Cisco

Exam Questions 350-401

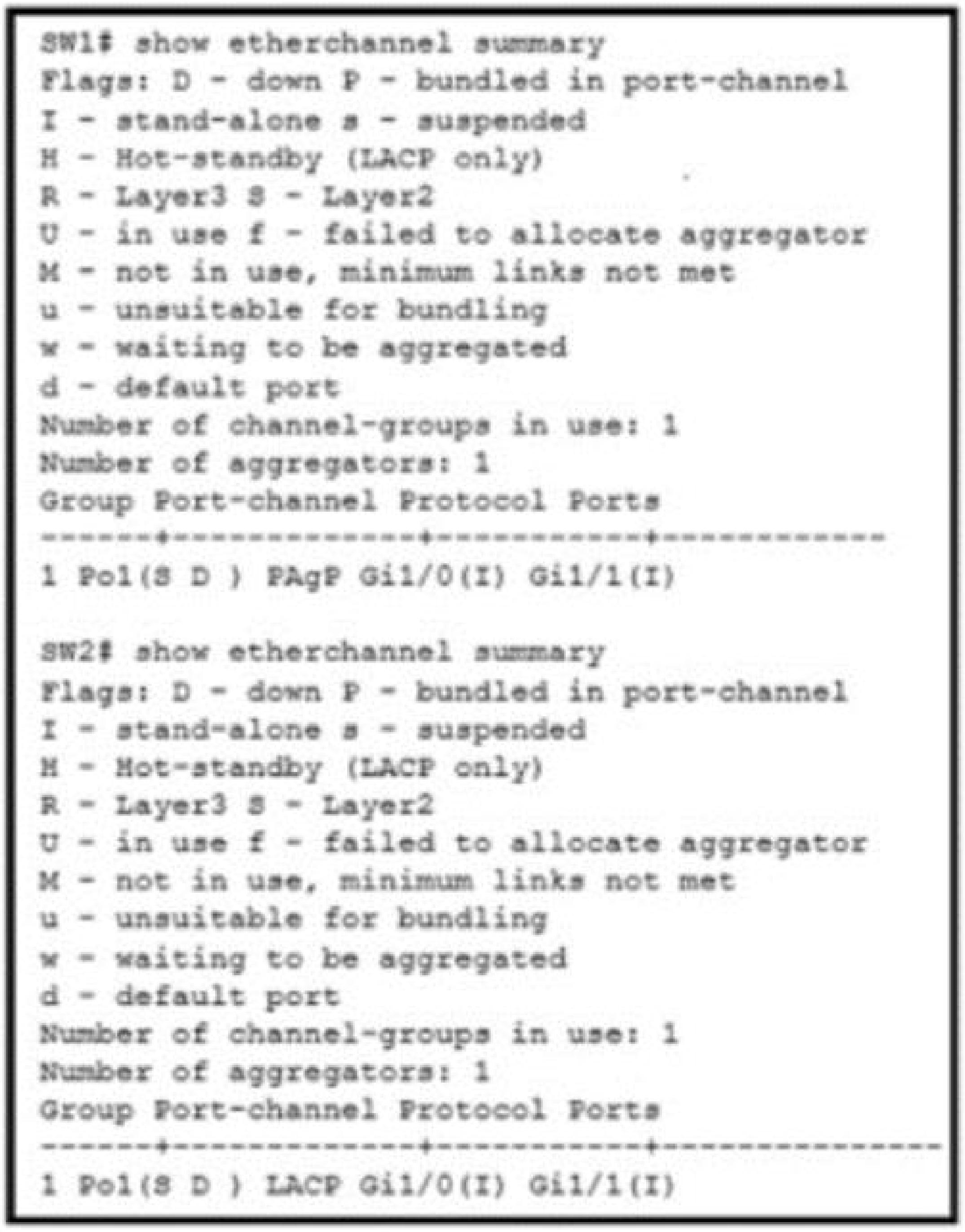
Implementing and Operating Cisco Enterprise Network Core Technologies

NEW QUESTION 1
- (Topic 4)
Which access control feature does MAB provide?

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

Answer: C

NEW QUESTION 2
- (Topic 4)



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

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

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

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

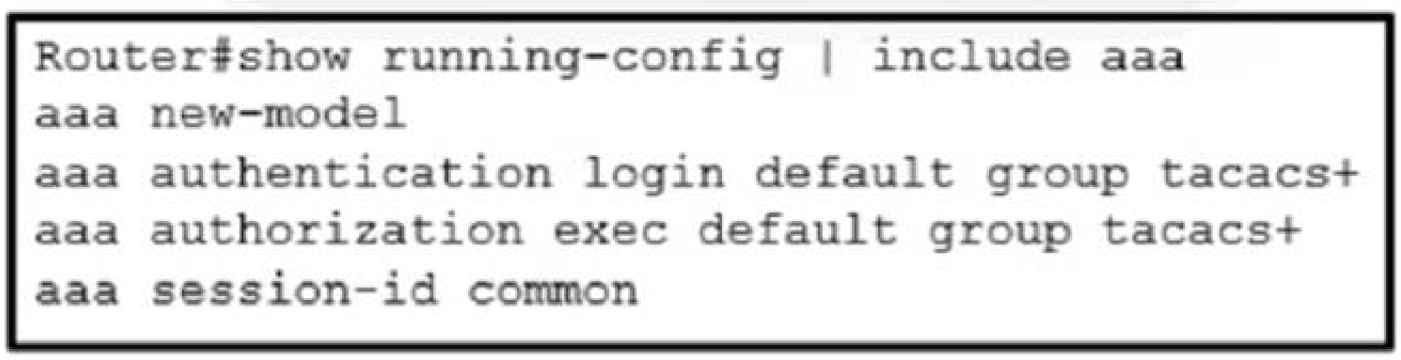
Answer: C

NEW QUESTION 3
- (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 4
- (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 5
- (Topic 4)
By default, which virtual MAC address does HSRP group 30 use?

A. 00:05:0c:07:ac:30
B. 00:00:0c:07:ac:1e
C. 05:0c:5e:ac:07:30
D. 00:42:18:14:05:1e

Answer: B

NEW QUESTION 6
- (Topic 4)
A customer has 20 stores located throughout a city. Each store has a single Cisco access point managed by a central WLC. The customer wants to gather analysis for users in each store. Which technique supports these requirements?

A. angle of arrival
B. hyperlocation
C. trilateration
D. presence

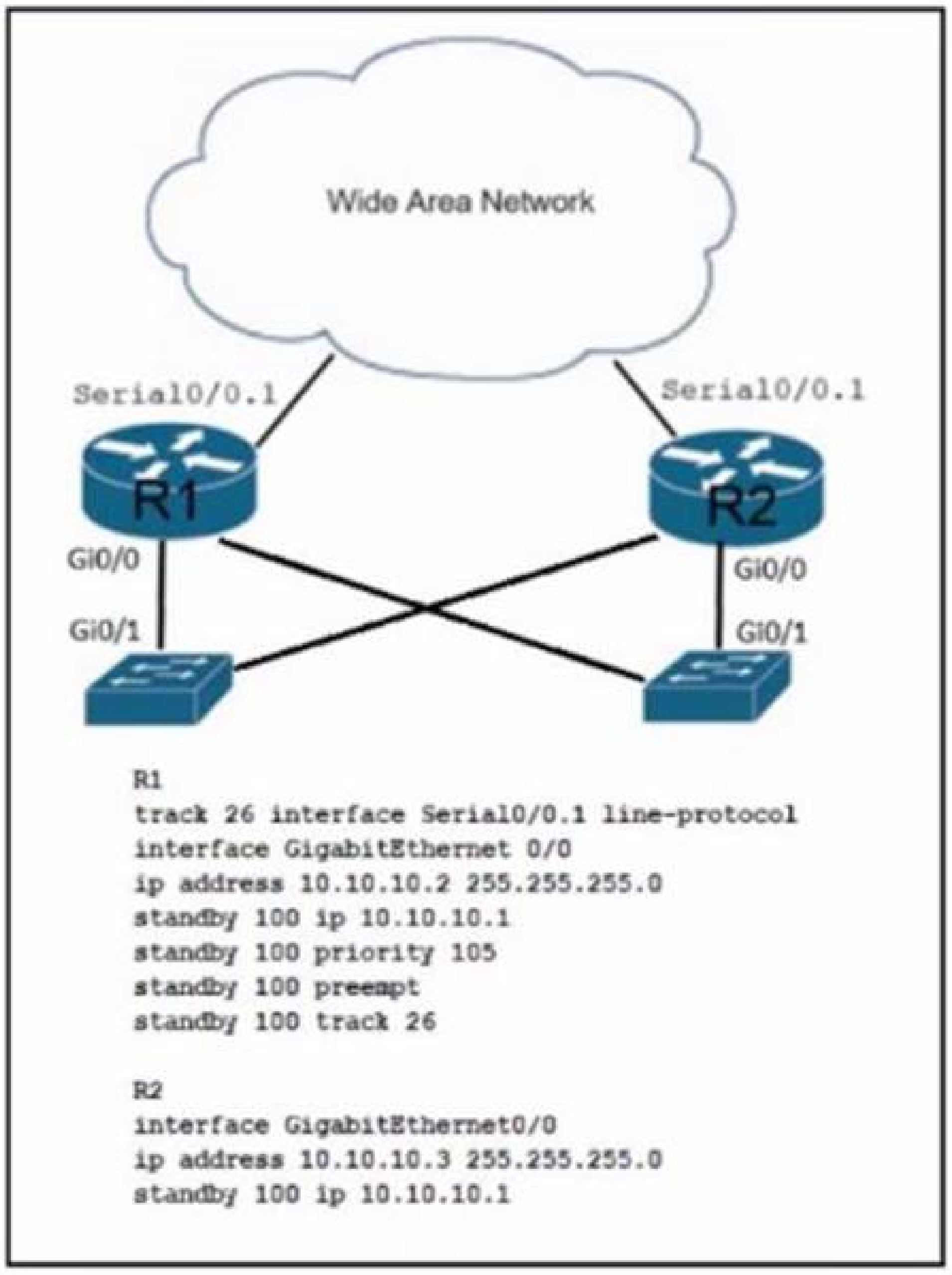
Answer: B

NEW QUESTION 7
- (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 8
- (Topic 4)
Relet lo Ibe exhibit.



```
R1
track 26 interface Serial0/0.1 line-protocol
interface GigabitEthernet 0/0
ip address 10.10.10.2 255.255.255.0
standby 100 ip 10.10.10.1
standby 100 priority 105
standby 100 preempt
standby 100 track 26

R2
interface GigabitEthernet0/0
ip address 10.10.10.3 255.255.255.0
standby 100 ip 10.10.10.1
```

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

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

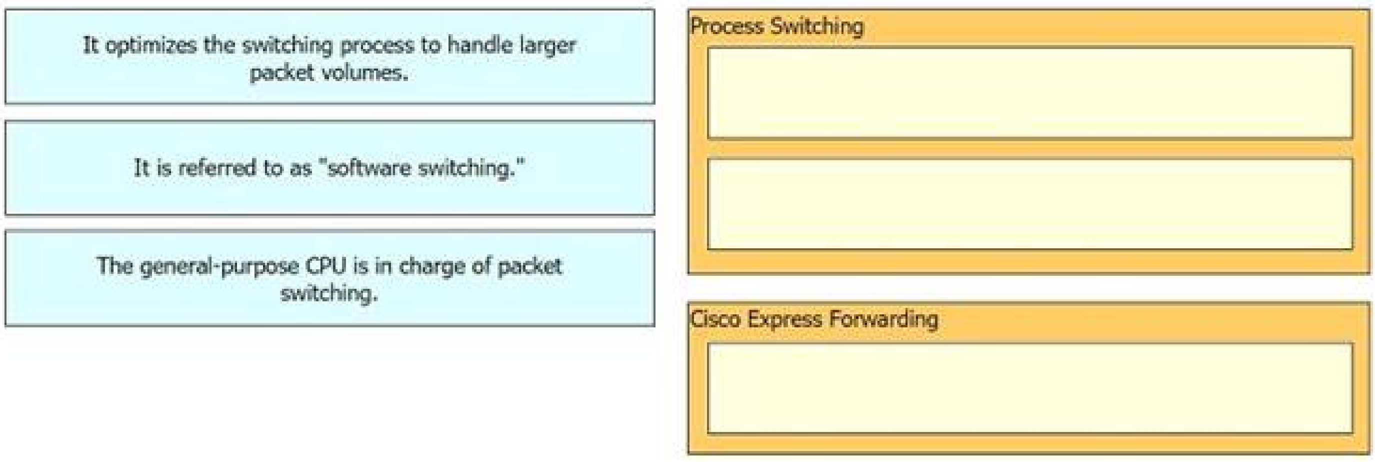
Answer: A

NEW QUESTION 9
- (Topic 4)
An engineer must configure router R1 to validate user logins via RADIUS and fall back to the local user database if the RADIUS server is not available. Which configuration must be applied?

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

Answer: C

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



It optimizes the switching process to handle larger packet volumes.

It is referred to as "software switching."

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

Process Switching

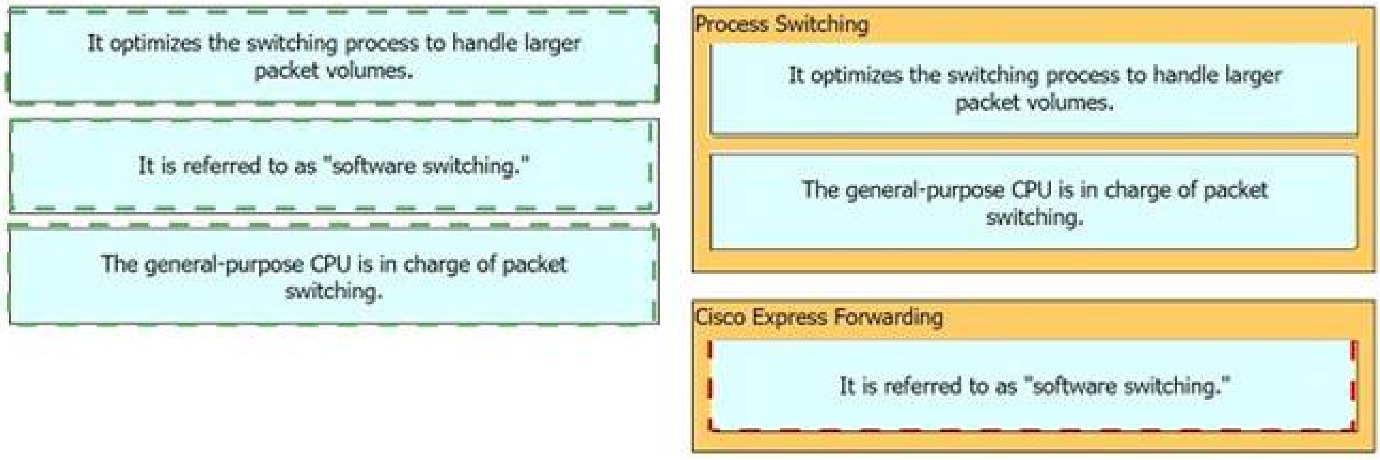
Cisco Express Forwarding

A. Mastered

B. Not Mastered

Answer: A

Explanation:



It optimizes the switching process to handle larger packet volumes.

It is referred to as "software switching."

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

Process Switching

It optimizes the switching process to handle larger packet volumes.

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

Cisco Express Forwarding

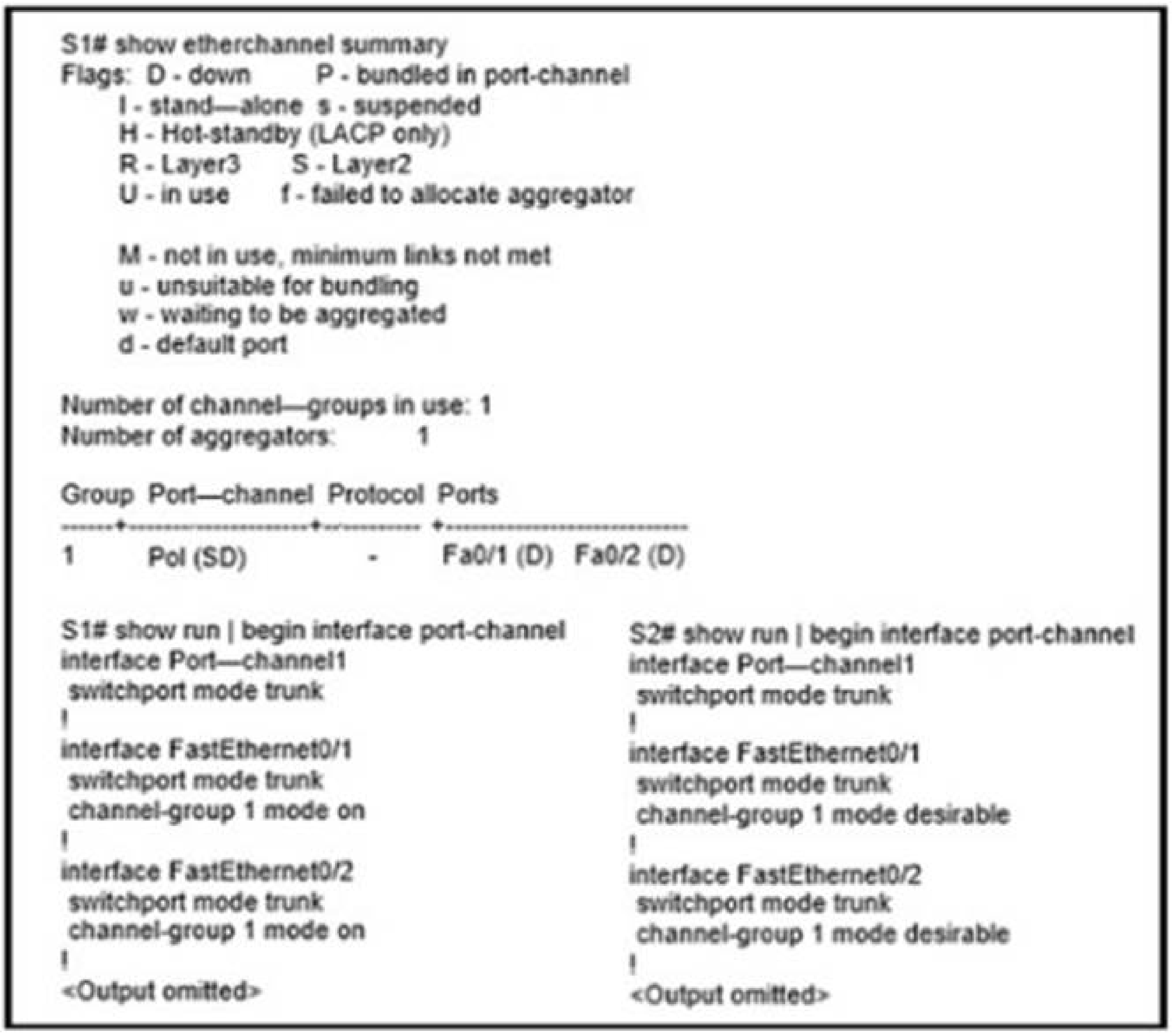
It is referred to as "software switching."

NEW QUESTION 10
- (Topic 4)
What is a benefit of Cisco TrustSec in a multilayered LAN network design?

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

Answer: C

NEW QUESTION 14
- (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>
```

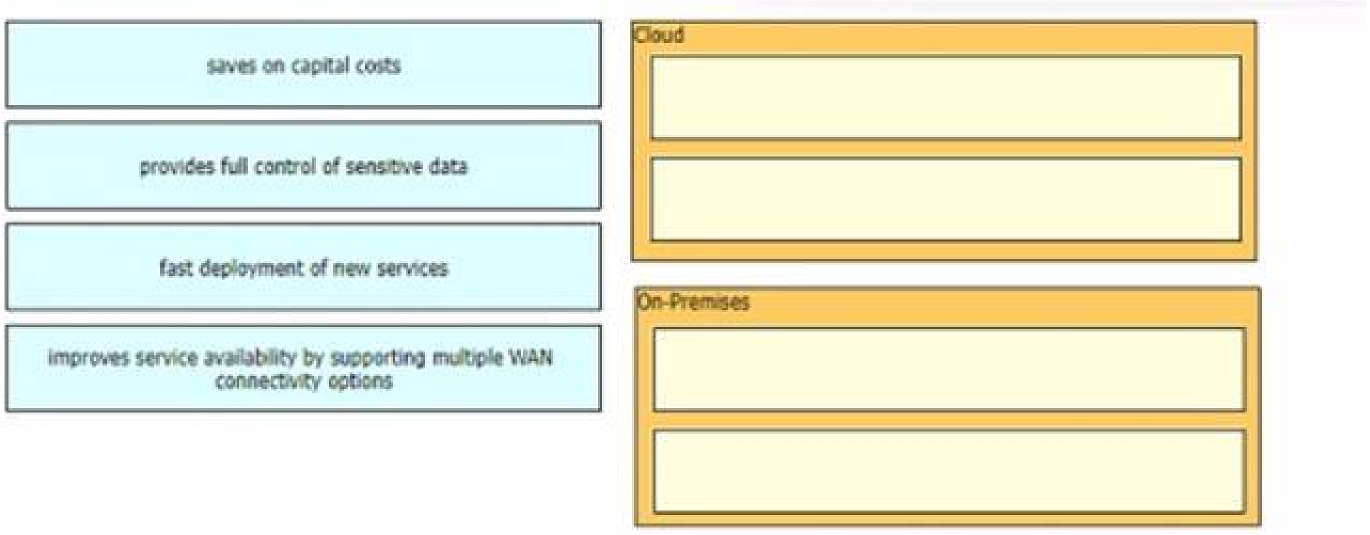
```
S2# show run | begin interface port-channel
interface Port—channel1
 switchport mode trunk
!
interface FastEthernet0/1
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 1 mode desirable
!
<Output omitted>
```

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

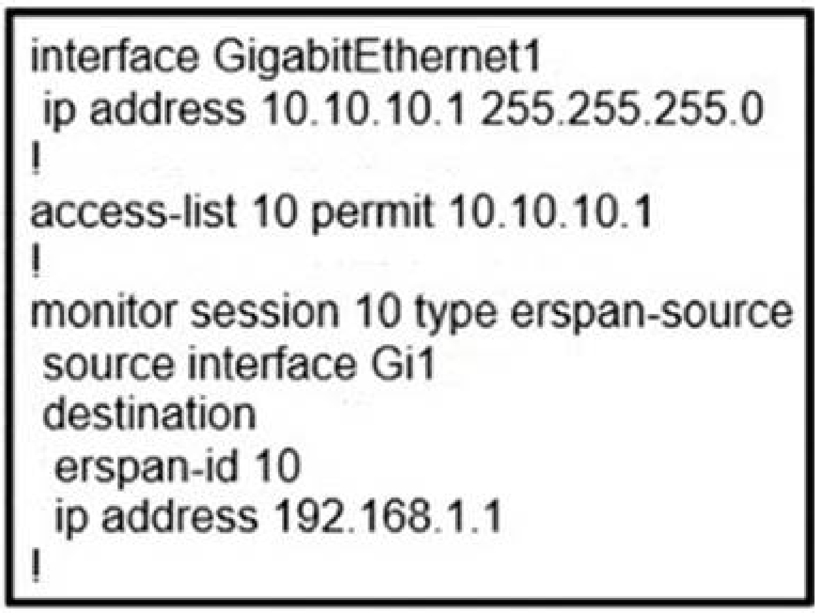

saves on capital costs
provides full control of sensitive data
fast deployment of new services
improves service availability by supporting multiple WAN connectivity options
Cloud
On-Premises

A. Mastered
B. Not Mastered

Answer: A

Explanation:
CLOUD1 and 3ON-PREMISES2 and 4

NEW QUESTION 21
- (Topic 4)



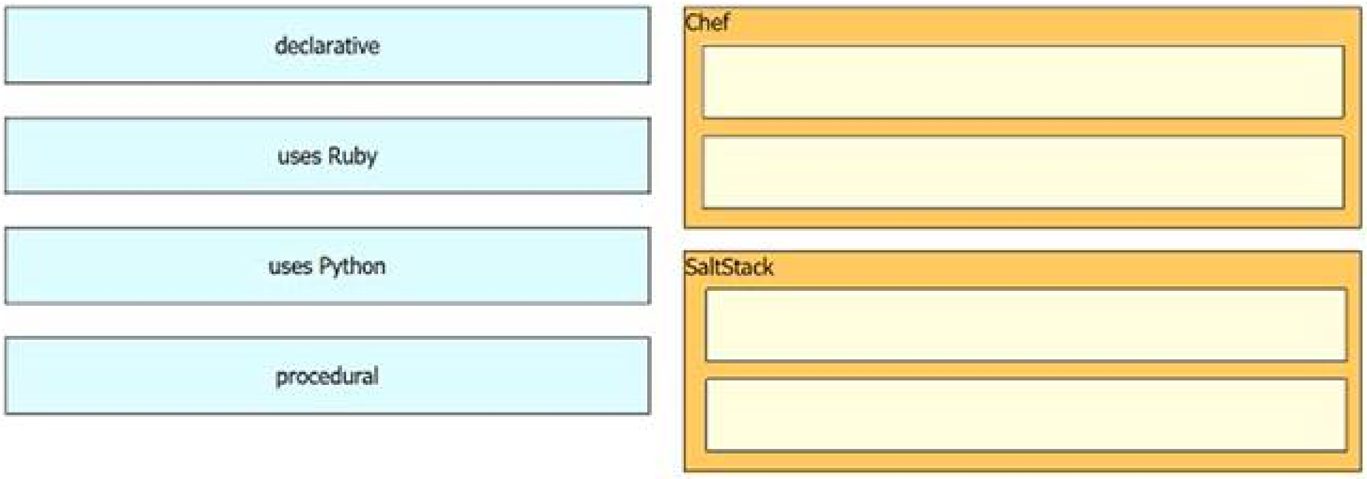
```
interface GigabitEthernet1
 ip address 10.10.10.1 255.255.255.0
!
access-list 10 permit 10.10.10.1
!
monitor session 10 type erspan-source
 source interface Gi1
 destination
  erspan-id 10
  ip address 192.168.1.1
!
```

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

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

Answer: C

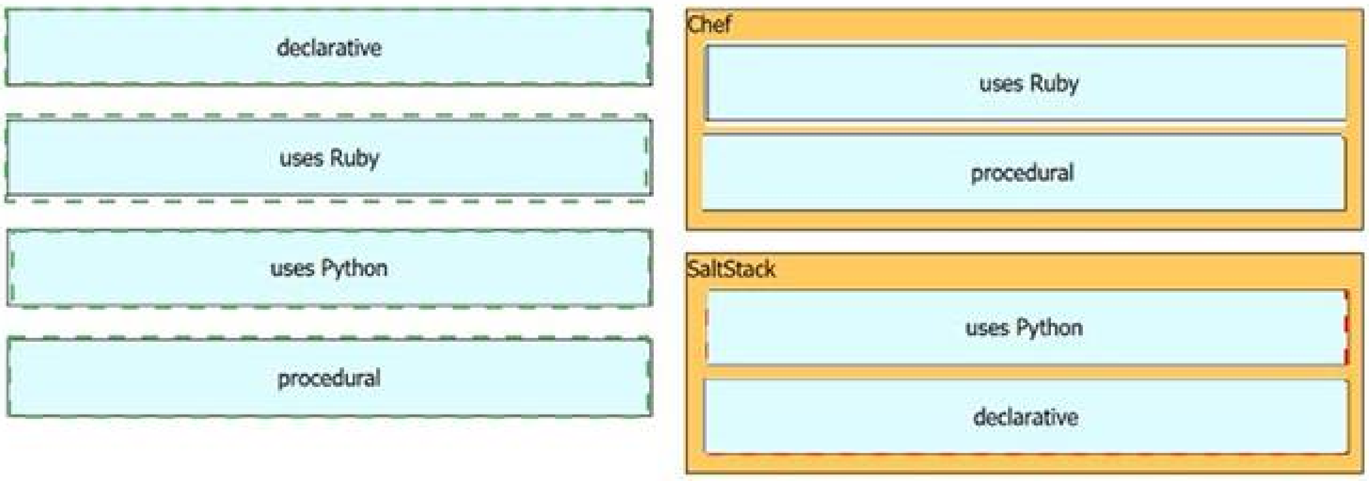
NEW QUESTION 24
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 27
- (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 31
- (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

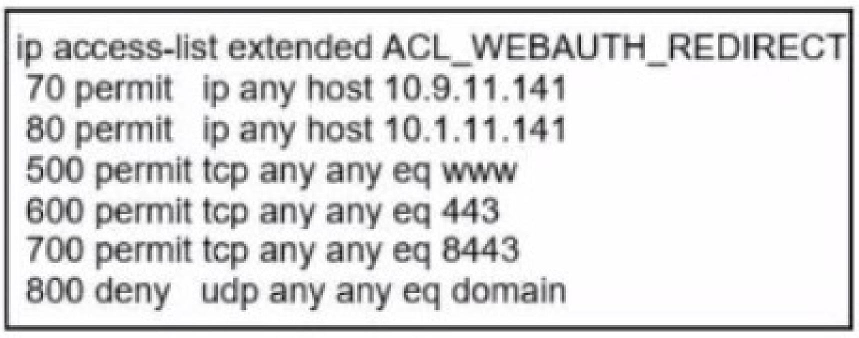
NEW QUESTION 34
- (Topic 4)
Where in Cisco DNA Center is documentation of each API call, organized by its functional area?

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

Answer: A

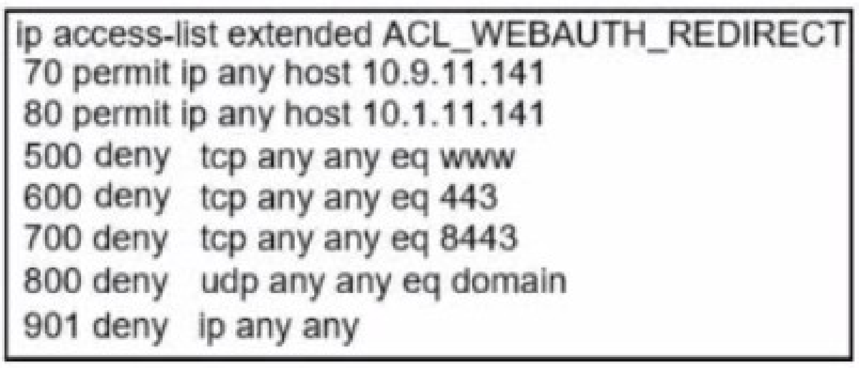
Explanation:
https://developer.cisco.com/docs/dna-center/#!api-quick-start/cisco-dna-center-platform-api-overview

NEW QUESTION 35
- (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)



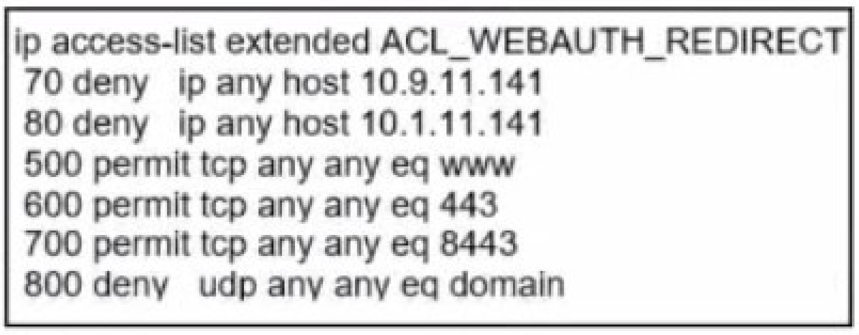
```
ip access-list extended ACL_WEBAUTH_REDIRECT
 70 permit   ip any host 10.9.11.141
 80 permit   ip any host 10.1.11.141
 500 permit tcp any any eq www
 600 permit tcp any any eq 443
 700 permit tcp any any eq 8443
 800 deny   udp any any eq domain
```

B)



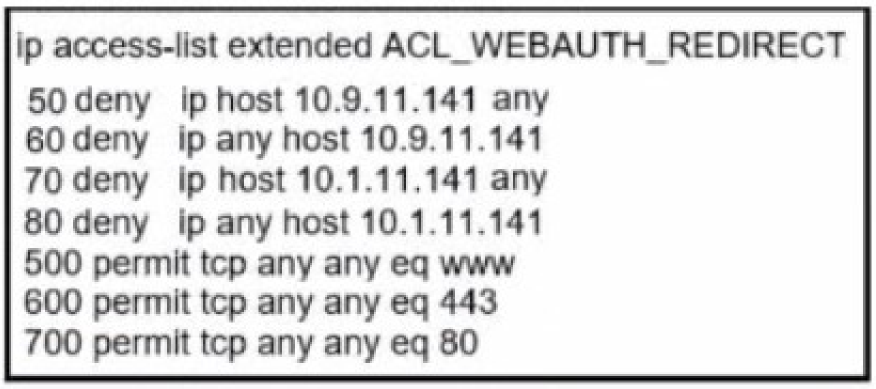
```
ip access-list extended ACL_WEBAUTH_REDIRECT
 70 permit ip any host 10.9.11.141
 80 permit ip any host 10.1.11.141
 500 deny   tcp any any eq www
 600 deny   tcp any any eq 443
 700 deny   tcp any any eq 8443
 800 deny   udp any any eq domain
 901 deny   ip any any
```

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

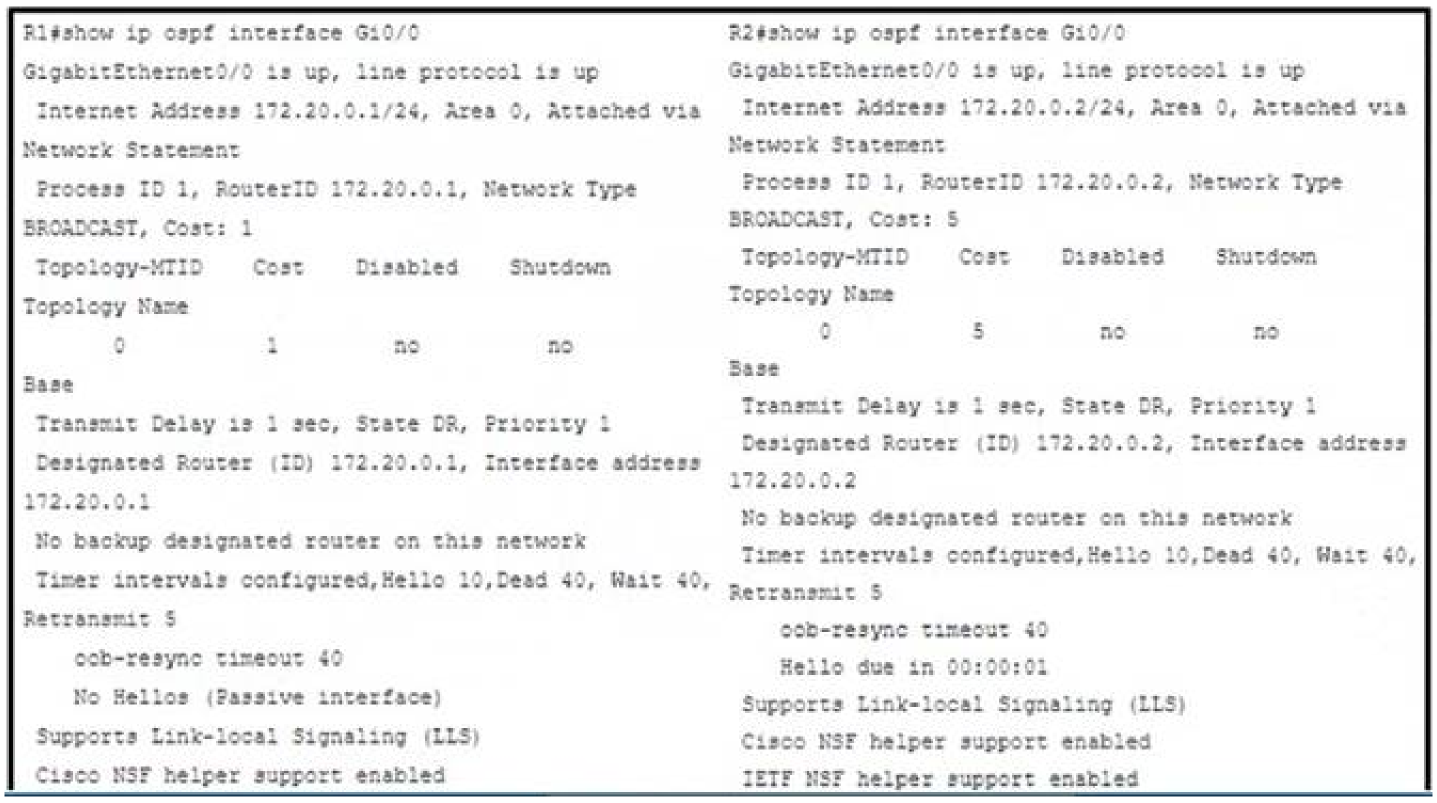
NEW QUESTION 37
- (Topic 4)
Which collection contains the resources to obtain a list of fabric nodes through the vManage API?

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

Answer: C

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

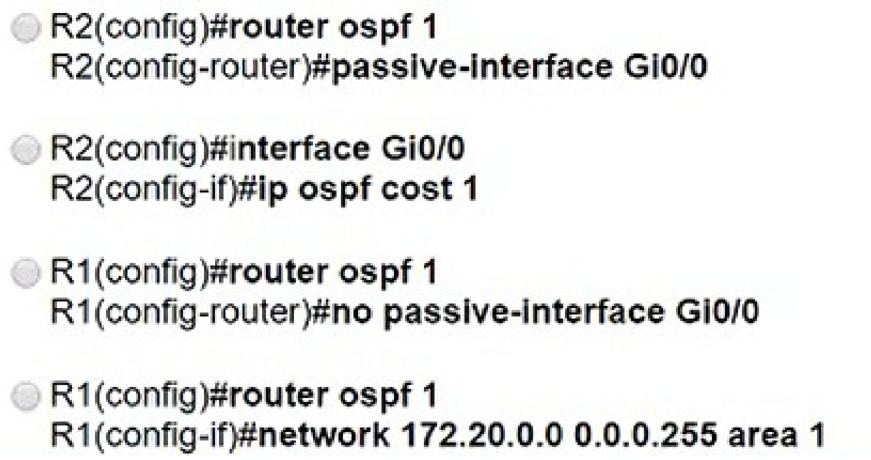
NEW QUESTION 39
- (Topic 4)



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

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

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



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

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

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

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

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

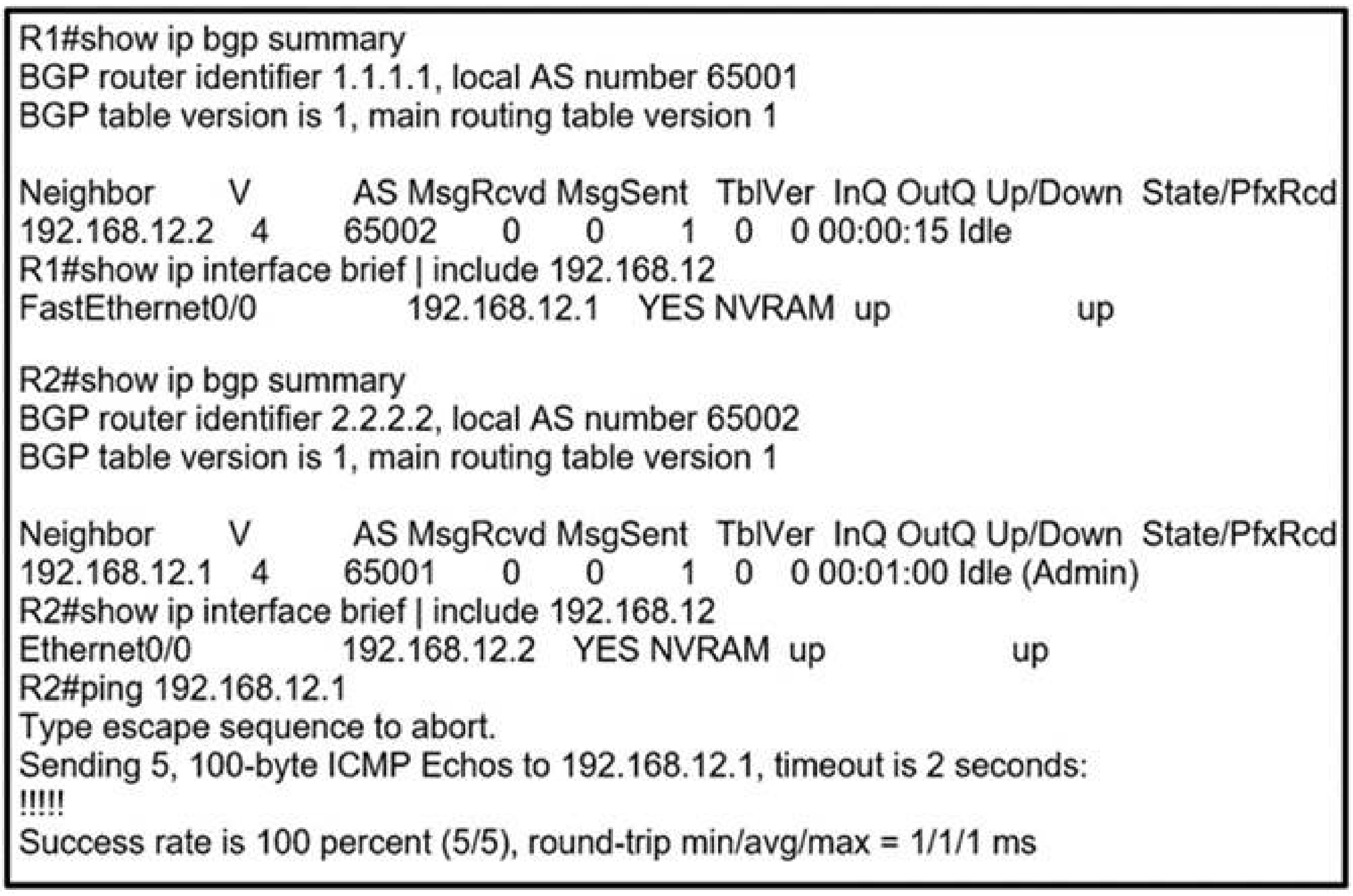
Answer: C

NEW QUESTION 42
- (Topic 4)
Where is the wireless LAN controller located in a mobility express deployment?

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

Answer: B

NEW QUESTION 47
- (Topic 4)



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

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

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

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

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

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

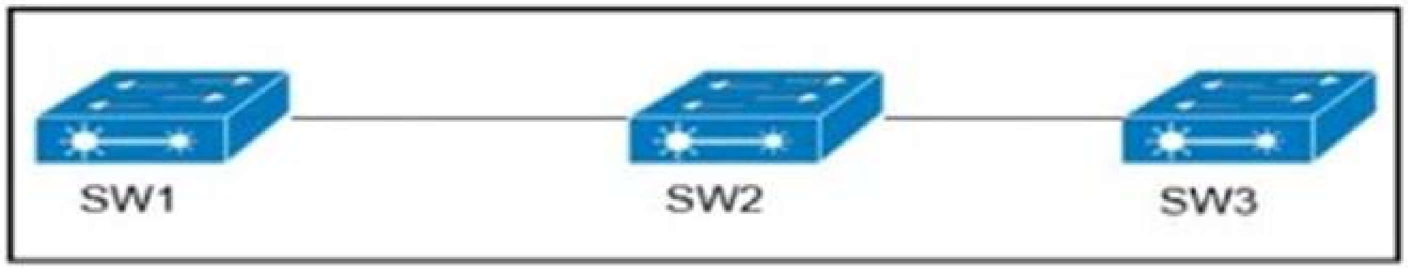
Answer: D

NEW QUESTION 48
- (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 49
- (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 53
- (Topic 1)
What is used to perform OoS packet classification?

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

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

Answer: D

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

NEW QUESTION 54
- (Topic 1)
Which method should an engineer use to deal with a long-standing contention issue between any two VMs on the same host?

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

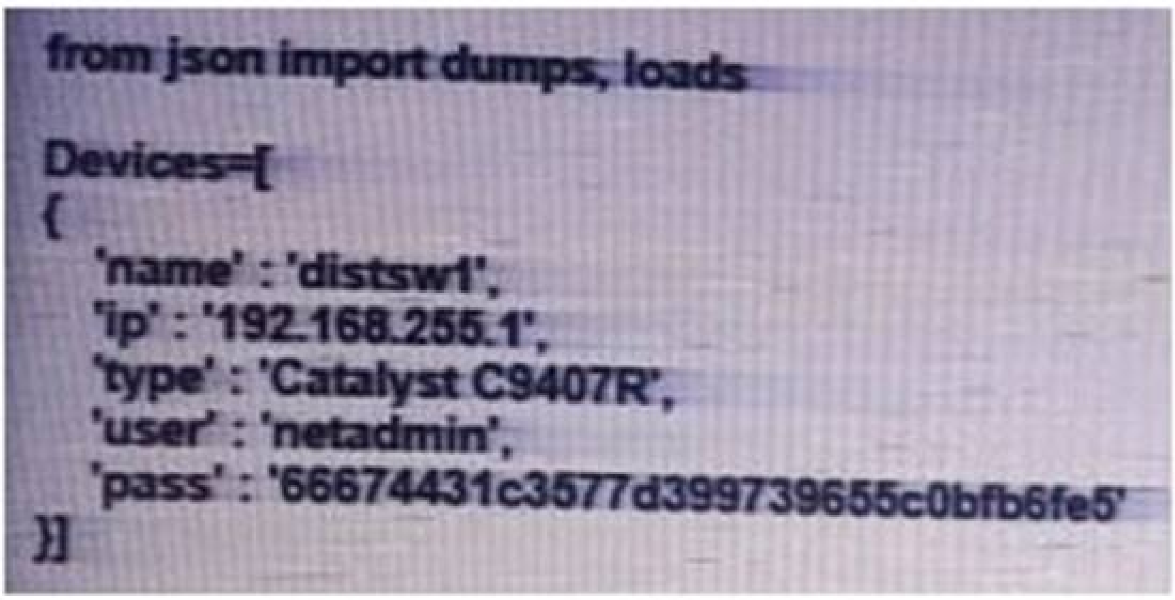
Answer: A

NEW QUESTION 55
- (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 59
- (Topic 2)
An engineer must export the contents of the devices object in JSON format. Which statement must be used?

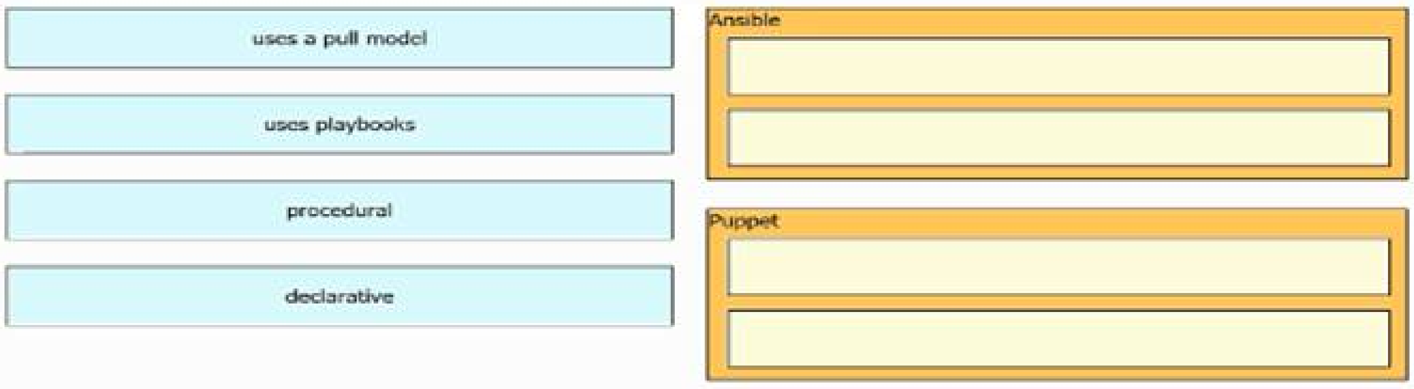


