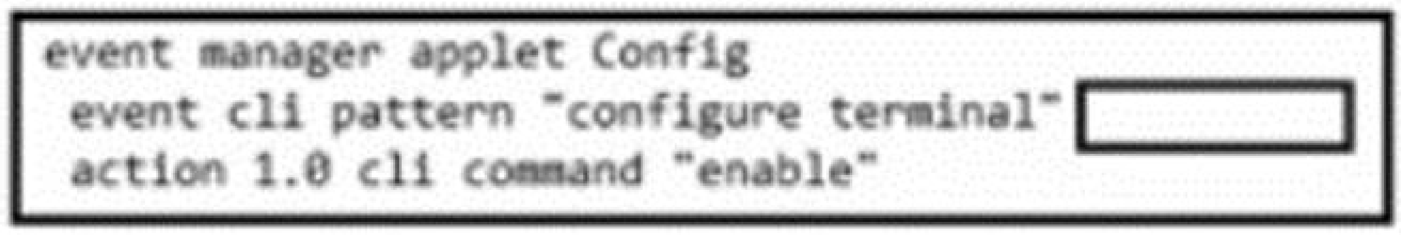


```
□ access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data
  access-list 101 permit ip any any

□ access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp
  access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data
  access-list 101 permit ip any any

□ interface GigabitEthernet0/0
   ip address 10.0.0.1 255.255.255.252
   ip access-group 101 out

□ interface GigabitEthernet0/0
   ip address 10.0.101.1 255.255.255.252
   ip access-group 101 in

□ access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp
  access-list 101 permit ip any any
```

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

Answer: BC

NEW QUESTION 465
- (Topic 4)



```
event manager applet Config
 event cli pattern "configure terminal" [          ]
 action 1.0 cli command "enable"
```

Refer to the exhibit. An engineer constructs an EEM applet to prevent anyone from entering configuration mode on a switch. Which snippet is required to complete the EEM applet?

A. sync yes skip yes
B. sync no skip yes
C. sync no skip no
D. sync yes skip no

Answer: B

NEW QUESTION 468
- (Topic 4)
A company hires a network architect to design a new OTT wireless solution within a Cisco SD-Access Fabric wired network. The architect wants to register access points to the WLC to centrally switch the traffic. Which AP mode must the design include?

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

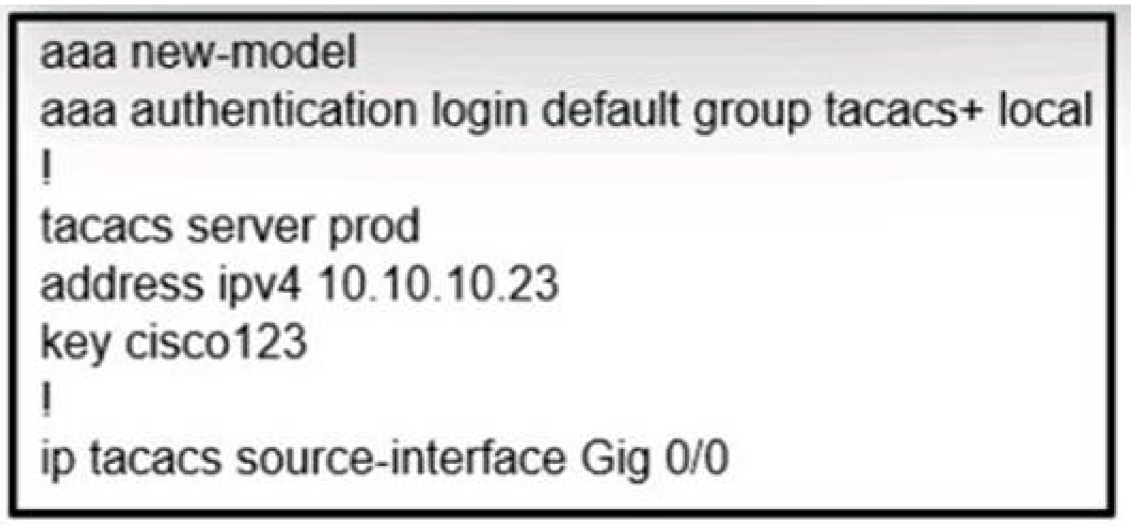
Answer: D

NEW QUESTION 473
- (Topic 4)
What is one method for achieving REST API security?

A. using built-in protocols known as Web Services Security
B. using a combination of XML encryption and XML signatures
C. using a MD5 hash to verify the integrity
D. using HTTPS and TLS encryption

Answer: D

NEW QUESTION 474
- (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
```

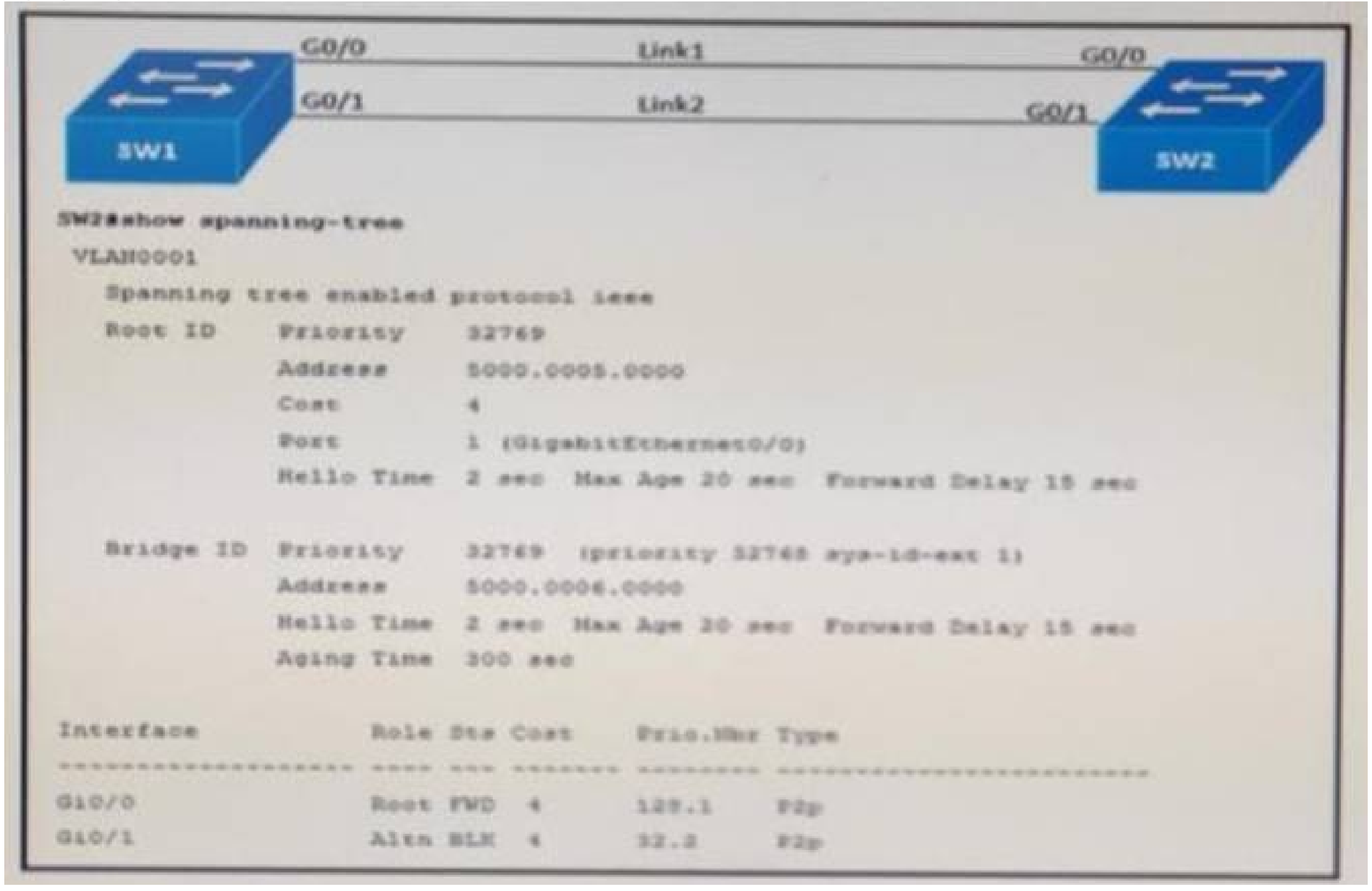
Which configuration must be applied for the TACACS+ server to grant access-level rights to remote users?

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 478
- (Topic 4)



```
SW2#show spanning-tree
 VLAN0001
   Spanning tree enabled protocol ieee
   Root ID     Priority    32769
               Address     5000.0005.0000
               Cost        4
               Port        1 (GigabitEthernet0/0)
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

   Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
               Address     5000.0006.0000
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
               Aging Time  300 sec

Interface          Role Sts Cost     Prio.Nbr Type
------------------ ---- --- -------- -------- ------------------------
Gi0/0              Root FWD  4       128.1    P2p
Gi0/1              Altn BLK  4       32.2     P2p
```

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

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

Answer: D

NEW QUESTION 483
- (Topic 4)
An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?

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

Answer: B

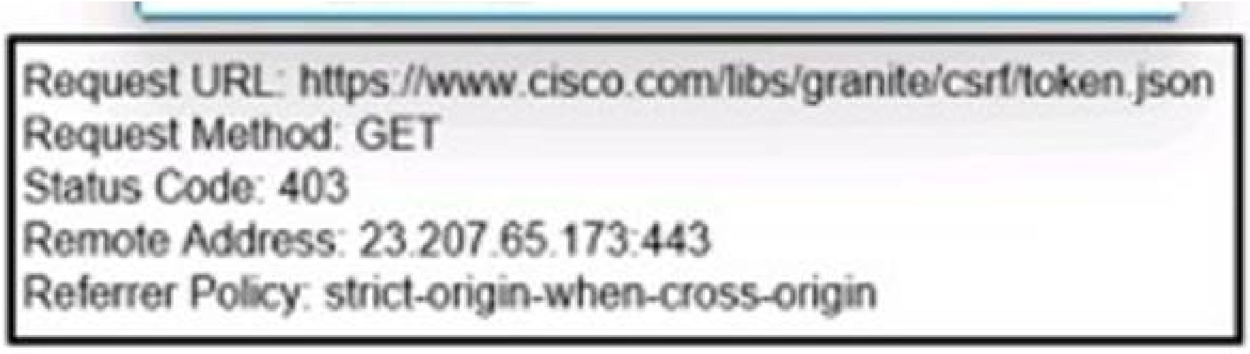
Explanation:
This is because the Design workflow in Cisco DNA Center allows the engineer to create a new network infrastructure by defining the physical network device hierarchy based on the location of the devices. The location hierarchy consists of four levels: global, area, building, and floor. The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

NEW QUESTION 484
- (Topic 4)
Which two steps are required for a complete Cisco DNA Center upgrade? (Choose two.)

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

Answer: DE

NEW QUESTION 487
- (Topic 4)



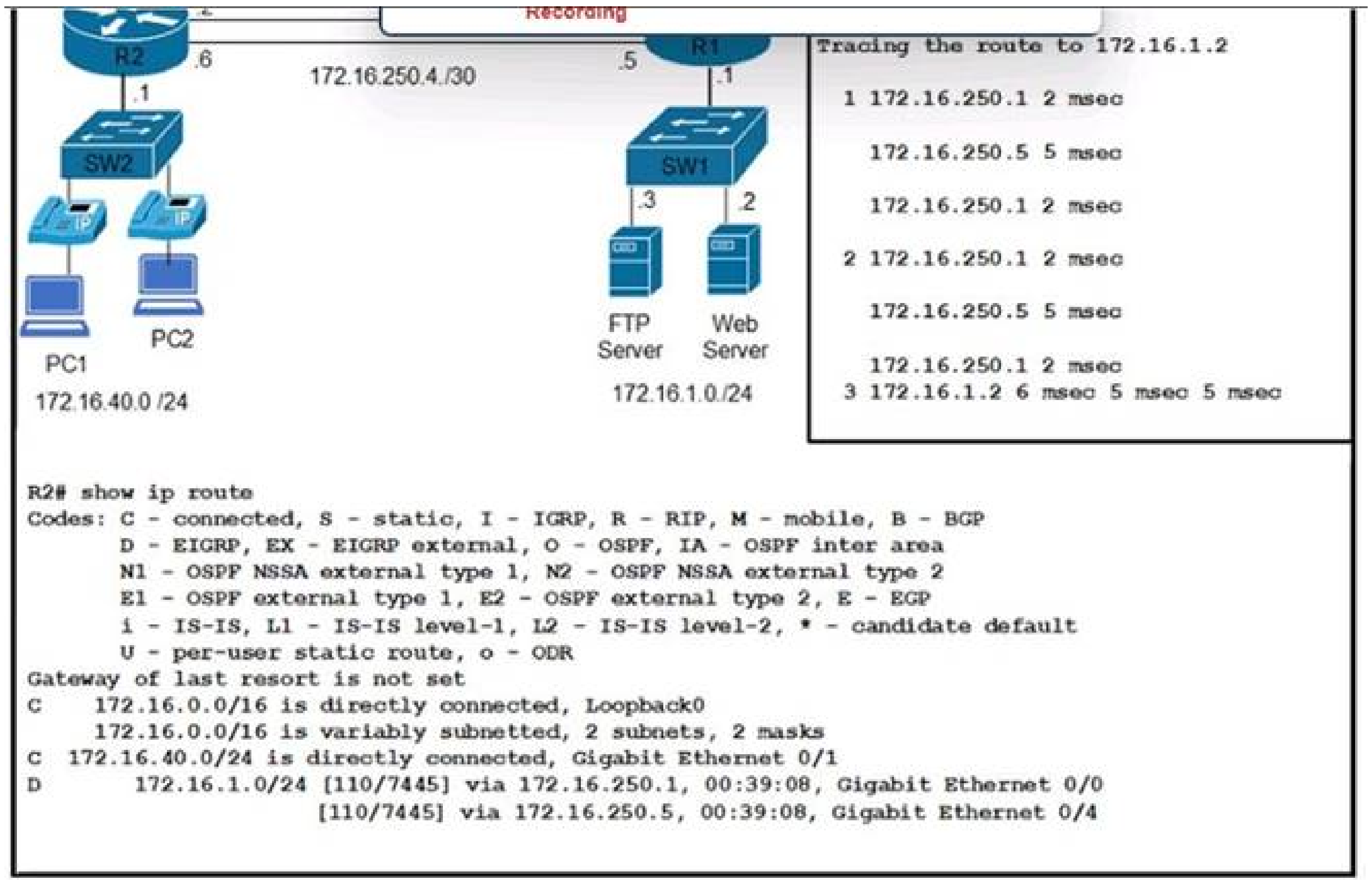
Request URL: https://www.cisco.com/libs/granite/csrf/token.json
Request Method: GET
Status Code: 403
Remote Address: 23.207.65.173:443
Referrer Policy: strict-origin-when-cross-origin

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

A. The resource was unreachable
B. Access was denied based on the user permissions.
C. The resource 15 no longer available on the server.
D. There Is a conflict in the current stale of the resource.

Answer: B

NEW QUESTION 491
- (Topic 4)
Refer to the exhibit.



