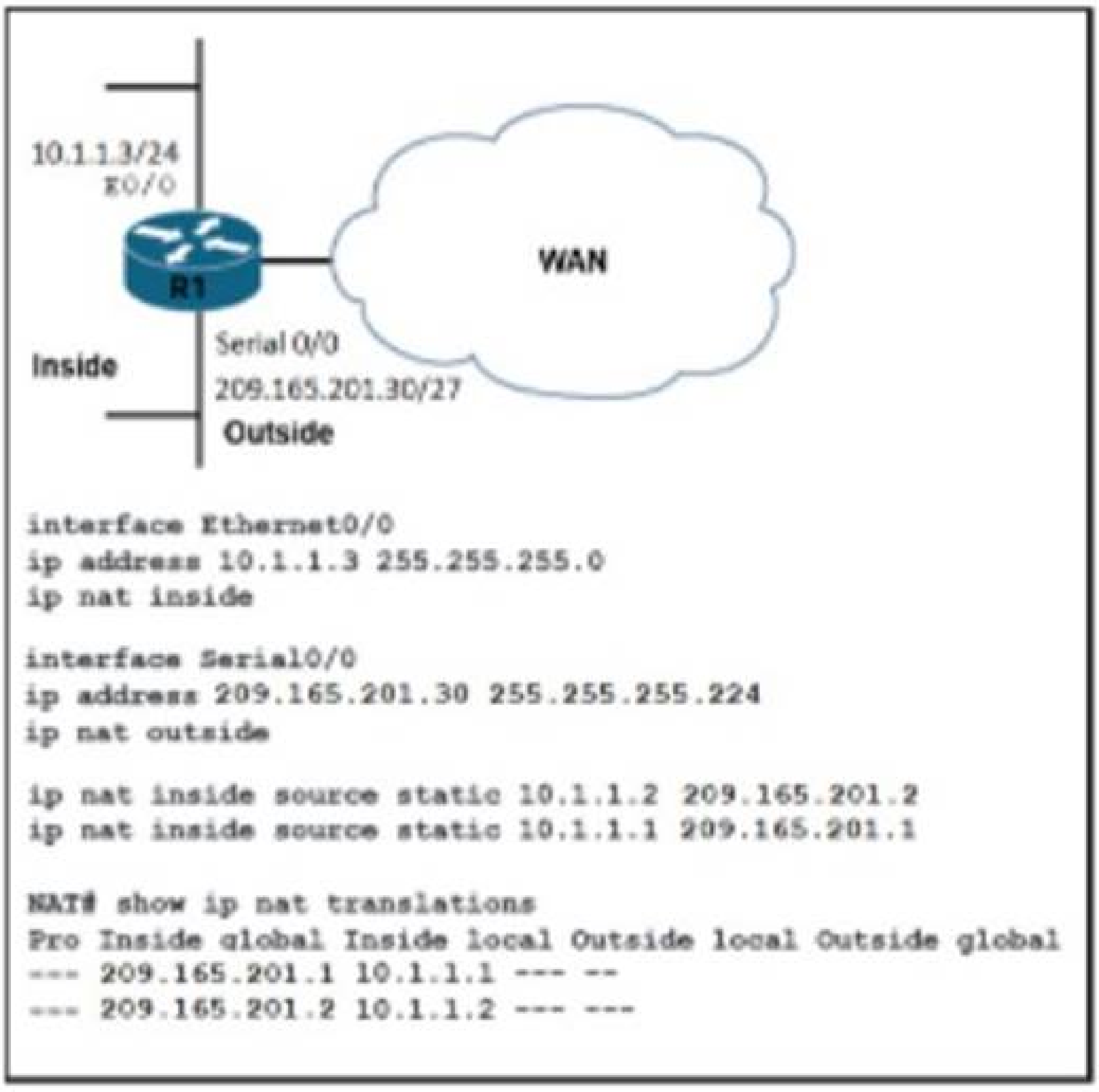
Cisco

Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies

NEW QUESTION 1
- (Topic 4)



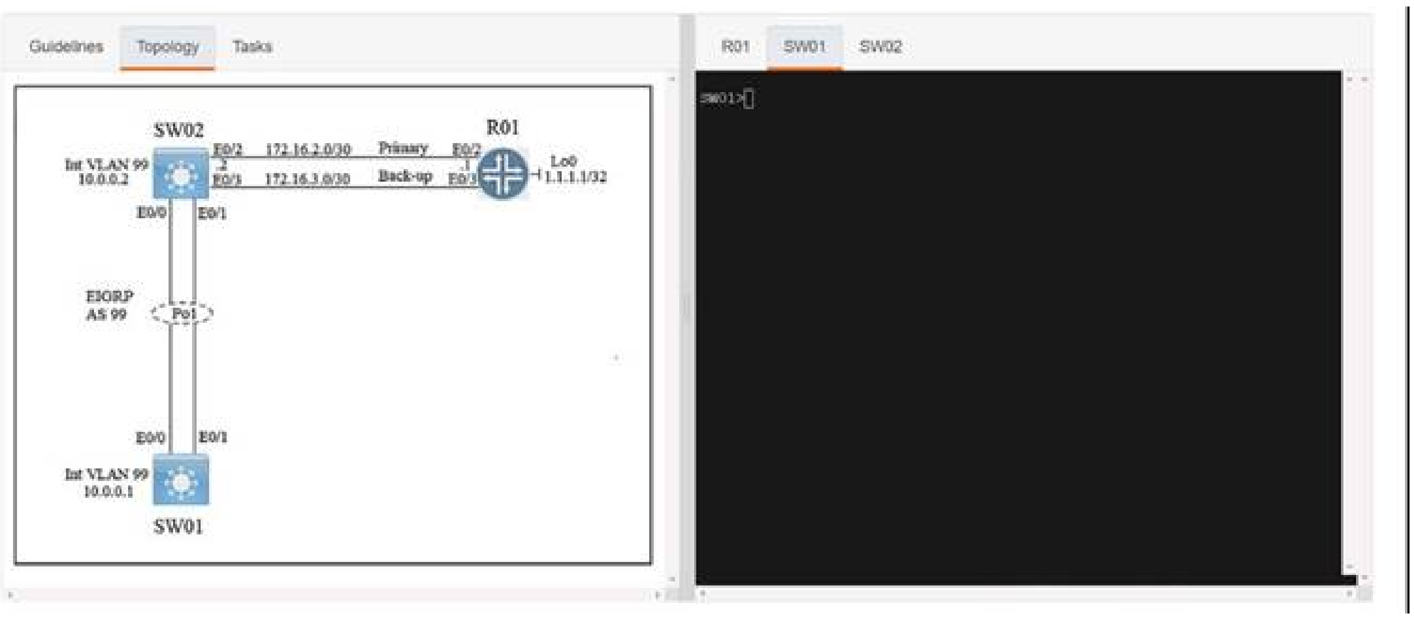
```
interface Ethernet0/0
ip address 10.1.1.3 255.255.255.0
ip nat inside

interface Serial0/0
ip address 209.165.201.30 255.255.255.224
ip nat outside

ip nat inside source static 10.1.1.2 209.165.201.2
ip nat inside source static 10.1.1.1 209.165.201.1

NAT# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.201.1 10.1.1.1 --- --
--- 209.165.201.2 10.1.1.2 --- ---
```

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

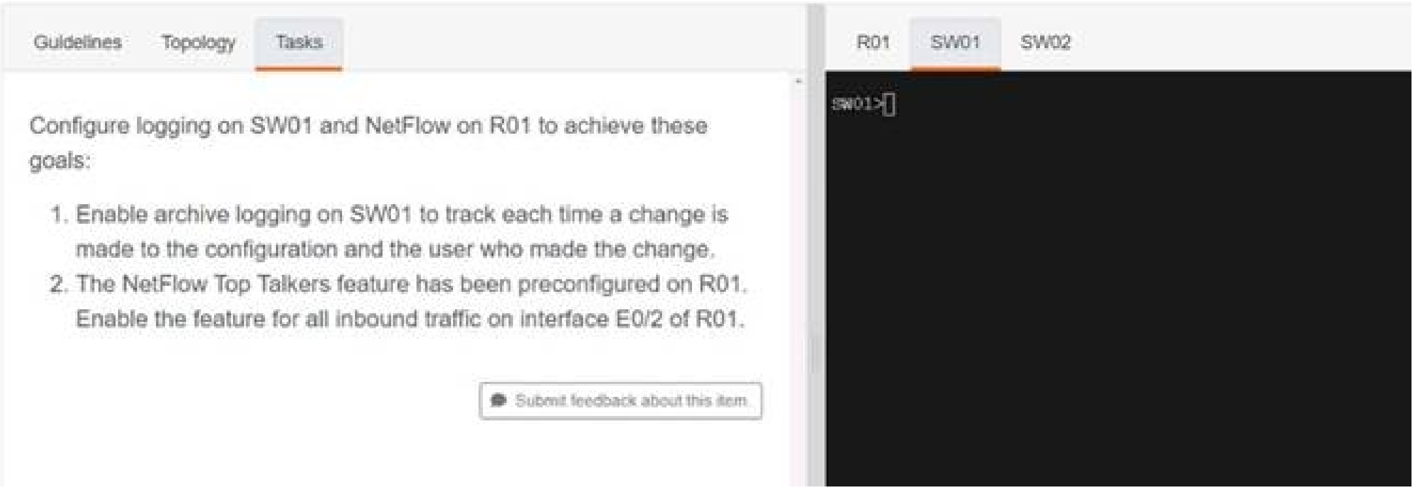
A. Packets with a destination of 200.1.1.1 are translated to 10.1.1.1 or .2. respectively.
B. A packet that is sent to 200.1.1.1 from 10.1.1.1 is translated to 209.165.201.1 on R1.
C. R1 looks at the destination IP address of packets entering S0/0 and destined for inside hosts.
D. R1 processes packets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

Answer: BC

NEW QUESTION 2
SIMULATION - (Topic 4)
Simulation 07



```
SW01>
```



Configure logging on SW01 and NetFlow on R01 to achieve these goals:

1. Enable archive logging on SW01 to track each time a change is made to the configuration and the user who made the change.
2. The NetFlow Top Talkers feature has been preconfigured on R01. Enable the feature for all inbound traffic on interface E0/2 of R01.

```
SW01>
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Sw1 Config t Archive Log config
Logging enable Notify syslog
R1
Config t
Ip flow-top-talkers
Match source address 172.16.2.1/30 Int et0/2
Ip flow ingress Copy run start

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

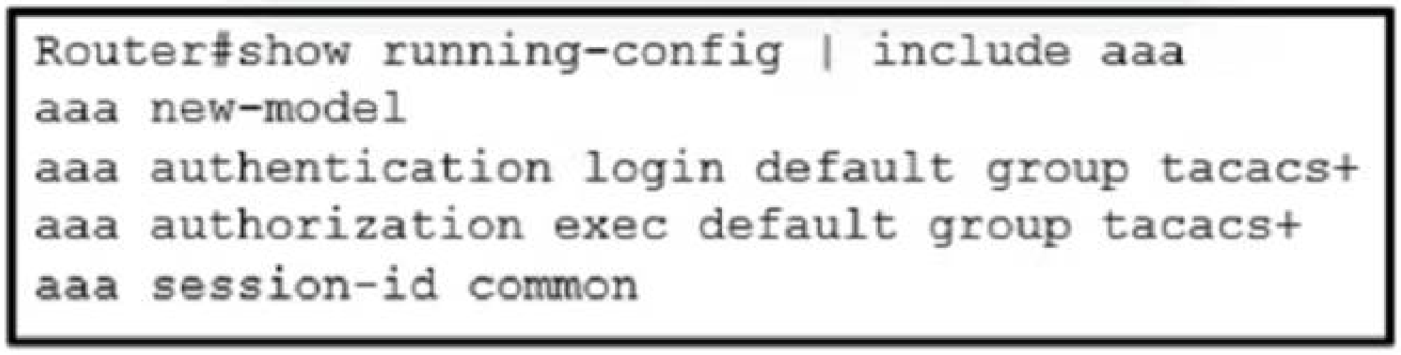
Answer: C

NEW QUESTION 6
- (Topic 4)
Which activity requires access to Cisco DNA Center CLI?

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

Answer: D

NEW QUESTION 7
- (Topic 4)
Refer to the exhibit.



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

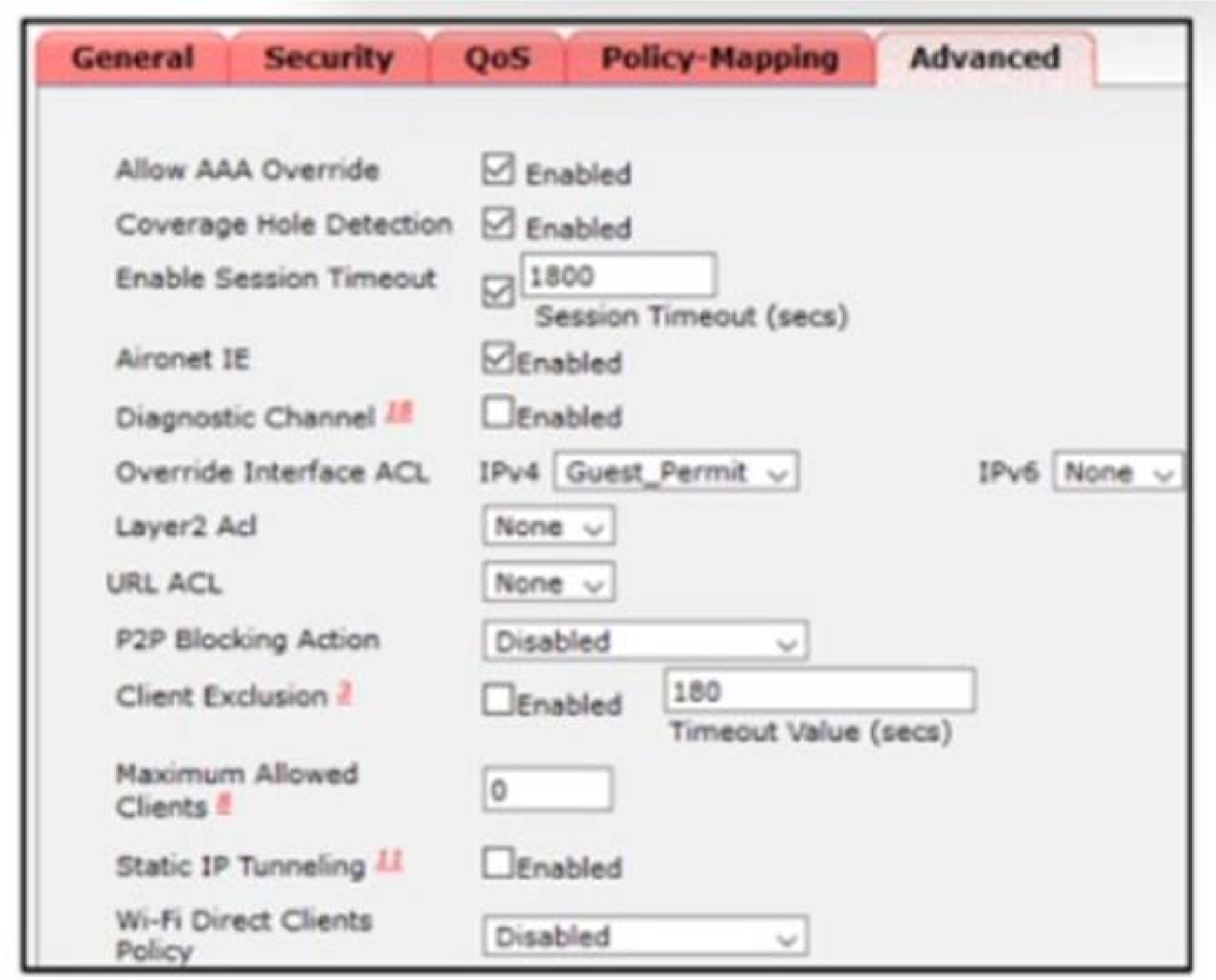
Which configuration enables fallback to local authentication and authorization when no TACACS+ server is available?

A. Router(config)# aaa authentication login default local Router(config)# aaa authorization exec default local
B. Router(config)# aaa authentication login default group tacacs+ local Router(config)# aaa authorization exec default group tacacs+ local

C. Router(config)# aaa fallback local
D. Router(config)# aaa authentication login FALLBACK local Router(config)# aaa authorization exec FALLBACK local

Answer: B

NEW QUESTION 8
- (Topic 4)
Refer to the exhibit.



Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑Enabled
Diagnostic Channel 18 □Enabled
Override Interface ACL IPv4 Guest_Permit IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion 2 □Enabled 180 Timeout Value (secs)
Maximum Allowed Clients 8 0
Static IP Tunneling 11 □Enabled
Wi-Fi Direct Clients Policy Disabled

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

A. Enable Client Exclusions.
B. Disable Aironet IE
C. Enable Wi-Fi Direct Client Policy
D. Enable P2P Blocking.

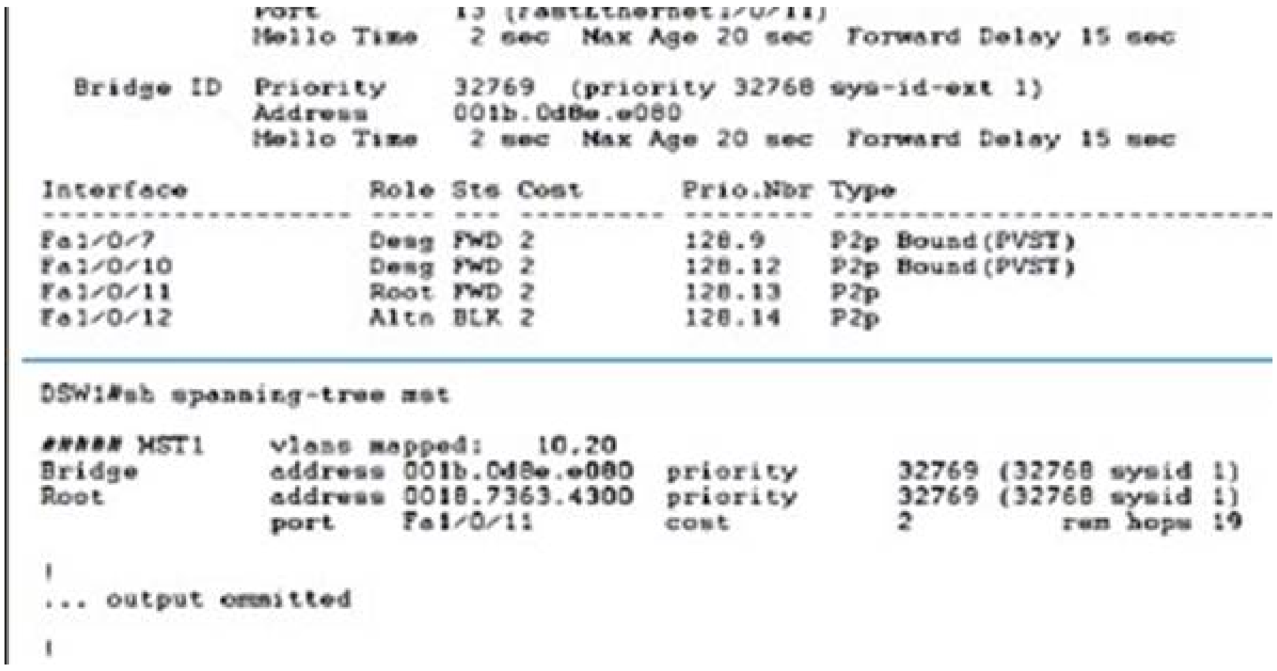
Answer: D

NEW QUESTION 9
- (Topic 4)
Which tunnel type al'ows clients to perform a seamless Layer 3 roam between a Cisco AireOS WLC and a Cisco IOS XE WLC?

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

Answer: A

NEW QUESTION 10
- (Topic 4)
Refer to the exhibit.



```
             Port        13 (FastEthernet1/0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     001b.0d8e.e080
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

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

DSW1#sh spanning-tree mst

##### MST1     vlans mapped:   10,20
Bridge         address 001b.0d8e.e080  priority      32769 (32768 sysid 1)
Root           address 0018.7363.4300  priority      32769 (32768 sysid 1)
               port    Fa1/0/11        cost          2          rem hops 19

!
... output ommitted

!
```

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

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

Answer: DE

NEW QUESTION 10
- (Topic 4)
A customer requires their wireless network to be fully functional, even if the wireless controller fails. Which wireless design supports these requirements?

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

Answer: A

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

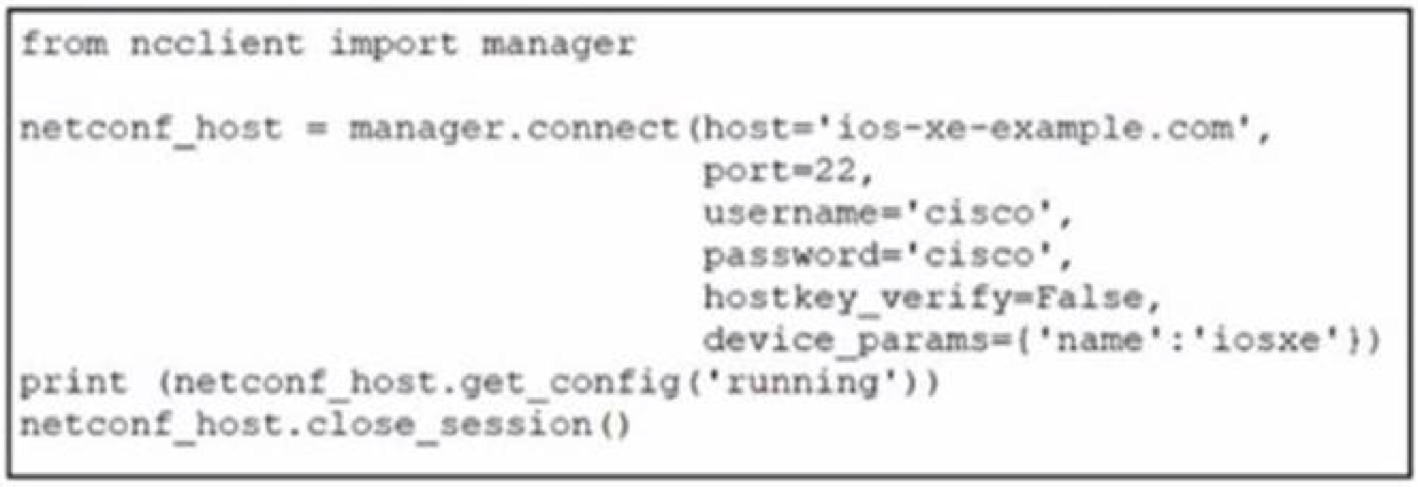
NEW QUESTION 13
- (Topic 4)
An engineer must protect the password for the VTY lines against over-the-shoulder attacks. Which configuration should be applied?

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 18
- (Topic 4)
Refer to the exhibit.



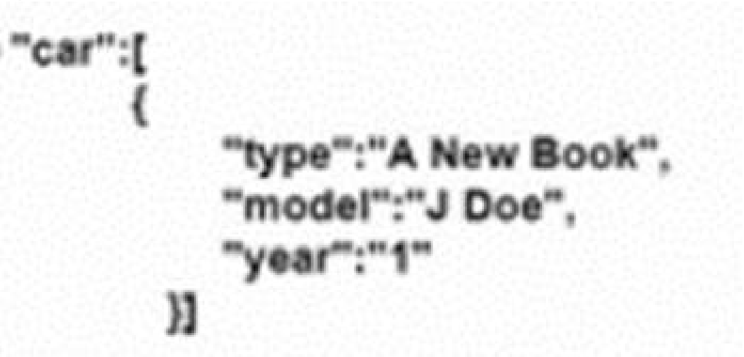
```
from ncclient import manager

netconf_host = manager.connect(host='ios-xe-example.com',
                               port=22,
                               username='cisco',
                               password='cisco',
                               hostkey_verify=False,
                               device_params={'name':'iosxe'})
print (netconf_host.get_config('running'))
netconf_host.close_session()
```

An engineer deploys a script to retrieve the running configuration from a NETCONF- capable Cisco IOS XE device that is configured with default settings. The script fails. Which configuration must be applied to retrieve the configurauon using NETCONF?

A. Print (netconf_host.get_config('show running'!)
B. hostkey_verify=True,
C. device_params={name':'ios-xe'})
D. port=830

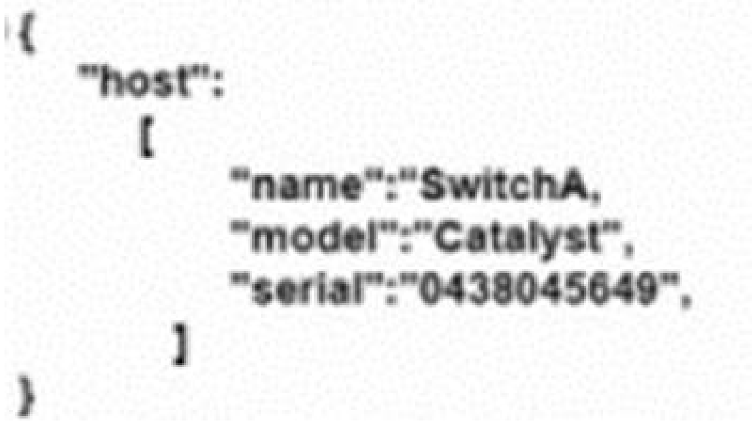
Answer: A

NEW QUESTION 19
- (Topic 4)
Which JSON script is properly formatted?
A)



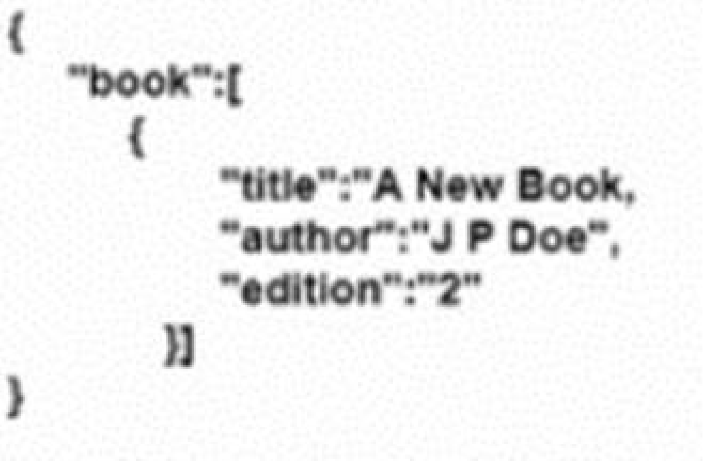
```
"car":[
      {
          "type":"A New Book",
          "model":"J Doe",
          "year":"1"
      }]
```

B)



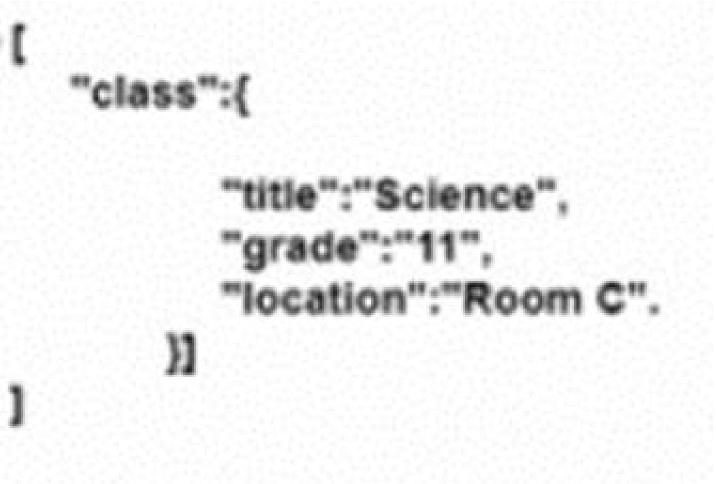
```
{
   "host":
      [
          "name":"SwitchA,
          "model":"Catalyst",
          "serial":"0438045649",
      ]
}
```

C)



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

D)

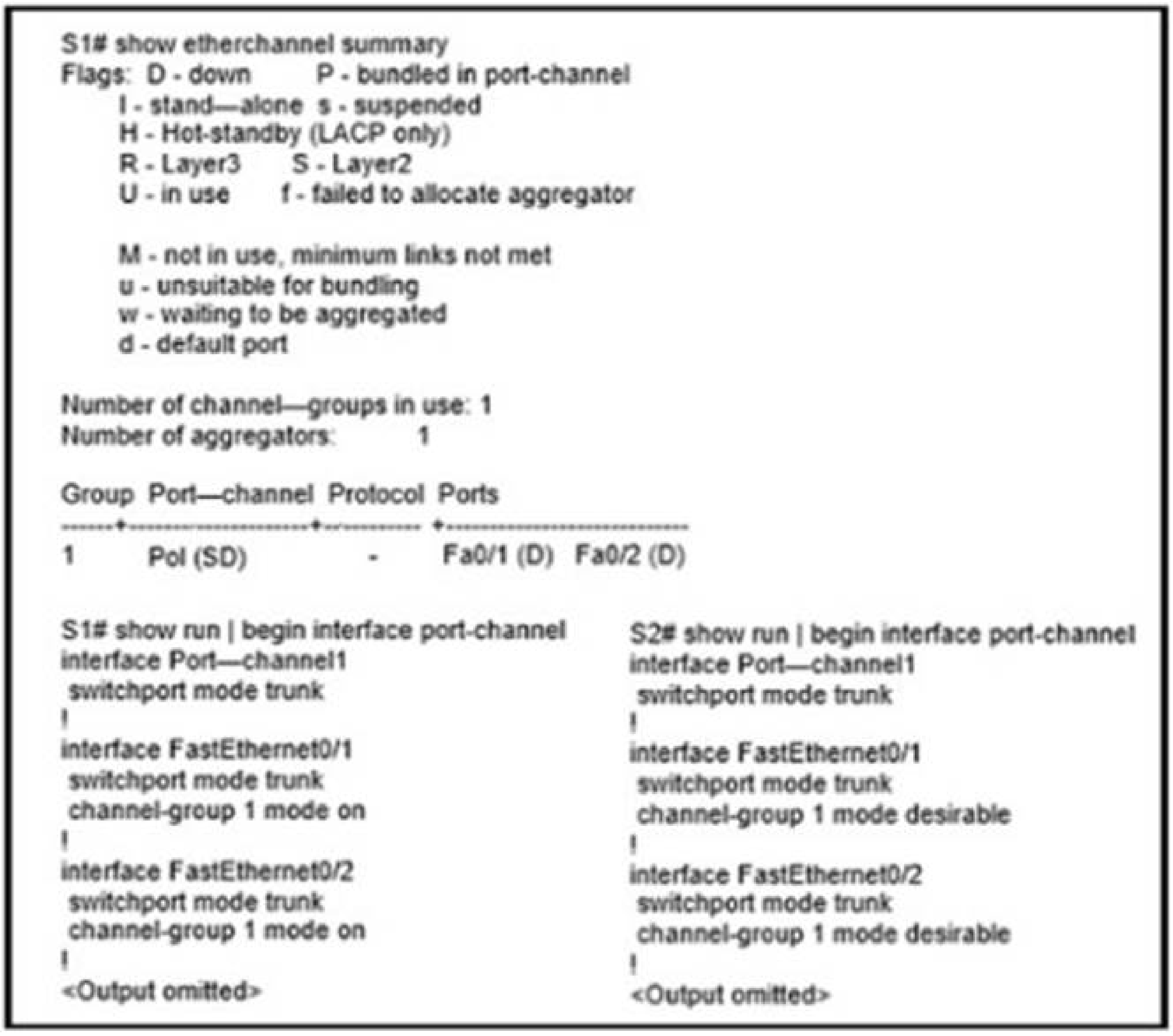


```
[
   "class":{

          "title":"Science",
          "grade":"11",
          "location":"Room C".
      }]
]
```

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

Answer: B

NEW QUESTION 21
- (Topic 4)



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

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

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

Group  Port—channel  Protocol  Ports
------+-------------+--------- +-------------------------
1      Pol (SD)          -      Fa0/1 (D)  Fa0/2 (D)
```

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

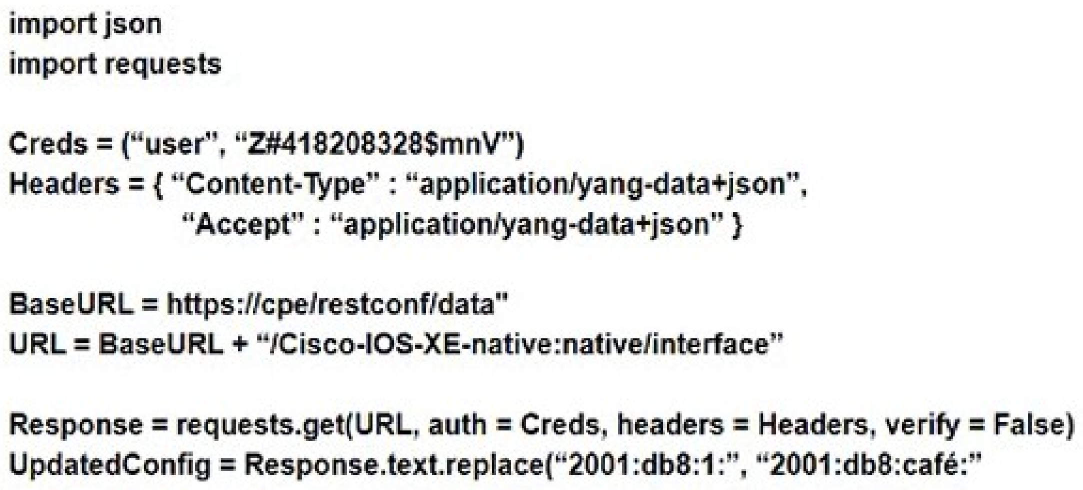
```
S2# show run | begin interface port-channel
interface Port—channel1
 switchport mode trunk
!
interface FastEthernet0/1
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 1 mode desirable
!
<Output omitted>
```

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

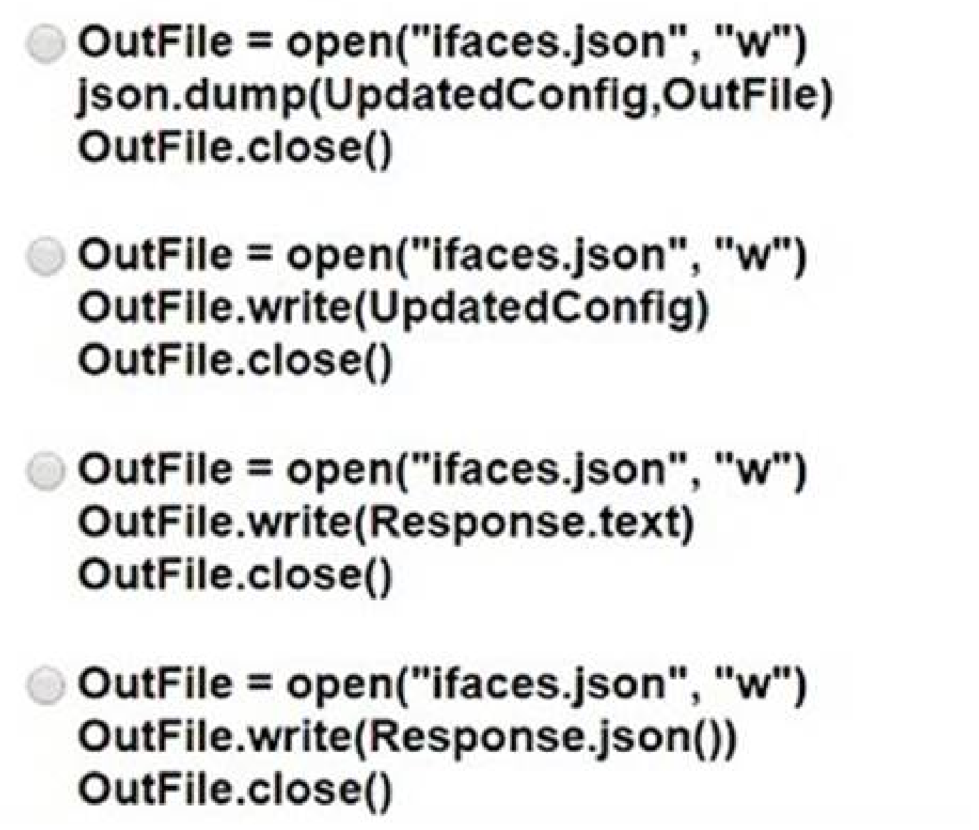
A. Configure LACP mode on S1 to passive.
B. Configure switch port mode to ISL on S2.
C. Configure PAgP mode on S1 to desirable.
D. Configure LACP mode on S1 to active.

Answer: C

NEW QUESTION 25
- (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

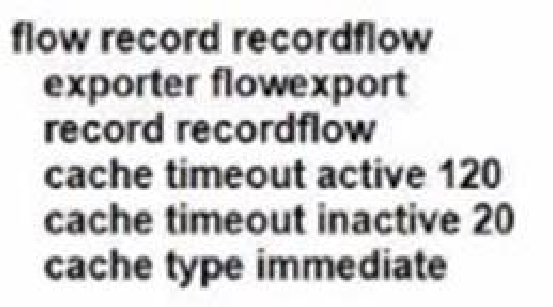
Answer: B

NEW QUESTION 30
- (Topic 4)
What is a characteristic of para-virtualization?

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

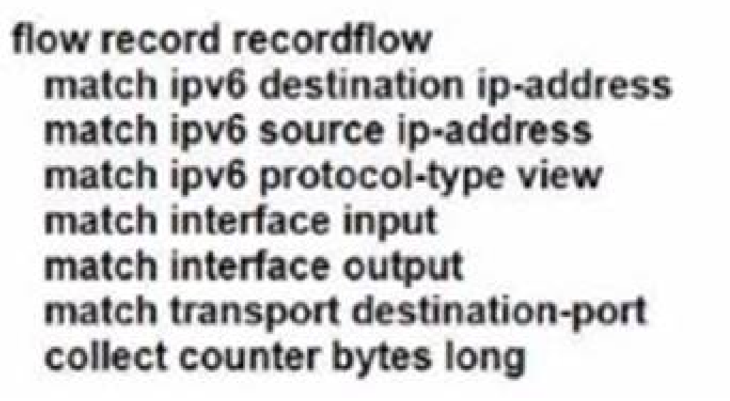
Answer: A

NEW QUESTION 35
- (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)



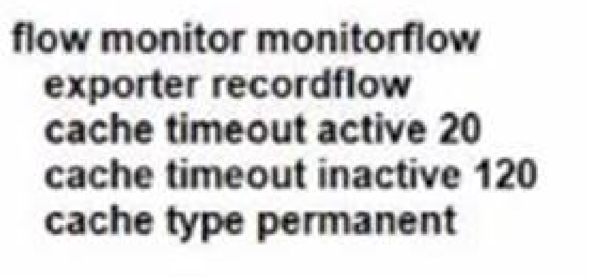
```
flow record recordflow
  exporter flowexport
  record recordflow
  cache timeout active 120
  cache timeout inactive 20
  cache type immediate
```

B)



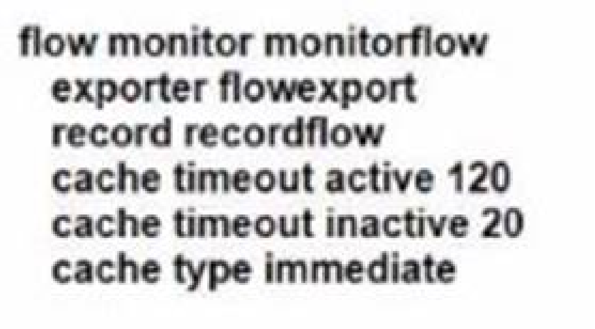
```
flow record recordflow
  match ipv6 destination ip-address
  match ipv6 source ip-address
  match ipv6 protocol-type view
  match interface input
  match interface output
  match transport destination-port
  collect counter bytes long
```

C)



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

D)



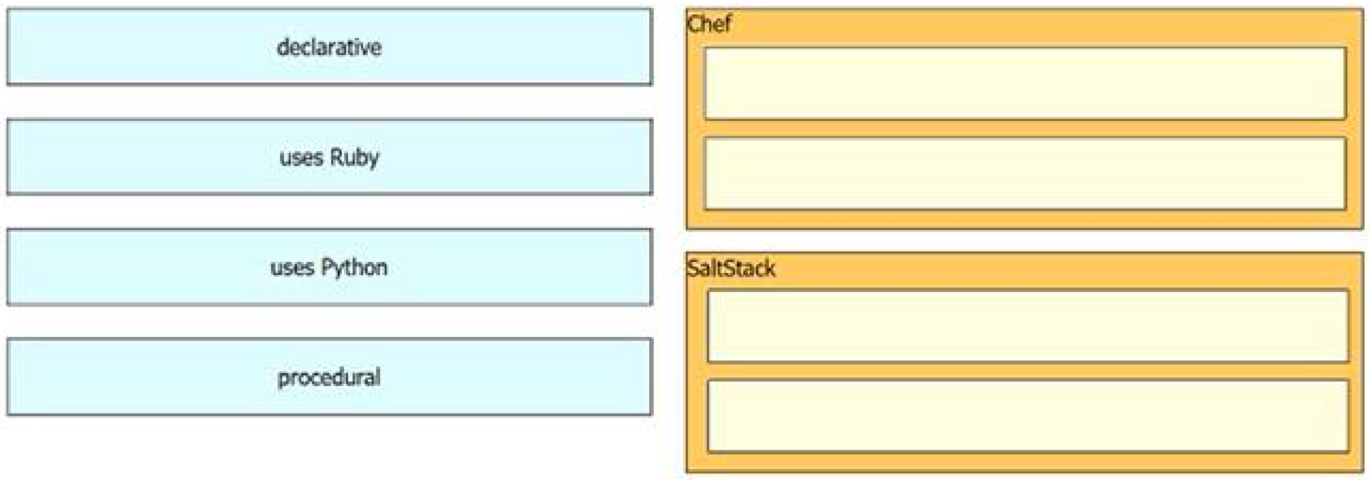
```
flow monitor monitorflow
  exporter flowexport
  record recordflow
  cache timeout active 120
  cache timeout inactive 20
  cache type immediate
```

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

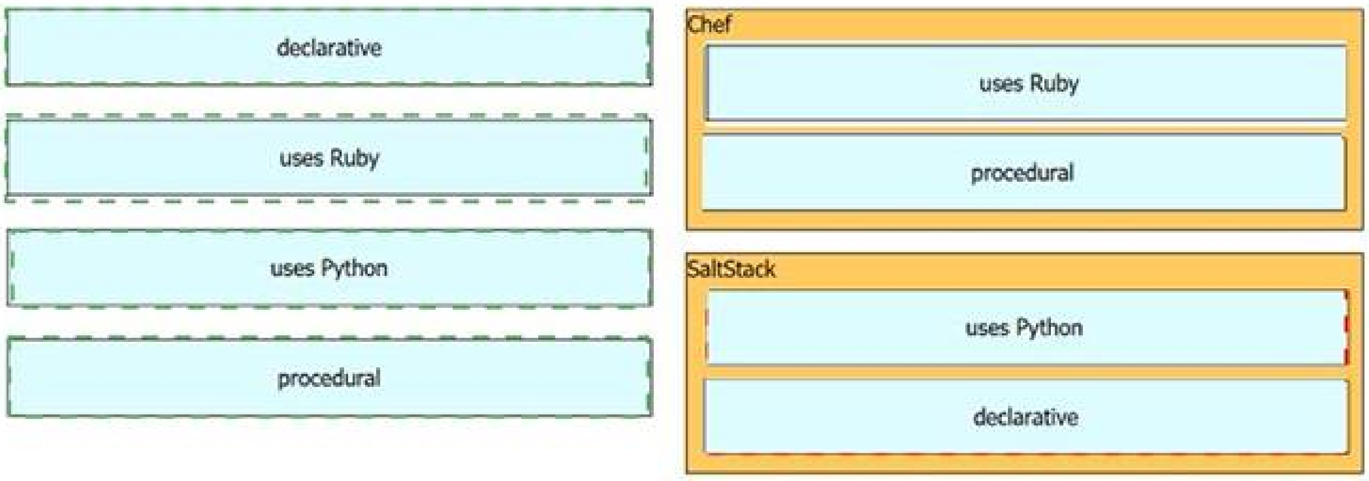
NEW QUESTION 36
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



declarative

uses Ruby

uses Python

procedural

Chef

uses Ruby

procedural

SaltStack

uses Python

declarative

NEW QUESTION 39
- (Topic 4)
An engineer is connected to a Cisco router through a Telnet session. Which command must be issued to view the logging messages from the current session as soon as they are generated by the router?

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

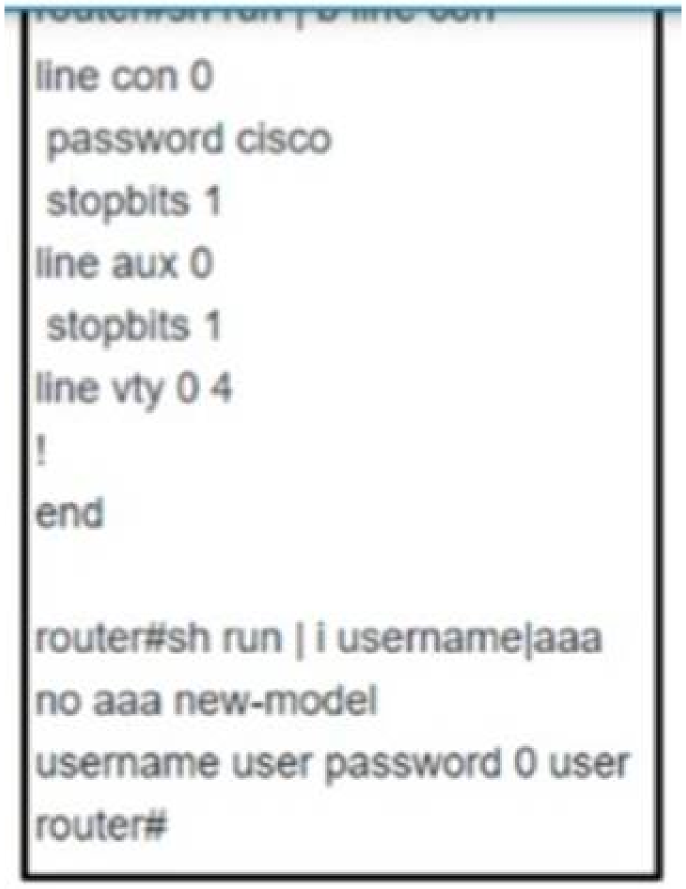
Answer: D

NEW QUESTION 44
- (Topic 4)
How is a data modelling language used?