```
from json import dumps, loads

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

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

Answer: B

NEW QUESTION 62
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

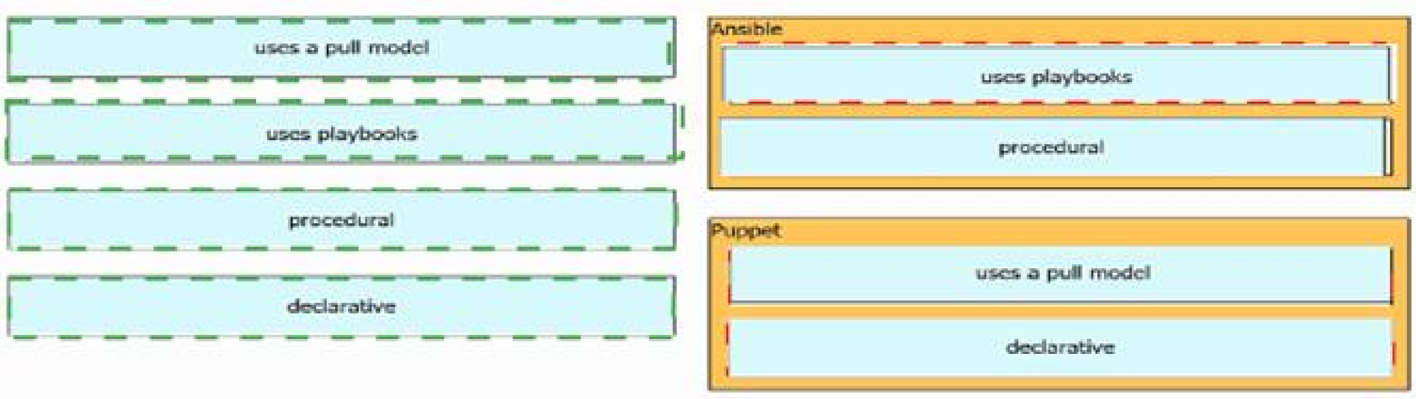
Ansible

Puppet

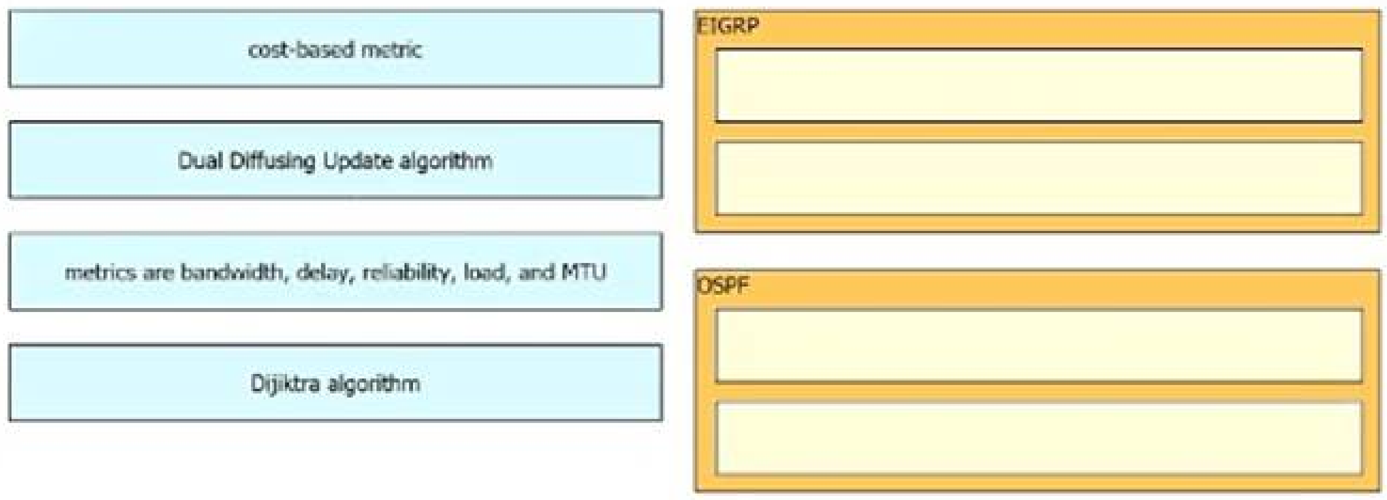
A. Mastered
B. Not Mastered

Answer: A

Explanation:



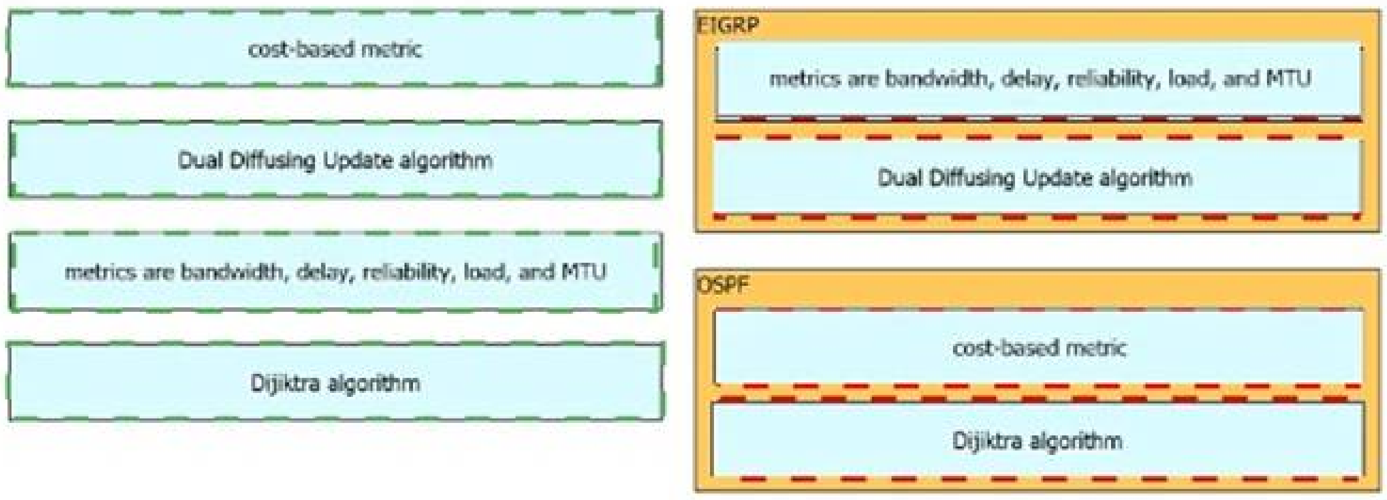
NEW QUESTION 64
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the routing protocols they describe on the right


cost-based metric
Dual Diffusing Update algorithm
metrics are bandwidth, delay, reliability, load, and MTU
Dijiktra algorithm
EIGRP
OSPF

A. Mastered
B. Not Mastered

Answer: A

Explanation:

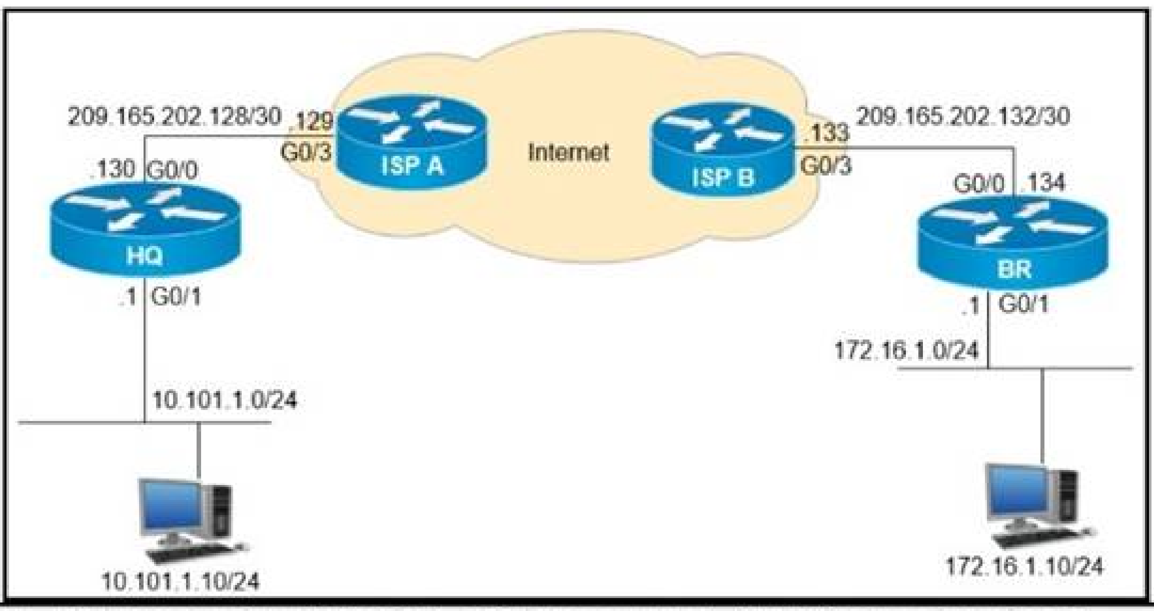

cost-based metric
Dual Diffusing Update algorithm
metrics are bandwidth, delay, reliability, load, and MTU
Dijiktra algorithm
EIGRP
metrics are bandwidth, delay, reliability, load, and MTU
Dual Diffusing Update algorithm
OSPF
cost-based metric
Dijiktra algorithm

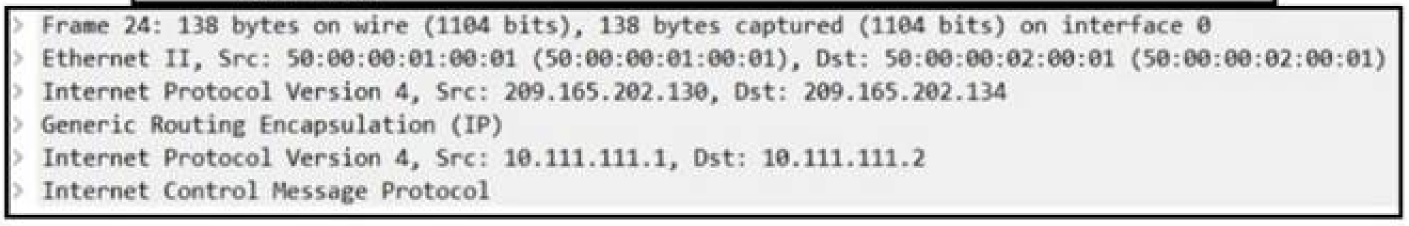
NEW QUESTION 68
- (Topic 2)
Why is an AP joining a different WLC than the one specified through option 43?

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 70
- (Topic 2)
Refer to the exhibit.





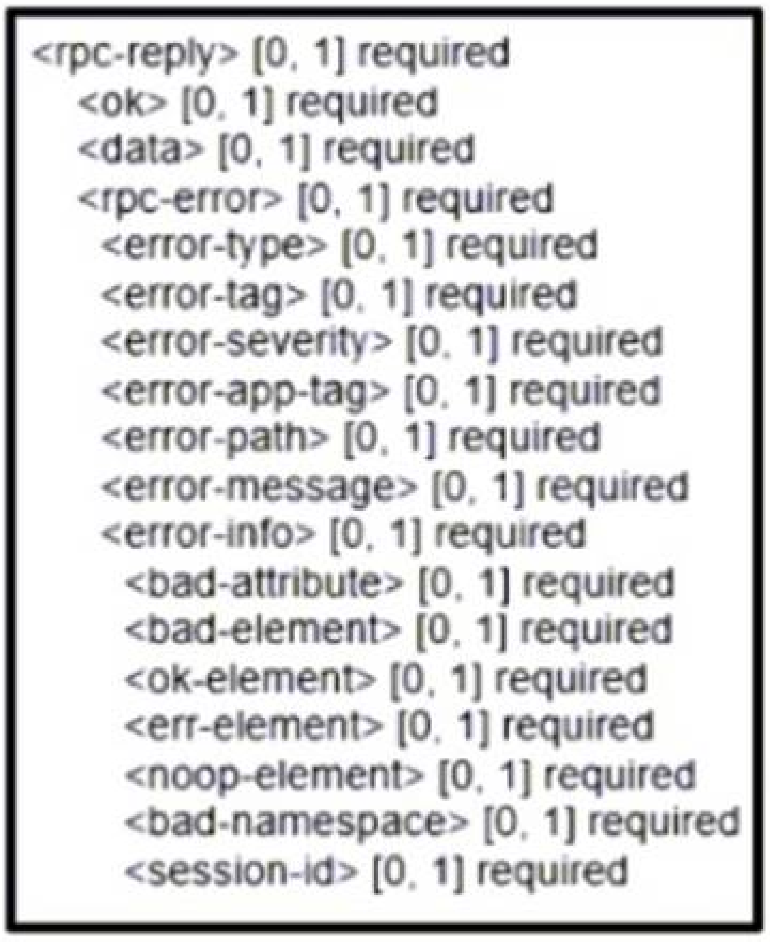
```
> Frame 24: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
> Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 50:00:00:02:00:01 (50:00:00:02:00:01)
> Internet Protocol Version 4, Src: 209.165.202.130, Dst: 209.165.202.134
> Generic Routing Encapsulation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

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

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

Answer: A

NEW QUESTION 73
- (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

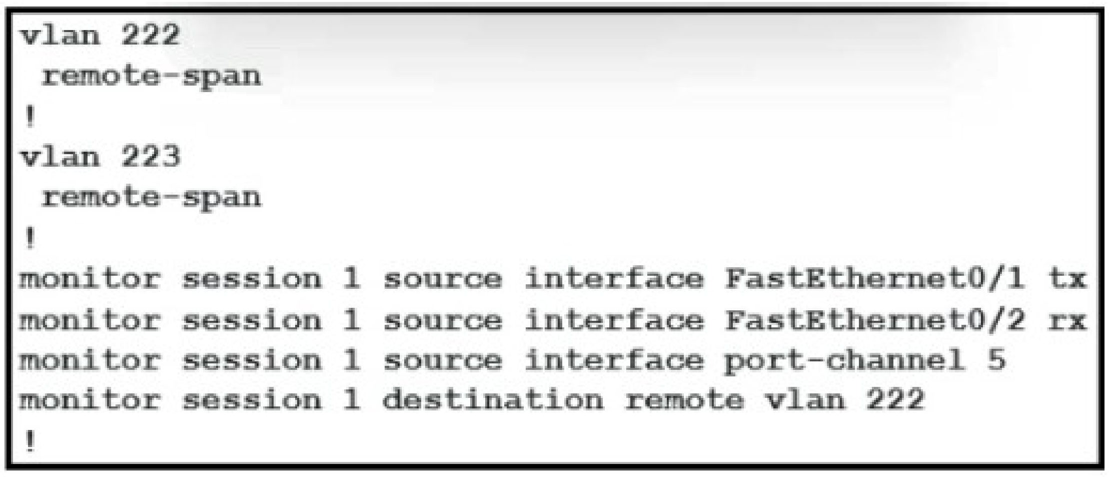
NEW QUESTION 74
- (Topic 2)
Which access point mode allows a supported AP to function like a WLAN client would, associating and identifying client connectivity issues?

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 78
- (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 83
- (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

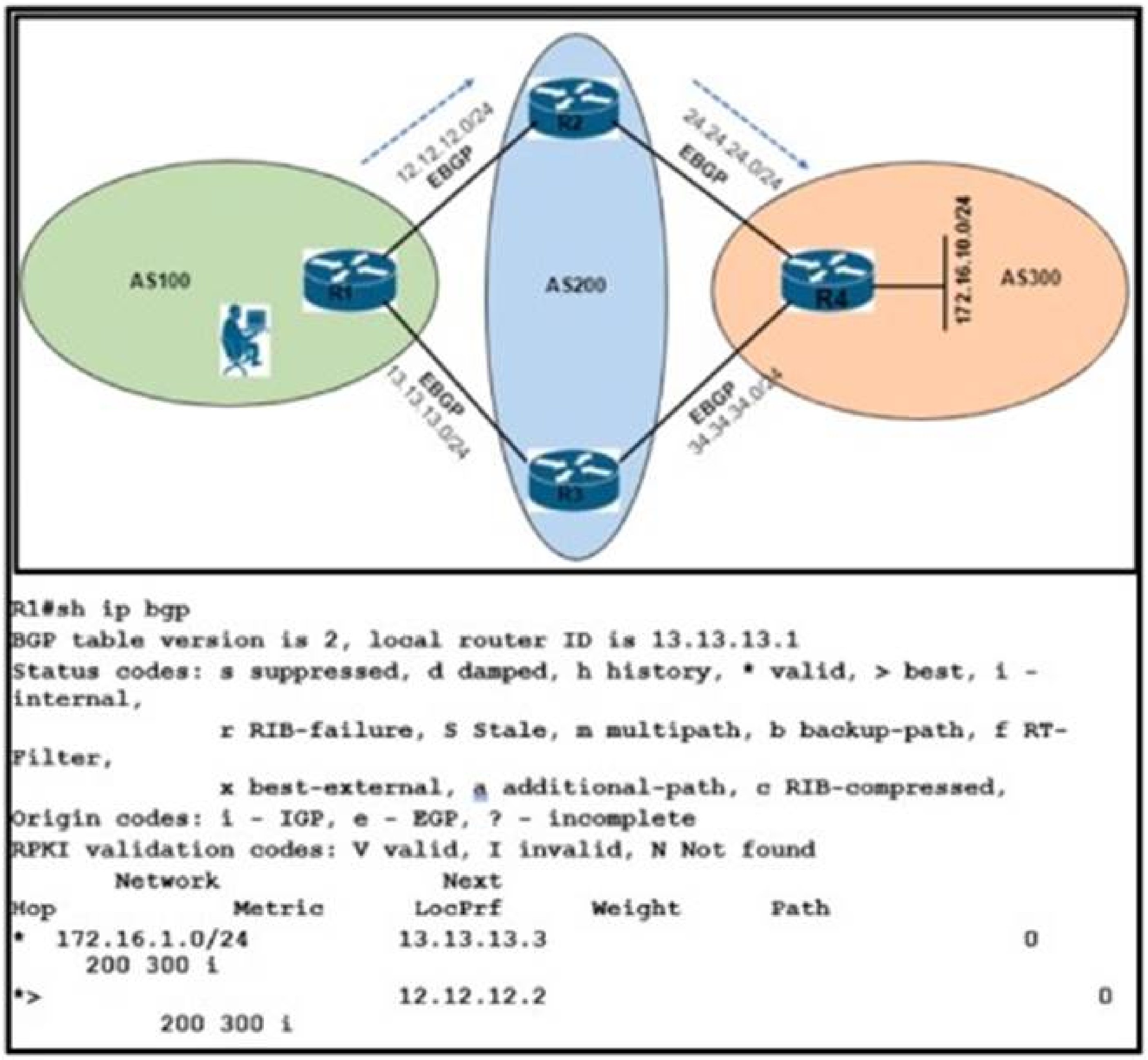
Explanation:
The Design area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Use the Design workflow if you do not already have an existing infrastructure. 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 87
- (Topic 2)
An engineer is implementing a Cisco MPLS TE tunnel to improve the streaming experience for the clients of a video-on-demand server. Which action must the engineer perform to configure extended discovery to support the MPLS LDP session between the headend and tailend routers?

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

Answer: B

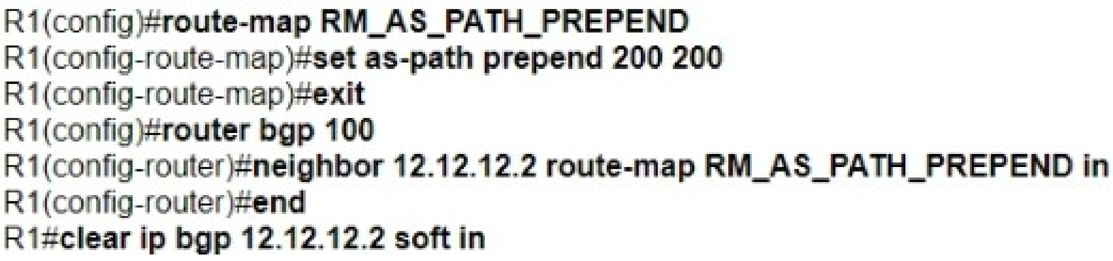
NEW QUESTION 92
- (Topic 2)
Refer to the exhibit.



```
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
```

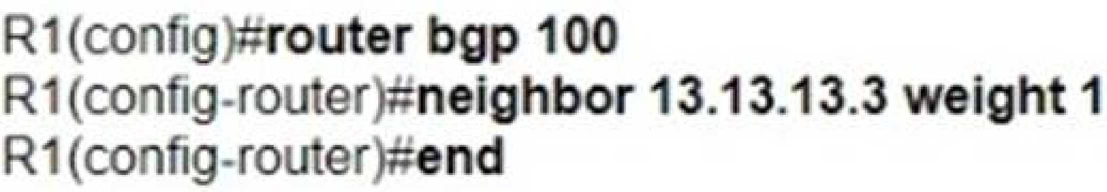
An engineers reaching network 172 16 10 0/24 via the R1-R2-R4 path. Which configuration forces the traffic to take a path of R1-R3-R4?

A)



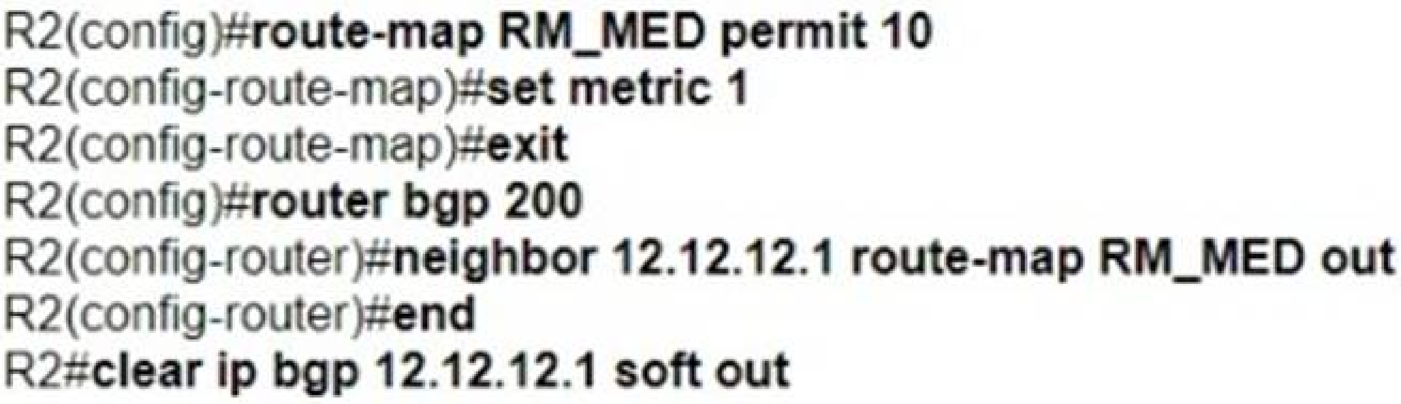
```
R1(config)#route-map RM_AS_PATH_PREPEND
R1(config-route-map)#set as-path prepend 200 200
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#neighbor 12.12.12.2 route-map RM_AS_PATH_PREPEND in
R1(config-router)#end
R1#clear ip bgp 12.12.12.2 soft in
```

B)



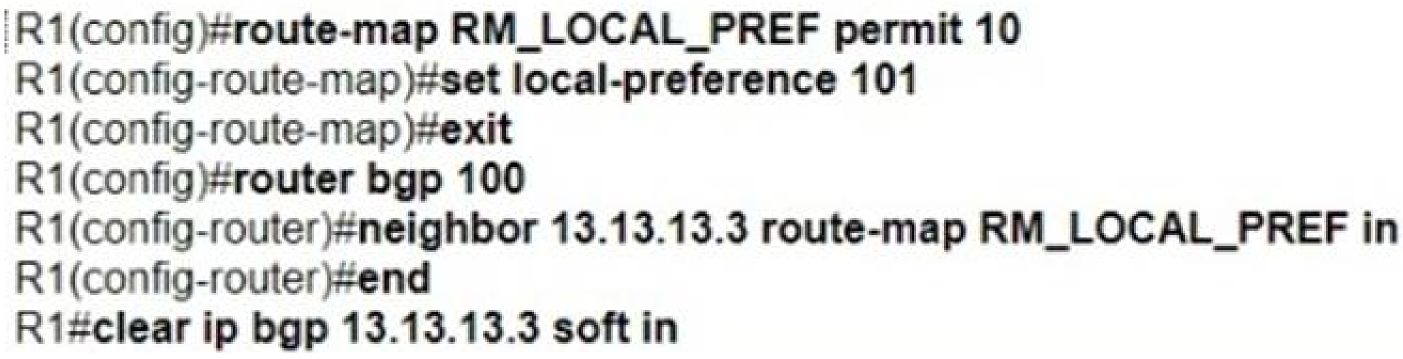
```
R1(config)#router bgp 100
R1(config-router)#neighbor 13.13.13.3 weight 1
R1(config-router)#end
```

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 94
- (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 97
- (Topic 2)
What is required for a virtual machine to run?

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

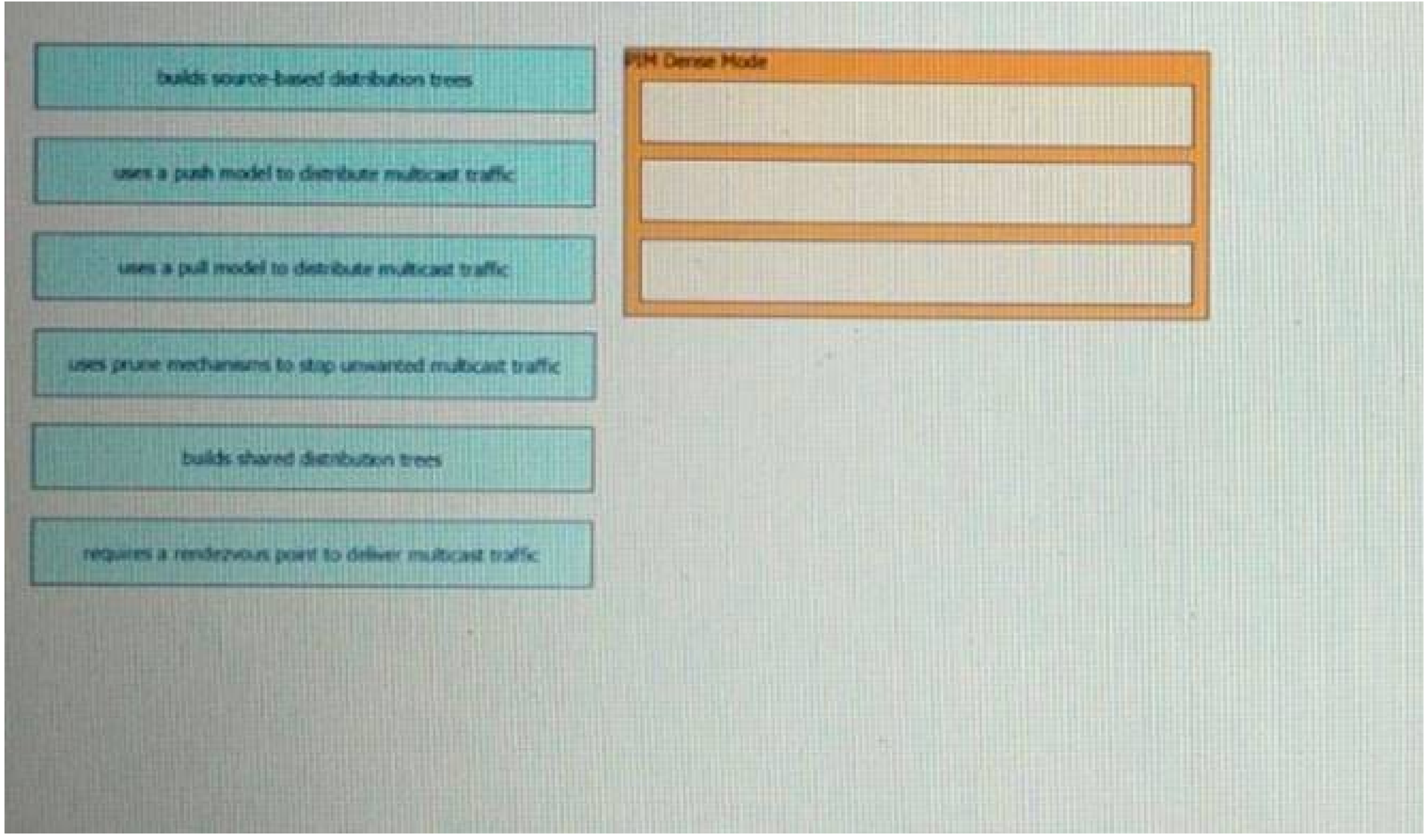
Answer: B

NEW QUESTION 101
- (Topic 2)
Which element enables communication between guest VMs within a virtualized environment?

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

Answer: B

NEW QUESTION 105
DRAG DROP - (Topic 2)
Drag and drop characteristics of PIM dense mode from the left to the right.



builds source-based distribution trees

uses a push model to distribute multicast traffic

uses a pull model to distribute multicast traffic

uses prune mechanisms to stop unwanted multicast traffic

builds shared distribution trees

requires a rendezvous point to deliver multicast traffic

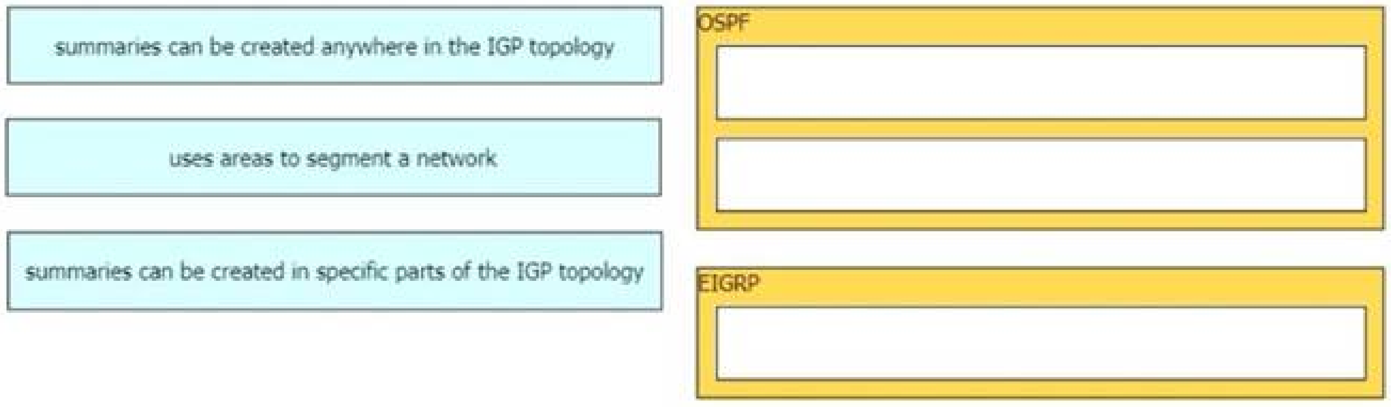
PIM Dense Mode

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 109
DRAG DROP - (Topic 2)
Drag and drop the descriptions from the left onto the routing protocol they describe on the right.



summaries can be created anywhere in the IGP topology

uses areas to segment a network

summaries can be created in specific parts of the IGP topology

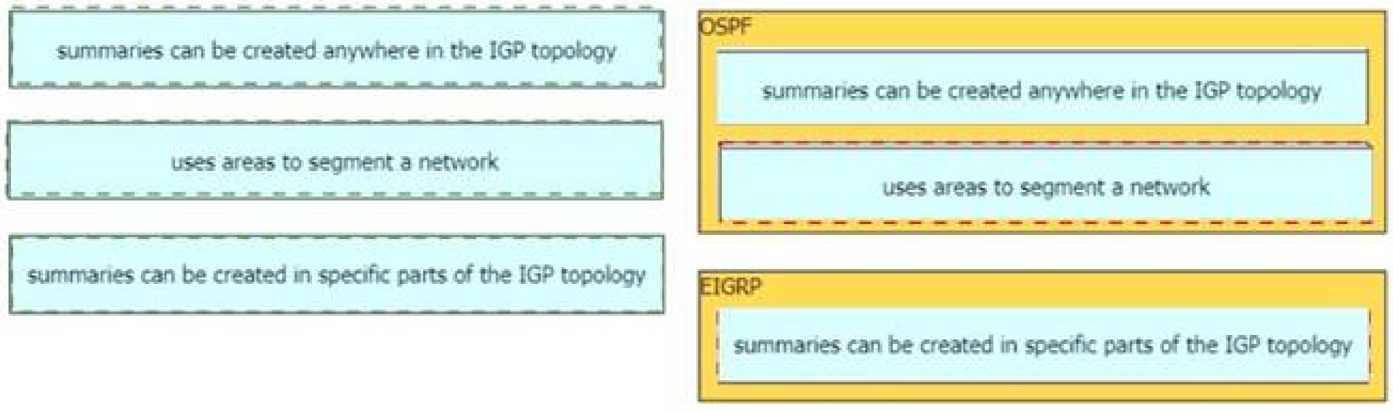
OSPF

EIGRP

A. Mastered
B. Not Mastered

Answer: A

Explanation:



summaries can be created anywhere in the IGP topology

uses areas to segment a network

summaries can be created in specific parts of the IGP topology

OSPF

summaries can be created anywhere in the IGP topology

uses areas to segment a network

EIGRP

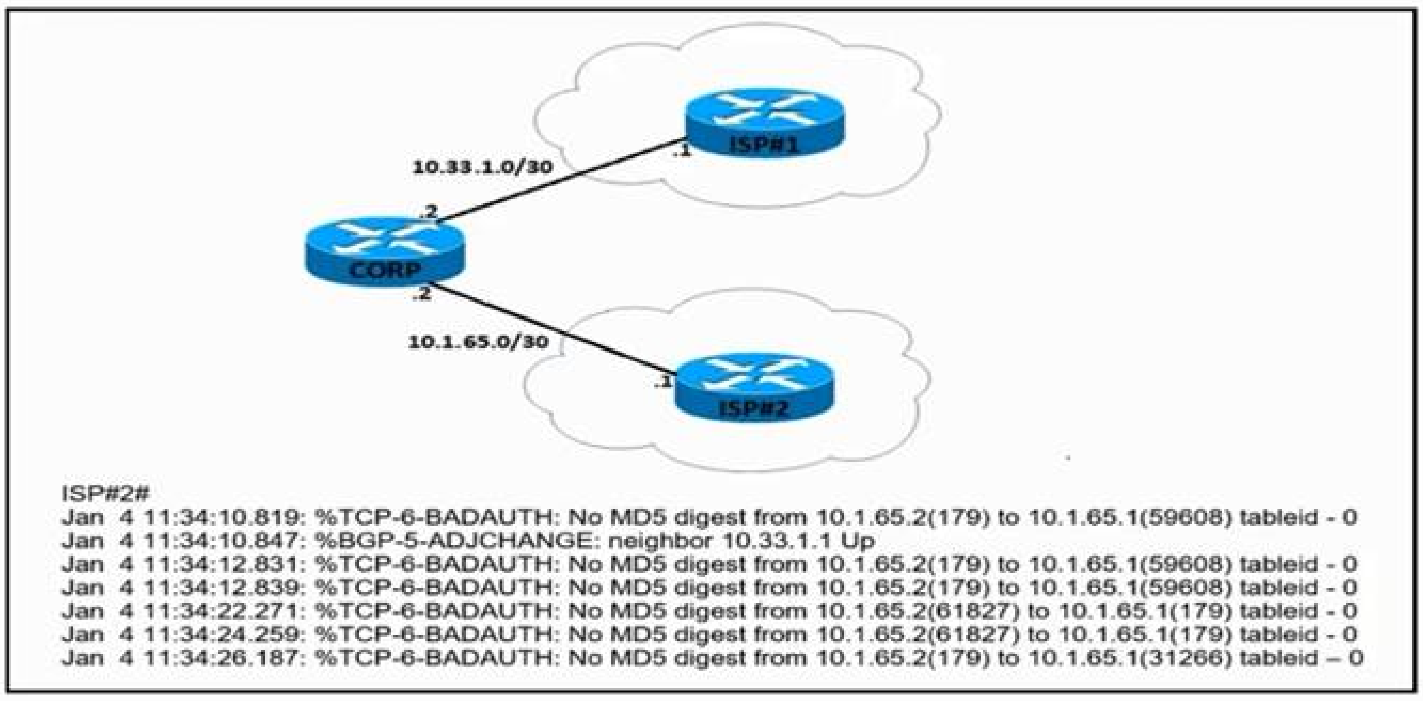
summaries can be created in specific parts of the IGP topology

NEW QUESTION 111
- (Topic 2)
How is a data modeling language used?

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

Answer: A

NEW QUESTION 116
- (Topic 2)
Refer to the exhibit.



```
ISP#2#
Jan  4 11:34:10.819: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(179) to 10.1.65.1(59608) tableid - 0
Jan  4 11:34:10.847: %BGP-5-ADJCHANGE: neighbor 10.33.1.1 Up
Jan  4 11:34:12.831: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(179) to 10.1.65.1(59608) tableid - 0
Jan  4 11:34:12.839: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(179) to 10.1.65.1(59608) tableid - 0
Jan  4 11:34:22.271: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(61827) to 10.1.65.1(179) tableid - 0
Jan  4 11:34:24.259: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(61827) to 10.1.65.1(179) tableid - 0
Jan  4 11:34:26.187: %TCP-6-BADAUTH: No MD5 digest from 10.1.65.2(179) to 10.1.65.1(31266) tableid – 0
```

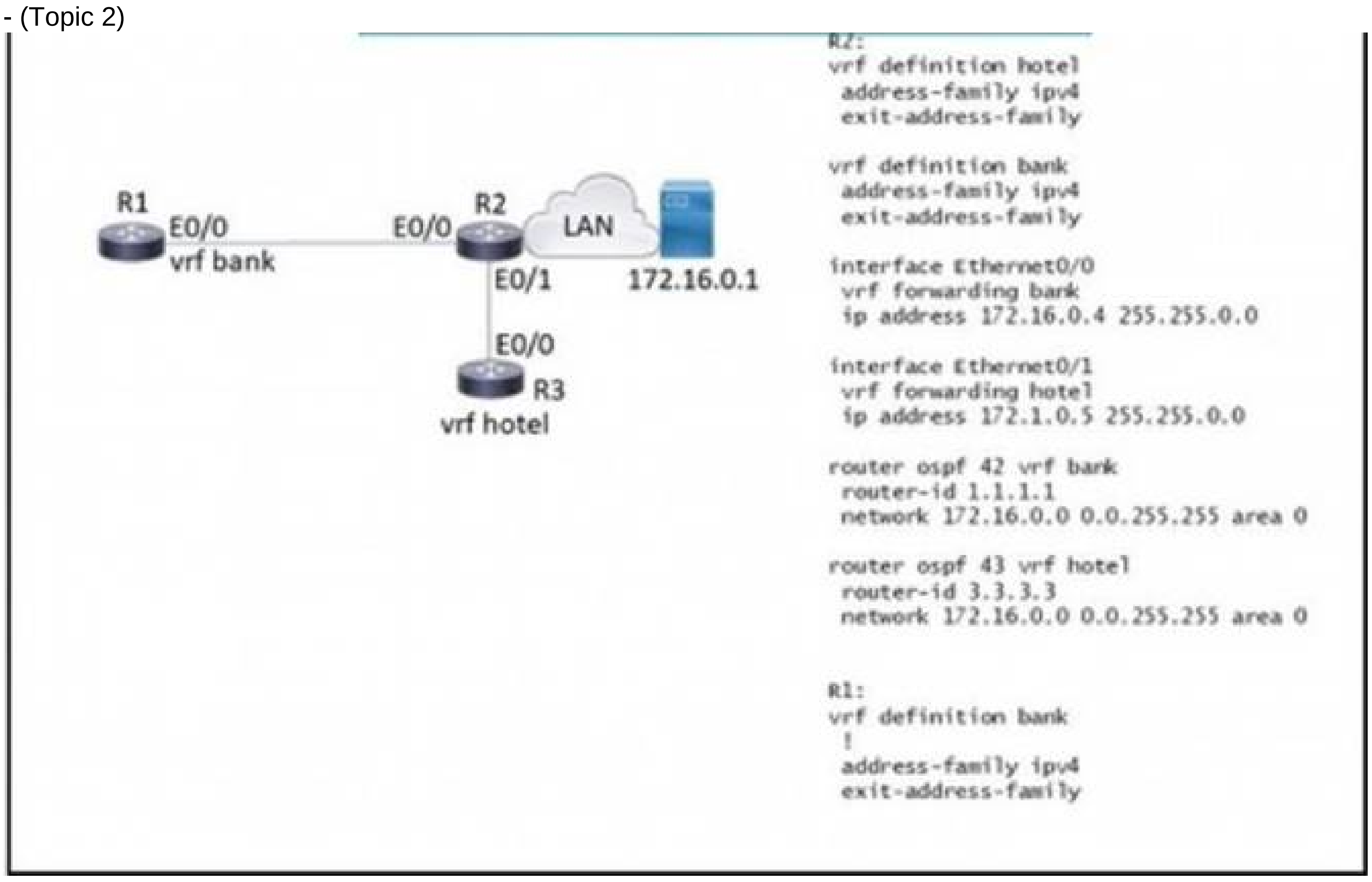
An engineer attempts to establish BGP peering between router CORP and two ISP routers. What is the root cause for the failure between CORP and ISP#2?

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

D. MD5 authorization is configured incorrectly on router ISP#2.

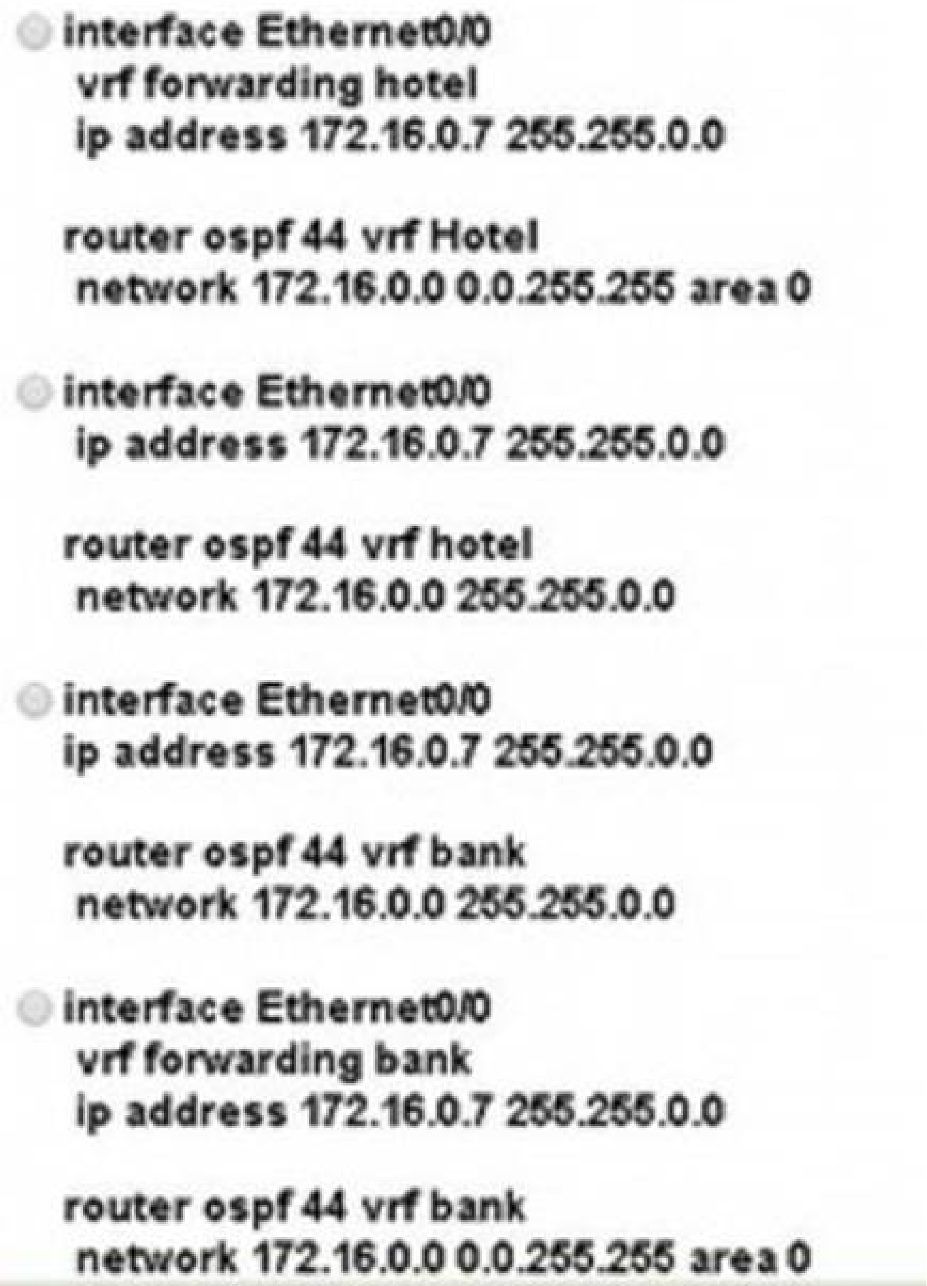
Answer: B

NEW QUESTION 121
- (Topic 2)



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

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

interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.4 255.255.0.0

interface Ethernet0/1
 vrf forwarding hotel
 ip address 172.1.0.5 255.255.0.0

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

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


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

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

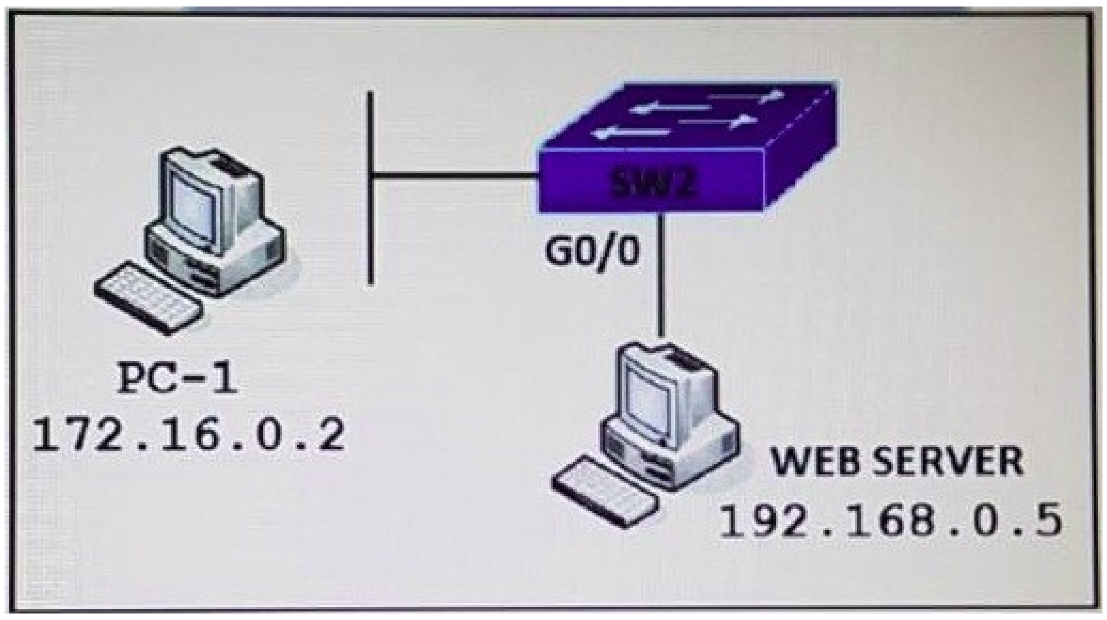


```
○ interface Ethernet0/0
   vrf forwarding hotel
   ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf Hotel
   network 172.16.0.0 0.0.255.255 area 0

○ interface Ethernet0/0
   ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf hotel
   network 172.16.0.0 255.255.0.0

○ interface Ethernet0/0
  ip address 172.16.0.7 255.255.0.0

  router ospf 44 vrf bank
   network 172.16.0.0 255.255.0.0

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

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

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

Answer: D

NEW QUESTION 124
- (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.