```
Tracing the route to 172.16.1.2

  1 172.16.250.1 2 msec

    172.16.250.5 5 msec

    172.16.250.1 2 msec

  2 172.16.250.1 2 msec

    172.16.250.5 5 msec

    172.16.250.1 2 msec
  3 172.16.1.2 6 msec 5 msec 5 msec
```

```
R2# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C    172.16.0.0/16 is directly connected, Loopback0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C  172.16.40.0/24 is directly connected, Gigabit Ethernet 0/1
D       172.16.1.0/24 [110/7445] via 172.16.250.1, 00:39:08, Gigabit Ethernet 0/0
                      [110/7445] via 172.16.250.5, 00:39:08, Gigabit Ethernet 0/4
```

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:

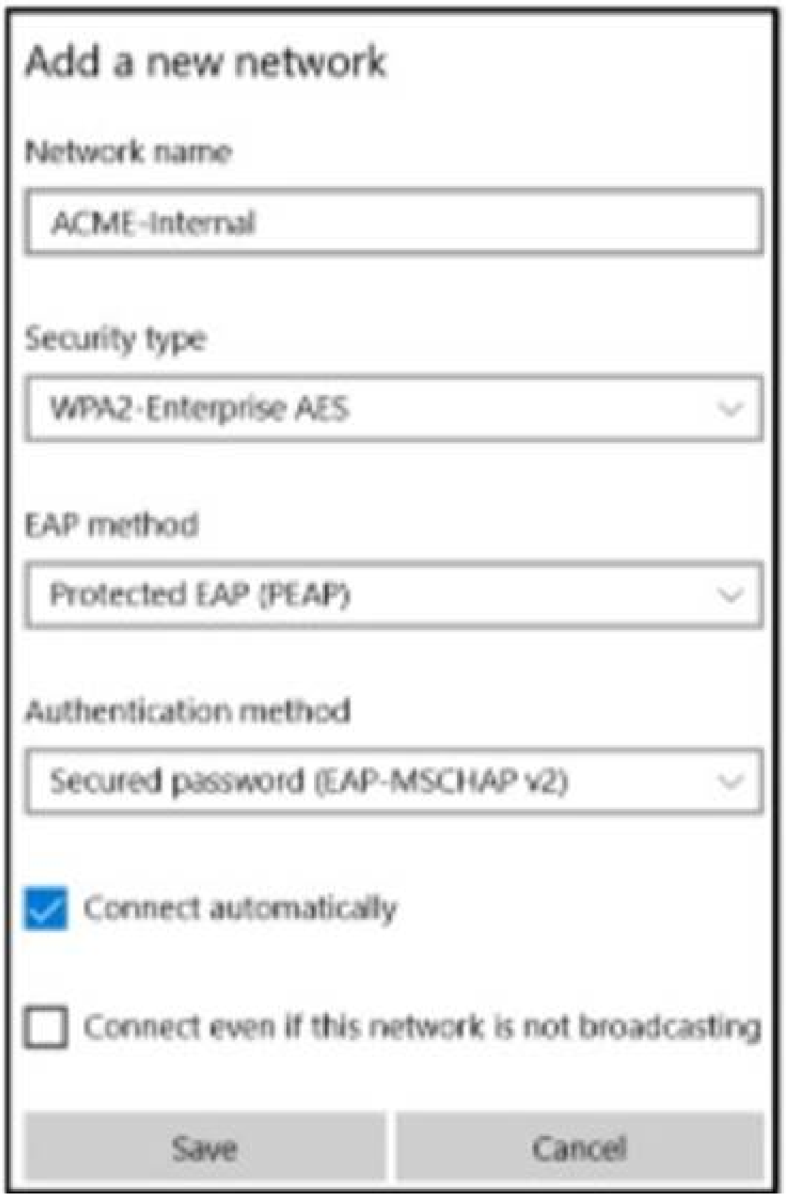
Traffic is load-balancing over both links, causing packets to arrive out of order. This can cause voice quality issues, such as jitter and delay. To avoid this problem, voice traffic should be sent over a single path, using a routing protocol that supports unequal-cost load balancing, such as EIGRP.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

NEW QUESTION 493
- (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 496
- (Topic 4)
Refer to the exhibit.



Add a new network

Network name

ACME-Internal

Security type

WPA2-Enterprise AES

EAP method

Protected EAP (PEAP)

Authentication method

Secured password (EAP-MSCHAP v2)

☑ Connect automatically

□ Connect even if this network is not broadcasting

A company has an internal wireless network with a hidden SSID and RADIUS-based client authentication for increased security. An employee attempts to manually add the company network to a laptop, but the laptop does not attempt to connect to the network. The regulatory domains of the access points and the laptop are identical. Which action resolves this issue?

A. Ensure that the "Connect even if this network is not broadcasting" option is selected.
B. Limit the enabled wireless channels on the laptop to the maximum channel range that is supported by the access points.
C. Change the security type to WPA2-Personal AES.
D. Use the empty string as the hidden SSID network name.

Answer: A

NEW QUESTION 497
- (Topic 4)
In a wireless network environment, what is calculated using the numerical values of the transmitter power level, cable loss, and antenna gain?

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

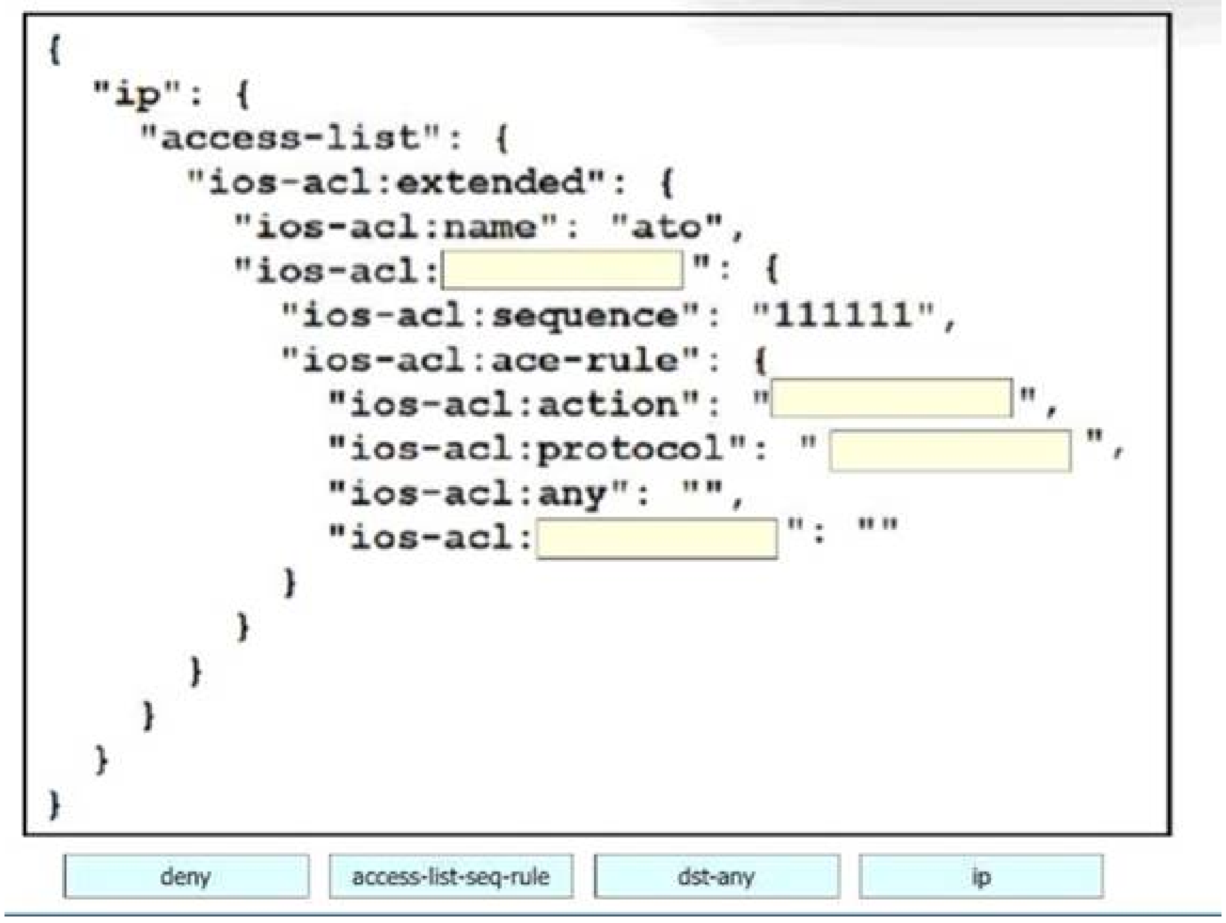
Answer: B

NEW QUESTION 502
- (Topic 4)
In lhe Cisco DNA Center Image Repository, what is a golden image?

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

Answer: B

NEW QUESTION 504
DRAG DROP - (Topic 4)
Drag and drop the code snippets from the bottom onto the blanks in the code to construct a request that configures a deny rule on an access list?

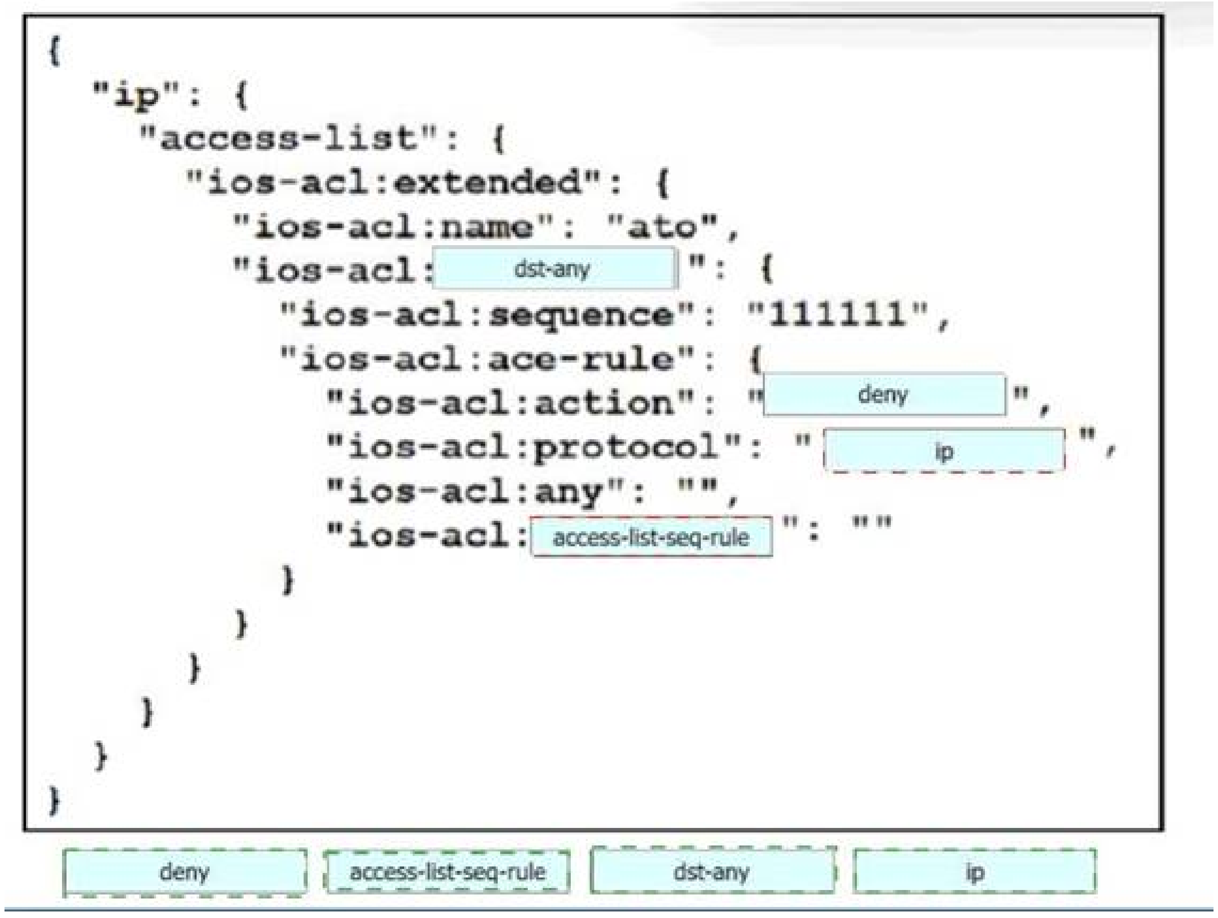


```
{
  "ip": {
    "access-list": {
      "ios-acl:extended": {
        "ios-acl:name": "ato",
        "ios-acl:          ": {
          "ios-acl:sequence": "111111",
          "ios-acl:ace-rule": {
            "ios-acl:action": "          ",
            "ios-acl:protocol": "           ",
         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

A. Mastered
B. Not Mastered

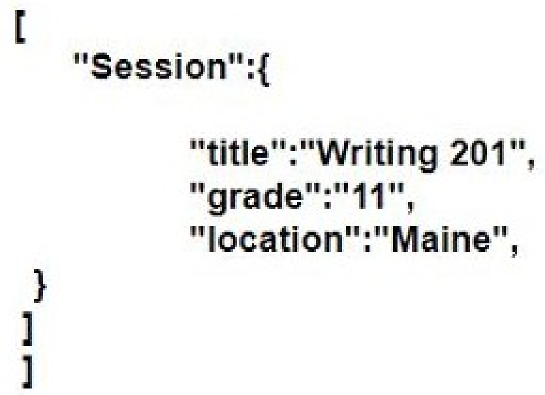
Answer: A

Explanation:



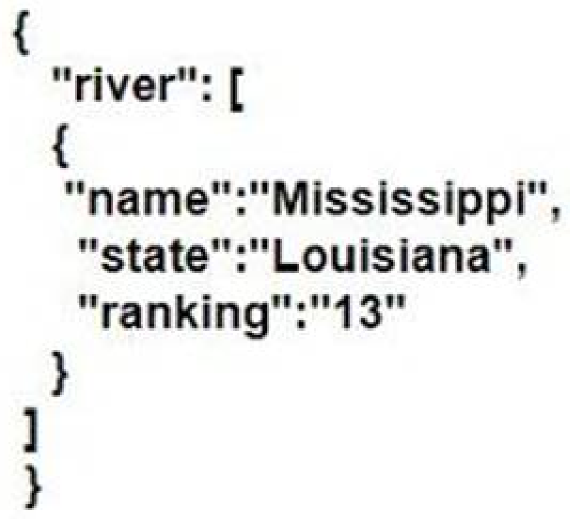
```
{
  "ip": {
    "access-list": {
      "ios-acl:extended": {
        "ios-acl:name": "ato",
        "ios-acl:dst-any": {
          "ios-acl:sequence": "111111",
          "ios-acl:ace-rule": {
            "ios-acl:action": "deny",
            "ios-acl:protocol": " ip ",
            "ios-acl:any":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

NEW QUESTION 506
- (Topic 4)
Which JSON script is properly formatted?
A)



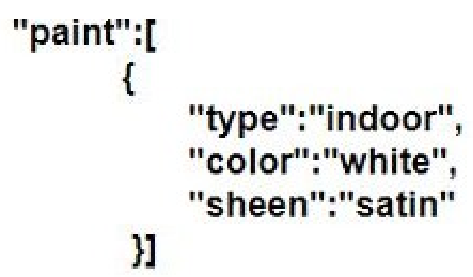
```
[
    "Session":{

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

B)



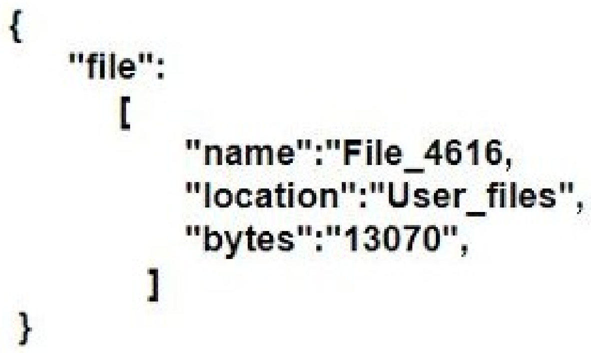
```
{
  "river": [
  {
   "name":"Mississippi",
    "state":"Louisiana",
    "ranking":"13"
  }
 ]
 }
```

C)



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

D)



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

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

Answer: A

Explanation:
Option A is the properly formatted JSON script. JSON (JavaScript Object Notation) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client, so it can be displayed on a web page, or vice versa). The JSON syntax rules are as follows12:
? Data is in name/value pairs, separated by commas. A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value: "name": "value".
? Curly braces hold objects. An object can contain multiple name/value pairs: {"name": "value", "name": "value", ...}.
? Square brackets hold arrays. An array can contain multiple values, separated by commas: ["value", "value", ...].
? Values can be strings (in double quotes), numbers, booleans (true or false), null, objects, or arrays.
Option A follows these rules and is a valid JSON script. It defines an object with four name/value pairs: "name", "age", "hobbies", and "address". The value of "name" is a string, the value of "age" is a number, the value of "hobbies" is an array of strings, and the value of "address" is another object with two name/value pairs: "city" and "country". The object is enclosed in curly braces and the name/value pairs are separated by commas.
Option B is not a valid JSON script because it uses single quotes instead of double quotes for the field names and string values. JSON requires double quotes for strings12.
Option C is not a valid JSON script because it does not use commas to separate the name/value pairs. JSON requires commas to separate the data elements within an object or an array12.
Option D is not a valid JSON script because it uses a semicolon instead of a colon to separate the field name and the value. JSON requires a colon to separate the name and the value in a name/value pair12. References: 1: JSON Introduction, 2: JSON Syntax

NEW QUESTION 511
- (Topic 4)

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

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

Answer: A

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

NEW QUESTION 513
- (Topic 4)
What is an advantage of utilizing data models in a multivendor environment?

A. lowering CPU load incurred to managed devices
B. improving communication security with binary encoded protocols
C. facilitating a unified approach to configuration and management
D. removing the distinction between configuration and runtime state data

Answer: C

NEW QUESTION 518
- (Topic 4)
In which two ways does the routing protocol OSPF differ from EIGRP? (Choose two.)

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

Answer: AD

NEW QUESTION 520
- (Topic 4)
A customer has a wireless network deployed within a multi-tenant building. The network provides client access, location-based services, and is monitored using Cisco DNA Center. The security department wants to locate and track malicious devices based on threat signatures. Which feature is required for this solution?

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

Answer: B

NEW QUESTION 522
- (Topic 4)
A technician needs to find the MAC address of a connecting router. Which of the following commands should the technician use?

A. arp
B. traceroute
C. nslookup
D. ping

Answer: A

Explanation:
This is because the arp command is used to display or manipulate the Address Resolution Protocol (ARP) cache, which is a table that maps IP addresses to MAC addresses. The arp command can show the MAC address of a connecting router by using the -a option, which displays the current ARP entries. For example, arp -a 192.168.1.1 will show the MAC address of the router with the IP address 192.168.1.1. The source of this answer is the Cisco ENCOR v1.1 course, module 3, lesson 3.1: Implementing IPv4 and IPv6 Addressing.

NEW QUESTION 526
- (Topic 4)
A VoIP phone is plugged in to a port but cannot receive calls. Which of the following needs to be done on the port to address the issue?

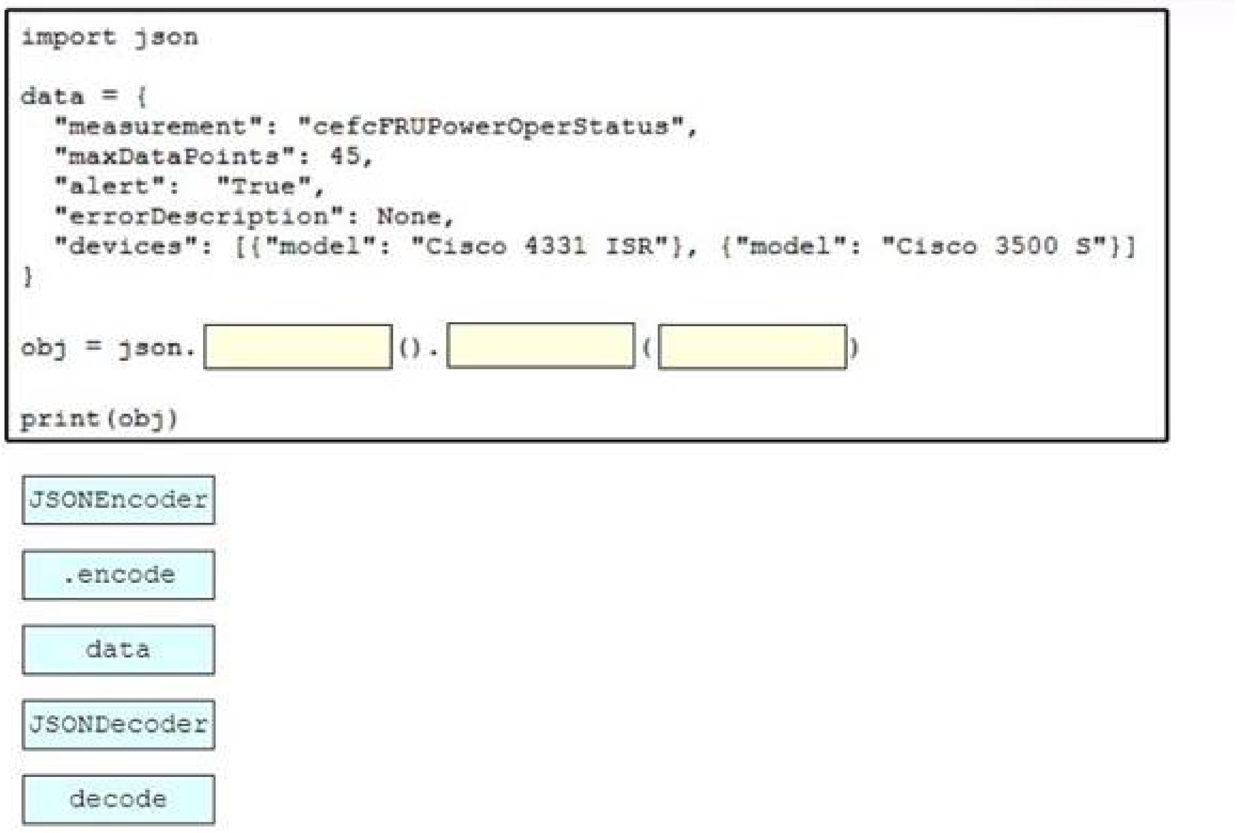
A. Trunk all VLANs on the port.
B. Configure the native VLAN.

C. Tag the traffic to voice VLAN.
D. Disable VLANs.

Answer: C

Explanation:
This is because the voice VLAN is a special VLAN that is used to separate the voice traffic from the data traffic on a switch port. The voice VLAN allows the VoIP phone to communicate with the voice server and receive calls. The voice VLAN is usually configured with a higher priority than the data VLAN to ensure the quality of service for the voice traffic. The voice VLAN is tagged with a VLAN ID that is different from the data VLAN ID. The switch port must be configured to tag the traffic to the voice VLAN, either manually or automatically using protocols such as CDP or LLDP. The source of this answer is the Cisco ENCOR v1.1 course, module 3, lesson 3.2: Implementing VLANs and Trunks.

NEW QUESTION 529
DRAG DROP - (Topic 4)
Drag and drop the code snippets from the bottom onto the blanks in the script to convert a Python object into a JSON string. Not all options are used.



```
import json

data = {
  "measurement": "cefcFRUPowerOperStatus",
  "maxDataPoints": 45,
  "alert":  "True",
  "errorDescription": None,
  "devices": [{"model": "Cisco 4331 ISR"}, {"model": "Cisco 3500 S"}]
}

obj = json.          ().          (          )

print(obj)
```

A. Mastered
B. Not Mastered

Answer: A

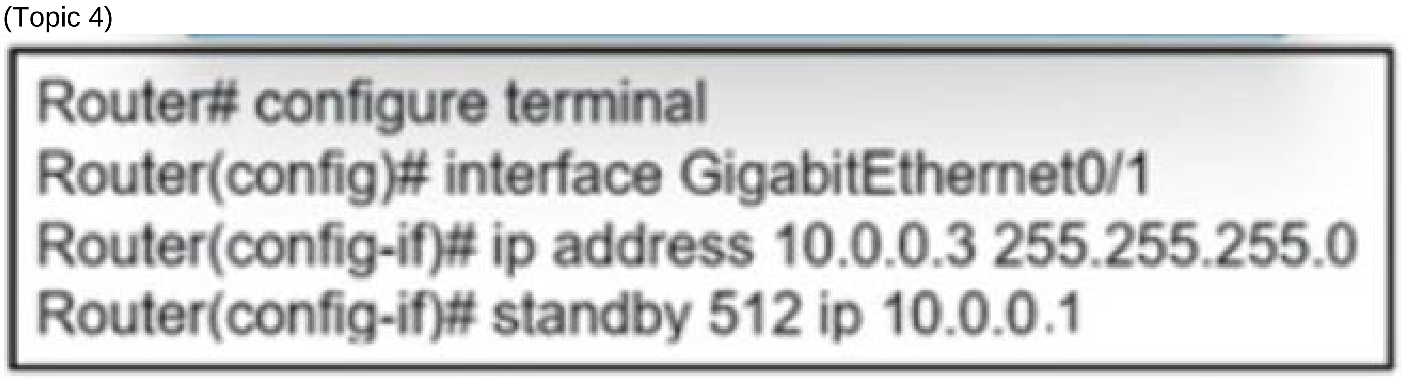
Explanation:
obj = json.JSONEncoder().encode(data)

NEW QUESTION 530
- (Topic 4)
What is one characteristic of VXLAN?

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

Answer: B

NEW QUESTION 535
- (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

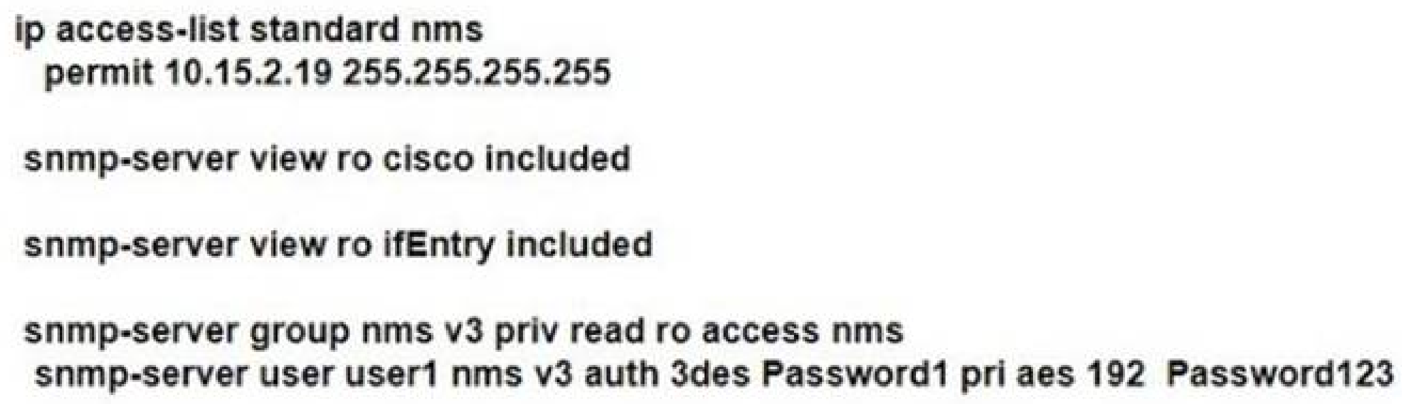
Answer: A

NEW QUESTION 538
- (Topic 4)
By default, which virtual MAC address does HSRP group 22 use?