A. To enable data to 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

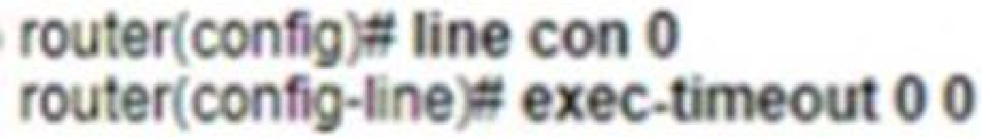
Answer: A

NEW QUESTION 46
- (Topic 4)



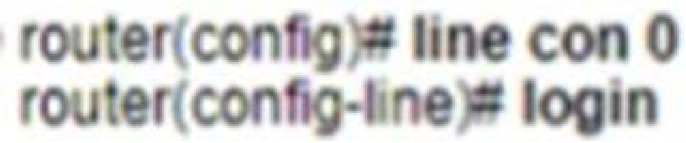
```
router#sh run | b line con
line con 0
 password cisco
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
!
end

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

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



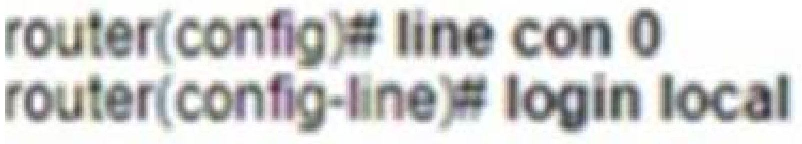
```
router(config)# line con 0
router(config-line)# exec-timeout 0 0
```

B)



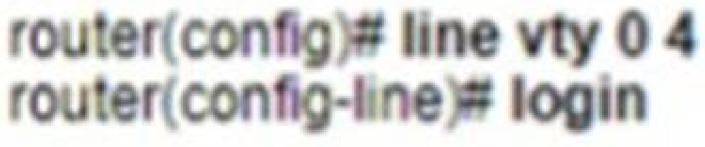
```
router(config)# line con 0
router(config-line)# login
```

C)



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

D)

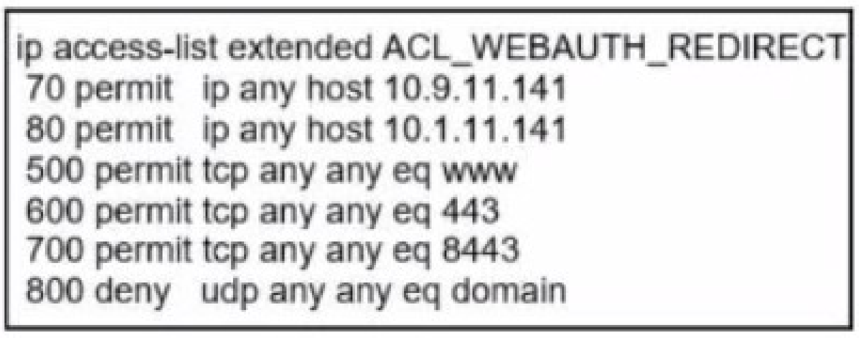


```
router(config)# line vty 0 4
router(config-line)# login
```

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

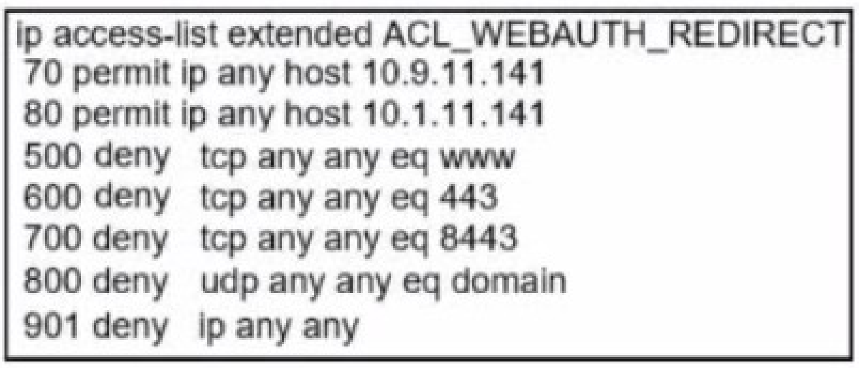
Answer: B

NEW QUESTION 49
- (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)



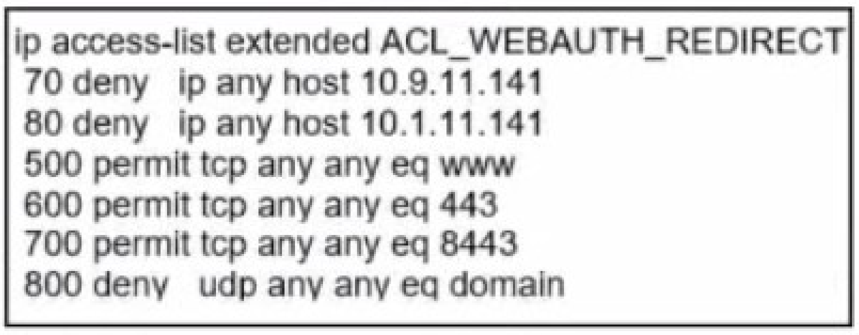
```
ip access-list extended ACL_WEBAUTH_REDIRECT
 70 permit   ip any host 10.9.11.141
 80 permit   ip any host 10.1.11.141
 500 permit tcp any any eq www
 600 permit tcp any any eq 443
 700 permit tcp any any eq 8443
 800 deny   udp any any eq domain
```

B)



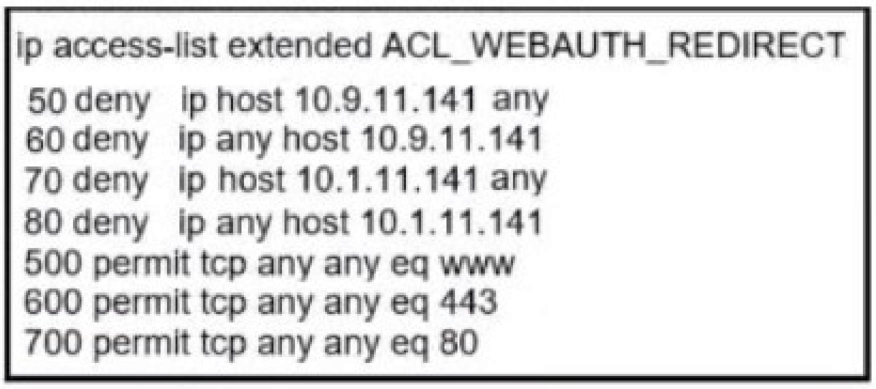
```
ip access-list extended ACL_WEBAUTH_REDIRECT
 70 permit ip any host 10.9.11.141
 80 permit ip any host 10.1.11.141
 500 deny   tcp any any eq www
 600 deny   tcp any any eq 443
 700 deny   tcp any any eq 8443
 800 deny   udp any any eq domain
 901 deny   ip any any
```

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)



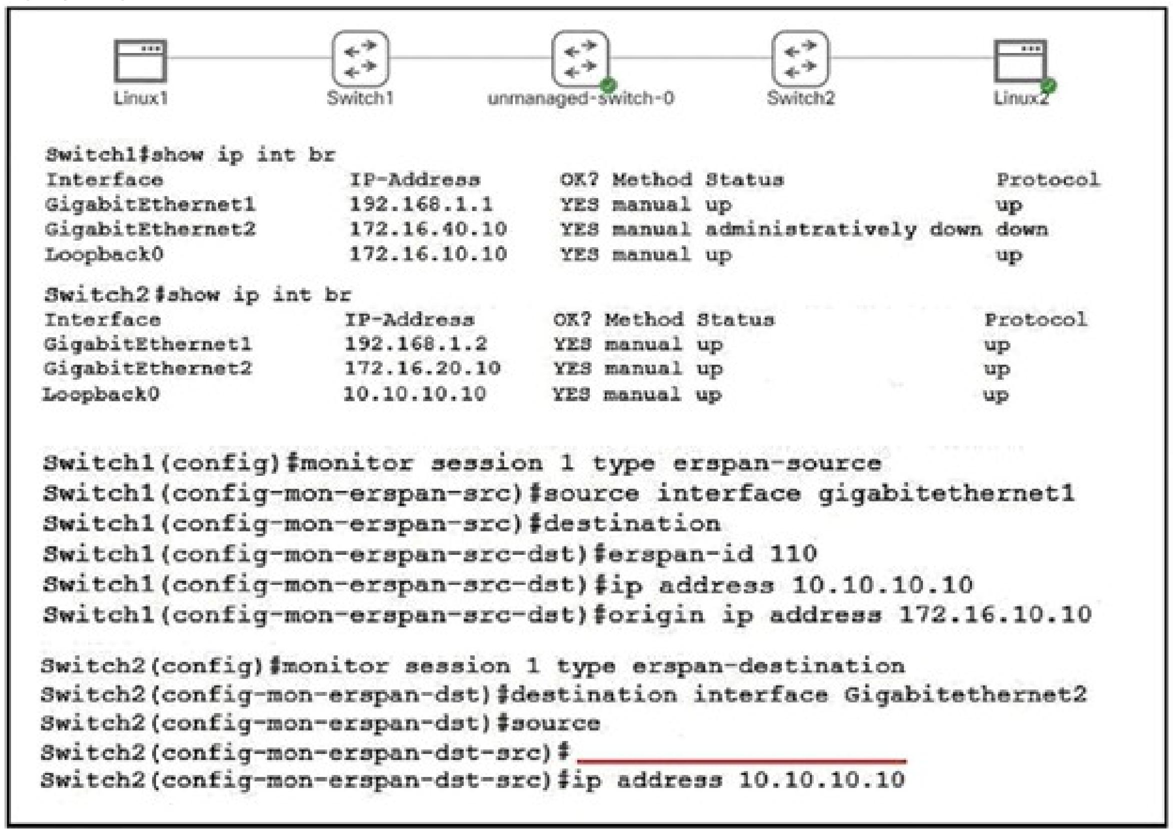
```
ip access-list extended ACL_WEBAUTH_REDIRECT
 50 deny   ip host 10.9.11.141 any
 60 deny   ip any host 10.9.11.141
 70 deny   ip host 10.1.11.141 any
 80 deny   ip any host 10.1.11.141
 500 permit tcp any any eq www
 600 permit tcp any any eq 443
 700 permit tcp any any eq 80
```

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 53
- (Topic 4)



```
Switch1#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.1.1     YES manual up                    up
GigabitEthernet2       172.16.40.10    YES manual administratively down down
Loopback0              172.16.10.10    YES manual up                    up

Switch2#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.1.2     YES manual up                    up
GigabitEthernet2       172.16.20.10    YES manual up                    up
Loopback0              10.10.10.10     YES manual up                    up

Switch1(config)#monitor session 1 type erspan-source
Switch1(config-mon-erspan-src)#source interface gigabitethernet1
Switch1(config-mon-erspan-src)#destination
Switch1(config-mon-erspan-src-dst)#erspan-id 110
Switch1(config-mon-erspan-src-dst)#ip address 10.10.10.10
Switch1(config-mon-erspan-src-dst)#origin ip address 172.16.10.10

Switch2(config)#monitor session 1 type erspan-destination
Switch2(config-mon-erspan-dst)#destination interface Gigabitethernet2
Switch2(config-mon-erspan-dst)#source
Switch2(config-mon-erspan-dst-src)# ______________________
Switch2(config-mon-erspan-dst-src)#ip address 10.10.10.10
```

Refer to the exhibit. An engineer must configure an ERSPAN tunnel that mirrors traffic from linux1 on Switch1 to Linux2 on Switch2. Which command must be added to the destination configuration to enable the ERSPAN tunnel?

A. (config-mon-erspan-dst-src)# origin ip address 172.16.10.10
B. (config-mon-erspan-dst-src)# erspan-id 172.16.10.10
C. (config-mon-erspan-dst-src)# no shut
D. (config-mon-erspan-dst-src)# erspan-id 110

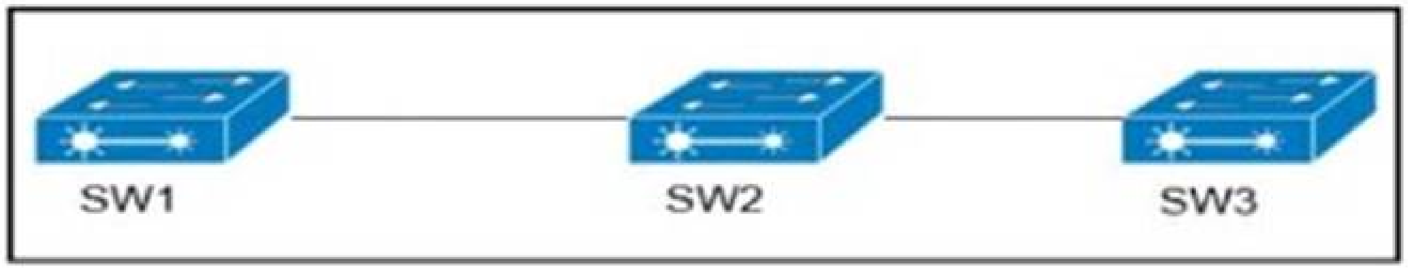
Answer: D

NEW QUESTION 58
- (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 63
- (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

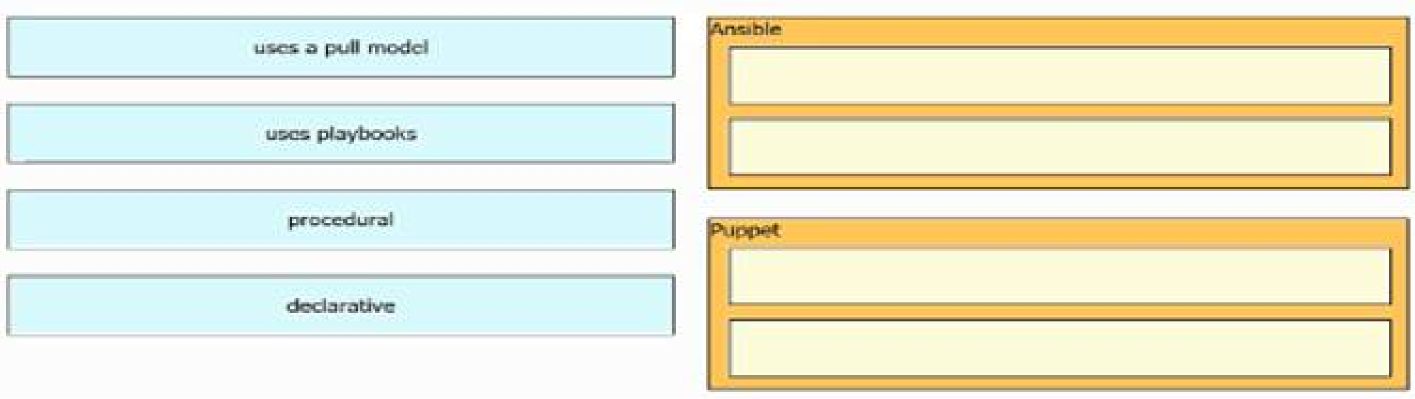
Explanation:
SW3 does not have VLAN 60 so it should not receive traffic for this VLAN (sent from SW2). Therefore we should configure VTP Pruning on SW3 so that SW2 does not forward VLAN 60 traffic to SW3. Also notice that we need to configure pruning on SW1 (the VTP Server), not SW2.

NEW QUESTION 64
- (Topic 1)
What is the function of a VTEP in VXLAN?

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

Answer: C

NEW QUESTION 68
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.



uses a pull model
uses playbooks
procedural
declarative

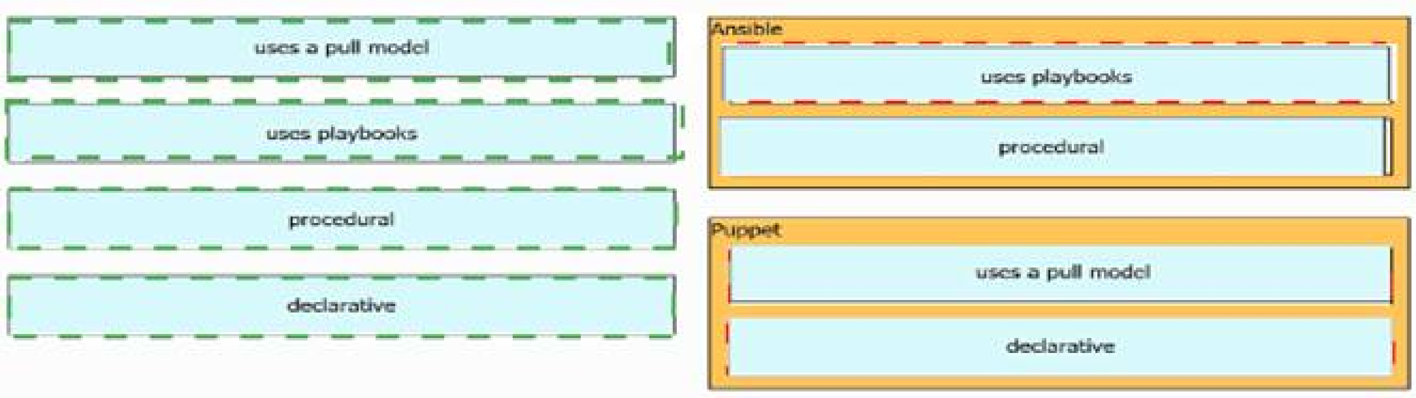
Ansible

Puppet

A. Mastered
B. Not Mastered

Answer: A

Explanation:



uses a pull model
uses playbooks
procedural
declarative

Ansible
uses playbooks
procedural

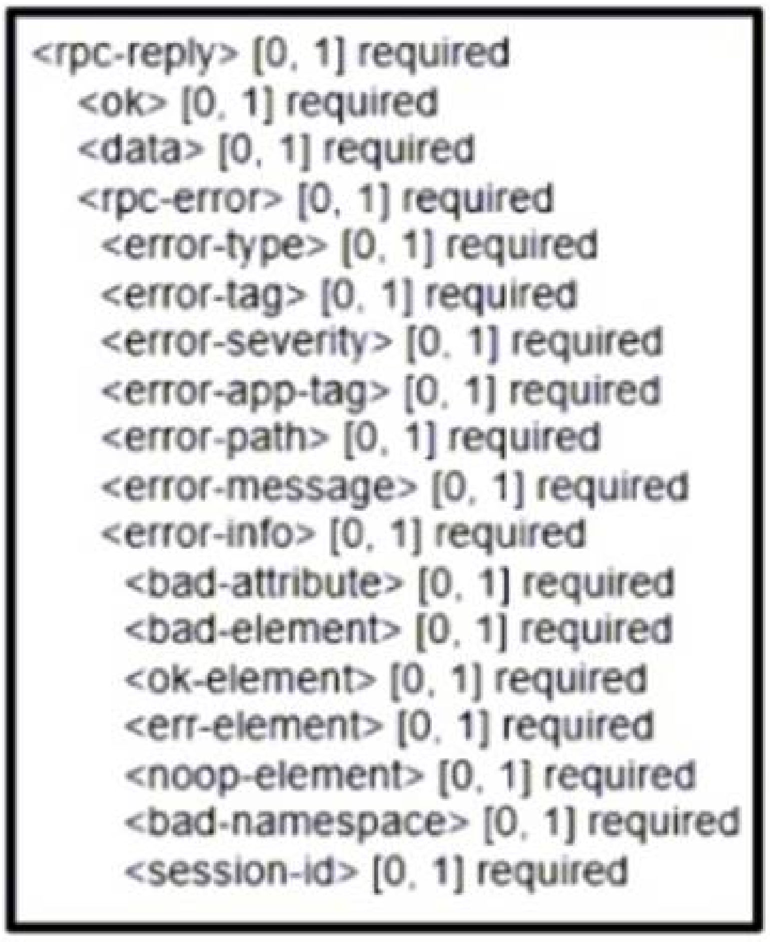
Puppet
uses a pull model
declarative

NEW QUESTION 73
- (Topic 2)
Why is an AP joining a different WLC than the one specified through option 43?

A. The WLC is running a different software version.
B. The API is joining a primed WLC
C. The AP multicast traffic unable to reach the WLC through Layer 3.
D. The APs broadcast traffic is unable to reach the WLC through Layer 2.

Answer: B

NEW QUESTION 74
- (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 75
- (Topic 2)
How can an engineer prevent basic replay attacks from people who try to brute force a system via REST API?

A. Add a timestamp to the request In the API header.
B. Use a password hash
C. Add OAuth to the request in the API header.
D. UseHTTPS

Answer: B

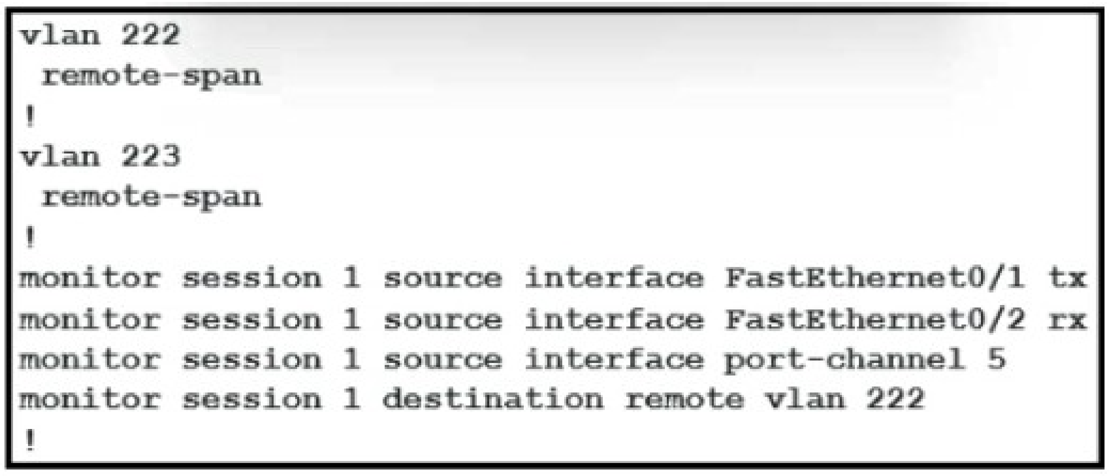
NEW QUESTION 76
- (Topic 2)
Which access point mode allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues?

A. client mode
B. SE-connect mode
C. sensor mode
D. sniffer mode

Answer: C

Explanation:
As these wireless networks grow especially in remote facilities where IT professionals may not always be onsite, it becomes even more important to be able to quickly identify and resolve potential connectivity issuesideally before the users complain or notice connectivity degradation. To address these issues we have created Cisco’s Wireless Service Assurance and a new AP mode called “sensor”mode. Cisco’s Wireless Service Assurance platform has three components, namely, Wireless PerformanceAnalytics, Real-time Client Troubleshooting, and Proactive Health Assessment. Using a supported AP ordedicated sensor the device can actually function much like a WLAN client would associating andidentifying client connectivity issues within the network in real time without requiring an IT or technician to beon site.
Reference:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-5/b_Cisco_Aironet_Sensor_Deployment_Guide.html.xml

NEW QUESTION 79
- (Topic 2)
Refer to the exhibit.



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

What is the result when a technician adds the monitor session 1 destination remote vlan 223 command1?

A. The RSPAN VLAN is replaced by VLAN 223.
B. RSPAN traffic is sent to VLANs 222 and 223
C. An error is flagged for configuring two destinations.
D. RSPAN traffic is split between VLANs 222 and 223.

Answer: A

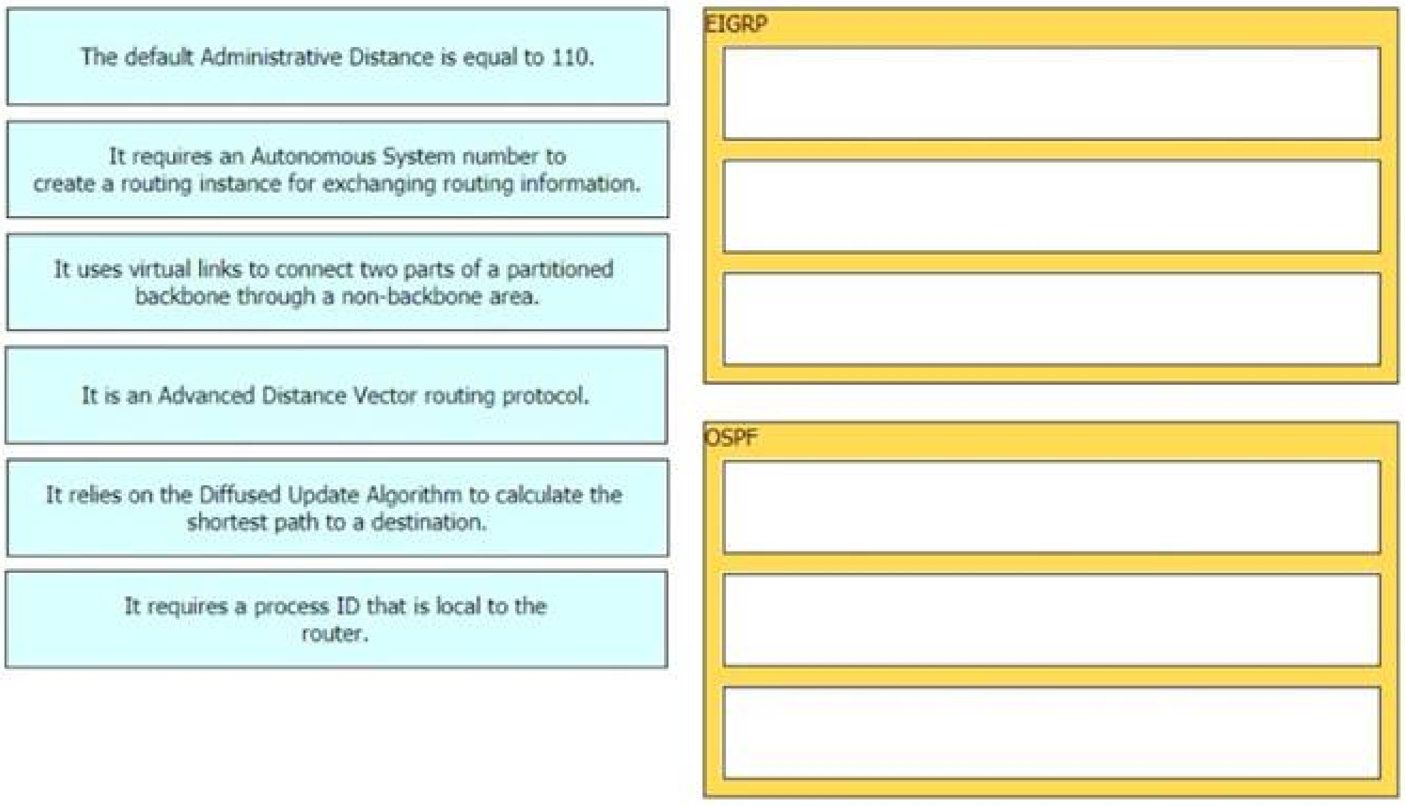
NEW QUESTION 82
- (Topic 2)
Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

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 87
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.

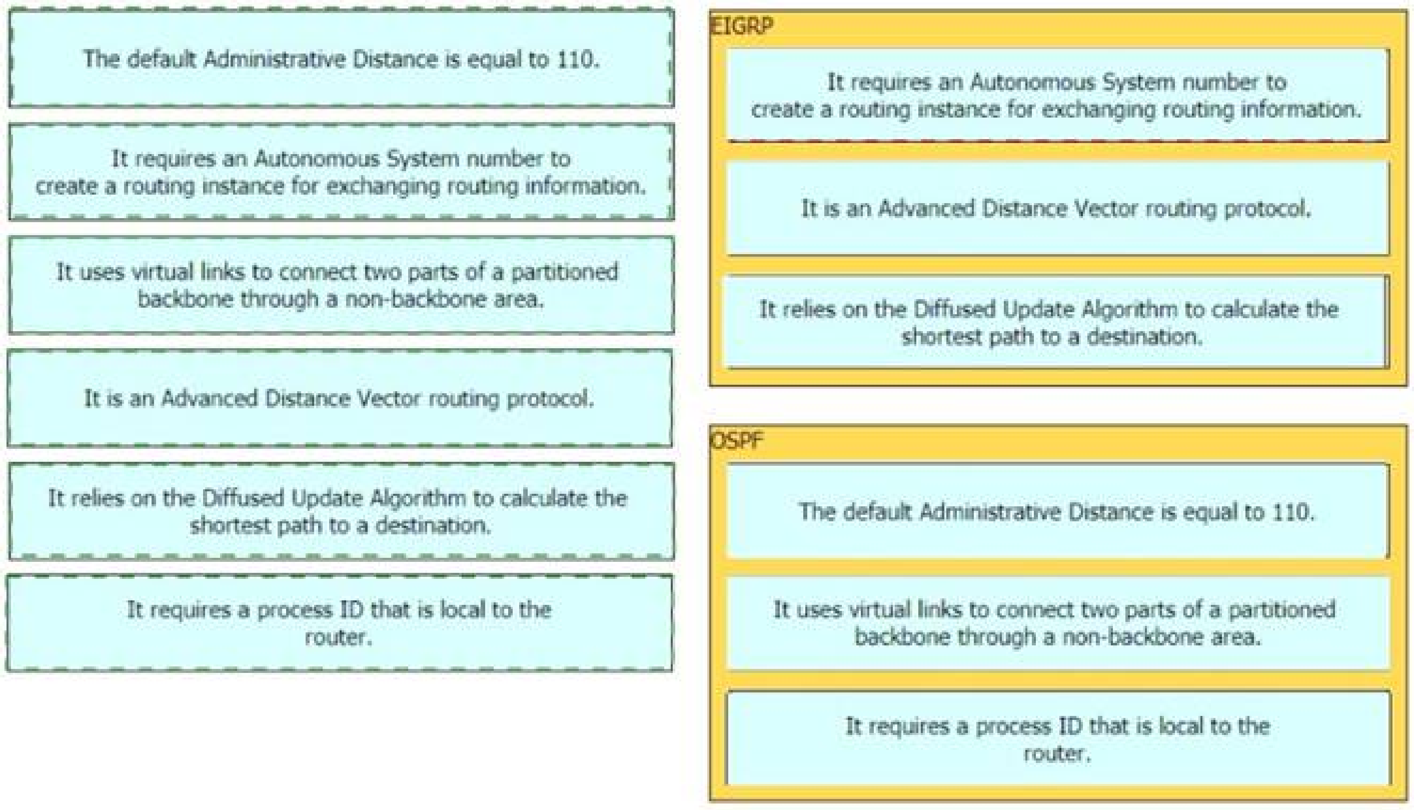
It relies on the Diffused Update Algorithm to calculate the shortest path to a destination.

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

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 89
- (Topic 2)
When is the Design workflow used In Cisco DNA Center?

A. in a greenfield deployment, with no existing infrastructure
B. in a greenfield or brownfield deployment, to wipe out existing data
C. in a brownfield deployment, to modify configuration of existing devices in the network
D. in a brownfield deployment, to provision and onboard new network devices

Answer: A

Explanation:
The Design area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Use the Design workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the Discovery feature.
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/user_guide/b_cisco_dna_center_ug_2_1_2/b_cisco_dna_center_ug_2_1_1_chapter_011 0.html
Reference: https://synoptek.com/insights/it-blogs/greenfield-vs-brownfield-software- development/“Greenfield development refers to developing a system for a totally new environment and requires development from a clean slate – no legacy code around. It is an approach used when you’re starting fresh and with no restrictions or dependencies.”

NEW QUESTION 92
- (Topic 2)
What is the difference between a RIB and a FIB?

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

Answer: D

Explanation:
CEF uses a Forwarding Information Base (FIB) to make IP destination prefix- based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with earlier switching paths such as fast switching and optimum switching.
Note: In order to view the Routing information base (RIB) table, use the “show ip route” command. To view the Forwarding Information Base (FIB), use the “show ip cef” command. RIB is in Control plane while FIB is in Data plane.

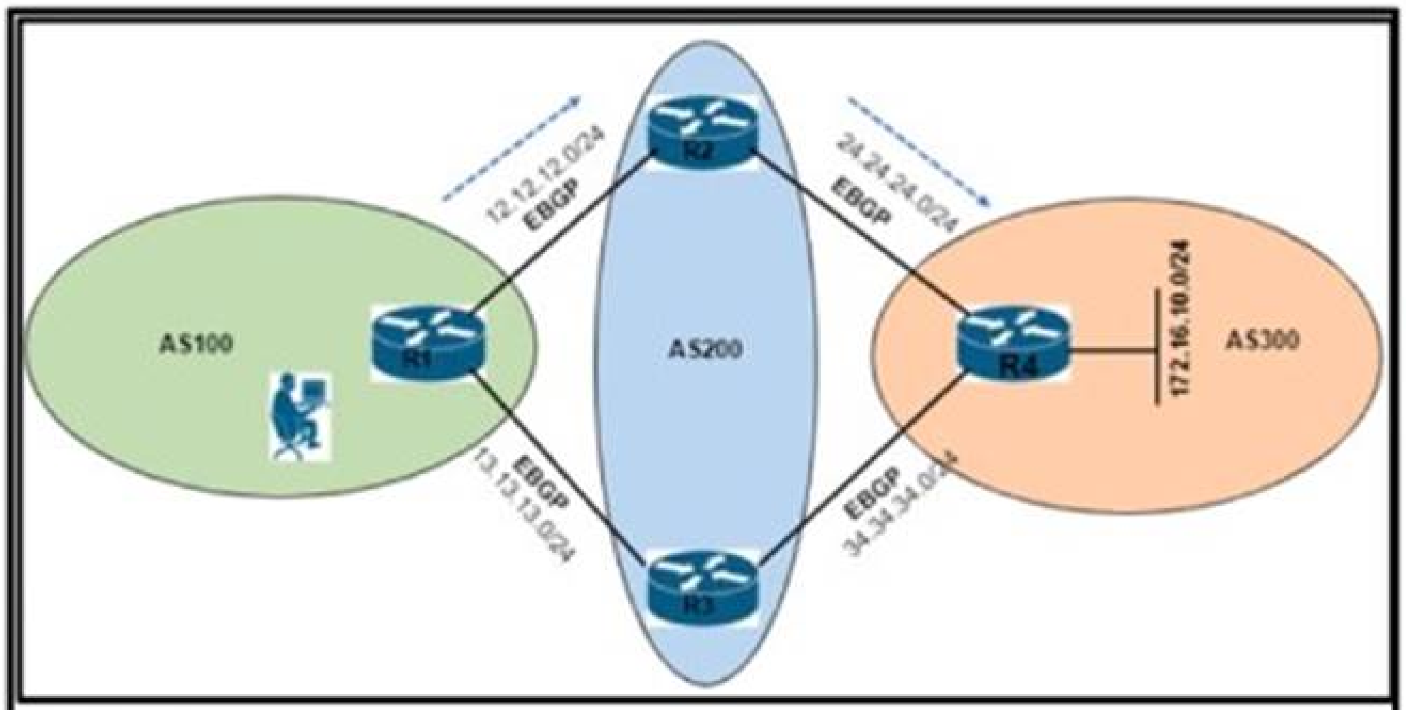
NEW QUESTION 97
- (Topic 2)
In a Cisco SD-WAN solution, how Is the health of a data plane tunnel monitored?

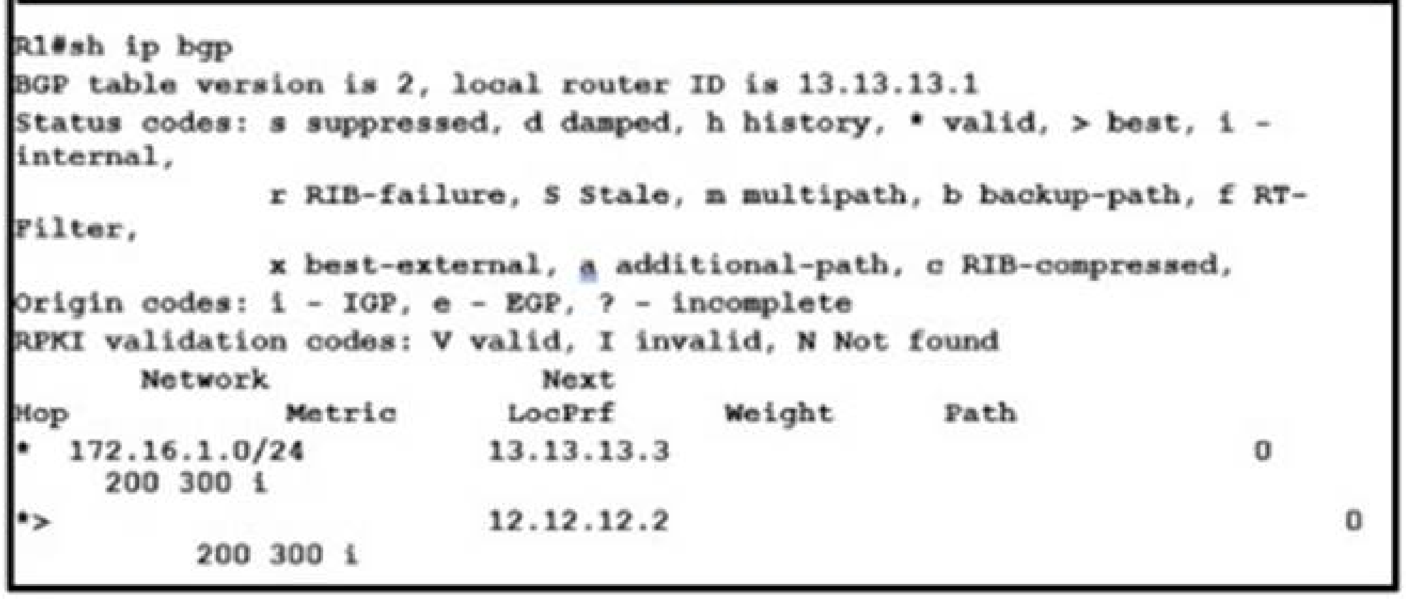
A. with IP SLA
B. ARP probing
C. using BFD
D. with OMP

Answer: C

NEW QUESTION 99

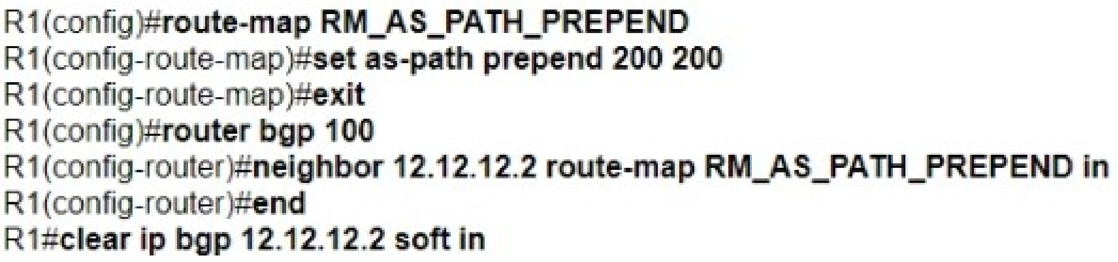
- (Topic 2)
Refer to the exhibit.





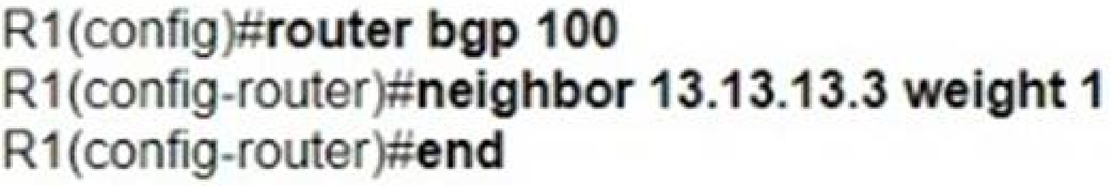
```
R1#sh ip bgp
BGP table version is 2, local router ID is 13.13.13.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin 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)



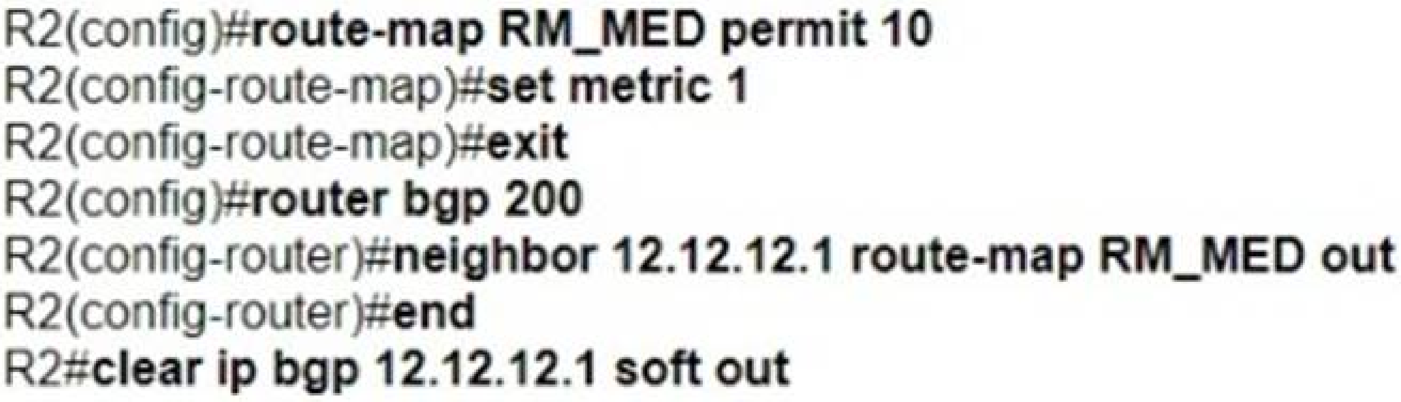
```
R1(config)#route-map RM_AS_PATH_PREPEND
R1(config-route-map)#set as-path prepend 200 200
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 12.12.12.2 route-map RM_AS_PATH_PREPEND in
R1(config-router)#end
R1#clear ip bgp 12.12.12.2 soft in
```

B)



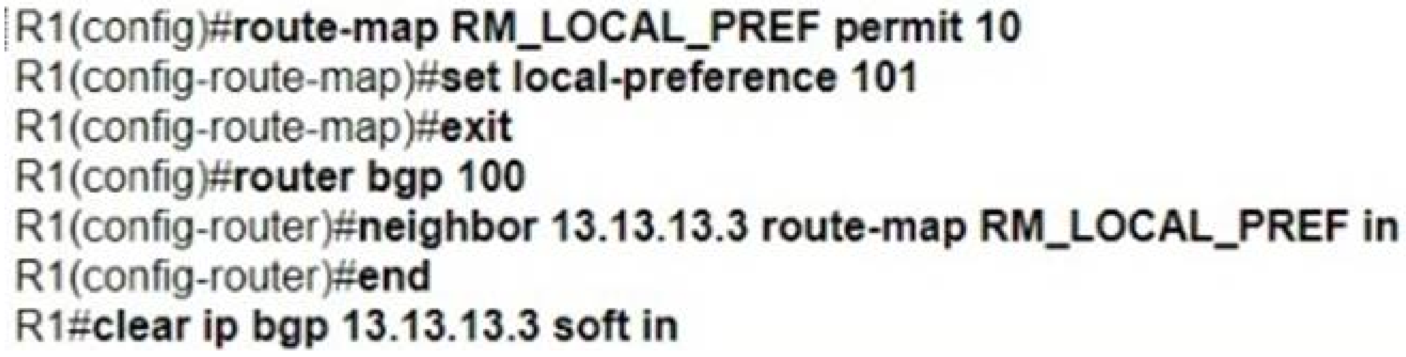
```
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 weight 1
R1(config-router)#end
```

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

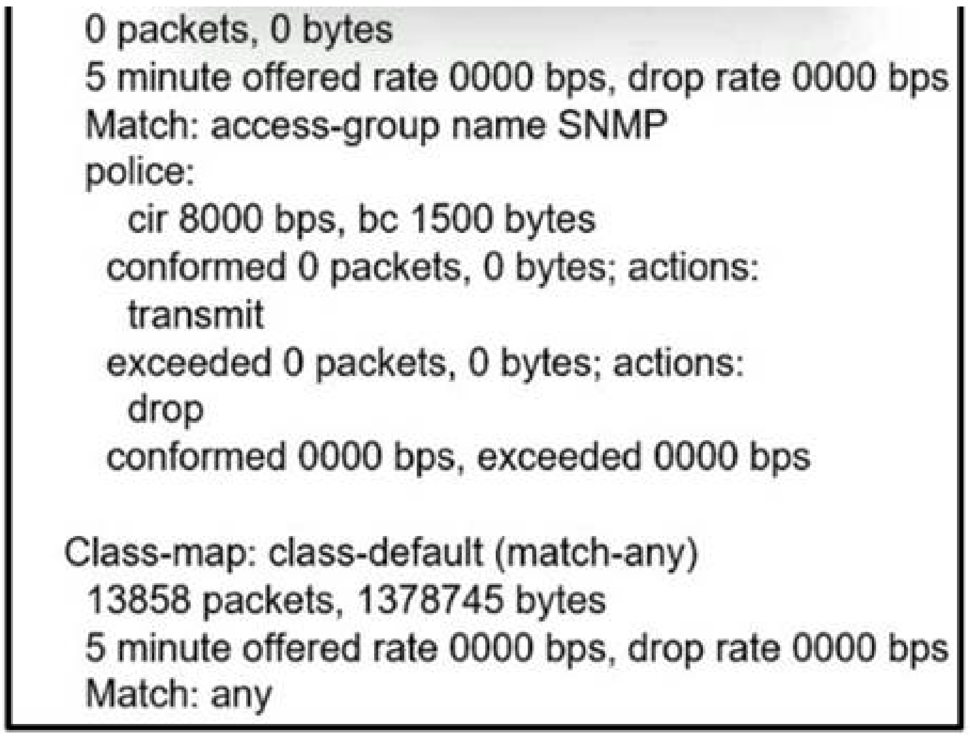
NEW QUESTION 101
- (Topic 2)
Which threat defence mechanism, when deployed at the network perimeter, protects against zero-day attacks?

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 102
- (Topic 2)
Refer to the exhibit.



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

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

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

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

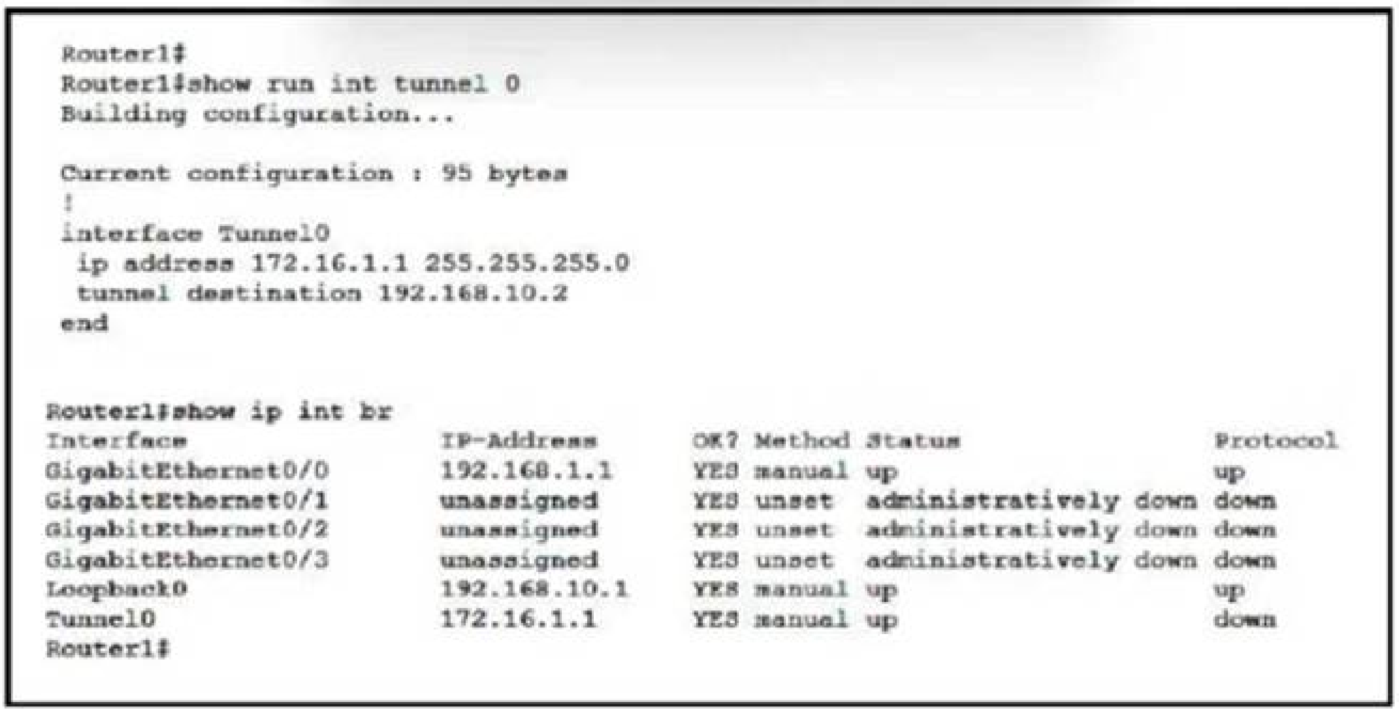
Answer: C

NEW QUESTION 106
- (Topic 2)
What is the function of a control-plane node In a Cisco SD-Access solution?

A. to run a mapping system that manages endpoint to network device relationships
B. to implement policies and communicate with networks outside the fabric
C. to connect external Layer 3 networks to the SD-Access fabric
D. to connect APs and wireless endpoints to the SD-Access fabric

Answer: A

NEW QUESTION 110
- (Topic 2)
Refer to the exhibit.



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

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


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

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

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

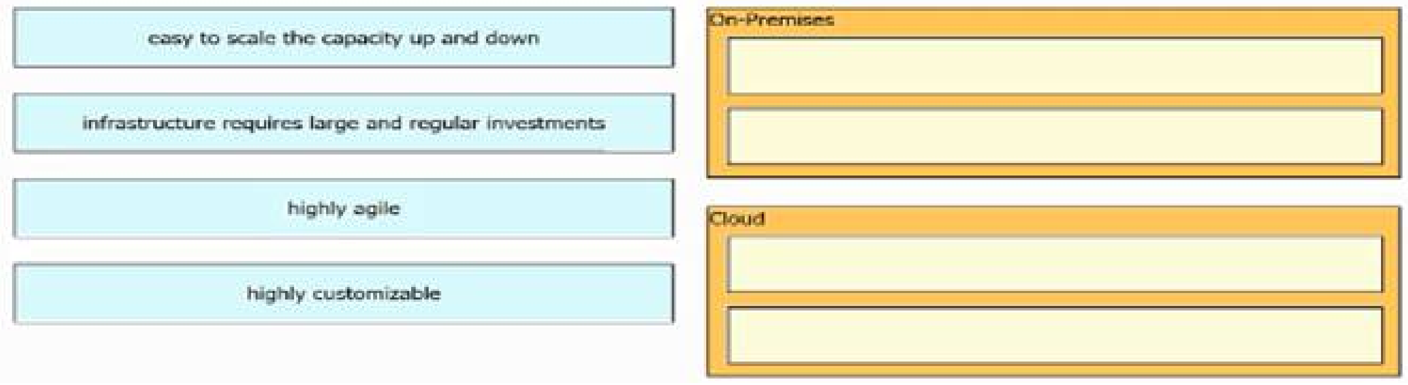
Answer: B

NEW QUESTION 114
- (Topic 2)
When firewall capabilities are considered, which feature is found only in Cisco next- generation firewalls?

A. malware protection
B. stateful inspection
C. traffic filtering
D. active/standby high availability

Answer: A

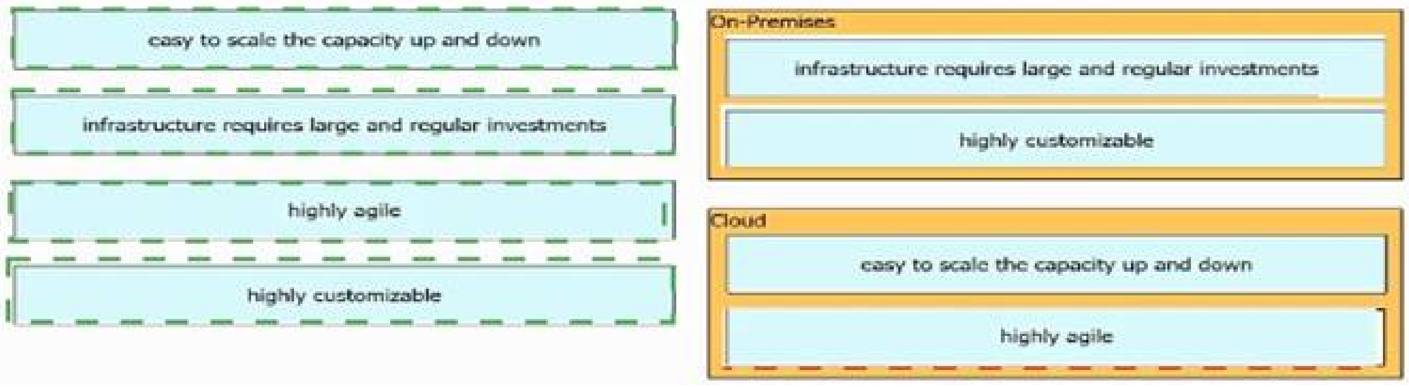
NEW QUESTION 117
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the infrastructure deployment models they describe on the right.


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

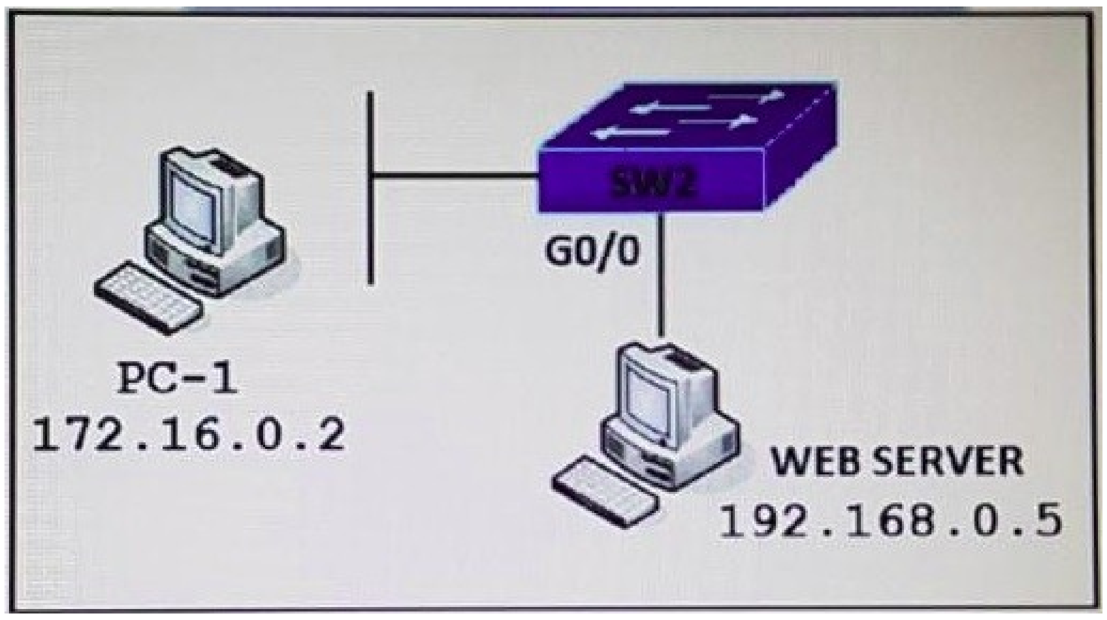
A. Mastered
B. Not Mastered

Answer: A

Explanation:


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

NEW QUESTION 120
- (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 125
- (Topic 2)
Which two actions, when applied in the LAN network segment, will facilitate Layer 3
CAPWAP discovery for lightweight AP? (Choose two.)

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

Answer: CE

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

NEW QUESTION 126
- (Topic 2)
What is one primary REST security design principle?

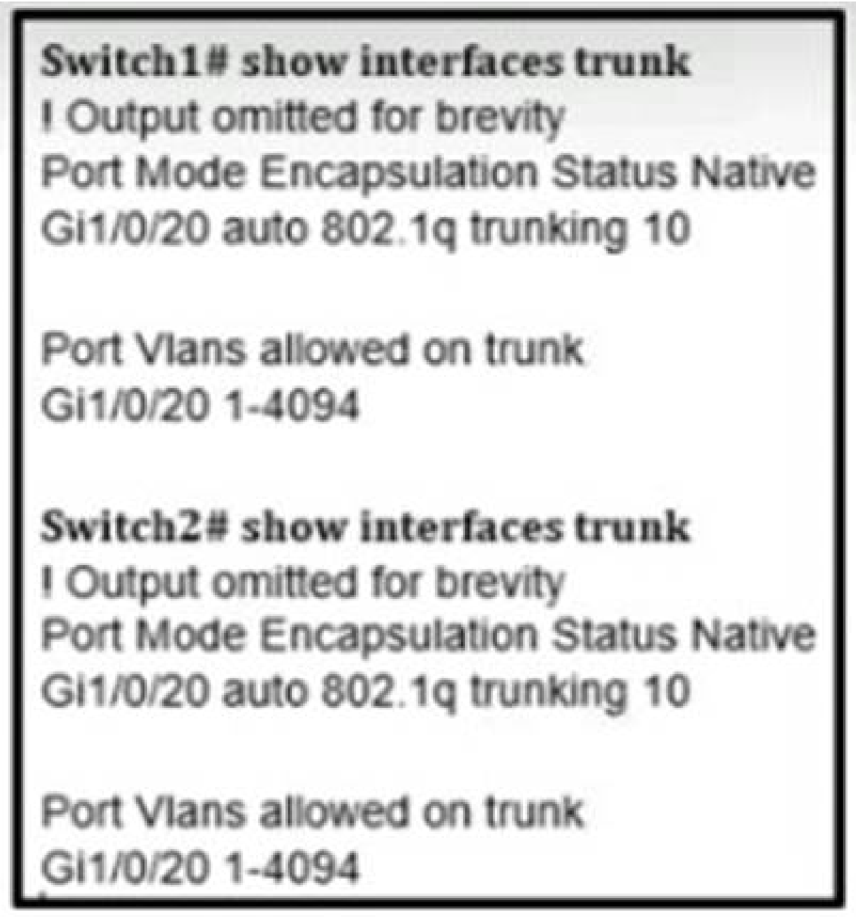
A. fail-safe defaults
B. password hash
C. adding a timestamp in requests
D. OAuth

Answer: A

Explanation:

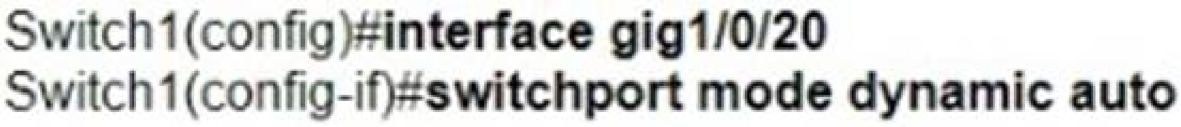
Reference: https://yurisubach.com/2017/04/04/restful-api-security-principles/“Fail-safe defaultsAccess to any resource (like API endpoint) should be denied by default. Access granted only in case of specific permission.