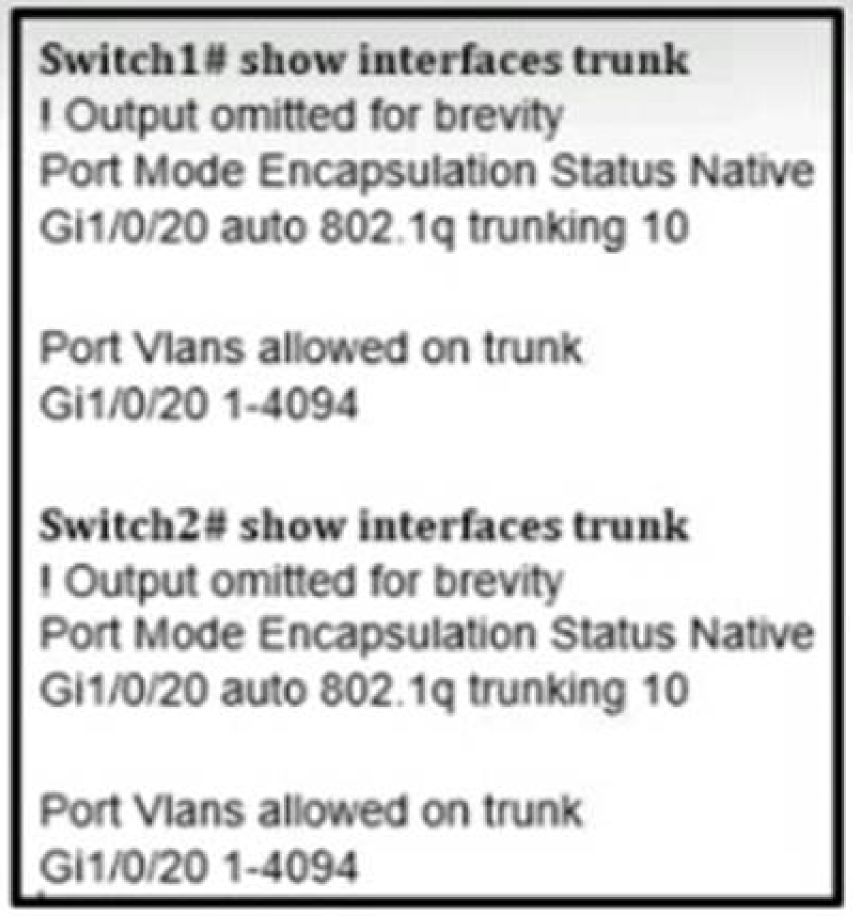
NEW QUESTION 127
- (Topic 2)
Which protocol infers that a YANG data model is being used?

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

Answer: D

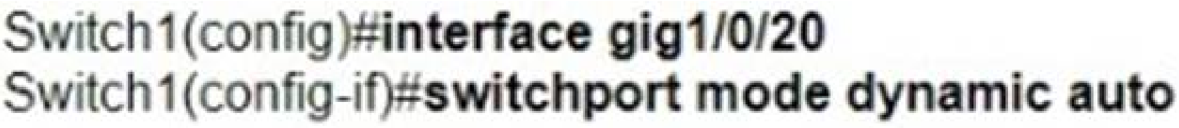
Explanation:
YANG (Yet another Next Generation) is a data modeling language for the definition
of data sent over network management protocols such as the NETCONF and RESTCONF.

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



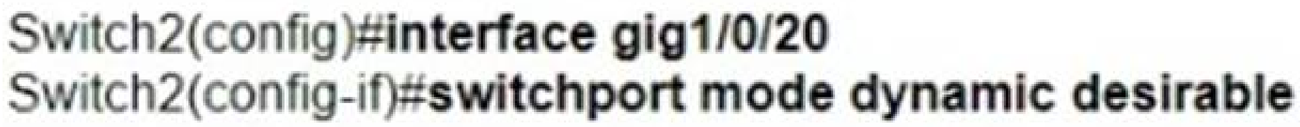
```
Switch1# show interfaces trunk
! Output omitted for brevity
Port Mode Encapsulation Status Native
Gi1/0/20 auto 802.1q trunking 10

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)



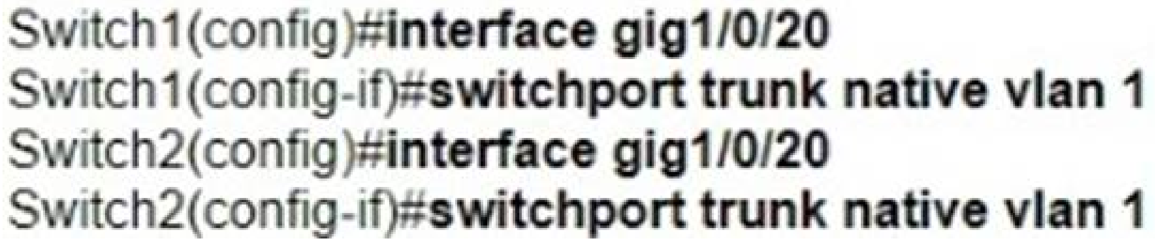
```
Switch1(config)#interface gig1/0/20
Switch1(config-if)#switchport mode dynamic auto
```

B)



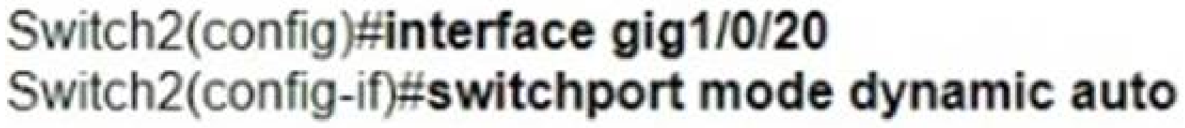
```
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic desirable
```

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)

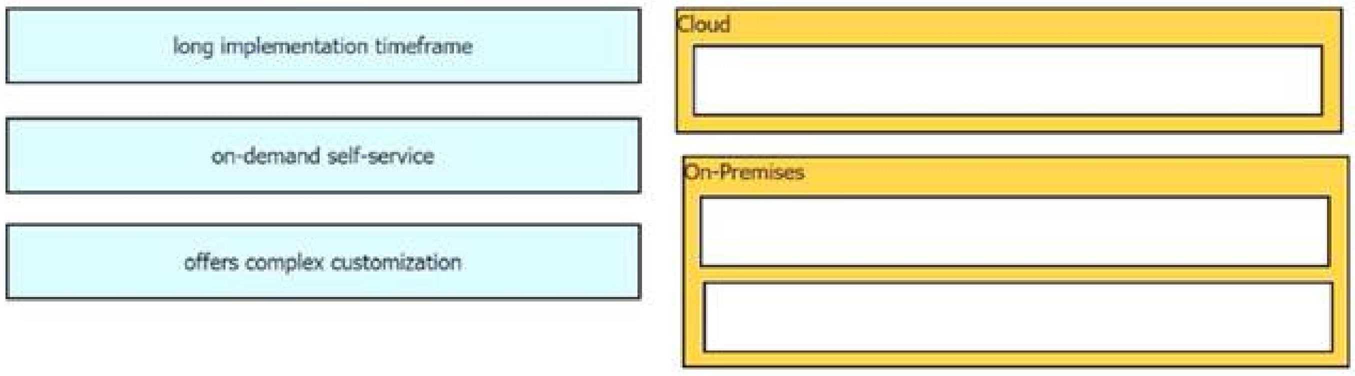


```
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic auto
```

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

Answer: B

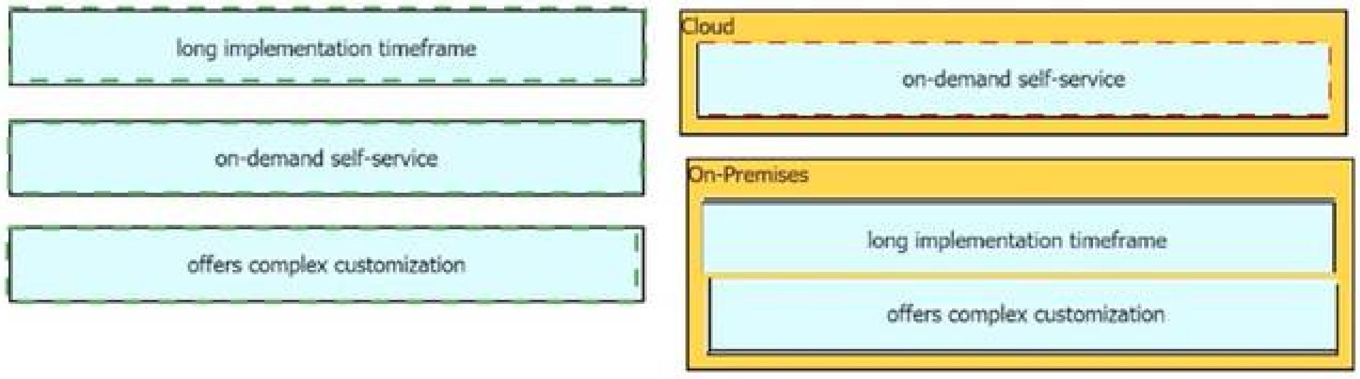
NEW QUESTION 132
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the deployment models on the right.



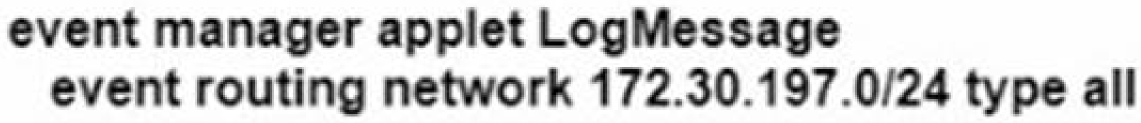
A. Mastered
B. Not Mastered

Answer: A

Explanation:


long implementation timeframe
on-demand self-service
offers complex customization
Cloud
on-demand self-service
On-Premises
long implementation timeframe
offers complex customization

NEW QUESTION 137
- (Topic 2)
An engineer must create an EEM applet that sends a syslog message in the event a change happens in the network due to trouble with an OSPF process. Which action should the engineer use?



```
event manager applet LogMessage
  event routing network 172.30.197.0/24 type all
```

A. action 1 syslog msg "OSPF ROUTING ERROR"
B. action 1 syslog send "OSPF ROUTING ERROR"
C. action 1 syslog pattern "OSPF ROUTING ERROR"
D. action 1syslog write "OSPF ROUTING ERROR"

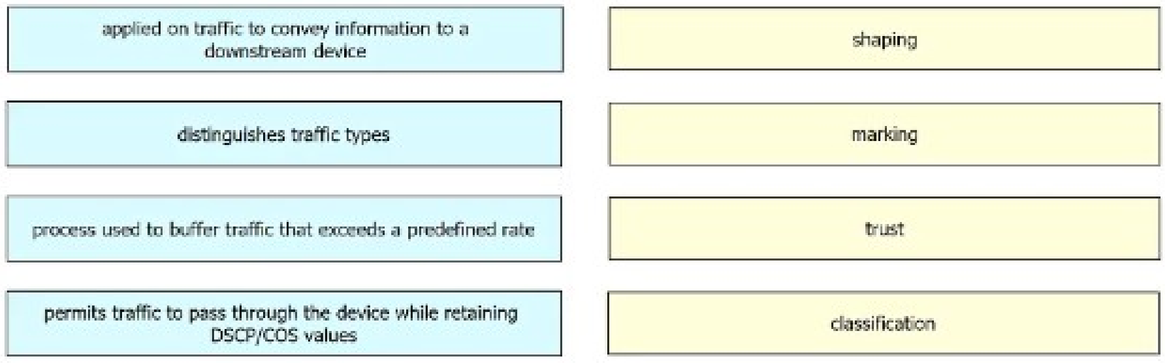
Answer: C

NEW QUESTION 139
- (Topic 2)
What is a characteristic of Cisco DNA Northbound APIs?

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

Answer: C

NEW QUESTION 140
DRAG DROP - (Topic 2)
Drag and drop the descriptions from the left onto the QoS components they describe on the right.

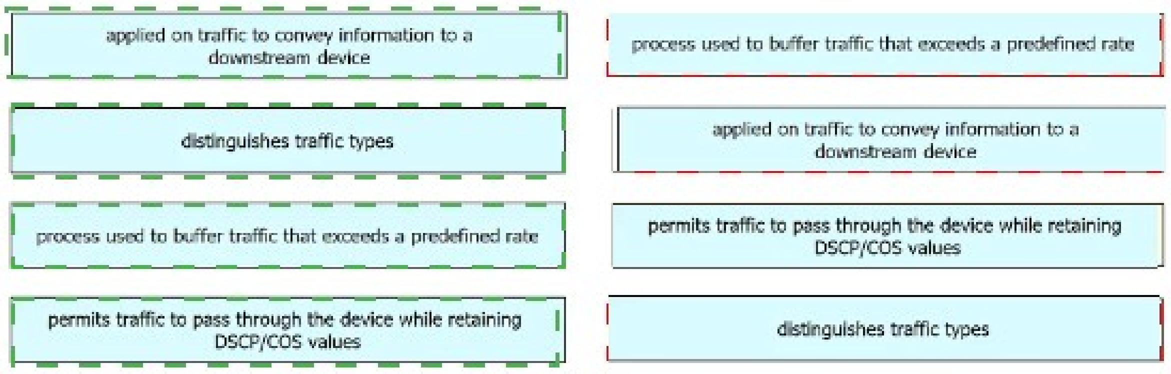


applied on traffic to convey information to a downstream device	shaping
distinguishes traffic types	marking
process used to buffer traffic that exceeds a predefined rate	trust
permits traffic to pass through the device while retaining DSCP/COS values	classification

A. Mastered
B. Not Mastered

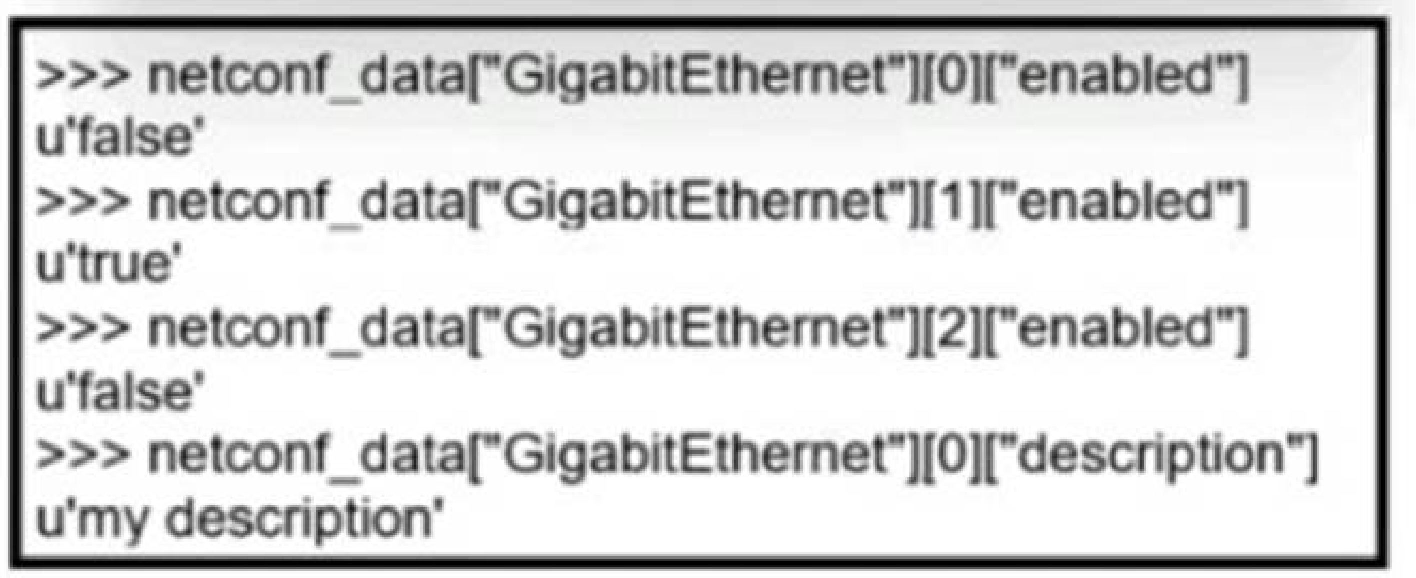
Answer: A

Explanation:



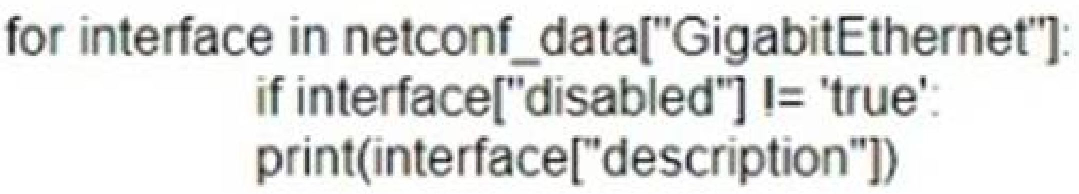
applied on traffic to convey information to a downstream device	process used to buffer traffic that exceeds a predefined rate
distinguishes traffic types	applied on traffic to convey information to a downstream device
process used to buffer traffic that exceeds a predefined rate	permits traffic to pass through the device while retaining DSCP/COS values
permits traffic to pass through the device while retaining DSCP/COS values	distinguishes traffic types

NEW QUESTION 141
- (Topic 2)
Refer to the exhibit.



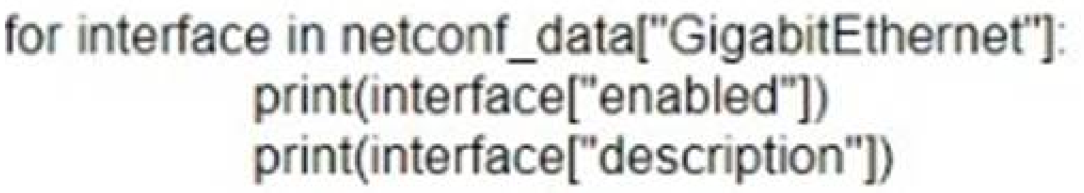
```
>>> netconf_data["GigabitEthernet"][0]["enabled"]
u'false'
>>> netconf_data["GigabitEthernet"][1]["enabled"]
u'true'
>>> netconf_data["GigabitEthernet"][2]["enabled"]
u'false'
>>> netconf_data["GigabitEthernet"][0]["description"]
u'my description'
```

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



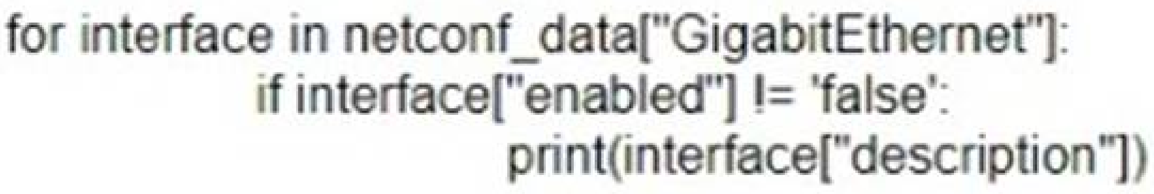
```
for interface in netconf_data["GigabitEthernet"]:
        if interface["disabled"] != 'true':
        print(interface["description"])
```

B)



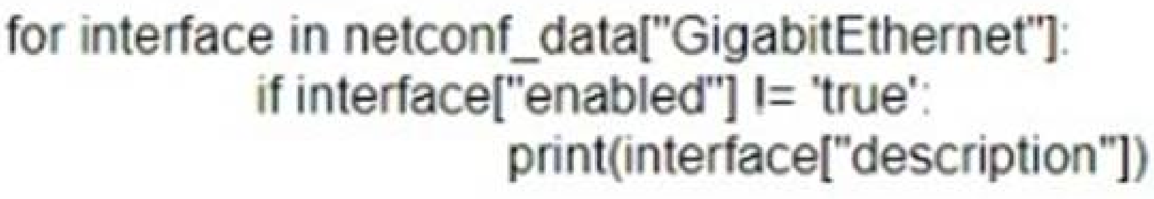
```
for interface in netconf_data["GigabitEthernet"]:
        print(interface["enabled"])
        print(interface["description"])
```

C)



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

D)



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

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

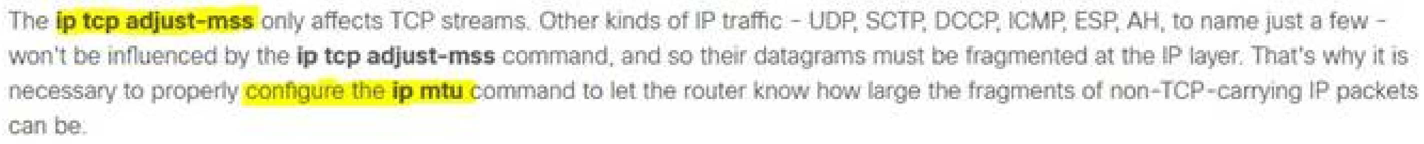
Answer: D

NEW QUESTION 142
- (Topic 2)
Which two GRE features are configured to prevent fragmentation? (Choose two.)

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

Answer: AE

Explanation:



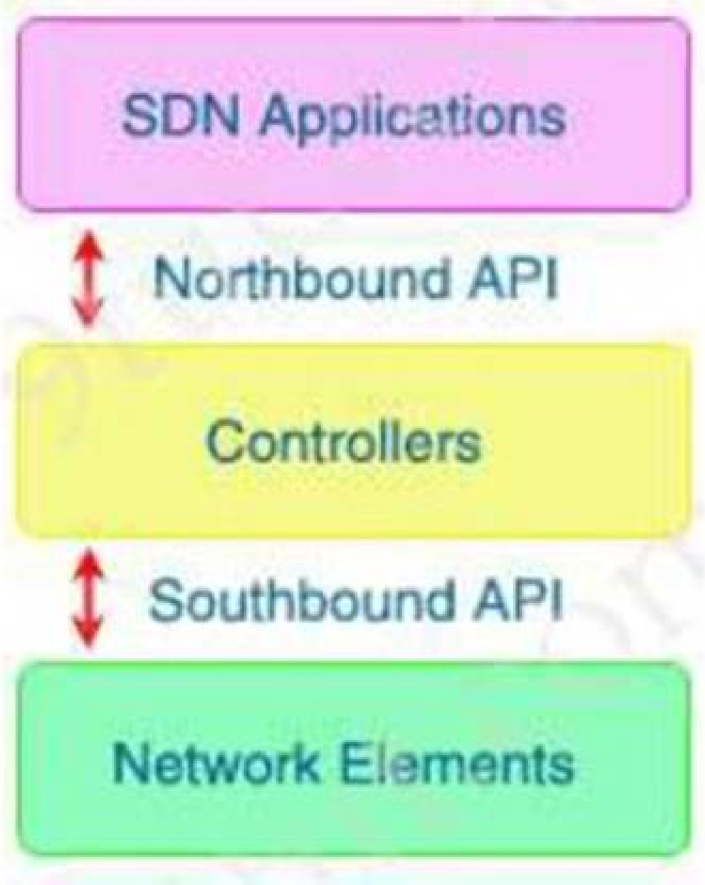
The **ip tcp adjust-mss** only affects TCP streams. Other kinds of IP traffic - UDP, SCTP, DCCP, ICMP, ESP, AH, to name just a few - won't be influenced by the **ip tcp adjust-mss** command, and so their datagrams must be fragmented at the IP layer. That's why it is necessary to properly configure the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

NEW QUESTION 146
- (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

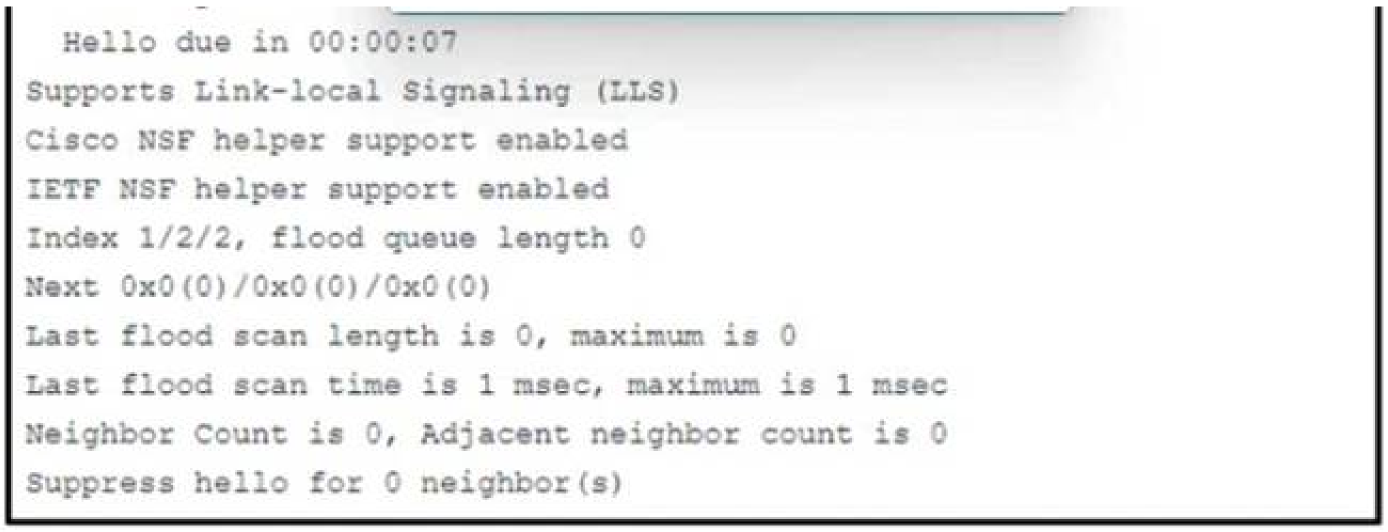
Explanation:
The Southbound API is used to communicate with network devices.



NEW QUESTION 150

- (Topic 2)

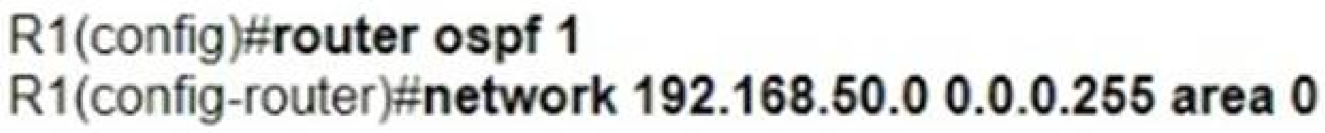
Refer to the exhibit.



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

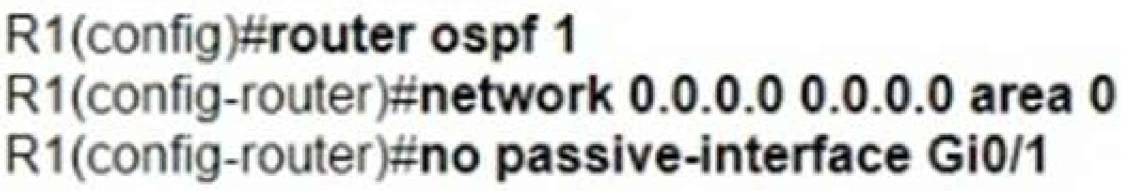
An engineer configures OSPF and wants to verify the configuration Which configuration is applied to this device?

A)



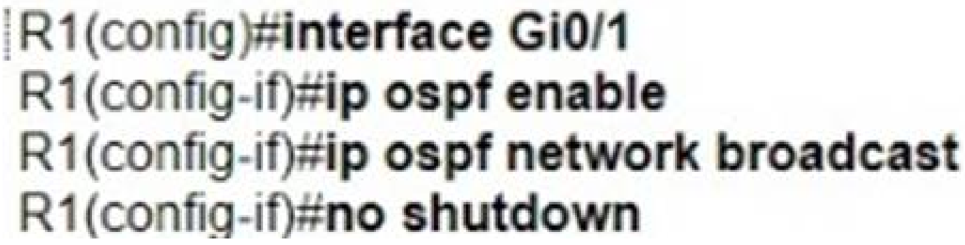
```
R1(config)#router ospf 1
R1(config-router)#network 192.168.50.0 0.0.0.255 area 0
```

B)



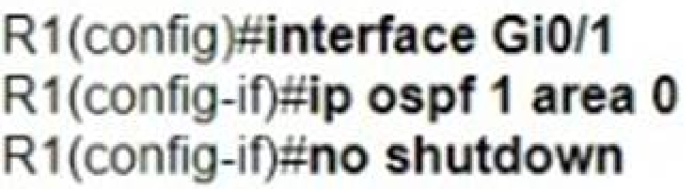
```
R1(config)#router ospf 1
R1(config-router)#network 0.0.0.0 0.0.0.0 area 0
R1(config-router)#no passive-interface Gi0/1
```

C)



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

D)



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

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

Answer: C

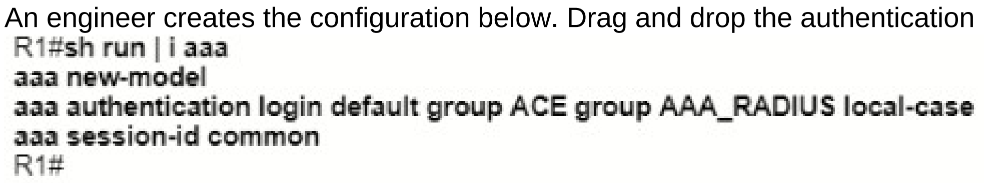
NEW QUESTION 154
- (Topic 2)
Which HHTP status code is the correct response for a request with an incorrect password applied to a REST API session?

A. HTTP Status Code 200
B. HTTP Status Code 302
C. HTTP Status Code 401
D. HTTP Status Code: 504

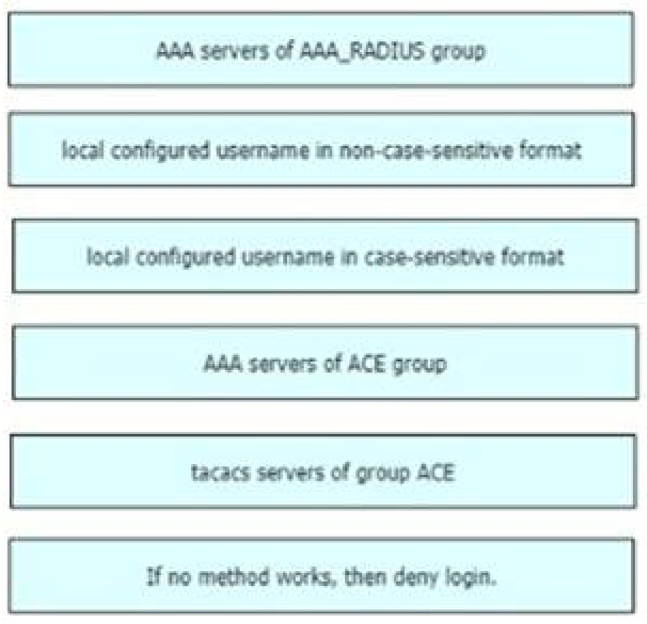
Answer: C

Explanation:
A 401 error response indicates that the client tried to operate on a protected resource without providing the proper authorization. It may have provided the wrong credentials or none at all.
Note: answer 'HTTP Status Code 200' 4xx code indicates a “client error” while a 5xx code indicates a “server error”.
Reference: https://restfulapi.net/http-status-codes/

NEW QUESTION 159
DRAG DROP - (Topic 2)
An engineer creates the configuration below. Drag and drop the authentication methods from the left into the order of priority on the right. Not all options are used.



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



AAA servers of AAA_RADIUS group

local configured username in non-case-sensitive format

local configured username in case-sensitive format

AAA servers of ACE group

tacacs servers of group ACE

If no method works, then deny login.

A. Mastered
B. Not Mastered

Answer: A

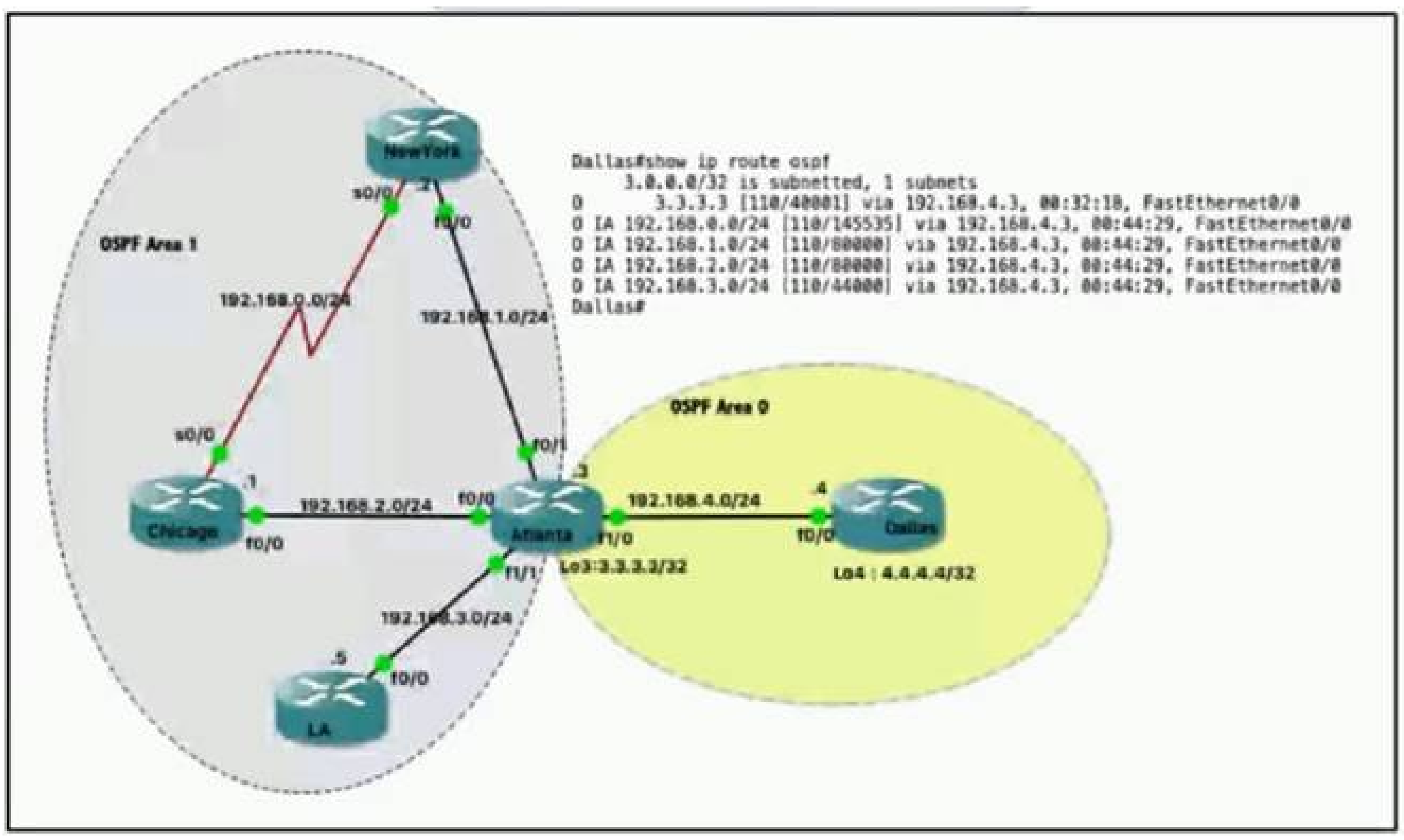
Explanation:
priority 1: AAA servers of ACE group
priority 2: AAA servers of AAA_RADIUS group
priority 3: local configured username in case-sensitive format priority 4: If no method works, then deny login

NEW QUESTION 162
- (Topic 2)
A network monitoring system uses SNMP polling to record the statistics of router interfaces The SNMP queries work as expected until an engineer installs a new interface and reloads the router After this action, all SNMP queries for the router fail What is the cause of this issue?

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

Answer: B

NEW QUESTION 165
- (Topic 2)
Refer to the exhibit.



```
Dallas#show ip route ospf
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/40001] via 192.168.4.3, 00:32:18, FastEthernet0/0
O IA 192.168.0.0/24 [110/145535] via 192.168.4.3, 00:44:29, FastEthernet0/0
O IA 192.168.1.0/24 [110/80000] via 192.168.4.3, 00:44:29, FastEthernet0/0
O IA 192.168.2.0/24 [110/80000] via 192.168.4.3, 00:44:29, FastEthernet0/0
O IA 192.168.3.0/24 [110/44000] via 192.168.4.3, 00:44:29, FastEthernet0/0
Dallas#
```

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

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

Answer: C

NEW QUESTION 170
- (Topic 2)
What NTP Stratum level is a server that is connected directly to an authoritative time source?

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

Answer: B

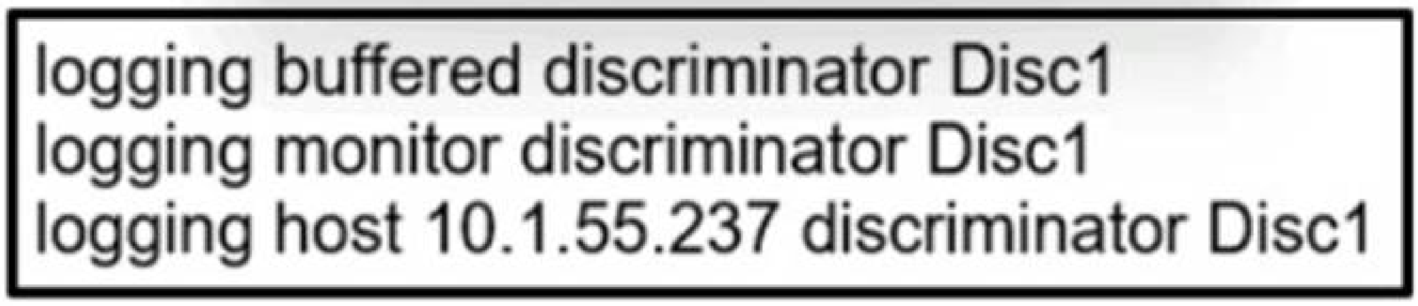
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/bsm/16-6-1/b-bsm-xe-16-6-1-asr920/bsm-timecalendar- set.html

NEW QUESTION 173
- (Topic 2)
Which two items are found in YANG data models? (Choose two.)

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

Answer: CE

NEW QUESTION 175
- (Topic 2)
Refer to the exhibit.



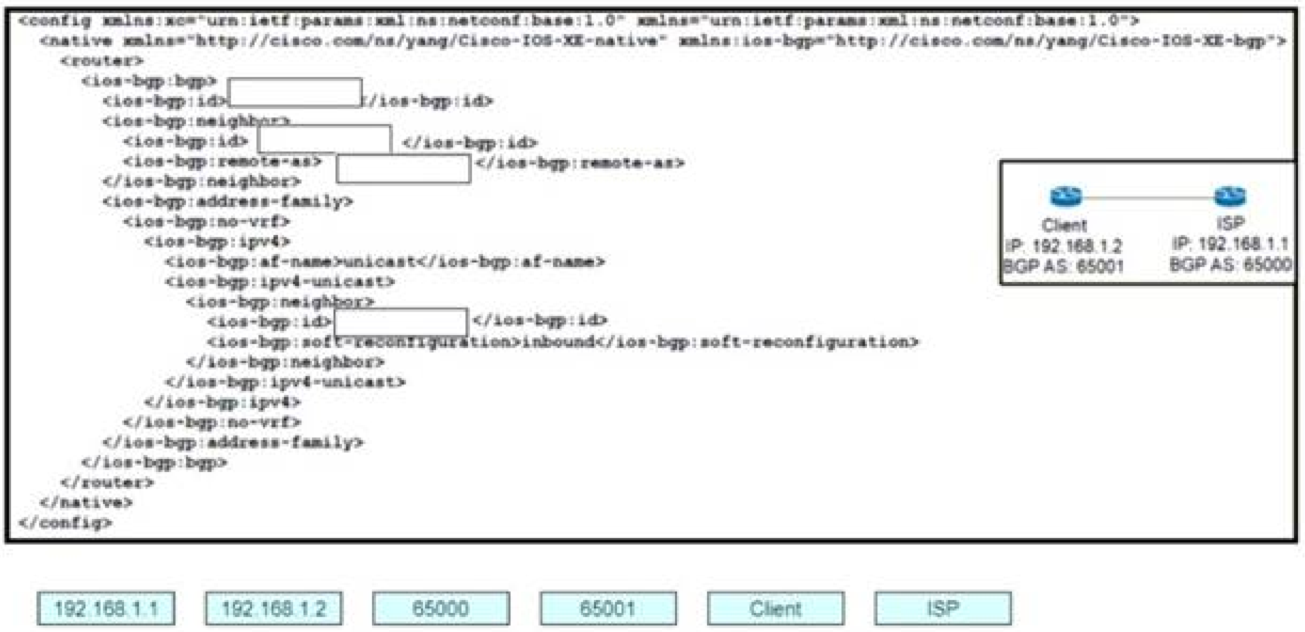
```
logging buffered discriminator Disc1
logging monitor discriminator Disc1
logging host 10.1.55.237 discriminator Disc1
```

A network engineer is enabling logging to a local buffer, to the terminal and to a syslog server for all debugging level logs filtered by facility code 7. Which command is needed to complete this configuration snippet?

A. logging buffered debugging
B. logging discriminator Disc1 severity includes 7
C. logging buffered discriminator Disc1 debugging
D. logging discriminator Disc1 severity includes 7 facility includes fac7

Answer: B

NEW QUESTION 176
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.

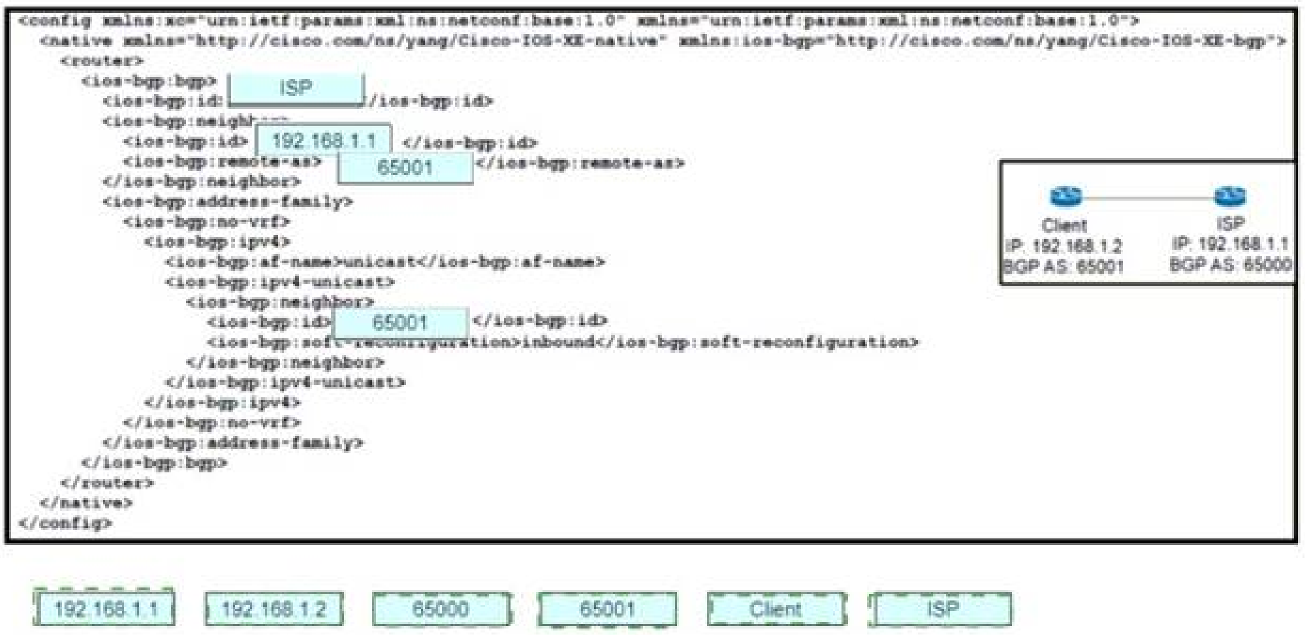