A. c0:42:01:67:05:16
B. c0:07:0c:ac:00:22
C. 00:00:0c:07:ac:16
D. 00:00:0c:07:ac:22

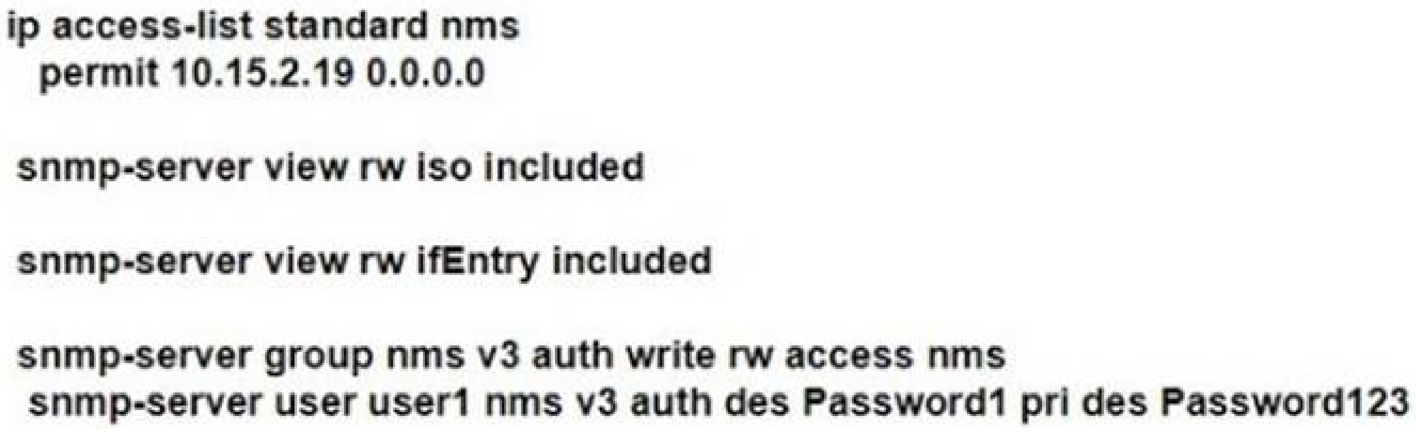
Answer: D

NEW QUESTION 539
- (Topic 4)
An engineer must configure Interface and sensor monitoring on a router. The NMS server is located in a trusted zone with IP address 10.15.2.19. Communication between the router and the NMS server must be encrypted and password-protected using the most secure algorithms. Access must be allowed only for the NMS server and with the minimum permission levels needed. Which configuration must the engineer apply?
A)



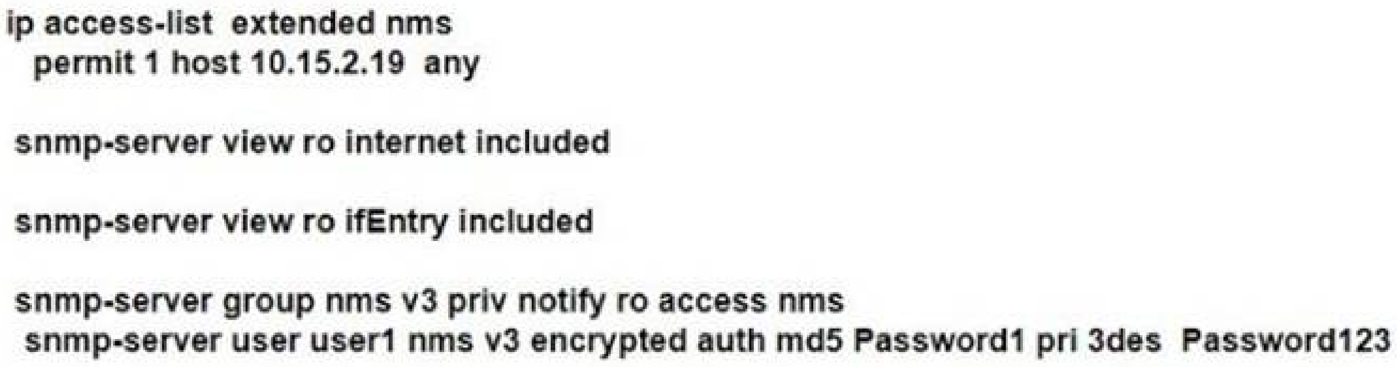
```
ip access-list standard nms
  permit 10.15.2.19 255.255.255.255

 snmp-server view ro cisco included

 snmp-server view ro ifEntry included

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

B)



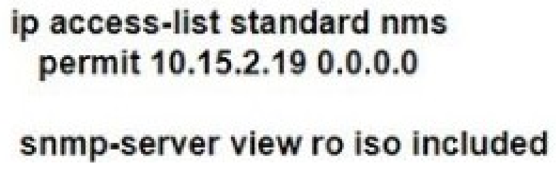
```
ip access-list standard nms
  permit 10.15.2.19 0.0.0.0

 snmp-server view rw iso included

 snmp-server view rw ifEntry included

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

C)



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

 snmp-server view ro internet included

 snmp-server view ro ifEntry included

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

D)



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

 snmp-server view ro iso included
```

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

Answer: A

Explanation:
Option A is the correct configuration to apply interface and sensor monitoring on a router with the given requirements. This option uses SNMPv3, which is the most secure version of SNMP that supports encryption and authentication. The configuration steps are as follows12:
? Create an access list named nms that permits only the NMS server with IP address 10.15.2.19 to access the router: ip access-list standard nms and permit 10.15.2.19 0.0.0.0.
? Create a view named rw that includes all the SNMP objects: snmp-server view rw included.
? Create a group named nms that uses SNMPv3 with privacy (encryption) and authentication, and assigns the view rw and the access list nms to the group: snmp-

server group nms v3 priv read rw access nms.
? Create a user named nms that belongs to the group nms and uses DES for authentication and AES for encryption, with the passwords despass and aespass respectively: snmp-server user nms nms v3 auth des despass priv aes 192 aespass.
Option B is incorrect because it does not use encryption for SNMP communication, which is required by the question. The noauth keyword in the snmp-server group command means that no authentication or encryption is used, which makes the SNMP packets vulnerable to eavesdropping and tampering1.
Option C is incorrect because it does not use the most secure algorithms for SNMP communication, which is required by the question. The md5 and des keywords in the snmp-server user command mean that MD5 and DES are used for authentication and encryption respectively, which are considered weak and outdated algorithms. AES and SHA are recommended instead1.
Option D is incorrect because it does not restrict the access to the NMS server only, which is required by the question. The snmp-server community command creates a community string that acts as a password for SNMP access, but it does not specify an access list to limit the source IP addresses that can use the community string. Therefore, any device that knows the community string can access the router via SNMP1. References: 1: Configuring SNMPv3, 2: SNMP Configuration Guide, Cisco IOS XE Gibraltar 16.12.x

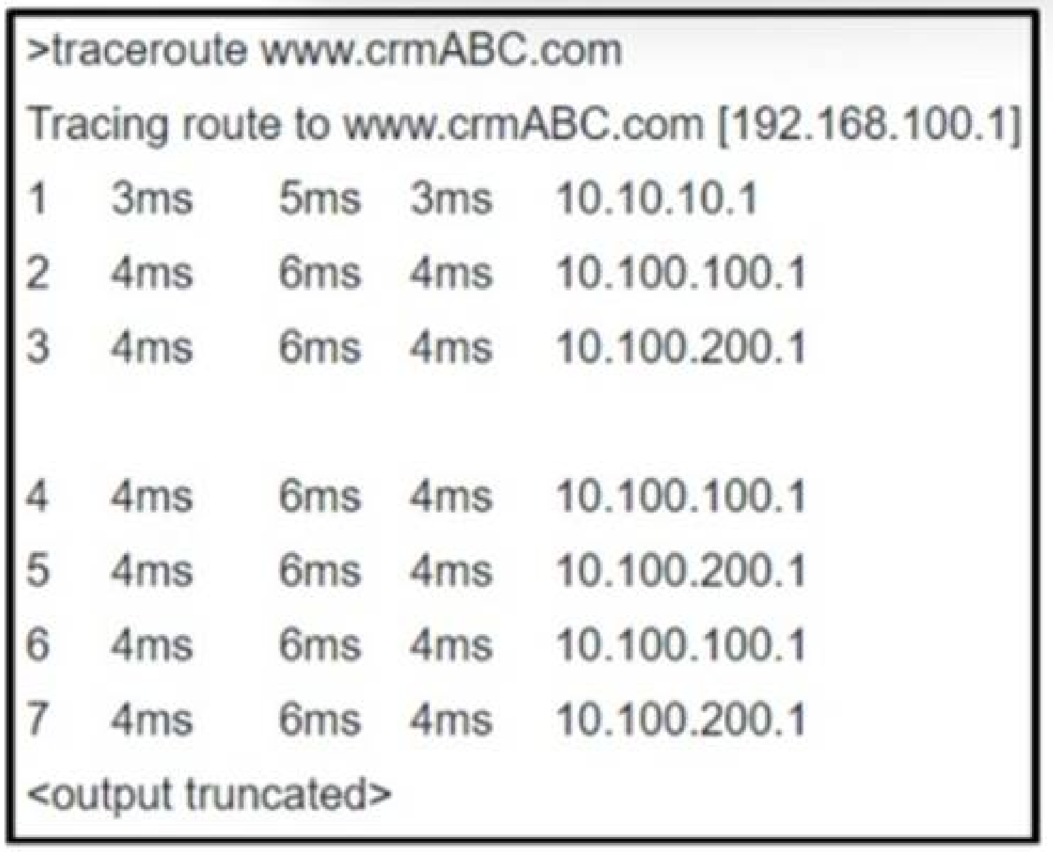
NEW QUESTION 544
- (Topic 4)
Which of the following should a junior security administrator recommend implementing to mitigate malicious network activity?

A. Intrusion prevention system
B. Load balancer
C. Access logging
D. Endpoint encryption

Answer: A

Explanation:
This is because an intrusion prevention system (IPS) is a security device that monitors the network traffic and detects and blocks any malicious or suspicious activity, such as attacks, exploits, or malware. An IPS can help mitigate malicious network activity by preventing it from reaching the intended target or spreading to other devices on the network. An IPS can also alert the administrator of any potential threats and provide information for further analysis and response. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.5: Implementing Firewall Technologies.

NEW QUESTION 547
- (Topic 4)



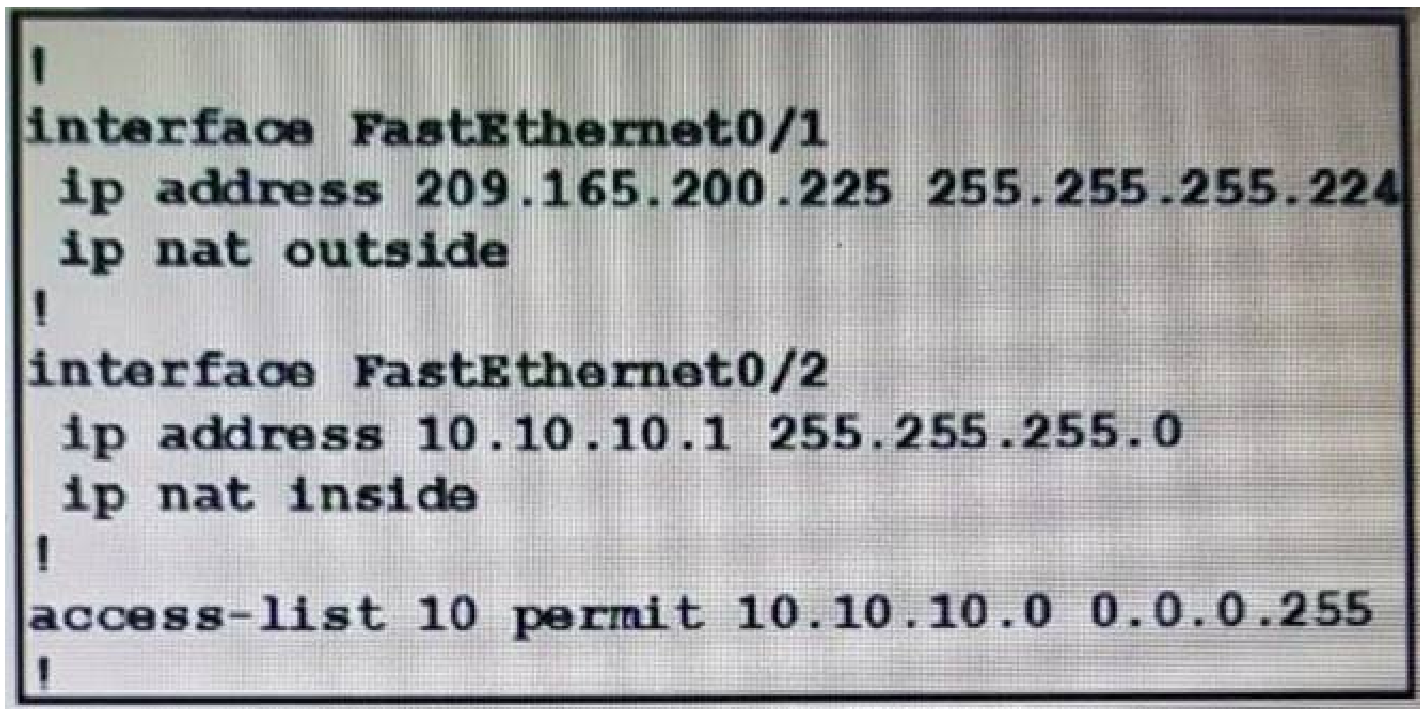
```
>traceroute www.crmABC.com
Tracing route to www.crmABC.com [192.168.100.1]
1    3ms    5ms   3ms    10.10.10.1
2    4ms    6ms   4ms    10.100.100.1
3    4ms    6ms   4ms    10.100.200.1


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

Refer to the exhibit Users cannot reach the web server at 192.168 100 1. What is the root cause for the failure?