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



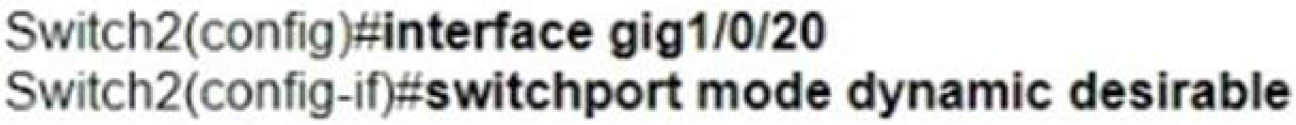
```
Switch1# show interfaces trunk
! Output omitted for brevity
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802.1q trunking 10

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

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

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

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



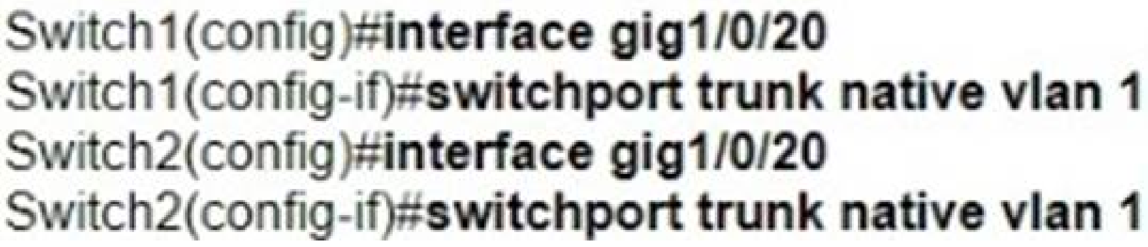
```
Switch1(config)#interface gig1/0/20
Switch1(config-if)#switchport mode dynamic auto
```

B)



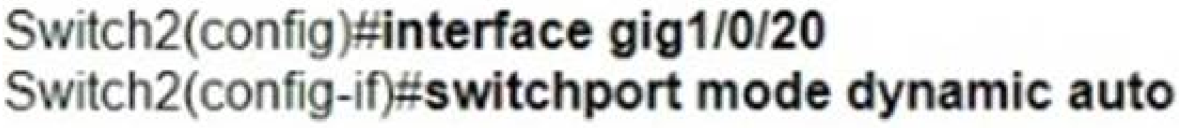
```
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic desirable
```

C)



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

D)



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

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

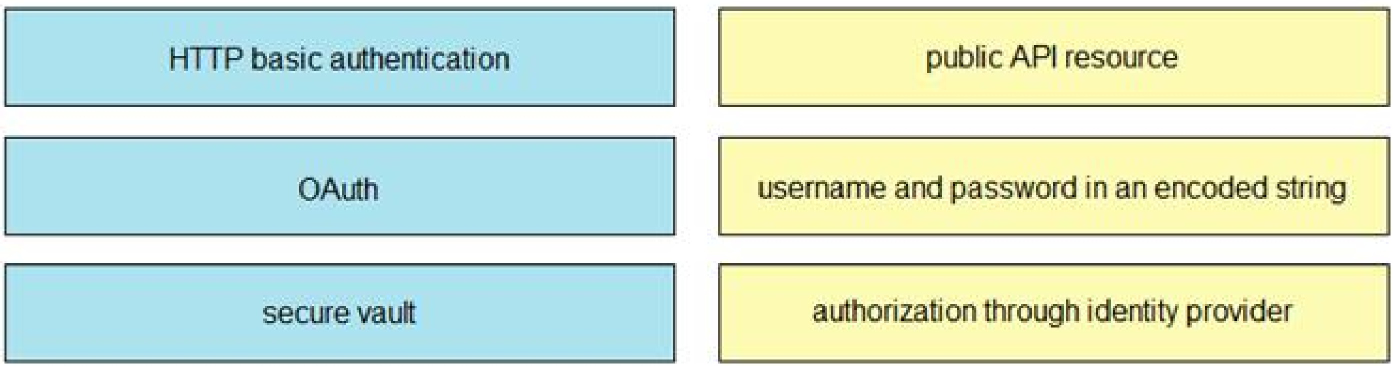
Answer: B

NEW QUESTION 130
- (Topic 2)
An engineer is configuring a new SSID to present users with a splash page for authentication. Which WLAN Layer 3 setting must be configured to provide this functionally?

A. CCKM
B. WPA2 Policy
C. Local Policy
D. Web Policy

Answer: D

NEW QUESTION 132
DRAG DROP - (Topic 2)
Drag and drop the REST API authentication methods from the left onto their descriptions on the right.

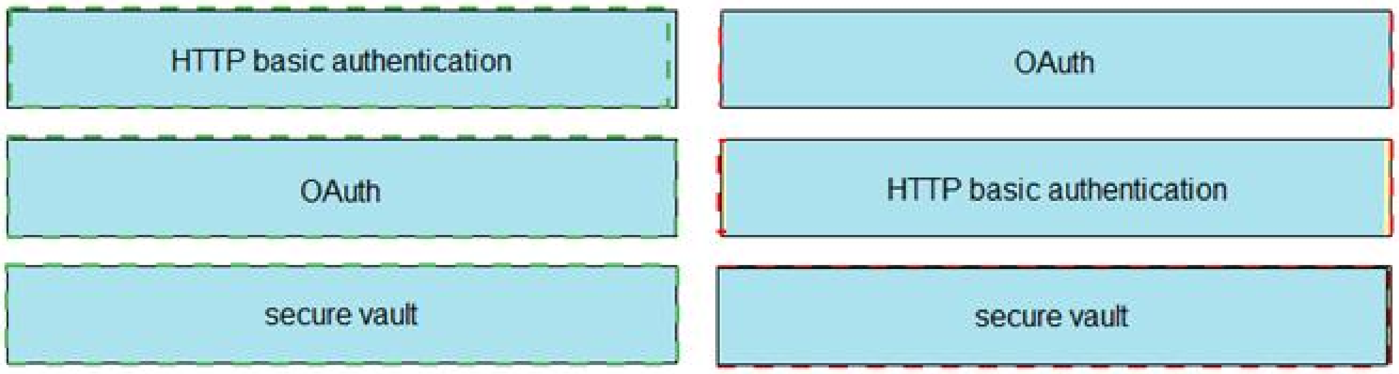


HTTP basic authentication	public API resource
OAuth	username and password in an encoded string
secure vault	authorization through identity provider

A. Mastered
B. Not Mastered

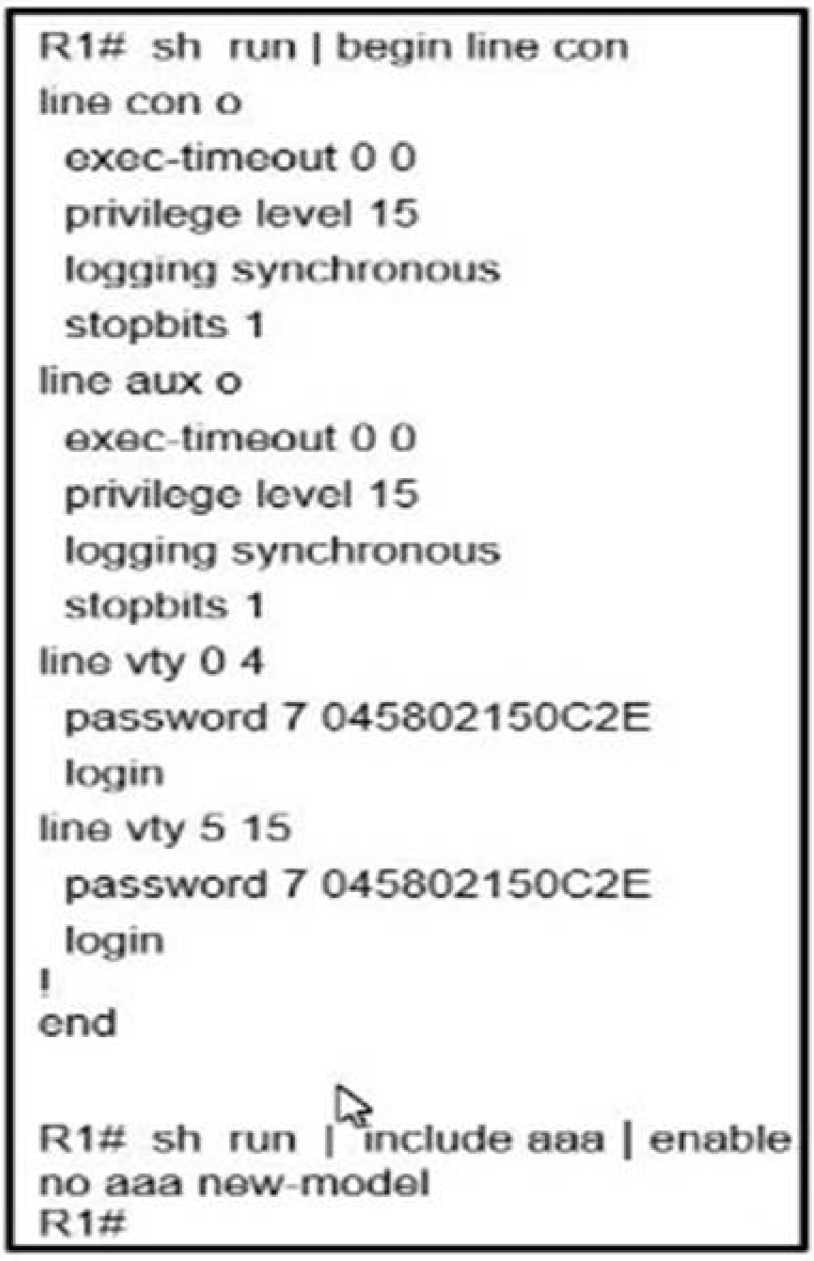
Answer: A

Explanation:



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

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



```
R1# sh  run | begin line con
line con o
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux o
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password 7 045802150C2E
  login
line vty 5 15
  password 7 045802150C2E
  login
!
end

R1# sh  run  |  include aaa | enable
no aaa new-model
R1#
```

Which privilege level is assigned to VTY users?

A. 1
B. 7
C. 13
D. 15

Answer: A

Explanation:
Lines (CON, AUX, VTY) default to level 1 privileges.

NEW QUESTION 138
- (Topic 2)
A customer wants to use a single SSID to authenticate loT devices using different passwords. Which Layer 2 security type must be configured in conjunction with Cisco ISE to achieve this requirement?

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

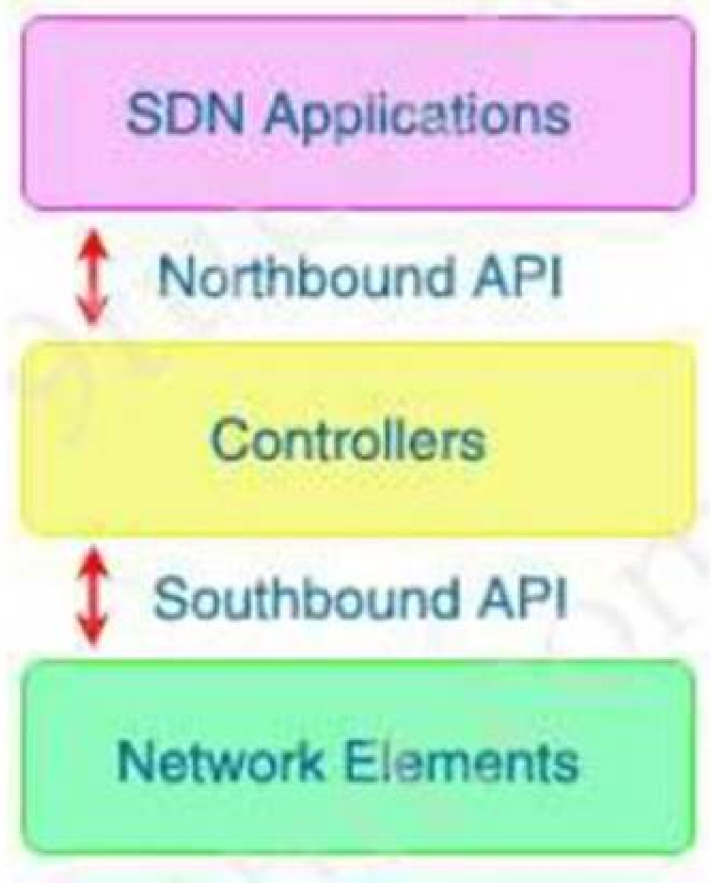
Answer: D

NEW QUESTION 141
- (Topic 2)
What do Cisco DNA southbound APIs provide?

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

Answer: A

Explanation:
The Southbound API is used to communicate with network devices.

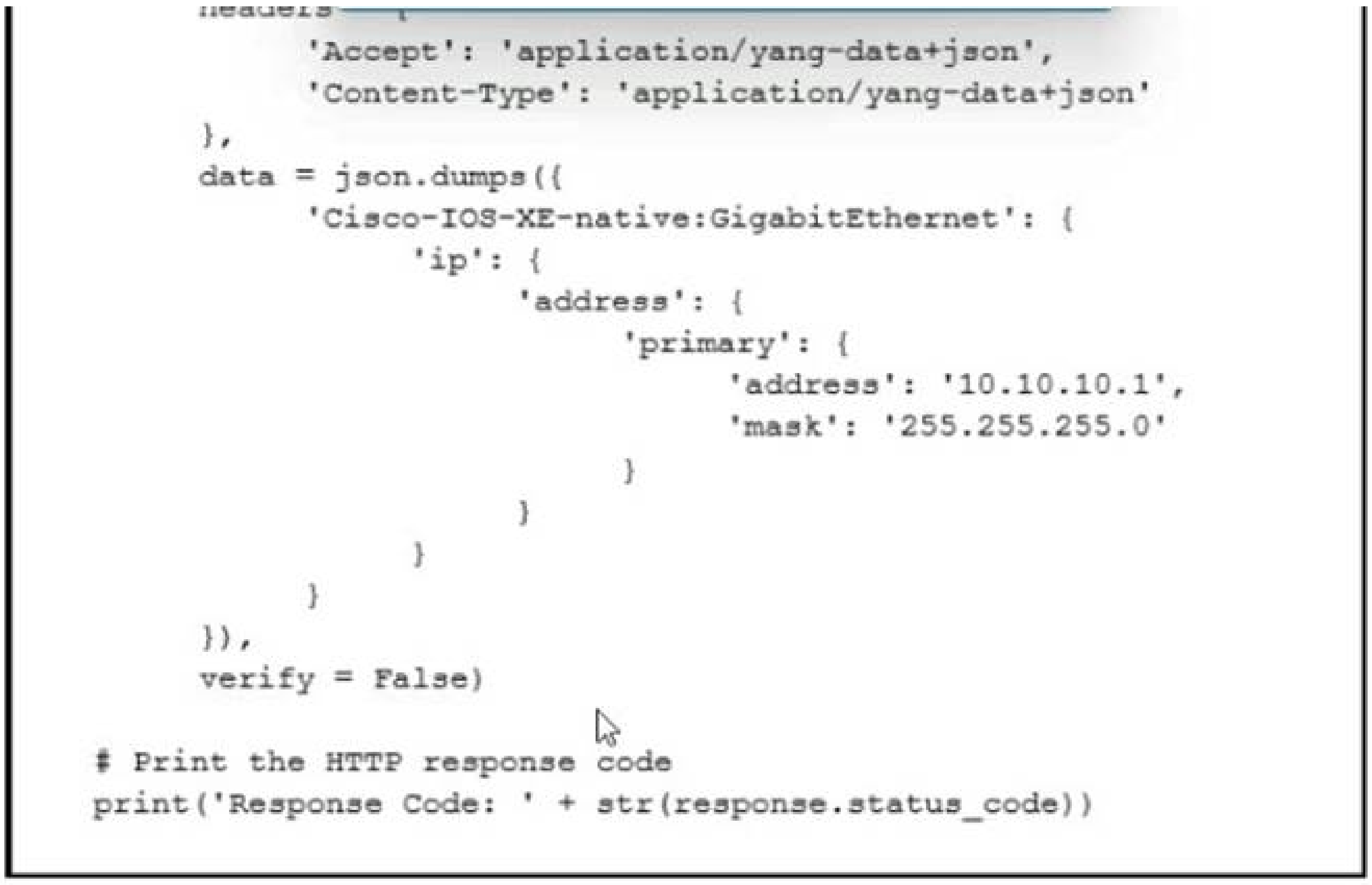


NEW QUESTION 142
- (Topic 2)
What Is a Type 2 hypervisor?

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

Answer: A

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



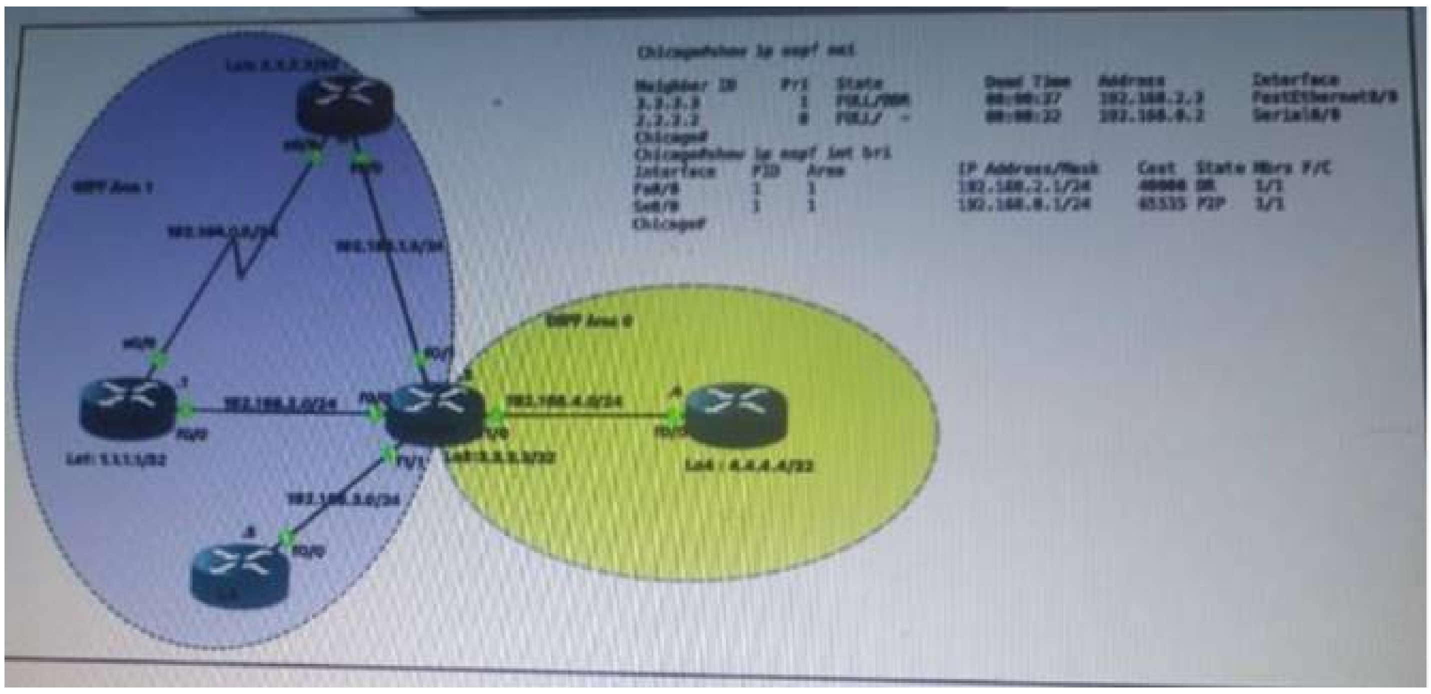
```
        headers = {
              'Accept': 'application/yang-data+json',
              'Content-Type': 'application/yang-data+json'
        },
        data = json.dumps({
              'Cisco-IOS-XE-native:GigabitEthernet': {
                    'ip': {
                          'address': {
  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

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

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

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

Answer: D

NEW QUESTION 151
- (Topic 2)
Refer the exhibit.



```
Chicago#show ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   FULL/DR         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 155
- (Topic 2)
What is the wireless received signal strength indicator?

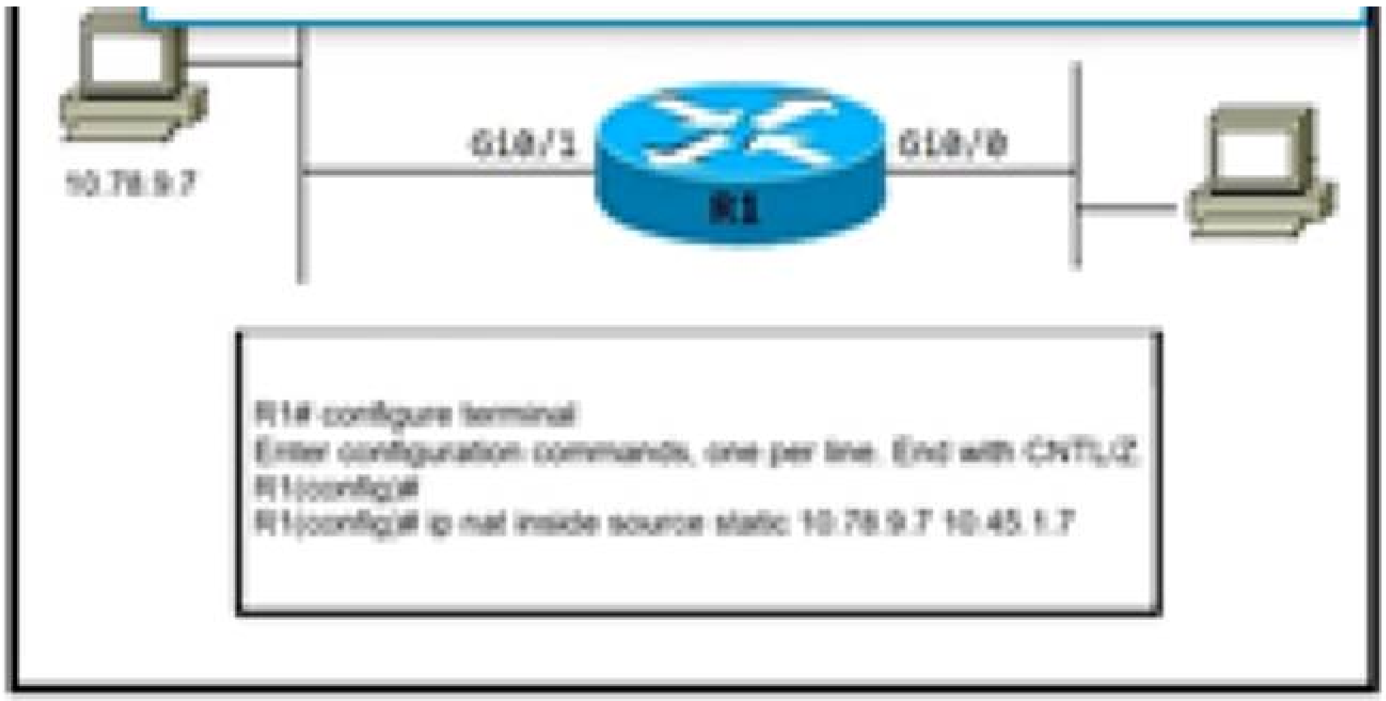
A. The value given to the strength of the wireless signal received compared to the noise level
B. The value of how strong the wireless signal Is leaving the antenna using transmit power, cable loss, and antenna gain
C. The value of how much wireless signal is lost over a defined amount of distance
D. 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 159
- (Topic 2)
Refer to the exhibit.



```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
R1(config)#
R1(config)# ip nat inside source static 10.78.9.7 10.45.1.7
```

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

A. R1(config)#interface GigabitEthernet0/0 R1(config)#ip pat outside R1(config)#interface GigabitEthernet0/1 R1(config)#ip pat inside
B. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat outside R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat inside
C. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat inside R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat outside
D. R1(config)#interface GigabitEthernet0/0 R1(config)#ip pat inside R1(config)#interface GigabitEthernet0/1 R1(config)#ip pat outside

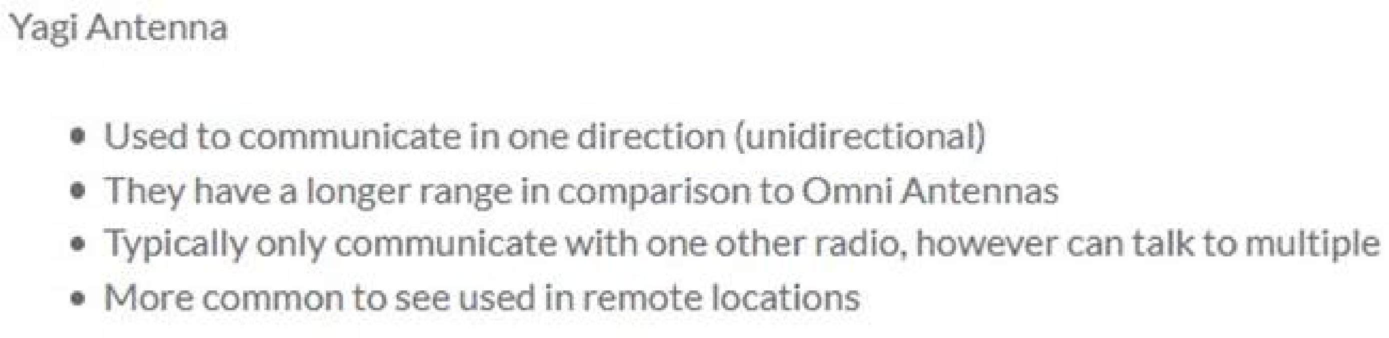
Answer: B

NEW QUESTION 160
- (Topic 2)
Which antenna type should be used for a site-to-site wireless connection?

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

Answer: D

Explanation:

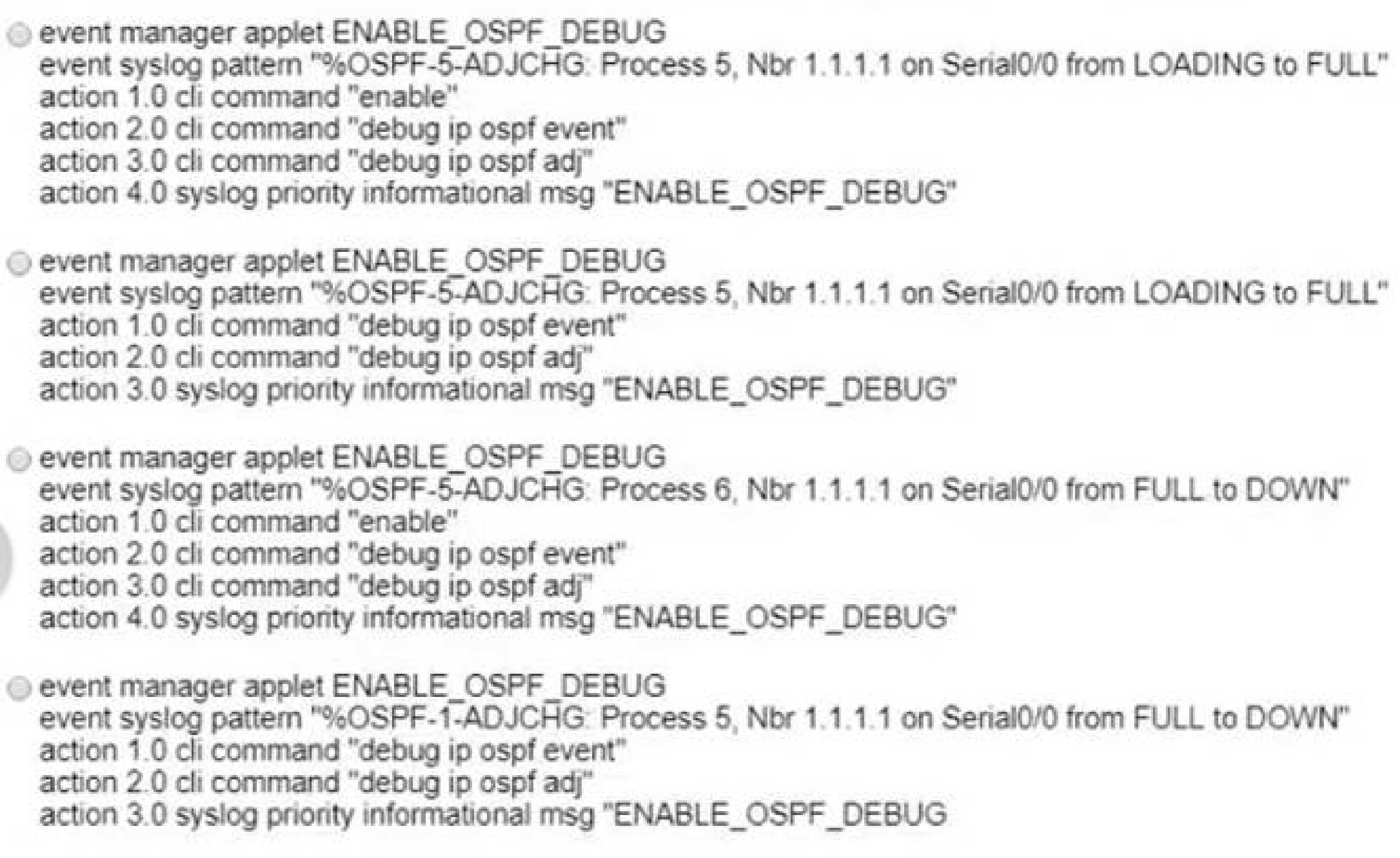


Yagi Antenna

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

Graphical user interface, text Description automatically generated

NEW QUESTION 165
- (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?

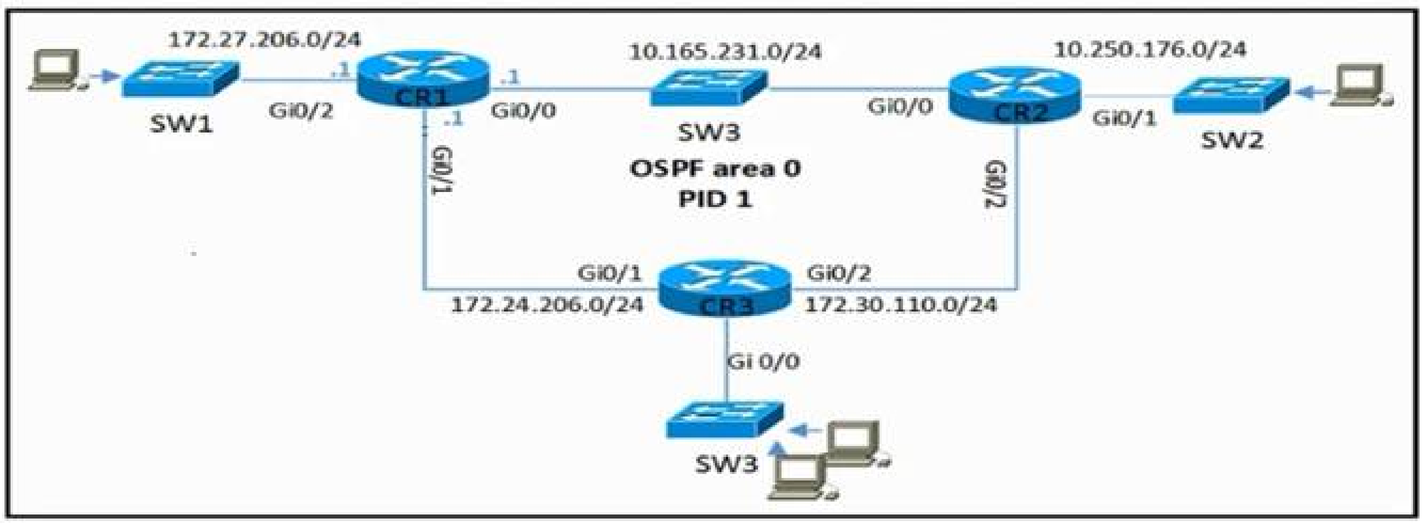


```
○ event manager applet ENABLE_OSPF_DEBUG
  event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL"
  action 1.0 cli command "enable"
  action 2.0 cli command "debug ip ospf event"
  action 3.0 cli command "debug ip ospf adj"
  action 4.0 syslog priority informational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

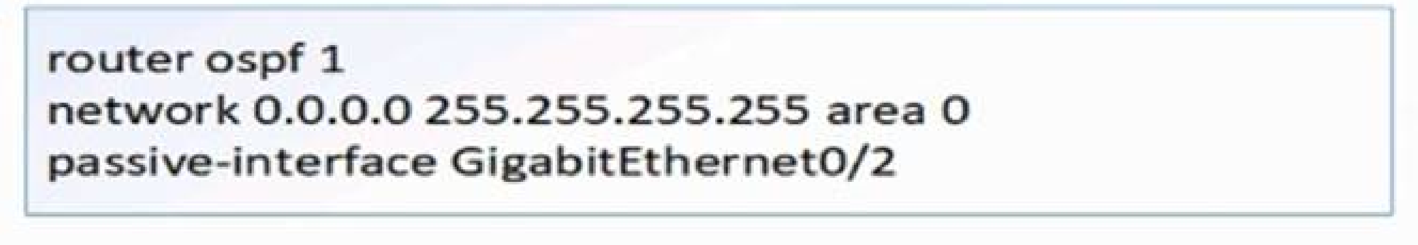
Answer: C

NEW QUESTION 166
- (Topic 2)
Refer to the exhibit.



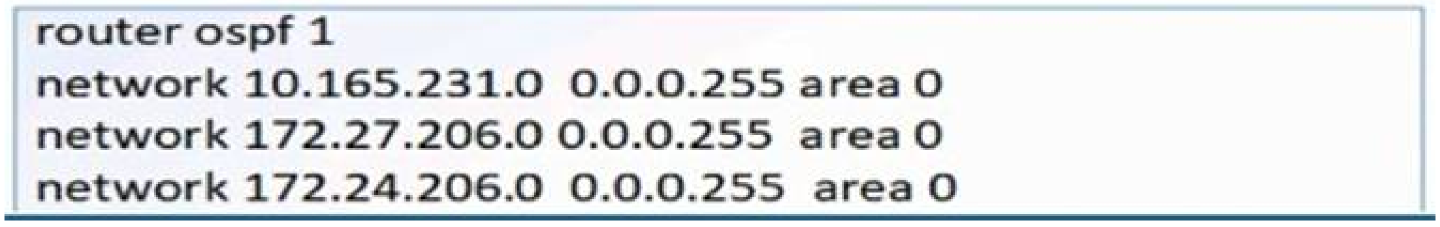
CR2 and CR3 ate configured with OSPF. Which configuration, when applied to CR1. allows CR1 to exchange OSPF Information with CR2 and CR3 but not with other network devices or on new Interfaces that are added to CR1?

A)



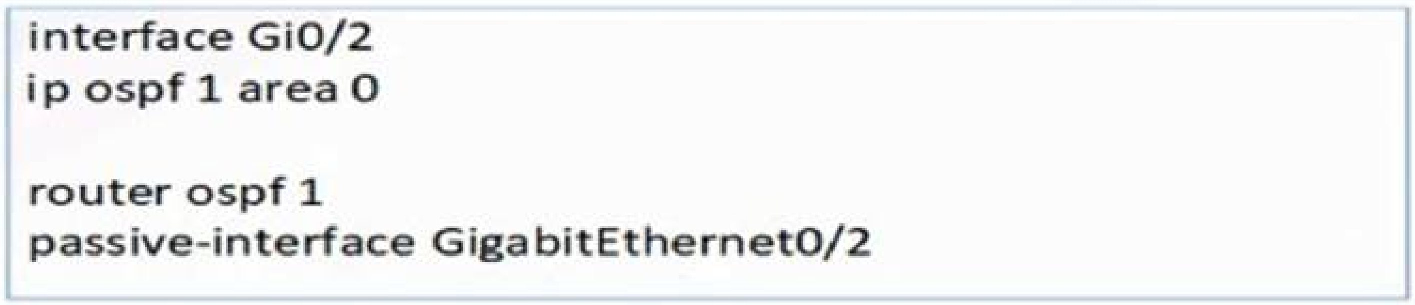
```
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
passive-interface GigabitEthernet0/2
```

B)



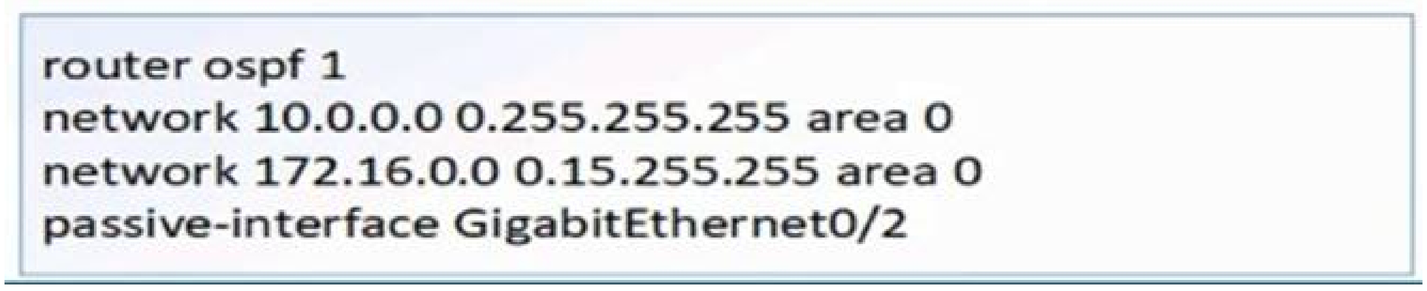
```
router ospf 1
network 10.165.231.0  0.0.0.255 area 0
network 172.27.206.0 0.0.0.255  area 0
network 172.24.206.0  0.0.0.255  area 0
```

C)



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

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

D)

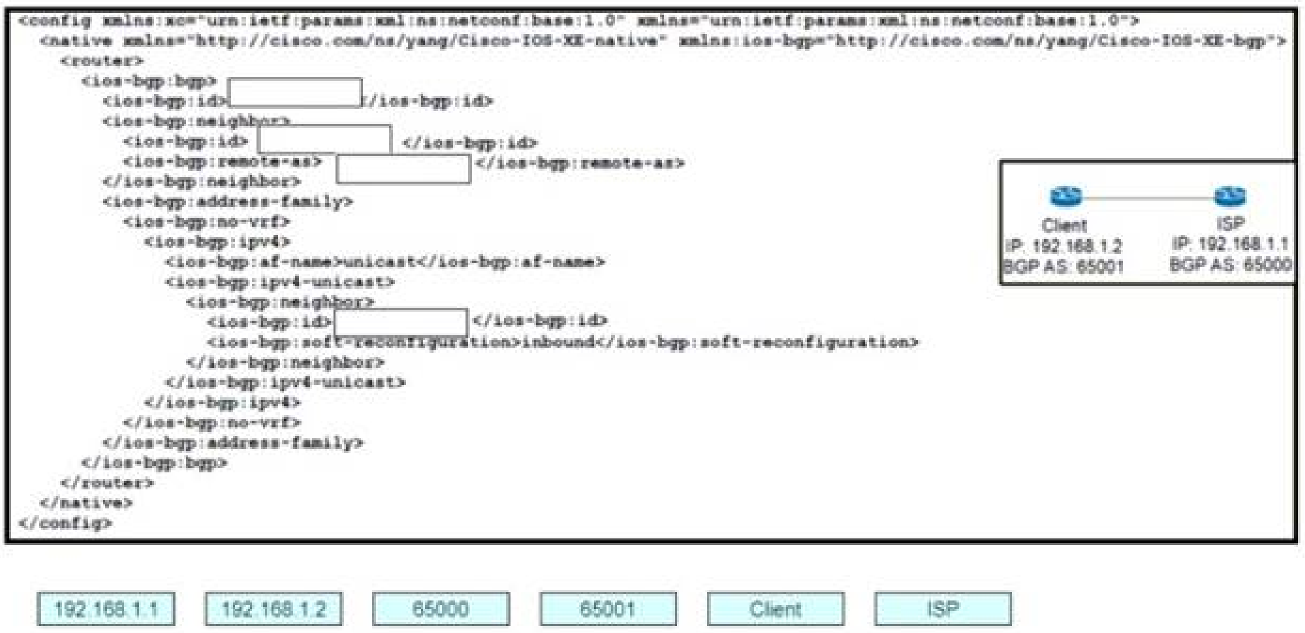


```
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
network 172.16.0.0 0.15.255.255 area 0
passive-interface GigabitEthernet0/2
```

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

Answer: D

NEW QUESTION 169
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.

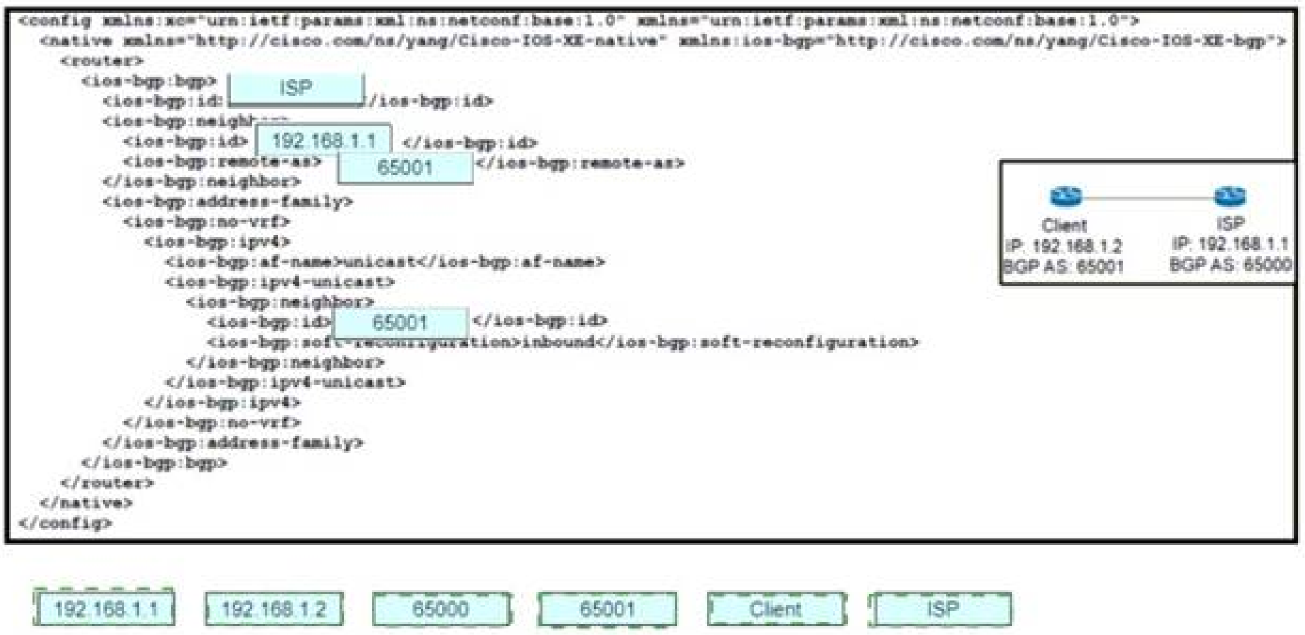


```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>
        <ios-bgp:id>          </ios-bgp:id>
        <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>
```

A. Mastered
B. Not Mastered

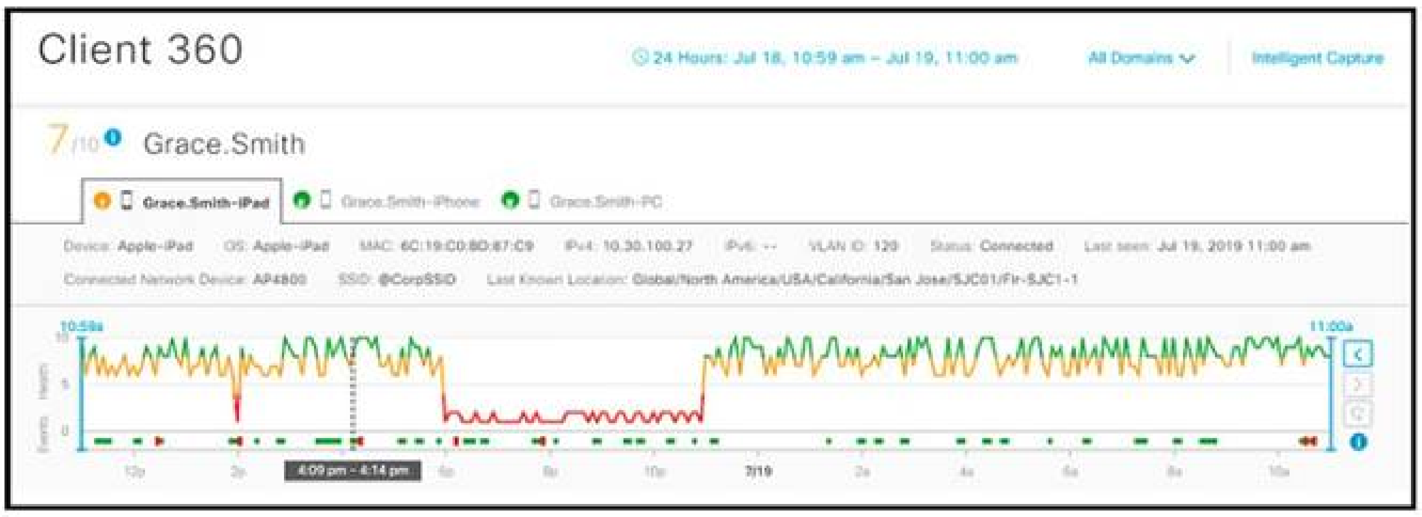
Answer: A

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>
        <ios-bgp:id> ISP </ios-bgp:id>
        <ios-bgp:neighbor>
          <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>
```

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



Client 360

24 Hours: Jul 18, 10:59 am – Jul 19, 11:00 am | All Domains | Intelligent Capture

7/10 Grace.Smith

Grace.Smith-iPad | Grace.Smith-iPhone | Grace.Smith-PC

Device: Apple-iPad OS: Apple-iPad MAC: 6C:19:C0:8D:87:C9 IPv4: 10.30.100.27 IPv6: -- VLAN ID: 120 Status: Connected Last seen: Jul 19, 2019 11:00 am

Connected Network Device: AP4800 SSID: @CorpSSID Last Known Location: Global/North America/USA/California/San Jose/SJC01/Flr-SJC1-1

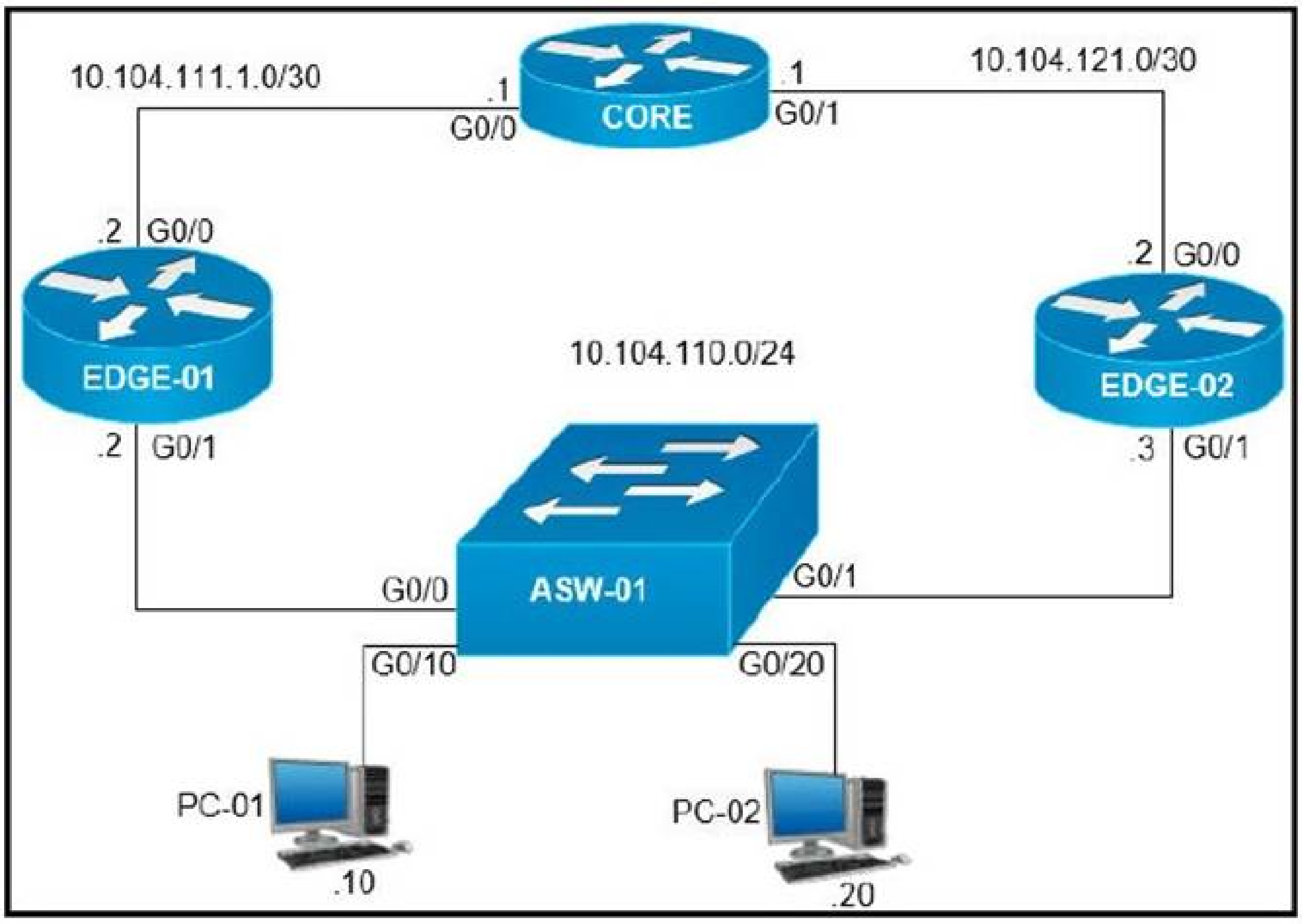
Cisco DNA Center has obtained the username of the client and the multiple devices that the client is using on the network. How is Cisco DNA Center getting these context details?

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

Answer: A

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

NEW QUESTION 174
- (Topic 2)
Refer to the exhibit.

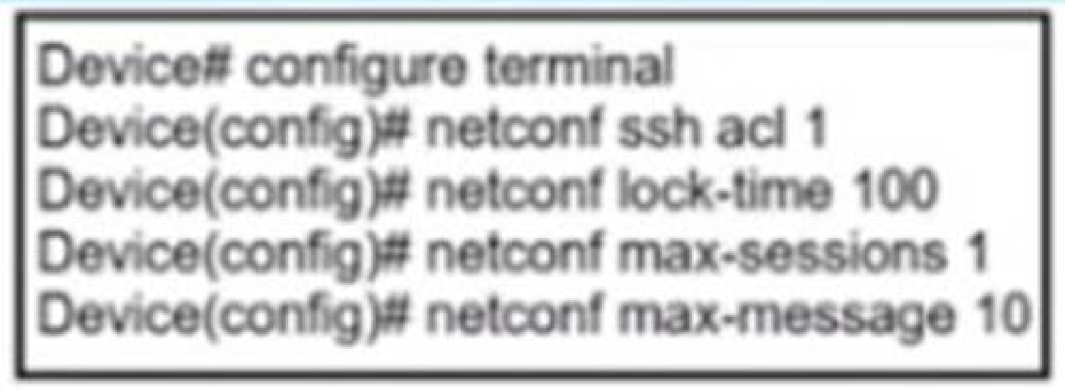


On which interfaces should VRRP commands be applied to provide first hop redundancy to PC-01 and PC-02?

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

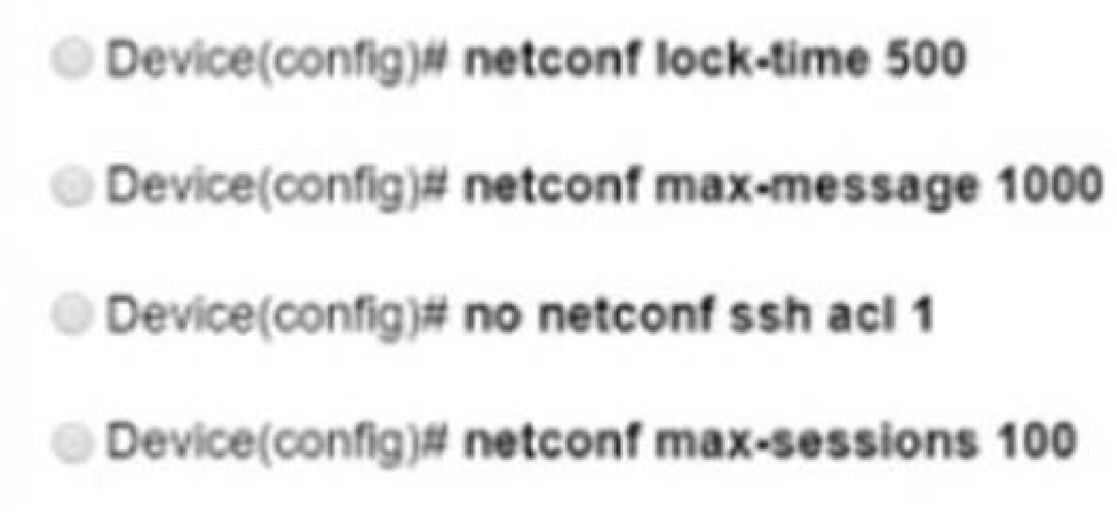
Answer: C

NEW QUESTION 177
- (Topic 2)



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

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



○ Device(config)# **netconf lock-time 500**

○ Device(config)# **netconf max-message 1000**

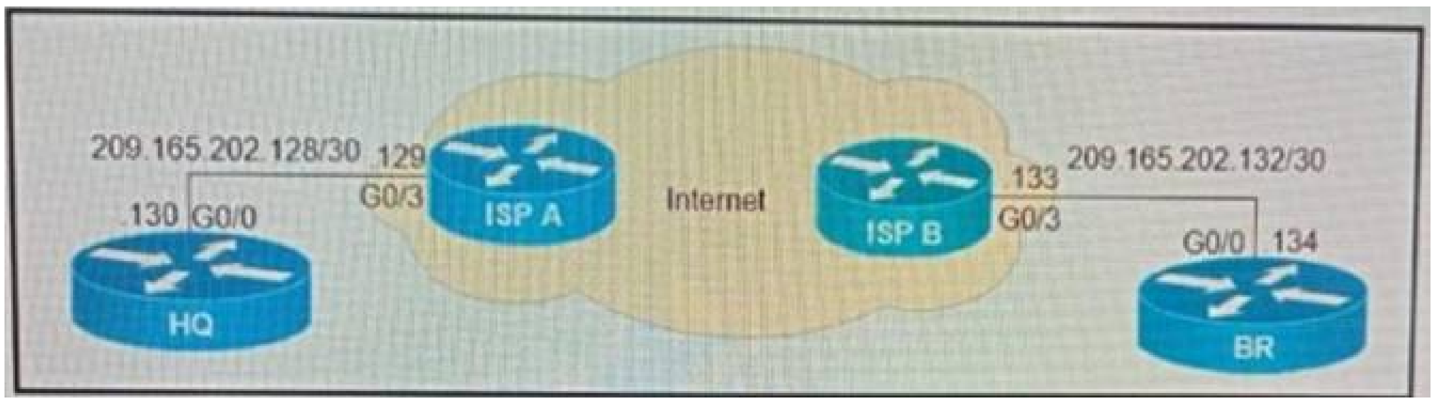
○ Device(config)# **no netconf ssh acl 1**

○ Device(config)# **netconf max-sessions 100**

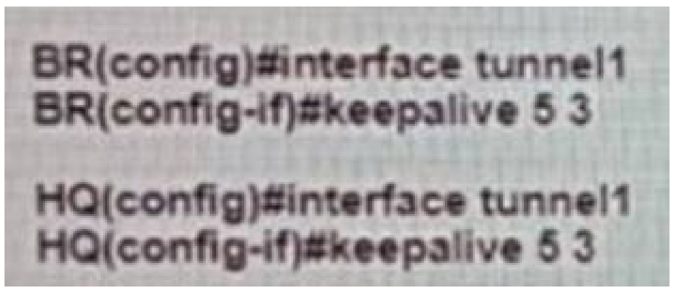
A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

NEW QUESTION 180
- (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 181
- (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.

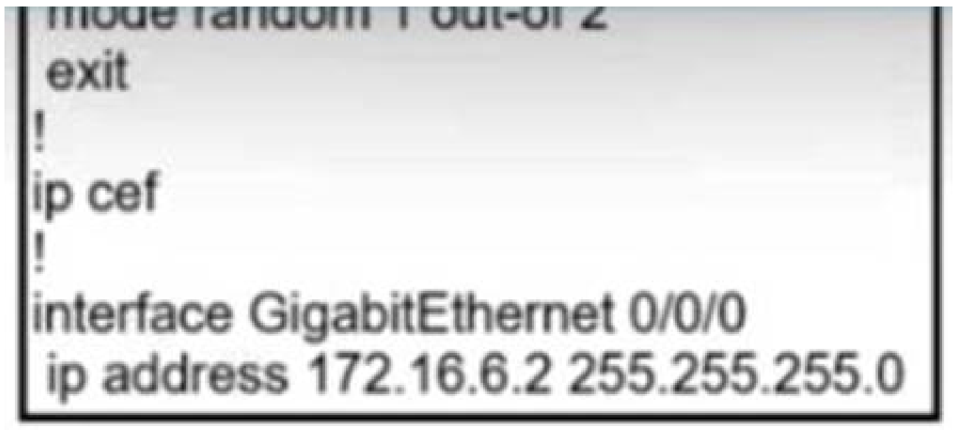
Answer: C

NEW QUESTION 183
- (Topic 2)
How does a fabric AP fit in the network?

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

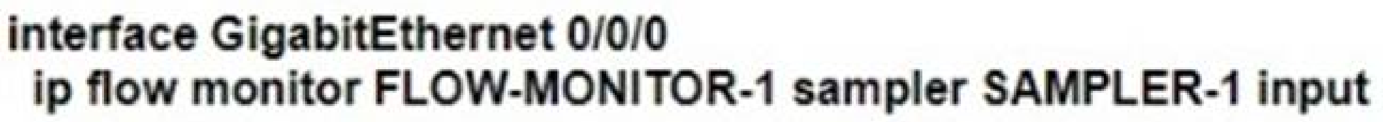
Answer: D

NEW QUESTION 184
- (Topic 2)
Refer to the exhibit.



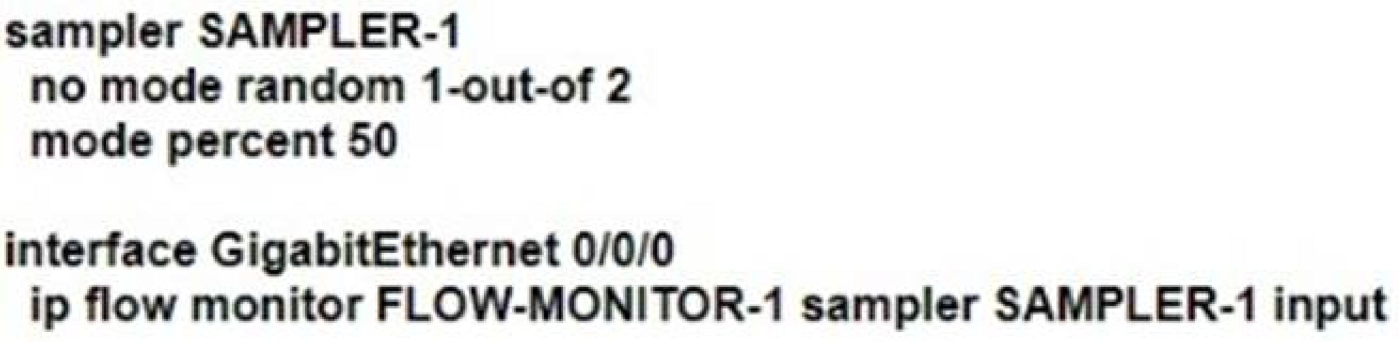
```
 mode random 1 out-of 2
 exit
!
ip cef
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
```

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



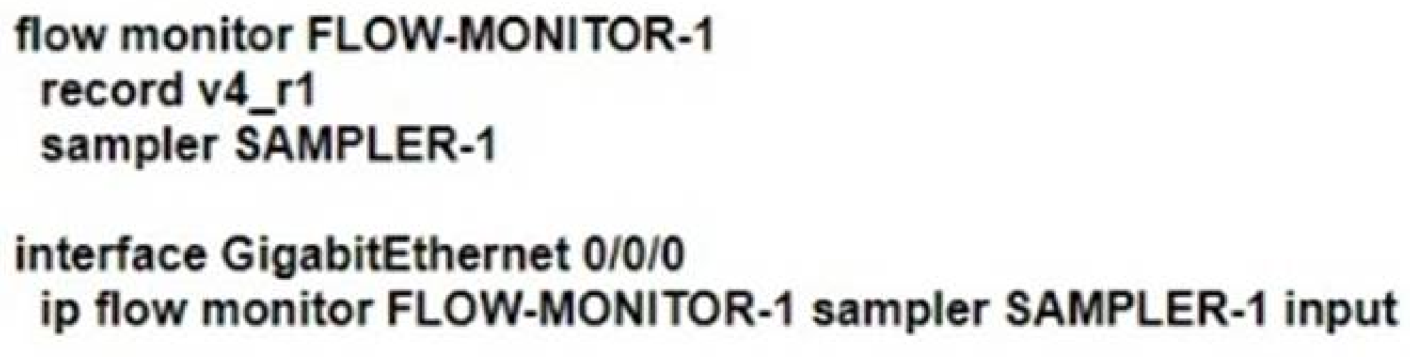
```
interface GigabitEthernet 0/0/0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