```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>
        <ios-bgp:id>            </ios-bgp:id>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

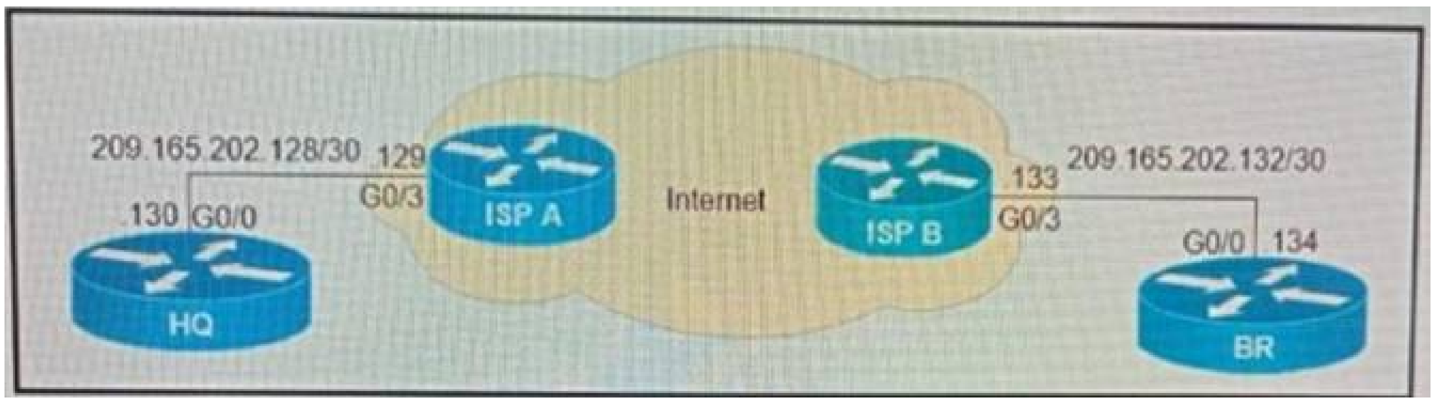
Answer: A

Explanation:

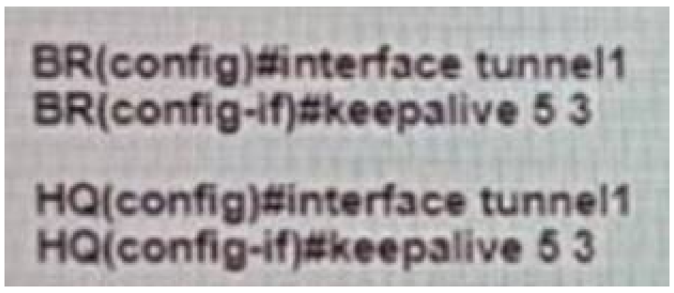


```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>   ISP
        <ios-bgp:id:             /ios-bgp:id>
        <ios-bgp:neigh
          <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:sof          ation>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 181
- (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 185
- (Topic 2)
What is the process for moving a virtual machine from one host machine to another with no downtime?

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

Answer: C

NEW QUESTION 188
- (Topic 2)
By default, which virtual MAC address does HSRP group 16 use?

A. c0:41:43:64:13:10
B. 00:00:0c 07:ac:10
C. 00:05:5c:07:0c:16
D. 05:00:0c:07:ac:16

Answer: B

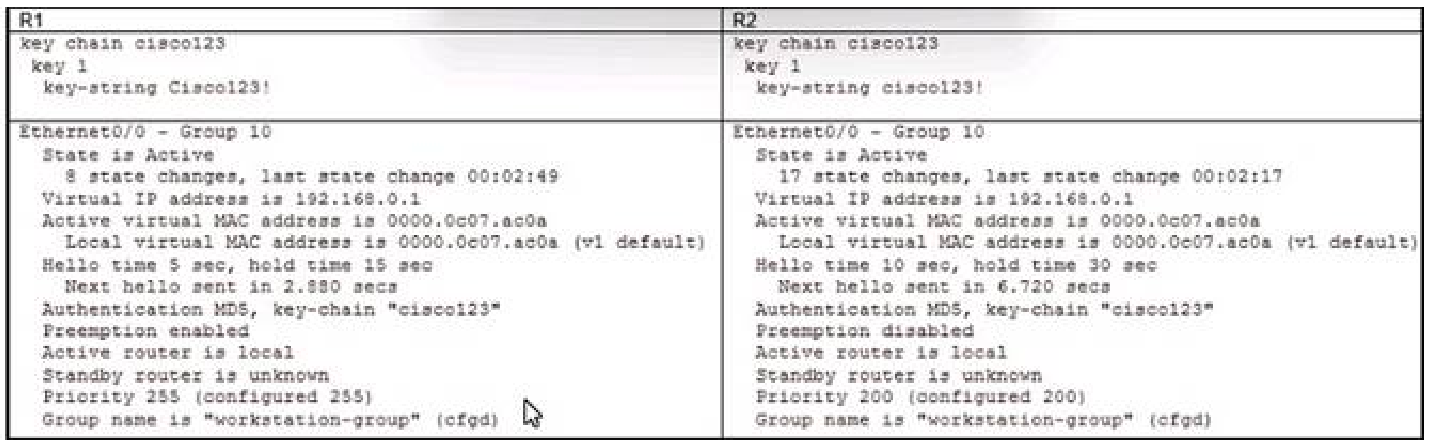
Explanation:
The last two-digit hex value in the MAC address presents the HSRP group number. In this case 16 in decimal is 10 in hexadecimal

NEW QUESTION 191
- (Topic 2)
Which technology uses network traffic telemetry, contextual information, and file reputation to provide insight into cyber threats?

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

Answer: C

NEW QUESTION 193
- (Topic 2)
Refer to the Exhibit.



R1

```
key chain cisco123
 key 1
  key-string Cisco123!
```

```
Ethernet0/0 - Group 10
  State is Active
    8 state changes, last state change 00:02:49
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 5 sec, hold time 15 sec
    Next hello sent in 2.880 secs
  Authentication MD5, key-chain "cisco123"
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 255 (configured 255)
  Group name is "workstation-group" (cfgd)
```

R2

```
key chain cisco123
 key 1
  key-string cisco123!
```

```
Ethernet0/0 - Group 10
  State is Active
    17 state changes, last state change 00:02:17
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 10 sec, hold time 30 sec
    Next hello sent in 6.720 secs
  Authentication MD5, key-chain "cisco123"
  Preemption disabled
  Active router is local
  Standby router is unknown
  Priority 200 (configured 200)
  Group name is "workstation-group" (cfgd)
```

An engineer is installing a new pair of routers in a redundant configuration. When checking on the standby status of each router the engineer notices that the routers are not
functioning as expected. Which action will resolve the configuration error?

A. configure matching hold and delay timers
B. configure matching key-strings
C. configure matching priority values
D. configure unique virtual IP addresses

Answer: B

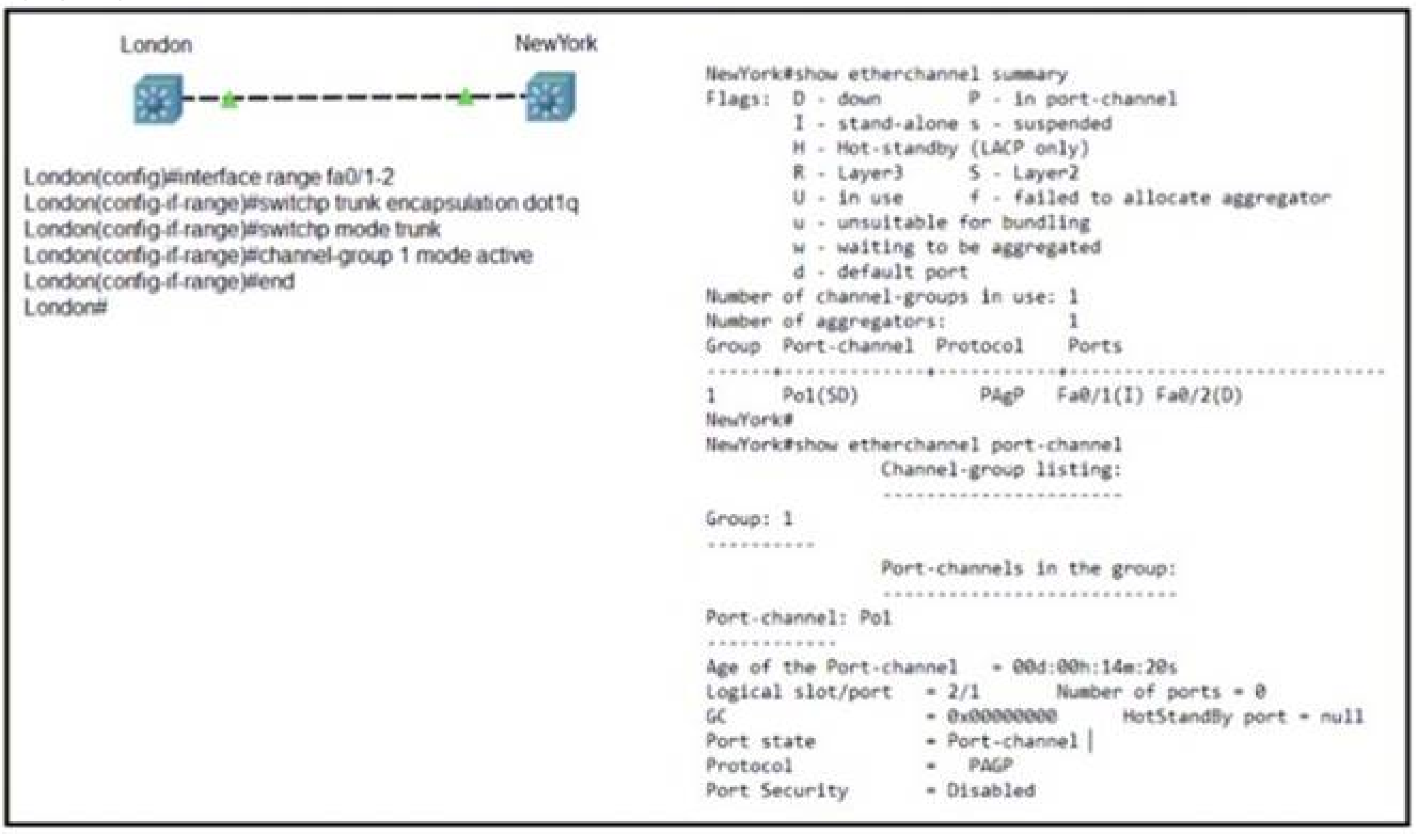
Explanation:
From the output exhibit, we notice that the key-string of R1 is Cisco123! (letter C is in capital) while that of R2 is cisco123!. This causes a mismatch in the authentication so we have to fix their key-strings.
key-string [encryption-type] text-string: Configures the text string for the key. The text- string argument is alphanumeric, case-sensitive, and supports special characters. Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_chapter_01111.pdf

NEW QUESTION 195
- (Topic 1)
A customer has several small branches and wants to deploy a WI-FI solution with local management using CAPWAP. Which deployment model meets this requirement?

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

Answer: B

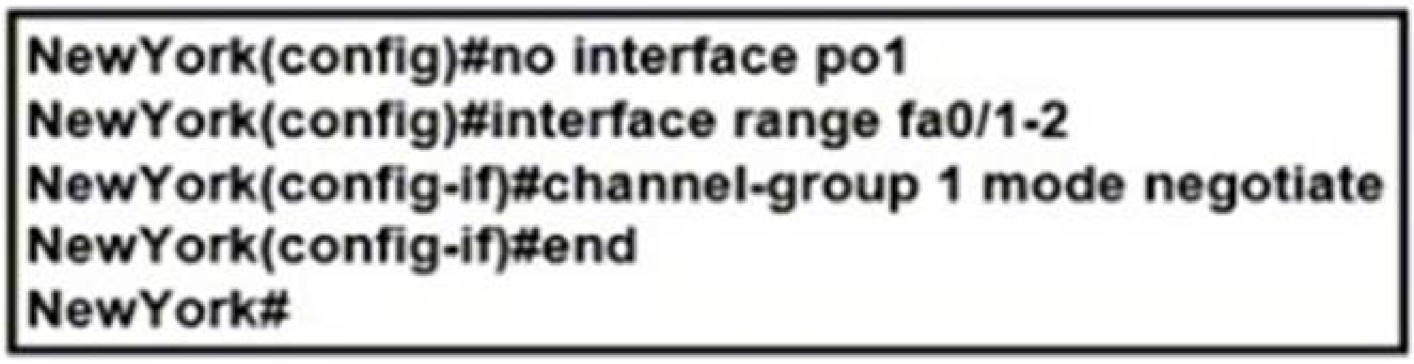
NEW QUESTION 197
- (Topic 1)



```
London(config)#interface range fa0/1-2
London(config-if-range)#switchp trunk encapsulation dot1q
London(config-if-range)#switchp mode trunk
London(config-if-range)#channel-group 1 mode active
London(config-if-range)#end
London#
```

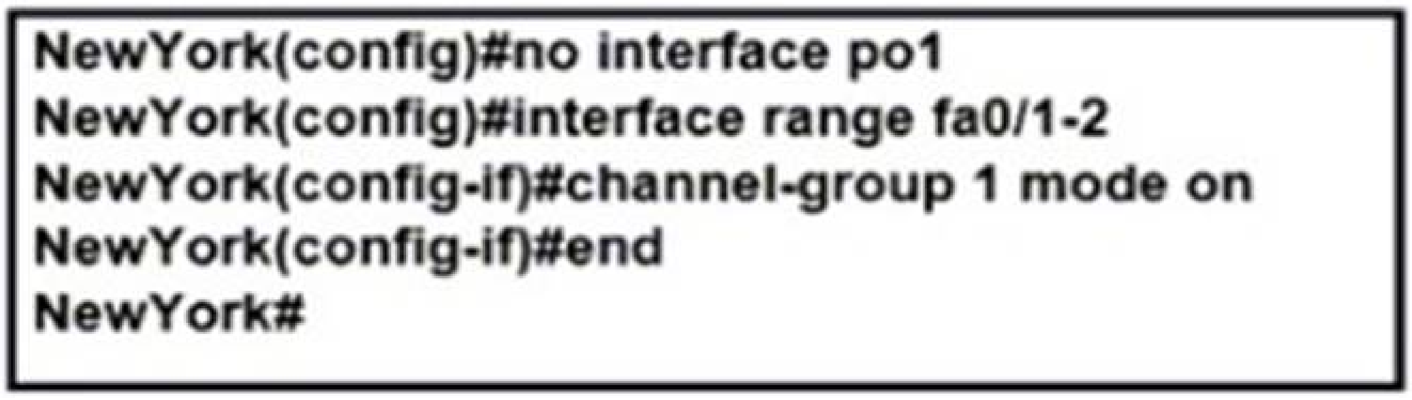
```
NewYork#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SD)           PAgP   Fa0/1(I) Fa0/2(D)
NewYork#
NewYork#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1
------------

Age of the Port-channel   = 00d:00h:14m:20s
Logical slot/port   = 2/1        Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel |
Protocol            =   PAGP
Port Security       = Disabled
```

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



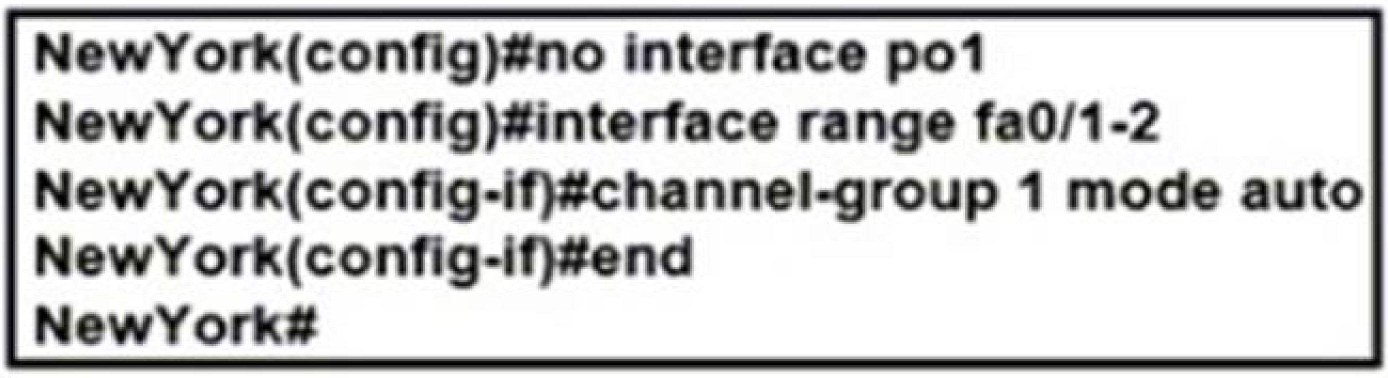
```
NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode negotiate
NewYork(config-if)#end
NewYork#
```

B)



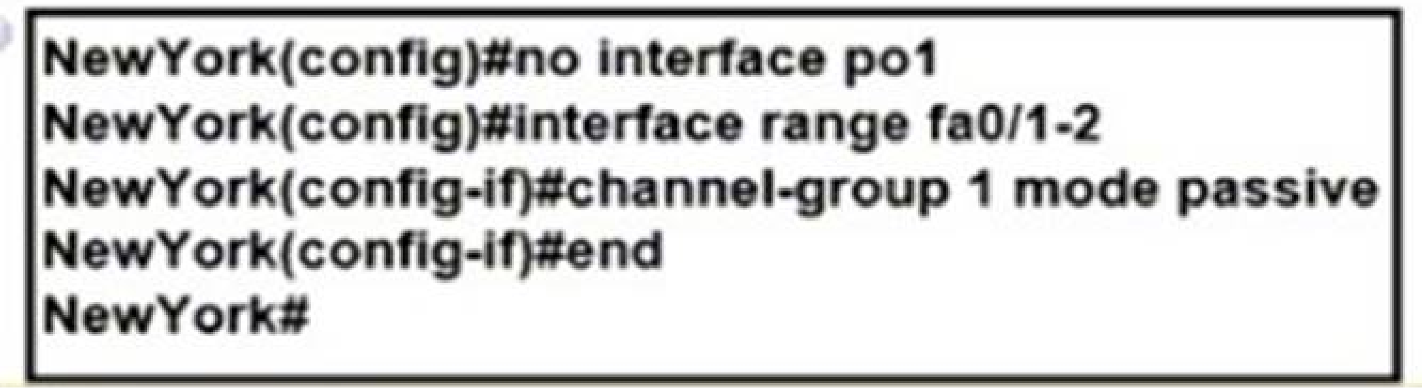
```
NewYork(config)#no interface po1
NewYork(config)#interface range fa0/1-2
NewYork(config-if)#channel-group 1 mode on
NewYork(config-if)#end
NewYork#
```

C)



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

D)



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

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

Answer: D

NEW QUESTION 200
- (Topic 1)
How is MSDP used to interconnect multiple PIM-SM domains?

A. MSDP depends on BGP or multiprotocol BGP for mterdomam operation
B. MSDP SA request messages are used to request a list of active sources for a specific group
C. SDP allows a rendezvous point to dynamically discover active sources outside of its domain
D. MSDP messages are used to advertise active sources in a domain

Answer: A

NEW QUESTION 201
- (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 202
- (Topic 1)
Which two operational models enable an AP to scan one or more wireless channels for rouge access points and at the same time provide wireless services to clients? (Choose two.)

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

Answer: DE

NEW QUESTION 206
- (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 210
- (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.

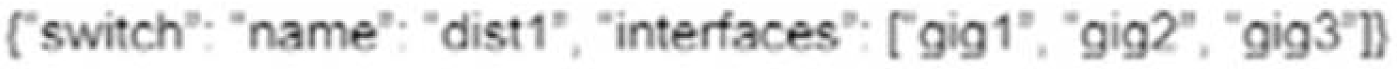
NEW QUESTION 214
- (Topic 1)
What is a benefit of data modeling languages like YANG?

A. They enable programmers to change or write their own application within the device operating system.
B. They create more secure and efficient SNMP OIDs.
C. They make the CLI simpler and more efficient.
D. They provide a standardized data structure, which results in configuration scalability and consistency.

Answer: D

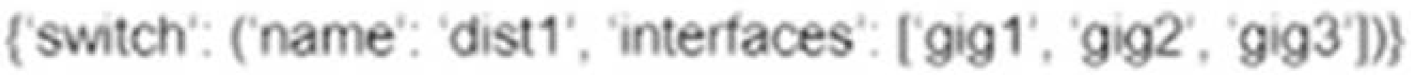
Explanation:
Yet Another Next Generation (YANG) is a language which is only used to describe data models (structure). It is not XML or JSON.

NEW QUESTION 219
- (Topic 1)
Which JSON syntax is valid?
A)



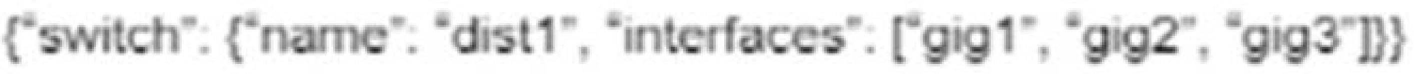
```
{"switch": "name": "dist1", "interfaces": ["gig1", "gig2", "gig3"]}
```

B)



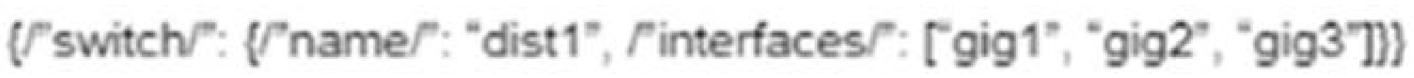
```
{'switch': ('name': 'dist1', 'interfaces': ['gig1', 'gig2', 'gig3'])}
```

C)



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

D)



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

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

Answer: C

Explanation:
This JSON can be written as follows:
{
'switch': { 'name': 'dist1',
'interfaces': ['gig1', 'gig2', 'gig3']
}
}

NEW QUESTION 220
- (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

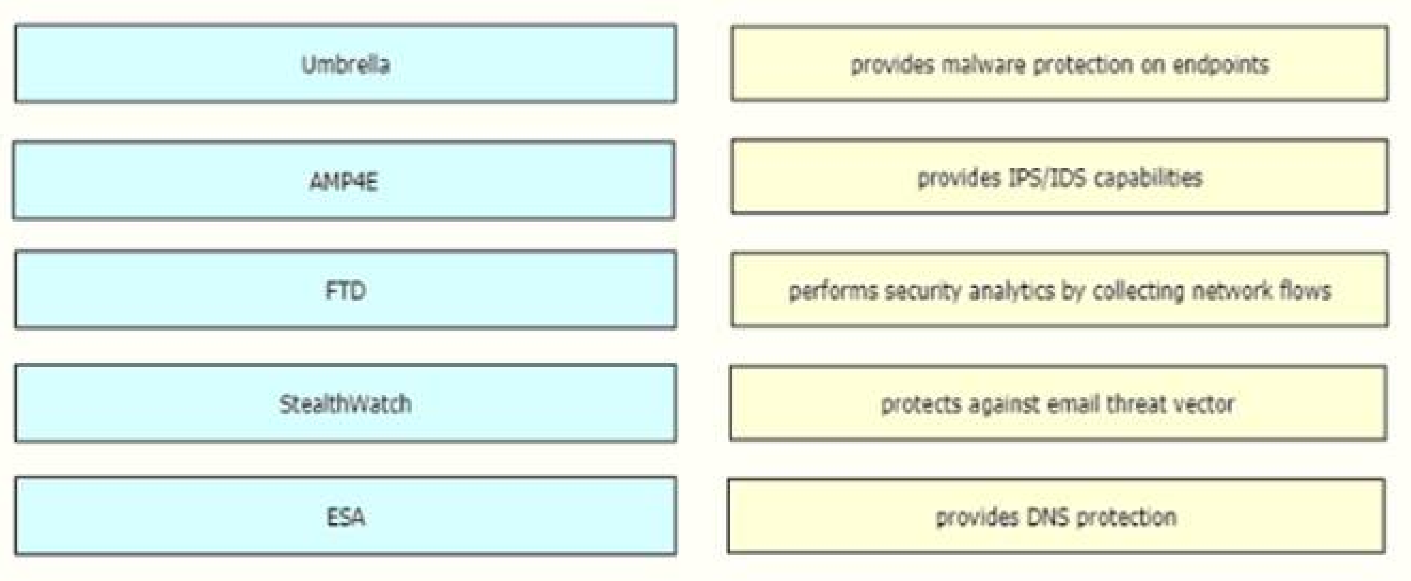
Answer: B

NEW QUESTION 222
- (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 224
DRAG DROP - (Topic 1)
Drag and drop the threat defense solutions from the left onto their descriptions on the right.

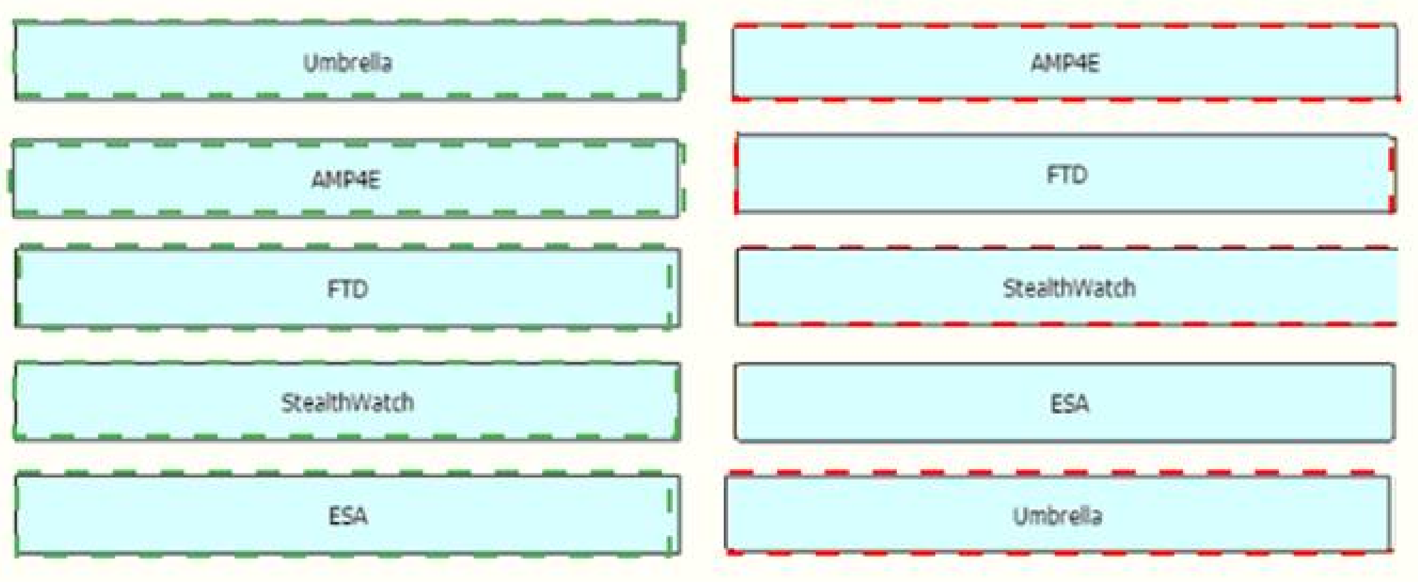


Umbrella	provides malware protection on endpoints
AMP4E	provides IPS/IDS capabilities
FTD	performs security analytics by collecting network flows
StealthWatch	protects against email threat vector
ESA	provides DNS protection

A. Mastered
B. Not Mastered

Answer: A

Explanation:



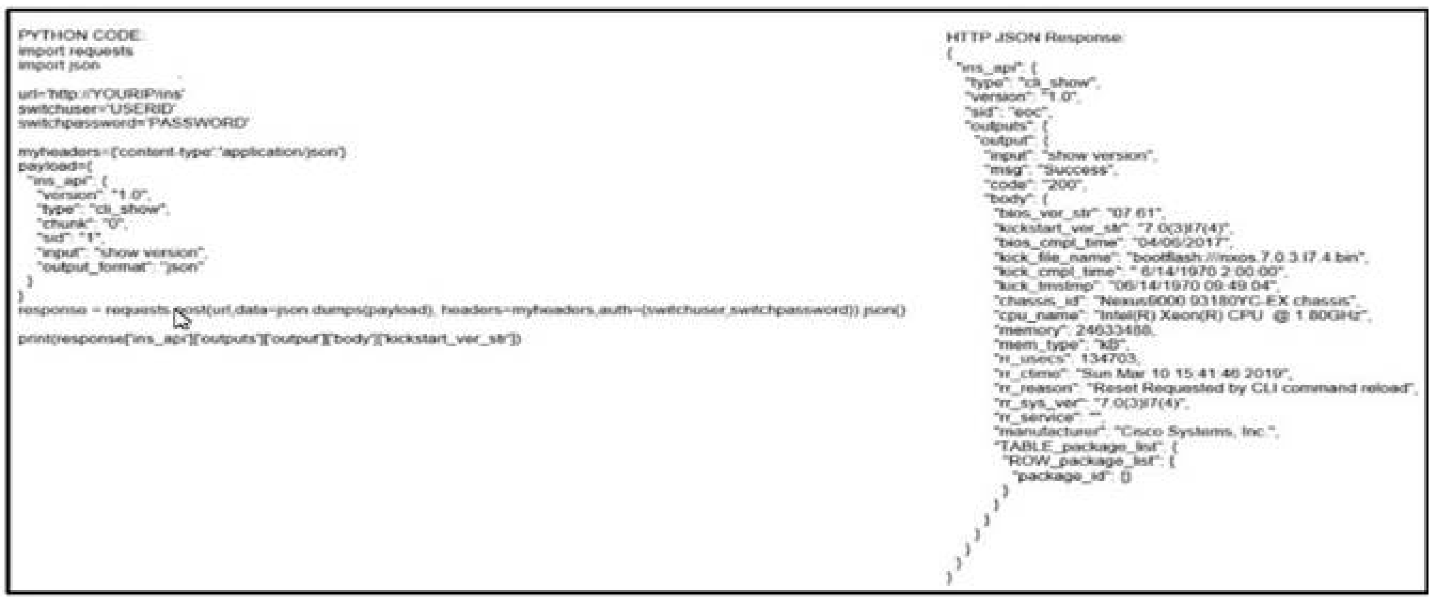
Umbrella	AMP4E
AMP4E	FTD
FTD	StealthWatch
StealthWatch	ESA
ESA	Umbrella

NEW QUESTION 227
- (Topic 1)
An engineer configures HSRP group 37. The configuration does not modify the default virtual MAC address. Which virtual MAC address does the group use?

A. C0:00:00:25:00:00
B. 00:00:0c:07:ac:37
C. C0:39:83:25:258:5
D. 00:00:0c:07:ac:25

Answer: D

NEW QUESTION 232
- (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 236
- (Topic 1)
When configuration WPA2 Enterprise on a WLAN, which additional security component configuration is required?

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

Answer: C

NEW QUESTION 241
- (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

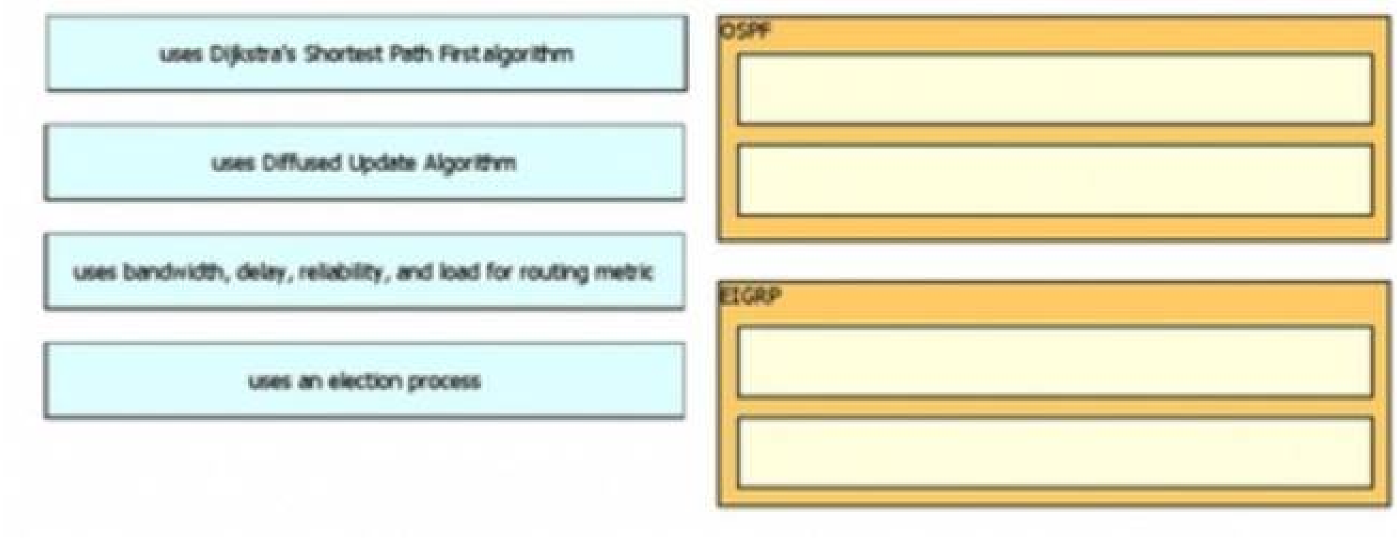
NEW QUESTION 242
- (Topic 1)
Which algorithms are used to secure REST API from brute attacks and minimize the impact?

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 245
DRAG DROP - (Topic 1)
Drag and drop the characteristics from the left onto the protocols they apply to on the right?



uses Dijkstra's Shortest Path First algorithm

uses Diffused Update Algorithm

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

uses an election process

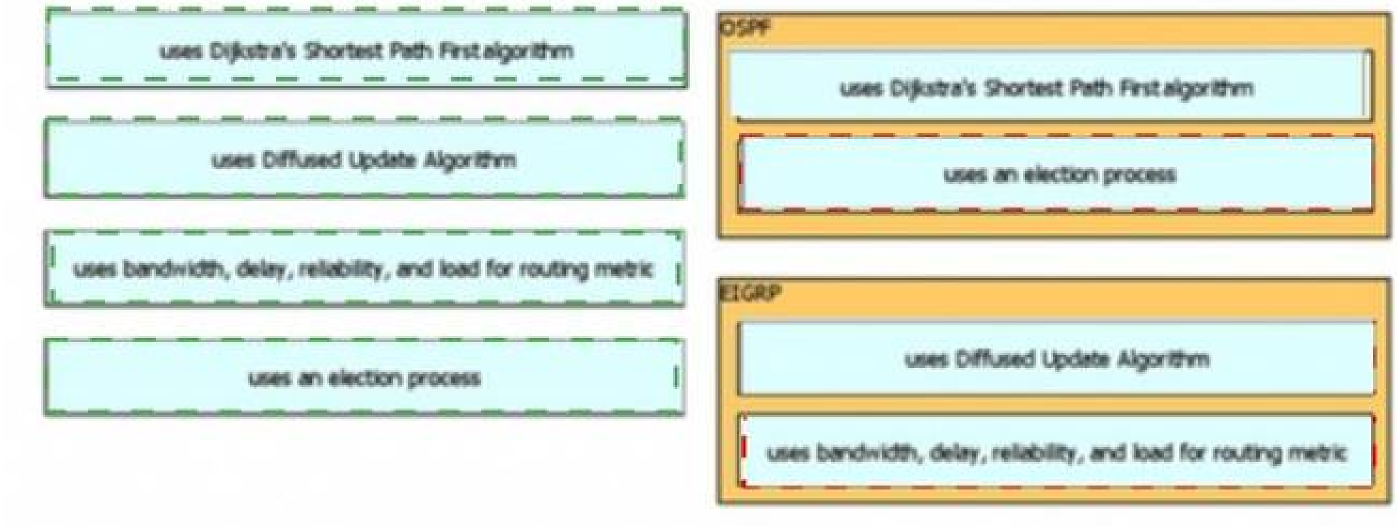
OSPF

EIGRP

A. Mastered
B. Not Mastered

Answer: A

Explanation:



uses Dijkstra's Shortest Path First algorithm

uses Diffused Update Algorithm

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

uses an election process

OSPF

uses Dijkstra's Shortest Path First algorithm

uses an election process

EIGRP

uses Diffused Update Algorithm

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

NEW QUESTION 248
- (Topic 1)
Which protocol does REST API rely on to secure the communication channel?

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

Answer: B

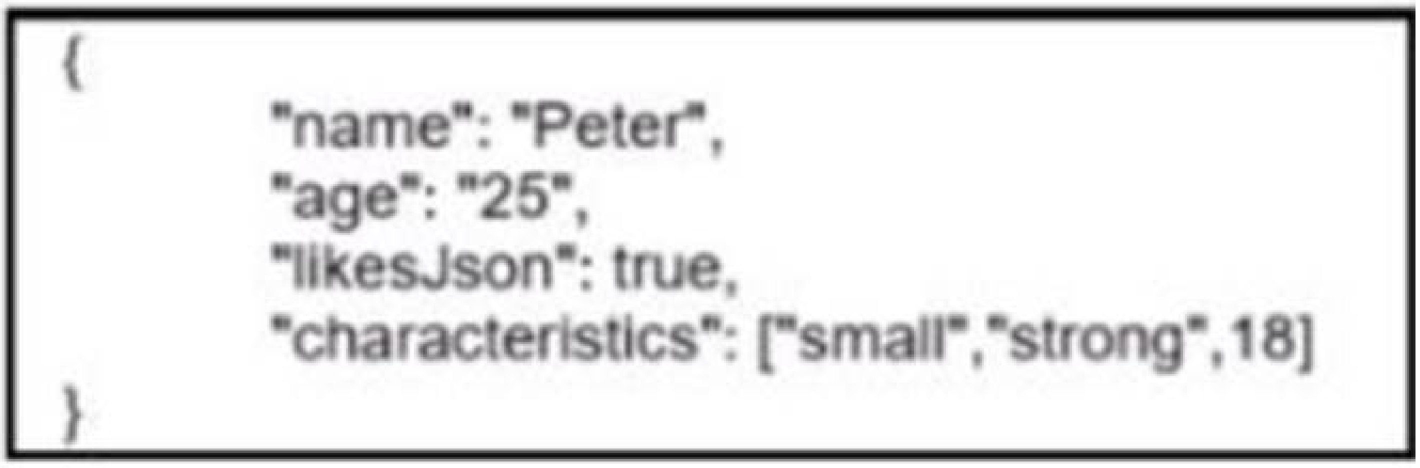
Explanation:
The REST API accepts and returns HTTP (not enabled by default) or HTTPS messages that contain JavaScript Object Notation (JSON) or Extensible Markup Language (XML) documents. You
can use any programming language to generate the messages and the JSON or XML documents that
contain the API 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 250
- (Topic 1)
When is an external antenna used inside a building?

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

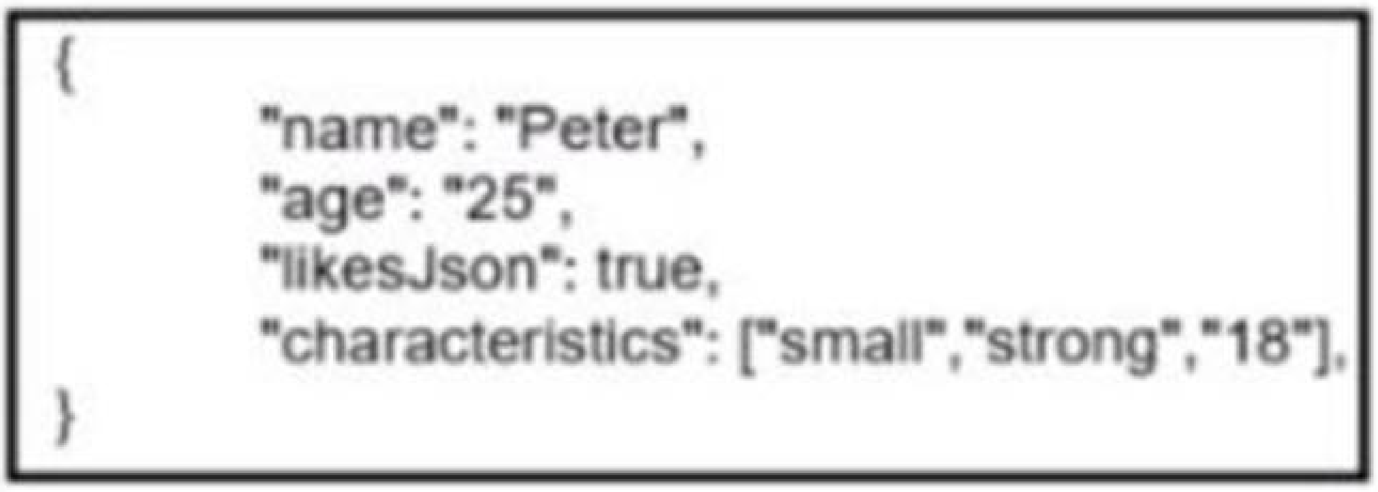
Answer: B

NEW QUESTION 251
- (Topic 1)
Which data is properly formatted with JSON?
A)



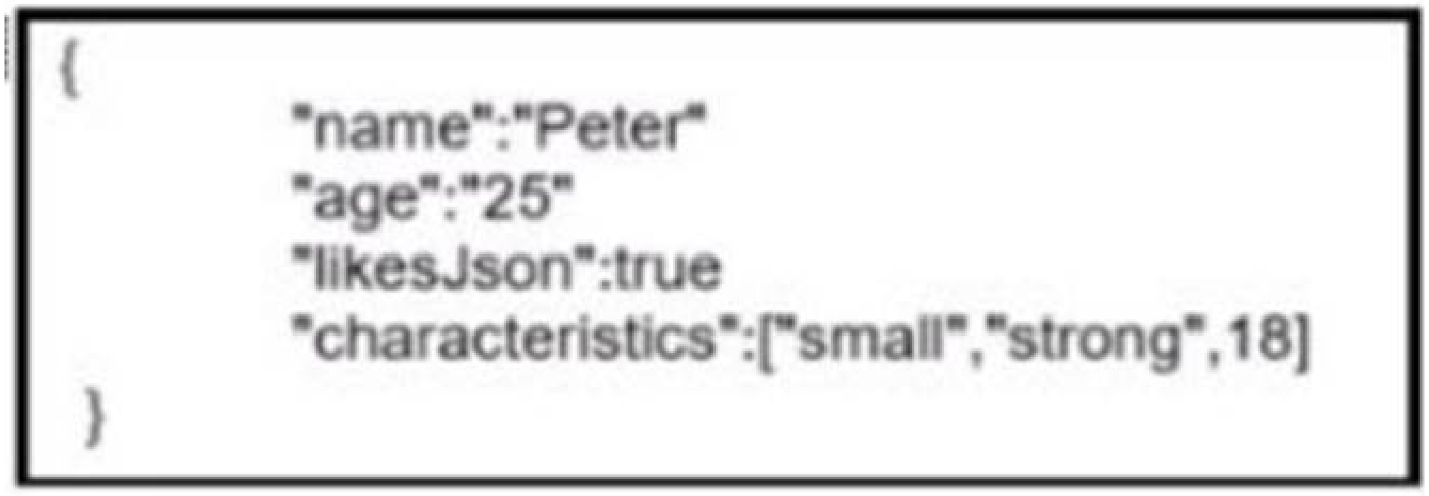
```
{
        "name": "Peter",
        "age": "25",
        "likesJson": true,
        "characteristics": ["small","strong",18]
}
```

B)



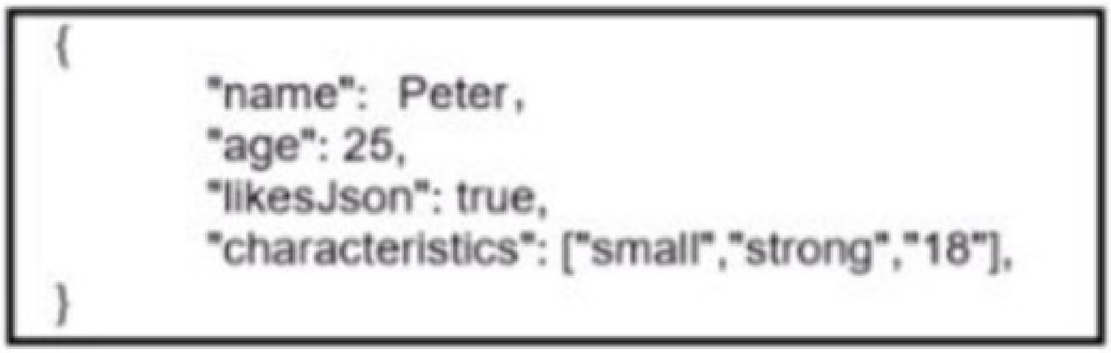
```
{
        "name": "Peter",
        "age": "25",
        "likesJson": true,
        "characteristics": ["small","strong","18"],
}
```

C)



```
{
        "name":"Peter"
        "age":"25"
        "likesJson":true
        "characteristics":["small","strong",18]
}
```

D)