A. The server is attempting to load balance between links 10.100 100.1 and 10 100.200.1.
B. The server is out of service.
C. There is a loop in the path to the server.
D. The gateway cannot translate the server domain name.

Answer: C

NEW QUESTION 550
- (Topic 4)



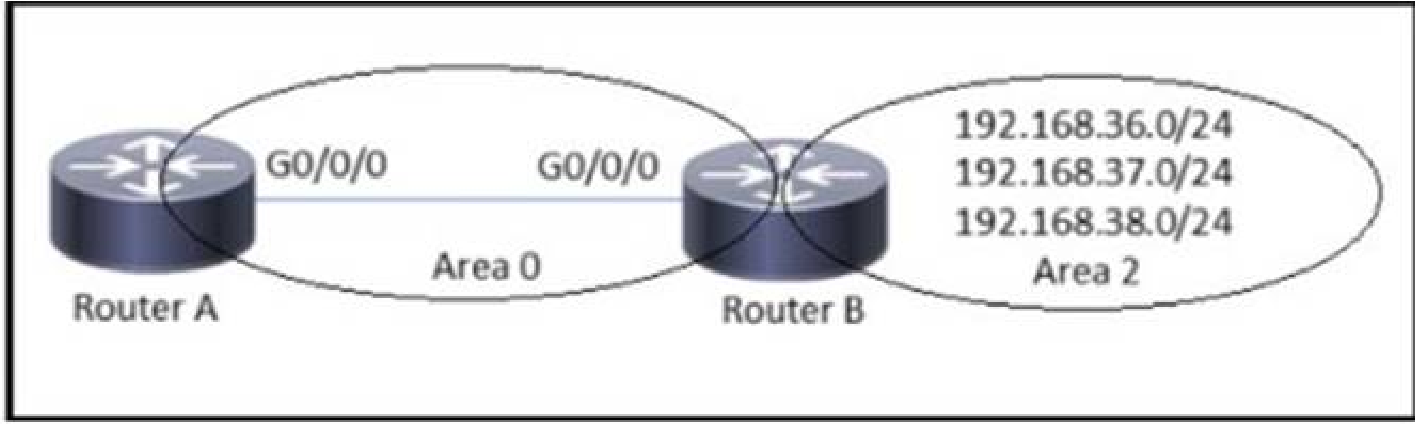
```
!
interface FastEthernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
!
interface FastEthernet0/2
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
access-list 10 permit 10.10.10.0 0.0.0.255
!
```

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

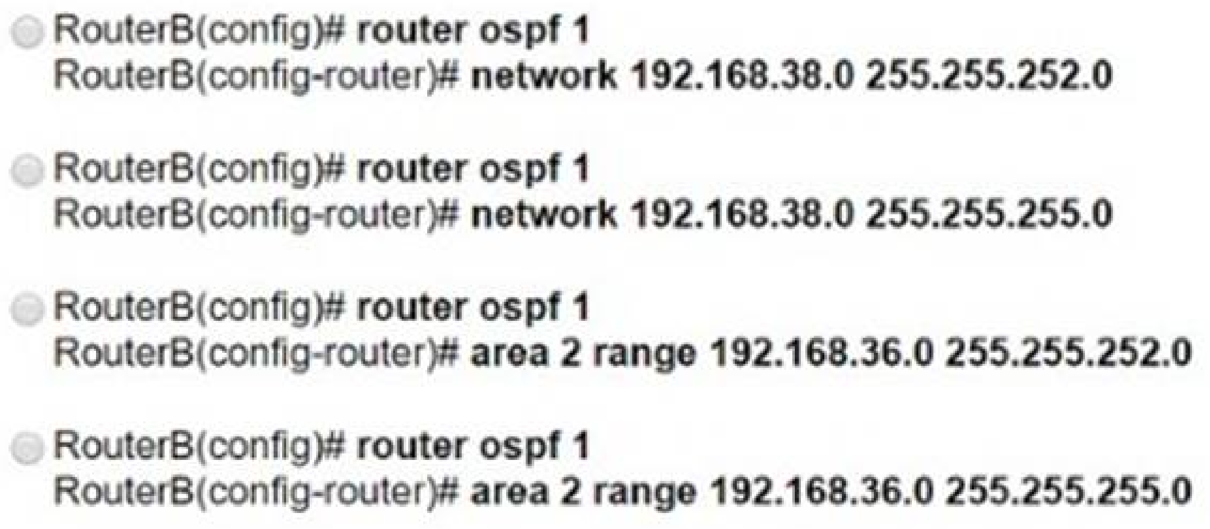
A. ip nat inside source list 10 interface FastEthernet0/1 overload
B. ip nat inside source list 10 interface FastEthernet0/2 overload
C. ip nat outside source list 10 interface FastEthernet0/2 overload
D. ip nat outside source static 209.165.200.225 10.10.10.0 overload

Answer: A

NEW QUESTION 554
- (Topic 4)



Refer to the exhibit. Which configuration is required to summarize the Area 2 networks that are advertised to Area 0?



○ RouterB(config)# **router ospf 1**
RouterB(config-router)# **network 192.168.38.0 255.255.252.0**

○ RouterB(config)# **router ospf 1**
RouterB(config-router)# **network 192.168.38.0 255.255.255.0**

○ RouterB(config)# **router ospf 1**
RouterB(config-router)# **area 2 range 192.168.36.0 255.255.252.0**

○ RouterB(config)# **router ospf 1**
RouterB(config-router)# **area 2 range 192.168.36.0 255.255.255.0**

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

Answer: C

NEW QUESTION 556
- (Topic 4)
Which router is elected the IGMP Querier when more than one router is in the same LAN segment?

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

Answer: B

NEW QUESTION 557
- (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 561
- (Topic 4)
Which tool is used in Cisco DNA Center to build generic configurations that are able to be applied on device with similar network settings?

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

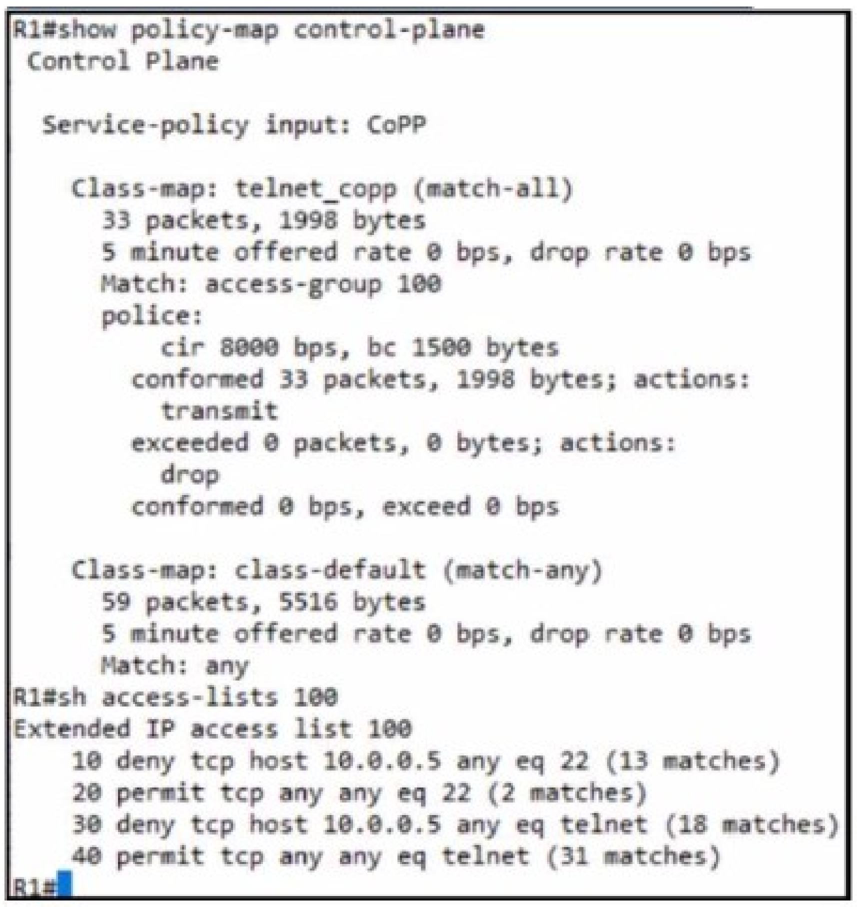
Answer: B

NEW QUESTION 562
- (Topic 4)
What does the Cisco DNA Center Authentication API provide?

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

Answer: B

NEW QUESTION 564
- (Topic 4)
Refer to the exhibit.



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

  Service-policy input: CoPP

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

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

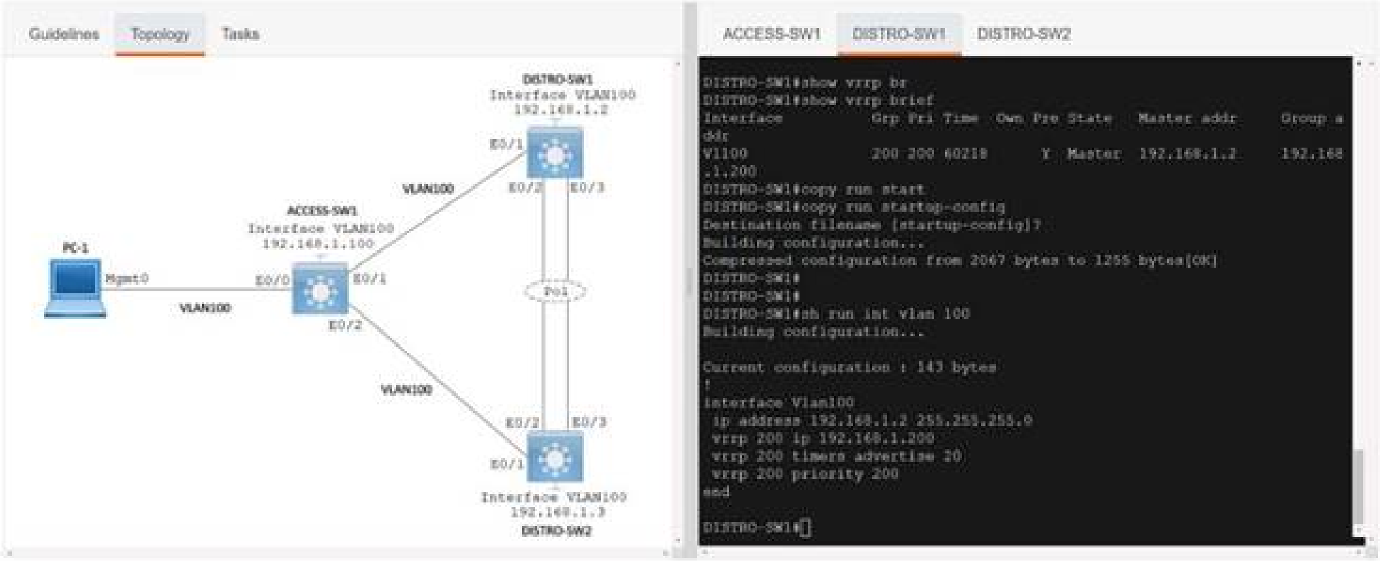
Which result Is achieved by the CoPP configuration?

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

Answer: C

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

NEW QUESTION 565
SIMULATION - (Topic 4)
Simulation 10

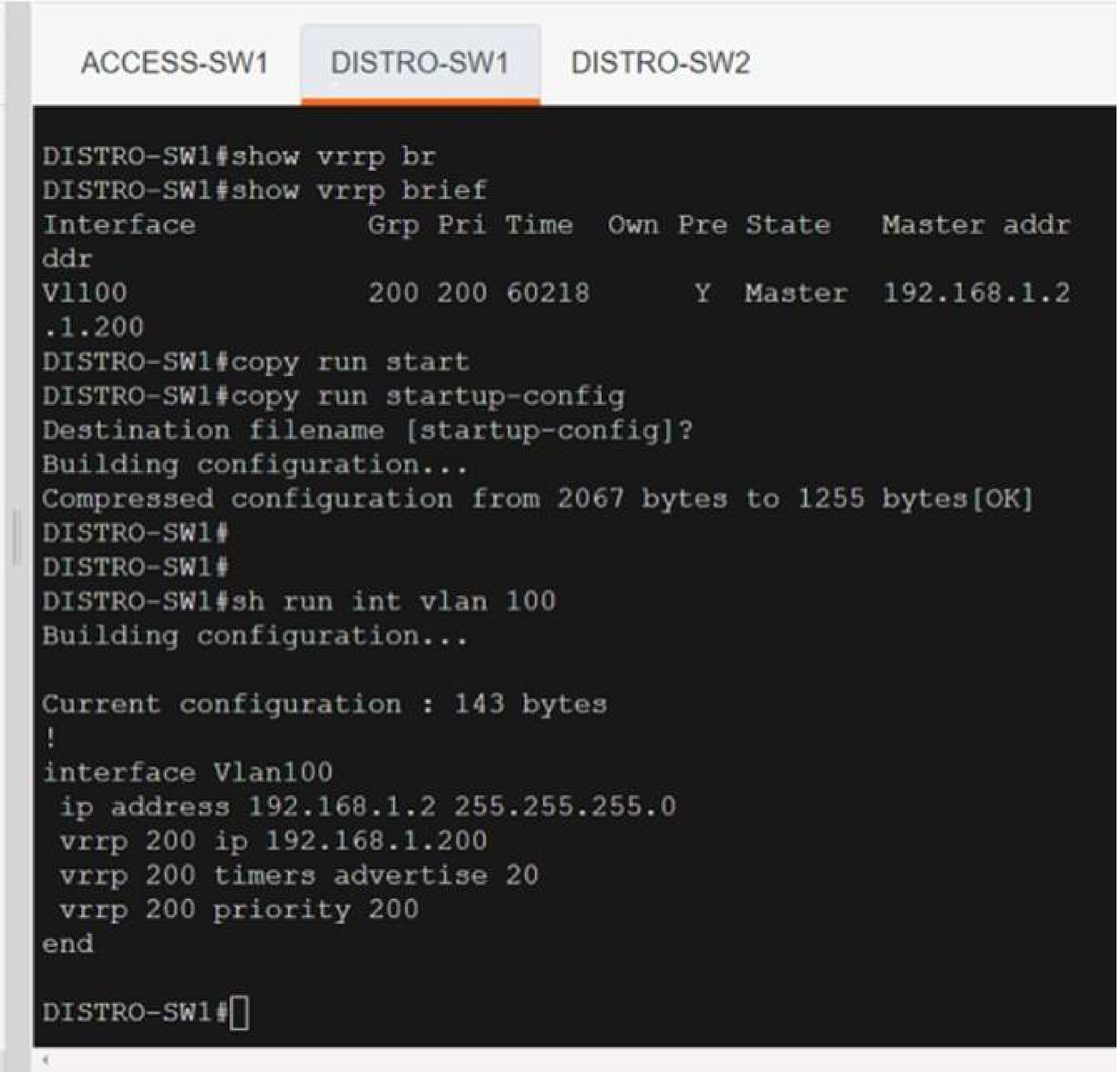


```
DISTRO-SW1#show vrrp br
DISTRO-SW1#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group a
ddr
V1100              200 200 60218      Y  Master  192.168.1.2     192.168
.1.200
DISTRO-SW1#copy run start
DISTRO-SW1#copy run startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2067 bytes to 1255 bytes[OK]
DISTRO-SW1#
DISTRO-SW1#
DISTRO-SW1#sh run int vlan 100
Building configuration...

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

DISTRO-SW1#
```