B)



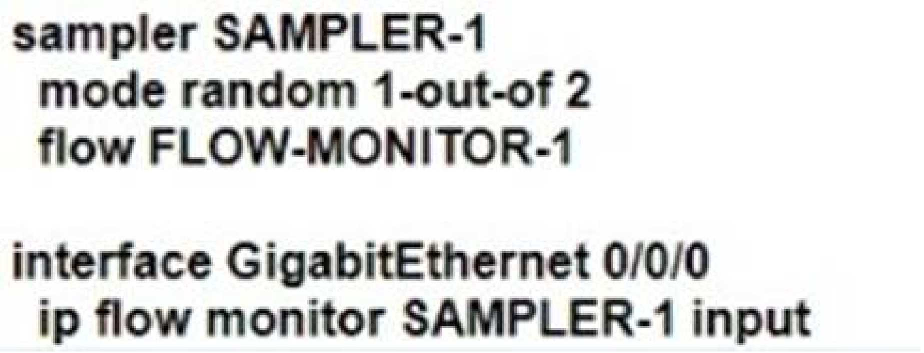
```
sampler SAMPLER-1
 no mode random 1-out-of 2
 mode percent 50

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

C)



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

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

D)

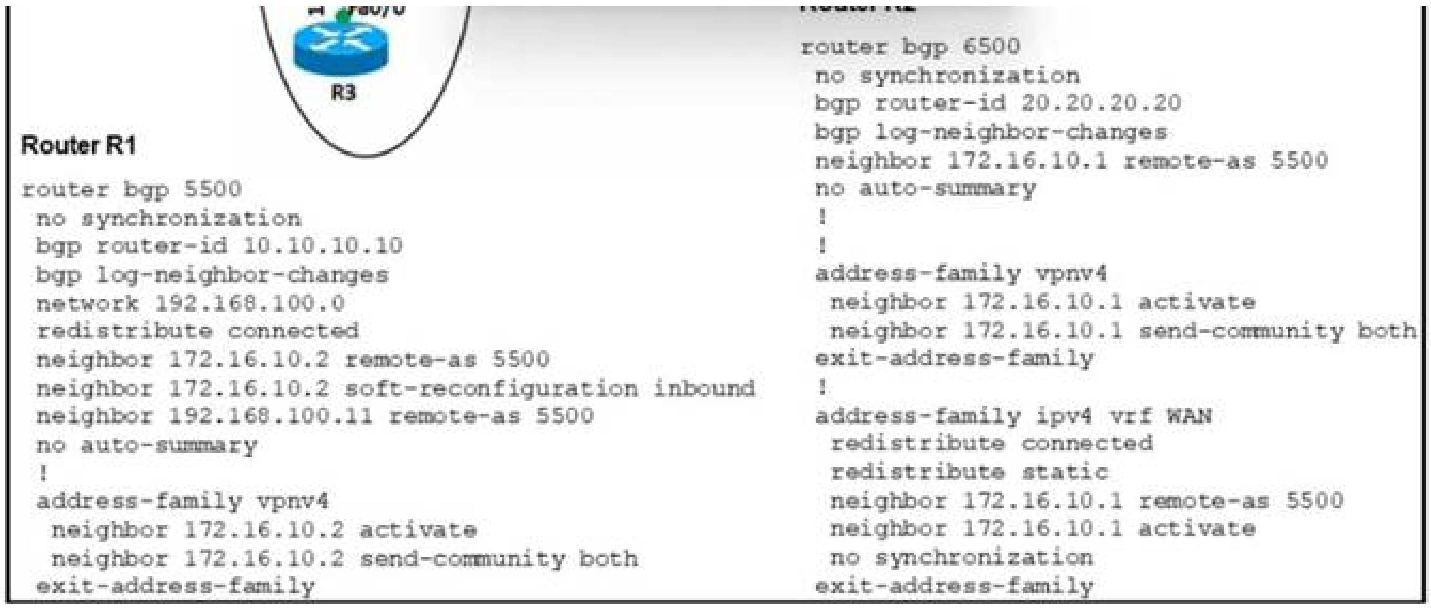


```
sampler SAMPLER-1
 mode random 1-out-of 2
 flow FLOW-MONITOR-1

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

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

Answer: A

NEW QUESTION 187
- (Topic 2)
Refer to the exhibit.



Router R1

```
router bgp 5500
 no synchronization
 bgp router-id 10.10.10.10
 bgp log-neighbor-changes
 network 192.168.100.0
 redistribute connected
 neighbor 172.16.10.2 remote-as 5500
 neighbor 172.16.10.2 soft-reconfiguration inbound
 neighbor 192.168.100.11 remote-as 5500
 no auto-summary
 !
 address-family vpnv4
  neighbor 172.16.10.2 activate
  neighbor 172.16.10.2 send-community both
 exit-address-family
```

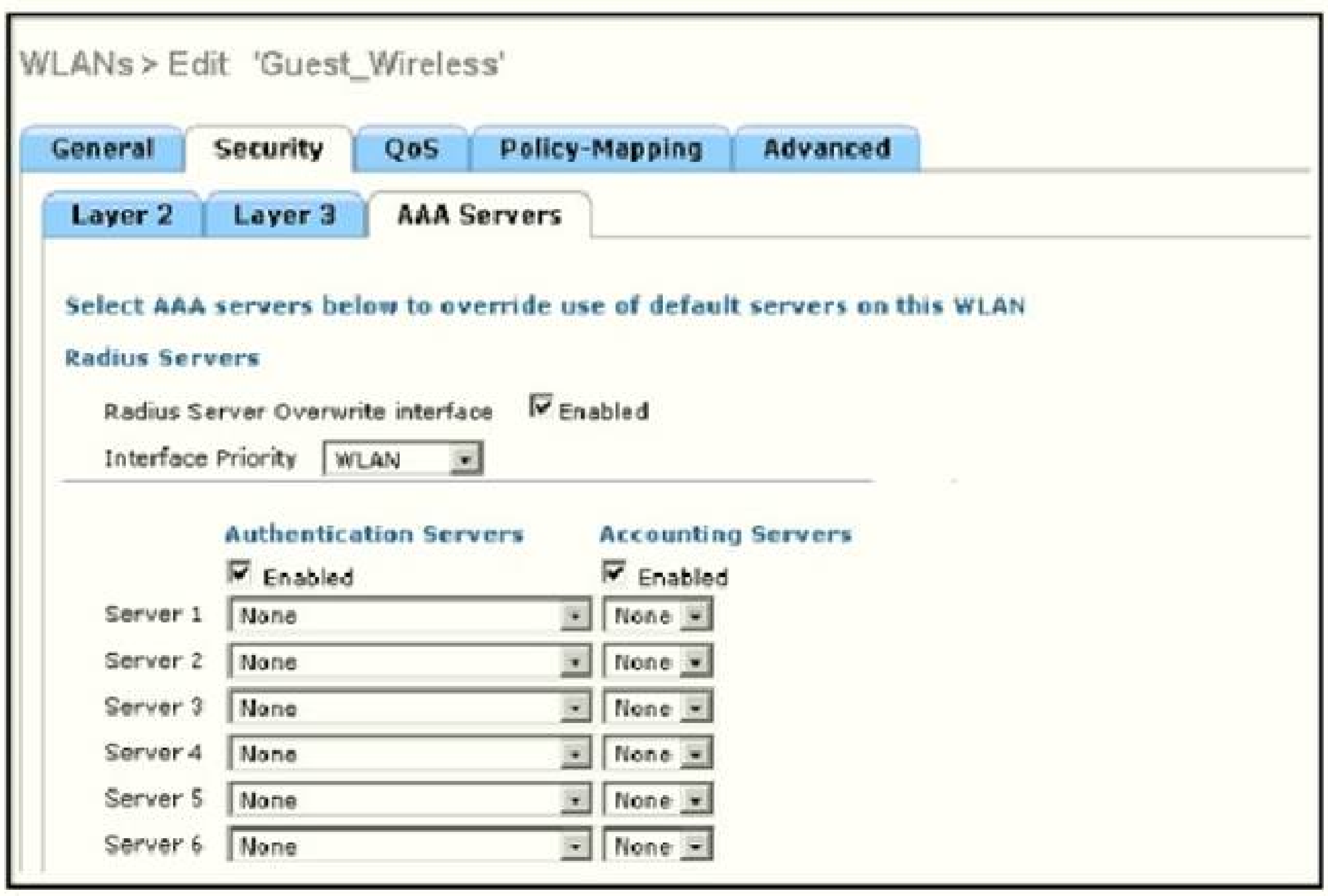
```
router bgp 6500
 no synchronization
 bgp router-id 20.20.20.20
 bgp log-neighbor-changes
 neighbor 172.16.10.1 remote-as 5500
 no auto-summary
 !
 !
 address-family vpnv4
  neighbor 172.16.10.1 activate
  neighbor 172.16.10.1 send-community both
 exit-address-family
 !
 address-family ipv4 vrf WAN
  redistribute connected
  redistribute static
  neighbor 172.16.10.1 remote-as 5500
  neighbor 172.16.10.1 activate
  no synchronization
 exit-address-family
```

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

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

Answer: D

NEW QUESTION 189
- (Topic 1)
Refer to the exhibit.



WLANs > Edit 'Guest_Wireless'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface ☑ Enabled

Interface Priority WLAN

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Assuming the WLC's interfaces are not in the same subnet as the RADIUS server, which interface would the WLC use as the source for all RADIUS-related traffic?

A. the interface specified on the WLAN configuration
B. any interface configured on the WLC
C. the controller management interface
D. the controller virtual interface

Answer: A

NEW QUESTION 191
- (Topic 1)
Which technology provides a secure communication channel for all traffic at Layer 2 of the OSI model?

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

Answer: A

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

NEW QUESTION 195
- (Topic 1)
What is the recommended MTU size for a Cisco SD-Access Fabric?

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

Answer: B

NEW QUESTION 196
- (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 200
- (Topic 1)
Which two mechanisms are available to secure NTP? (Choose two.)

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

Answer: DE

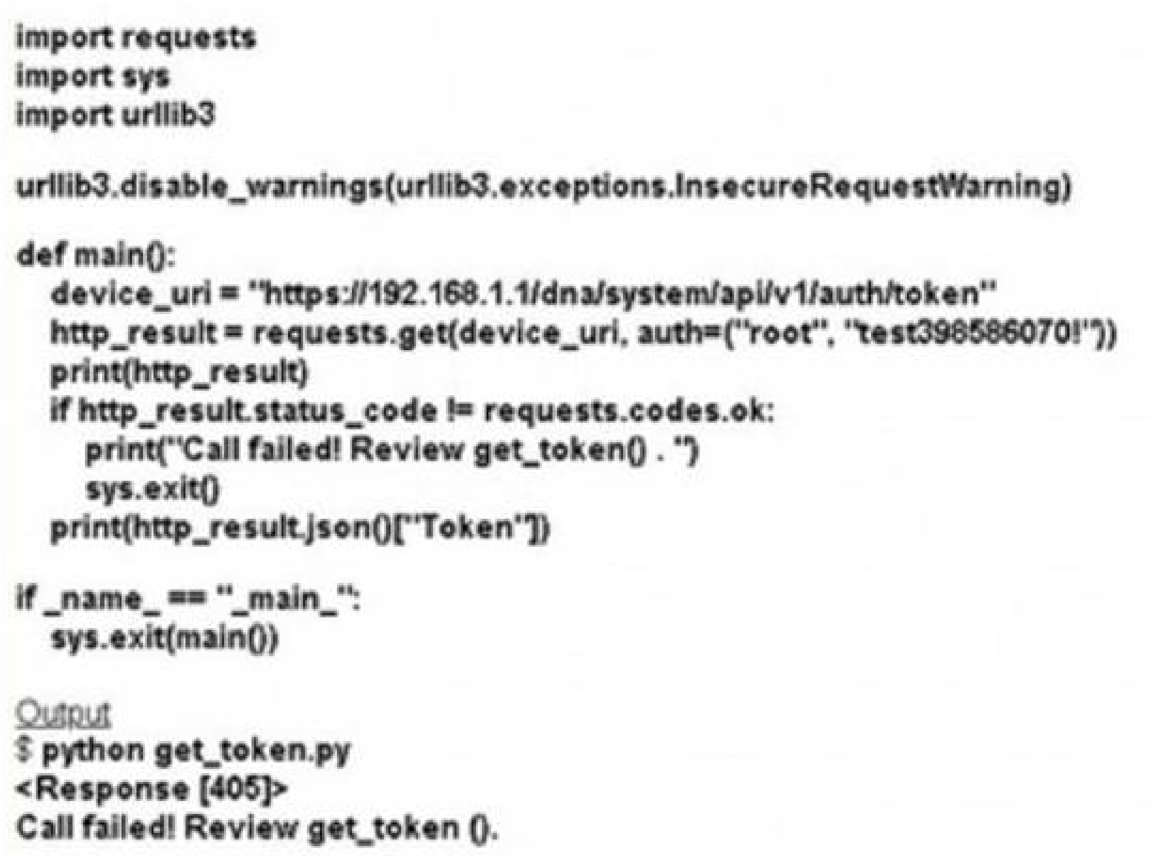
NEW QUESTION 201
- (Topic 1)
Which method of account authentication does OAuth 2.0 within REST APIs?

A. username/role combination
B. access tokens
C. cookie authentication
D. basic signature workflow

Answer: B

Explanation:
The most common implementations of OAuth (OAuth 2.0) use one or both of these tokens:
+ access token: sent like an API key, it allows the application to access a user's data; optionally, access tokens can expire.
+ refresh token: optionally part of an OAuth flow, refresh tokens retrieve a new access token if they have expired. OAuth2 combines Authentication and Authorization to allow more sophisticated scope and validity control.

NEW QUESTION 204
- (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 URl 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 208
- (Topic 1)
In a wireless Cisco SD-Access deployment, which roaming method is used when a user moves from one access point to another on a different access switch using a single WLC?

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

Answer: B

Explanation:
A fabric edge node provides onboarding and mobility services for wired users and devices (including fabric-enabled WLCs and APs) connected to the fabric. It is a LISP tunnel router (xTR) that also provides the anycast gateway, endpoint authentication, and assignment to overlay host pools (static or DHCP), as well as group-based policy enforcement (for traffic to fabric endpoints).
From Cisco's guide, under SDA roaming - When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter- xTR, like a highway. Intra is within intra is between. Like interstate highways. That's how I remember. https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config- guide/b_wl_16_10_cg/mobility.html

NEW QUESTION 210
- (Topic 1)
Which features does Cisco EDR use to provide threat detection and response protection?

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

Answer: B

NEW QUESTION 214
- (Topic 1)
Which measurement is used from a post wireless survey to depict the cell edge of the access points?

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

Answer: A

Explanation:

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

NEW QUESTION 217
- (Topic 1)
What does Call Admission Control require the client to send in order to reserve the bandwidth?

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

Answer: C

NEW QUESTION 218
- (Topic 1)
Which entity is responsible for maintaining Layer 2 isolation between segments In a VXLAN environment?

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

Answer: C

Explanation:

. The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.

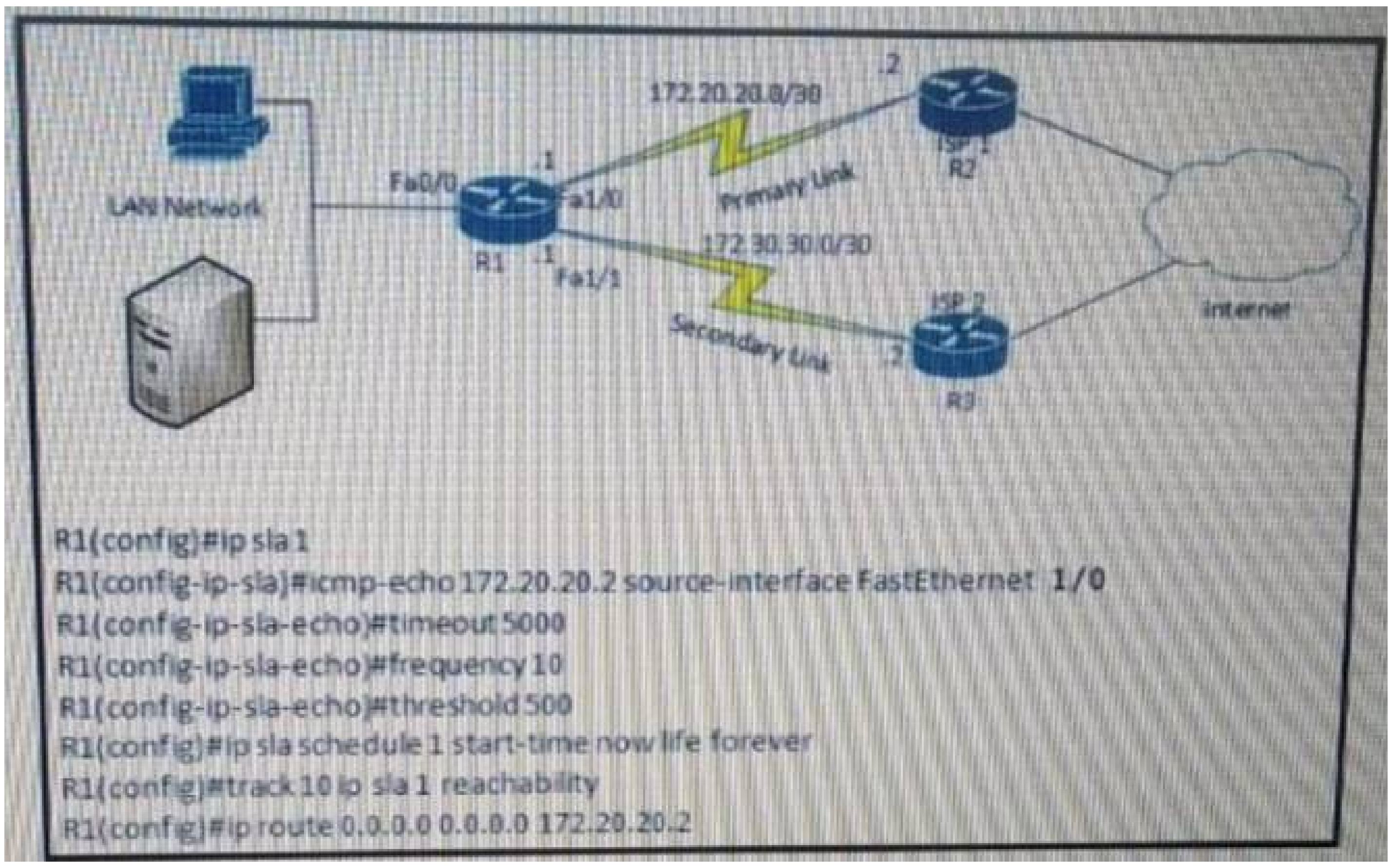
VXLAN uses an 8-byte VXLAN header that consists of a 24-bit VNID and a few reserved bits. The VXLAN header together with the original Ethernet frame goes in the UDP payload. The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX- OS_VXLAN_Configuration_Guide_7x_chapter_010.html

NEW QUESTION 222
- (Topic 1)
After a redundant route processor failure occurs on a Layer 3 device, which mechanism allows for packets to be forwarded from a neighboring router based on the most recent tables?

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

Answer: D

NEW QUESTION 226
- (Topic 1)
Refer to the exhibit.



```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 172.20.20.2 source-interface FastEthernet 1/0
R1(config-ip-sla-echo)#timeout 5000
R1(config-ip-sla-echo)#frequency 10
R1(config-ip-sla-echo)#threshold 500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track 10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2
```

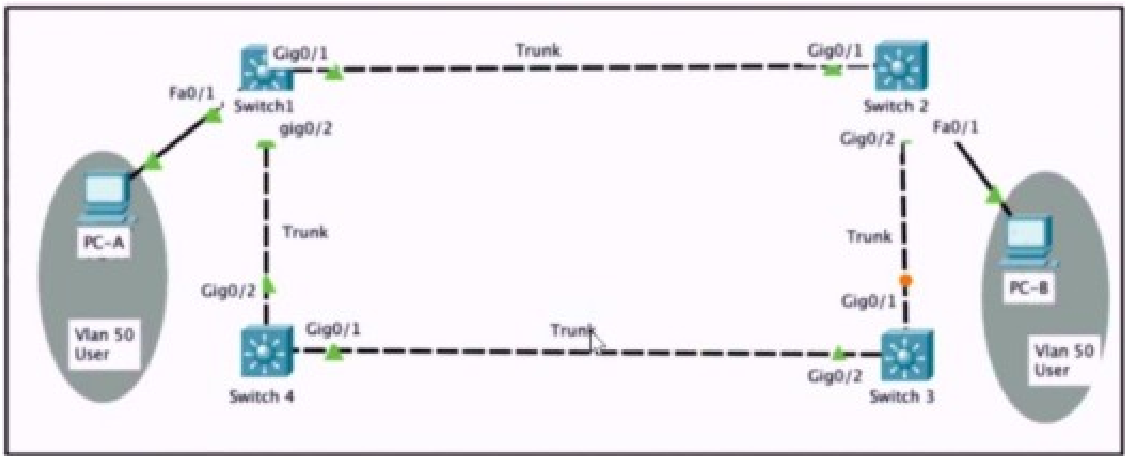
After implementing the configuration 172.20.20.2 stops replaying to ICMP echoes, but the default route fails to be removed. What is the reason for this behavior?

A. The source-interface is configured incorrectly.
B. The destination must be 172.30.30.2 for icmp-echo
C. The default route is missing the track feature
D. The threshold value is wrong.

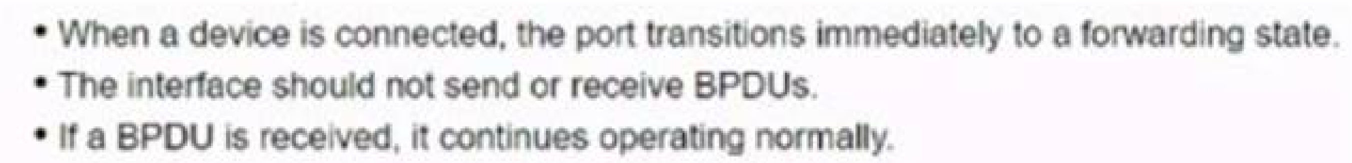
Answer: C

Explanation:
The last command should be “R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10”.

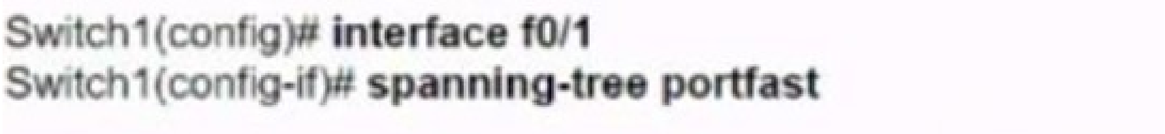
NEW QUESTION 231
- (Topic 1)



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

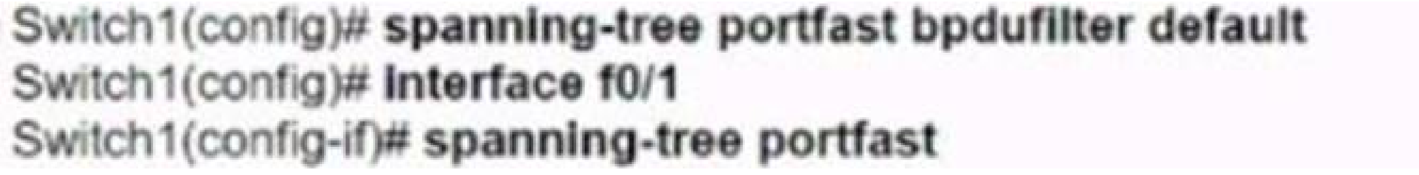

- When a device is connected, the port transitions immediately to a forwarding state.
- The interface should not send or receive BPDUs.
- If a BPDU is received, it continues operating normally.

A)



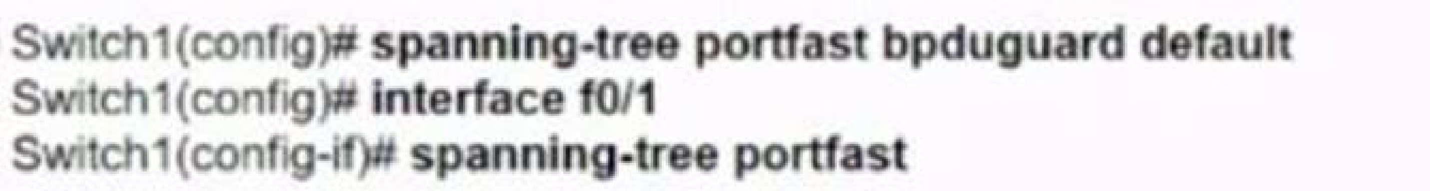
```
Switch1(config)# interface f0/1
Switch1(config-if)# spanning-tree portfast
```

B)



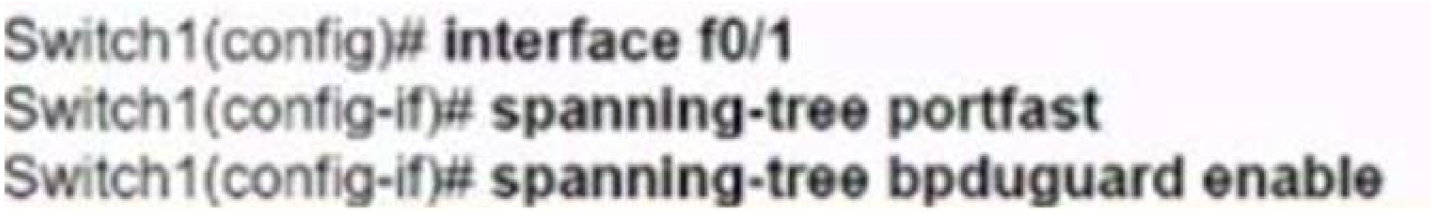
```
Switch1(config)# spanning-tree portfast bpdufilter default
Switch1(config)# interface f0/1
Switch1(config-if)# spanning-tree portfast
```

C)



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

D)

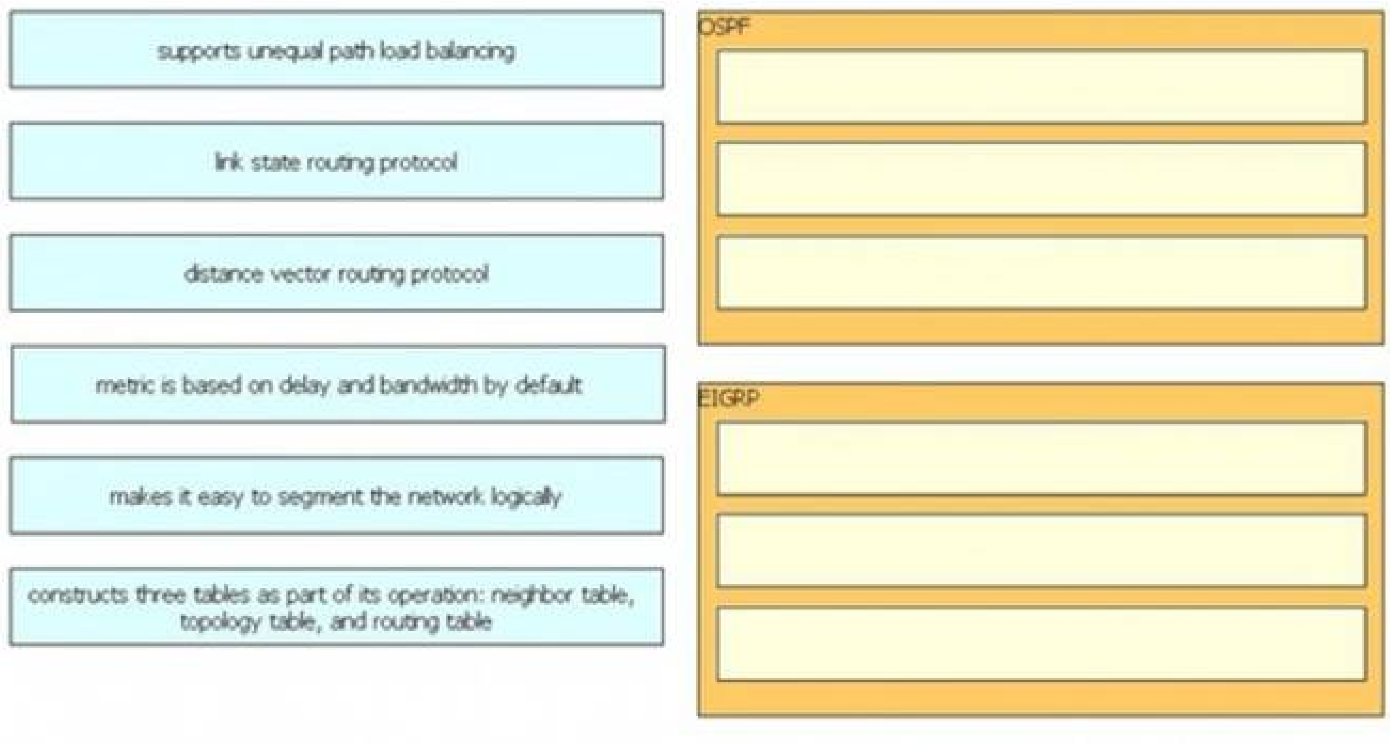


```
Switch1(config)# interface f0/1
Switch1(config-if)# spanning-tree portfast
Switch1(config-if)# spanning-tree bpduguard enable
```

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

Answer: D

NEW QUESTION 234
DRAG DROP - (Topic 1)
Drag and drop the characteristics from the left onto the routing protocols they describe on the right.



supports unequal path load balancing

link state routing protocol

distance vector routing protocol

metric is based on delay and bandwidth by default

makes it easy to segment the network logically

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

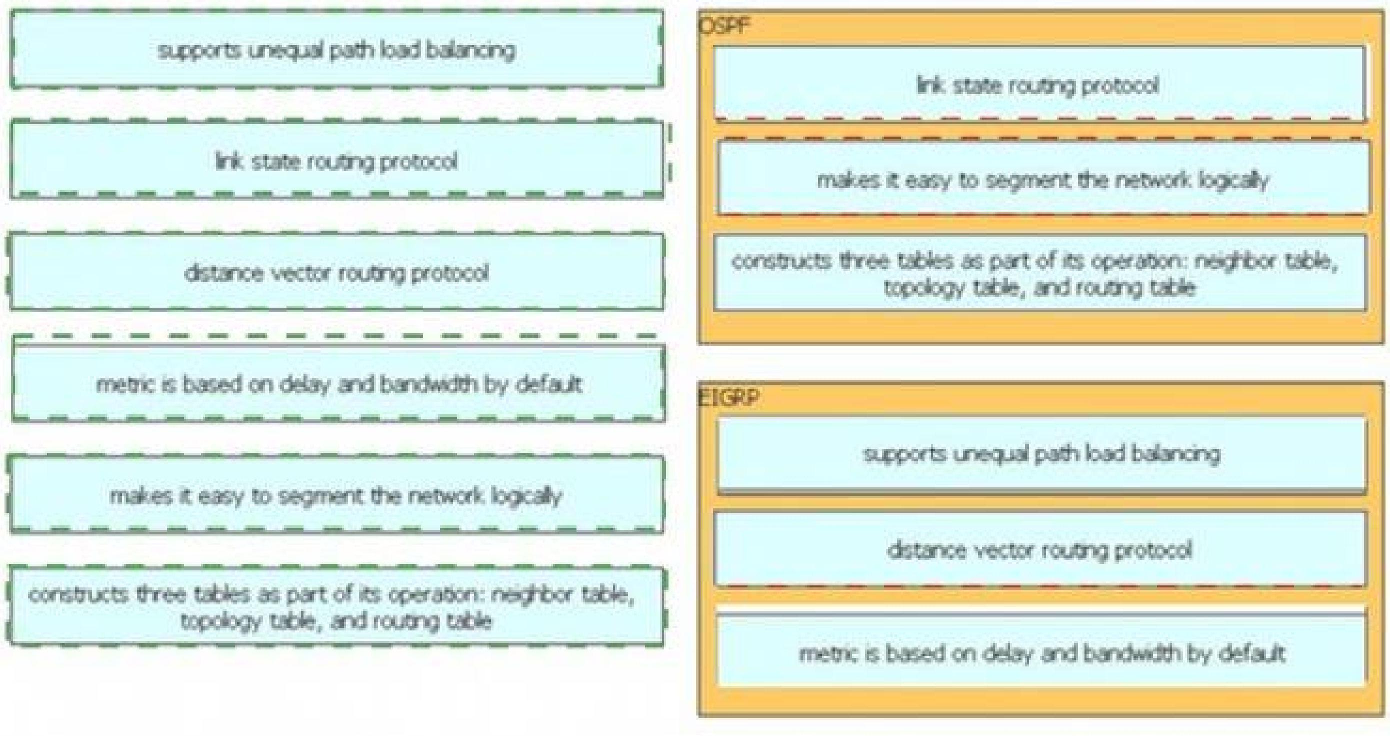
OSPF

EIGRP

A. Mastered
B. Not Mastered

Answer: A

Explanation:



supports unequal path load balancing

link state routing protocol

distance vector routing protocol

metric is based on delay and bandwidth by default

makes it easy to segment the network logically

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

OSPF
- link state routing protocol
- makes it easy to segment the network logically
- constructs three tables as part of its operation: neighbor table, topology table, and routing table

EIGRP
- supports unequal path load balancing
- distance vector routing protocol
- metric is based on delay and bandwidth by default

NEW QUESTION 235
- (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

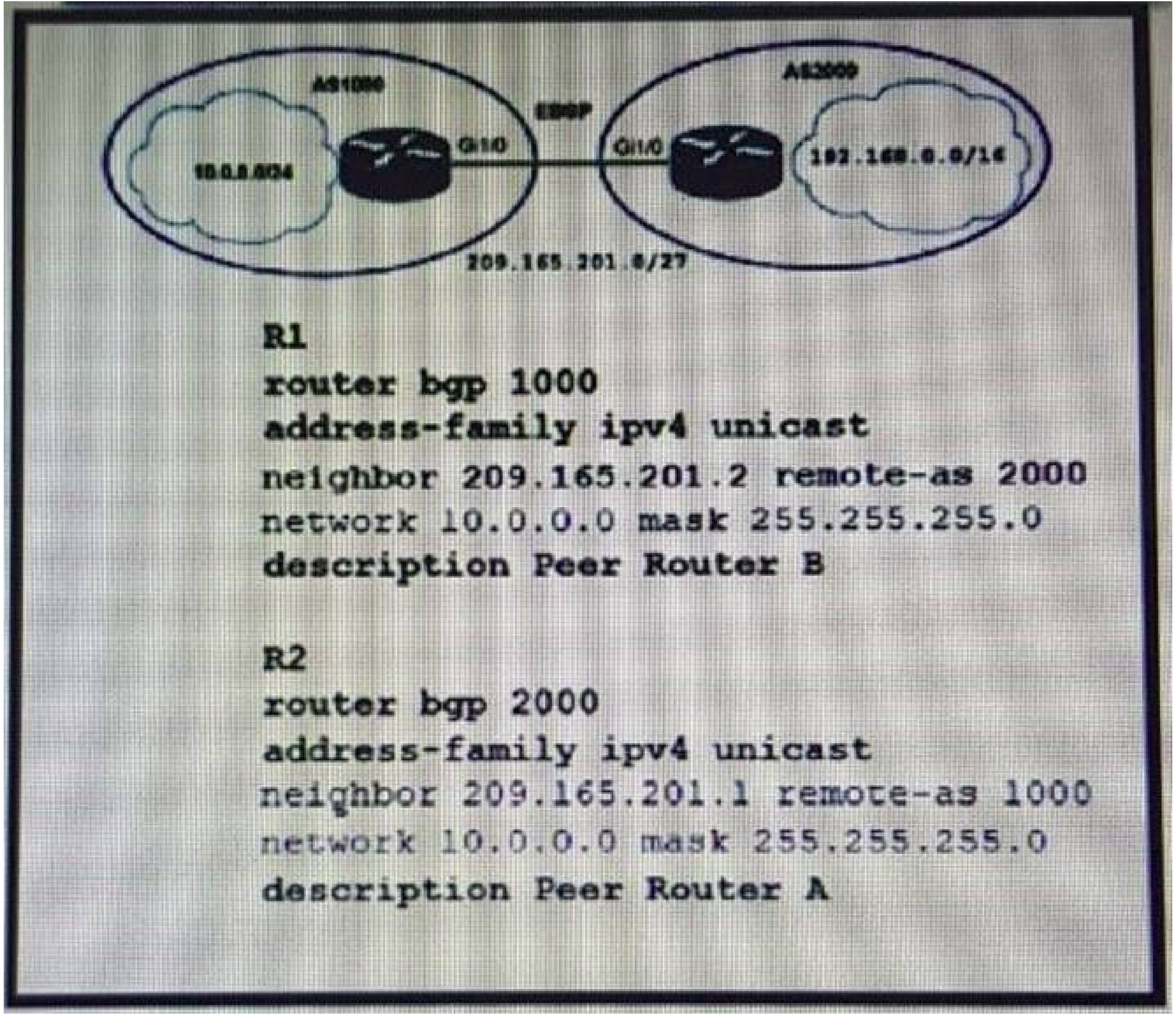
Answer: B

NEW QUESTION 238
- (Topic 1)
Which congestion queuing method on Cisco IOS based routers uses four static queues?

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

Answer: A

NEW QUESTION 239
- (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 241
- (Topic 1)
How does Cisco Trustsec enable more access controls for dynamic networking environments and data centers?

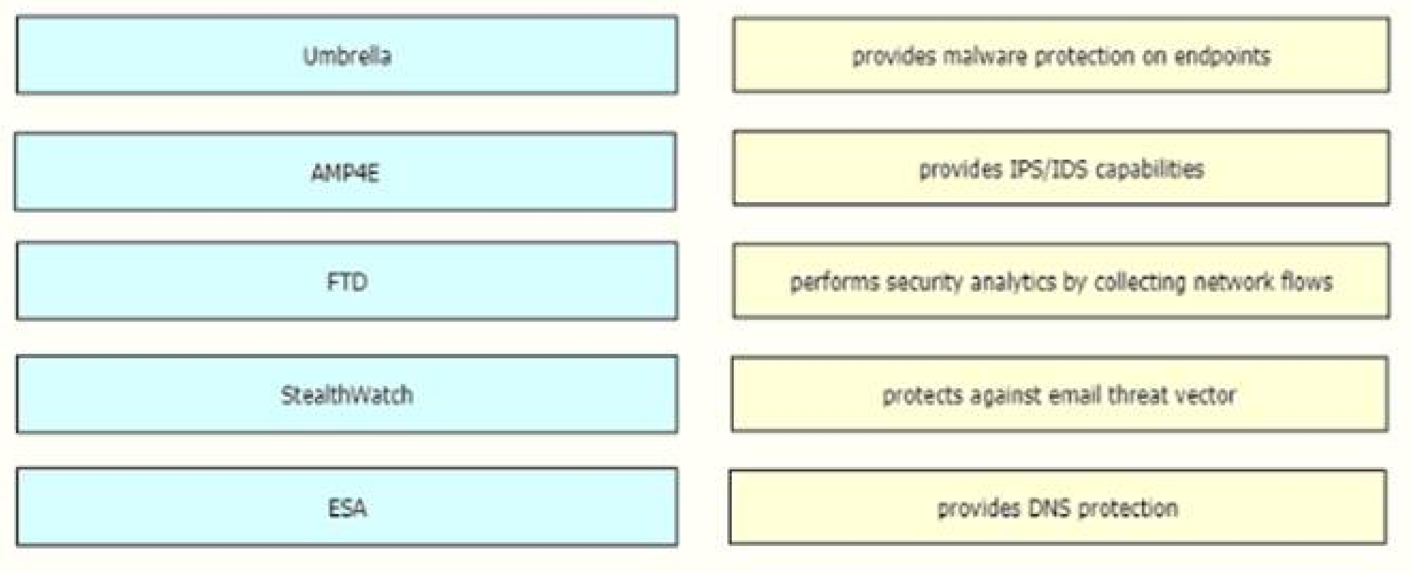
A. classifies traffic based on advanced application recognition
B. uses flexible NetFlow
C. classifies traffic based on the contextual identity of the endpoint rather than its IP address correct
D. assigns a VLAN to the endpoint

Answer: C

Explanation:
The Cisco TrustSec solution simplifies the provisioning and management of network access control through the use of software-defined segmentation to classify network traffic and enforce policies for more flexible access controls. Traffic classification is based on endpoint identity, not IP address, enabling policy change without net-work redesign.

NEW QUESTION 244

DRAG DROP - (Topic 1)
Drag and drop the threat defense solutions from the left onto their descriptions on the right.



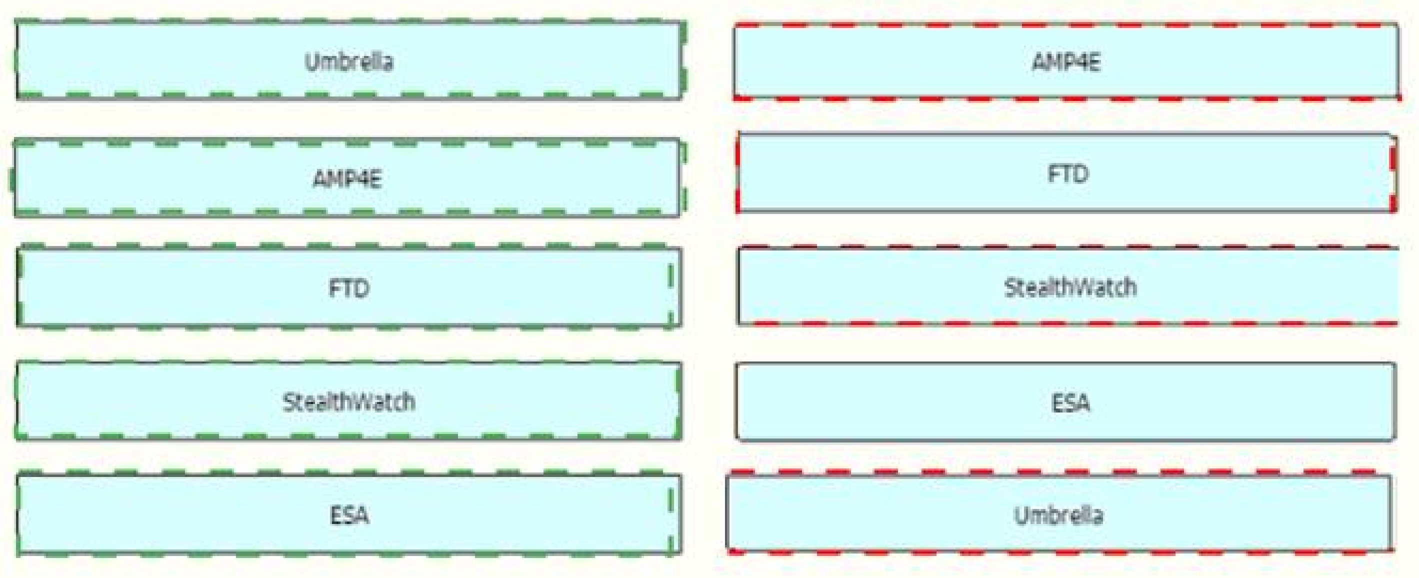
Umbrella
AMP4E
FTD
StealthWatch
ESA

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

A. Mastered
B. Not Mastered

Answer: A

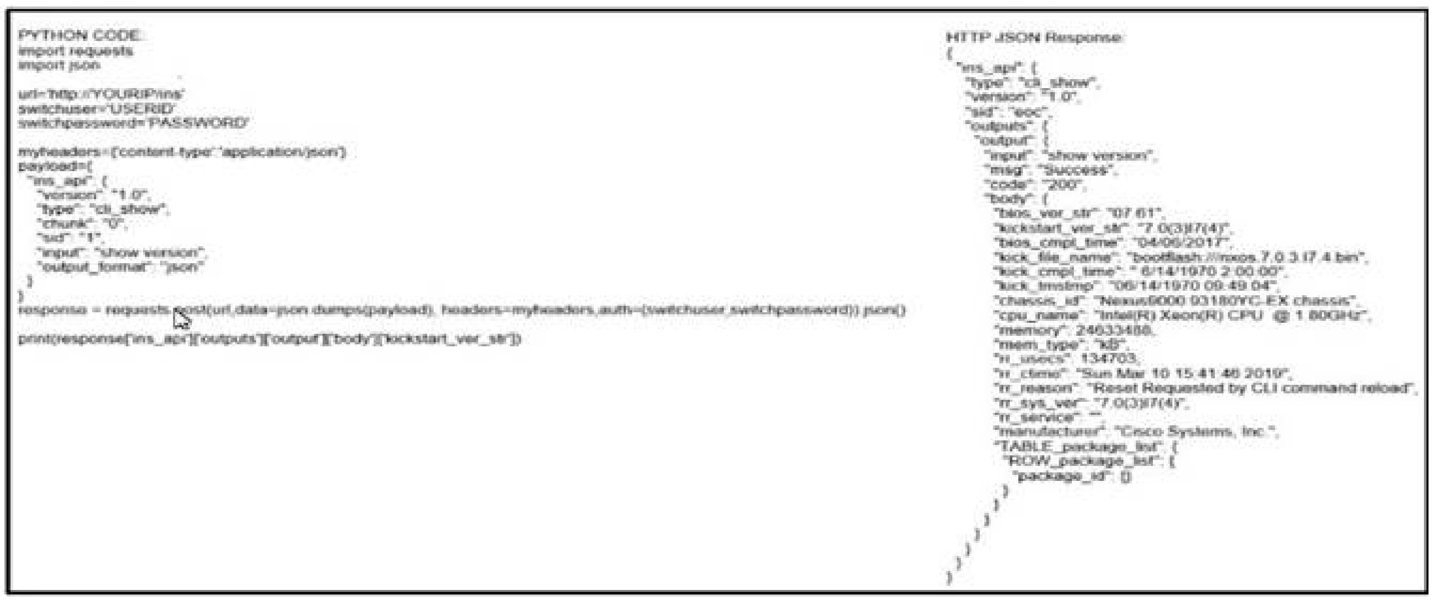
Explanation:



Umbrella
AMP4E
FTD
StealthWatch
ESA

AMP4E
FTD
StealthWatch
ESA
Umbrella

NEW QUESTION 247
- (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 249
- (Topic 1)
Which two components are supported by LISP? (Choose two.)