```
{
        "name":  Peter,
        "age": 25,
        "likesJson": true,
        "characteristics": ["small","strong","18"],
}
```

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

Answer: A

NEW QUESTION 252
- (Topic 1)
An engineer must provide wireless converge in a square office. The engineer has only one AP and believes that it should be placed it in the middle of the room. Which antenna type should the engineer use?

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

Answer: D

NEW QUESTION 256
- (Topic 1)

What is a fact about Cisco EAP-FAST?

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

Answer: A

NEW QUESTION 258
- (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 262
- (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.

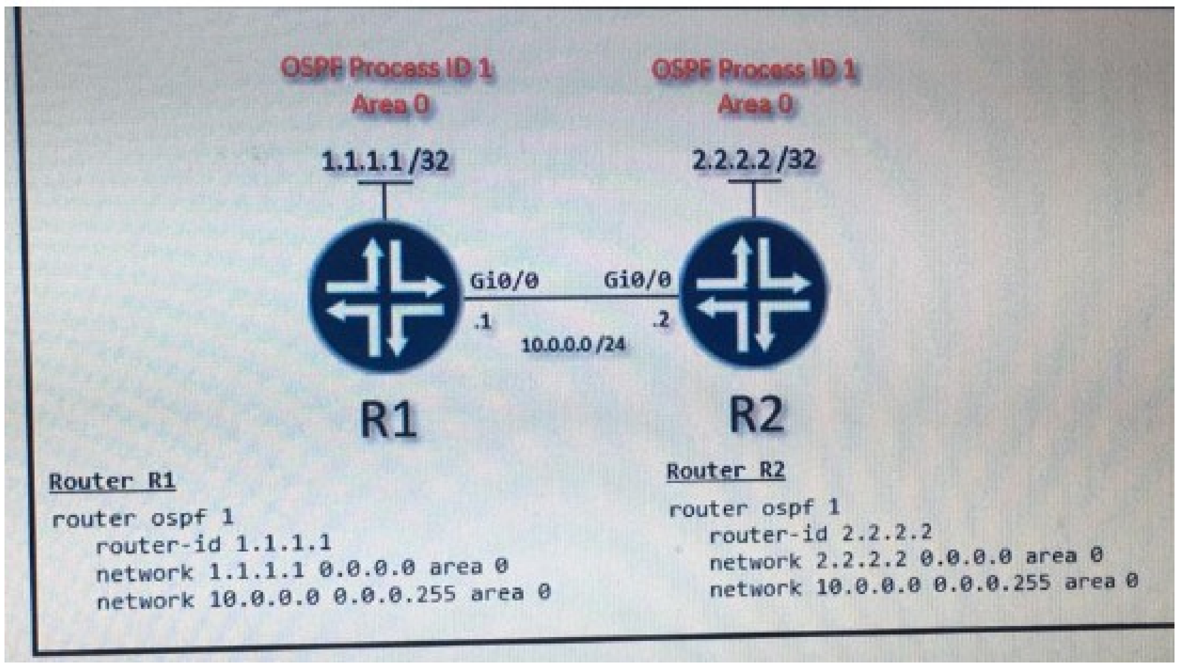
Answer: C

NEW QUESTION 263
- (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 264
- (Topic 1)
Refer to the exhibit.



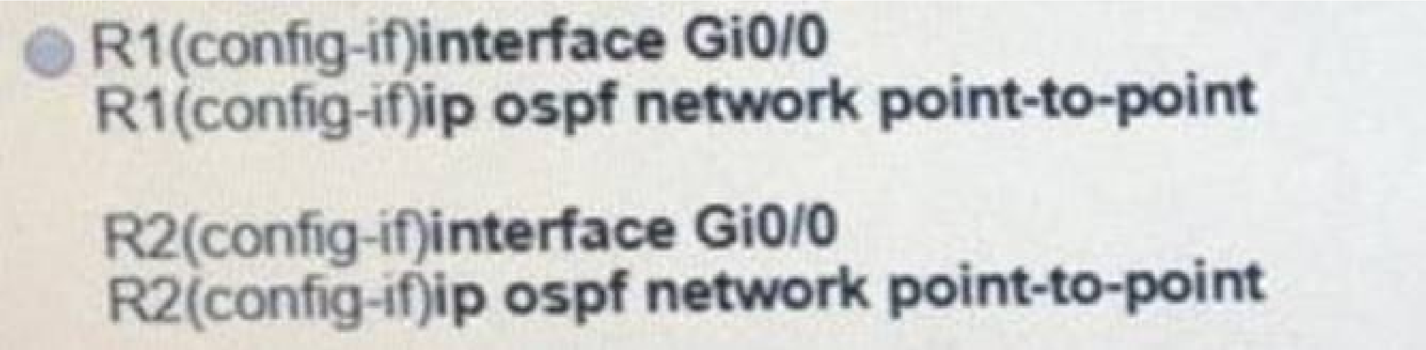
Router R1

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

Router R2

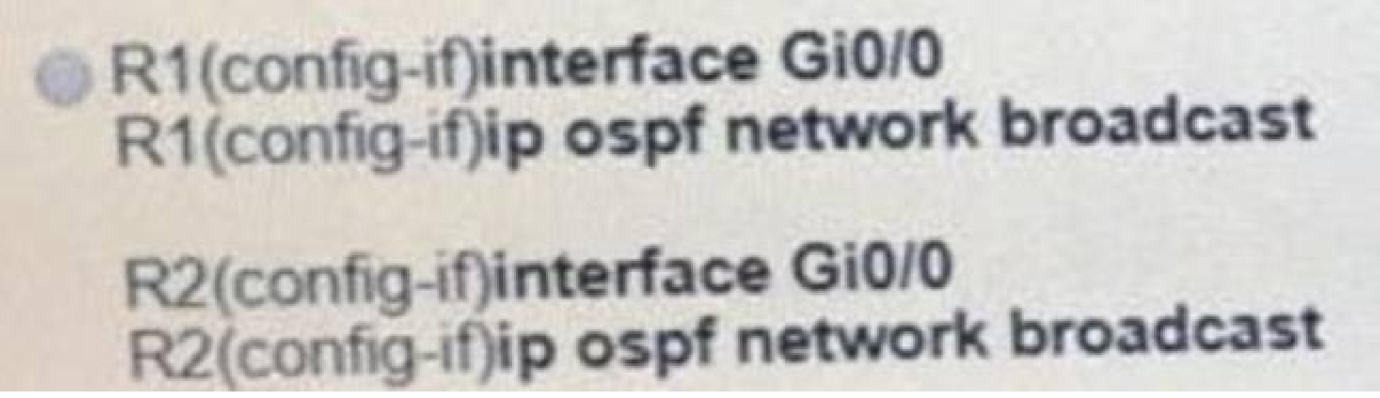
```
router ospf 1
   router-id 2.2.2.2
   network 2.2.2.2 0.0.0.0 area 0
   network 10.0.0.0 0.0.0.255 area 0
```

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



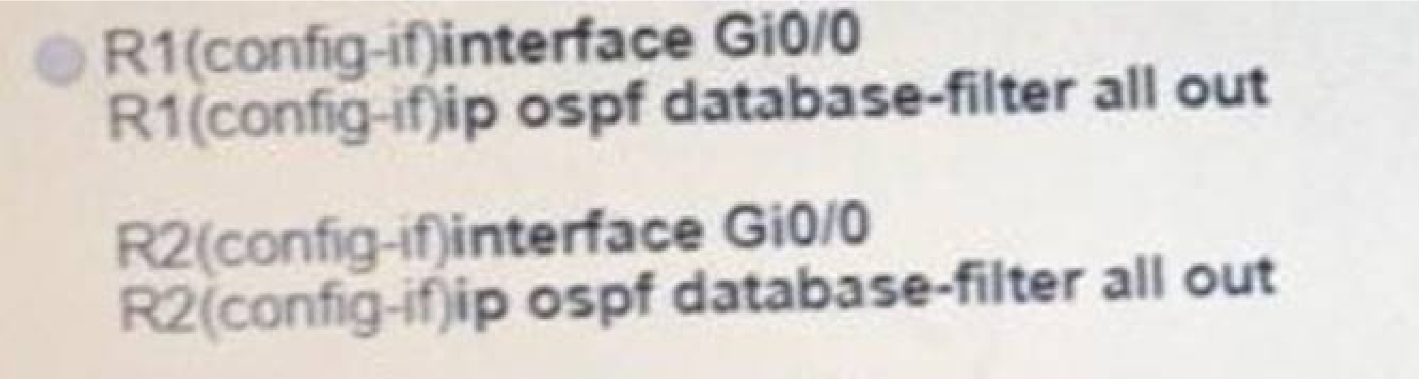
```
○ R1(config-if)interface Gi0/0
  R1(config-if)ip ospf network point-to-point

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

B)



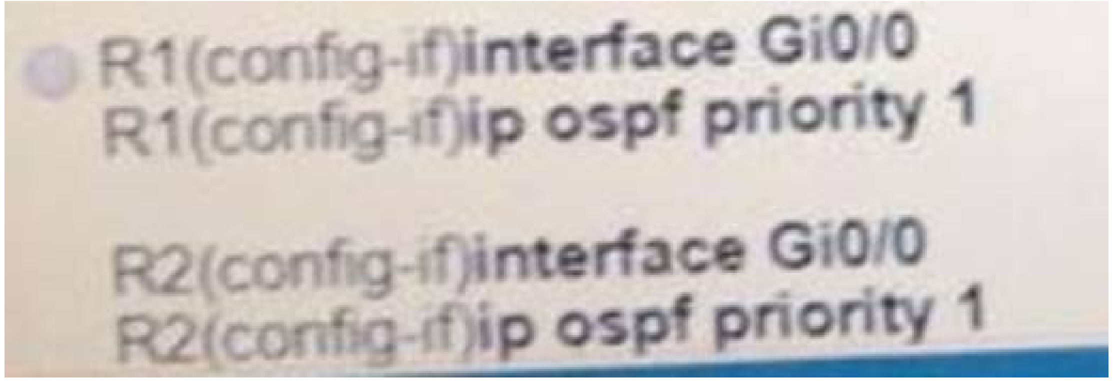
```
○ R1(config-if)interface Gi0/0
  R1(config-if)ip ospf network broadcast

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

C)



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

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

D)



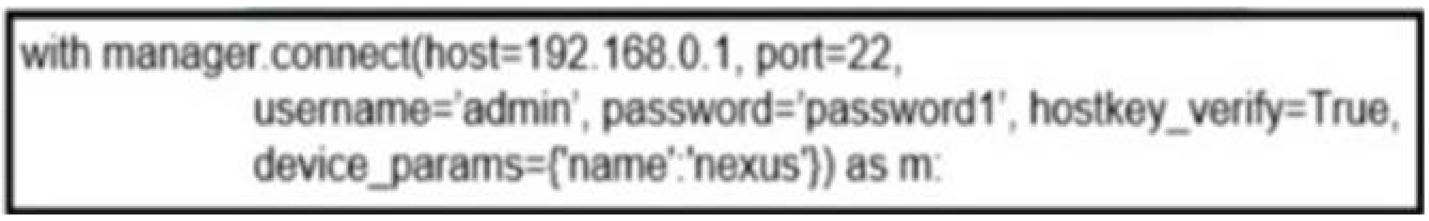
```
○ R1(config-if)interface Gi0/0
  R1(config-if)ip ospf priority 1

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

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

Answer: A

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

NEW QUESTION 265
- (Topic 1)
Refer to the exhibit.



```
with manager.connect(host=192.168.0.1, port=22,
                     username='admin', password='password1', hostkey_verify=True,
                     device_params={'name':'nexus'}) as m:
```

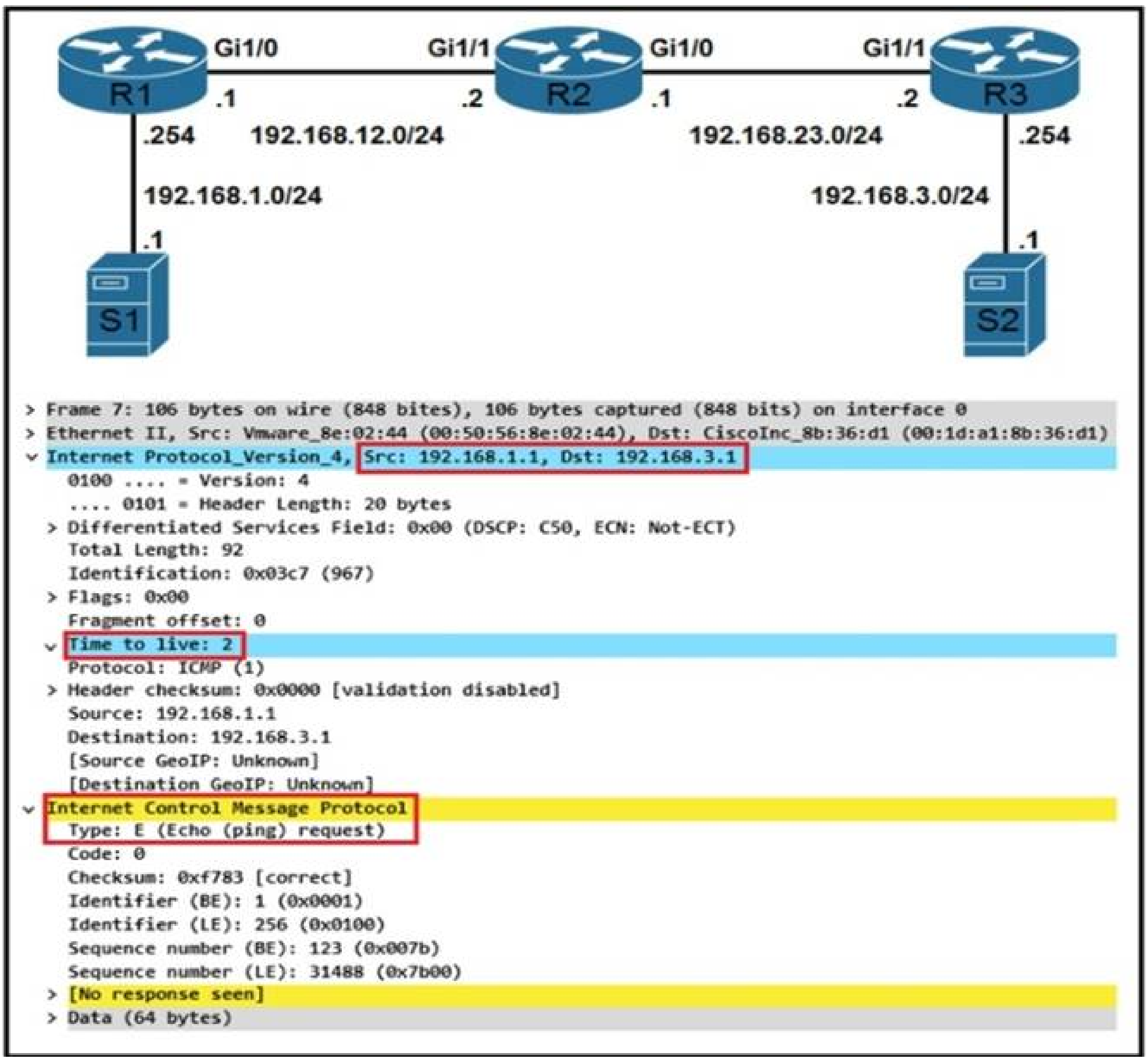
What does the snippet of code achieve?

A. It creates a temporary connection to a Cisco Nexus device and retrieves a token to be used for API calls.
B. It opens a tunnel and encapsulates the login information, if the host key is correct.
C. It opens an ncclient connection to a Cisco Nexus device and maintains it for the duration of the context.
D. It creates an SSH connection using the SSH key that is stored, and the password is ignored.

Answer: C

Explanation:
ncclient is a Python library that facilitates client-side scripting and application development around the NETCONF protocol.
The above Python snippet uses the ncclient to connect and establish a NETCONF session to a Nexus device (which is also a NETCONF server).

NEW QUESTION 266
- (Topic 1)
Refer to the exhibit.



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

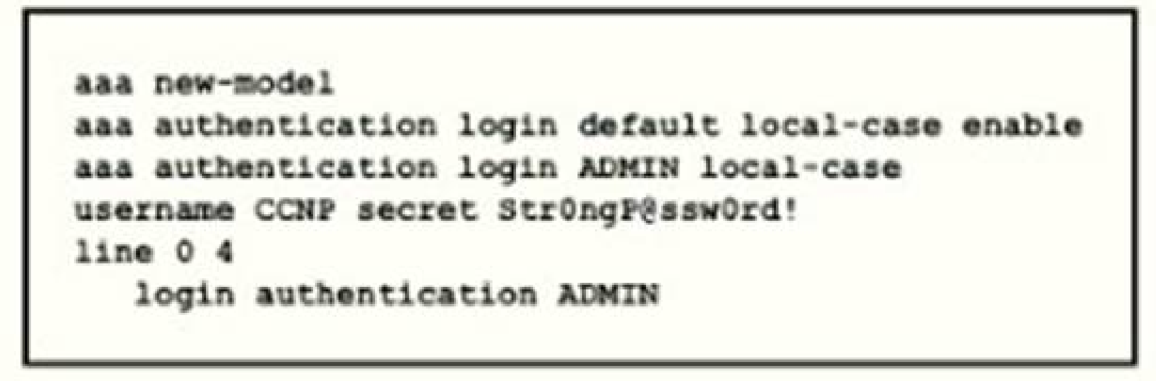
Which troubleshooting a routing issue, an engineer issues a ping from S1 to S2. When two actions from the initial value of the TTL? (Choose two.)

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

Answer: AD

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

NEW QUESTION 267
- (Topic 1)
Refer to the exhibit.



```
aaa new-model
aaa authentication login default local-case enable
aaa authentication login ADMIN local-case
username CCNP secret Str0ngP@ssw0rd!
line 0 4
   login authentication ADMIN
```

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

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

Answer: C

Explanation:
The autocommand causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated.

Because the command can be any length and can contain embedded spaces, commands using the autocommand keyword must be the last option on the line. In this specific question, we have to enter this line username CCNP autocommand show running-config.

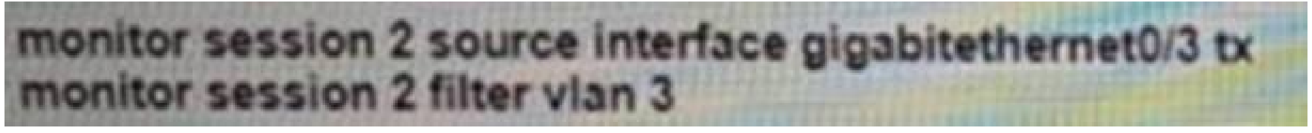
NEW QUESTION 271
- (Topic 1)
Which two threats does AMP4E have the ability to block? (Choose two.)

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

Answer: BC

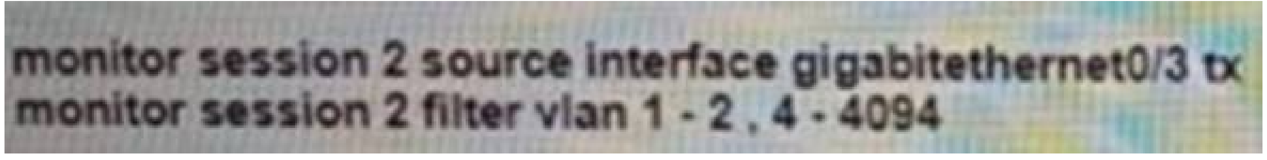
Explanation:
https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/c11-742008-00-cisco-amp-for-endpoints-wp-v2a.pdf

NEW QUESTION 273
- (Topic 1)
Which command set configures RSPAN to capture outgoing traffic from VLAN 3 on interface GigabitEthernet 0/3 while ignoring other VLAN traffic on the same interface?
A)



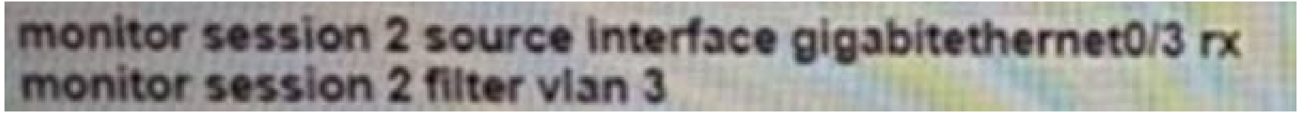
```
monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 3
```

B)



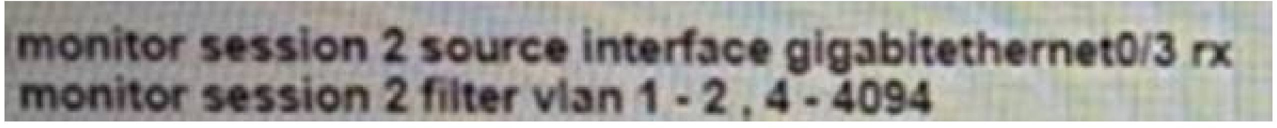
```
monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 1 - 2 , 4 - 4094
```

C)



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

D)

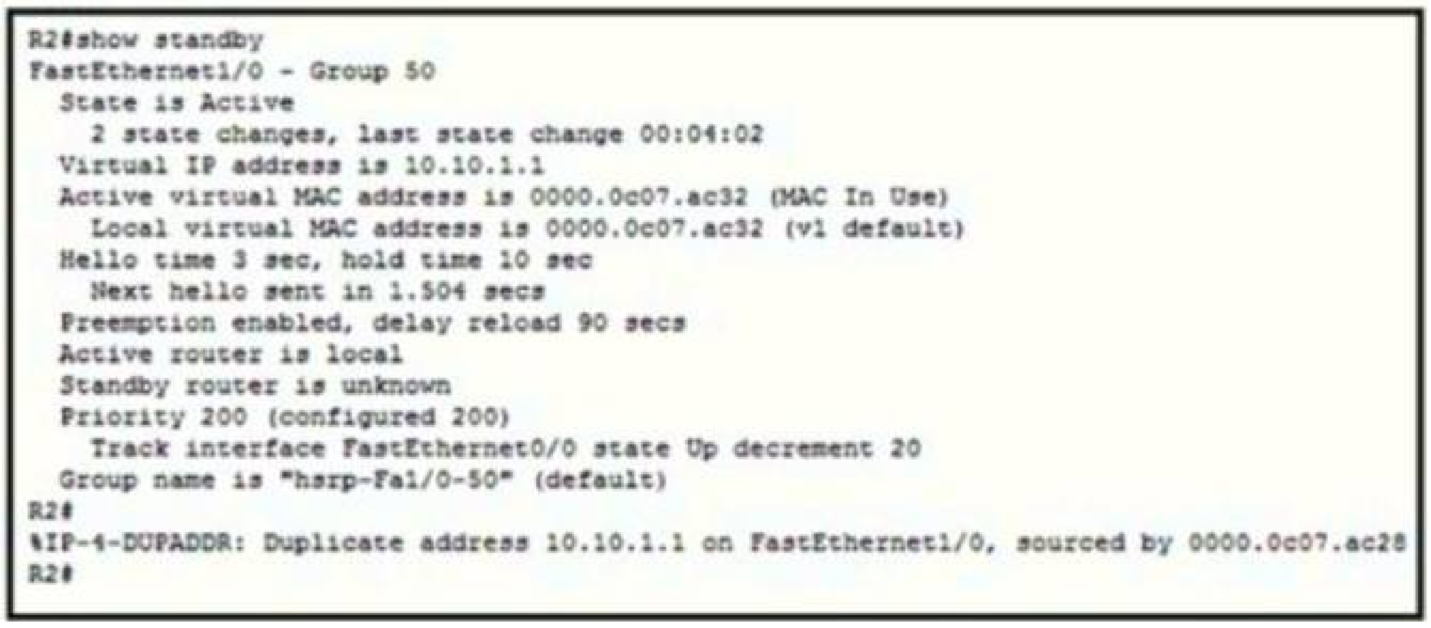


```
monitor session 2 source interface gigabitethernet0/3 rx
monitor session 2 filter vlan 1 - 2 , 4 - 4094
```

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

Answer: A

NEW QUESTION 278
- (Topic 1)



```
R2#show standby
FastEthernet1/0 - Group 50
  State is Active
    2 state changes, last state change 00:04:02
  Virtual IP address is 10.10.1.1
  Active virtual MAC address is 0000.0c07.ac32 (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac32 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.504 secs
  Preemption enabled, delay reload 90 secs
  Active router is local
  Standby router is unknown
  Priority 200 (configured 200)
    Track interface FastEthernet0/0 state Up decrement 20
  Group name is "hsrp-Fa1/0-50" (default)
R2#
%IP-4-DUPADDR: Duplicate address 10.10.1.1 on FastEthernet1/0, sourced by 0000.0c07.ac28
R2#
```

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

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

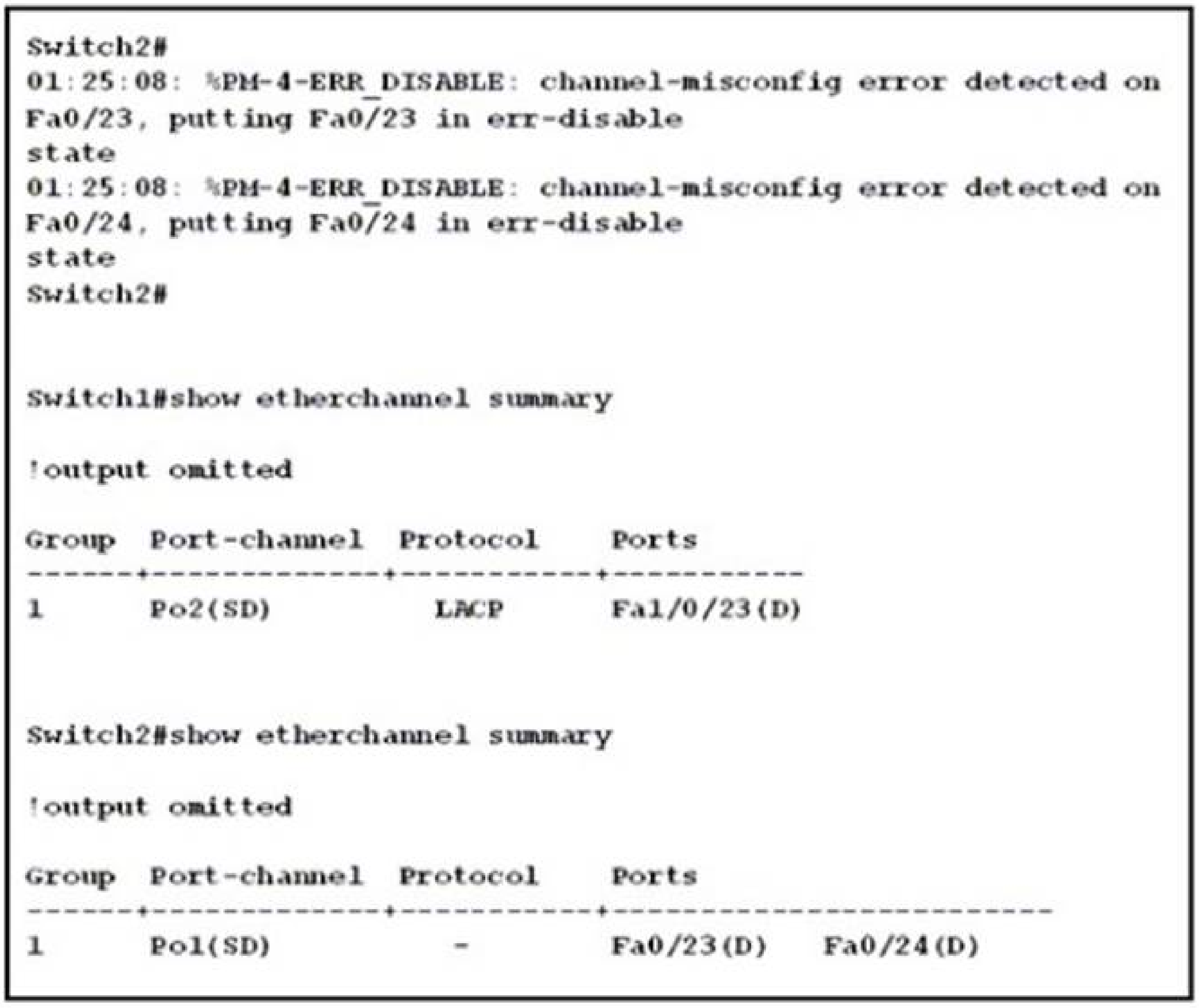
Answer: A

NEW QUESTION 282
- (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 285
- (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

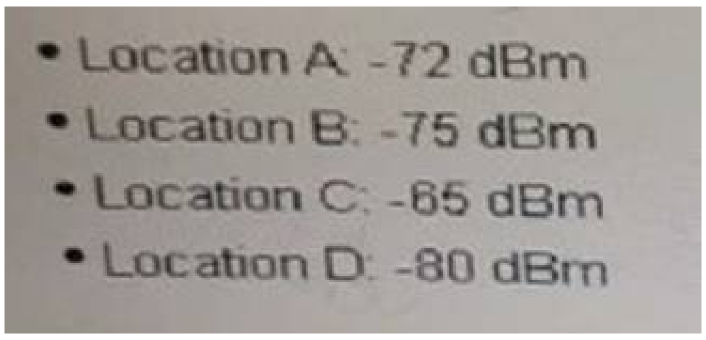
Explanation:
In this case, we are using your EtherChannel without a negotiation protocol on Switch2. As a result, if the opposite switch is not also configured for EtherChannel operation on the respective ports, there is a danger of a switching loop. The EtherChannel Misconfiguration Guard tries to prevent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

NEW QUESTION 288
- (Topic 1)
Under which network conditions is an outbound QoS policy that is applied on a router WAN interface most beneficial?

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

Answer: A

NEW QUESTION 289
- (Topic 1)
An engineer measures the Wi-Fi coverage at a customer site. The RSSI values are recorded as follows:



- Location A: -72 dBm
- Location B: -75 dBm
- Location C: -65 dBm
- Location D: -80 dBm

Which two statements does the engineer use to explain these values to the customer? (Choose two)

A. The signal strength at location C is too weak to support web surfing
B. Location D has the strongest RF signal strength
C. The RF signal strength at location B is 50% weaker than location A
D. The signal strength at location B is 10 dB better than location C
E. The RF signal strength at location C is 10 times stronger than location B

Answer: CE

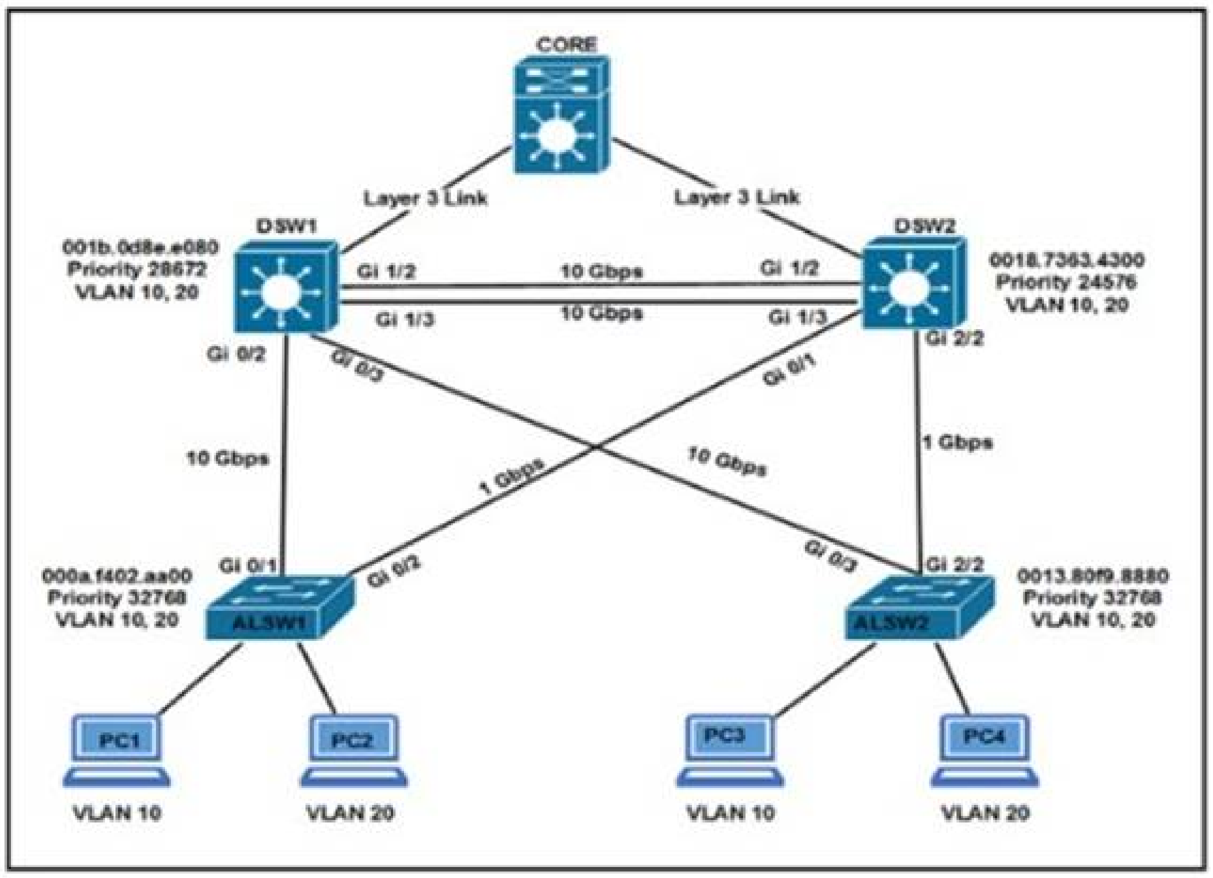
NEW QUESTION 293
- (Topic 1)
“HTTP/1.1 204 content” is returned when cur –I –x delete command is issued. Which situation has occurred?

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

Answer: B

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

NEW QUESTION 297
- (Topic 4)



Refer to the exhibit. Which two commands ensure that DSW1 becomes root bridge for VLAN 10? (Choose two)

A. DSW1(config)#spanning-tree vlan 10 priority 4096 Most Voted
B. DSW1(config)#spanning-tree vlan 10 priority root
C. DSW2(config)#spanning-tree vlan 10 priority 61440 Most Voted
D. DSW1(config)#spanning-tree vlan 10 port-priority 0
E. DSW2(config)#spanning-tree vlan 20 priority 0

Answer: CD

Explanation:
Ref: Scaling Networks v6 Companion Guide
“STP
…
Extended System ID
…
Bridge Priority
The bridge priority is a customizable value that can be used to influence which switch becomes the root bridge. The switch with the lowest priority, which implies the lowest BID, becomes the root bridge because a lower priority value takes precedence.
…

The default priority value for all Cisco switches is the decimal value 32768. The range is 0 to 61440, in increments of 4096. Therefore, valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. A bridge priority of 0 takes precedence over all other bridge priorities. All other values are rejected.

NEW QUESTION 298
- (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 300
- (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 302
- (Topic 4)
Which two methods are used by an AP that is typing to discover a wireless LAN controller? (Choose two.)

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

Answer: BD

NEW QUESTION 306
- (Topic 4)
Why would a small or mid-size business choose a cloud solution over an on-premises solution?

A. Cloud provides higher data security than on-premises.
B. Cloud provides more control over the implementation process than on-premises.
C. Cloud provides greater ability for customization than on-premises.
D. Cloud provides lower upfront cost than on-premises.

Answer: C

NEW QUESTION 309
- (Topic 4)
What does the statement print(format(0.8, '.0%')) display?

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

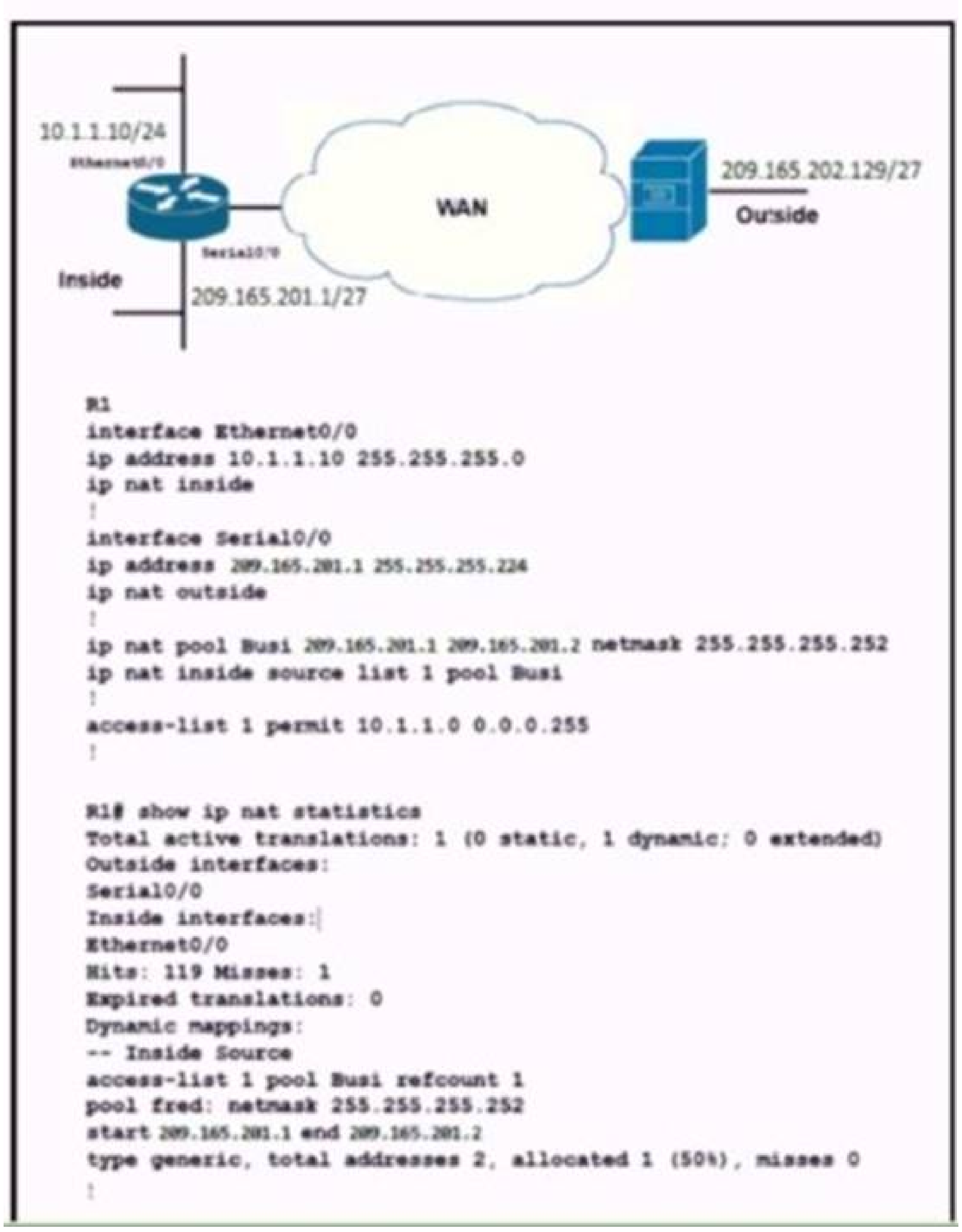
Answer: B

NEW QUESTION 313
- (Topic 4)
In which way are EIGRP and OSPF similar?

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

Answer: C

NEW QUESTION 317
- (Topic 4)



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

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

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

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

Answer: A

NEW QUESTION 320
- (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 322
- (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 325
- (Topic 4)
Which two functions is an edge node responsible for? (Choose two.)

A. provides multiple entry and exit points for fabric traffic

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

Answer: AD

NEW QUESTION 330
- (Topic 4)
A customer deploys a new wireless network to perform location-based services using Cisco DNA Spaces The customer has a single WLC located on-premises in a secure data center. The security team does not want to expose the WLC to the public Internet. Which solution allows the customer to securely send RSSI updates to Cisco DNA Spaces?

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

Answer: D

NEW QUESTION 334
- (Topic 4)
What is a characteristics of Cisco SD-WAN?

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

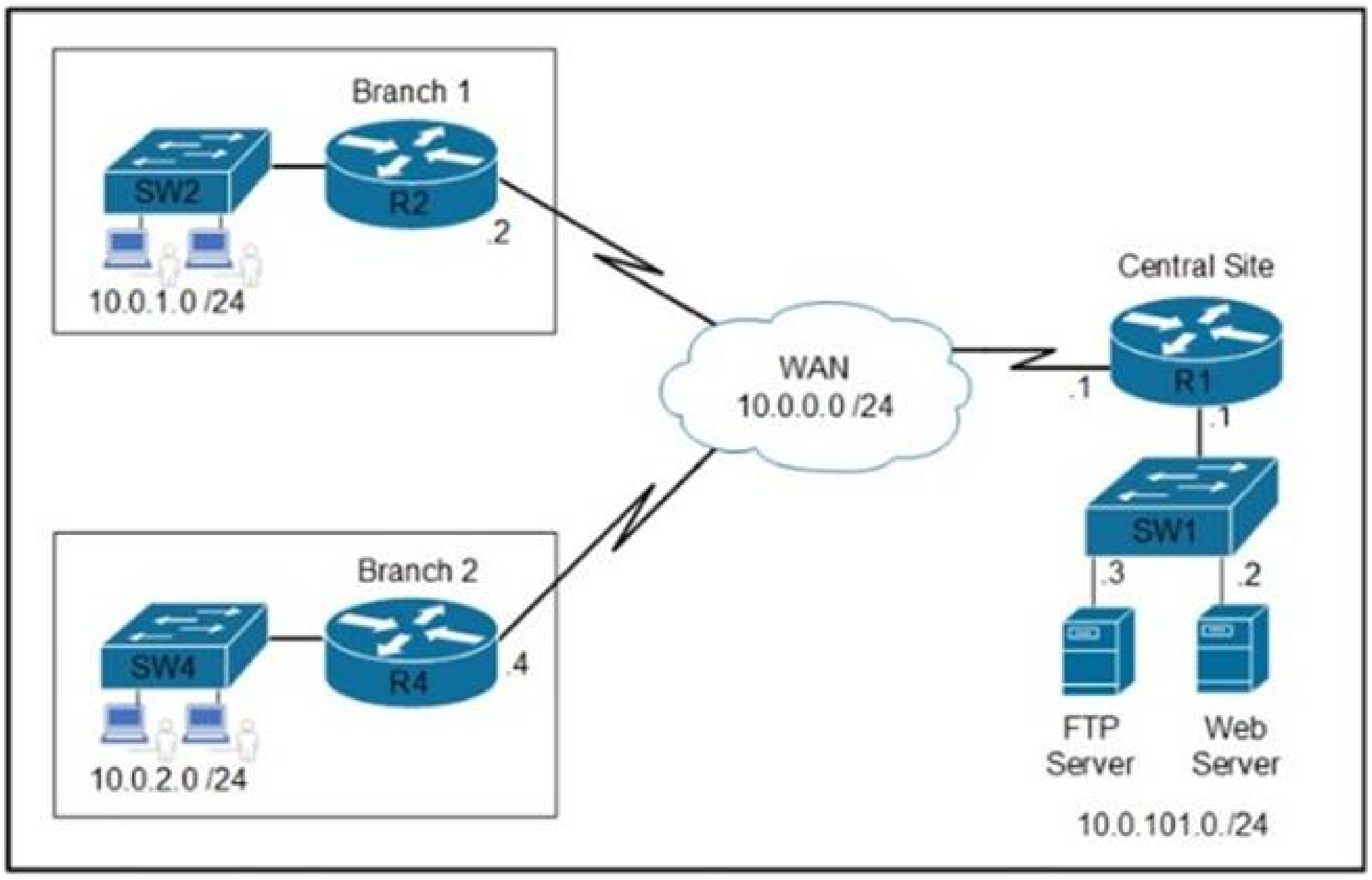
Answer: A

NEW QUESTION 338
- (Topic 4)
Which signal strength and noise values meet the minimum SNR for voice networks?

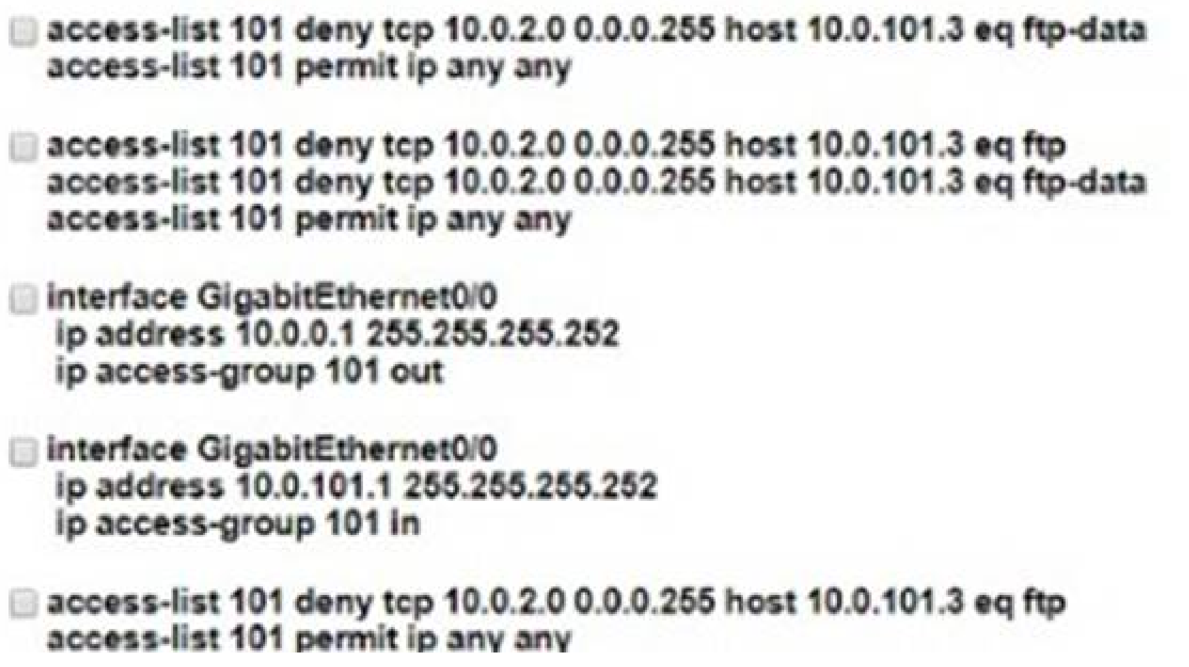
A. signal strength -67 dBm, noise 91 dBm
B. signal strength -69 dBm, noise 94 dBm
C. signal strength -68 dBm, noise 89 dBm
D. signal strength -66 dBm, noise 90 dBm

Answer: A

NEW QUESTION 343
- (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

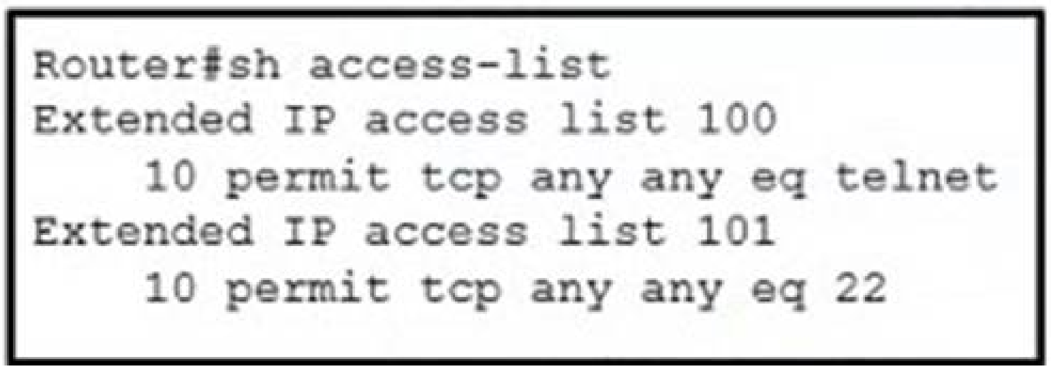
□ interface GigabitEthernet0/0
ip address 10.0.101.1 255.255.255.252
ip access-group 101 in

□ 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

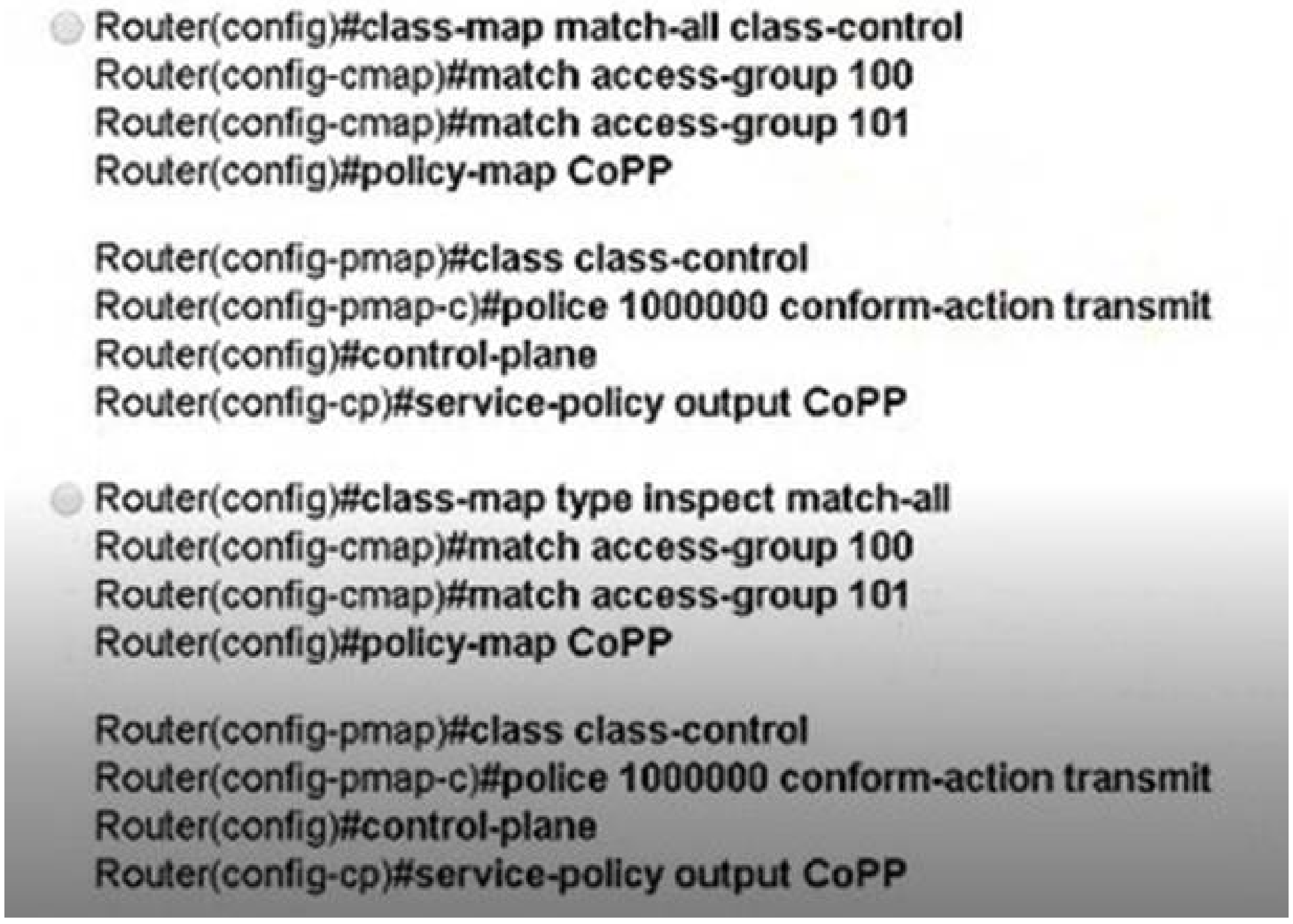
Answer: BC

NEW QUESTION 347
- (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?