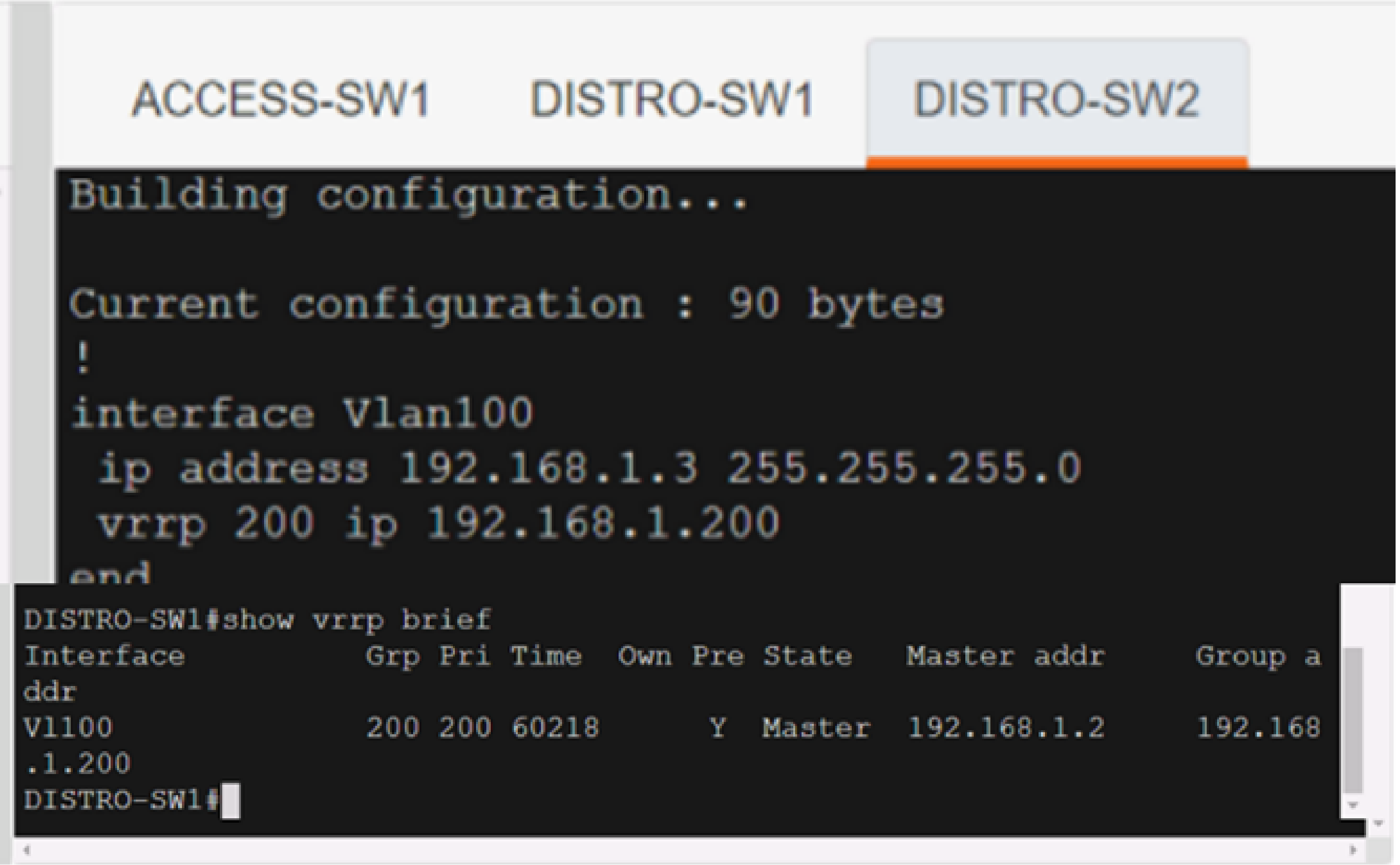
A. Mastered
B. Not Mastered

Answer: A

Explanation:



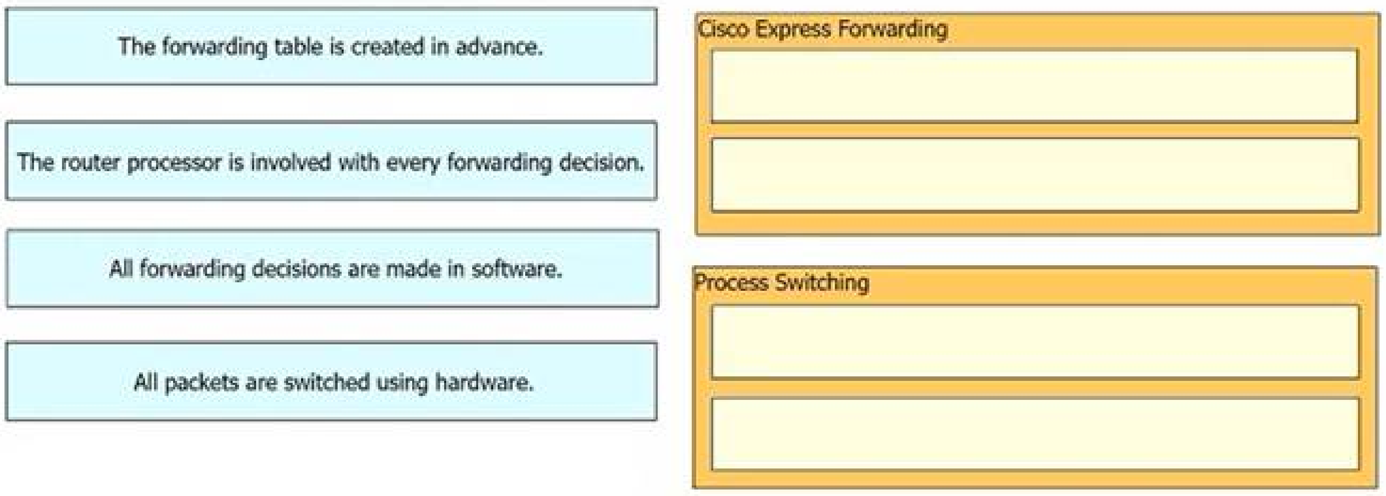
```
DISTRO-SW1#show vrrp br
DISTRO-SW1#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr
ddr
V1100              200 200 60218      Y  Master  192.168.1.2
.1.200
DISTRO-SW1#copy run start
DISTRO-SW1#copy run startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2067 bytes to 1255 bytes[OK]
DISTRO-SW1#
DISTRO-SW1#
DISTRO-SW1#sh run int vlan 100
Building configuration...

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

DISTRO-SW1#
```



```
Building configuration...

Current configuration : 90 bytes
!
interface Vlan100
 ip address 192.168.1.3 255.255.255.0
 vrrp 200 ip 192.168.1.200
end
```

```
DISTRO-SW1#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group a
ddr
Vl100              200 200 60218       Y  Master  192.168.1.2     192.168
.1.200
DISTRO-SW1#
```

NEW QUESTION 568
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.

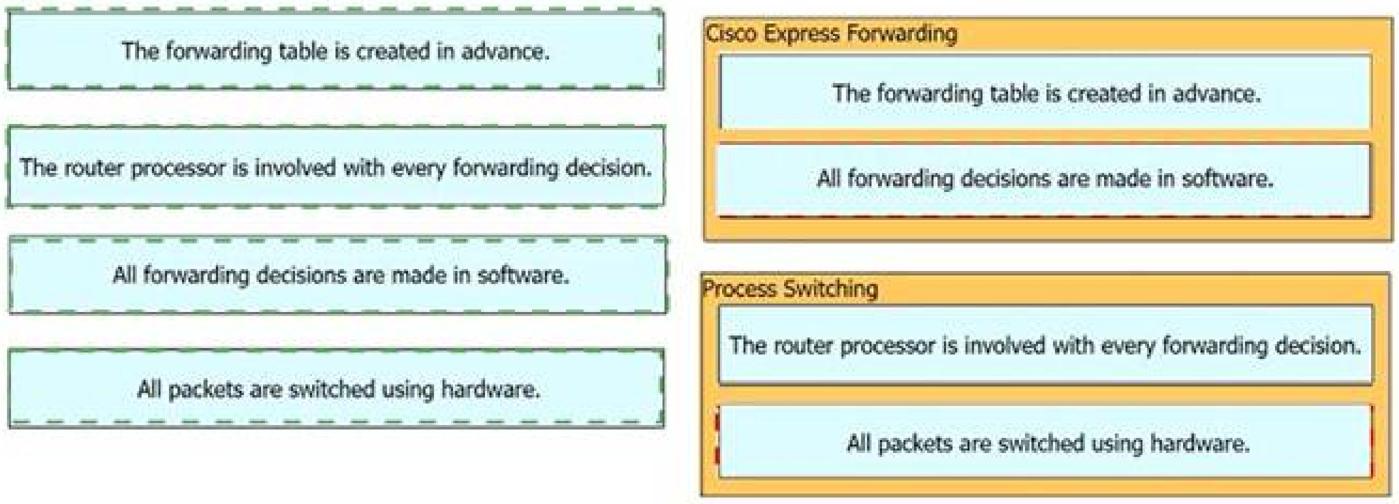
Cisco Express Forwarding

Process Switching

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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 572
- (Topic 4)
Refer to the exhibit. What is the result of this Python code?

A. 1
B. 7
C. 7.5

Answer: D

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

NEW QUESTION 577
- (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

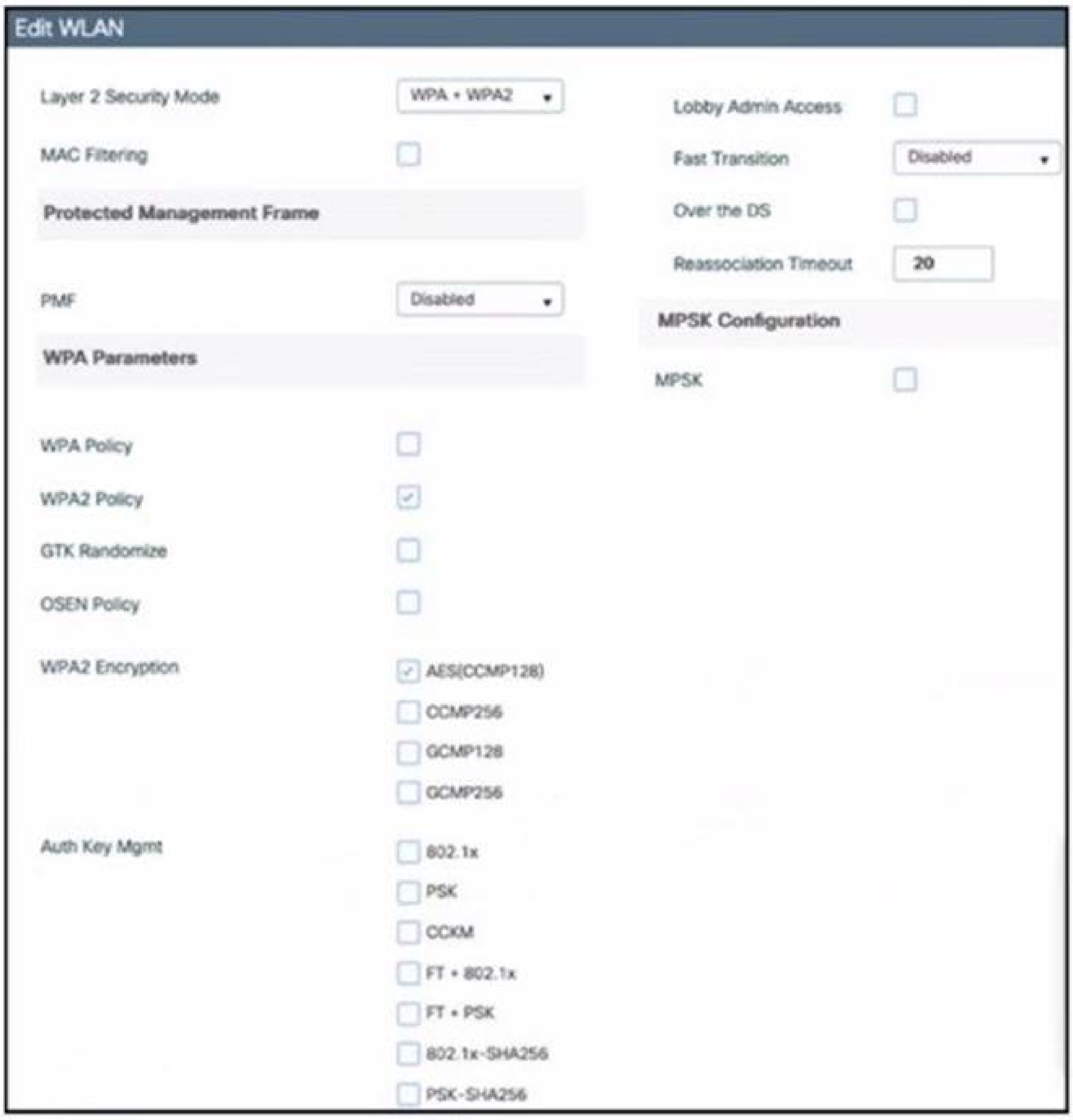
Explanation:
The workstation was configured with a static IP that is the same as the server. This is because if two devices on the same network have the same IP address, they will cause an IP address conflict, which will prevent them from communicating with other devices on the network. The users who 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 581
- (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 584
- (Topic 4)
Refer to the exhibit.