A. Proxy ETR
B. egress tunnel router

C. route reflector
D. HMAC algorithm
E. spoke

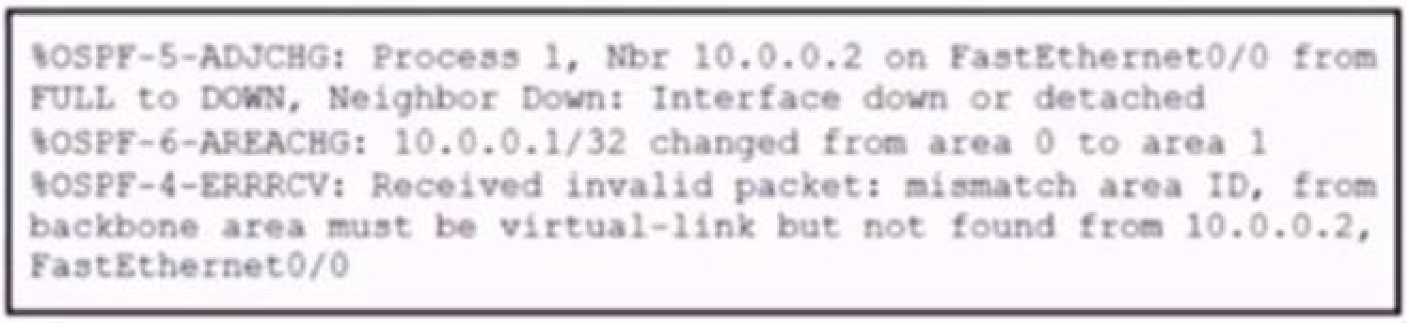
Answer: AB

NEW QUESTION 252
- (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 254
- (Topic 1)



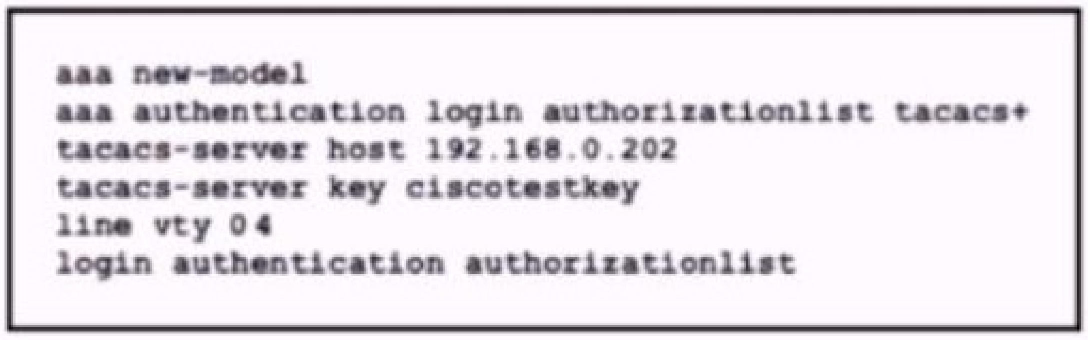
```
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.2 on FastEthernet0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
%OSPF-6-AREACHG: 10.0.0.1/32 changed from area 0 to area 1
%OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from
backbone area must be virtual-link but not found from 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 259
- (Topic 1)



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

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

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

Answer: B

NEW QUESTION 264
- (Topic 1)
Which algorithms are used to secure REST API from brute attacks and minimize the impact?

A. SHA-512 and SHA-384
B. MD5 algorithm-128 and SHA-384
C. SHA-1, SHA-256, and SHA-512
D. PBKDF2, BCrypt, and SCrypt

Answer: D

Explanation:
One of the best practices to secure REST APIs is using password hash.
Passwords must always be hashed to protect the system (or minimize the damage) even if it is compromised in some hacking attempts. There are many such hashing algorithms which can prove really effective for password security e.g. PBKDF2, bcrypt and scrypt algorithms.
Other ways to secure REST APIs are: Always use HTTPS, Never expose information on URLs
(Usernames, passwords, session tokens, and API keys should not appear in the URL), Adding Timestamp in Request, Using OAuth, Input Parameter Validation.
Reference: https://restfulapi.net/security-essentials/

NEW QUESTION 265
- (Topic 1)
Which protocol does REST API rely on to secure the communication channel?

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

Answer: B

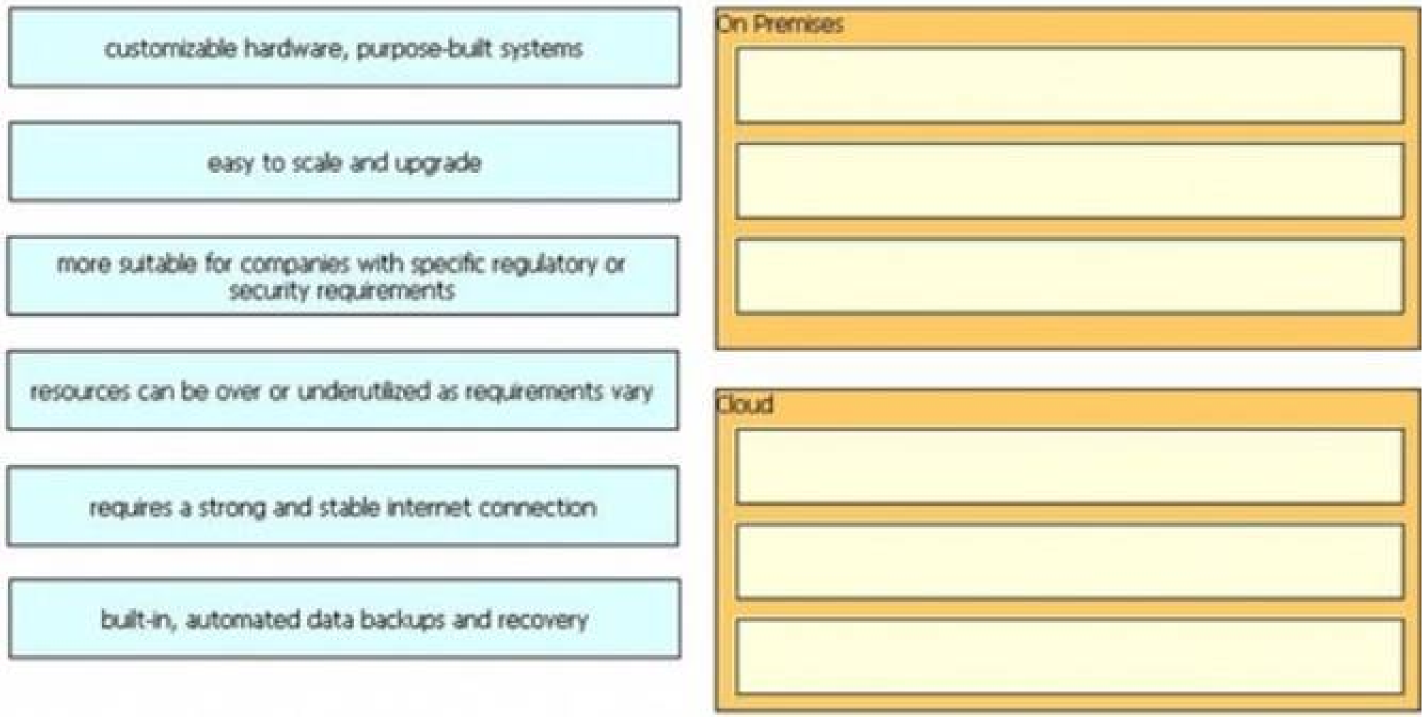
Explanation:
The REST API accepts and returns HTTP (not enabled by default) or HTTPS messages that contain JavaScript Object Notation (JSON) or Extensible Markup Language (XML) documents. You
can use any programming language to generate the messages and the JSON or XML documents that
contain the API methods or Managed Object (MO) descriptions.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_ API_Configuration_Guide_chapter_01.html

NEW QUESTION 268
- (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 273
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

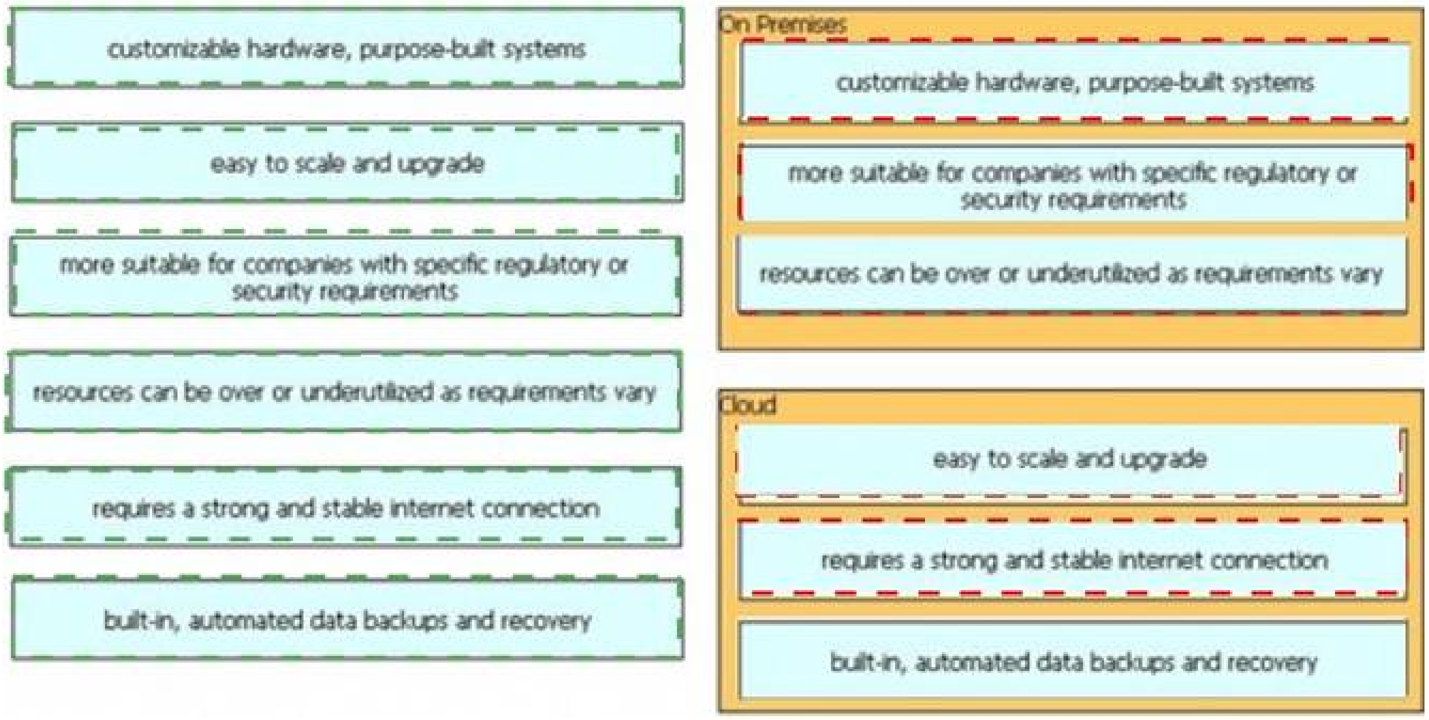
On Premises

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

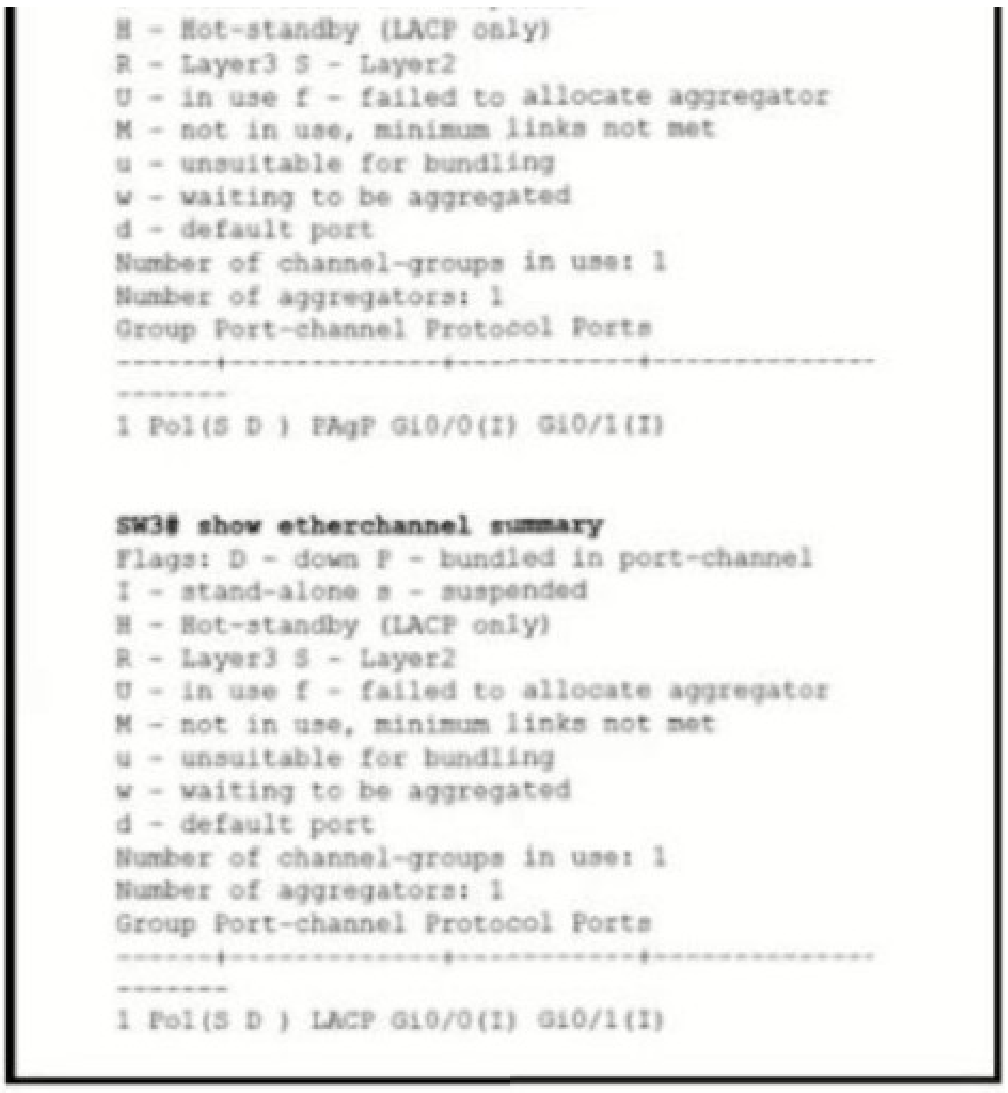
built-in, automated data backups and recovery

NEW QUESTION 275
- (Topic 1)
What are two characteristics of VXLAN? (Choose two)

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

Answer: AC

NEW QUESTION 278
- (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 282

- (Topic 1)
Which device makes the decision for a wireless client to roam?

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

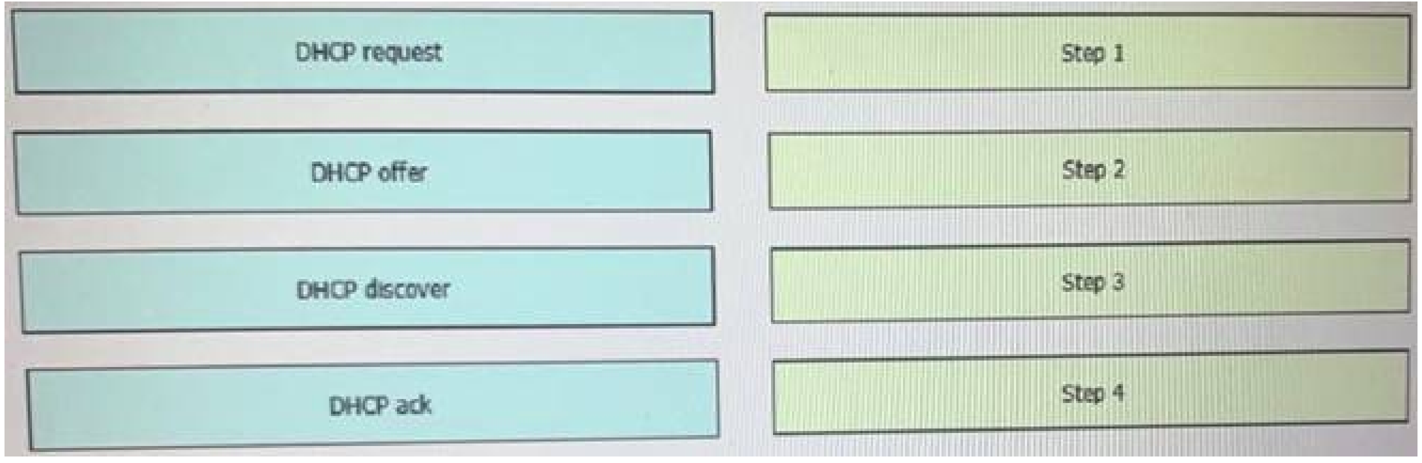
Answer: A

NEW QUESTION 284
- (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 288
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 292
- (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 296
- (Topic 1)
What are two differences between the RIB and the FIB? (Choose two.)

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

Answer: BE

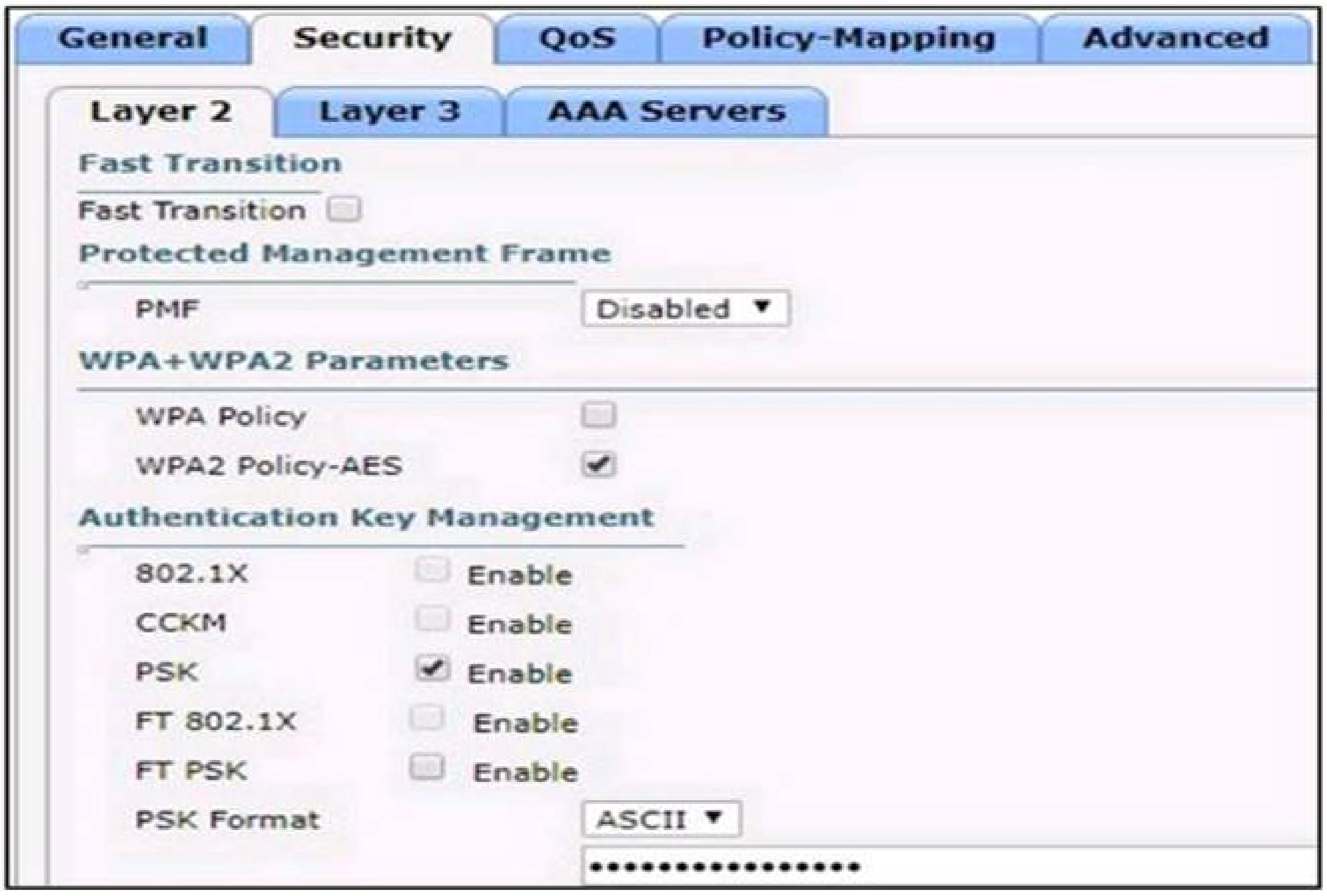
NEW QUESTION 300
- (Topic 1)
Which characteristic distinguishes Ansible from Chef?

A. Ansible lacs redundancy support for the master serve
B. Chef runs two masters in an active/active mode.

C. Ansible uses Ruby to manage configuration
D. Chef uses YAML to manage configurations.
E. Ansible pushes the configuration to the clien
F. Chef client pulls the configuration from the server.
G. The Ansible server can run on Linux, Unix or Window
H. The Chef server must run on Linux or Unix.

Answer: C

NEW QUESTION 302
- (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

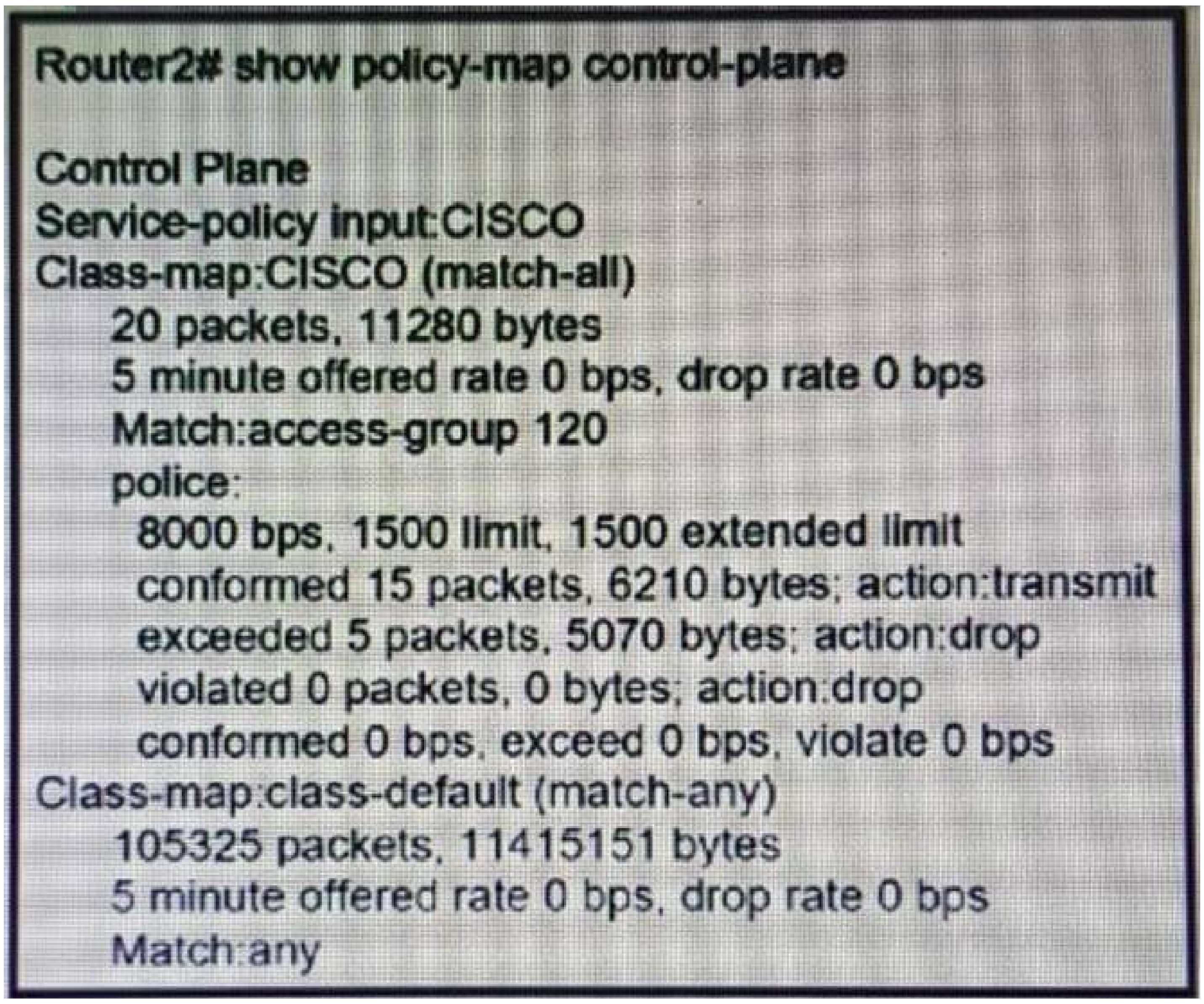
Answer: A

NEW QUESTION 306
- (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 310
- (Topic 1)



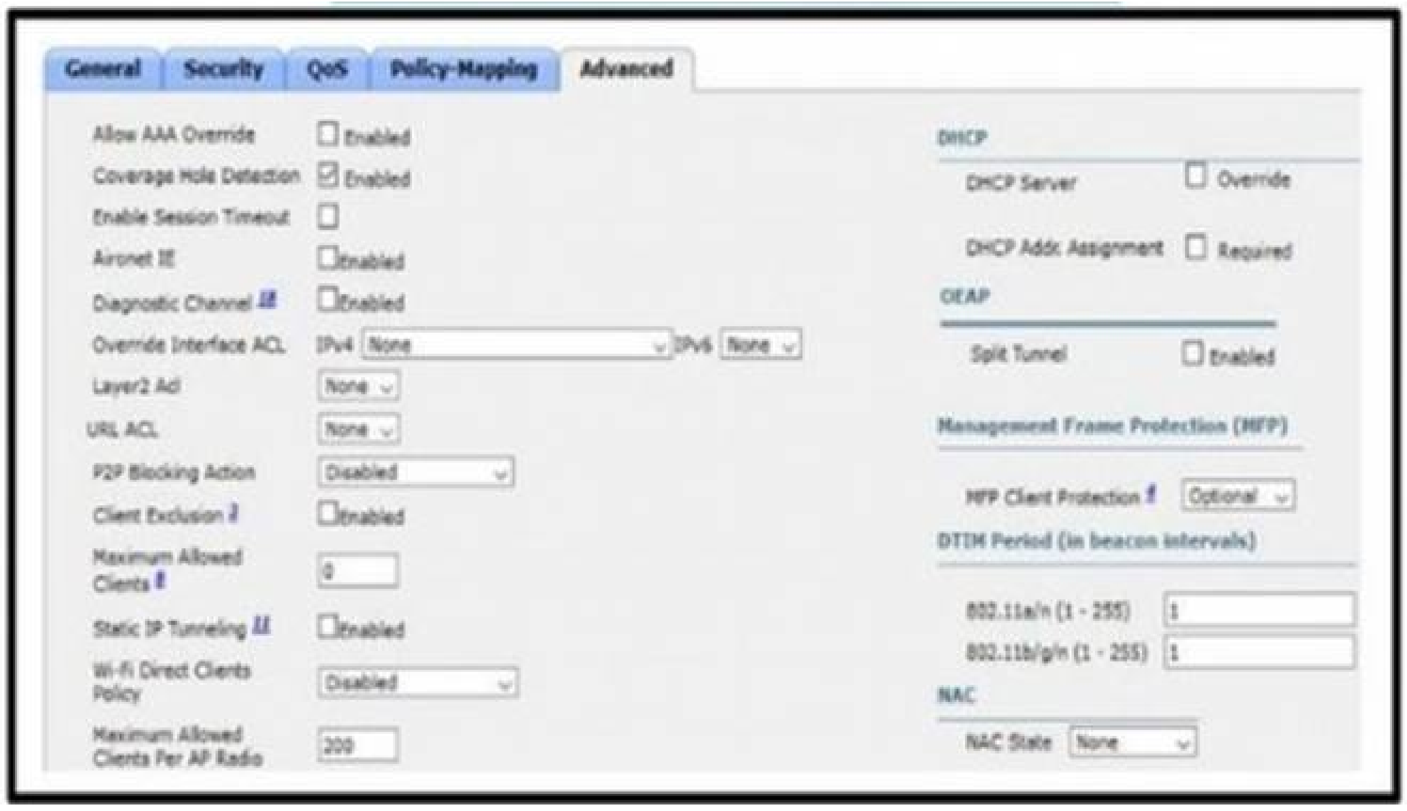
```
Router2# show policy-map control-plane

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

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

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

Answer: A

NEW QUESTION 315
- (Topic 1)



Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout □
Aironet IE □Enabled
Diagnostic Channel □Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion □Enabled
Maximum Allowed Clients 0
Static IP Tunneling □Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP
Split Tunnel □ Enabled

Management Frame Protection (MFP)
MFP Client Protection Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State None

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

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

Answer: B

NEW QUESTION 317
- (Topic 1)
If the noise floor is -90 dBm and wireless client is receiving a signal of -75 dBm, what is the SNR?

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

Answer: A

NEW QUESTION 319
- (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

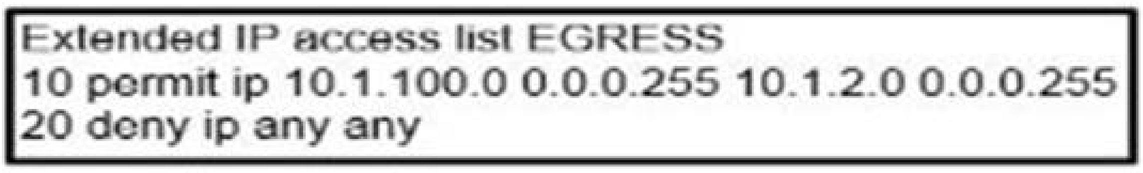
Explanation:
https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/c11-742008-00-cisco-amp-for-endpoints-wp-v2a.pdf

NEW QUESTION 324
- (Topic 1)
What is one fact about Cisco SD-Access wireless network deployments?

A. The access point is part of the fabric underlay
B. The WLC is part of the fabric underlay
C. The access point is part the fabric overlay
D. The wireless client is part of the fabric overlay

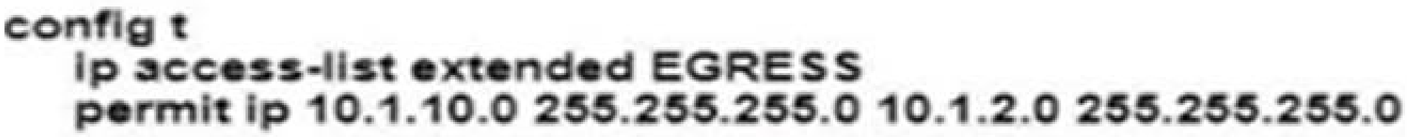
Answer: C

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



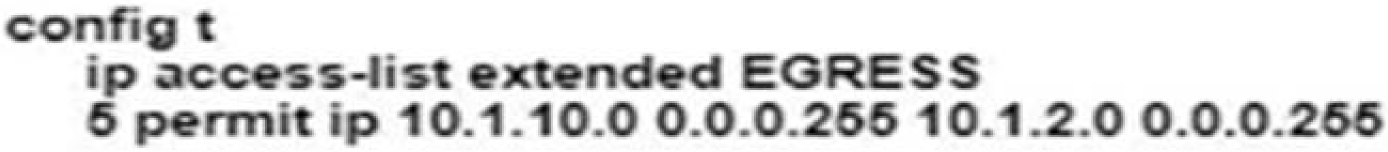
```
Extended IP access list EGRESS
10 permit ip 10.1.100.0 0.0.0.255 10.1.2.0 0.0.0.255
20 deny ip any any
```

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



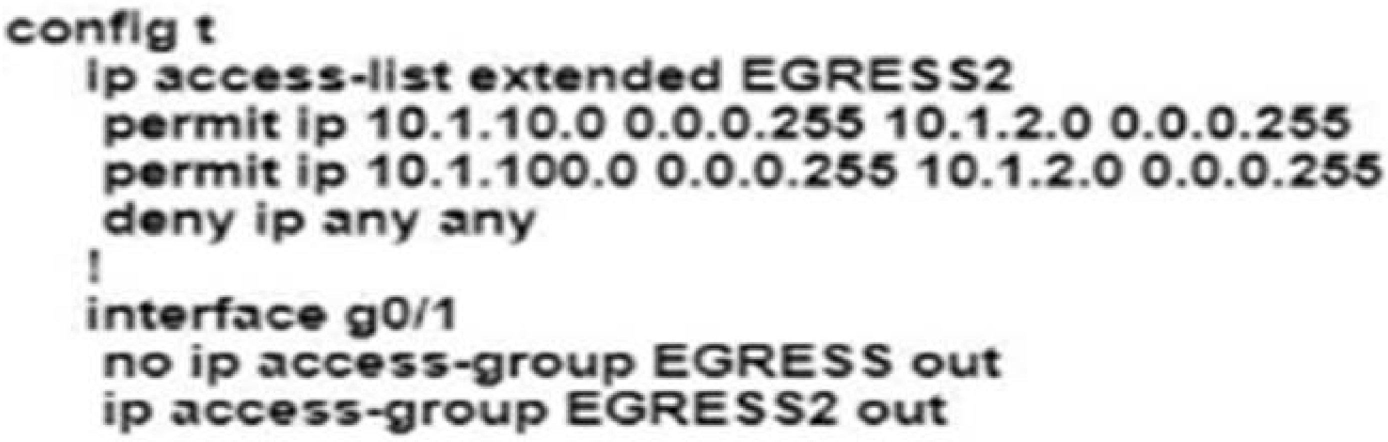
```
config t
    ip access-list extended EGRESS
    permit ip 10.1.10.0 255.255.255.0 10.1.2.0 255.255.255.0
```

B)



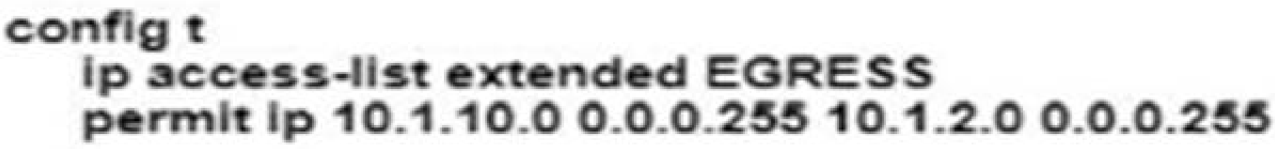
```
config t
    ip access-list extended EGRESS
    5 permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
```

C)



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

D)



```
config t
    ip access-list extended EGRESS
    permit ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
```

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

Answer: B

NEW QUESTION 329
- (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 333
- (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