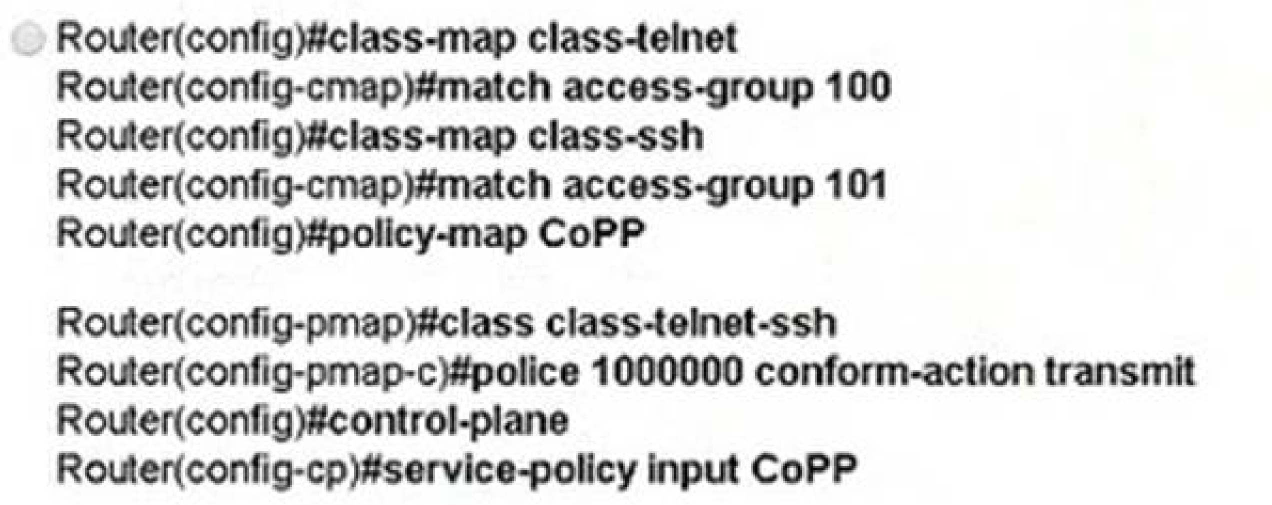


○ Router(config)#class-map match-all class-control
Router(config-cmap)#match access-group 100
Router(config-cmap)#match access-group 101
Router(config)#policy-map CoPP

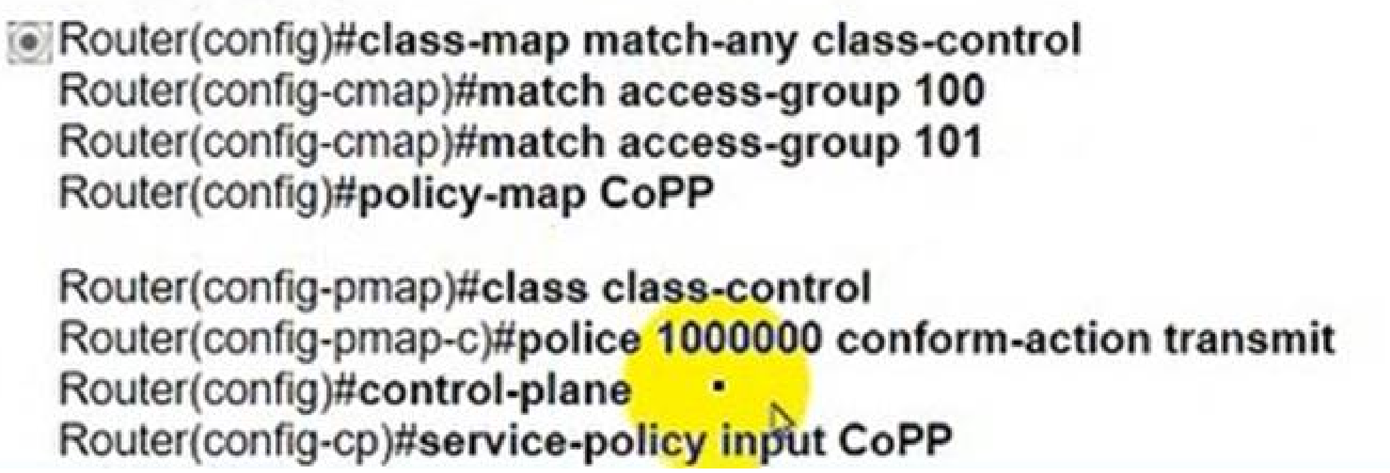
Router(config-pmap)#class class-control
Router(config-pmap-c)#police 1000000 conform-action transmit
Router(config)#control-plane
Router(config-cp)#service-policy output CoPP

○ 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
```

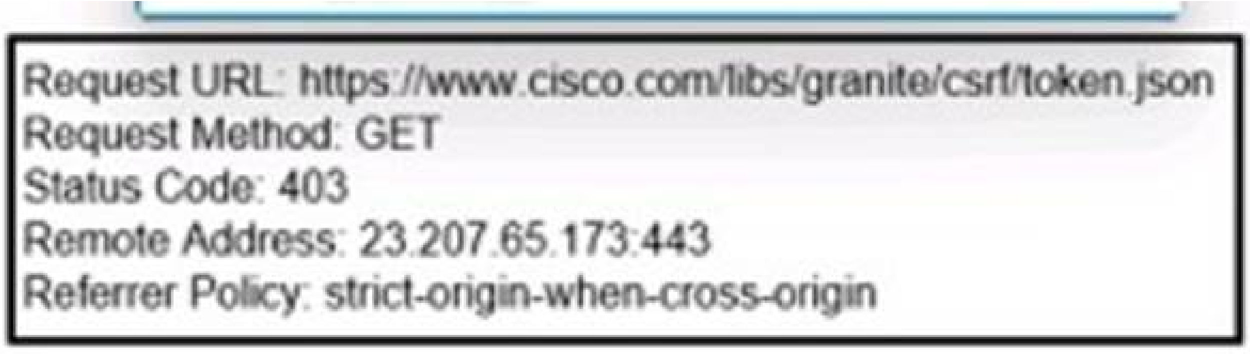


```
● Router(config)#class-map match-any class-control
  Router(config-cmap)#match access-group 100
  Router(config-cmap)#match access-group 101
  Router(config)#policy-map CoPP

  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 352
- (Topic 4)



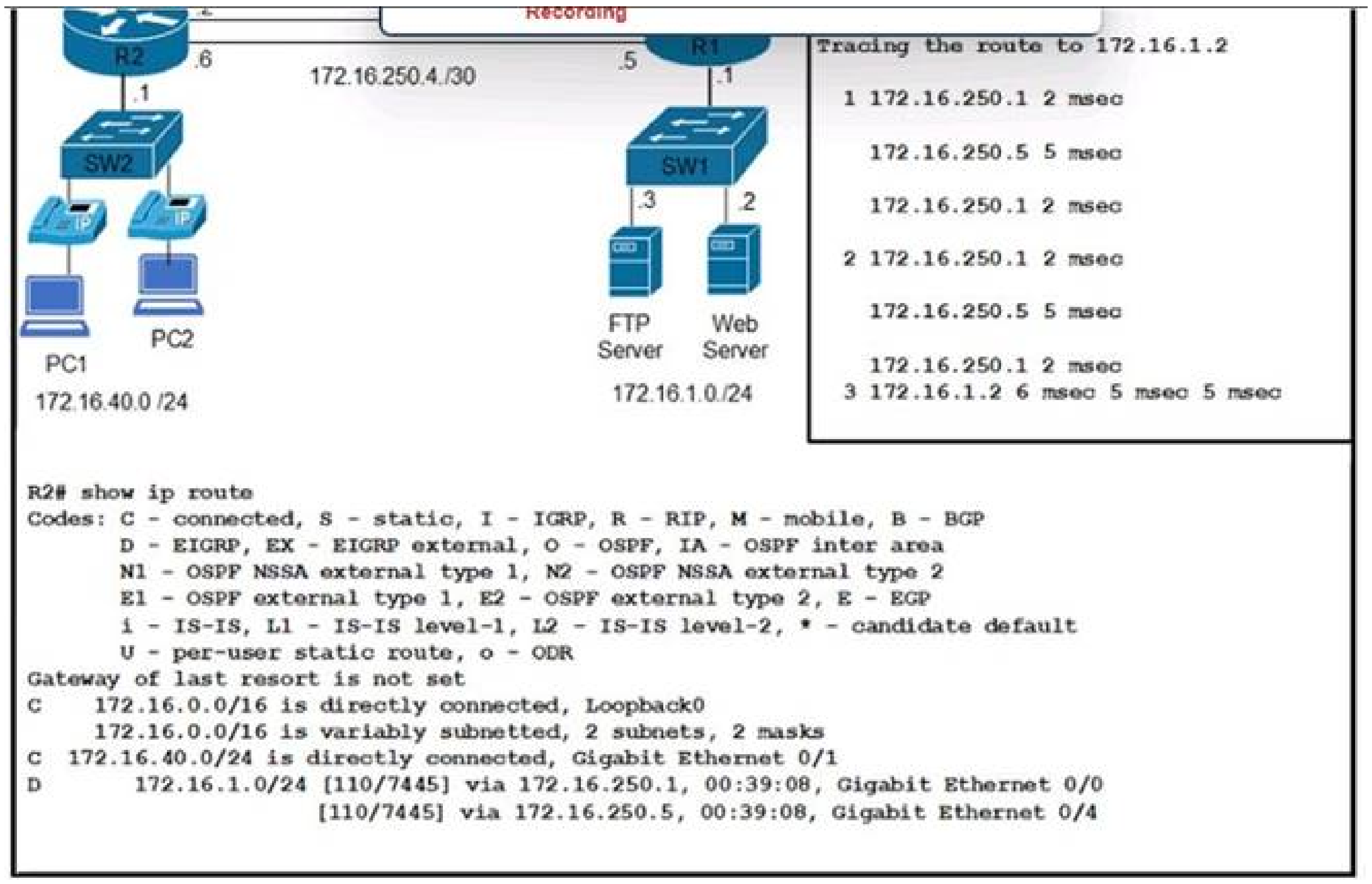
```
Request URL: https://www.cisco.com/libs/granite/csrf/token.json
Request Method: GET
Status Code: 403
Remote Address: 23.207.65.173:443
Referrer Policy: strict-origin-when-cross-origin
```

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 357
- (Topic 4)
Refer to the exhibit.



```
Tracing the route to 172.16.1.2
 1 172.16.250.1 2 msec
   172.16.250.5 5 msec
   172.16.250.1 2 msec
 2 172.16.250.1 2 msec
   172.16.250.5 5 msec
   172.16.250.1 2 msec
 3 172.16.1.2 6 msec 5 msec 5 msec
```

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

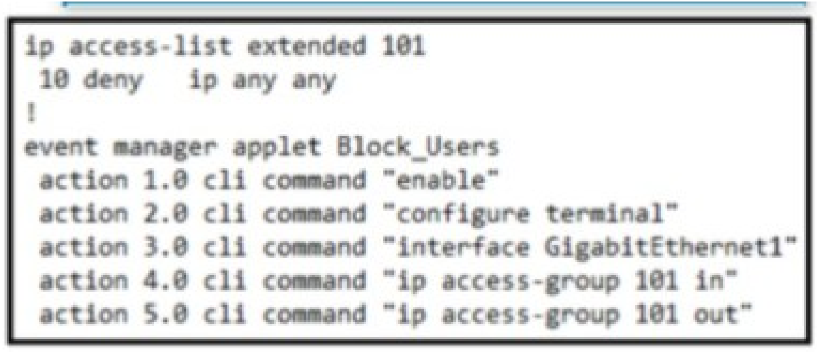
Clients are reporting an issue with the voice traffic from the branch site to the central site. What is the cause of this issue?

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

Answer: C

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

NEW QUESTION 360
- (Topic 4)



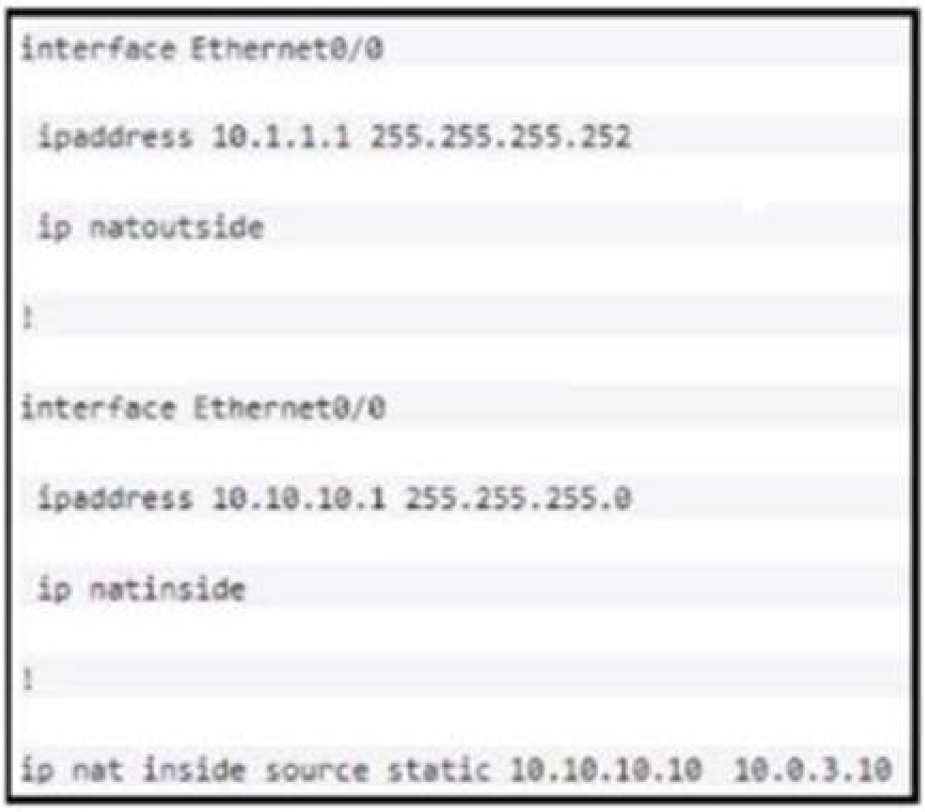
```
ip access-list extended 101
 10 deny   ip any any
!
event manager applet Block_Users
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "interface GigabitEthernet1"
 action 4.0 cli command "ip access-group 101 in"
 action 5.0 cli command "ip access-group 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 363
- (Topic 4)
Refer lo the exhibit.



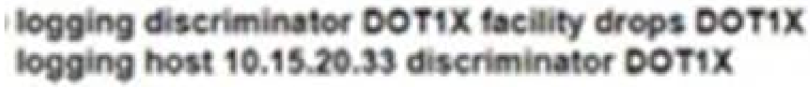
```
interface Ethernet0/0

 ipaddress 10.1.1.1 255.255.255.252

 ip natoutside

!

interface Ethernet0/0

 ipaddress 10.10.10.1 255.255.255.0

 ip natinside

!

ip nat inside source static 10.10.10.10  10.0.3.10
```

Which address type is 10.10.10.10 configured for?

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

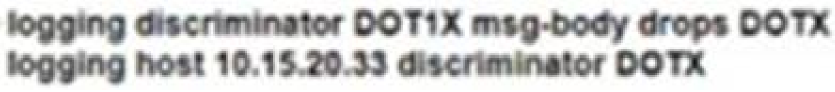
Answer: D

NEW QUESTION 368
- (Topic 4)
Which configuration filters out DOT1X messages in the format shown below from being sent toward Syslog server 10.15.20.33?
A)



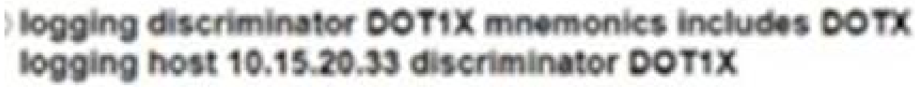
```
logging discriminator DOT1X facility drops DOT1X
logging host 10.15.20.33 discriminator DOT1X
```

B)



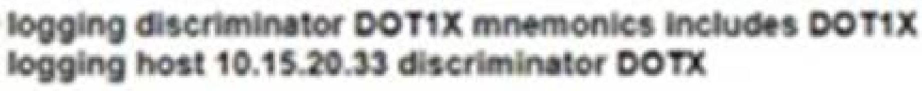
```
logging discriminator DOT1X msg-body drops DOTX
logging host 10.15.20.33 discriminator DOTX
```

C)



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

D)

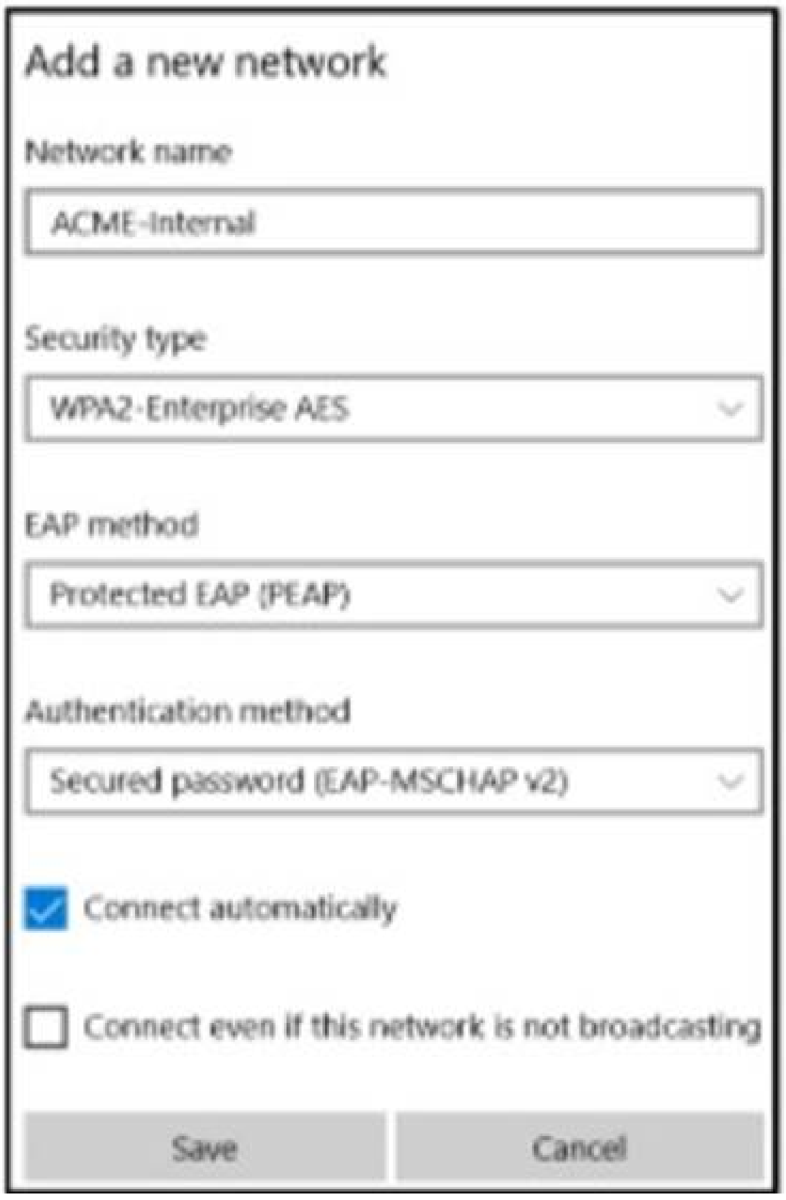


```
logging discriminator DOT1X mnemonics includes DOT1X
logging host 10.15.20.33 discriminator DOTX
```

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

Answer: A

NEW QUESTION 373
- (Topic 4)
Refer to the exhibit.



Add a new network

Network name

ACME-Internal

Security type

WPA2-Enterprise AES

EAP method

Protected EAP (PEAP)

Authentication method

Secured password (EAP-MSCHAP v2)

☑ Connect automatically

□ Connect even if this network is not broadcasting

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

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

Answer: A

NEW QUESTION 376
- (Topic 4)
In a wireless network environment, what is calculated using the numerical values of the transmitter power level, cable loss, and antenna gain?

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

Answer: B

NEW QUESTION 378
- (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:

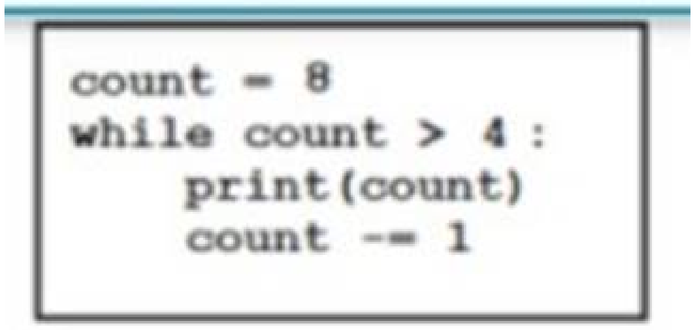
```
 interface Ethernet0/0.100 encapsulation dot1Q 100
ip address 10.0.111.1 255.255.255.0
standby 15 ip 10.0.111.254
!
cisco(config-subif)#do s stand Ethernet0/0.100 - Group 15
State is Speak
Virtual IP address is 10.0.111.254 Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac0f (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 381
- (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 386
- (Topic 4)
Refer to the exhibit.



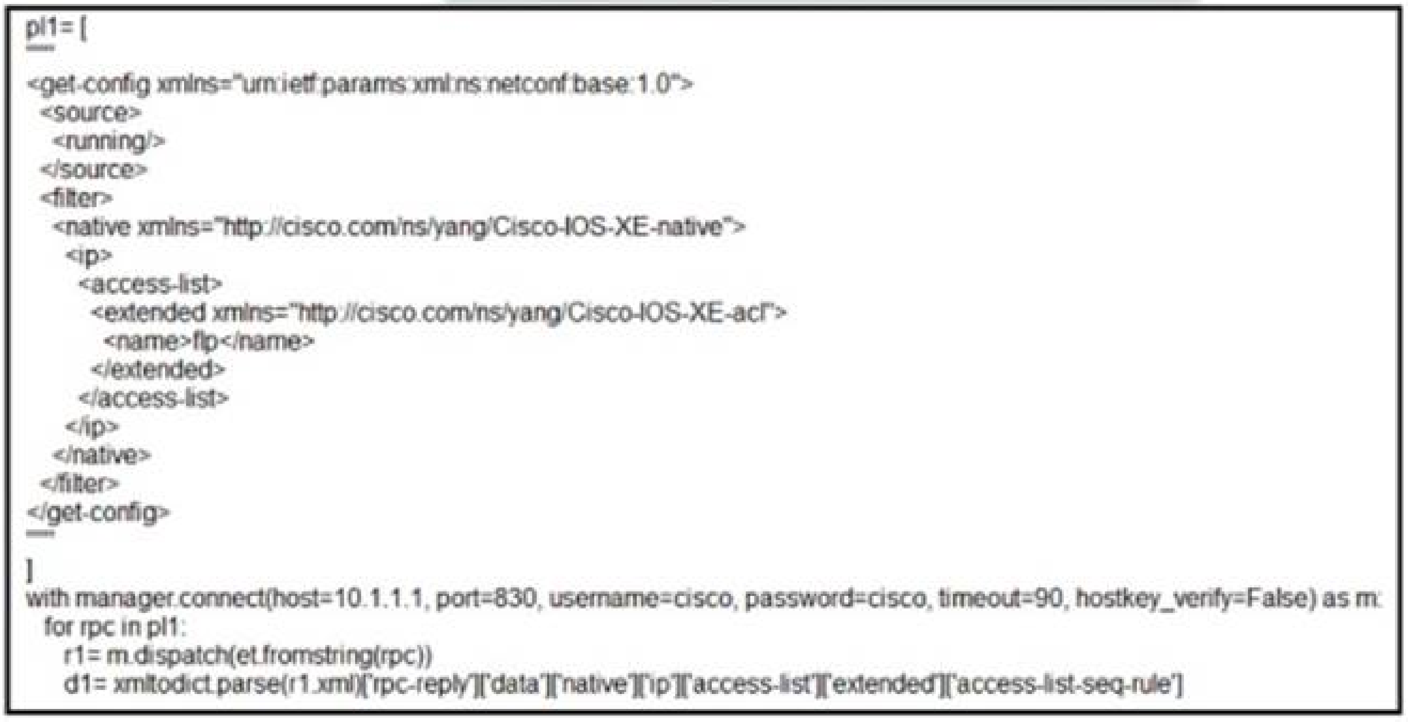
```
count = 8
while count > 4 :
    print(count)
    count -= 1
```

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 387
- (Topic 4)
Refer to the exhibit.



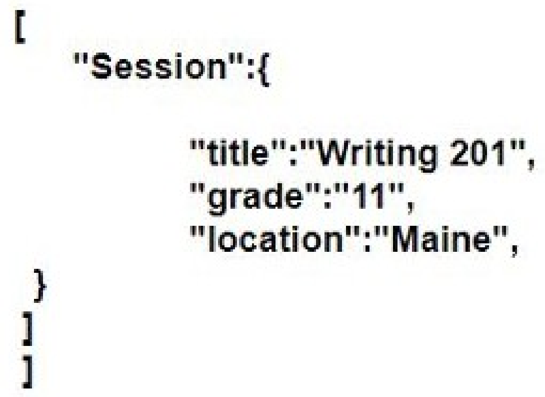
```
pl1= [

<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.

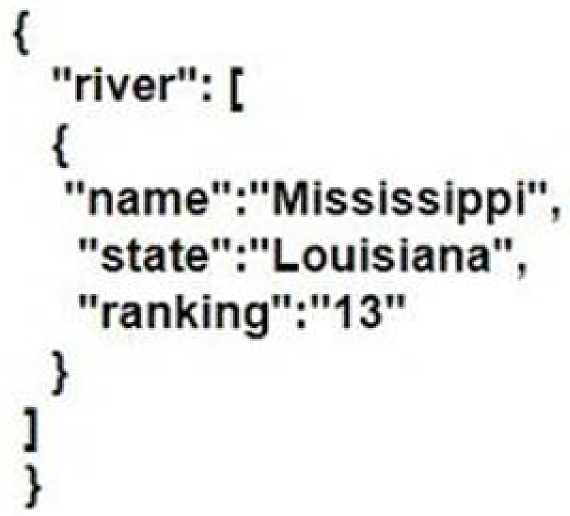
Answer: A

NEW QUESTION 391
- (Topic 4)
Which JSON script is properly formatted?
A)



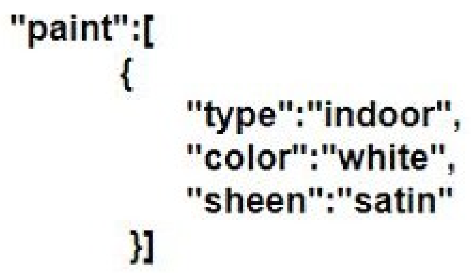
```
[
   "Session":{

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

B)



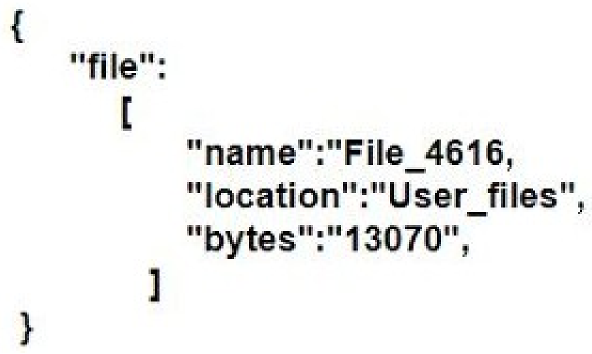
```
{
  "river": [
  {
   "name":"Mississippi",
    "state":"Louisiana",
    "ranking":"13"
  }
 ]
 }
```

C)



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

D)



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

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

Answer: A

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

NEW QUESTION 394
- (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 397
- (Topic 4)
In which two ways does the routing protocol OSPF differ from EIGRP? (Choose two.)

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

Answer: AD

NEW QUESTION 398
- (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 402
- (Topic 4)
A customer has a pair of Cisco 5520 WLCs set up in an SSO cluster to manage all APs. Guest traffic is anchored to a Cisco 3504 WLC located in a DMZ. Which action is needed to ensure that the EolP tunnel remains in an UP state in the event of failover on the SSO cluster?

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

Answer: B

NEW QUESTION 404
- (Topic 4)
Which element is unique to a Type 2 hypervisor?

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

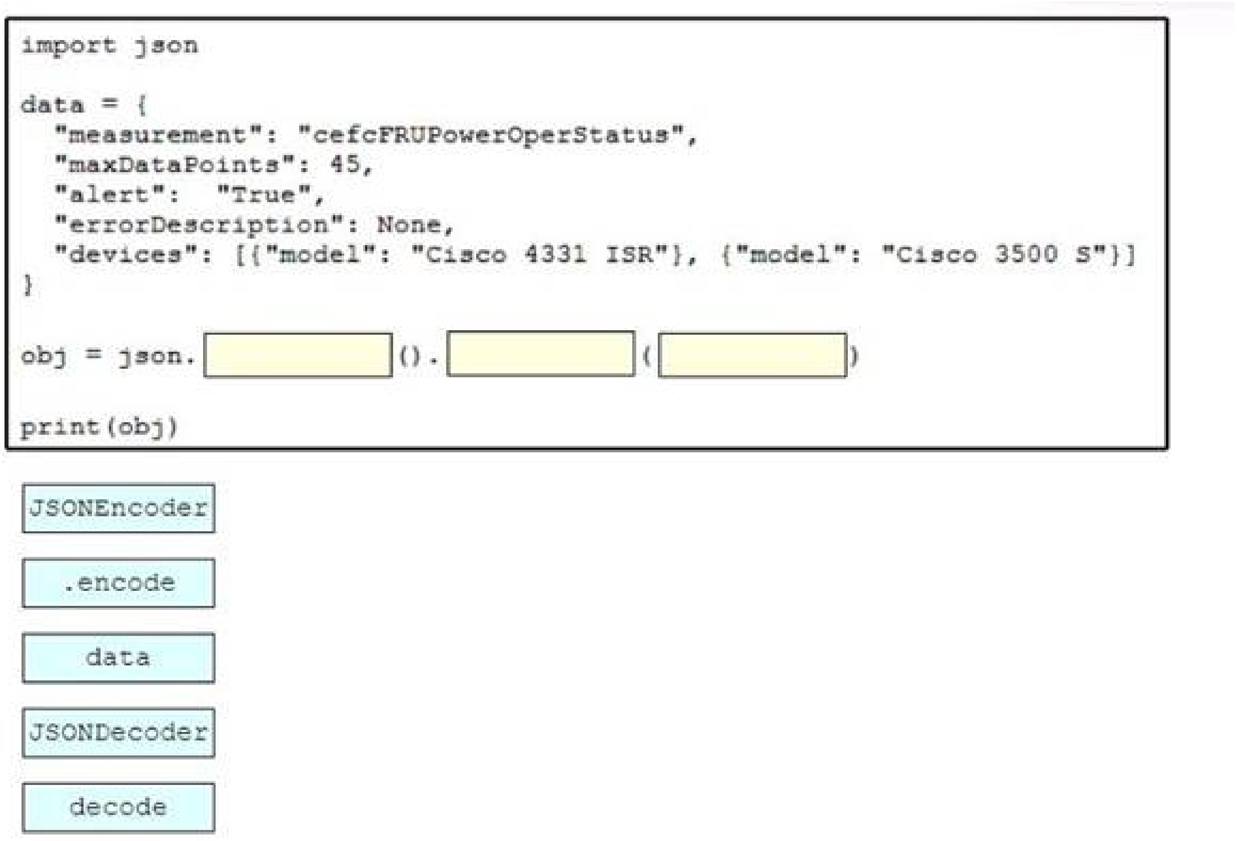
Answer: C

NEW QUESTION 406
- (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 411
DRAG DROP - (Topic 4)
Drag and drop the code snippets from the bottom onto the blanks in the script to convert a Python object into a JSON string. Not all options are used.



```
import json

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

obj = json.            ().            (            )

print(obj)
```

JSONEncoder

.encode

data

JSONDecoder

decode

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 413
- (Topic 4)
How do stratum levels relate to the distance from a time source?

A. Stratum 1 devices are connected directly to an authoritative time source.
B. Stratum 15 devices are connected directly to an authoritative time source
C. Stratum 0 devices are connected directly to an authoritative time source.
D. Stratum 15 devices are an authoritative time source.

Answer: C

NEW QUESTION 418
- (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.

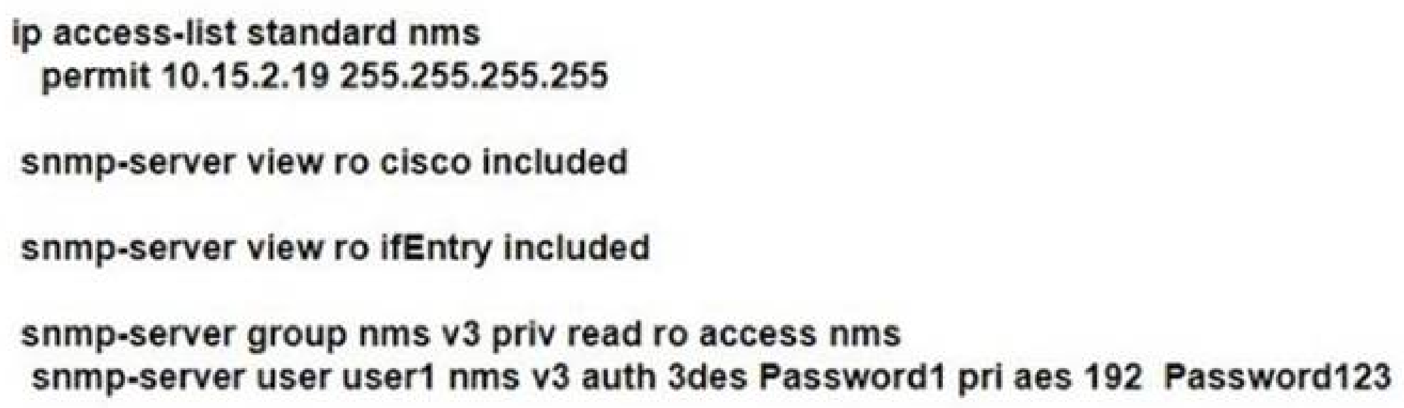
Answer: B

NEW QUESTION 422
- (Topic 4)
When is GLBP preferred over HSRP?

A. When encrypted helm are required between gateways h a single group.
B. When the traffic load needs to be shared between multiple gateways using a single virtual IP.
C. When the gateway routers are a mix of Cisco and non-Cisco routers
D. When clients need the gateway MAC address lo Be the same between multiple gateways

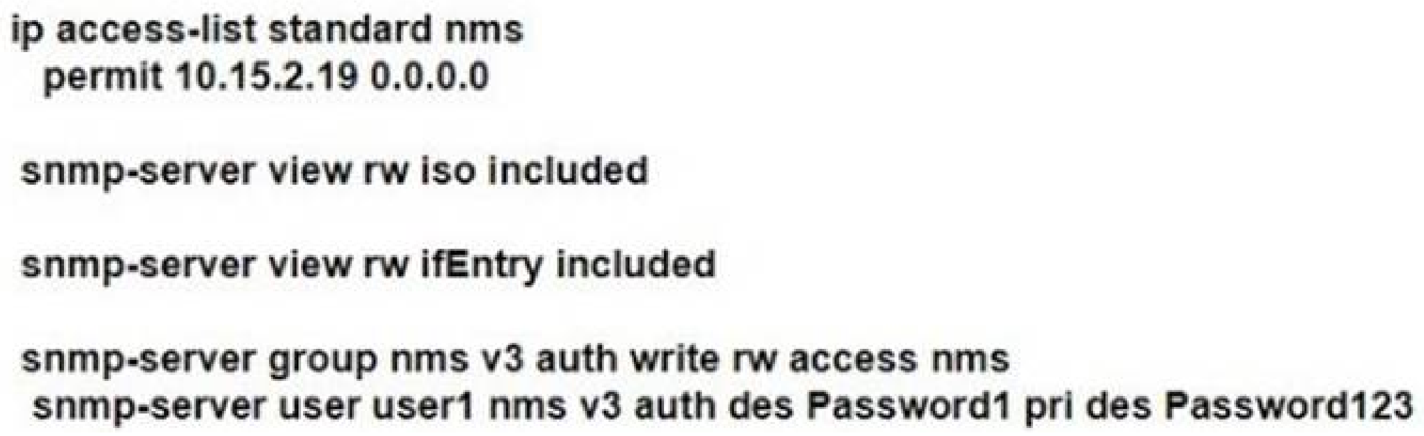
Answer: B

NEW QUESTION 427
- (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)



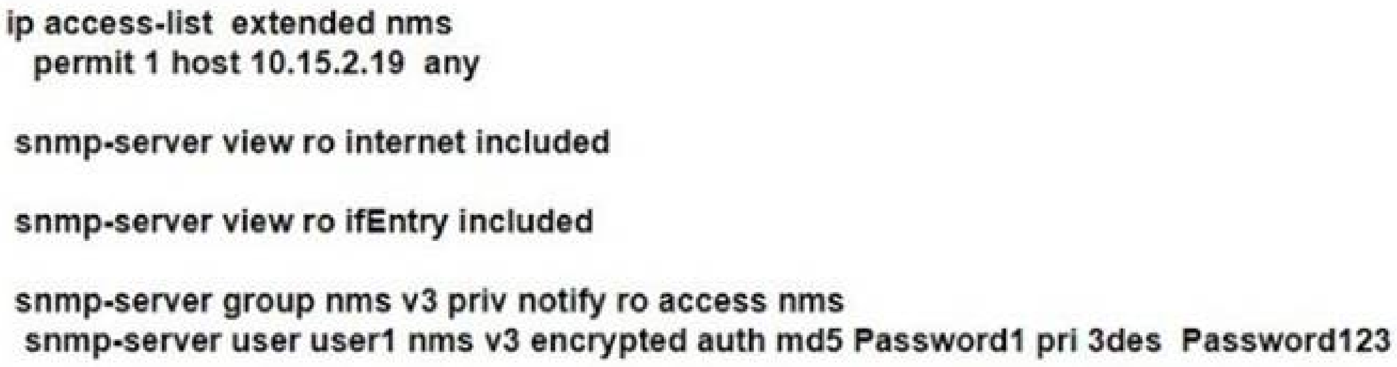
```
ip access-list standard nms
  permit 10.15.2.19 255.255.255.255

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)



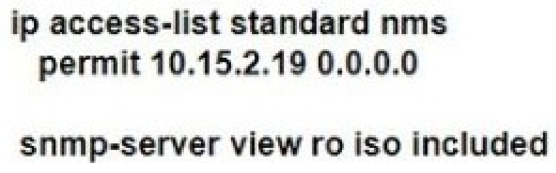
```
ip access-list standard nms
  permit 10.15.2.19 0.0.0.0

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)