Edit WLAN

Layer 2 Security Mode: WPA + WPA2
MAC Filtering: □

Protected Management Frame

PMF: Disabled

WPA Parameters

WPA Policy: □
WPA2 Policy: ☑
GTK Randomize: □
OSEN Policy: □
WPA2 Encryption: ☑ AES(CCMP128) □ CCMP256 □ GCMP128 □ GCMP256
Auth Key Mgmt: □ 802.1x □ PSK □ CCKM □ FT + 802.1x □ FT + PSK □ 802.1x-SHA256 □ PSK-SHA256

Lobby Admin Access: □
Fast Transition: Disabled
Over the DS: □
Reassociation Timeout: 20

MPSK Configuration

MPSK: □

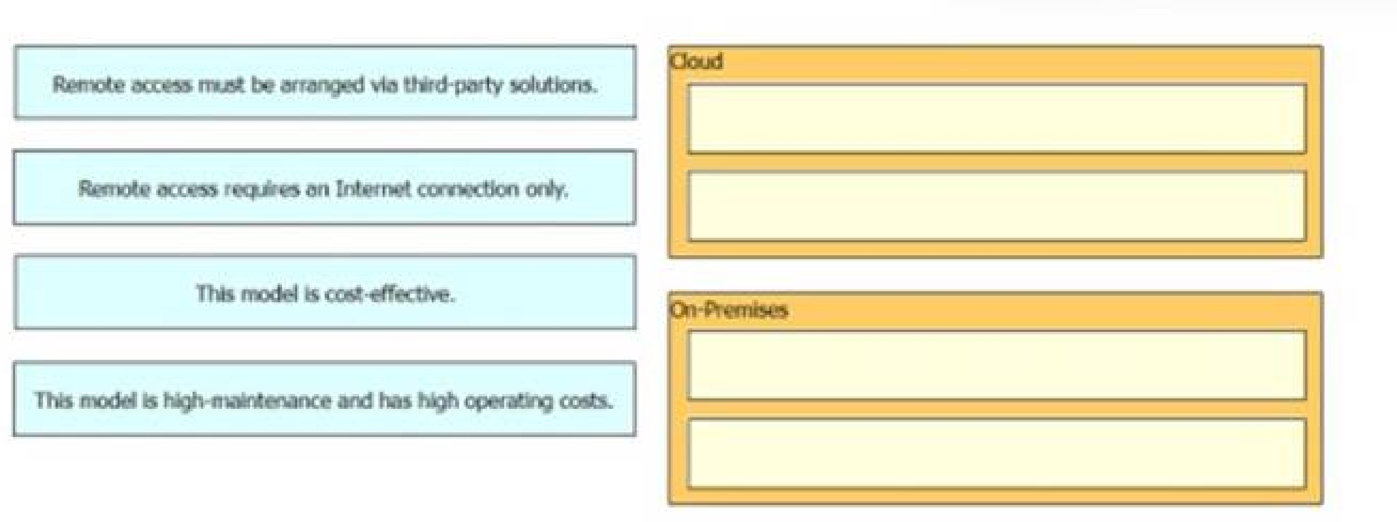
Which action must be taken to configure a WLAN for WPA2-AES with PSK and allow only 802.l1r-capable clients to connect?

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

Answer: A

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

NEW QUESTION 585
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the deployment models on the right.



Remote access must be arranged via third-party solutions.

Remote access requires an Internet connection only.

This model is cost-effective.

This model is high-maintenance and has high operating costs.

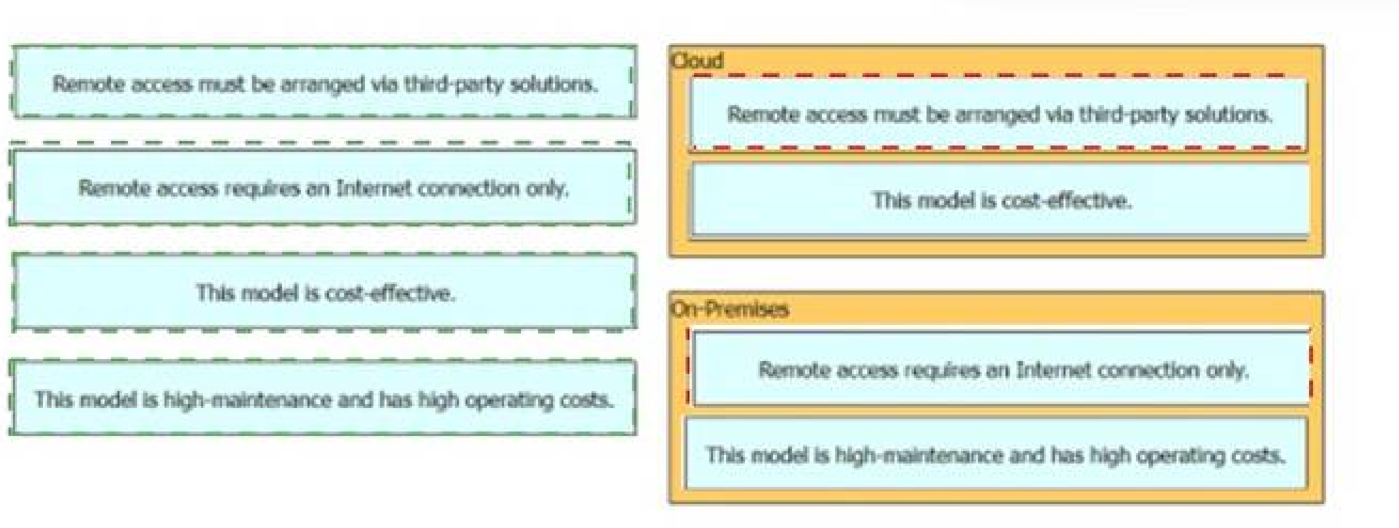
Cloud

On-Premises

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Remote access must be arranged via third-party solutions.

Remote access requires an Internet connection only.

This model is cost-effective.

This model is high-maintenance and has high operating costs.

Cloud

Remote access must be arranged via third-party solutions.

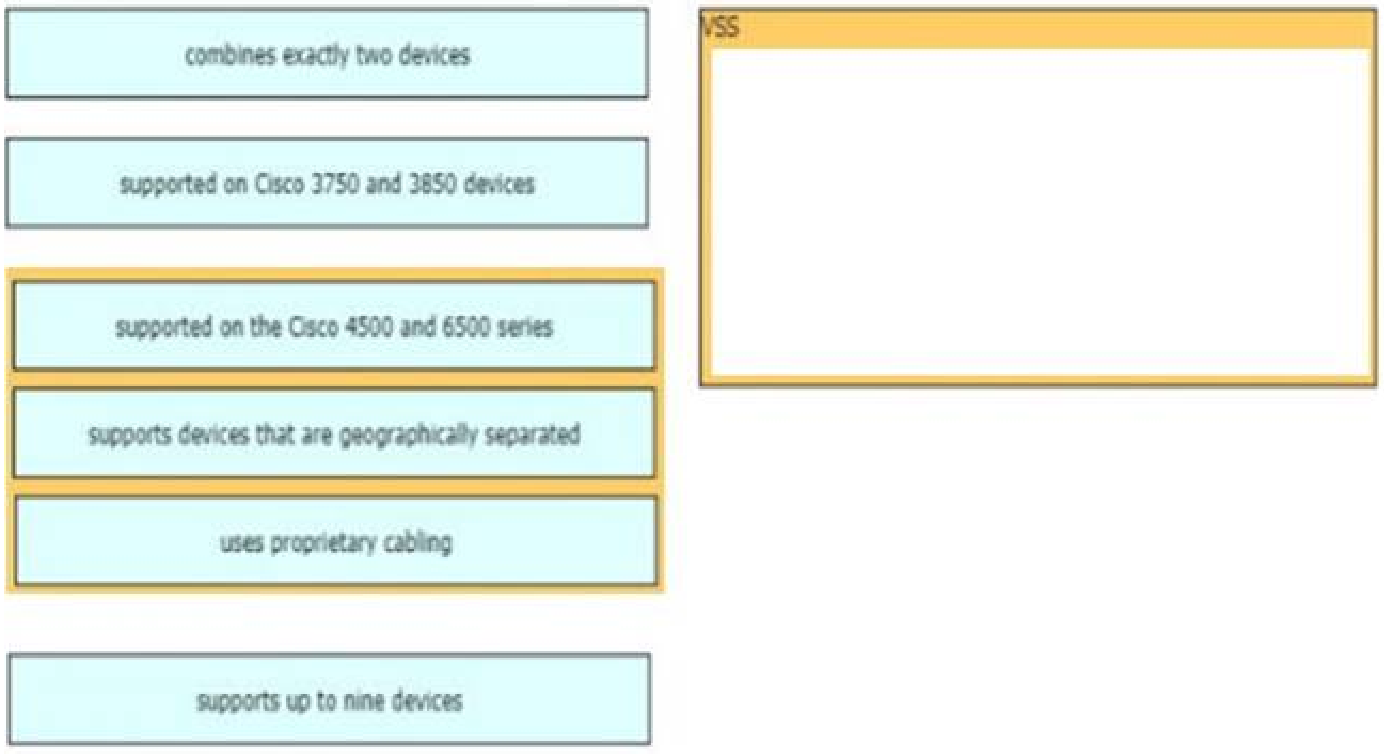
This model is cost-effective.

On-Premises

Remote access requires an Internet connection only.

This model is high-maintenance and has high operating costs.

NEW QUESTION 590
DRAG DROP - (Topic 4)
Drag and drop the description of the VSS technology from the left to the right. NOT all options are used.



combines exactly two devices

supported on Cisco 3750 and 3850 devices

supported on the Cisco 4500 and 6500 series

supports devices that are geographically separated

uses proprietary cabling

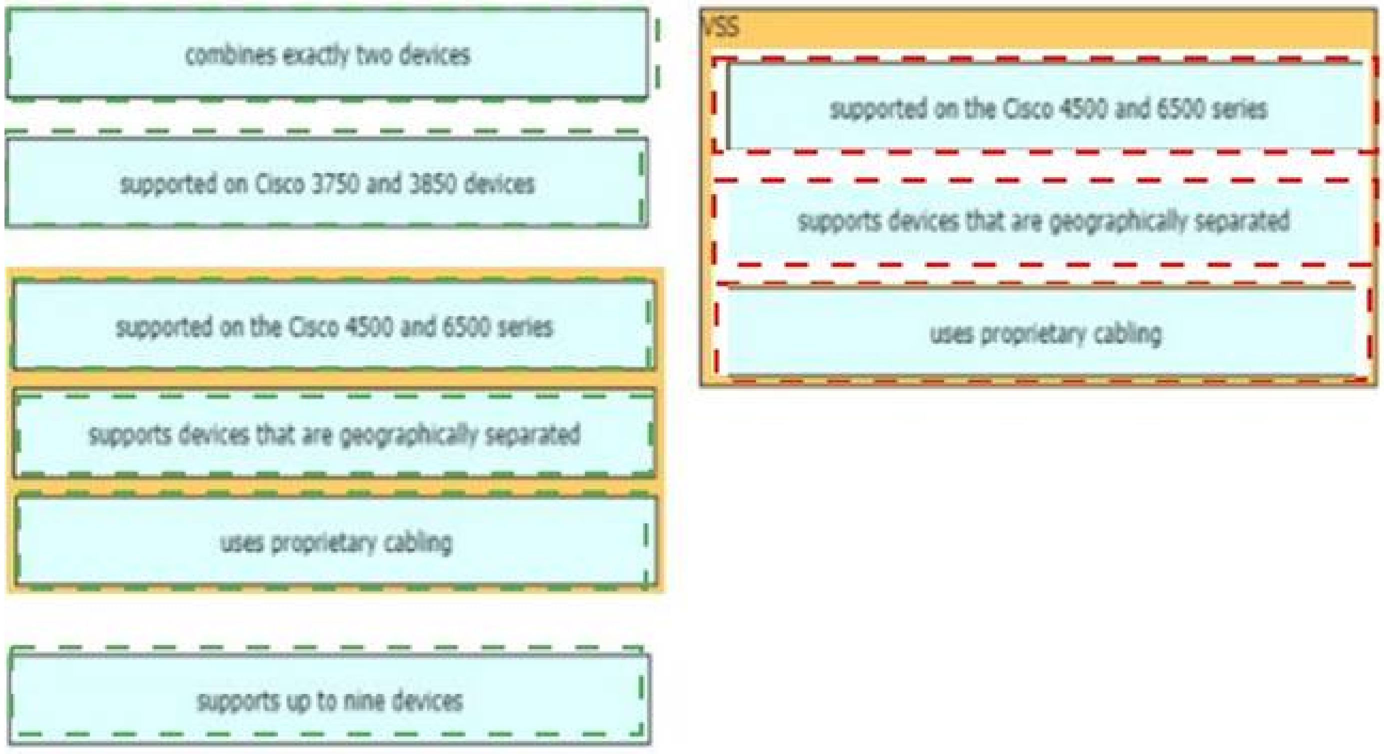
supports up to nine devices

VSS

A. Mastered
B. Not Mastered

Answer: A

Explanation:



combines exactly two devices

supported on Cisco 3750 and 3850 devices

supported on the Cisco 4500 and 6500 series

supports devices that are geographically separated

uses proprietary cabling

supports up to nine devices

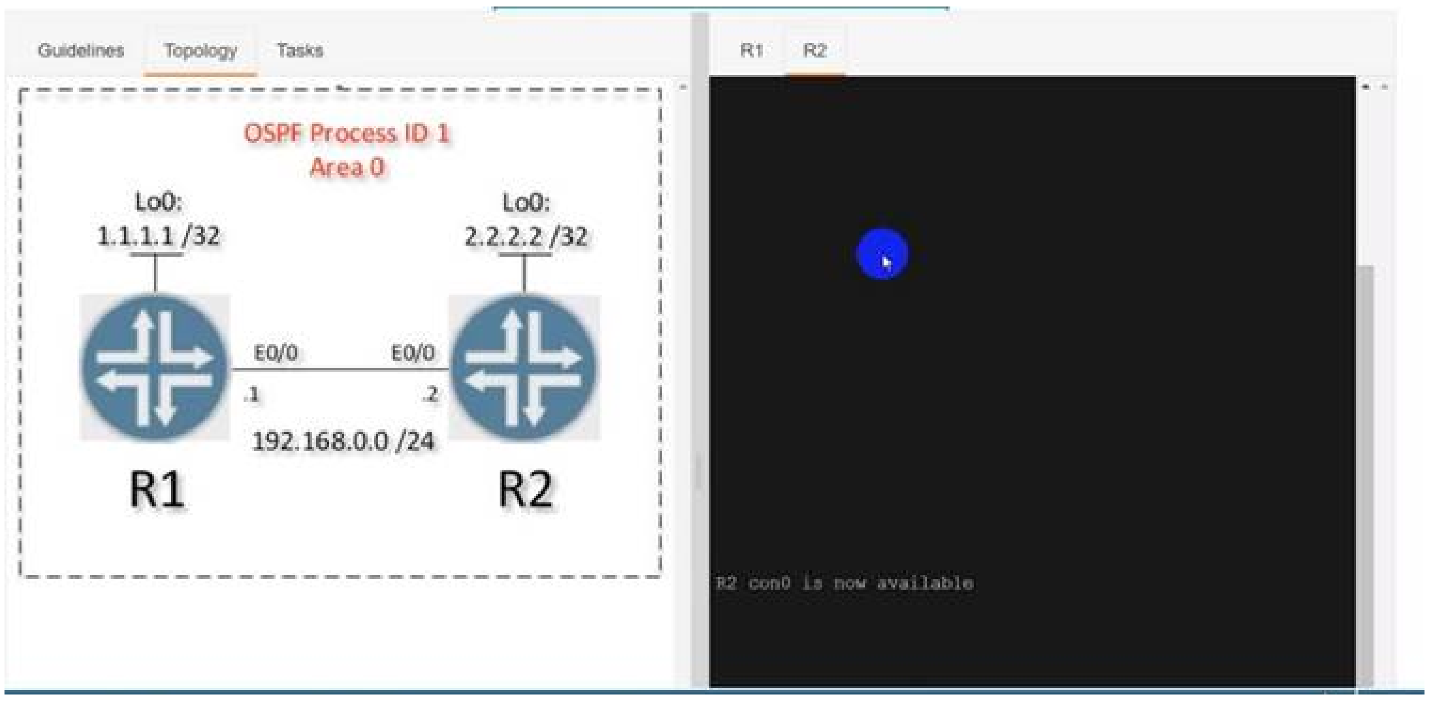
VSS

supported on the Cisco 4500 and 6500 series

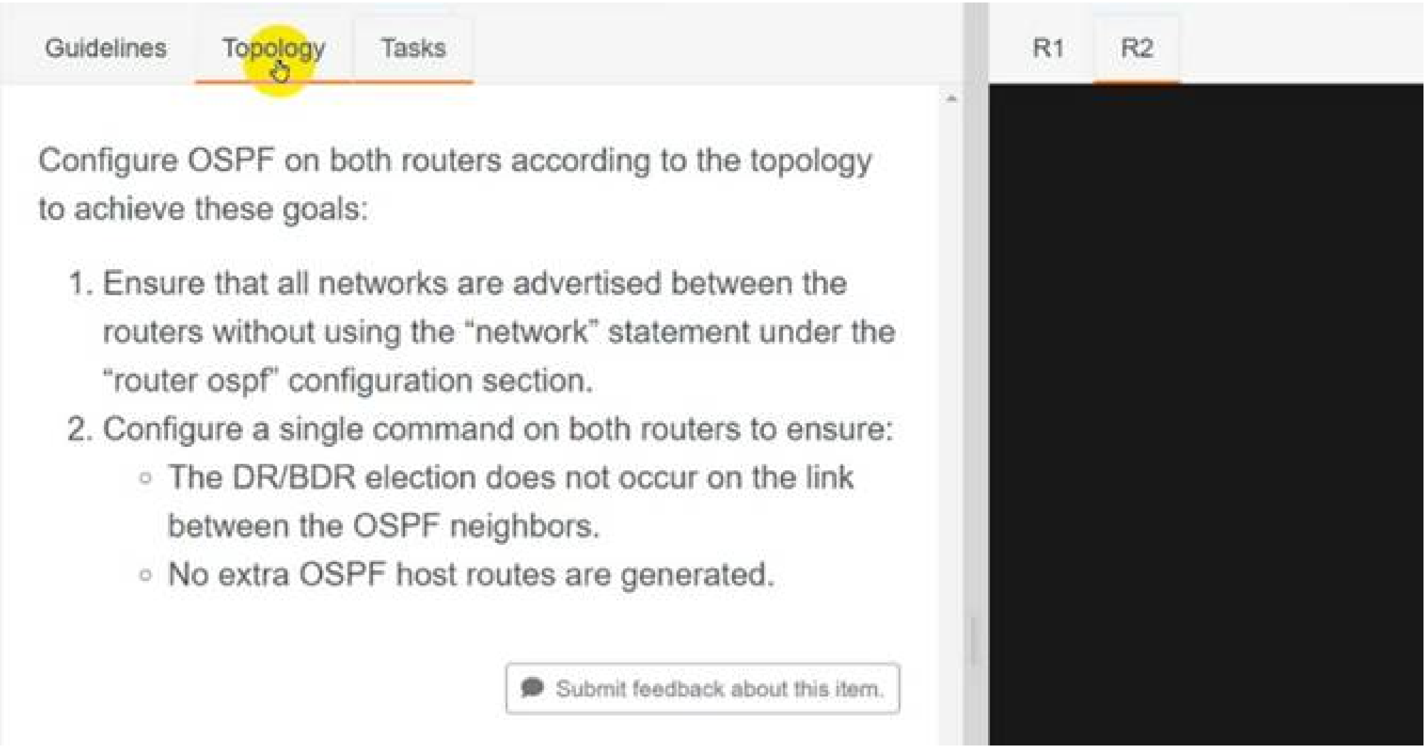
supports devices that are geographically separated

uses proprietary cabling

NEW QUESTION 592
SIMULATION - (Topic 4)
Simulation 04
Configure OSPF on both routers according to the topology to achieve these goals:



```
R2 con0 is now available
```



Configure OSPF on both routers according to the topology to achieve these goals:

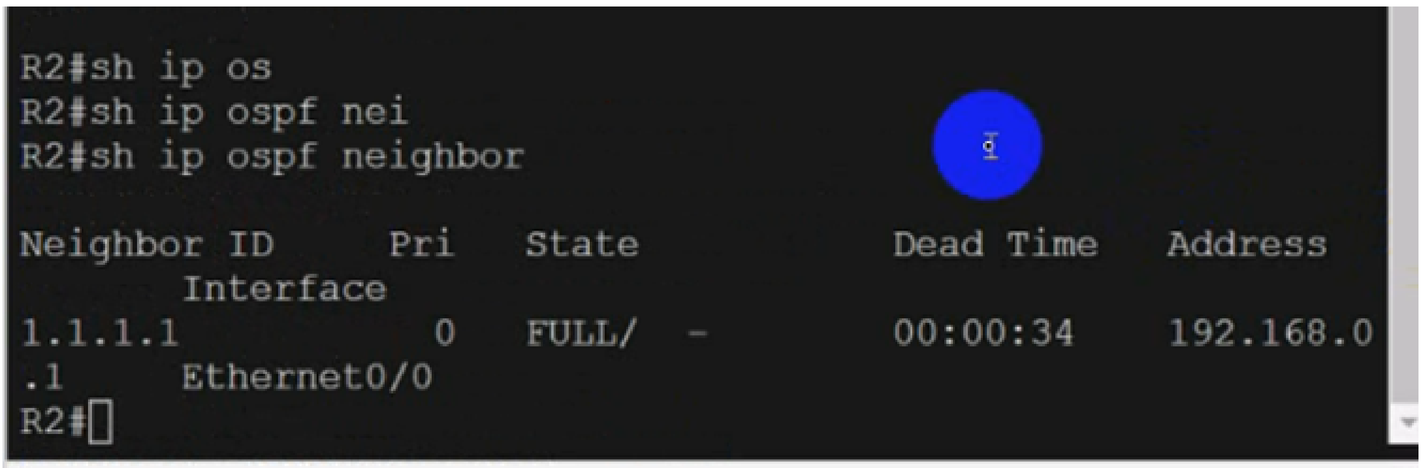
1. Ensure that all networks are advertised between the routers without using the “network” statement under the “router ospf” configuration section.
2. Configure a single command on both routers to ensure:
   - The DR/BDR election does not occur on the link between the OSPF neighbors.
   - No extra OSPF host routes are generated.

A. Mastered
B. Not Mastered

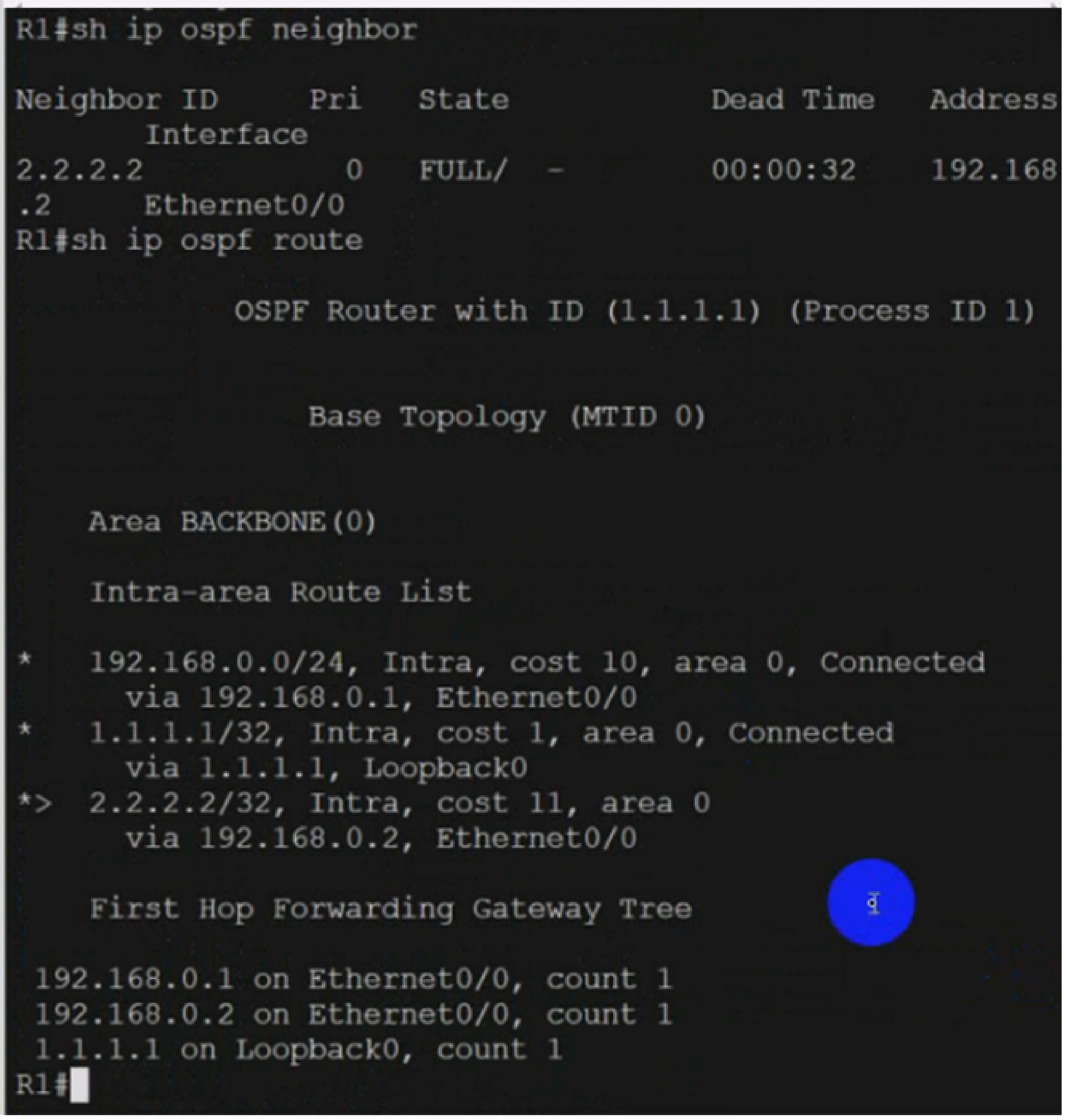
Answer: A

Explanation:

Solution:
R1
Router ospf 1 Int loop0
Ip ospf 1 area 0 Int et0/0
Ip ospf 1 area 0
Ip ospf network point-to-point Copy run start
R2
Router ospf 1 Int loop0
Ip ospf 1 area 0 Int et0/0
Ip ospf 1 area 0
Ip ospf network point-to-point Copy run start
Verification:-



```
R2#sh ip os
R2#sh ip ospf nei
R2#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
        Interface
1.1.1.1           0   FULL/  -        00:00:34    192.168.0
.1      Ethernet0/0
R2#
```



```
R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
        Interface
2.2.2.2           0   FULL/  -        00:00:32    192.168
.2      Ethernet0/0
R1#sh ip ospf route

            OSPF Router with ID (1.1.1.1) (Process ID 1)


                Base Topology (MTID 0)


    Area BACKBONE(0)

    Intra-area Route List

*   192.168.0.0/24, Intra, cost 10, area 0, Connected
      via 192.168.0.1, Ethernet0/0
*   1.1.1.1/32, Intra, cost 1, area 0, Connected
      via 1.1.1.1, Loopback0
*>  2.2.2.2/32, Intra, cost 11, area 0
      via 192.168.0.2, Ethernet0/0

    First Hop Forwarding Gateway Tree

 192.168.0.1 on Ethernet0/0, count 1
 192.168.0.2 on Ethernet0/0, count 1
 1.1.1.1 on Loopback0, count 1
R1#
```

NEW QUESTION 596

......

Relate Links

Contact us