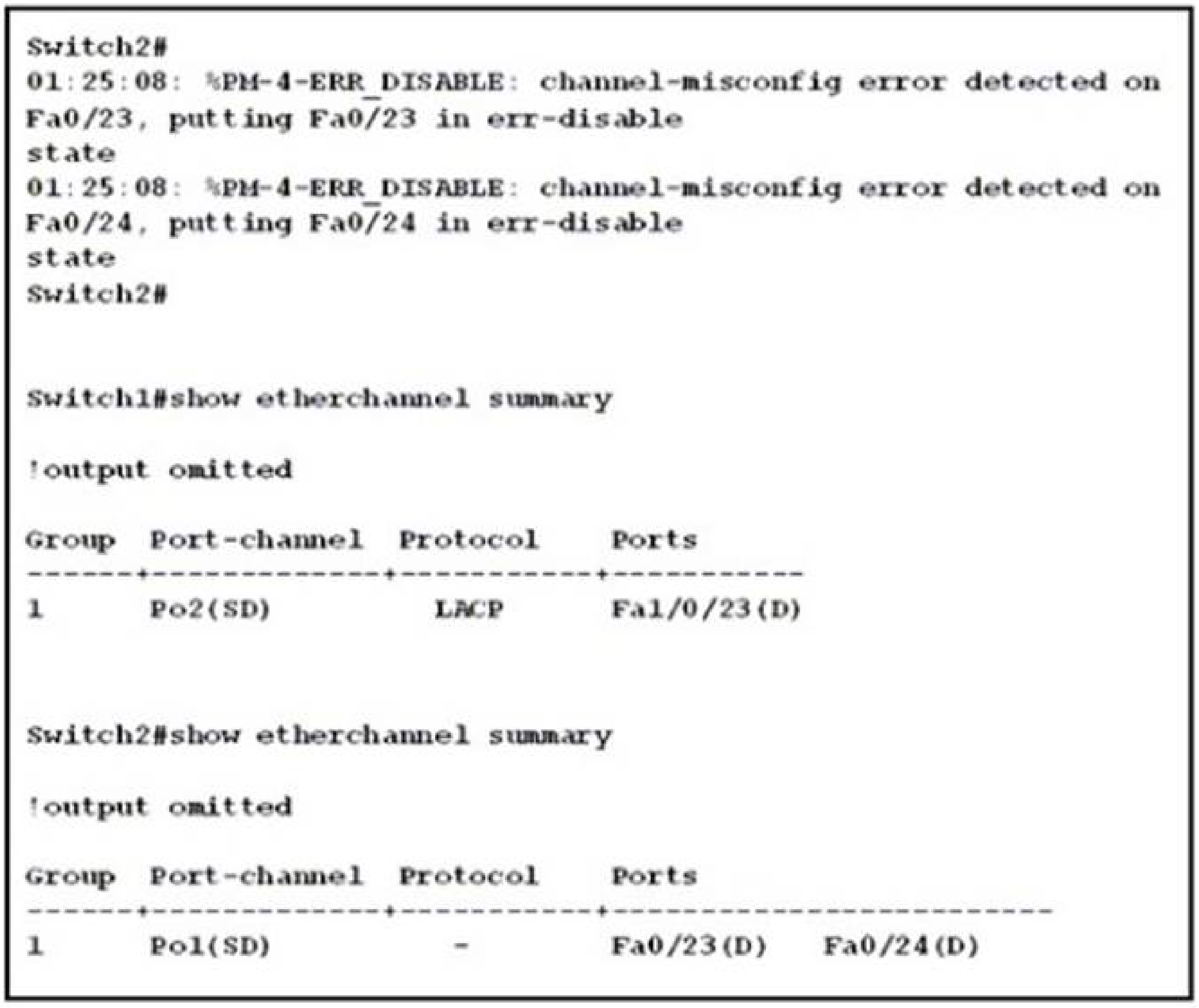
Explanation:
Fabric wireless controllers manage and control the fabric-mode APs using the same general model as the traditional local-mode controllers which offers the same operational advantages such as mobility control and radio resource management. A significant difference is that client traffic from 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 334
- (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 339
- (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)
```

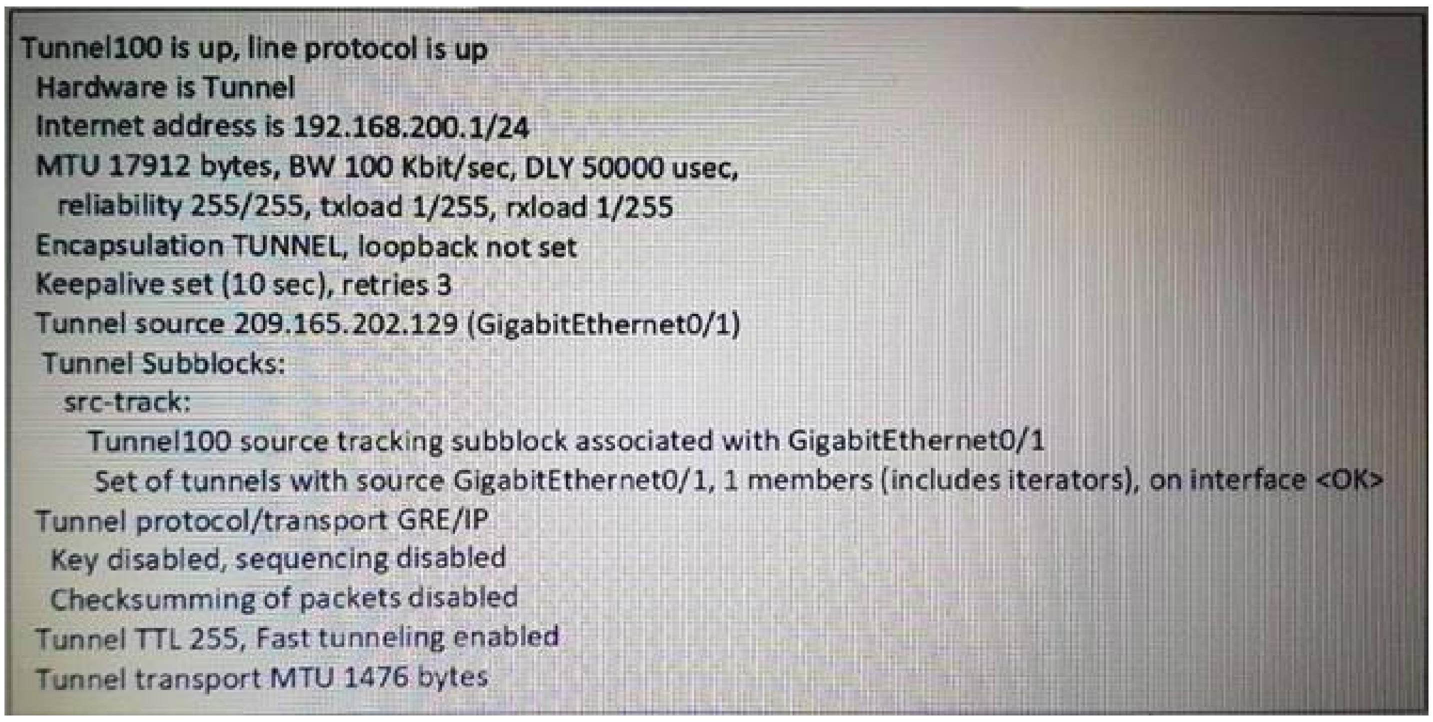
Refer to the exhibit. An engineer is configuring an EtherChannel between Switch1 and Switch2 and notices the console message on switch2. Based on the output, which action resolves this issue?

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 343
- (Topic 1)
Refer to the exhibit.



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

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

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

Answer: C

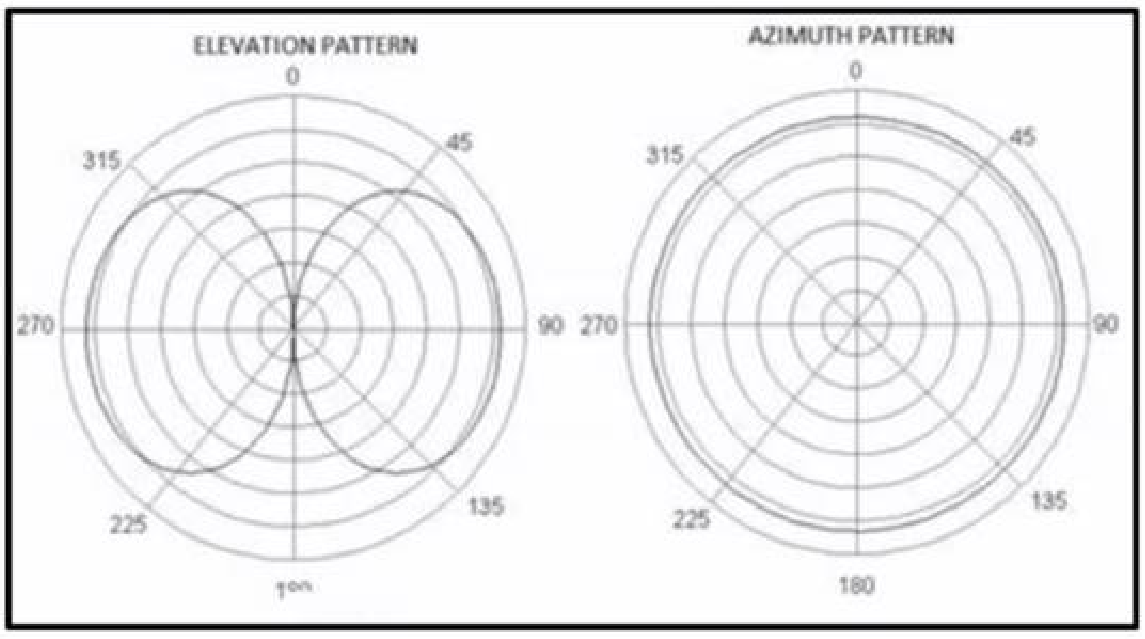
NEW QUESTION 346
- (Topic 1)
Which encryption hashing algorithm does NTP use for authentication?

A. SSL
B. MD5
C. AES128
D. AES256

Answer: B

Explanation:
An example of configuring NTP authentication is shown below: Router1(config)#ntp authentication-key 2 md5 itexamanswersRouter1(config)#ntp authenticateRouter1(config)#ntp trusted-key 2

NEW QUESTION 349
- (Topic 4)
Refer to the exhibit.



Which antenna emits this radiation pattern?

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

Answer: A

NEW QUESTION 352
- (Topic 4)
What is one characteristic of Cisco DNA Center and vManage northbound APIs?

A. They push configuration changes down to devices.
B. They implement the RESTCONF protocol.
C. They exchange XML-formatted content.
D. They implement the NETCONF protocol.

Answer: B

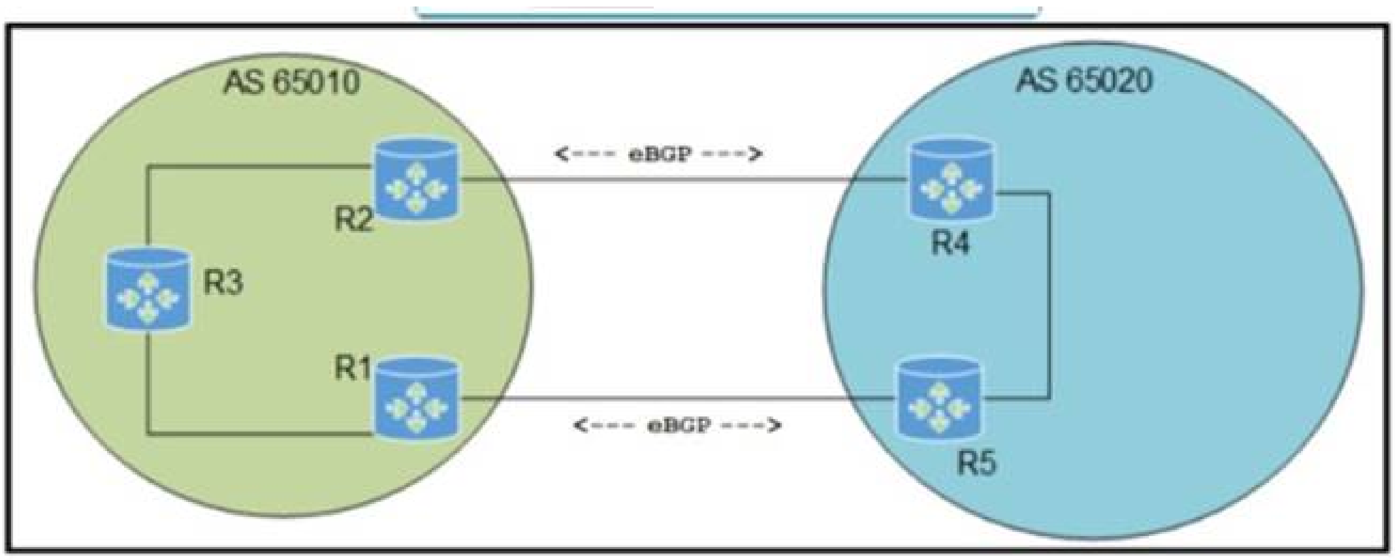
NEW QUESTION 354
- (Topic 4)
A network administrator is designing a new network for a company that has frequent power spikes. The company wants to ensure that employees can the best solution for the administrator to recommend?

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

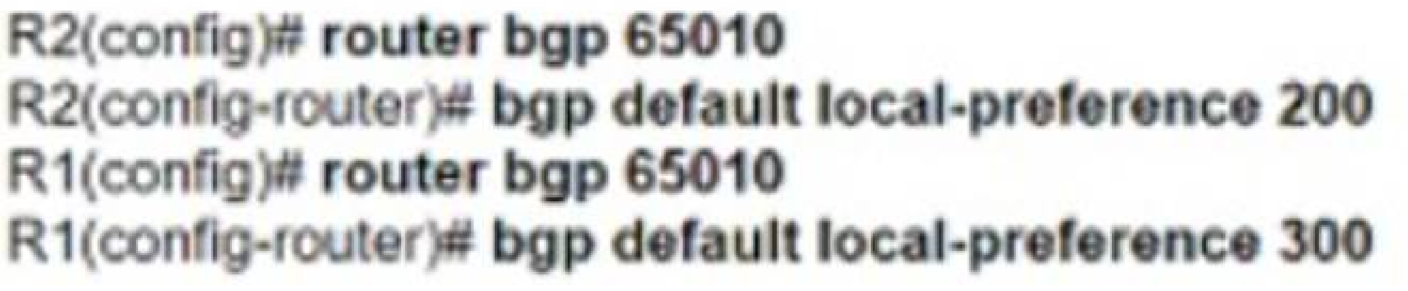
Answer: D

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

NEW QUESTION 358
- (Topic 4)

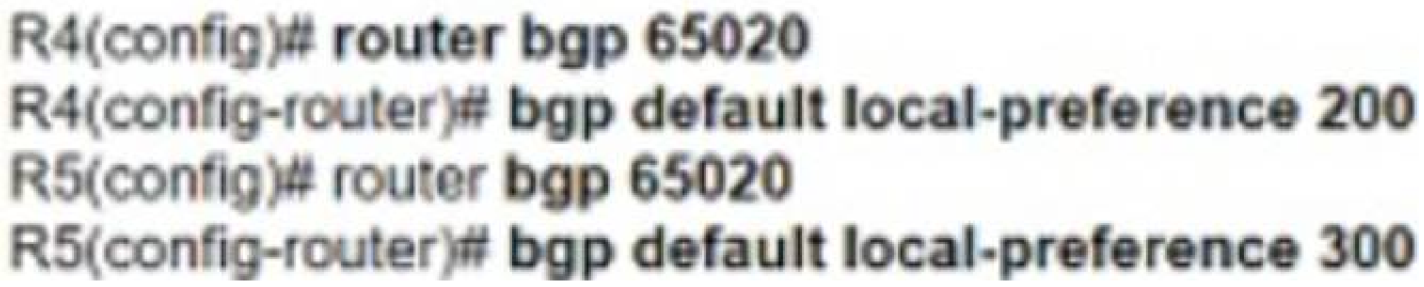


Refer to the exhibit. Which configuration must be applied to ensure that the preferred path for traffic from AS 65010 toward AS 65020 uses the R2 to R4 path?
A)



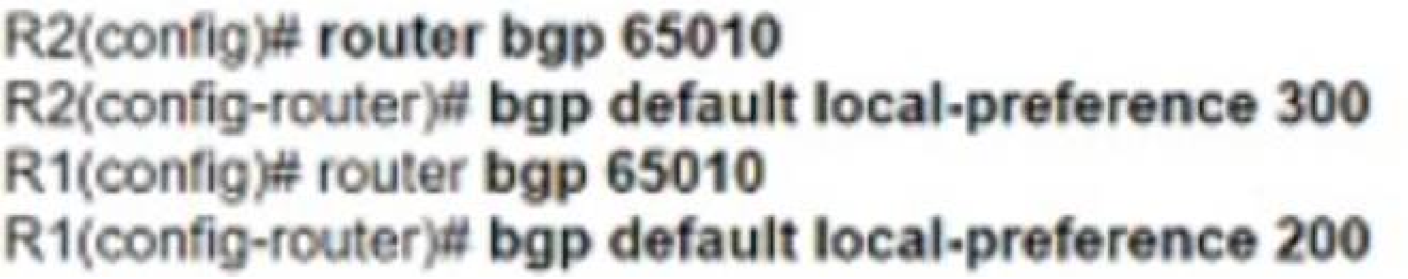
```
R2(config)# router bgp 65010
R2(config-router)# bgp default local-preference 200
R1(config)# router bgp 65010
R1(config-router)# bgp default local-preference 300
```

B)



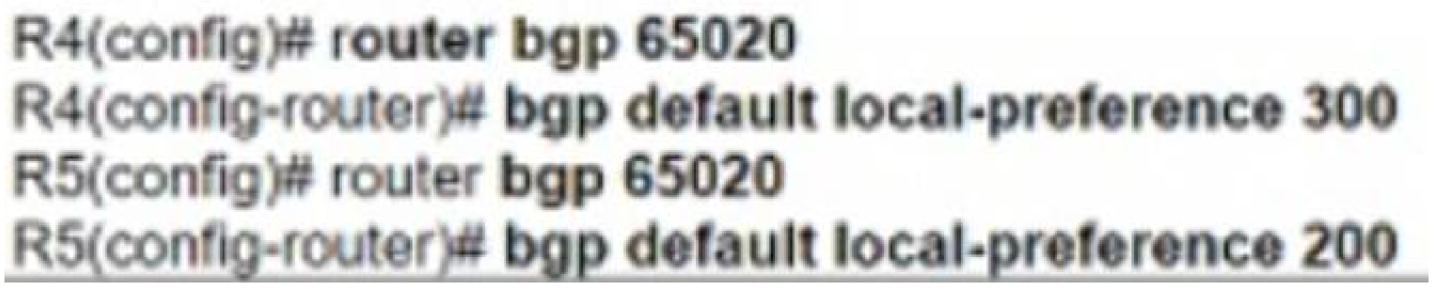
```
R4(config)# router bgp 65020
R4(config-router)# bgp default local-preference 200
R5(config)# router bgp 65020
R5(config-router)# bgp default local-preference 300
```

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

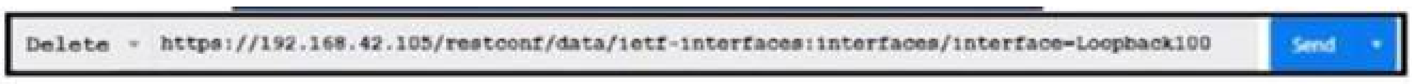
Answer: C

NEW QUESTION 363
- (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 367
- (Topic 4)
Refer to the exhibit.



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

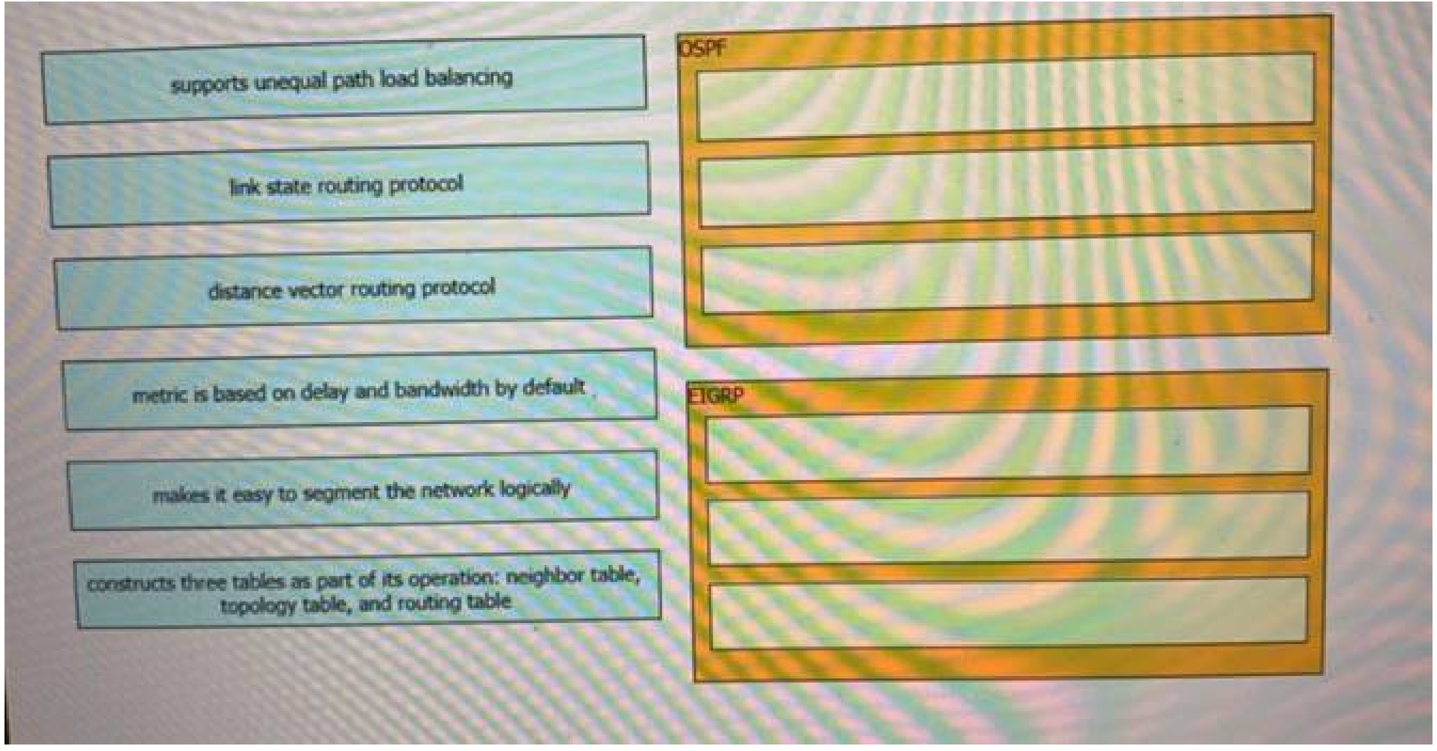
What does the response "204 No Content mean for the REST API request?

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 369
DRAG DROP - (Topic 4)
Drag the drop the description from the left onto the routing protocol they describe on the right.



supports unequal path load balancing

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

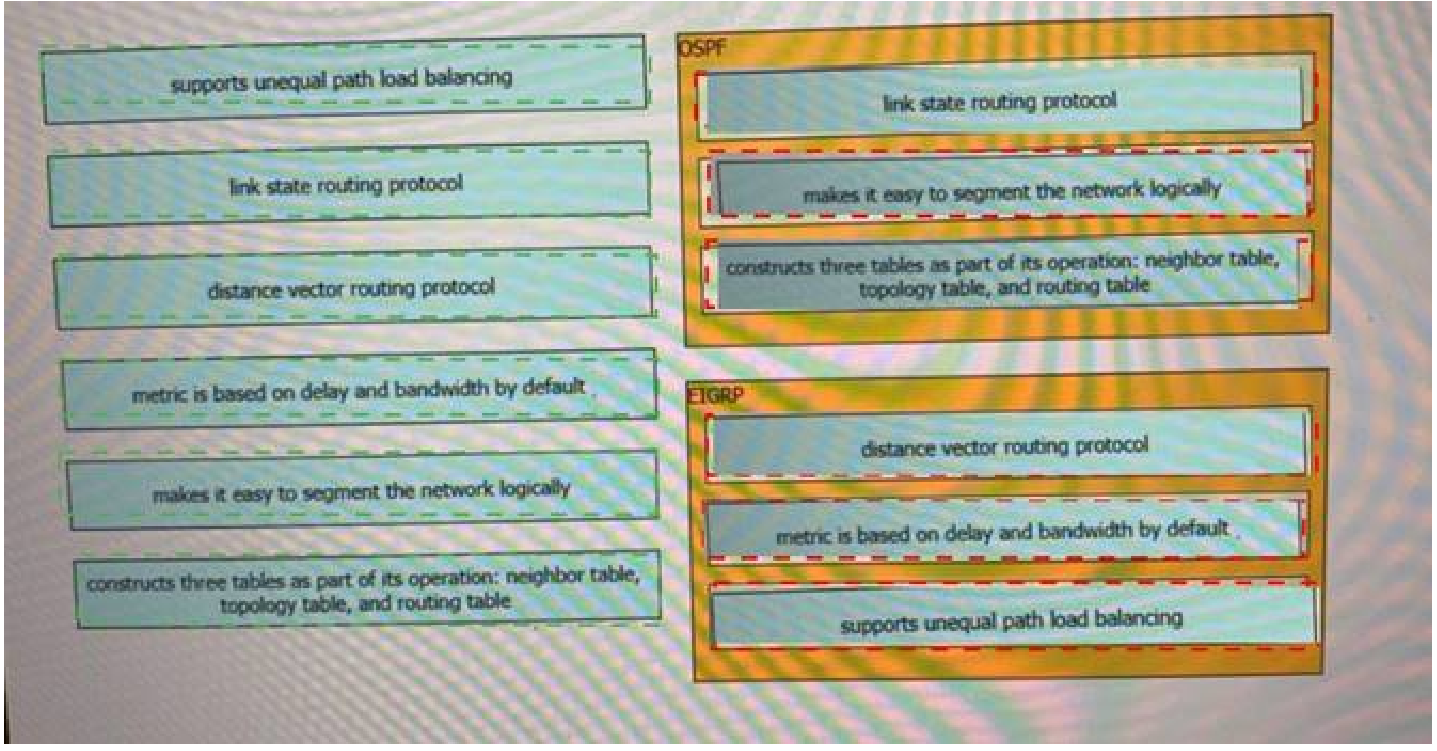
OSPF

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

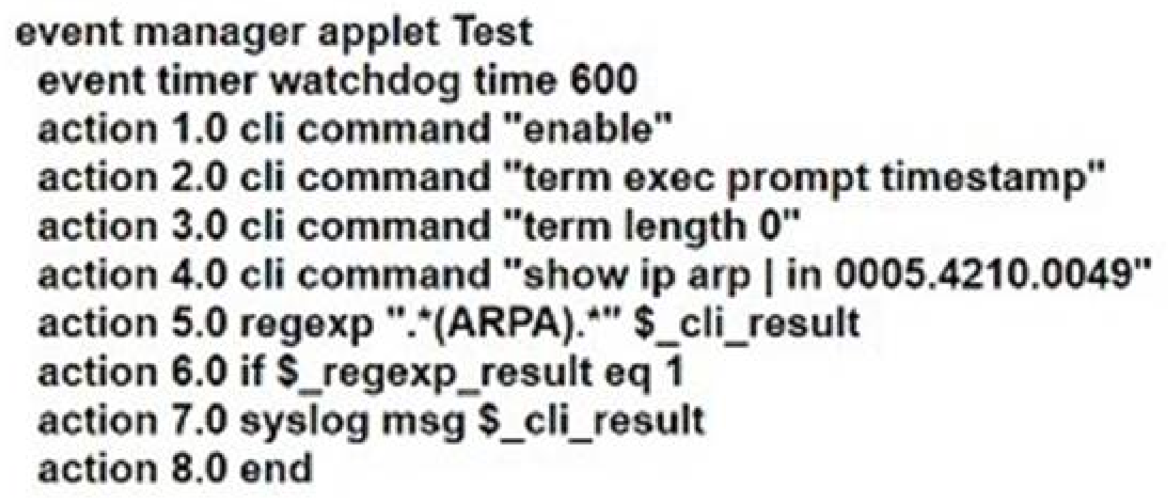
EIGRP

distance vector routing protocol

metric is based on delay and bandwidth by default

supports unequal path load balancing

NEW QUESTION 373
- (Topic 4)
An engineer applies this EEM applet to a router:



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

What does the applet accomplish?

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

Answer: B

NEW QUESTION 374
- (Topic 4)
Which action limits the total amount of memory and CPU that is used by a collection of VMs?

A. Place the collection of VMs in a resource pool.
B. Place the collection of VMs in a vApp.
C. Limit the amount of memory and CPU that is available to the cluster.
D. Limit the amount of memory and CPU that is available to the individual VMs.

Answer: A

NEW QUESTION 378
- (Topic 4)
In a Cisco SD-Access wireless environment, which device is responsible for hosting the anycast gateway?

A. fusion router
B. control plane node
C. fabric border node
D. fabric edge node

Answer: D

NEW QUESTION 381
- (Topic 4)
How do the RIB and the FIB differ?

A. FIB contains routes learned through a dynamic routing protocol, and the RIB contains routes that are static or directly connected.
B. RIB contains the interface for a destination, and the FIB contains the next hop information.
C. FIB is derived from the control plane, and the RIB is derived from the data plane.
D. RIB is derived from the control plane, and the FIB is derived from the RIB.

Answer: D

NEW QUESTION 382
- (Topic 4)
What does the statement print(format(0.8, '.0%')) display?

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

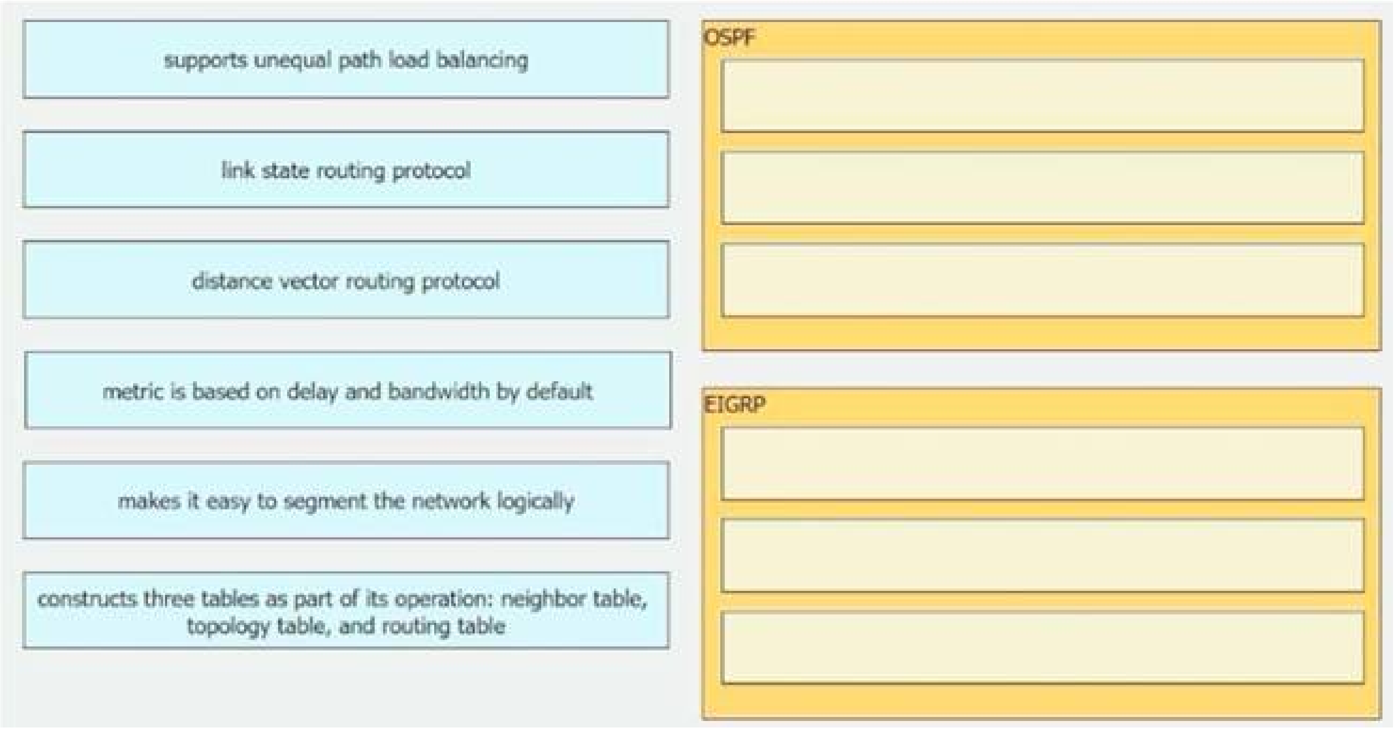
Answer: B

NEW QUESTION 386
- (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 387
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

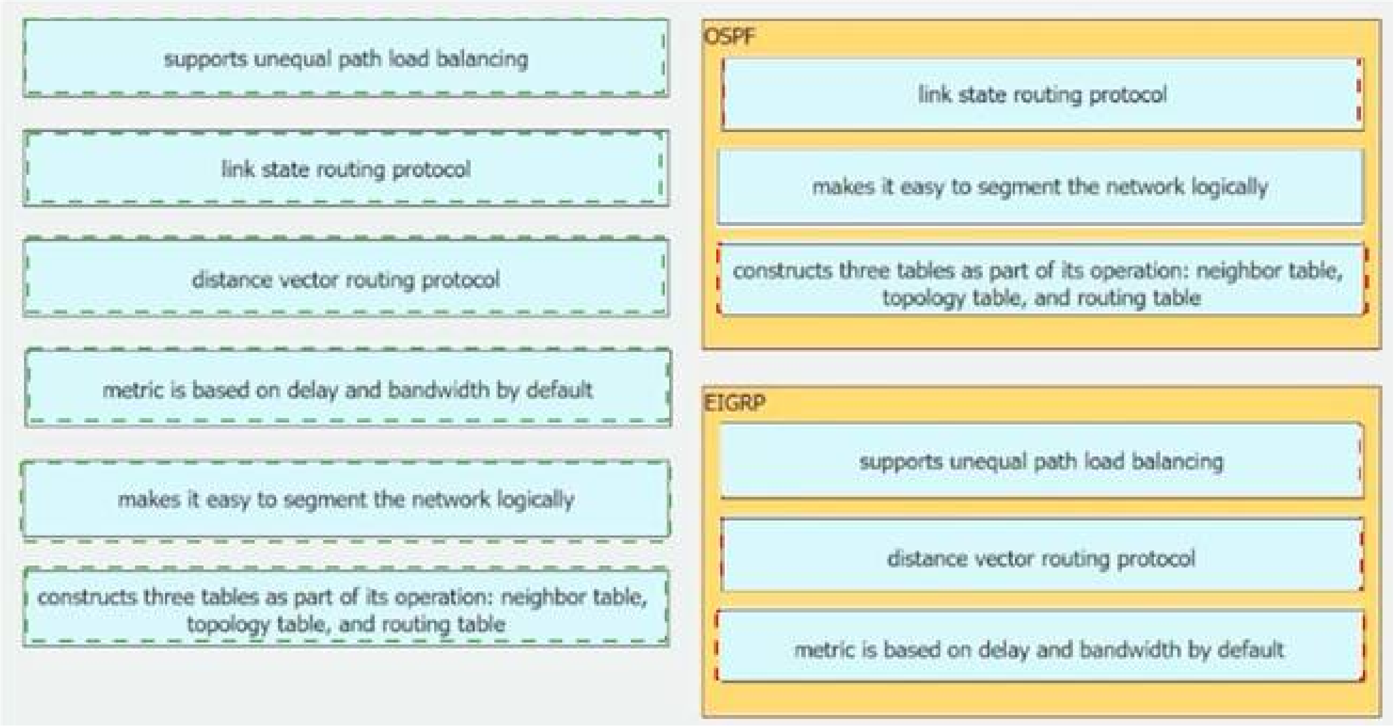
OSPF

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

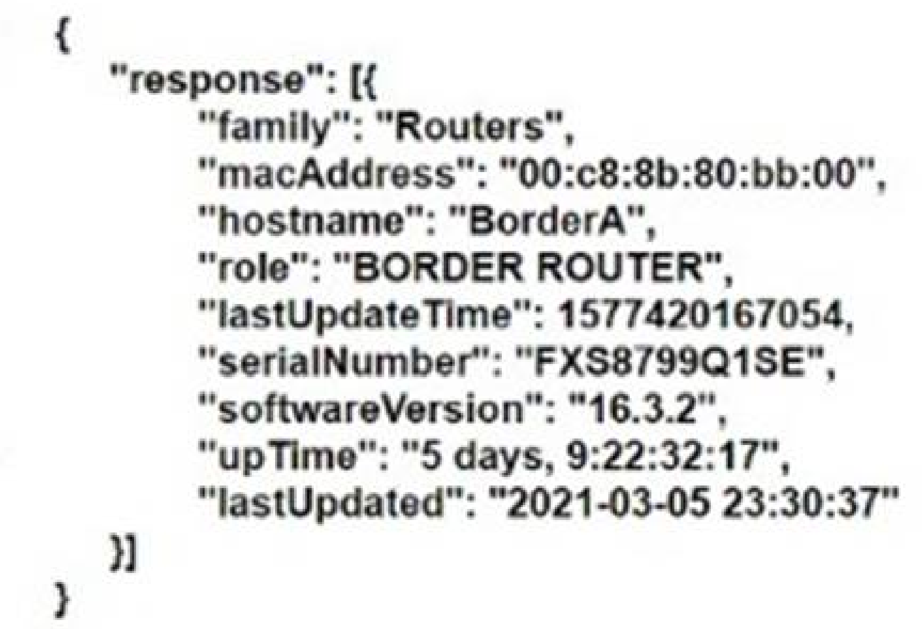
EIGRP

supports unequal path load balancing

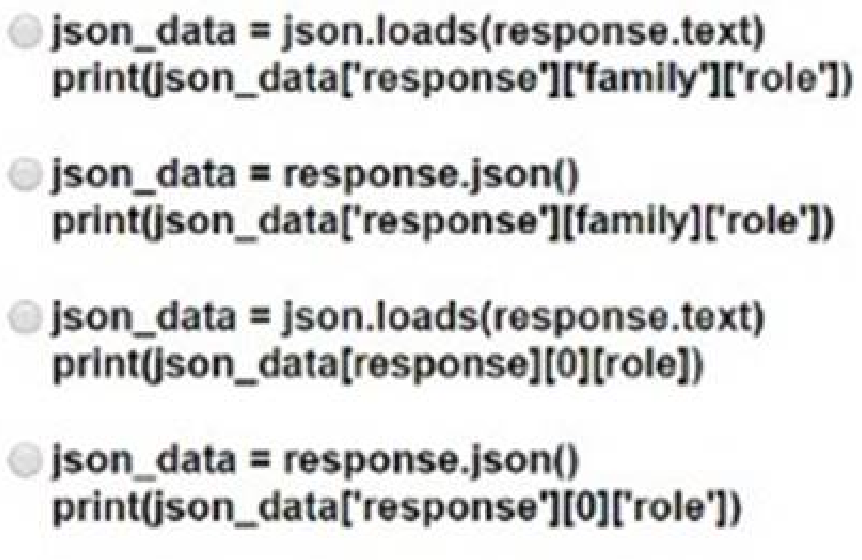
distance vector routing protocol

metric is based on delay and bandwidth by default

NEW QUESTION 392
- (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 397
- (Topic 4)
Which of the following protocols has a default administrative distance value of 90?

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

Answer: B

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

NEW QUESTION 398
- (Topic 4)
What do Chef and Ansible have in common?

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

Answer: B

NEW QUESTION 401
- (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 404
- (Topic 4)
A technician is assisting a user who cannot connect to a website. The technician attempts to ping the default gateway and DNS server of the workstation. According to troubleshooting methodology, this is an example of:

A. a divide-and-conquer approach.
B. a bottom-up approach.
C. a top-to-bottom approach.
D. implementing a solution.

Answer: C

Explanation:
This is because a top-to-bottom approach is a troubleshooting methodology that starts from the highest layer of the OSI model and works its way down to the lowest layer. The technician is using this approach by first testing the network layer connectivity with the ping command, which uses the ICMP protocol. If the ping

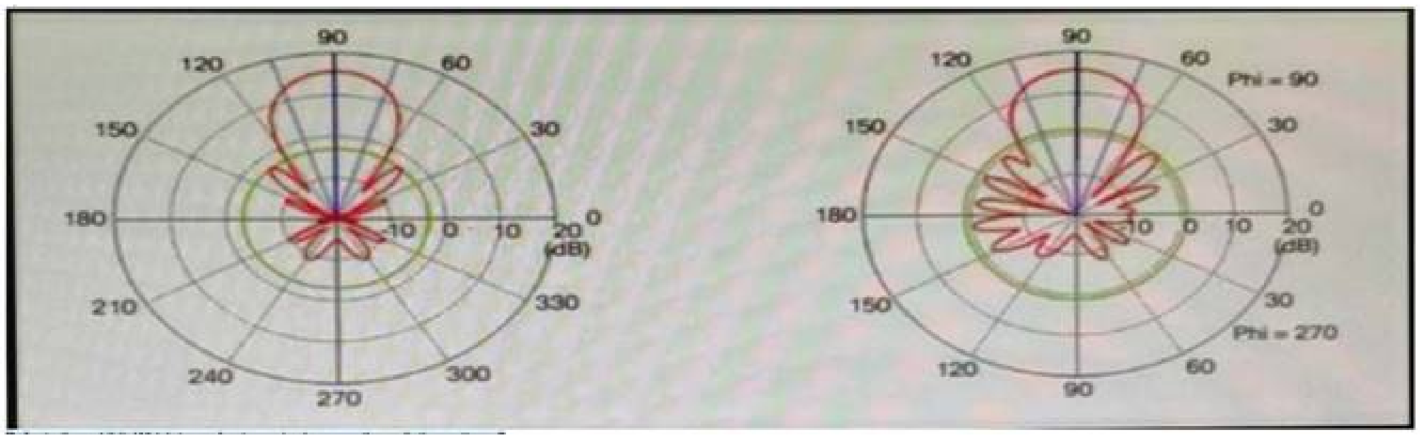
is successful, the technician can move on to the next layer, such as the transport layer or the application layer. If the ping fails, the technician can troubleshoot the lower layers, such as the data link layer or the physical layer. The source of this answer is the Cisco ENCOR v1.1 course, module 10, lesson 10.3: Applying Troubleshooting Methodologies.

NEW QUESTION 406
- (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 409
- (Topic 4)
Refer to the exhibit.



Which type of antenna is shown on the radiation patterns?

A. Yagi
B. dipole
C. patch
D. omnidirectional

Answer: A

NEW QUESTION 412
- (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 413
- (Topic 4)
Which Cisco WLC feature allows a wireless device to perform a Layer 3 roam between two separate controllers without changing the client IP address?

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

Answer: B

NEW QUESTION 417
- (Topic 4)
Which QoS queuing method transmits packets out of the interface in the order the packets arrive?

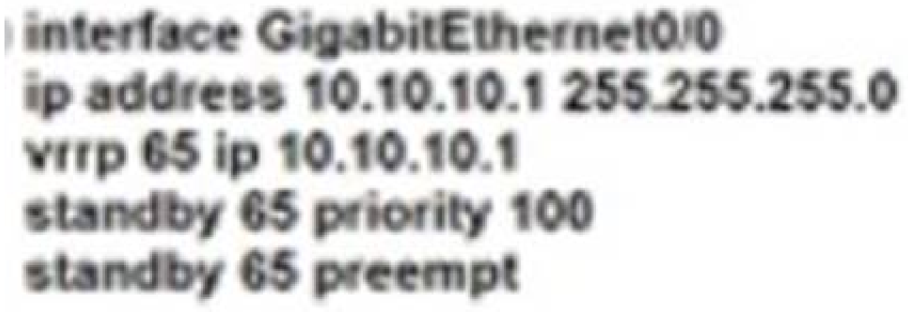
A. custom
B. weighted- fair
C. FIFO
D. priority

Answer: C

NEW QUESTION 418
- (Topic 4)

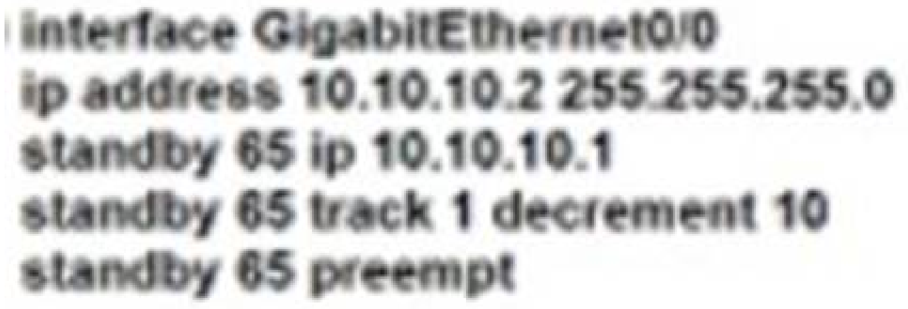
An engineer must configure GigabitEthernet 0/0 for VRRP group 65. The rouler must assume the primary rote when it has the highest priority in the group. Which command set must be applied?

A)



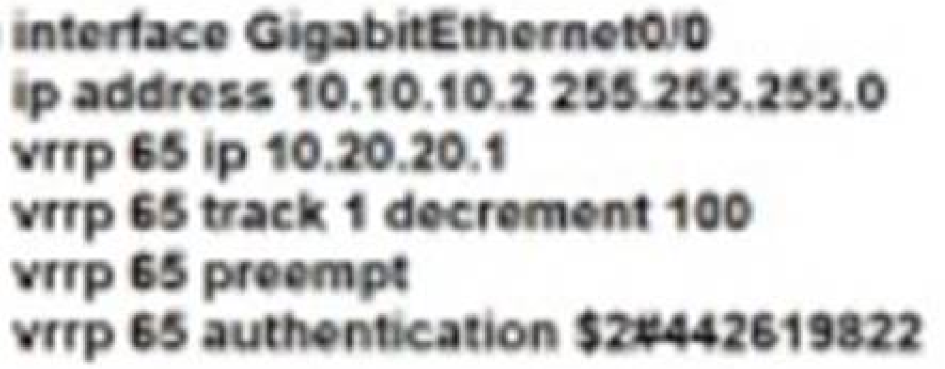
```
interface GigabitEthernet0/0
ip address 10.10.10.1 255.255.255.0
vrrp 65 ip 10.10.10.1
standby 65 priority 100
standby 65 preempt
```

B)



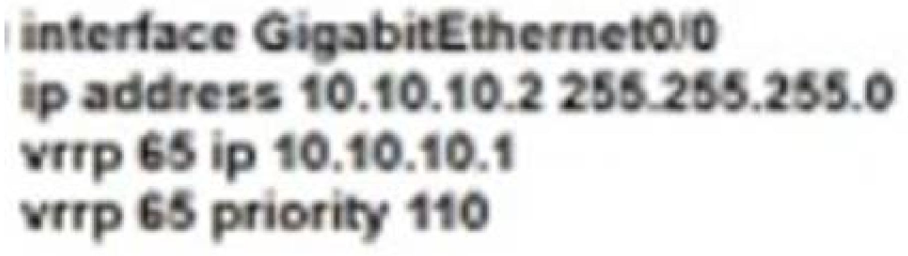
```
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.255.0
standby 65 ip 10.10.10.1
standby 65 track 1 decrement 10
standby 65 preempt
```

C)



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

D)



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

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

Answer: D

NEW QUESTION 419
- (Topic 4)
How is traffic classified when using Cisco TrustSec technology?

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

Answer: D

NEW QUESTION 421
- (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:

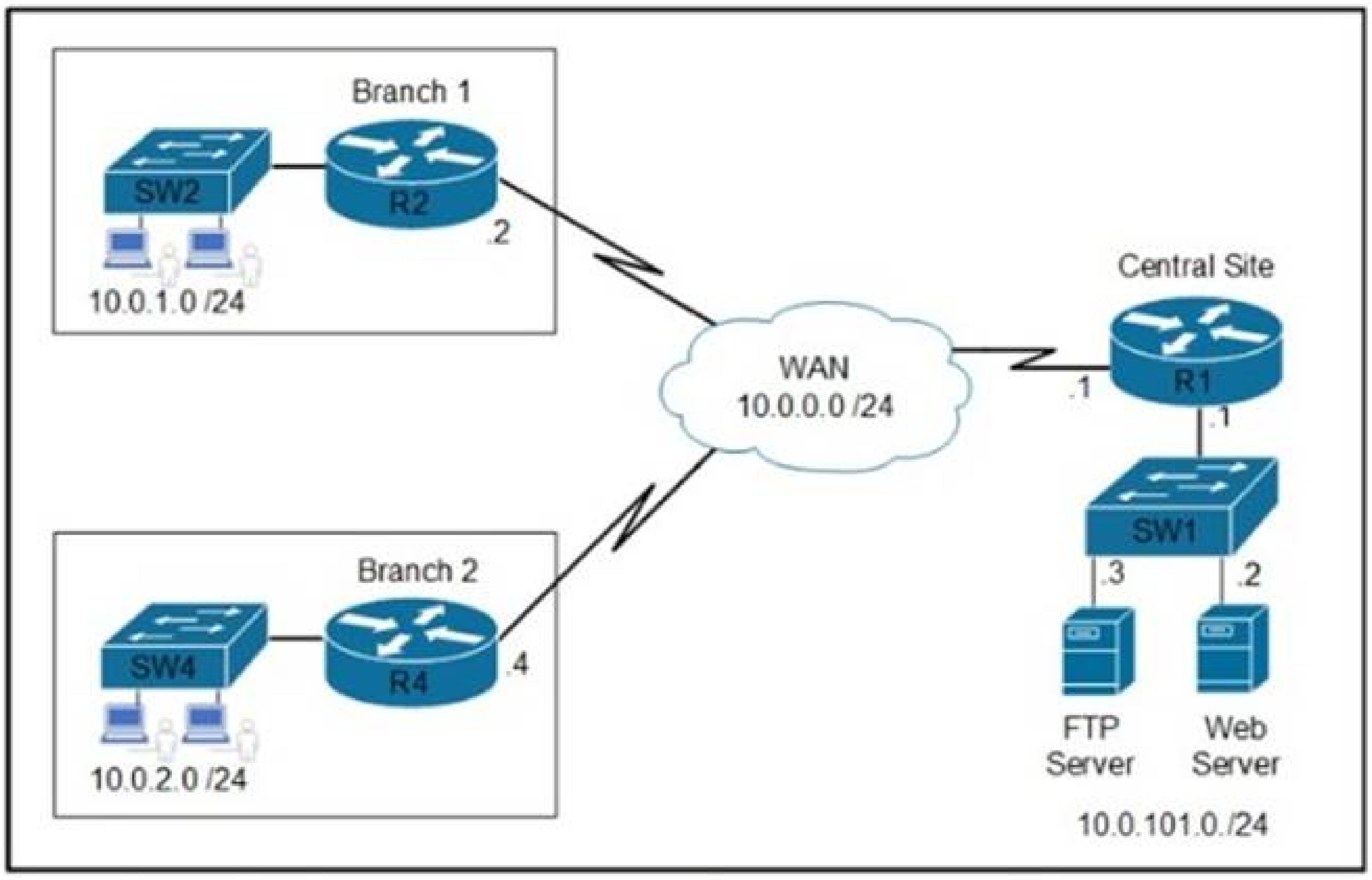
Source 1: https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-1000v-switch-vmware-vsphere/at_a_glance_c45-532467.pdf
Source 2: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/vm_fex/vmware/gui/confi g_guide/2-1/b_GUI_VMware_VM-FEX_UCSM_Configuration_Guide_2_1/b_GUI_VMware_VM-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

NEW QUESTION 422
- (Topic 4)
Why does the vBond orchestrator have a public IP?
to enable vBond to team the public IP of WAN Edge devices that are behind NAT gateways or in private address space

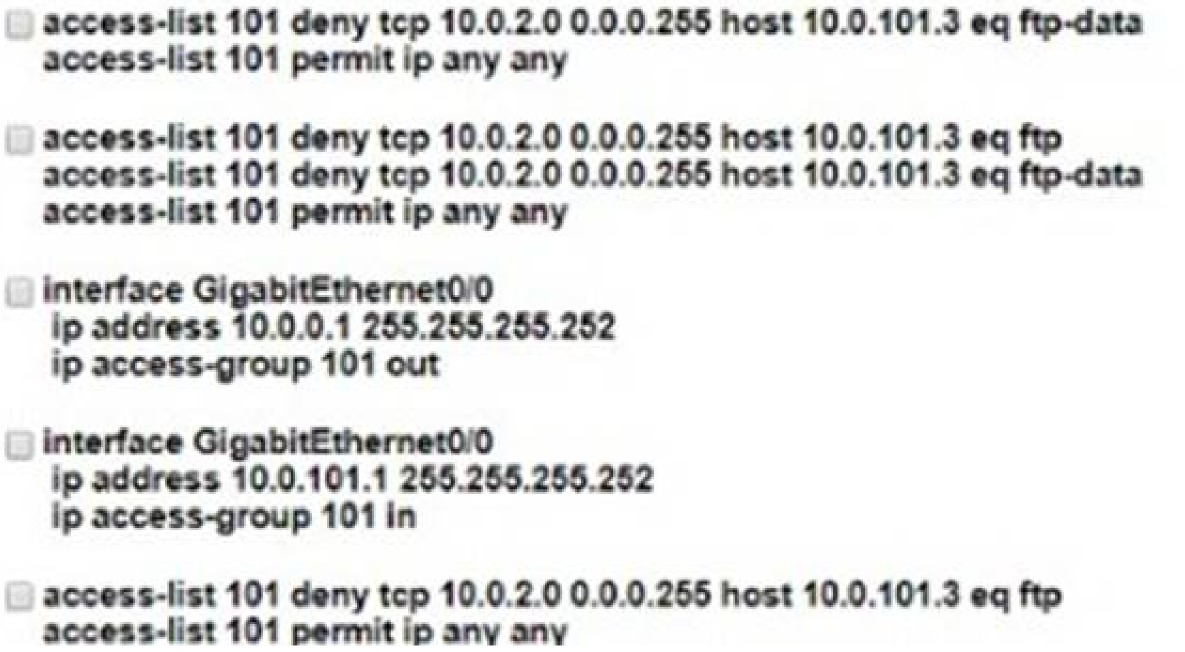
A. to facilitate downloading and distribution of operational and security patches
B. to allow for global reachability from all WAN Edges in the Cisco SD-WAN and
C. to facilitate NAT traversal to provide access
D. to Cisco Smart Licensing servers for license enablement

Answer: C

NEW QUESTION 427
- (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)

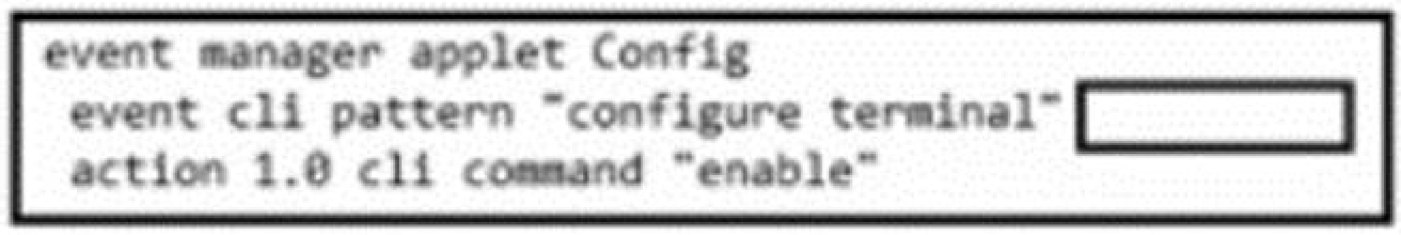


```
□ access-list 101 deny tcp 10.0.2.0 0.0.0.255 host 10.0.101.3 eq ftp-data
  access-list 101 permit ip any any

□ 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 432
- (Topic 4)



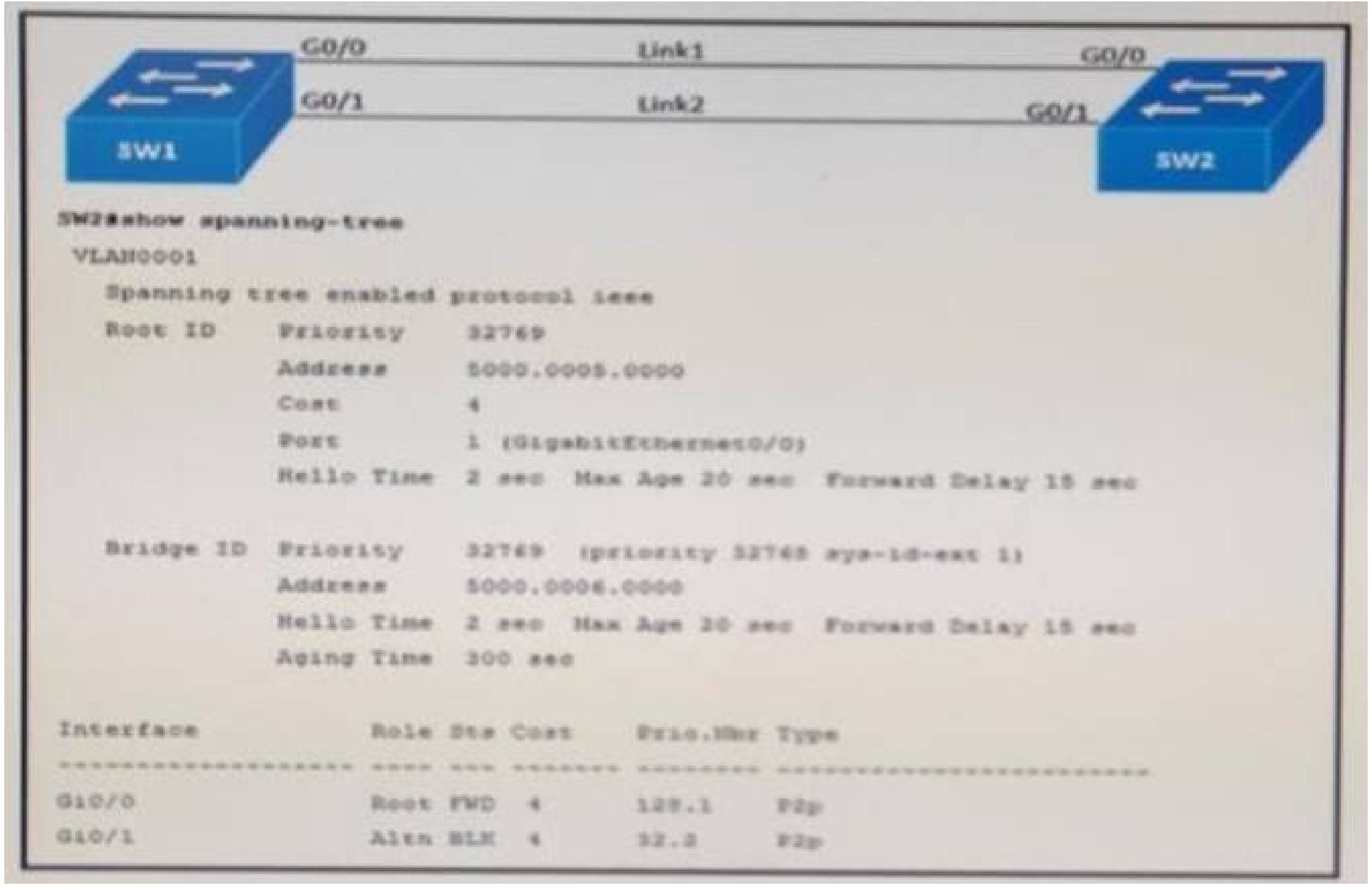
```
event manager applet Config
 event cli pattern "configure terminal" □
 action 1.0 cli command "enable"
```

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 436
- (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 438
- (Topic 4)
A customer wants to connect a device to an autonomous Cisco AP configured as a WGB. The WGB is configured properly: however, it fails to associate to a CAPWAP- enabled AP. Which change must be applied in the advanced WLAN settings to resolve this issue?

A. Enable Aironet IE.
B. Enable passive client.
C. Disable AAA override.
D. Disable FlexConnect local switching.

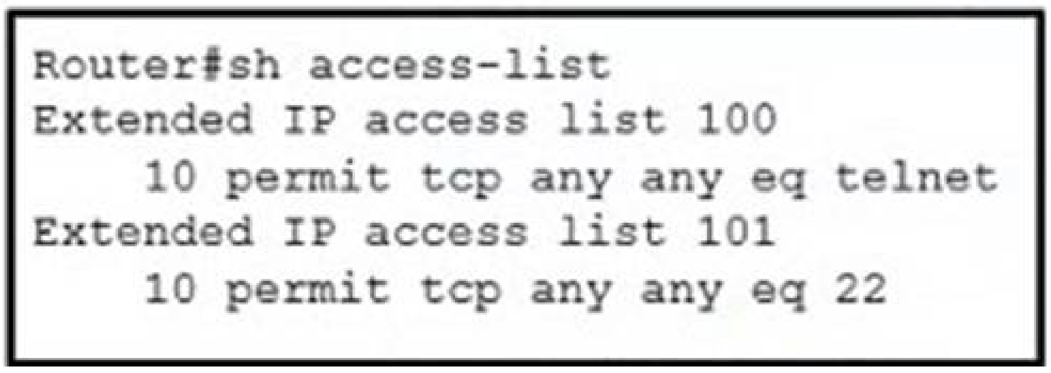
Answer: A

NEW QUESTION 441
- (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

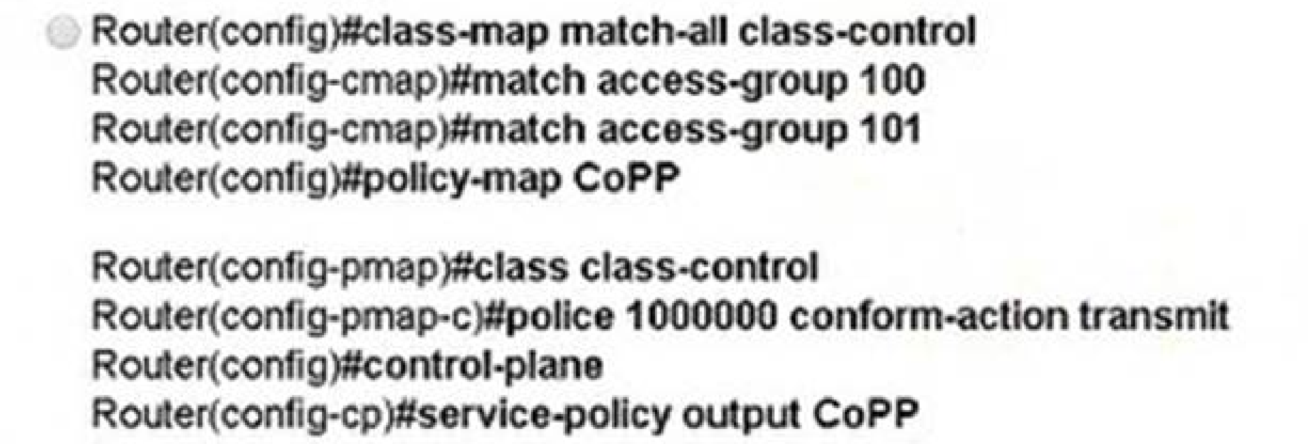
Answer: DE

NEW QUESTION 444
- (Topic 4)

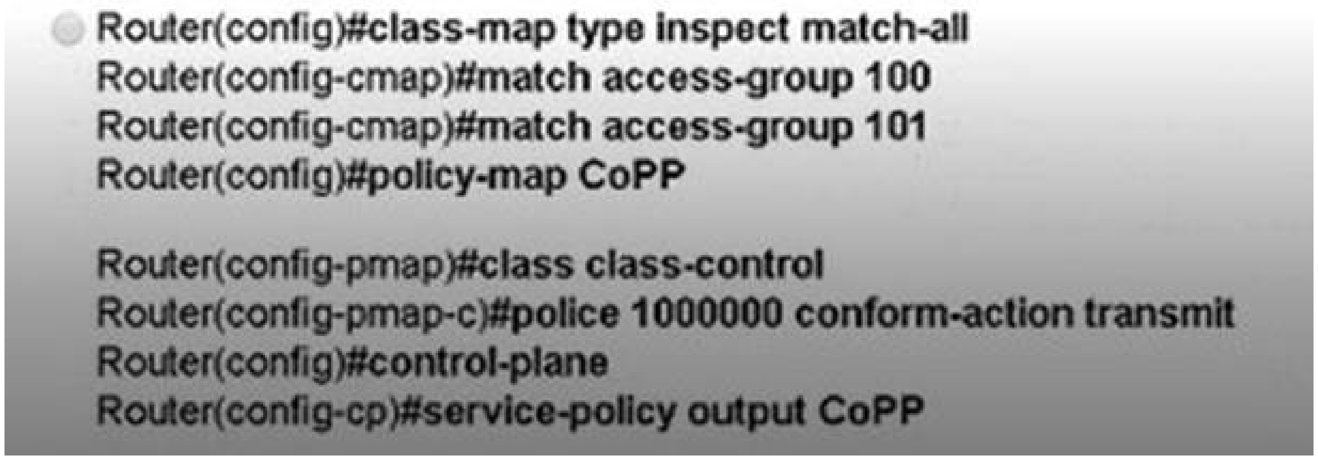


```
Router#sh access-list
Extended IP access list 100
    10 permit tcp any any eq telnet
Extended IP access list 101
    10 permit tcp any any eq 22
```

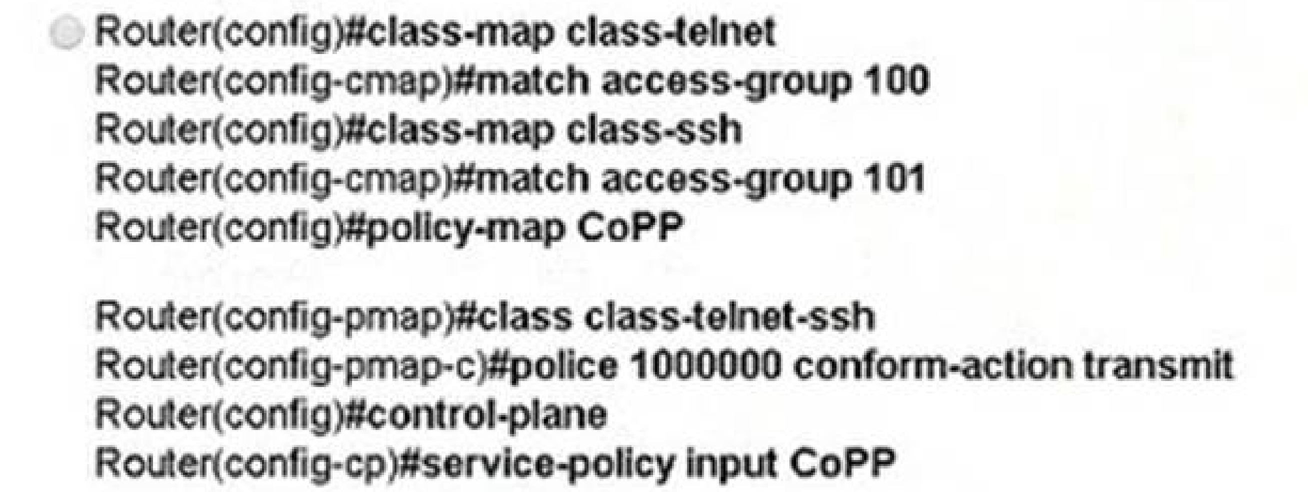
Refer to the exhibit. Which configuration set implements Control plane Policing for SSH and Telnet?



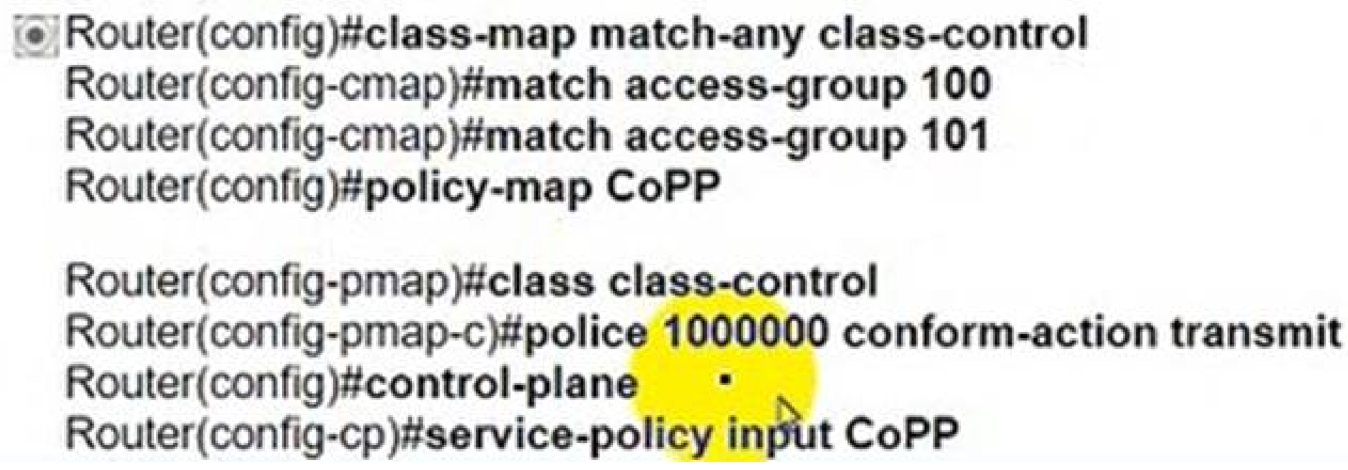
```
○ Router(config)#class-map match-all class-control
  Router(config-cmap)#match access-group 100
  Router(config-cmap)#match access-group 101
  Router(config)#policy-map CoPP

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



```
○ Router(config)#class-map type inspect match-all
  Router(config-cmap)#match access-group 100
  Router(config-cmap)#match access-group 101
  Router(config)#policy-map CoPP

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



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

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

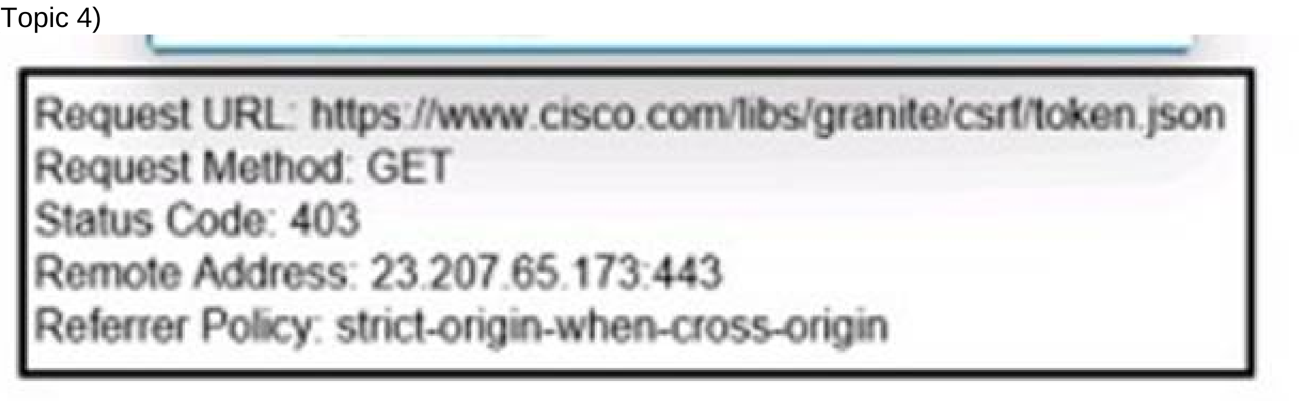


```
● Router(config)#class-map match-any class-control
  Router(config-cmap)#match access-group 100
  Router(config-cmap)#match access-group 101
  Router(config)#policy-map CoPP

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

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

Answer: D

NEW QUESTION 445
- (Topic 4)



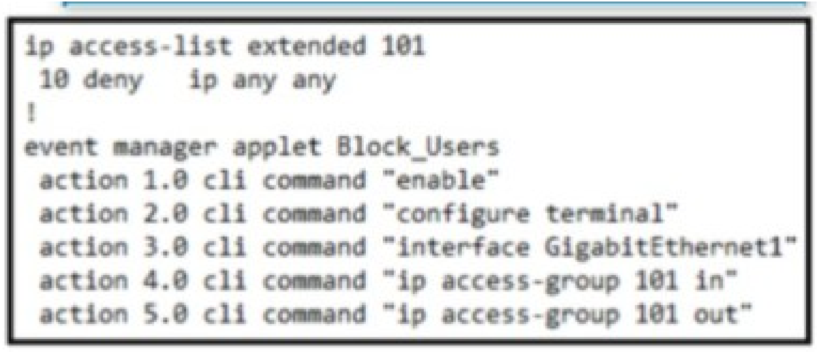
Request URL: https://www.cisco.com/libs/granite/csrf/token.json
Request Method: GET
Status Code: 403
Remote Address: 23.207.65.173:443
Referrer Policy: strict-origin-when-cross-origin

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 449
- (Topic 4)



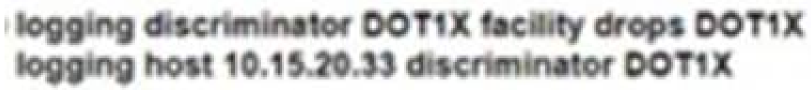
```
ip access-list extended 101
 10 deny   ip any any
!
event manager applet Block_Users
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "interface GigabitEthernet1"
 action 4.0 cli command "ip access-group 101 in"
 action 5.0 cli command "ip access-group 101 out"
```

Refer to the exhibit. An engineer builds an EEM script to apply an access list. Which statement must be added to complete the script?

A. event none
B. action 2.1 cli command "ip action 3.1 ell command 101"
C. action 6.0 ell command "ip access-list extended 101"
D. action 6.0 cli command "ip access-list extended 101"

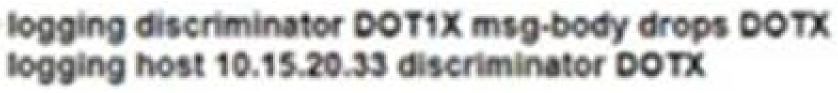
Answer: A

NEW QUESTION 454
- (Topic 4)
Which configuration filters out DOT1X messages in the format shown below from being sent toward Syslog server 10.15.20.33?
A)



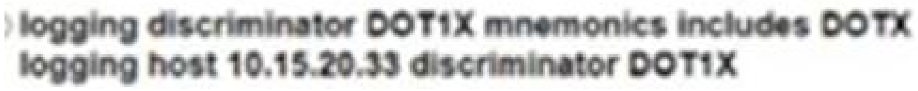
```
logging discriminator DOT1X facility drops DOT1X
logging host 10.15.20.33 discriminator DOT1X
```

B)



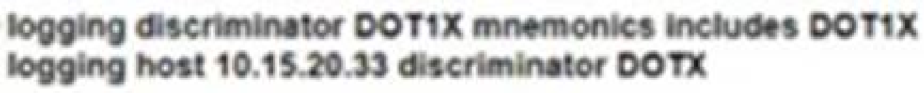
```
logging discriminator DOT1X msg-body drops DOTX
logging host 10.15.20.33 discriminator DOTX
```

C)



```
logging discriminator DOT1X mnemonics includes DOTX
logging host 10.15.20.33 discriminator DOT1X
```

D)



```
logging discriminator DOT1X mnemonics includes DOT1X
logging host 10.15.20.33 discriminator DOTX
```

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

Answer: A

NEW QUESTION 455
- (Topic 4)
By default, which virtual MAC address does HSRP group 15 use?

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

Answer: C

Explanation:
interface Ethernet0/0.100 encapsulation dot1Q 100
ip address 10.0.111.1 255.255.255.0
standby 15 ip 10.0.111.254
!
cisco(config-subif)#do s stand Ethernet0/0.100 - Group 15
State is Speak
Virtual IP address is 10.0.111.254 Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac0f (v1 default) Hello time 3 sec, hold time 10 sec
Next hello sent in 1.200 secs Preemption disabled
Active router is unknown Standby router is unknown

NEW QUESTION 457
- (Topic 4)
In Cisco DNA Center, what is the integration API?

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

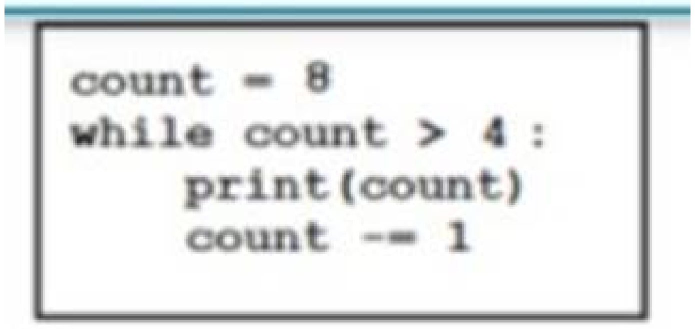
Answer: B

NEW QUESTION 461
- (Topic 4)
Which unit of measure is used to measure wireless RF SNR?

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

Answer: C

NEW QUESTION 462
- (Topic 4)
Refer to the exhibit.



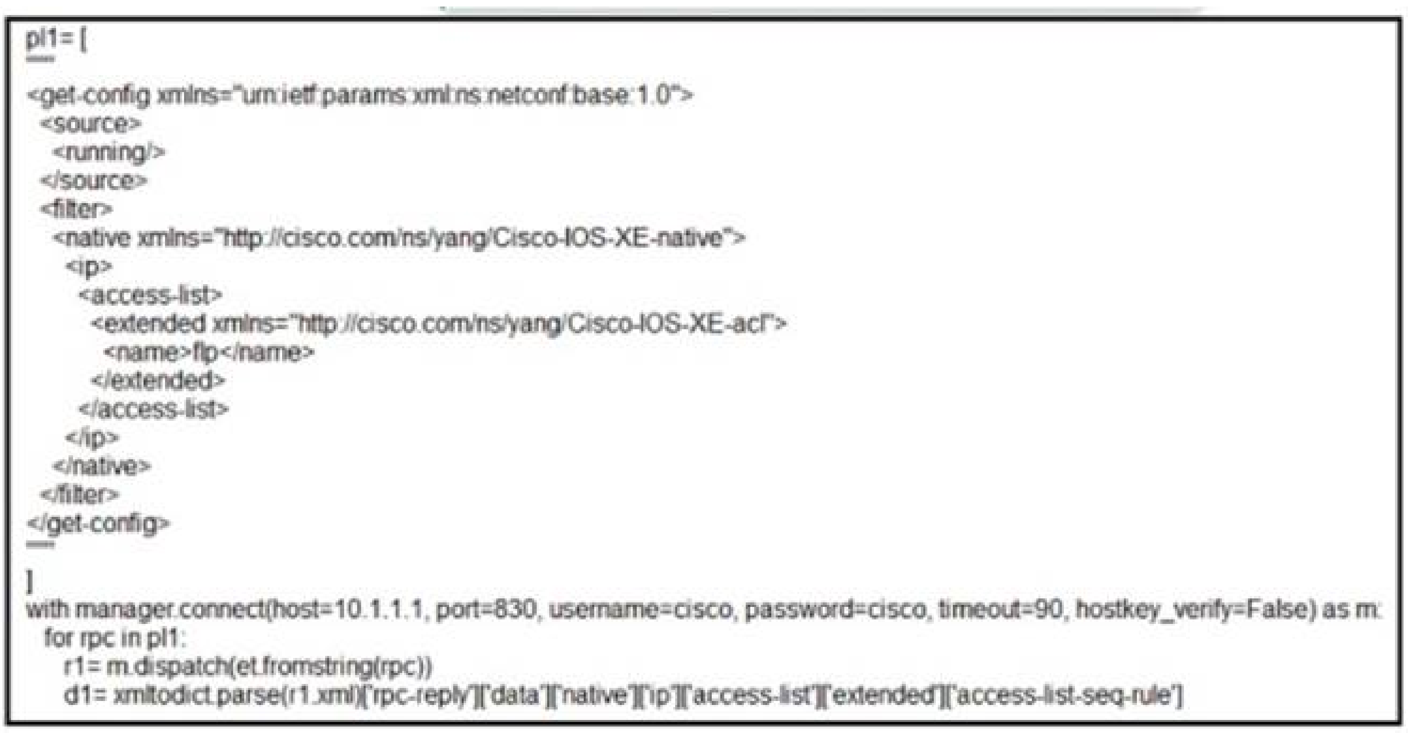
```
count = 8
while count > 4 :
     print(count)
     count -= 1
```

What is output by this code?

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

Answer: A

NEW QUESTION 466
- (Topic 4)
Refer to the exhibit.