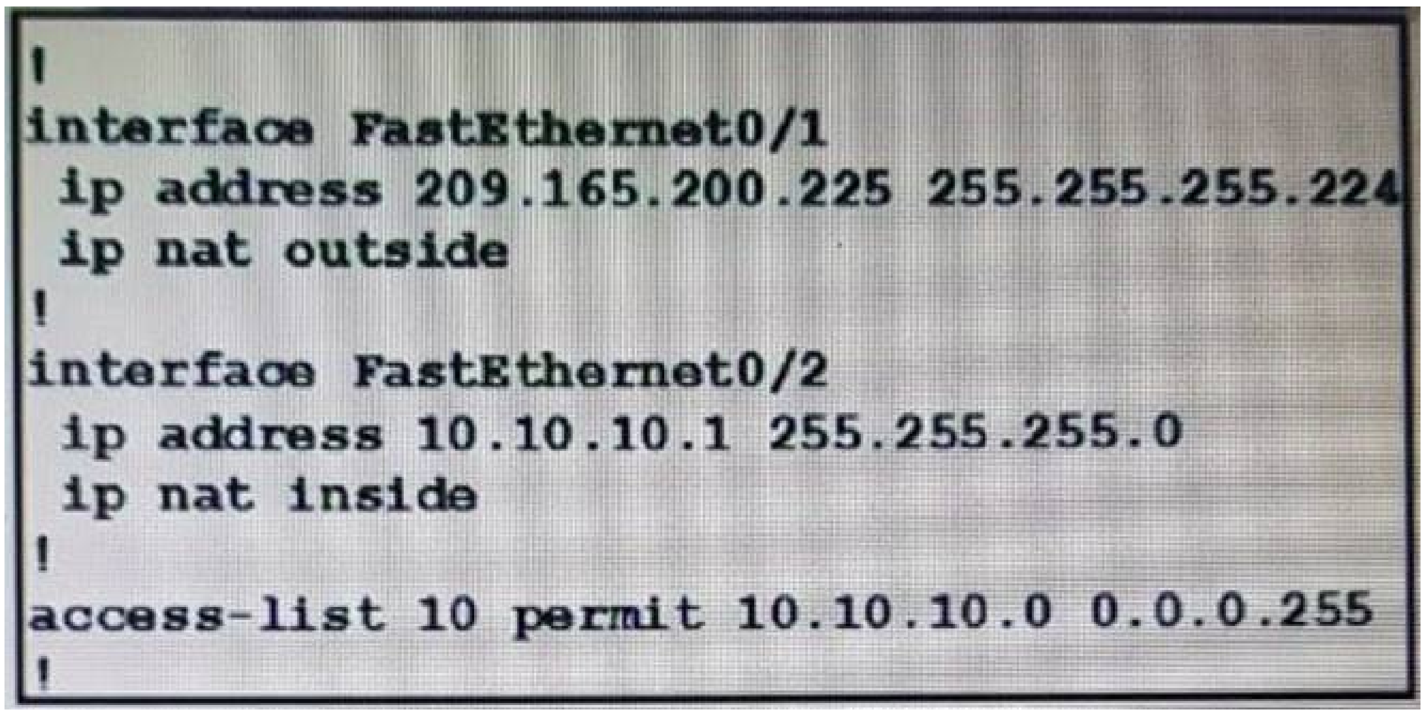
```
ip access-list standard nms
  permit 10.15.2.19 0.0.0.0

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 431
- (Topic 4)



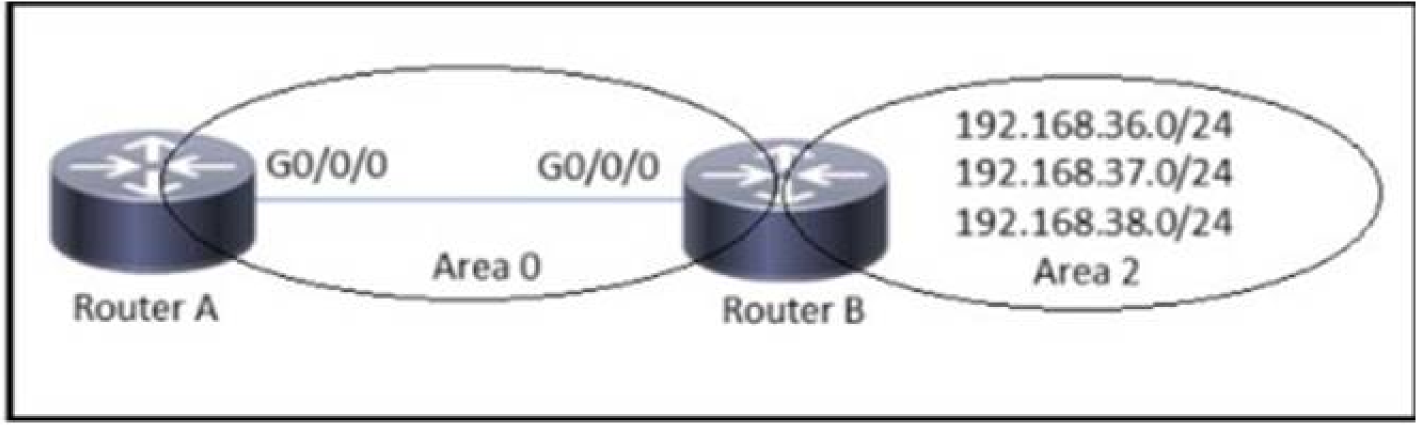
```
!
interface FastEthernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
!
interface FastEthernet0/2
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
access-list 10 permit 10.10.10.0 0.0.0.255
!
```

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

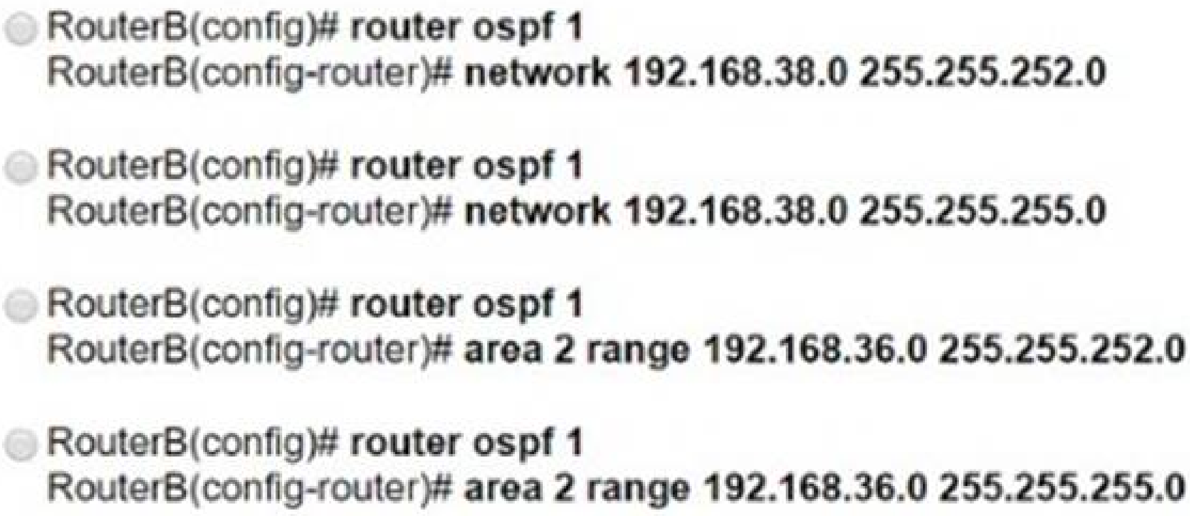
A. ip nat inside source list 10 interface FastEthernet0/1 overload
B. ip nat inside source list 10 interface FastEthernet0/2 overload
C. ip nat outside source list 10 interface FastEthernet0/2 overload
D. ip nat outside source static 209.165.200.225 10.10.10.0 overload

Answer: A

NEW QUESTION 433
- (Topic 4)



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



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

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

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

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

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

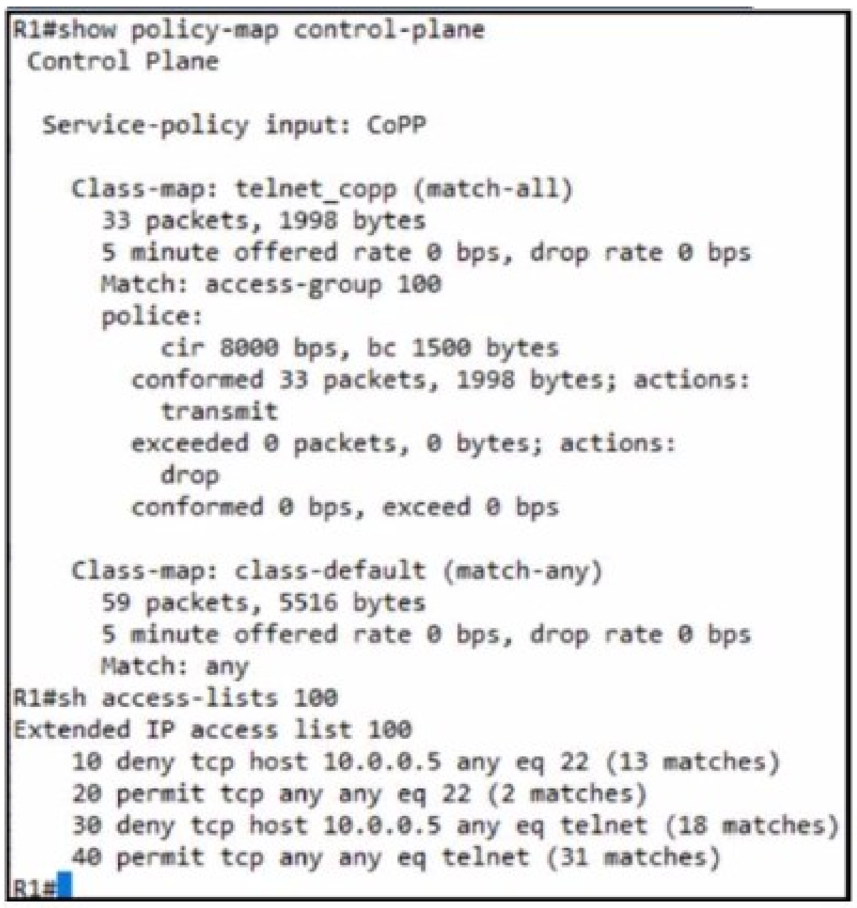
Answer: C

NEW QUESTION 435
- (Topic 4)
Which tool is used in Cisco DNA Center to build generic configurations that are able to be applied on device with similar network settings?

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

Answer: B

NEW QUESTION 438
- (Topic 4)
Refer to the exhibit.



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

  Service-policy input: CoPP

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

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

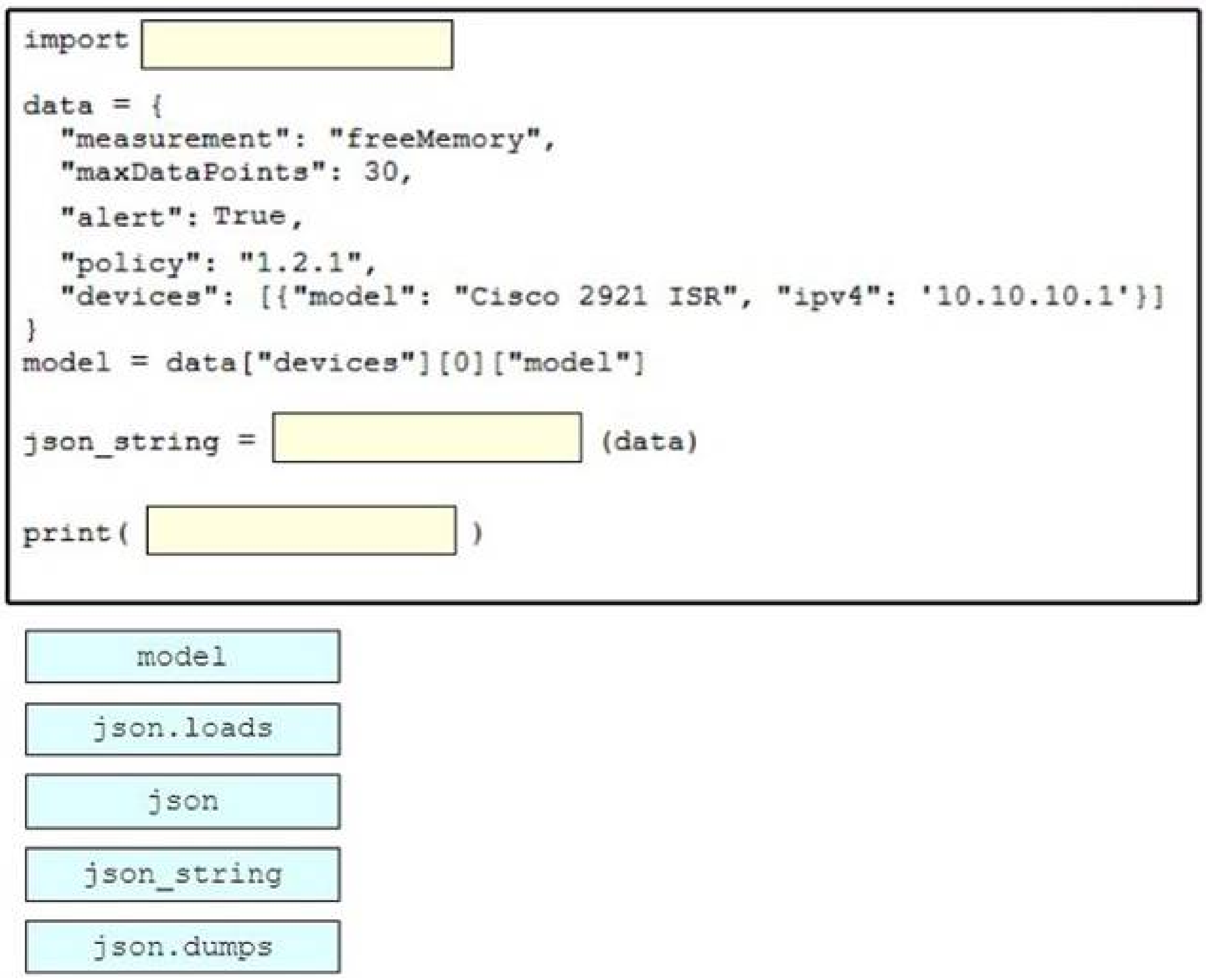
Which result Is achieved by the CoPP configuration?

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

Answer: C

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

NEW QUESTION 439
DRAG DROP - (Topic 4)
Drag and drop the code snippets from the bottom onto the blanks in the Python script to convert a Python object into a JSON string. Not all options are used.



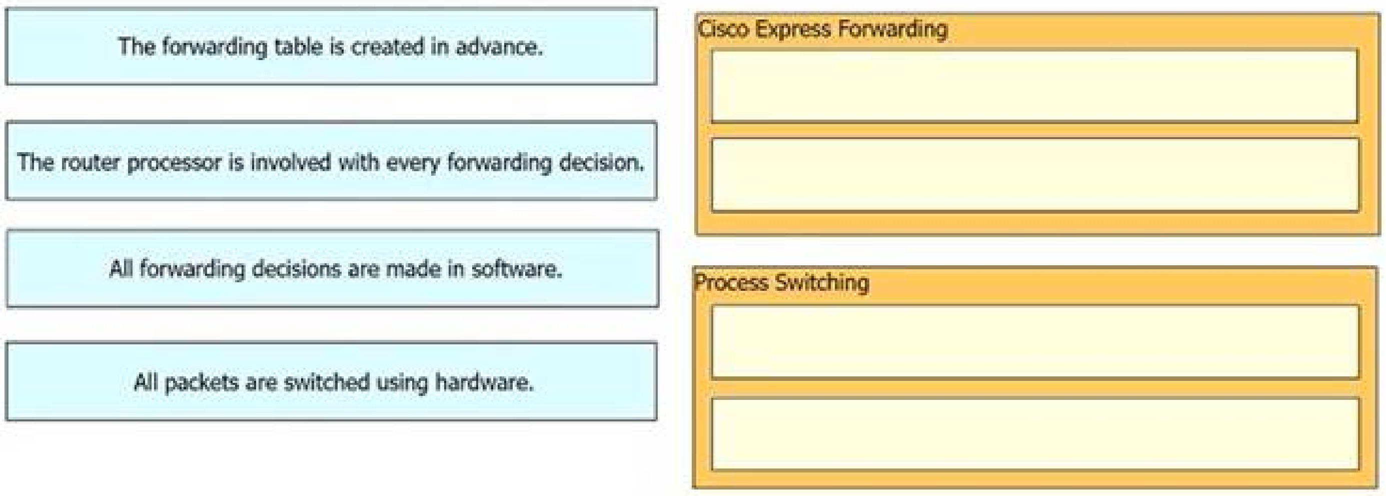
```
import

data = {
   "measurement": "freeMemory",
   "maxDataPoints": 30,
   "alert": True,
   "policy": "1.2.1",
   "devices": [{"model": "Cisco 2921 ISR", "ipv4": '10.10.10.1'}]
}
model = data["devices"][0]["model"]

json_string =                  (data)

print(                  )
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://stackoverflow.com/questions/45834577/turn-python-object-into-json-output

NEW QUESTION 442
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the switching mechanisms they describe on the right.



The forwarding table is created in advance.

The router processor is involved with every forwarding decision.

All forwarding decisions are made in software.

All packets are switched using hardware.

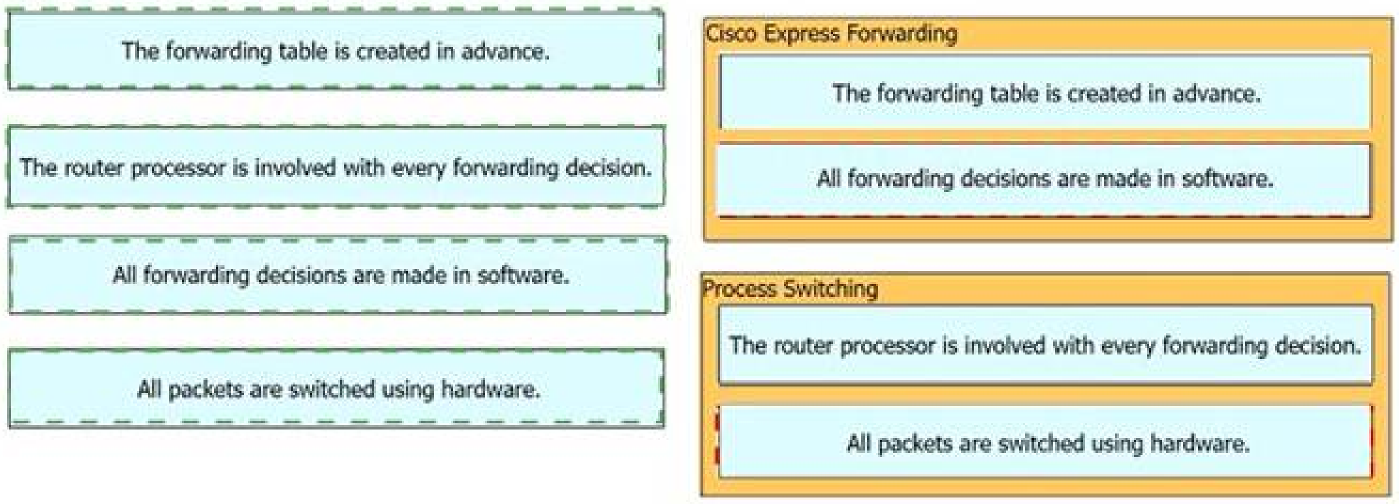
Cisco Express Forwarding

Process Switching

A. Mastered
B. Not Mastered

Answer: A

Explanation:



The forwarding table is created in advance.

The router processor is involved with every forwarding decision.

All forwarding decisions are made in software.

All packets are switched using hardware.

Cisco Express Forwarding

The forwarding table is created in advance.

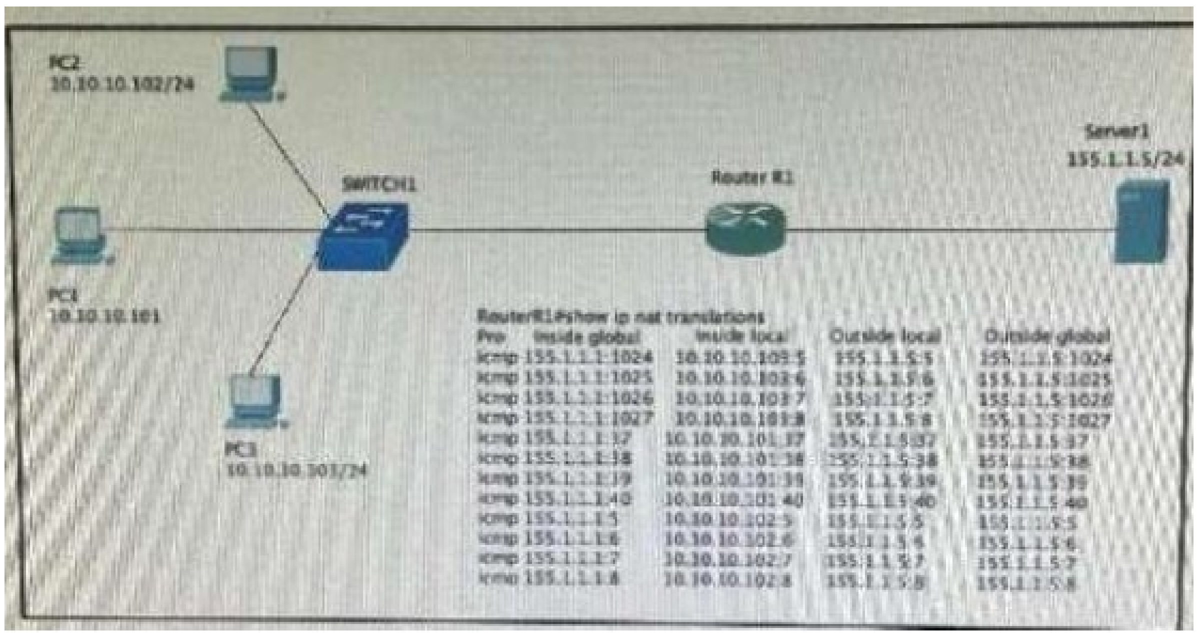
All forwarding decisions are made in software.

Process Switching

The router processor is involved with every forwarding decision.

All packets are switched using hardware.

NEW QUESTION 447
- (Topic 4)
Refer to the exhibit.



```
RouterR1#show ip nat translations
Pro  Inside global        Inside local         Outside local      Outside global
icmp 155.1.1.1:1024      10.10.10.103:5       155.1.1.5:5        155.1.1.5:1024
icmp 155.1.1.1:1025      10.10.10.103:6       155.1.1.5:6        155.1.1.5:1025
icmp 155.1.1.1:1026      10.10.10.103:7       155.1.1.5:7        155.1.1.5:1026
icmp 155.1.1.1:1027      10.10.10.103:8       155.1.1.5:8        155.1.1.5:1027
icmp 155.1.1.1:37       10.10.10.101:37      155.1.1.5:37       155.1.1.5:37
icmp 155.1.1.1:38       10.10.10.101:38      155.1.1.5:38       155.1.1.5:38
icmp 155.1.1.1:39       10.10.10.101:39      155.1.1.5:39       155.1.1.5:39
icmp 155.1.1.1:40       10.10.10.101:40      155.1.1.5:40       155.1.1.5:40
icmp 155.1.1.1:5        10.10.10.102:5       155.1.1.5:5        155.1.1.5:5
icmp 155.1.1.1:6        10.10.10.102:6       155.1.1.5:6        155.1.1.5:6
icmp 155.1.1.1:7        10.10.10.102:7       155.1.1.5:7        155.1.1.5:7
icmp 155.1.1.1:8        10.10.10.102:8       155.1.1.5:8        155.1.1.5:8
```

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

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

Answer: A

NEW QUESTION 450
- (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

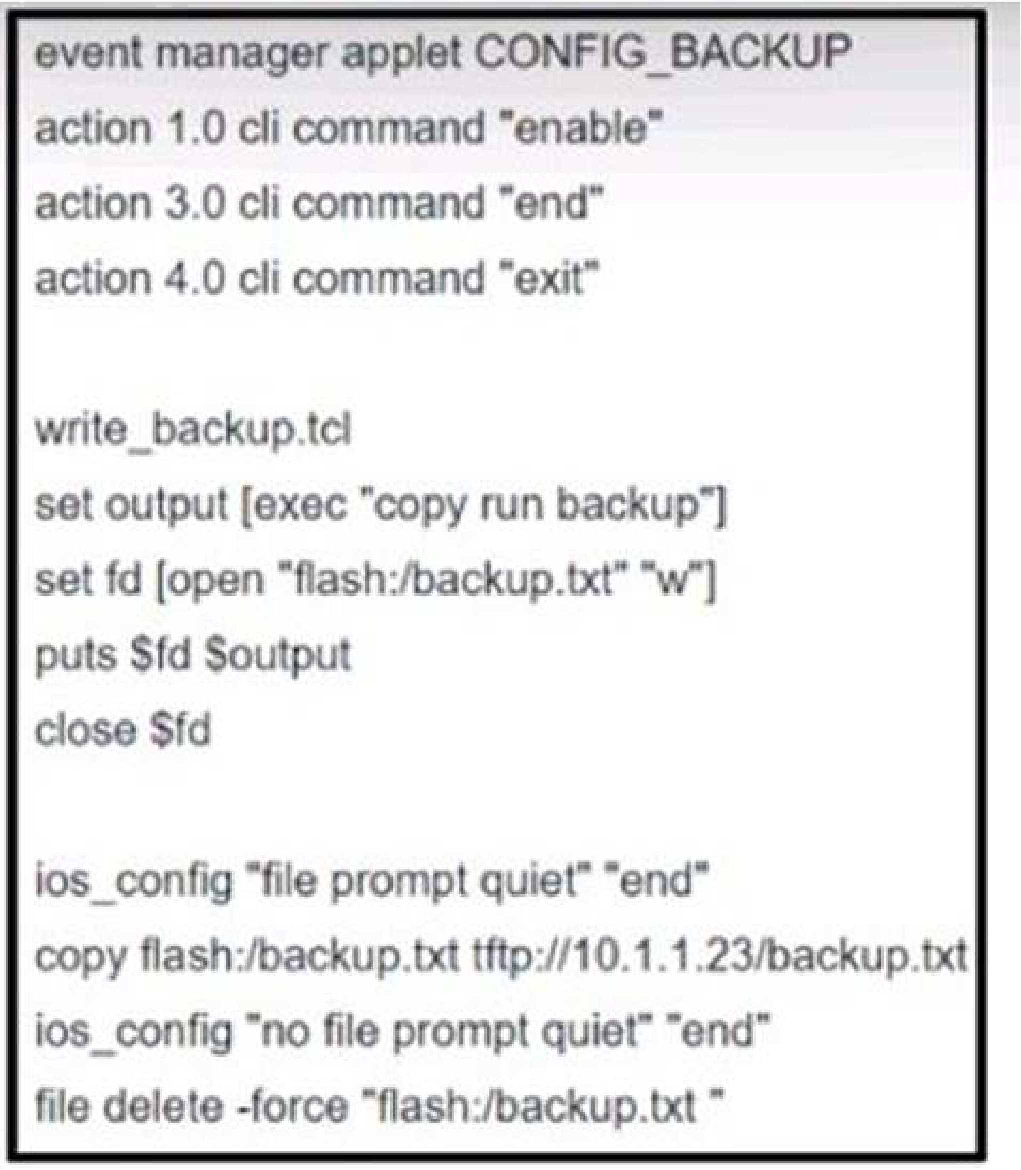
Explanation:
This is because VXLAN is a network virtualization technology that encapsulates Layer 2 frames in UDP headers and allows them to be transported over Layer 3 networks. VXLAN is used in Cisco SD-Access to create virtual networks that span across multiple physical locations and devices. VXLAN 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 452
- (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 454
- (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 "
```

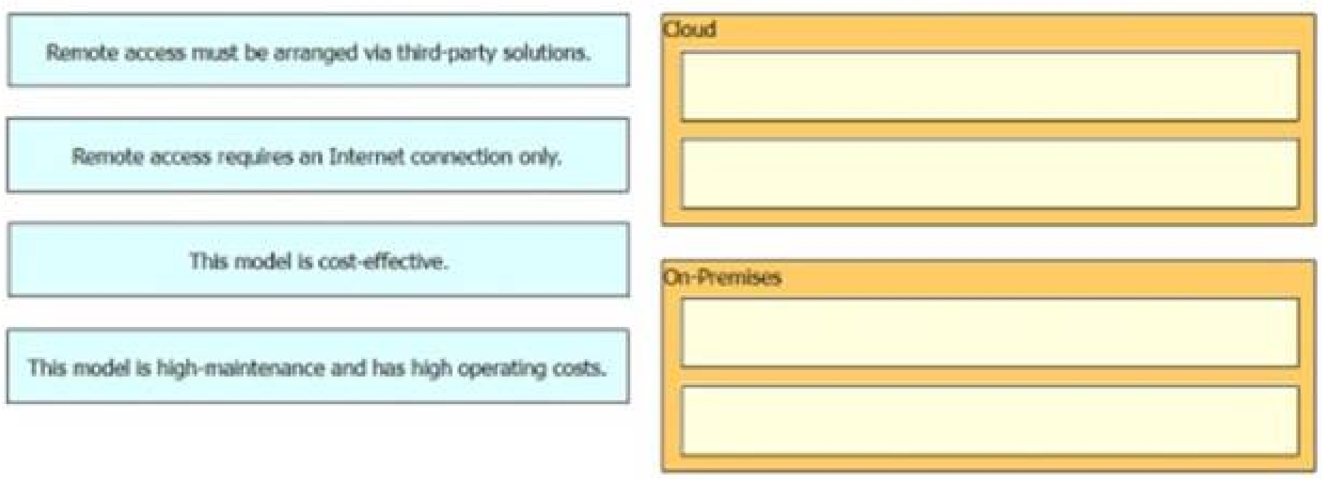
Which statement is needed to complete the EEM applet and use the Tel script to store the backup file?

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 459
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.

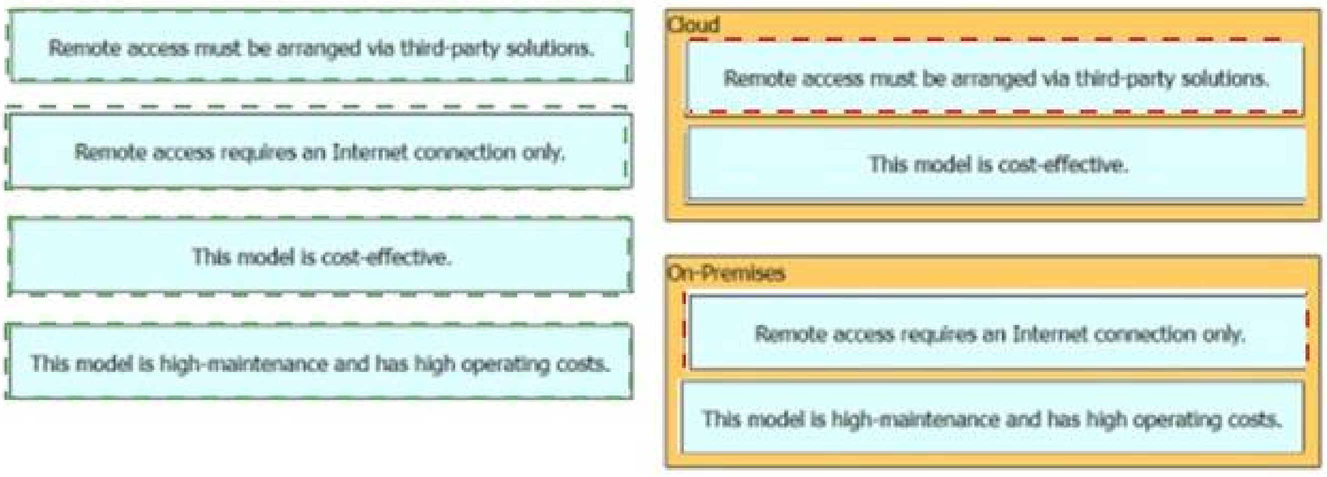
Cloud

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.

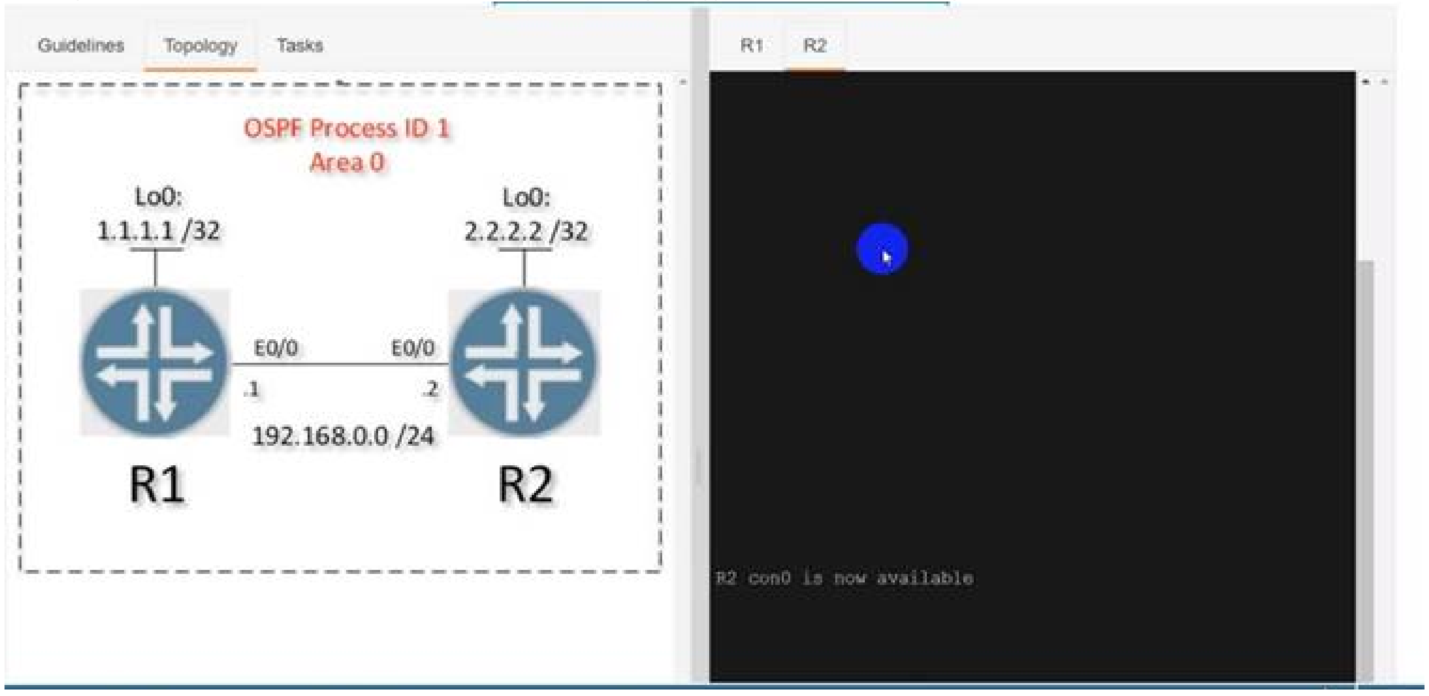
This model is cost-effective.

On-Premises

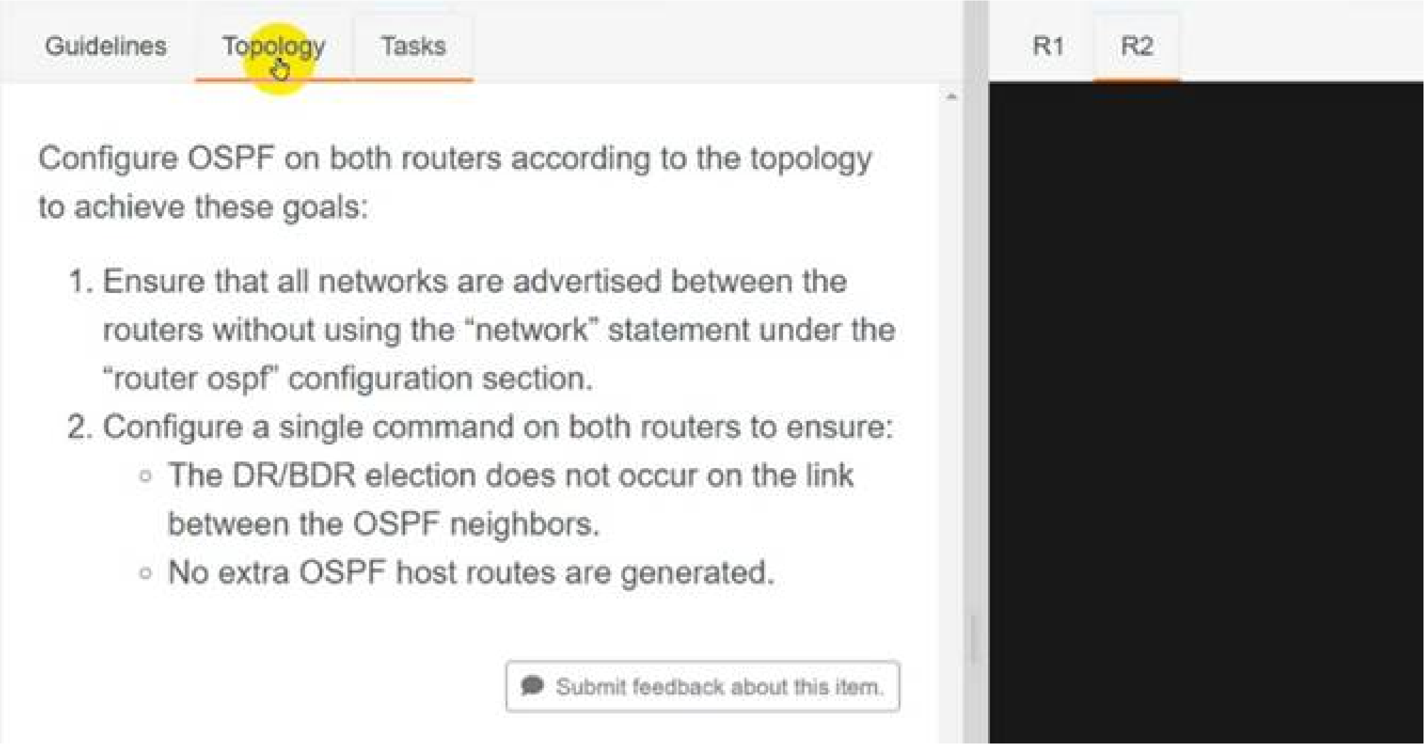
Remote access requires an Internet connection only.

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

NEW QUESTION 462
SIMULATION - (Topic 4)
Simulation 04
Configure OSPF on both routers according to the topology to achieve these goals:



```
R2 con0 is now available
```



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

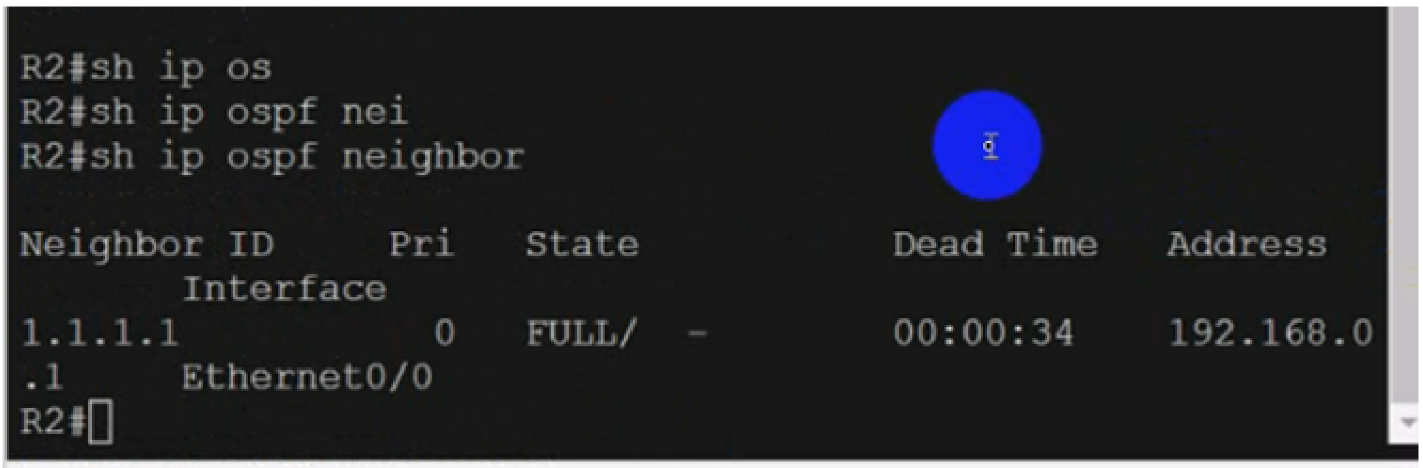
1. Ensure that all networks are advertised between the routers without using the “network” statement under the “router ospf” configuration section.
2. Configure a single command on both routers to ensure:
   - The DR/BDR election does not occur on the link between the OSPF neighbors.
   - No extra OSPF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

A. Mastered
B. Not Mastered

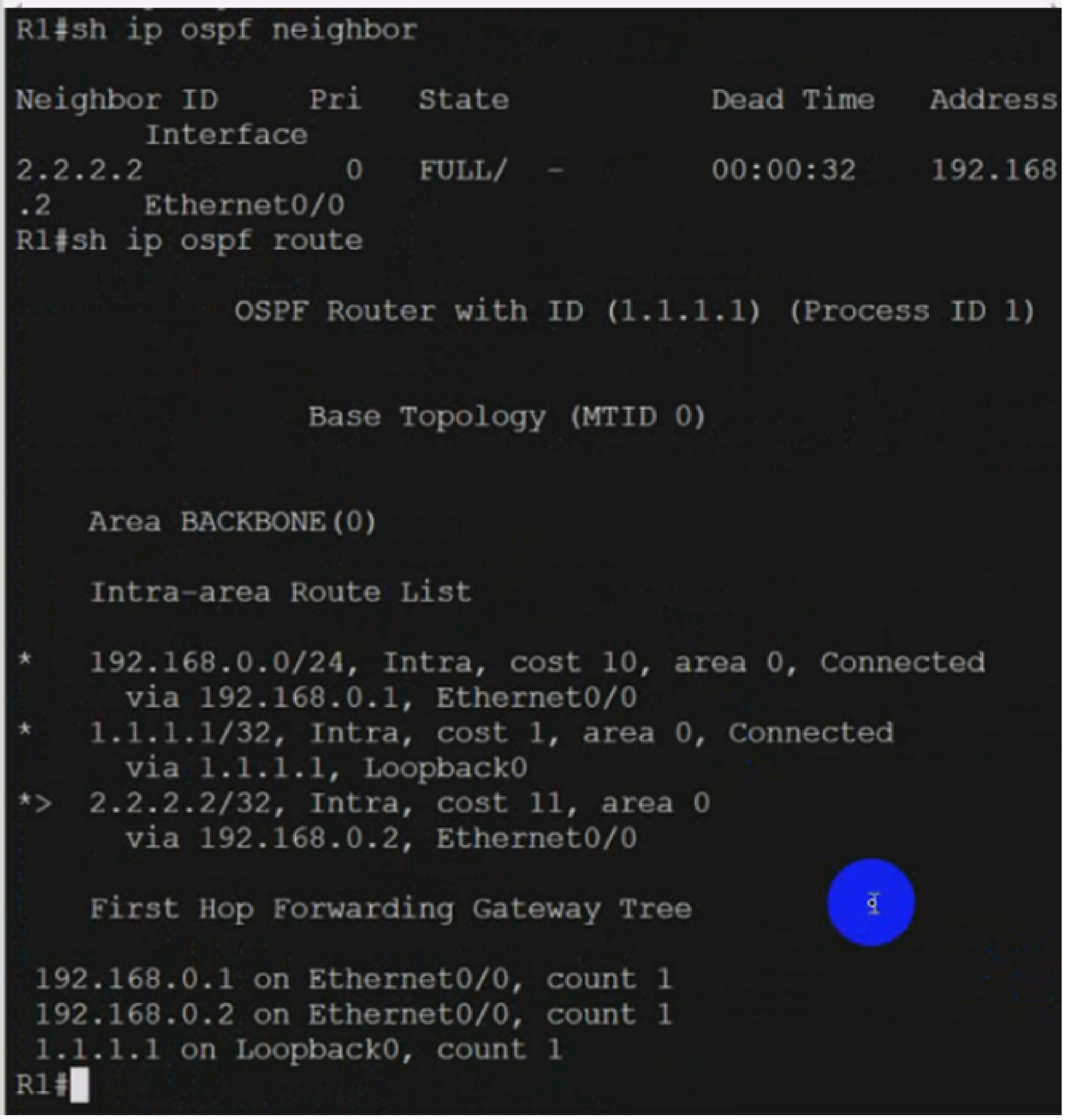
Answer: A

Explanation:

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

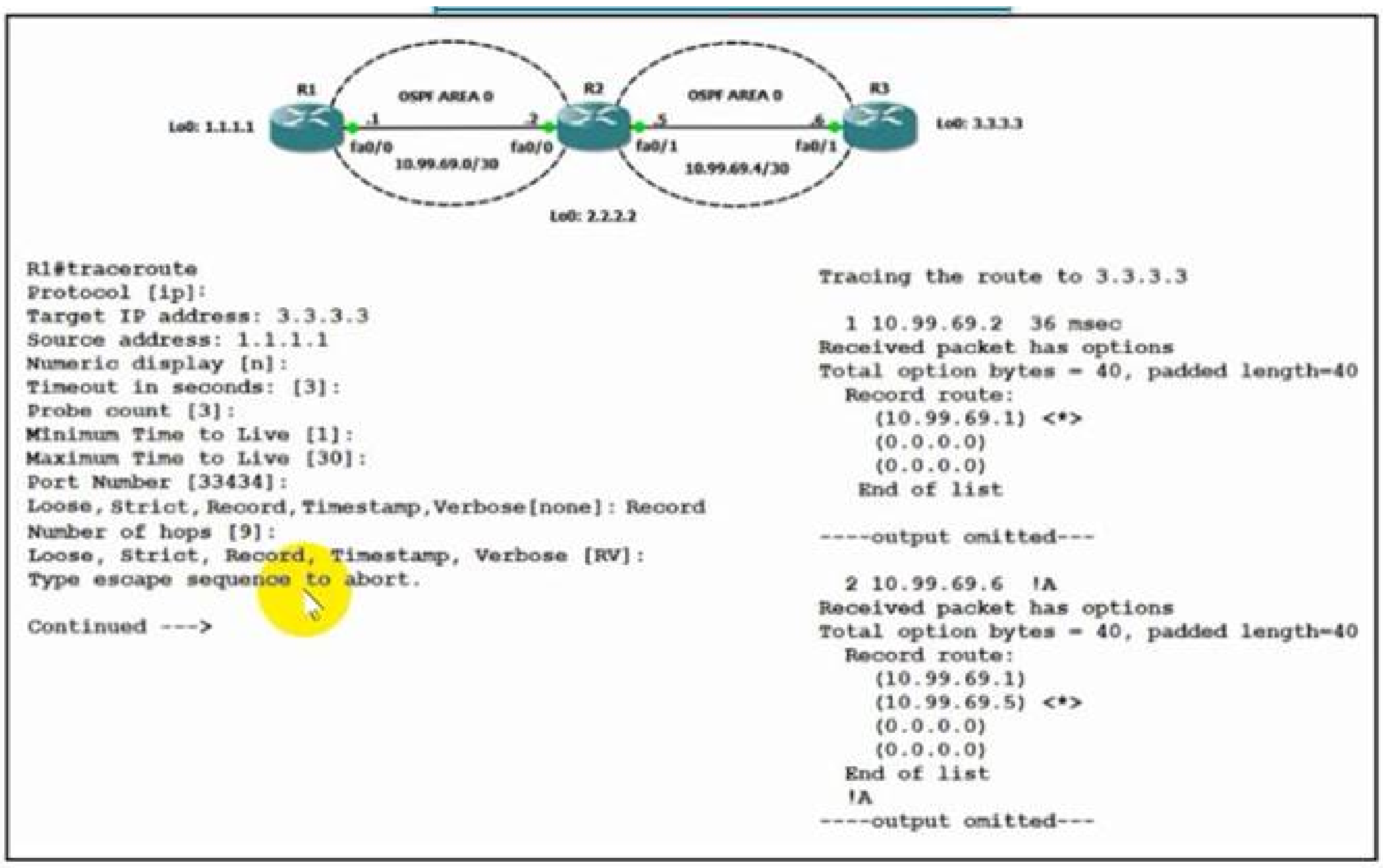


```
R2#sh ip os
R2#sh ip ospf nei
R2#sh ip ospf neighbor

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



```
R1#sh ip ospf neighbor

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

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


                Base Topology (MTID 0)


    Area BACKBONE(0)

    Intra-area Route List

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

    First Hop Forwarding Gateway Tree

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

NEW QUESTION 464
- (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 --->
```