```
pl1= [
"""
<get-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <source>
  <running/>
 </source>
 <filter>
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
   <ip>
    <access-list>
     <extended xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-acl">
      <name>flp</name>
     </extended>
    </access-list>
   </ip>
  </native>
 </filter>
</get-config>
"""
]
with manager.connect(host=10.1.1.1, port=830, username=cisco, password=cisco, timeout=90, hostkey_verify=False) as m:
  for rpc in pl1:
    r1= m.dispatch(et.fromstring(rpc))
    d1= xmltodict.parse(r1.xml)['rpc-reply']['data']['native']['ip']['access-list']['extended']['access-list-seq-rule']
```

What is achieved by the XML code?

A. It reads the access list sequence numbers from the output of the show ip access-list extended flp command into a dictionary list.
B. It displays the output of the show ip access-list extended flp command on the terminal screen
C. It displays the access list sequence numbers from the output of the show Ip access-list extended flp command on the terminal screen
D. It reads the output of the show ip access-list extended flp command into a dictionary list.

Answer: A

NEW QUESTION 470
- (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 475
- (Topic 4)
By default, which virtual MAC address does HSRP group 12 use?

A. 00 5e0c:07:ac:12
B. 05:44:33:83:68:6c
C. 00:00:0c:07:ac:0c
D. 00:05:5e:00:0c:12

Answer: C

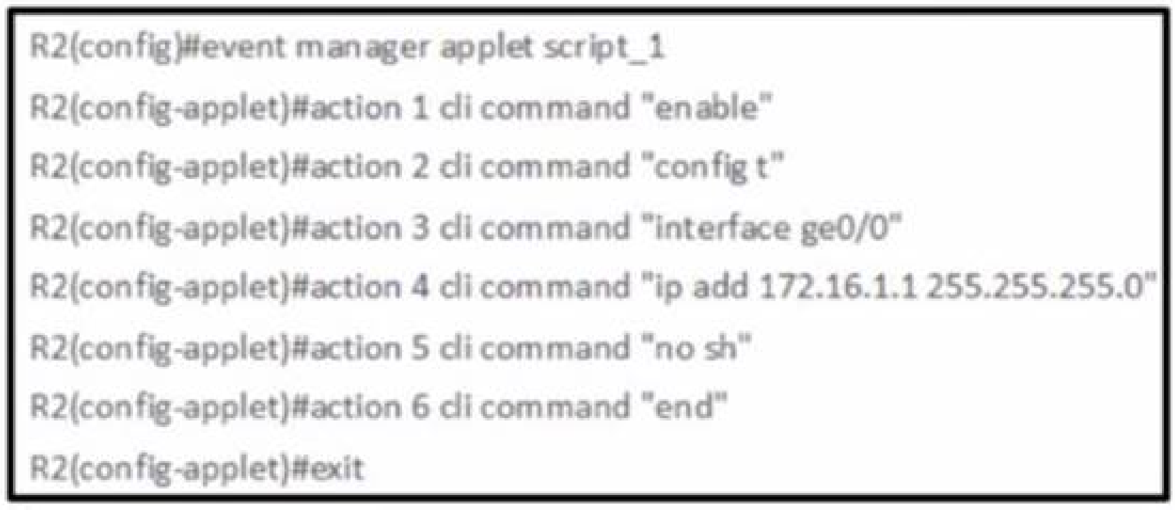
NEW QUESTION 479
- (Topic 4)
A technician needs to find the MAC address of a connecting router. Which of the following commands should the technician use?

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 482
- (Topic 4)
Refer to the exhibit.



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

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

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

Answer: D

NEW QUESTION 487
- (Topic 4)
Which two methods are used to assign security group tags to the user in a Cisco Trust Sec architecture? (Choose two)

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

Answer: CE

NEW QUESTION 490
- (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

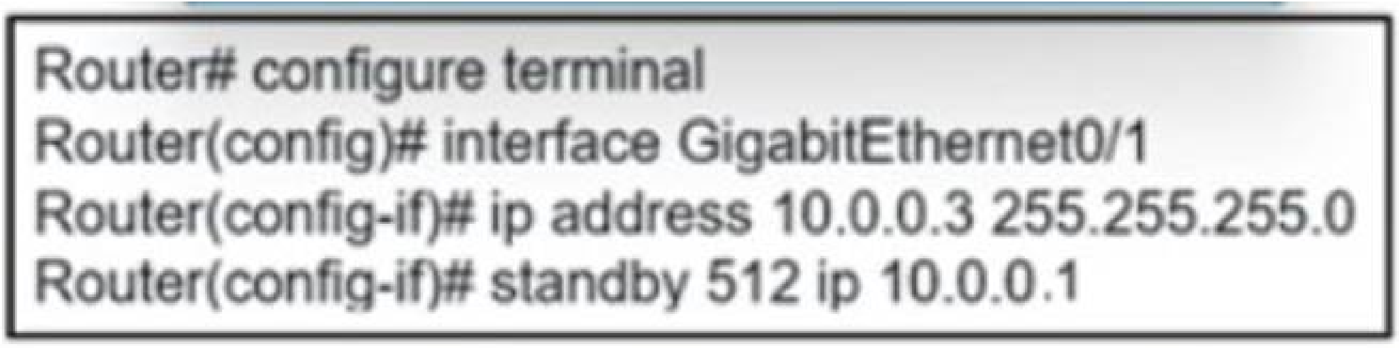
Explanation:
This is because the voice VLAN is a special VLAN that is used to separate the voice traffic from the data traffic on a switch port. The voice VLAN allows the VoIP phone to communicate with the voice server and receive calls. The voice VLAN is usually configured with a higher priority than 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 495
- (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 499
- (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

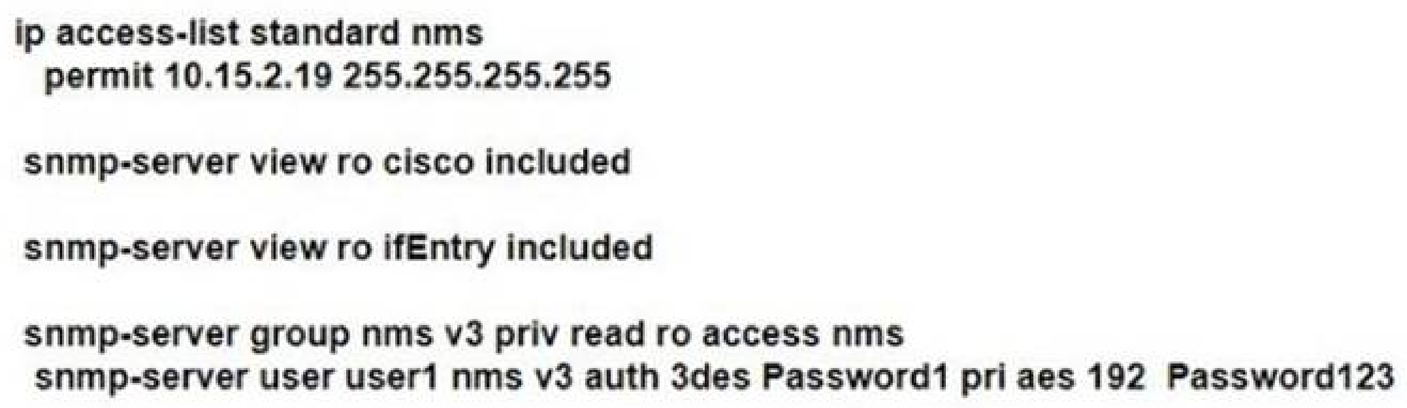
Answer: A

NEW QUESTION 502
- (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

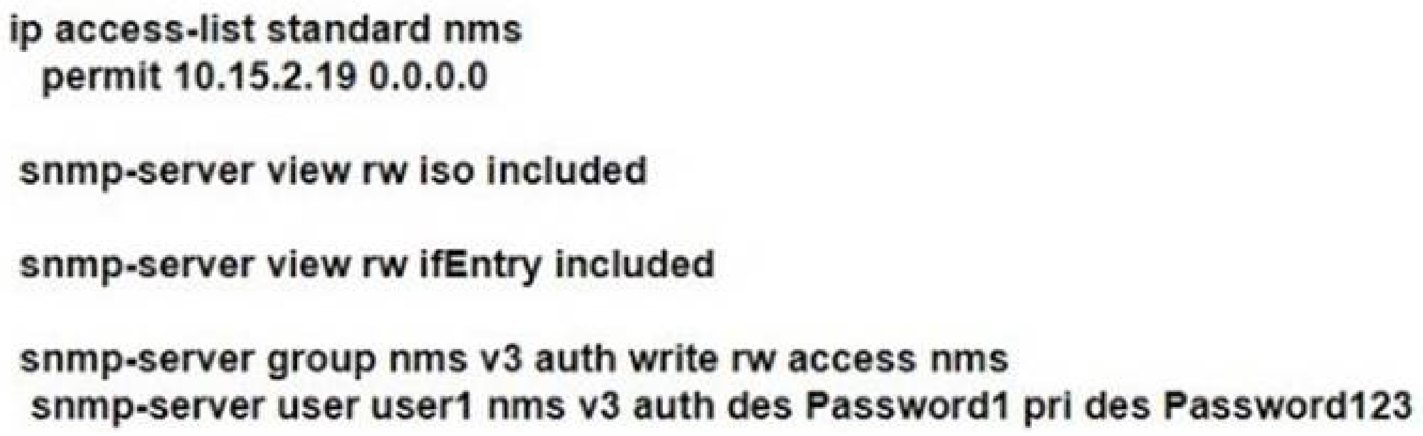
Answer: D

NEW QUESTION 503
- (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)



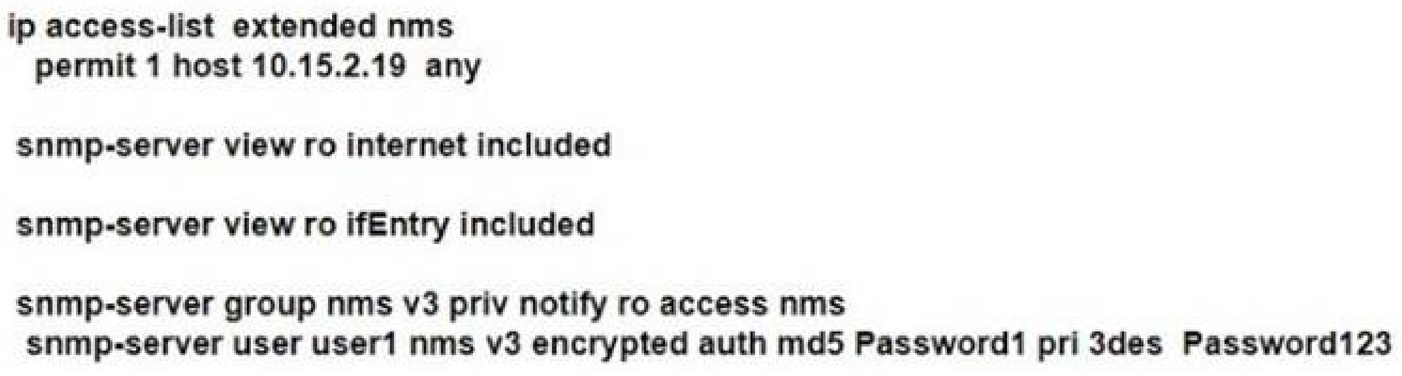
```
ip access-list standard nms
  permit 10.15.2.19 255.255.255.255

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)



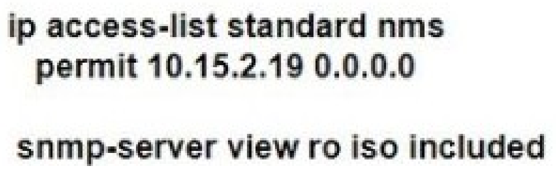
```
ip access-list standard nms
  permit 10.15.2.19 0.0.0.0

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)



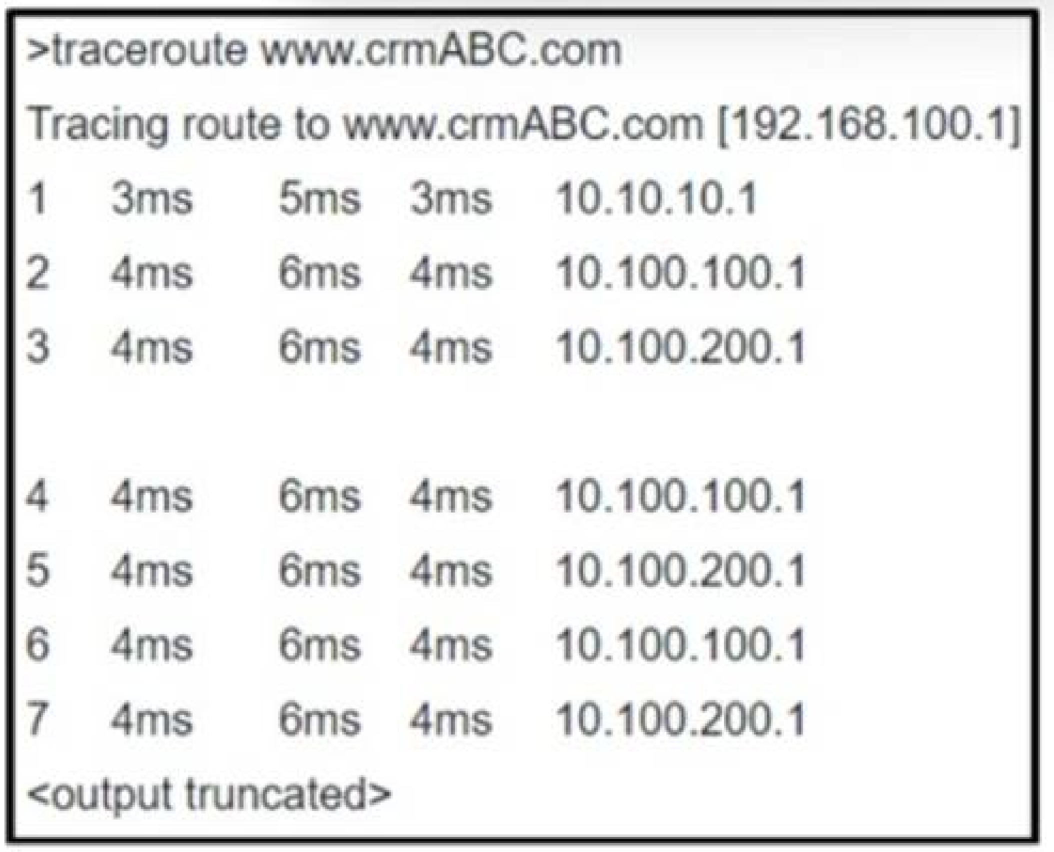
```
ip access-list standard nms
  permit 10.15.2.19 0.0.0.0

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 506
- (Topic 4)



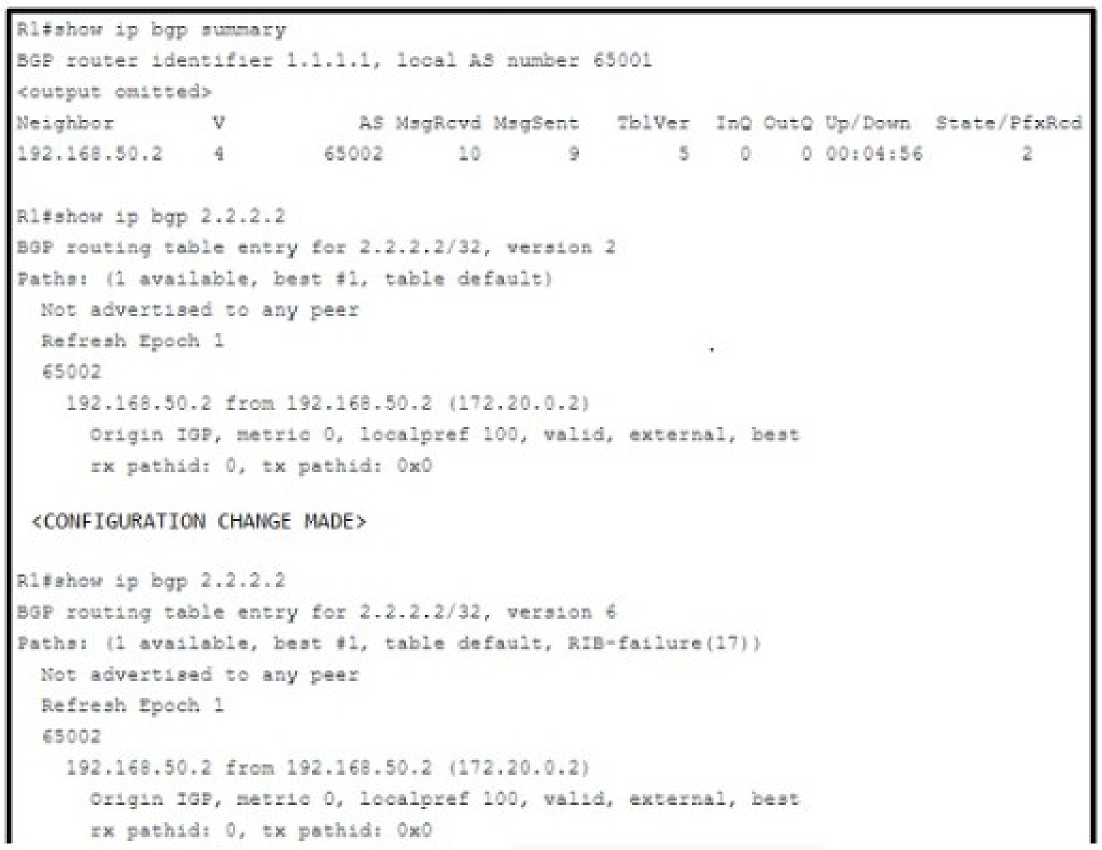
```
>traceroute www.crmABC.com
Tracing route to www.crmABC.com [192.168.100.1]
1   3ms   5ms   3ms   10.10.10.1
2   4ms   6ms   4ms   10.100.100.1
3   4ms   6ms   4ms   10.100.200.1

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 508
- (Topic 4)
Refer to the exhibit.



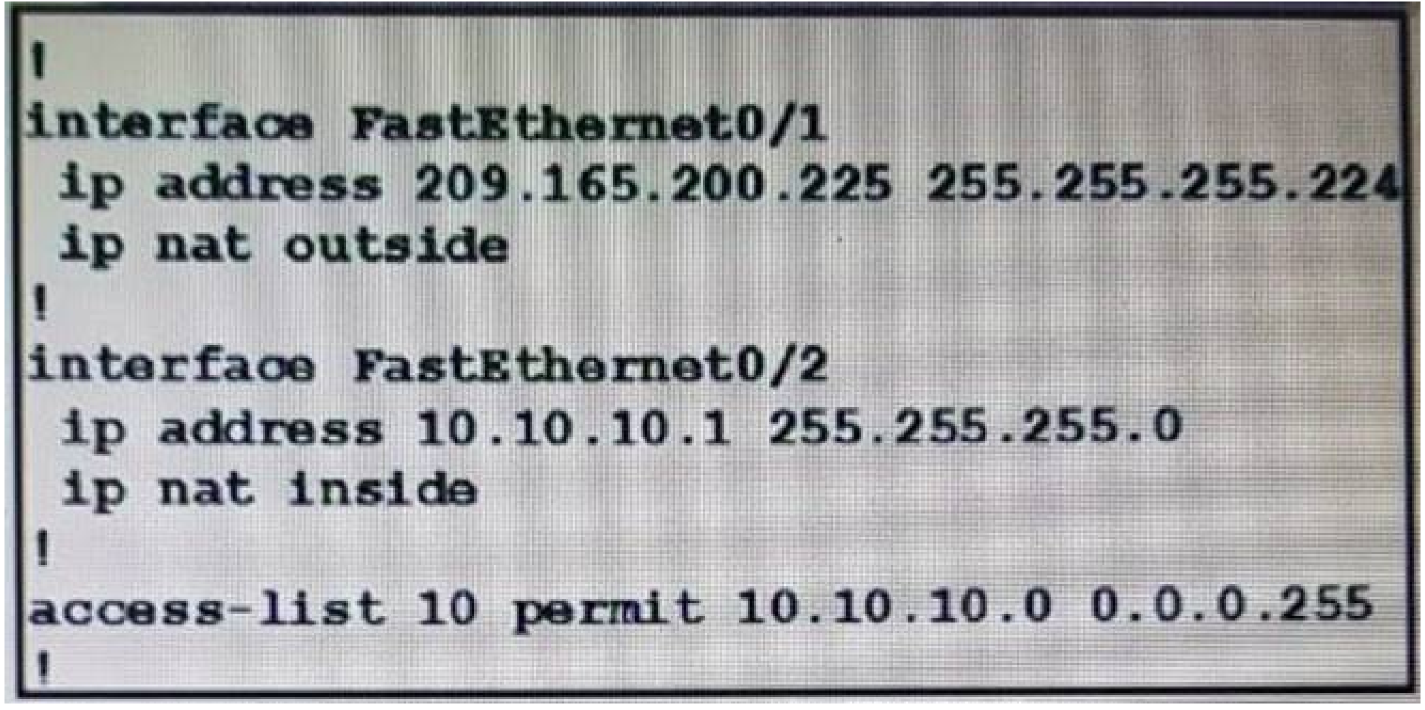
```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 65001
<output omitted>
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.50.2    4        65002      10       9        5    0    0 00:04:56        2

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

 <CONFIGURATION CHANGE MADE>

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

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

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

Answer: D

NEW QUESTION 513
- (Topic 4)



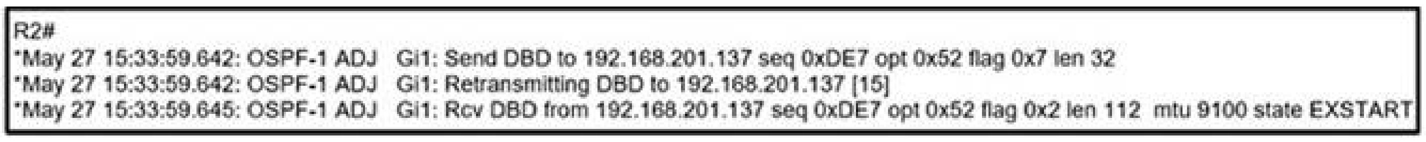
```
!
interface FastEthernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
!
interface FastEthernet0/2
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
access-list 10 permit 10.10.10.0 0.0.0.255
!
```

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 514
- (Topic 4)
Refer to the exhibit.



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

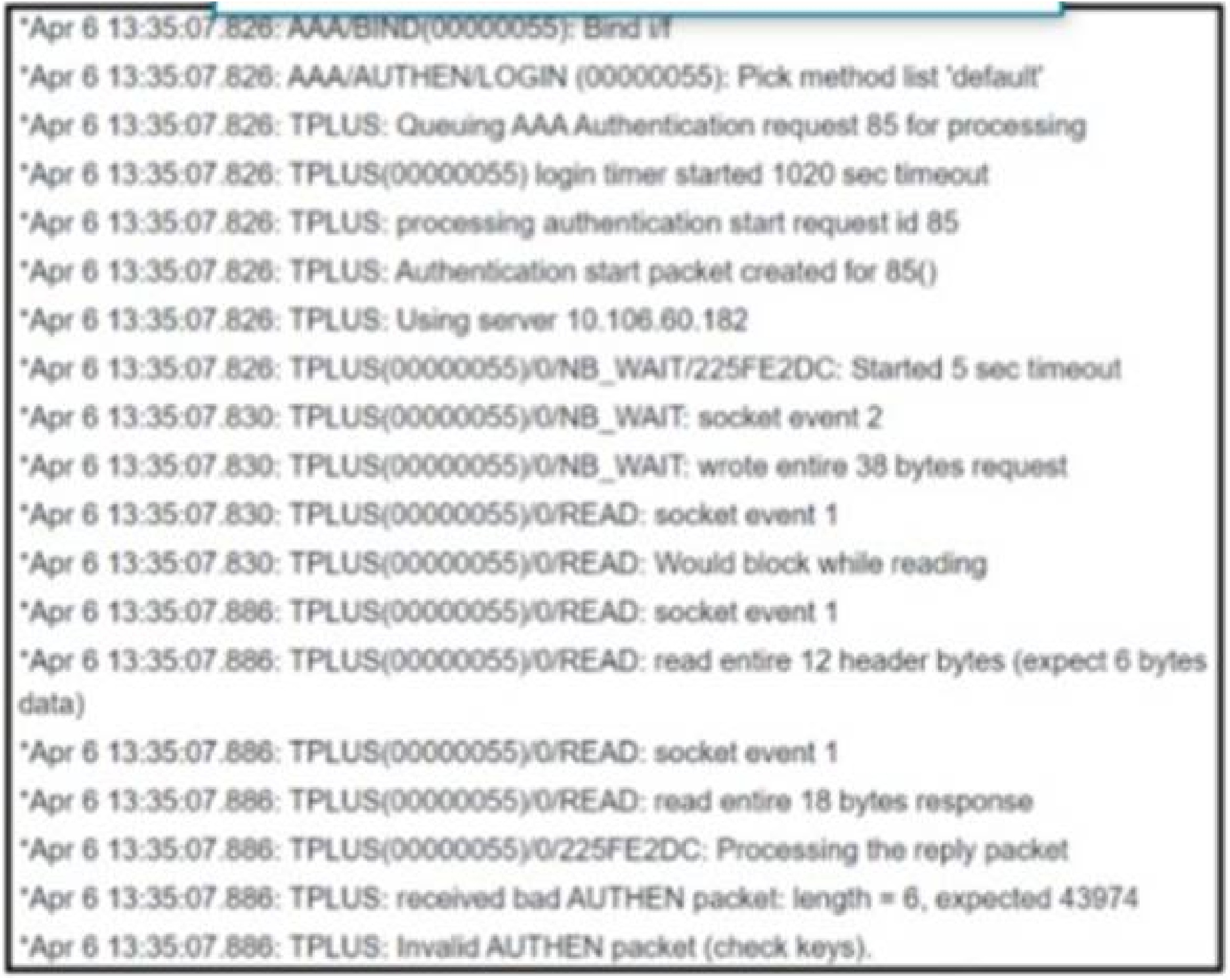
The OSPF neighborship fails between two routers. What is the cause of this issue?

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

Answer: C

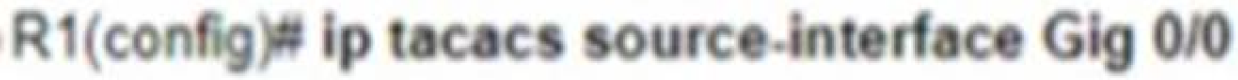
Explanation:
cisco_R2(config-subif)#do debug ip osp adj OSPF adjacency debugging is on
cisco_R2(config-subif)#ip mtu 1111 <<<<<<<<<<<<<<<< cisco_R2(config-subif)#
cisco_R2(config-subif)# cisco_R2(config-subif)#do clear ip ospf
!!!debug shows this: cisco_R2(config-subif)#
*Dec 23 13:02:27.164: OSPF-1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

NEW QUESTION 515
- (Topic 4)



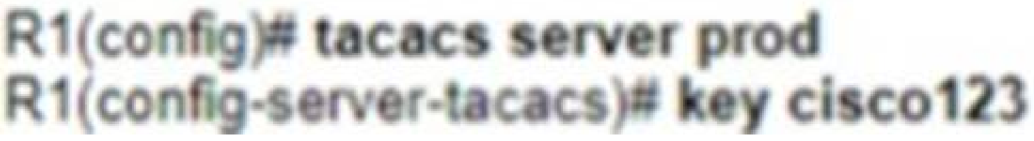
```
*Apr 6 13:35:07.826: AAA/BIND(00000055): Bind i/f
*Apr 6 13:35:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Apr 6 13:35:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*Apr 6 13:35:07.826: TPLUS(00000055) login timer started 1020 sec timeout
*Apr 6 13:35:07.826: TPLUS: processing authentication start request id 85
*Apr 6 13:35:07.826: TPLUS: Authentication start packet created for 85()
*Apr 6 13:35:07.826: TPLUS: Using server 10.106.60.182
*Apr 6 13:35:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: Would block while reading
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes
data)
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*Apr 6 13:35:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*Apr 6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr 6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

Refer to the exhibit. An engines configured TACACS^ to authenticate remote users but the configuration is not working as expected Which configuration must be applied to enable access?
A)



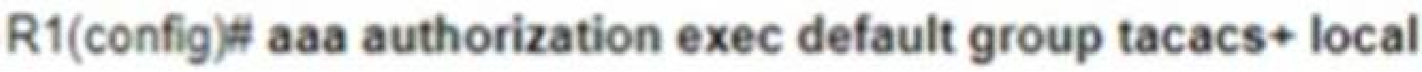
```
R1(config)# ip tacacs source-interface Gig 0/0
```

B)



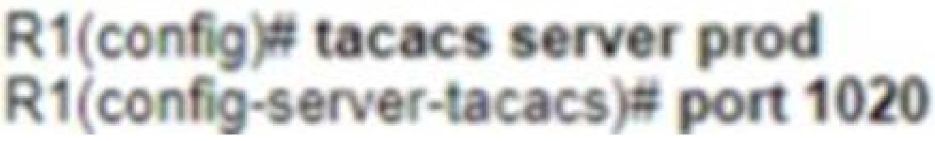
```
R1(config)# tacacs server prod
R1(config-server-tacacs)# key cisco123
```

C)



```
R1(config)# aaa authorization exec default group tacacs+ local
```

D)



```
R1(config)# tacacs server prod
R1(config-server-tacacs)# port 1020
```

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

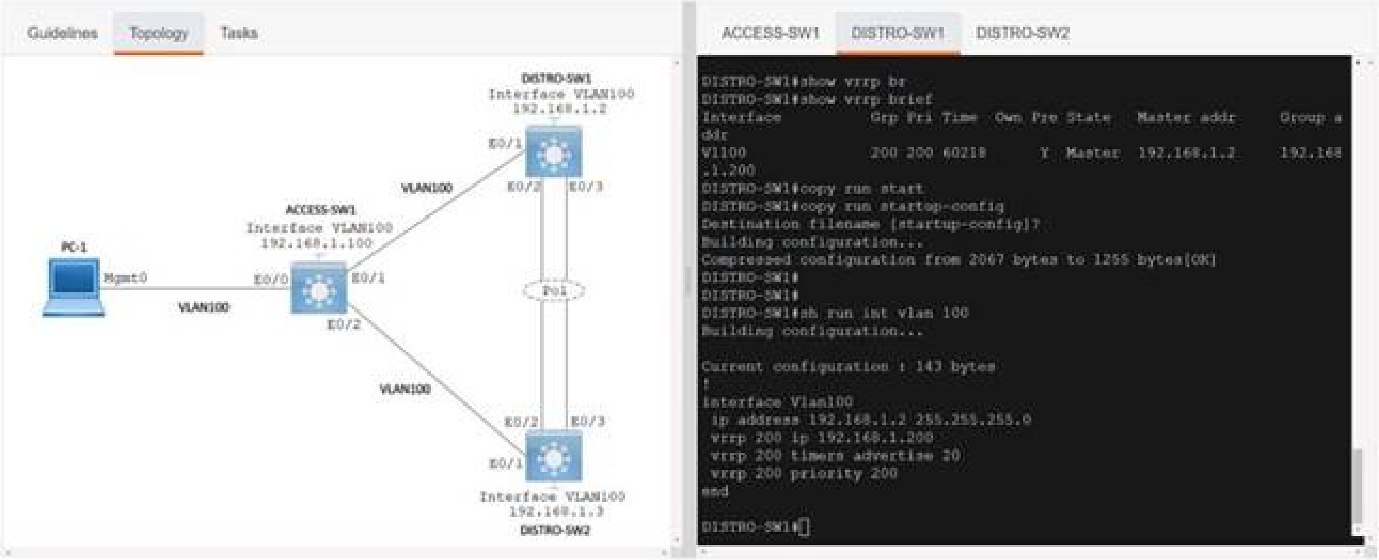
Answer: C

NEW QUESTION 518
- (Topic 4)
Which language defines the structure or modelling of data for NETCONF and RESTCONF?

A. YAM
B. YANG
C. JSON
D. XML

Answer: C

NEW QUESTION 520
SIMULATION - (Topic 4)
Simulation 10

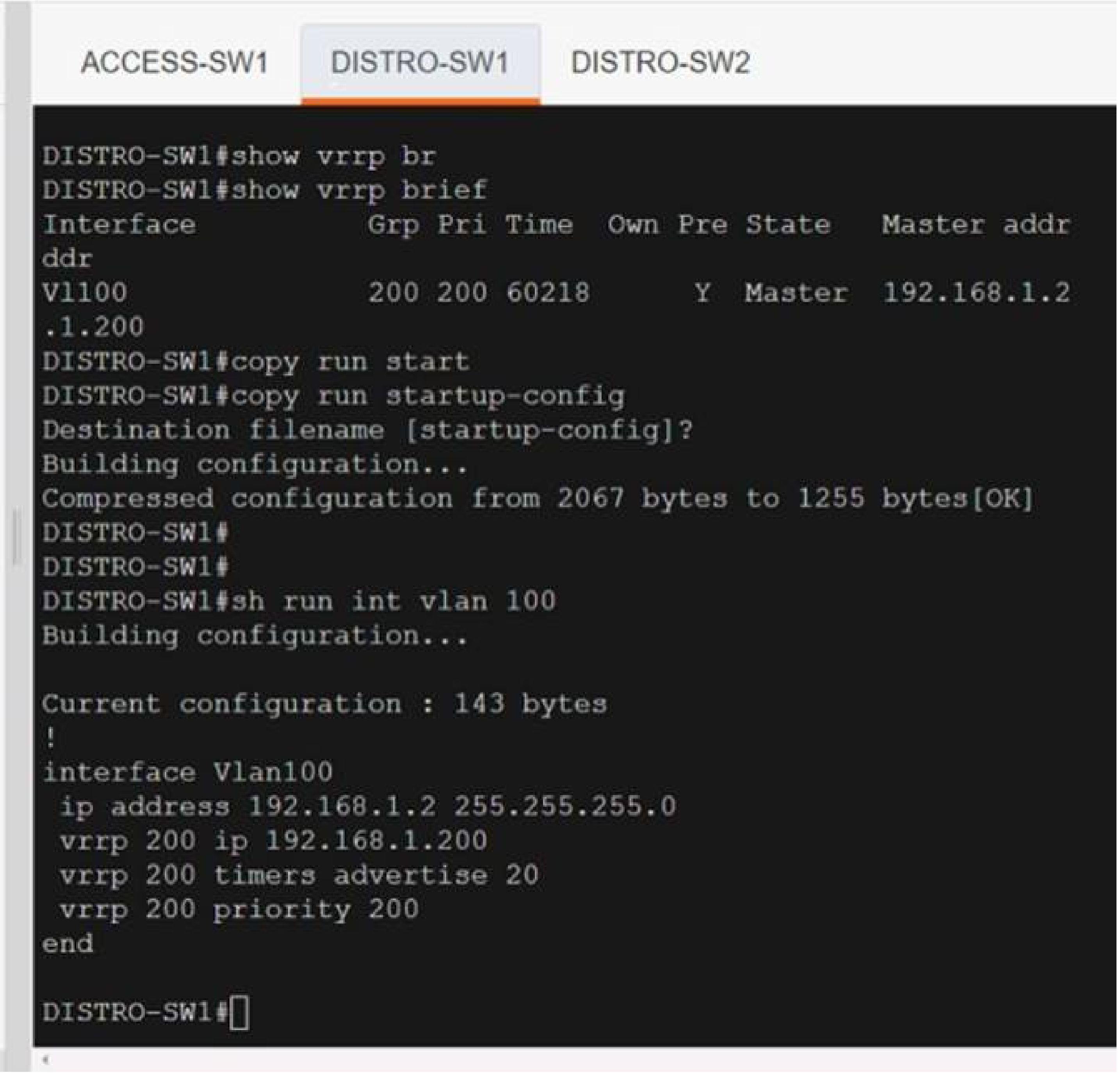


```
DISTRO-SW1#show vrrp br
DISTRO-SW1#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group a
ddr
Vl100              200 200 60218      Y  Master  192.168.1.2     192.168
.1.200
DISTRO-SW1#copy run start
DISTRO-SW1#copy run startup-config
Destination filename [startup-config]?
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#
```

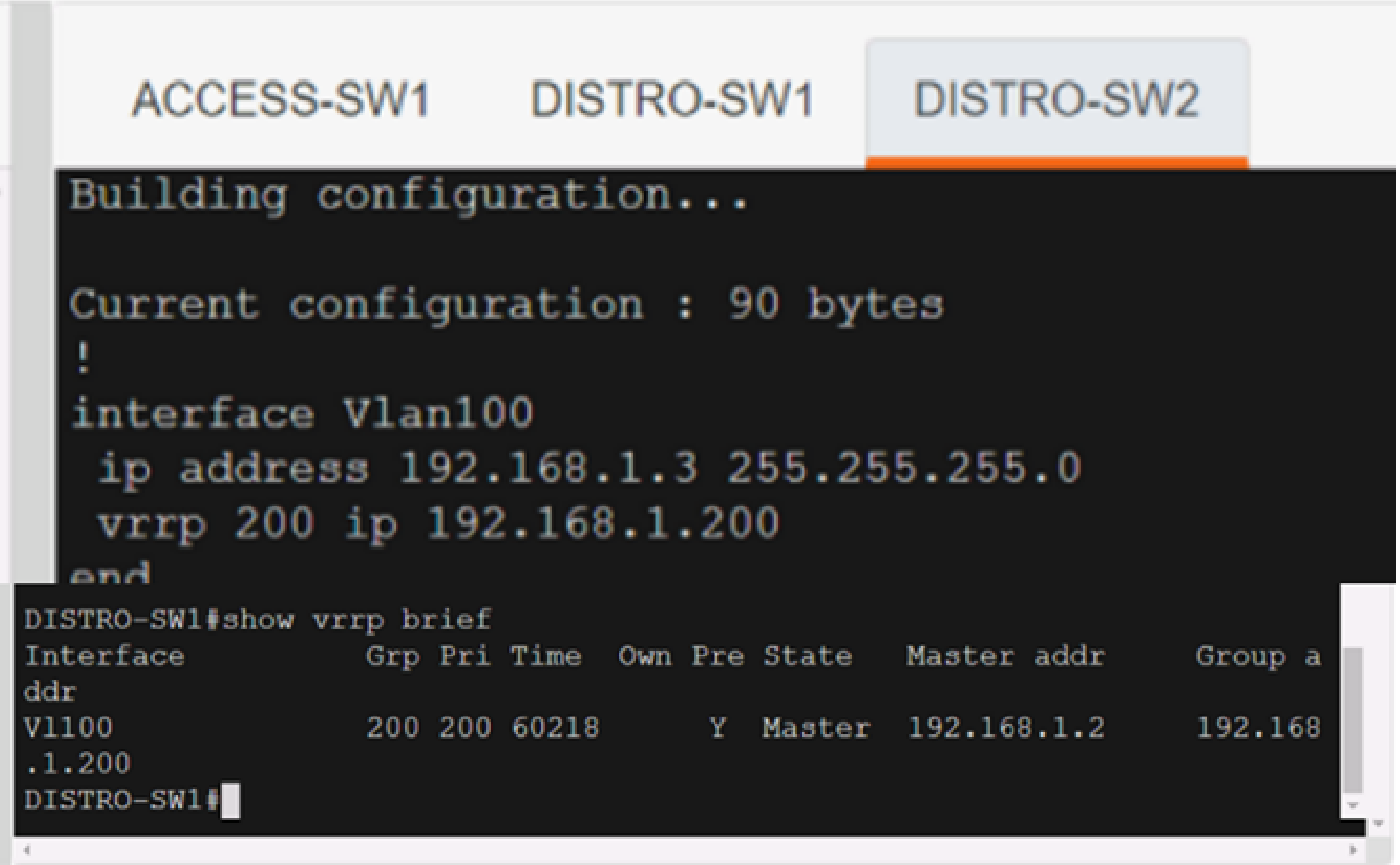
A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

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

DISTRO-SW1#
```

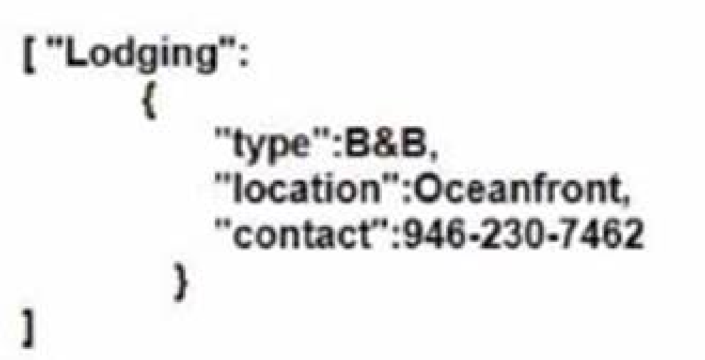


```
Building configuration...

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#
```

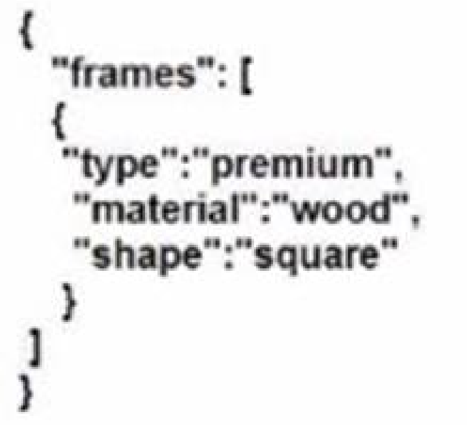
NEW QUESTION 522
- (Topic 4)
Which JSON script is properly formatted?

A)



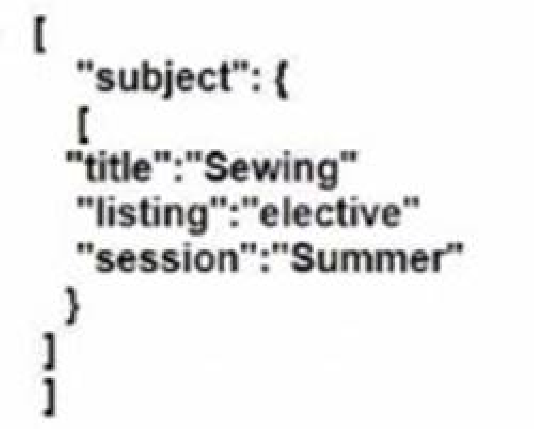
```
[ "Lodging":
        {
            "type":B&B,
            "location":Oceanfront,
            "contact":946-230-7462
          }
]
```

B)



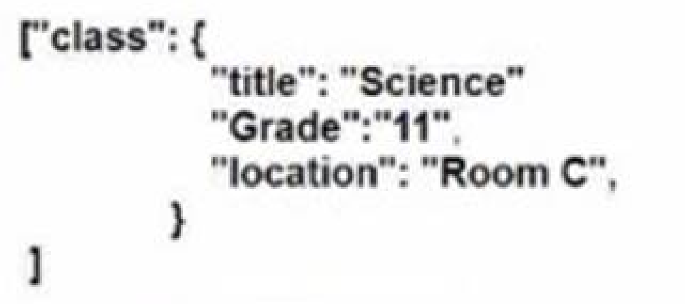
```
{
  "frames": [
  {
   "type":"premium",
    "material":"wood",
    "shape":"square"
   }
 ]
}
```

C)



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

D)



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

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

Answer: A

Explanation:
Option A is the properly formatted JSON script. JSON (JavaScript Object Notation) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client, so it can be displayed on a web page, or vice versa). The JSON syntax rules are as 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 525
- (Topic 4)
What is a characteristic of the Cisco DMA Center Template Editor feature?

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

Answer: D

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

NEW QUESTION 526
- (Topic 4)
What is the result when an active route processor fails that combines NSF with SSO?

A. An NSF-capable device immediately updates the standby route processor RIB without churning the network.
B. The standby route processor immediately takes control and forwards packets along known routes.
C. An NSF-aware device immediately updates the standby route processor RIB without churning the network.
D. The standby route processor temporarily forwards packets until route convergence is complete.

Answer: B

NEW QUESTION 531
- (Topic 4)
A network administrator is preparing a Python scrip to configure a Cisco IOS XE-based device on the network. The administrator is worried that colleagues will make changes to the device while the script is running. Which operation of he in client manager prevent colleague making changes to the device while the scrip is running?

A. m.lock(config='running')
B. m.lock(target='running')
C. m.freeze(target='running')
D. m.freeze(config='running')

Answer: B

NEW QUESTION 536
- (Topic 4)
What function does VXLAN perform in a Cisco SD-Access deployment?

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

Answer: A

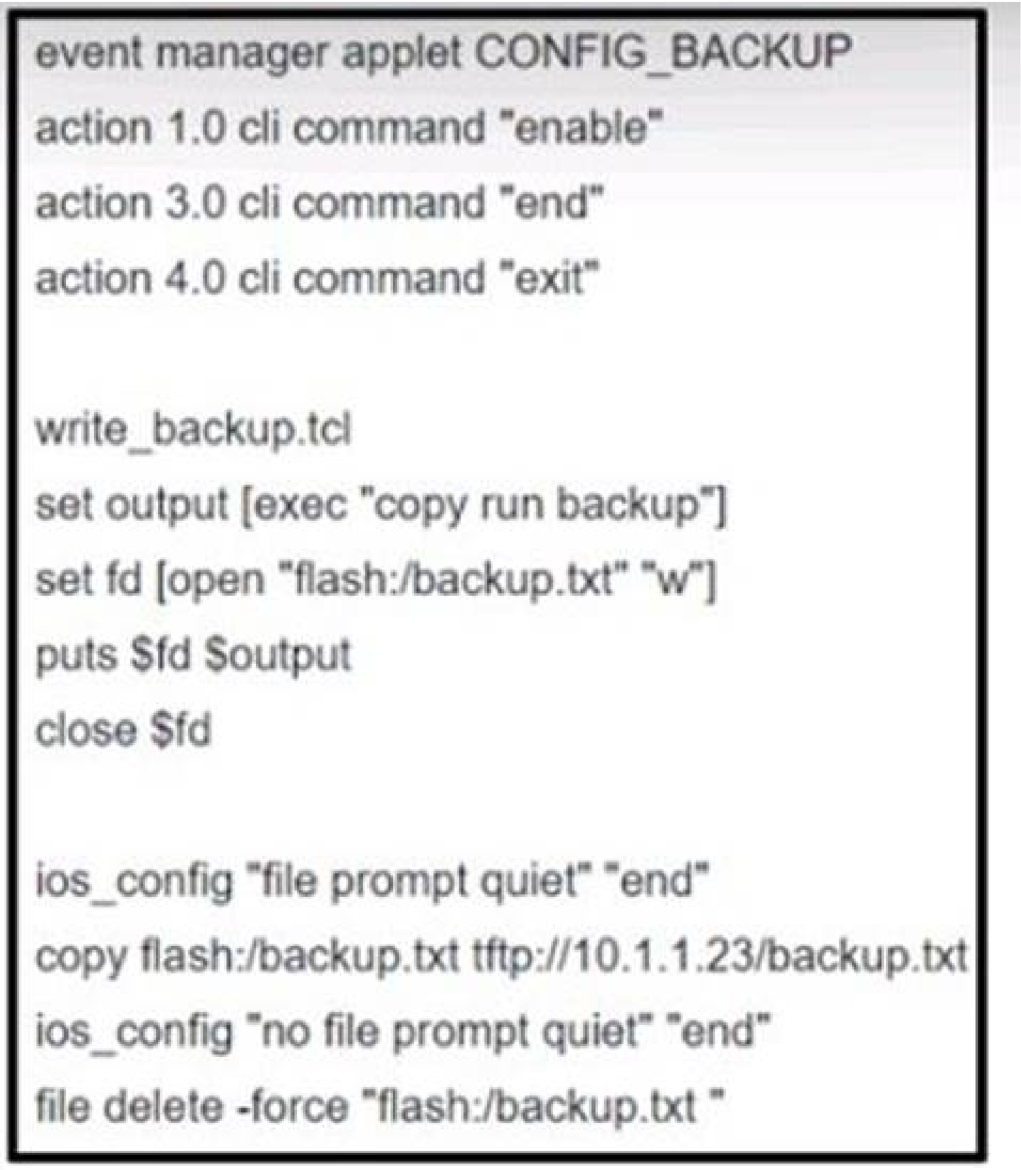
Explanation:
This is because VXLAN is a network virtualization technology that encapsulates Layer 2 frames in UDP headers and allows them to be transported over Layer 3 networks. VXLAN is used in Cisco SD-Access to create virtual networks that span across multiple physical locations and devices. VXLAN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

NEW QUESTION 539
- (Topic 4)
Which method ensures the confidentiality ot data exchanged over a REST API?

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

Answer: B

NEW QUESTION 540
- (Topic 4)
Refer to the exhibit.



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

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

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

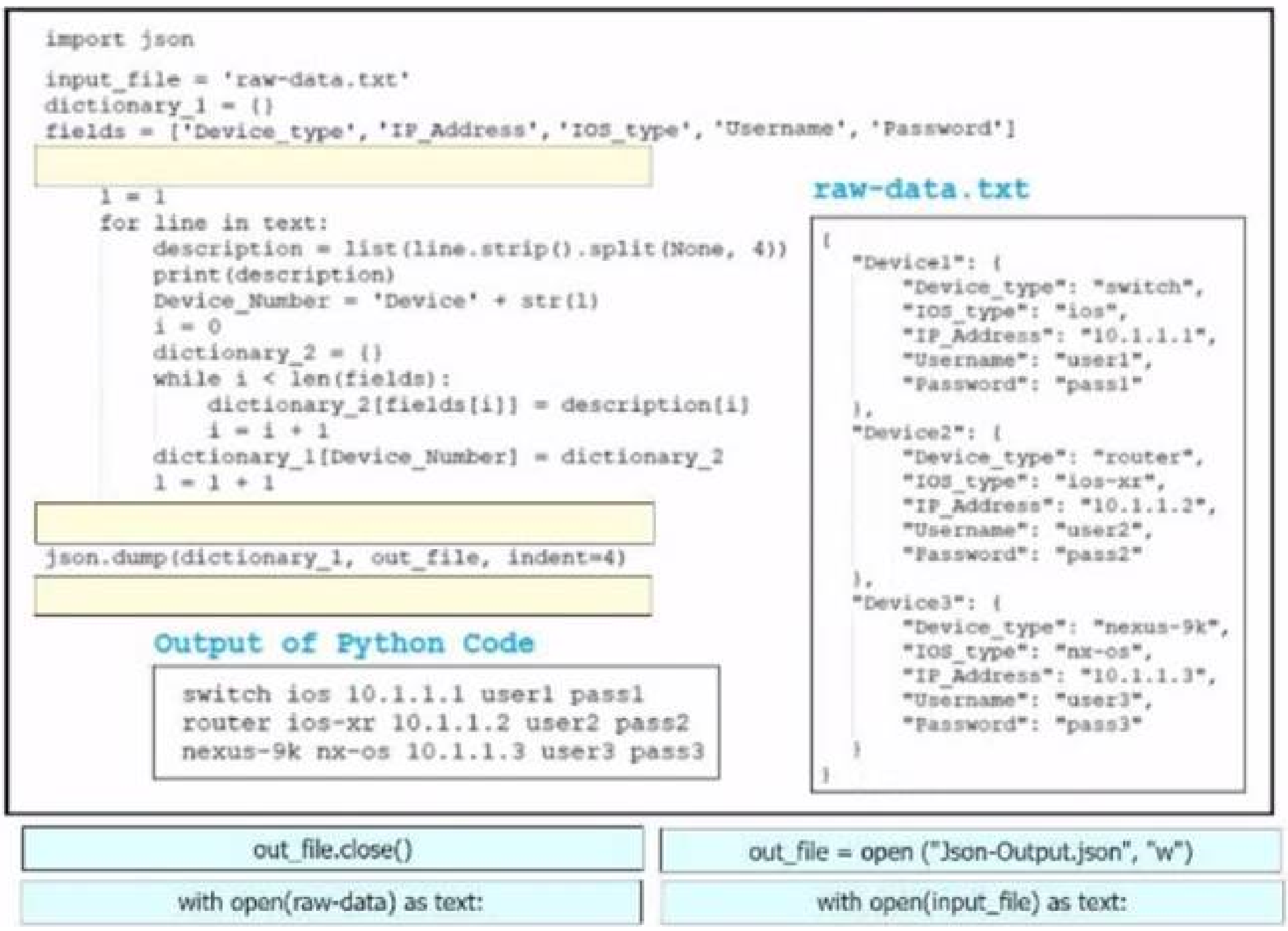
Which statement is needed to complete the EEM applet and use the Tel script to store the backup file?

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

Answer: B

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

NEW QUESTION 543
DRAG DROP - (Topic 4)
An engineer plans to use Python to convert text files that contain device information lo JSON. Drag and drop the code snippets from the bottom onto the blanks in the code to construct the request. Not all options are used.



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

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

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

raw-data.txt

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

Output of Python Code

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

out_file.close()

out_file = open ("Json-Output.json", "w")

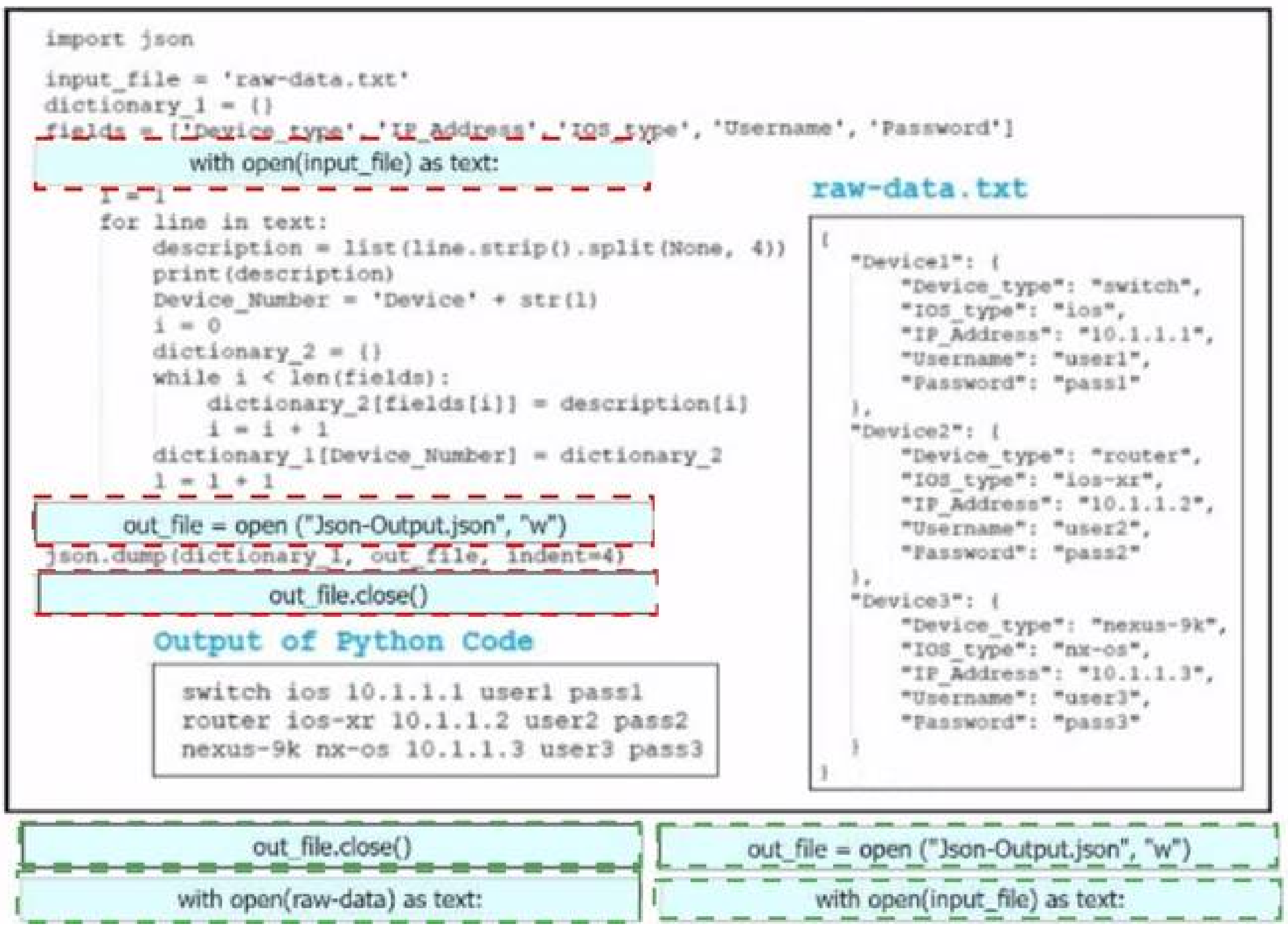
with open(raw-data) as text:

with open(input_file) as text:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



```
import json
input_file = 'raw-data.txt'
dictionary_1 = {}
fields = ['Device_type', 'IP_Address', 'IOS_type', 'Username', 'Password']
with open(input_file) as text:
    l = 1
    for line in text:
        description = list(line.strip().split(None, 4))
        print(description)
        Device_Number = 'Device' + str(l)
        i = 0
        dictionary_2 = {}
        while i < len(fields):
            dictionary_2[fields[i]] = description[i]
            i = i + 1
        dictionary_1[Device_Number] = dictionary_2
        l = l + 1
out_file = open ("Json-Output.json", "w")
json.dump(dictionary_1, out_file, indent=4)
out_file.close()
```

raw-data.txt

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

Output of Python Code

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

out_file.close()

out_file = open ("Json-Output.json", "w")

with open(raw-data) as text:

with open(input_file) as text:

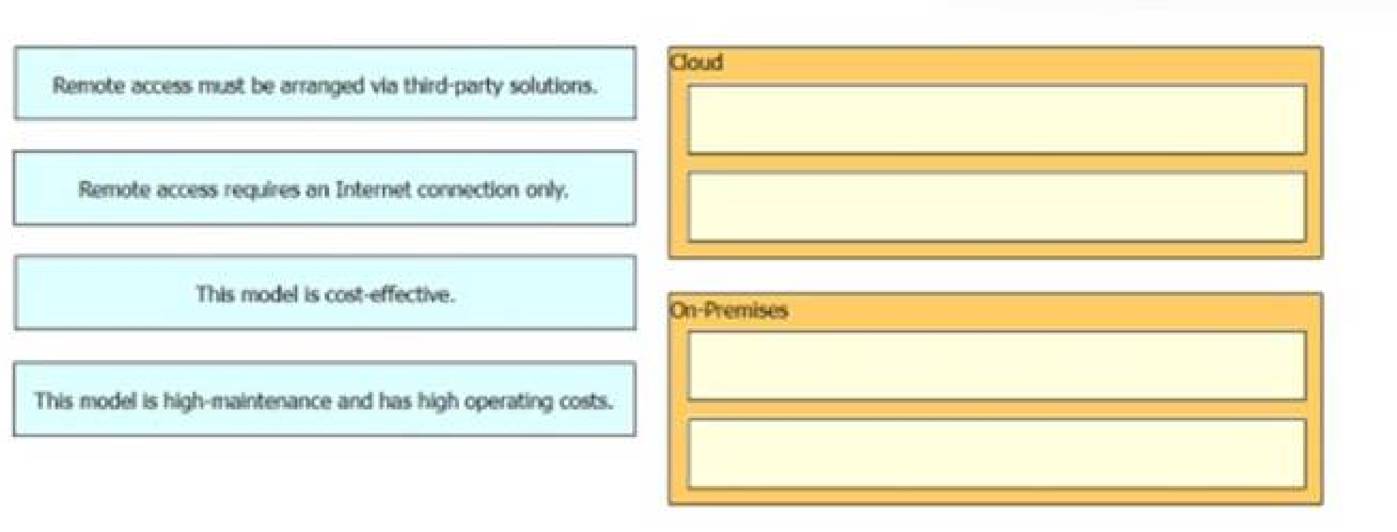
NEW QUESTION 546
- (Topic 4)
Which two new security capabilities are introduced by using a next-generation firewall at the Internet edge? (Choose two.)

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

Answer: DE

NEW QUESTION 551

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.

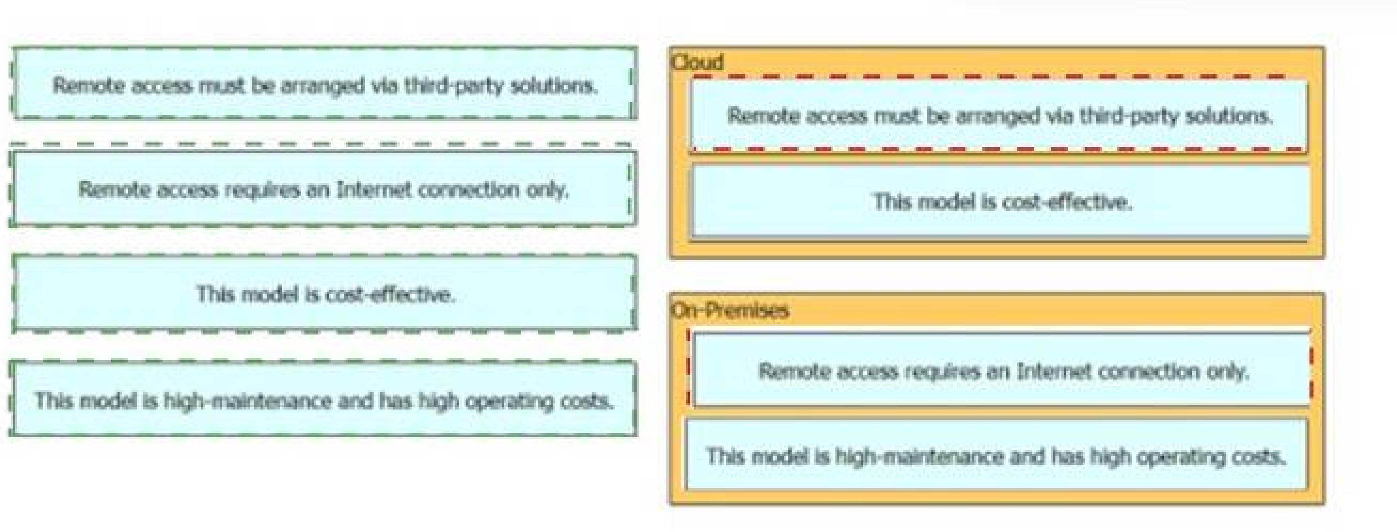
Cloud

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.

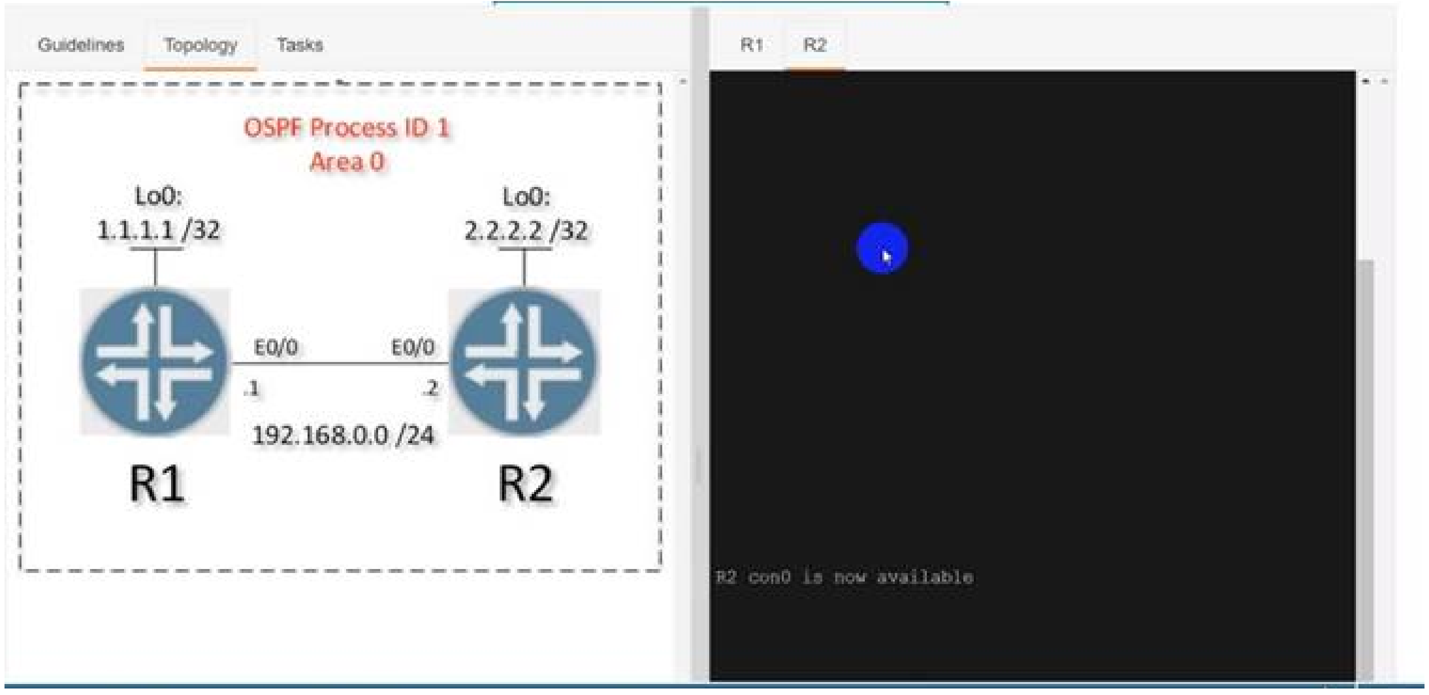
This model is cost-effective.

On-Premises

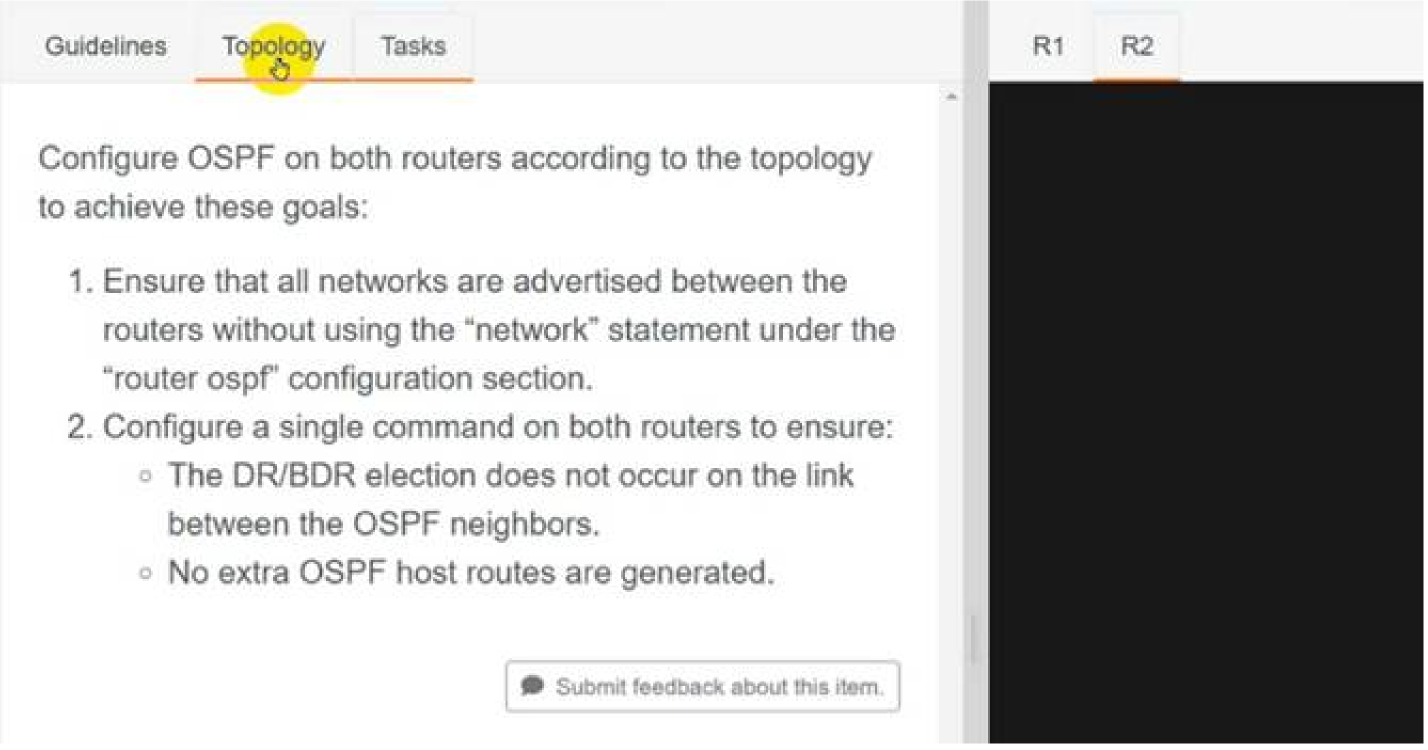
Remote access requires an Internet connection only.

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

NEW QUESTION 553
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.

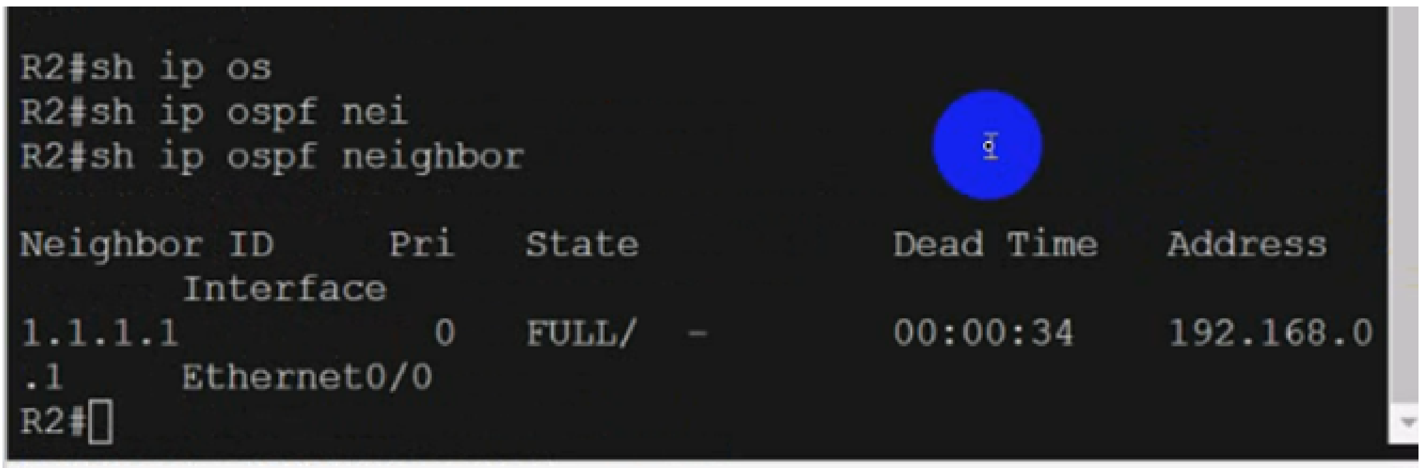
Submit feedback about this item.

A. Mastered
B. Not Mastered

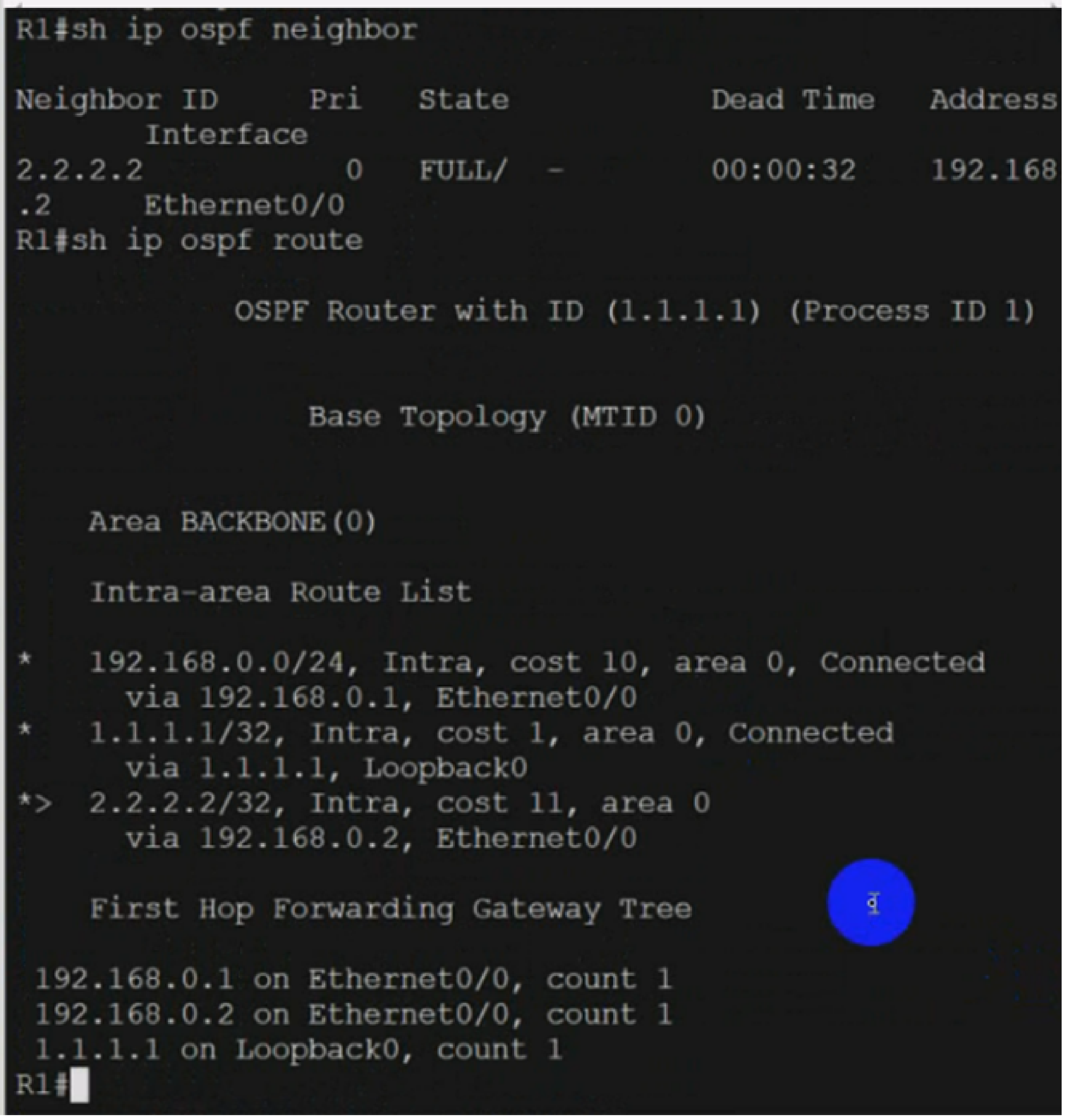
Answer: A

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:-

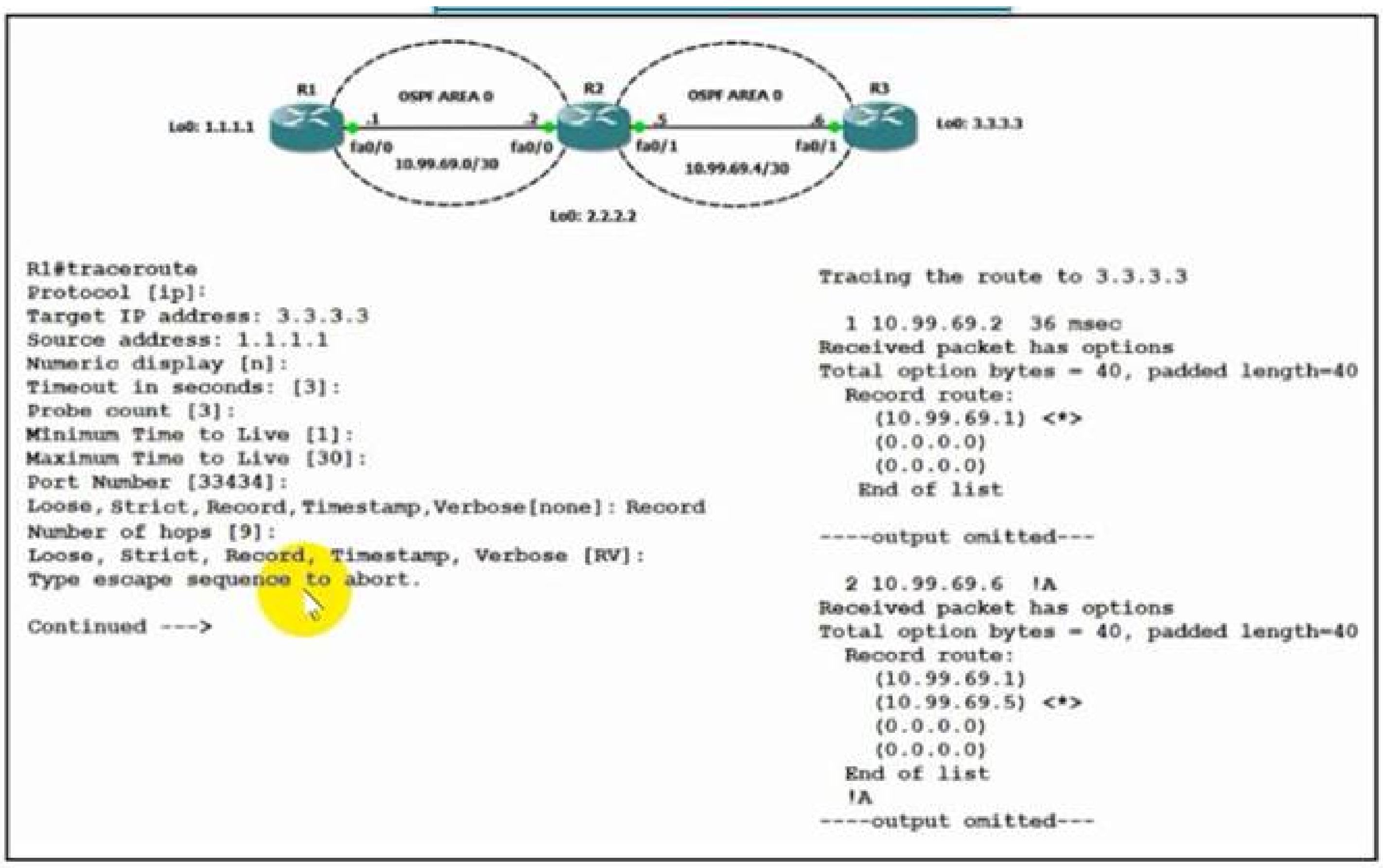


```
R2#sh ip os
R2#sh ip ospf nei
R2#sh ip ospf neighbor

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 554
- (Topic 4)
Refer to the exhibit.



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

Continued --->
```

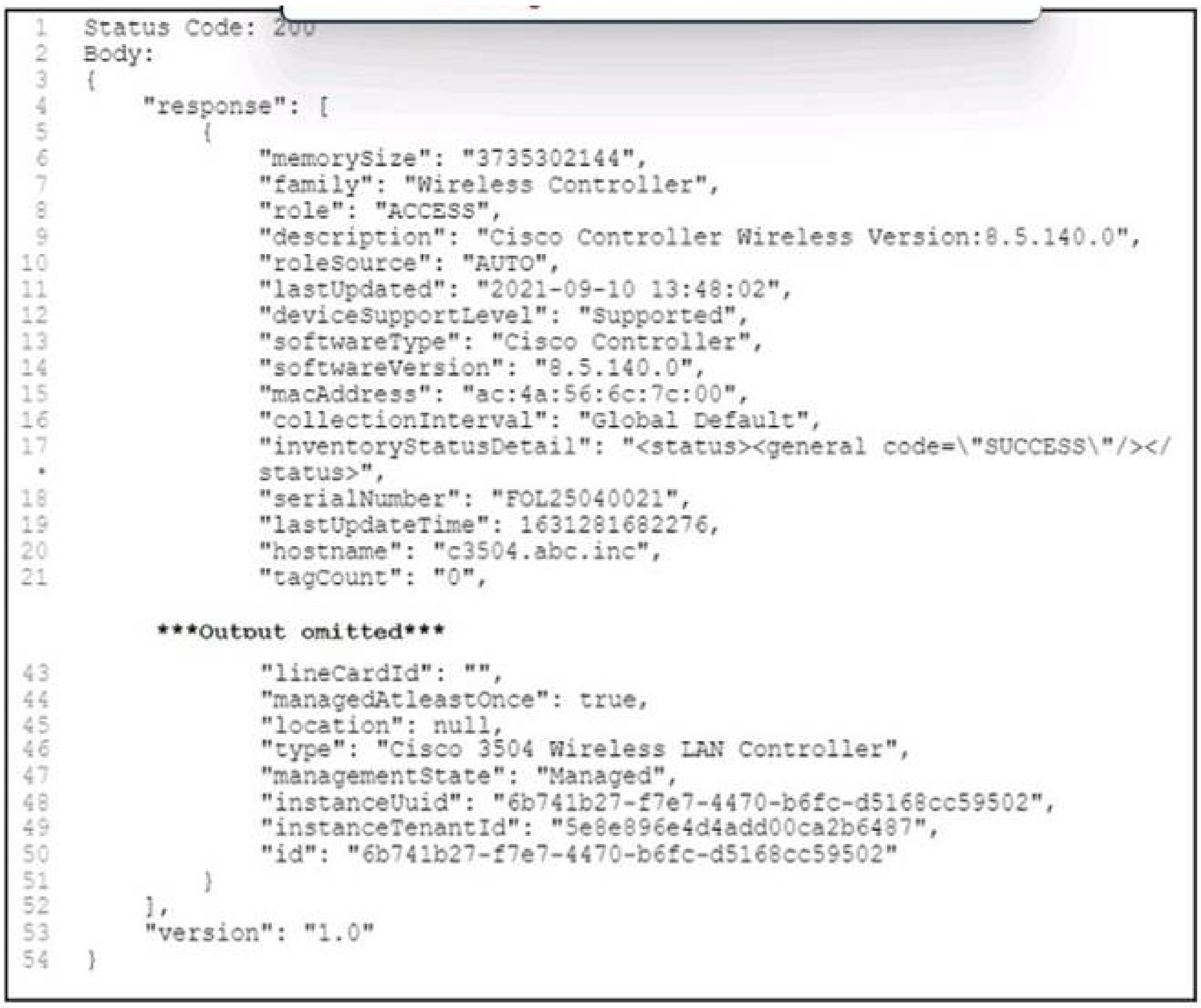
```
Tracing the route to 3.3.3.3

  1 10.99.69.2  36 msec
Received packet has options
Total option bytes = 40, padded length=40
  Record route:
     (10.99.69.1) <*>
     (0.0.0.0)
     (0.0.0.0)
   End of list

----output omitted---

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

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

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

Answer: C

NEW QUESTION 557
- (Topic 4)
Refer to the exhibit.



```
Status Code: 200
Body:
{
    "response": [
        {
            "memorySize": "3735302144",
            "family": "Wireless Controller",
            "role": "ACCESS",
            "description": "Cisco Controller Wireless Version:8.5.140.0",
            "roleSource": "AUTO",
            "lastUpdated": "2021-09-10 13:48:02",
            "deviceSupportLevel": "Supported",
            "softwareType": "Cisco Controller",
            "softwareVersion": "8.5.140.0",
            "macAddress": "ac:4a:56:6c:7c:00",
            "collectionInterval": "Global Default",
            "inventoryStatusDetail": "<status><general code=\"SUCCESS\"/></
            status>",
            "serialNumber": "FOL25040021",
            "lastUpdateTime": 1631281682276,
            "hostname": "c3504.abc.inc",
            "tagCount": "0",

     ***Output omitted***

            "lineCardId": "",
            "managedAtleastOnce": true,
            "location": null,
            "type": "Cisco 3504 Wireless LAN Controller",
            "managementState": "Managed",
            "instanceUuid": "6b741b27-f7e7-4470-b6fc-d5168cc59502",
            "instanceTenantId": "5e8e896e4d4add00ca2b6487",
            "id": "6b741b27-f7e7-4470-b6fc-d5168cc59502"
        }
    ],
    "version": "1.0"
}
```

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

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

Answer: C

Explanation:
This is because the REST API response shows the details of a network device with the specified MAC address. The GET method is used to retrieve information

from the Cisco DNA Center server. The network-device resource is used to access the network device inventory. The macAddress parameter is used to filter the results by the MAC address of the device. The source of this answer is the Cisco ENCOR v1.1 course, module 8, lesson 8.4: Implementing REST API.

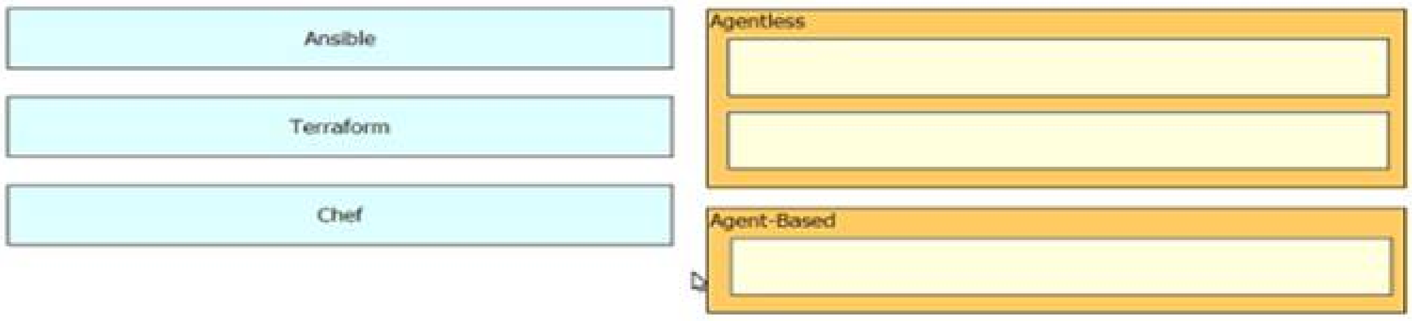
NEW QUESTION 562
- (Topic 4)
Which of the following fiber connector types is the most likely to be used on a network interface card?

A. LC
B. SC
C. ST
D. MPO

Answer: A

Explanation:
This is because the LC connector is a small form factor connector that is commonly used on network interface cards (NICs) and transceivers. The LC connector has a push-pull locking mechanism that makes it easy to insert and remove. The LC connector can support both single-mode and multimode fibers. The LC connector is also compatible with the SFP and SFP+ transceiver modules that are widely used on NICs. The source of this answer is the Cisco ENCOR v1.1 course, module 1, lesson 1.3: Comparing Copper and Fiber Cabling.

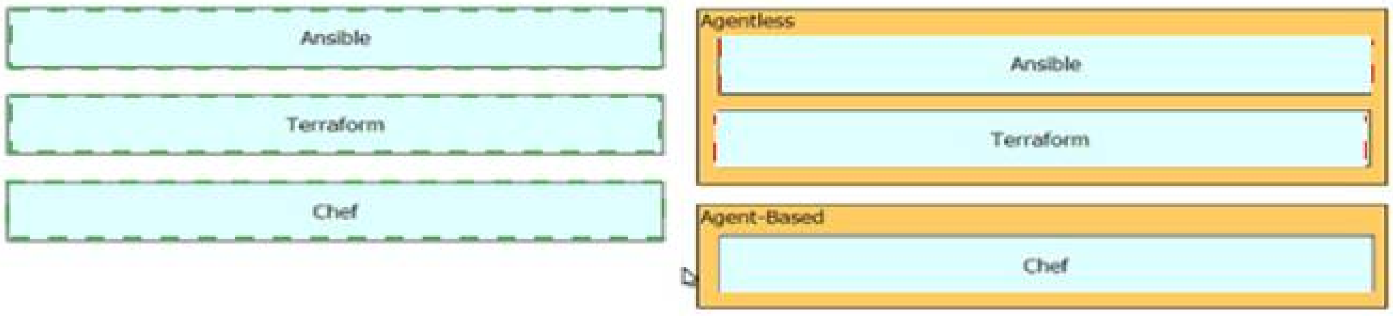
NEW QUESTION 566
DRAG DROP - (Topic 4)
Drag and drop the tools from the left onto the agent types on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

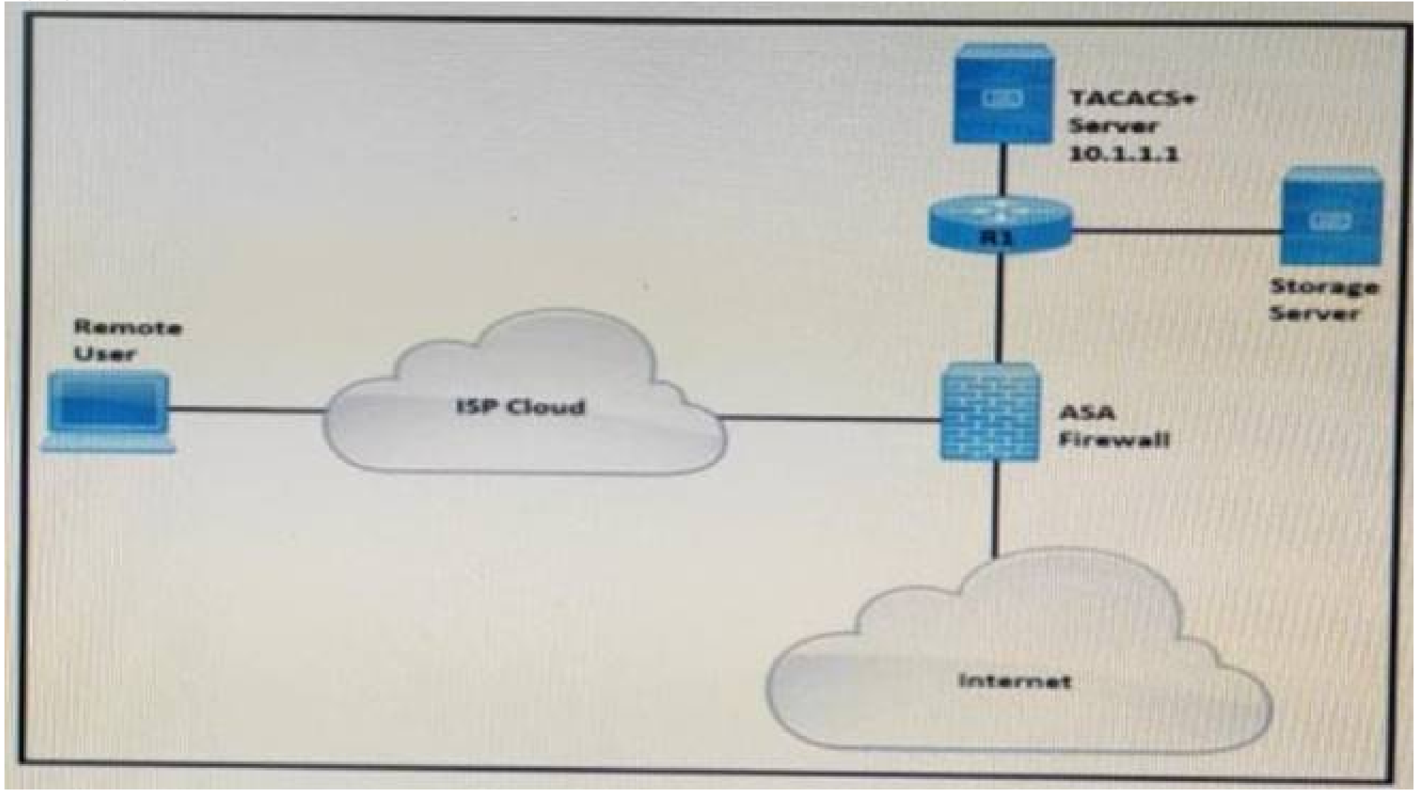


Ansible
Terraform
Chef

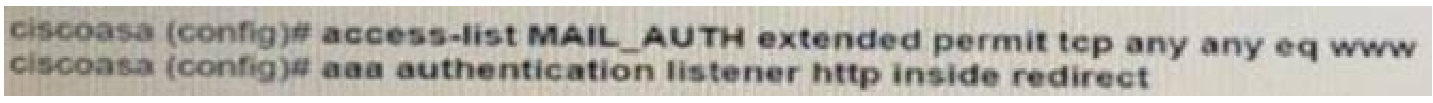
Agentless
Ansible
Terraform

Agent-Based
Chef

NEW QUESTION 569
- (Topic 4)

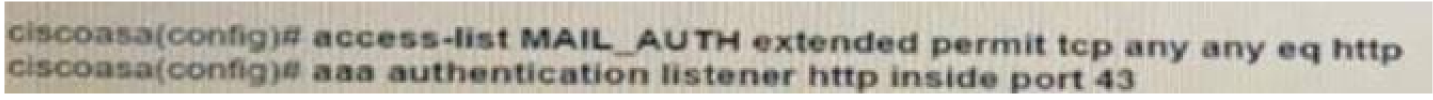


Refer to the exhibit Remote users cannot access the Internet but can upload files to the storage server Which configuration must be applied to allow Internet access?
A)



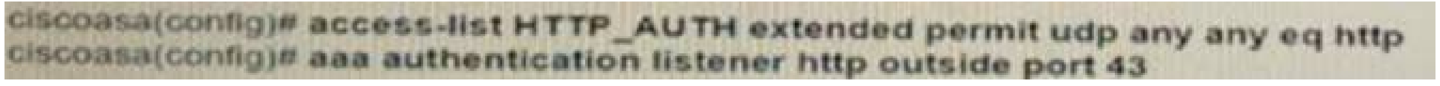
```
ciscoasa (config)# access-list MAIL_AUTH extended permit tcp any any eq www
ciscoasa (config)# aaa authentication listener http inside redirect
```

B)



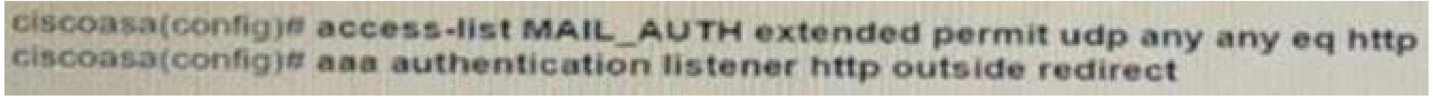
```
ciscoasa(config)# access-list MAIL_AUTH extended permit tcp any any eq http
ciscoasa(config)# aaa authentication listener http inside port 43
```

C)



```
ciscoasa(config)# access-list HTTP_AUTH extended permit udp any any eq http
ciscoasa(config)# aaa authentication listener http outside port 43
```

D)



```
ciscoasa(config)# access-list MAIL_AUTH extended permit udp any any eq http
ciscoasa(config)# aaa authentication listener http outside redirect
```

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

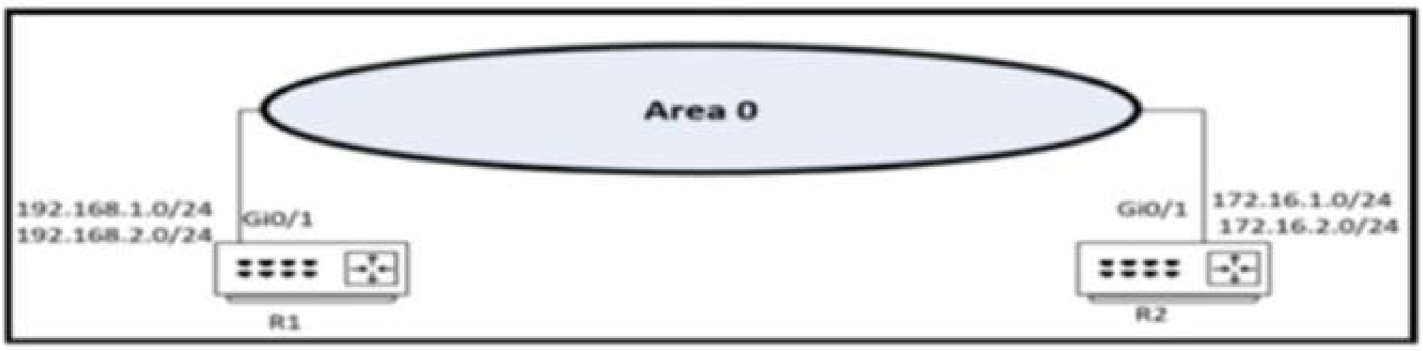
Answer: A

NEW QUESTION 570
- (Topic 4)
How does Cisco Express Forwarding switching differ from process switching on Cisco devices?

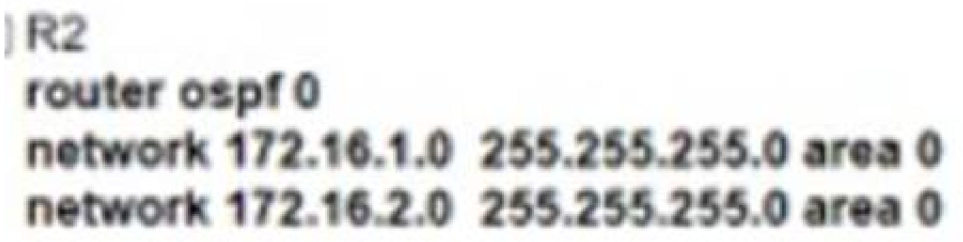
A. Cisco Express Forwarding switching uses adjacency tables built by the CDP protocol, and process switching uses the routing table.
B. Cisco Express Forwarding switching uses dedicated hardware processors, and process switching uses the main processor.
C. Cisco Express Forwarding swithing saves memory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

Answer: C

NEW QUESTION 575
- (Topic 4)

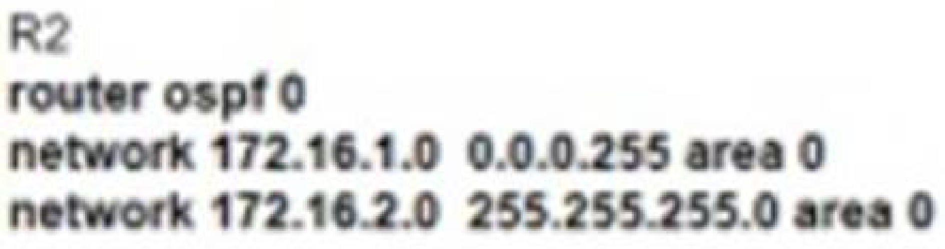


Refer to the exhibit. Which two configurations enable R1 and R2 to advertise routes into OSPF? (Choose two)
A)



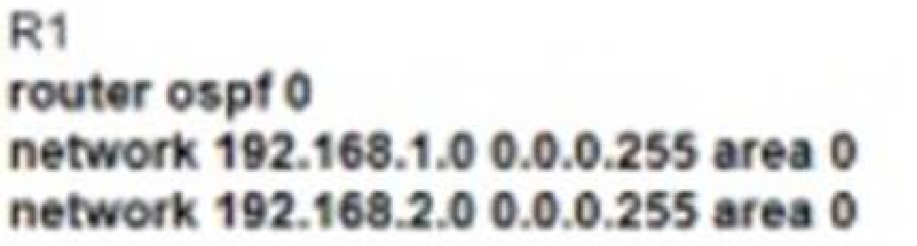
```
R2
router ospf 0
network 172.16.1.0  255.255.255.0 area 0
network 172.16.2.0  255.255.255.0 area 0
```

B)



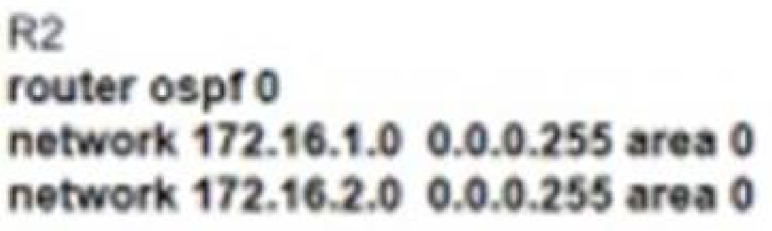
```
R2
router ospf 0
network 172.16.1.0  0.0.0.255 area 0
network 172.16.2.0  255.255.255.0 area 0
```

C)



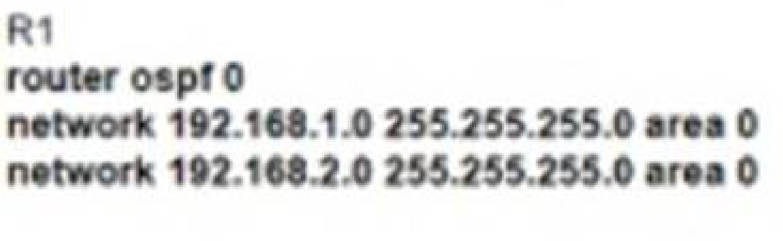
```
R1
router ospf 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
```

D)



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

E)



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

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

Answer: CD

NEW QUESTION 578
- (Topic 4)
How does a Type 1 hypervisor function?

A. It runs directly on a physical server and depends on a previously installed operating system.
B. It runs directly on a physical server and includes its own operating system.
C. It runs on a virtual server and depends on a previously installed operating systems
D. It runs on a virtual server and includes its own operating system.

Answer: B

Explanation:
A type 1 hypervisor, also known as a bare-metal or native hypervisor, runs directly on the physical server and its underlying hardware. It does not depend on a previously installed operating system, but rather includes its own operating system that is designed to run virtual machines. A type 1 hypervisor provides excellent performance and stability, as it has direct access to the hardware resources and can allocate them to the virtual machines. A type 1 hypervisor is typically used in enterprise environments, where multiple virtual machines run on a single server.
Reference: What is a Hypervisor? Types of Hypervisors 1 & 2 - phoenixNAP

NEW QUESTION 582
- (Topic 2)
What occurs when a high bandwidth multicast stream is sent over an MVPN using Cisco hardware?

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

Answer: D

NEW QUESTION 583
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

350-401 Practice Exam Features:

* 350-401 Questions and Answers Updated Frequently

* 350-401 Practice Questions Verified by Expert Senior Certified Staff

* 350-401 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

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