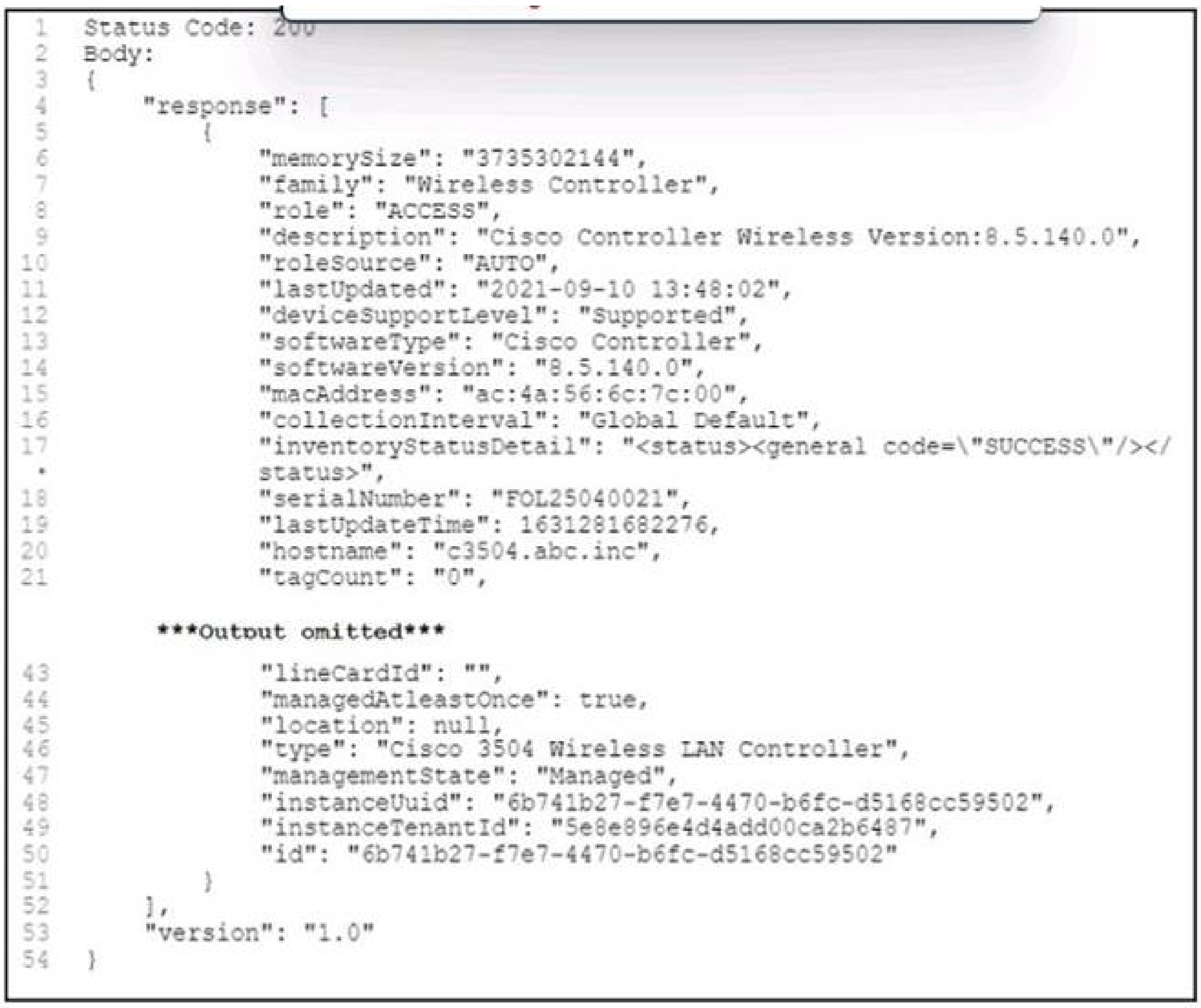
```
Tracing the route to 3.3.3.3

  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 465
- (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 467
- (Topic 4)
Which function is performed by vSmart in the Cisco SD-WAN architecture?

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

Answer: B

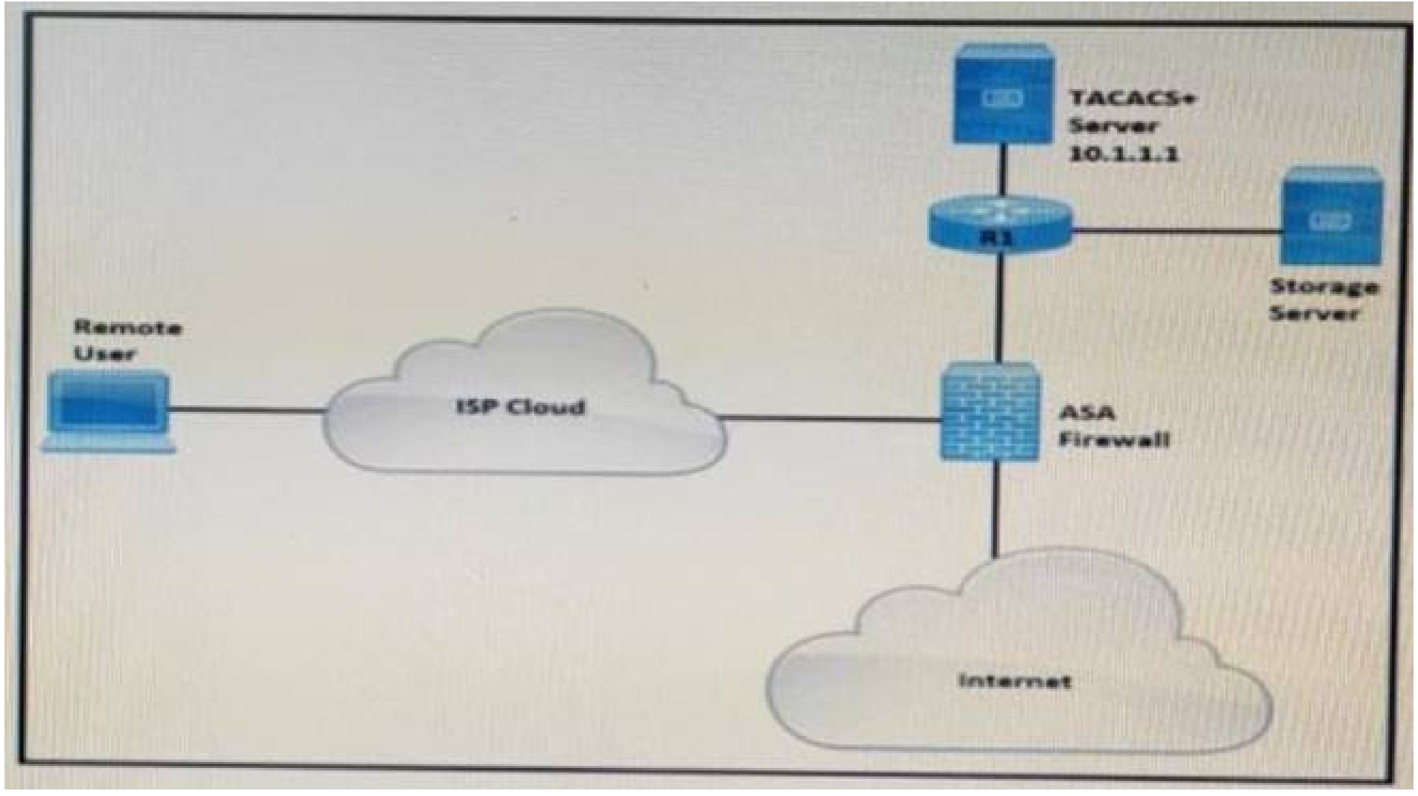
NEW QUESTION 470
- (Topic 4)
Which of the following attacks becomes more effective because of global leakages of users' passwords?

A. Dictionary
B. Brute-force
C. Phishing
D. Deauthentication

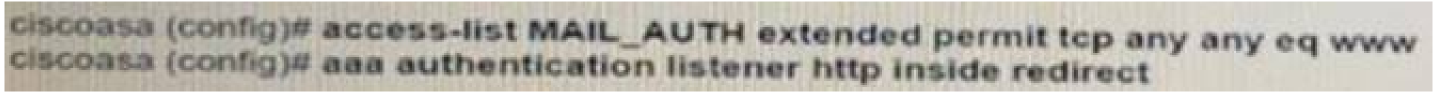
Answer: A

Explanation:
This is because a dictionary attack is a type of password cracking attack that uses a list of common or previously leaked passwords to guess the credentials of a user. A dictionary attack becomes more effective because of global leakages of users' passwords, as the attacker can use the leaked passwords as a source for the dictionary. The source of this answer is the Cisco ENCOR v1.1 course, module 2, lesson 2.3: Implementing Wireless Security.

NEW QUESTION 471
- (Topic 4)

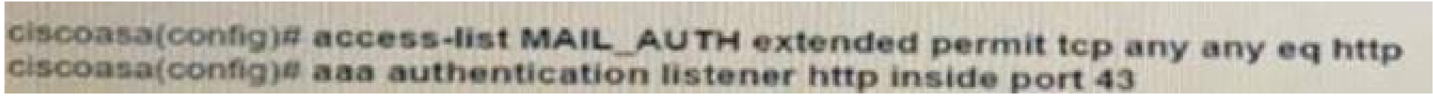


Refer to the exhibit Remote users cannot access the Internet but can upload files to the storage server Which configuration must be applied to allow Internet access?
A)



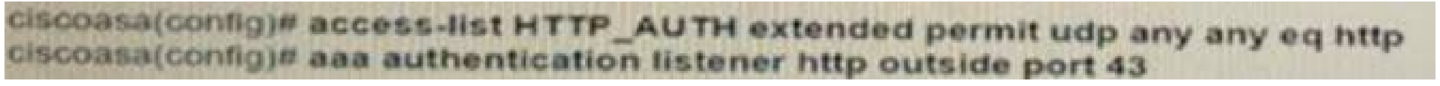
```
ciscoasa (config)# access-list MAIL_AUTH extended permit tcp any any eq www
ciscoasa (config)# aaa authentication listener http inside redirect
```

B)



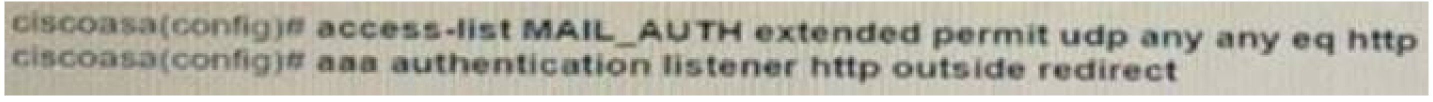
```
ciscoasa(config)# access-list MAIL_AUTH extended permit tcp any any eq http
ciscoasa(config)# aaa authentication listener http inside port 43
```

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

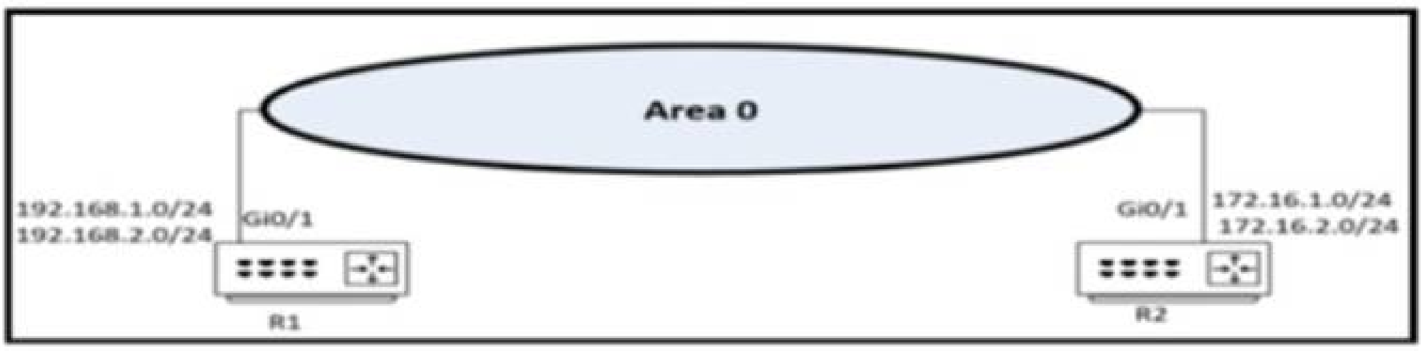
Answer: A

NEW QUESTION 476
- (Topic 4)
Which LISP component decapsulates messages and forwards them to the map server responsible for the egress tunnel routers?

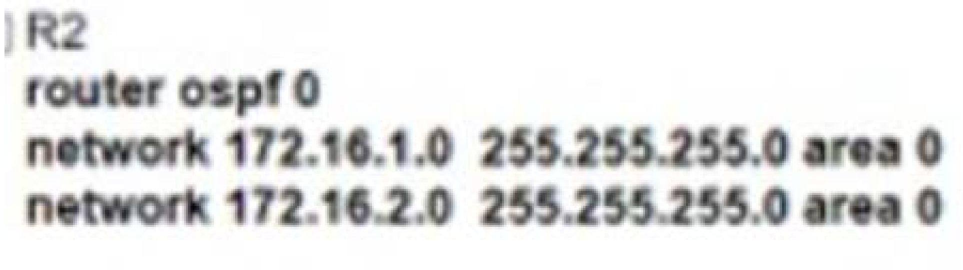
A. Ingress Tunnel Router
B. Map Resolver
C. Proxy ETR
D. Router Locator

Answer: B

NEW QUESTION 477
- (Topic 4)

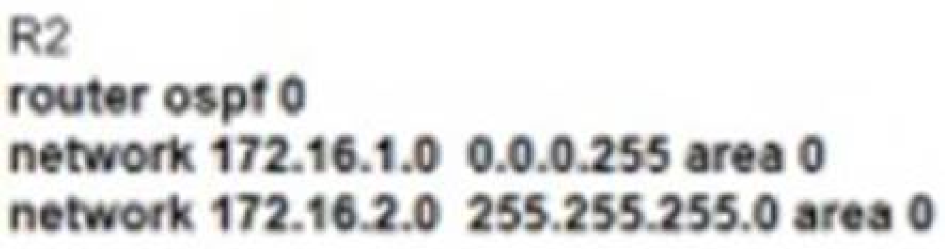


Refer to the exhibit. Which two configurations enable R1 and R2 to advertise routes into OSPF? (Choose two)
A)



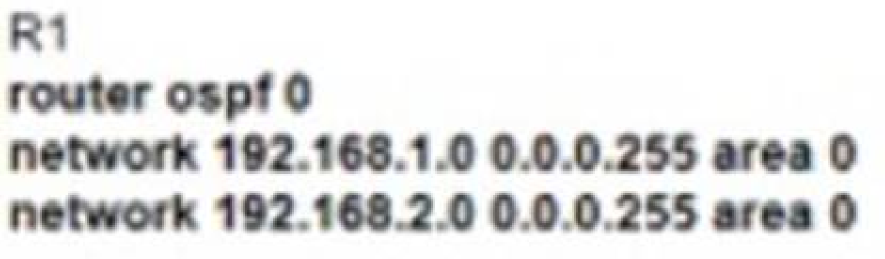
```
R2
router ospf 0
network 172.16.1.0  255.255.255.0 area 0
network 172.16.2.0  255.255.255.0 area 0
```

B)



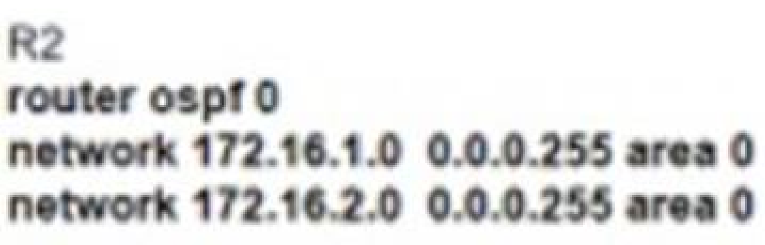
```
R2
router ospf 0
network 172.16.1.0  0.0.0.255 area 0
network 172.16.2.0  255.255.255.0 area 0
```

C)



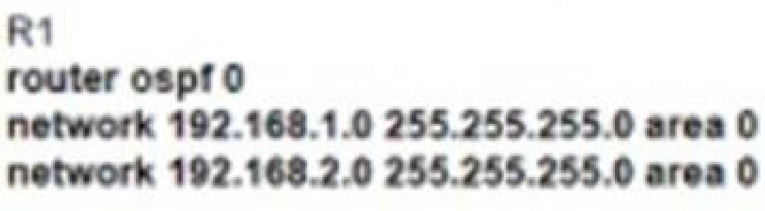
```
R1
router ospf 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
```

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

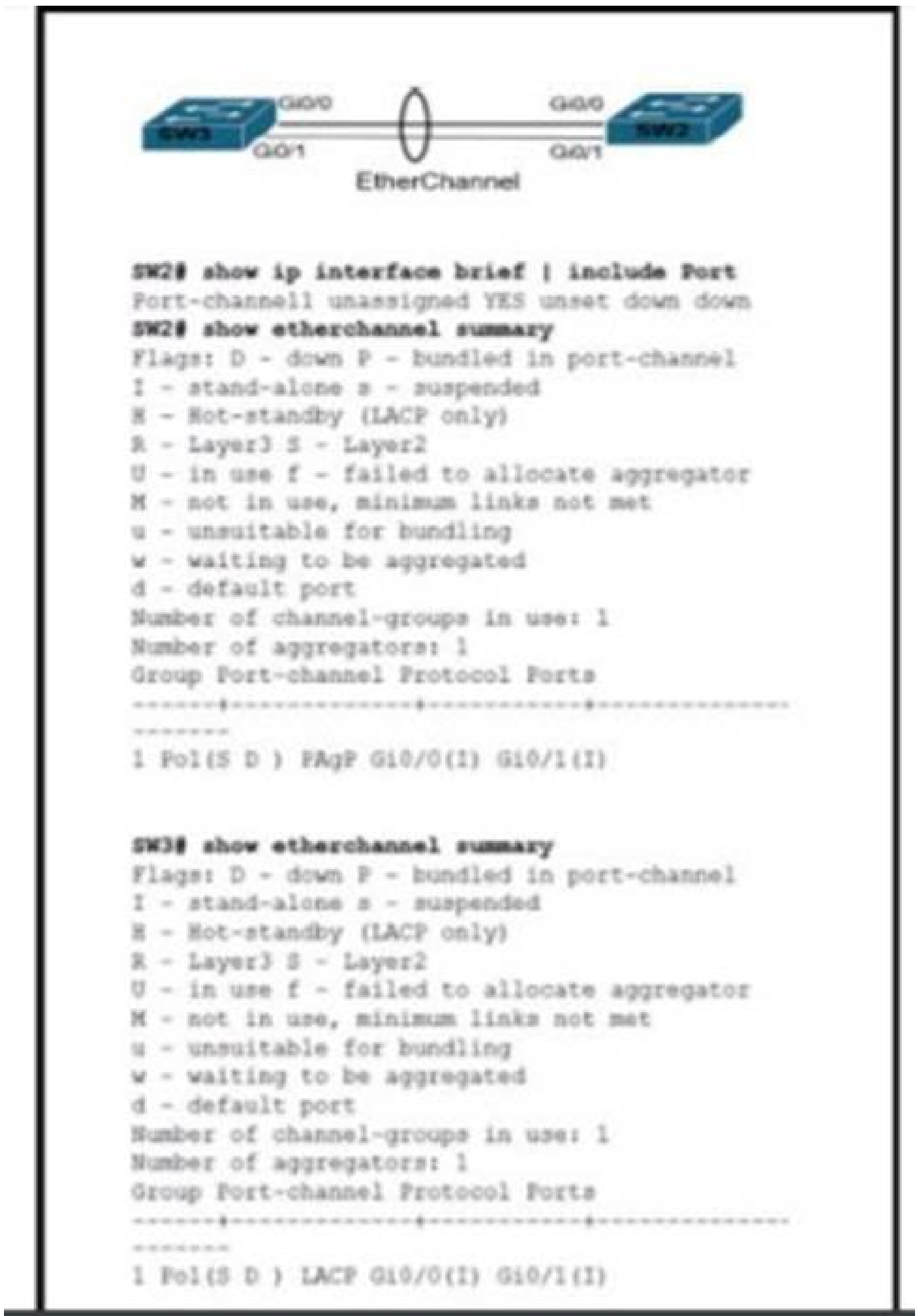
Answer: CD

NEW QUESTION 481
- (Topic 4)
What is a characteristic of a Type 2 hypervisor?

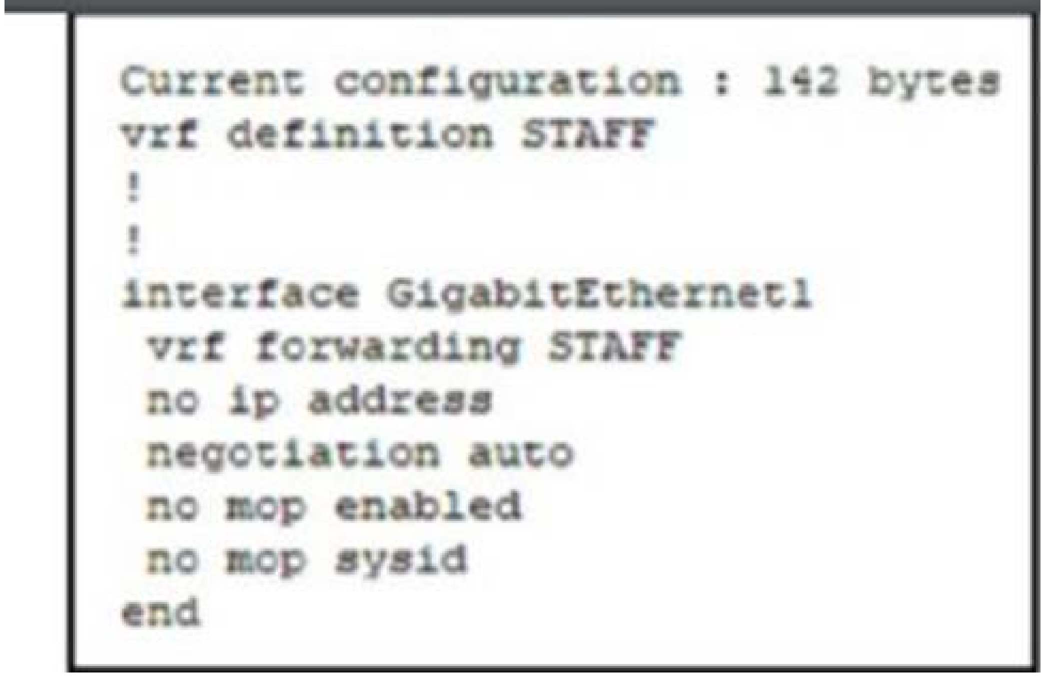
A. It eliminates the need for an underlying operating system.
B. Its main task is to manage hardware resources between different operating systems
C. Problems in the base operating system can affect the entire system.
D. It is completely independent of the operating system

Answer: C

NEW QUESTION 483
- (Topic 4)
Refer to the exhibit.



```
SW2# show ip interface brief | include Port
Port-channel1 unassigned YES unset down down
SW2# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+---------------
-------
1 Po1(S D ) 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 Po1(S D ) LACP Gi0/0(I) Gi0/1(I)
```



```
Current configuration : 142 bytes
vrf definition STAFF
!
!
interface GigabitEthernet1
 vrf forwarding STAFF
 no ip address
 negotiation auto
 no mop enabled
 no mop sysid
end
```

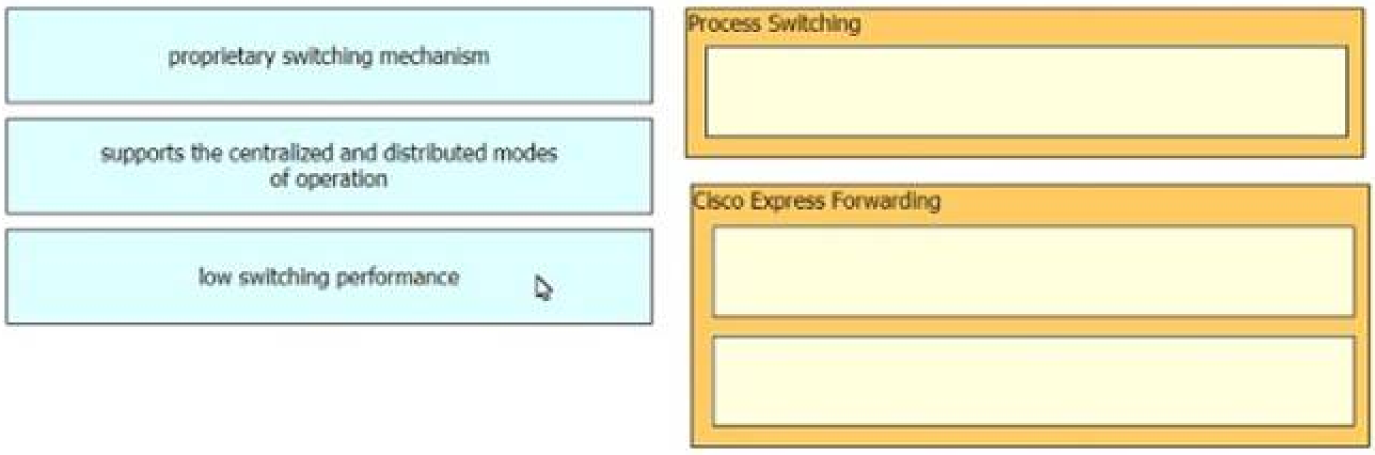
An engineer must assign an IP address of 192.168.1.1/24 to the GigabitEtherenet1 interface. Which two commands must be added to the existing configuration to accomplish this task? (Choose two.)

A. Router(config-vrf)#ip address 192.168.1.1 255.255.255.0
B. Router(config-vrf)#address-family ipv4

C. Router(config-if)#address-family ipv4
D. Router(config-vrf)#address-family ipv6
E. Router(config-if)#ip address 192.168.1.1 255.255.255.0

Answer: BE

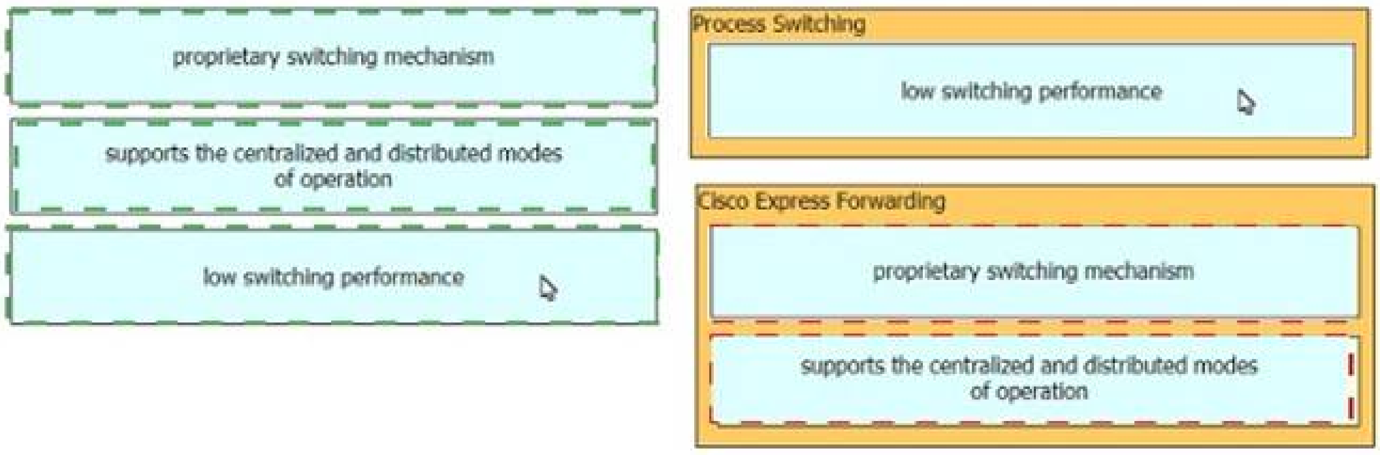
NEW QUESTION 488
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the switching architectures on the right.


proprietary switching mechanism
supports the centralized and distributed modes of operation
low switching performance
Process Switching
Cisco Express Forwarding

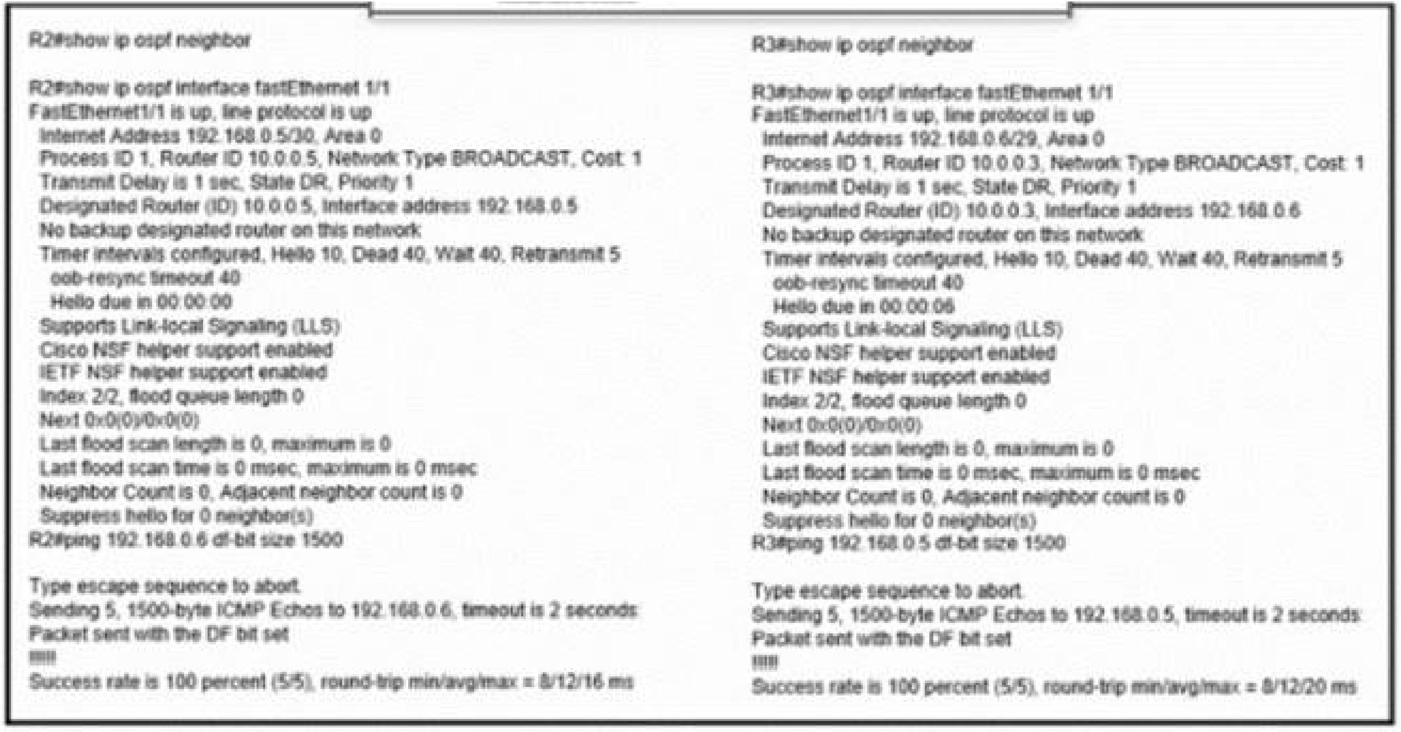
A. Mastered
B. Not Mastered

Answer: A

Explanation:


proprietary switching mechanism
supports the centralized and distributed modes of operation
low switching performance
Process Switching
low switching performance
Cisco Express Forwarding
proprietary switching mechanism
supports the centralized and distributed modes of operation

NEW QUESTION 492
- (Topic 4)



```
R2#show ip ospf neighbor

R2#show ip ospf interface fastEthernet 1/1
FastEthernet1/1 is up, line protocol is up
  Internet Address 192.168.0.5/30, Area 0
  Process ID 1, Router ID 10.0.0.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.0.0.5, Interface address 192.168.0.5
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R2#ping 192.168.0.6 df-bit size 1500

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 192.168.0.6, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/16 ms
```

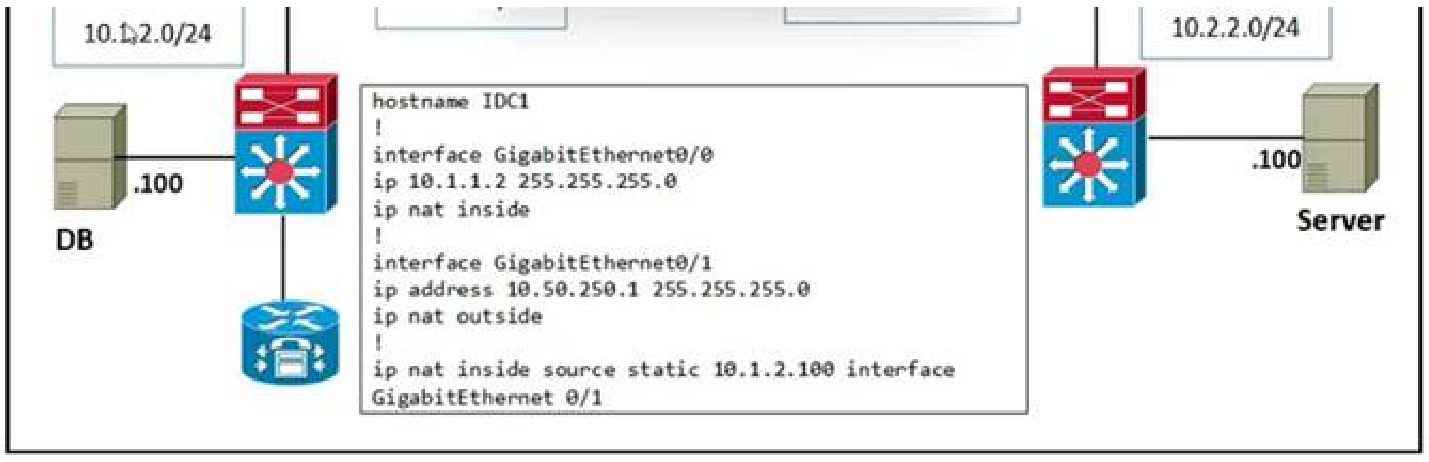
```
R3#show ip ospf neighbor

R3#show ip ospf interface fastEthernet 1/1
FastEthernet1/1 is up, line protocol is up
  Internet Address 192.168.0.6/29, Area 0
  Process ID 1, Router ID 10.0.0.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.0.0.3, Interface address 192.168.0.6
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R3#ping 192.168.0.5 df-bit size 1500

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 192.168.0.5, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/20 ms
```

Refer to the exhibit.
Why does the OSPF neighborship fail between the two interfaces?

A. The IP subnet mask is not the same.
B. There is a mismatch in the OSPF interface network type.
C. The OSPF timers are different.
D. The MTU is nor the same.

Answer: A

NEW QUESTION 494
- (Topic 4)
Refer to the exhibit.



```
hostname IDC1
!
interface GigabitEthernet0/0
ip 10.1.1.2 255.255.255.0
ip nat inside
!
interface GigabitEthernet0/1
ip address 10.50.250.1 255.255.255.0
ip nat outside
!
ip nat inside source static 10.1.2.100 interface
GigabitEthernet 0/1
```

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

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

Answer: C

NEW QUESTION 498
- (Topic 2)
What does the Cisco DNA Center use to enable the delivery of applications through a network and to yield analytics for innovation?

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

Answer: C

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

NEW QUESTION 500
- (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 501
- (Topic 2)
An engineer must create a new SSID on a Cisco 9800 wireless LAN controller. The client has asked to use a pre-shared key for authentication Which profile must the engineer edit to achieve this requirement?

A. RF
B. Policy
C. WLAN
D. Flex

Answer: B

Explanation:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116880-config-wpa2-psk-00.html

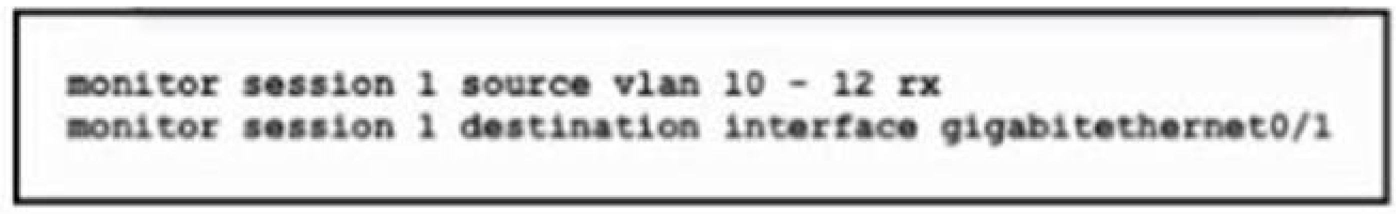
NEW QUESTION 504
- (Topic 2)
What is the function of cisco DNA center in a cisco SD-access deployment?

A. It is responsible for routing decisions inside the fabric
B. It is responsible for the design, management, deployment, provisioning and assurance of the fabric network devices.

C. It possesses information about all endpoints, nodes and external networks related to the fabric
D. It provides integration and automation for all nonfabric nodes and their fabric counterparts.

Answer: B

NEW QUESTION 505
- (Topic 2)
Refer to the exhibit.



```
monitor session 1 source vlan 10 - 12 rx
monitor session 1 destination interface gigabitethernet0/1
```

An engineer must configure a SPAN session. What is the effect of the configuration?

A. Traffic sent on VLANs 10, 11, and 12 is copied and sent to interface g0/1.
B. Traffic sent on VLANs 10 and 12 only is copied and sent to interface g0/1.
C. Traffic received on VLANs 10, 11, and 12 is copied and sent to Interface g0/1.
D. Traffic received on VLANs 10 and 12 only is copied and sent to interface g0/1.

Answer: C

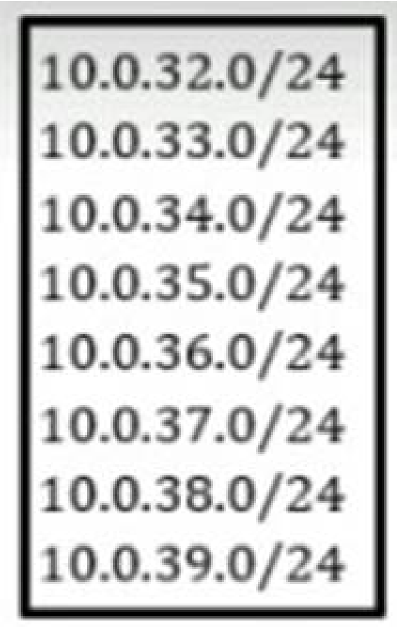
NEW QUESTION 510
- (Topic 2)
Which OSPF networks types are compatible and allow communication through the two peering devices?

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

Answer: A

Explanation:
The following different OSPF types are compatible with each other:
+ Broadcast and Non-Broadcast (adjust hello/dead timers)
+ Point-to-Point and Point-to-Multipoint (adjust hello/dead timers)
Broadcast and Non-Broadcast networks elect DR/BDR so they are compatible. Point- topoint/multipoint do not elect DR/BDR so they are compatible.

NEW QUESTION 512
- (Topic 2)
Refer to the exhibit.



10.0.32.0/24
10.0.33.0/24
10.0.34.0/24
10.0.35.0/24
10.0.36.0/24
10.0.37.0/24
10.0.38.0/24
10.0.39.0/24

An engineer must permit traffic from these networks and block all other traffic An informational log message should be triggered when traffic enters from these prefixes Which access list must be used?

A. access-list acl_subnets permit ip 10.0.32.0 0 0.0.255 log
B. access-list acl_subnets permit ip 10.0.32.0 0.0.7.255 log
C. access-list acl_subnets permit ip 10.0.32.0 0.0.7.255 access-list acl_subnets deny ip any log
D. access-list acl_subnets permit ip 10.0.32.0 255.255.248.0 log

Answer: B

NEW QUESTION 514
- (Topic 2)
An engineer is configuring local web authentication on a WLAN. The engineer chooses the Authentication radio button under the Layer 3 Security options for Web Policy. Which device presents the web authentication for the WLAN?

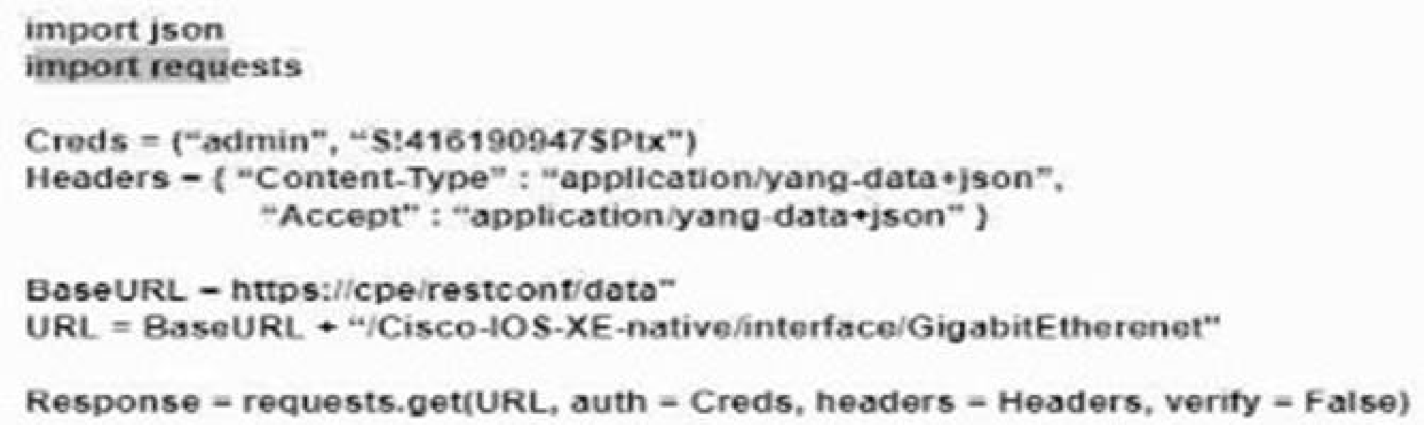
A. ISE server
B. local WLC

C. RADIUS server
D. anchor WLC

Answer: B

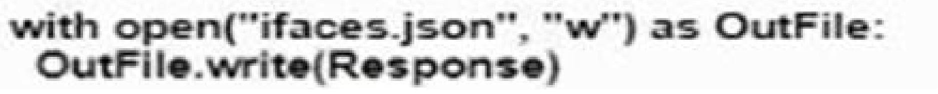
Explanation:
“The next step is to configure the WLC for the Internal web authentication. Internal web authentication is the defaultweb authentication type on WLCs.”
In step 4 of the link above, we will configure Security as described in this question. Therefore we can deduce thisconfiguration is for Internal web authentication.
This paragraph was taken from the link https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/69340-web-auth-config.html#c5 :

NEW QUESTION 517
- (Topic 2)
Which Python code snippet must be added to the script to save the returned configuration as a JSON-formatted file?



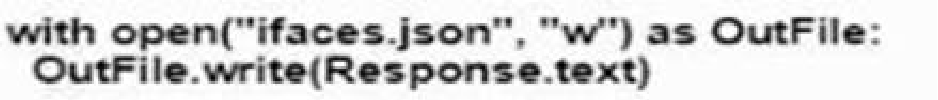
```
import json
import requests

Creds = (“admin”, “S!4161909475Ptx”)
Headers – { “Content-Type” : “application/yang-data+json”,
                    “Accept” : “application/yang-data+json” }

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

Response = requests.get(URL, auth = Creds, headers = Headers, verify = False)
```

A)



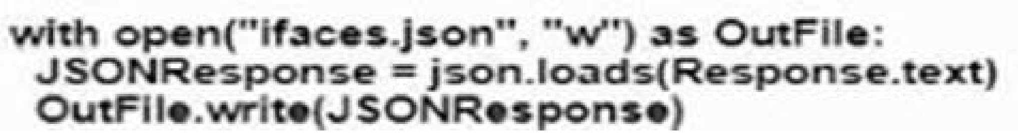
```
with open("ifaces.json", "w") as OutFile:
  OutFile.write(Response)
```

B)



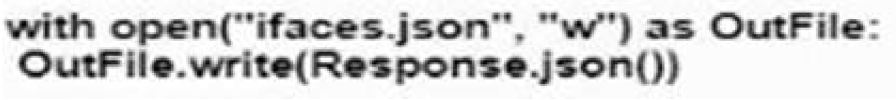
```
with open("ifaces.json", "w") as OutFile:
  OutFile.write(Response.text)
```

C)



```
with open("ifaces.json", "w") as OutFile:
  JSONResponse = json.loads(Response.text)
  OutFile.write(JSONResponse)
```

D)

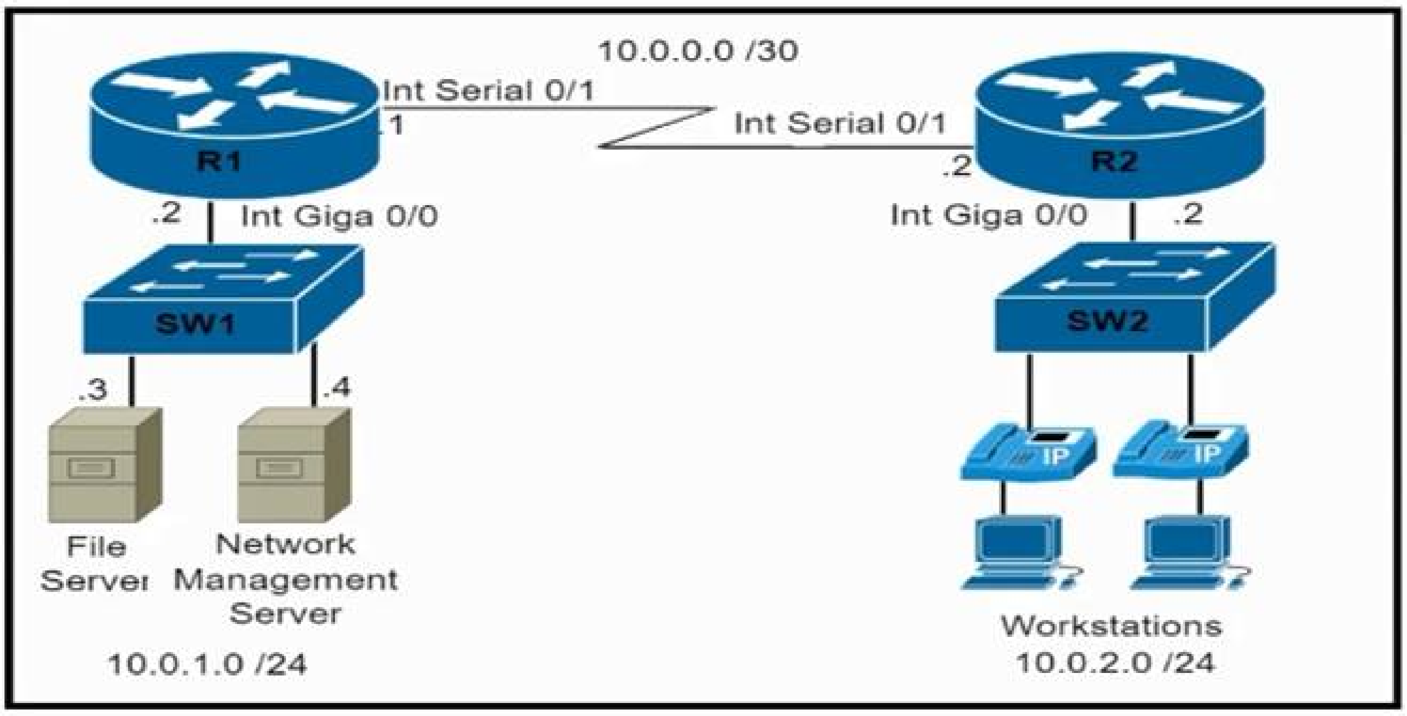


```
with open("ifaces.json", "w") as OutFile:
 OutFile.write(Response.json())
```

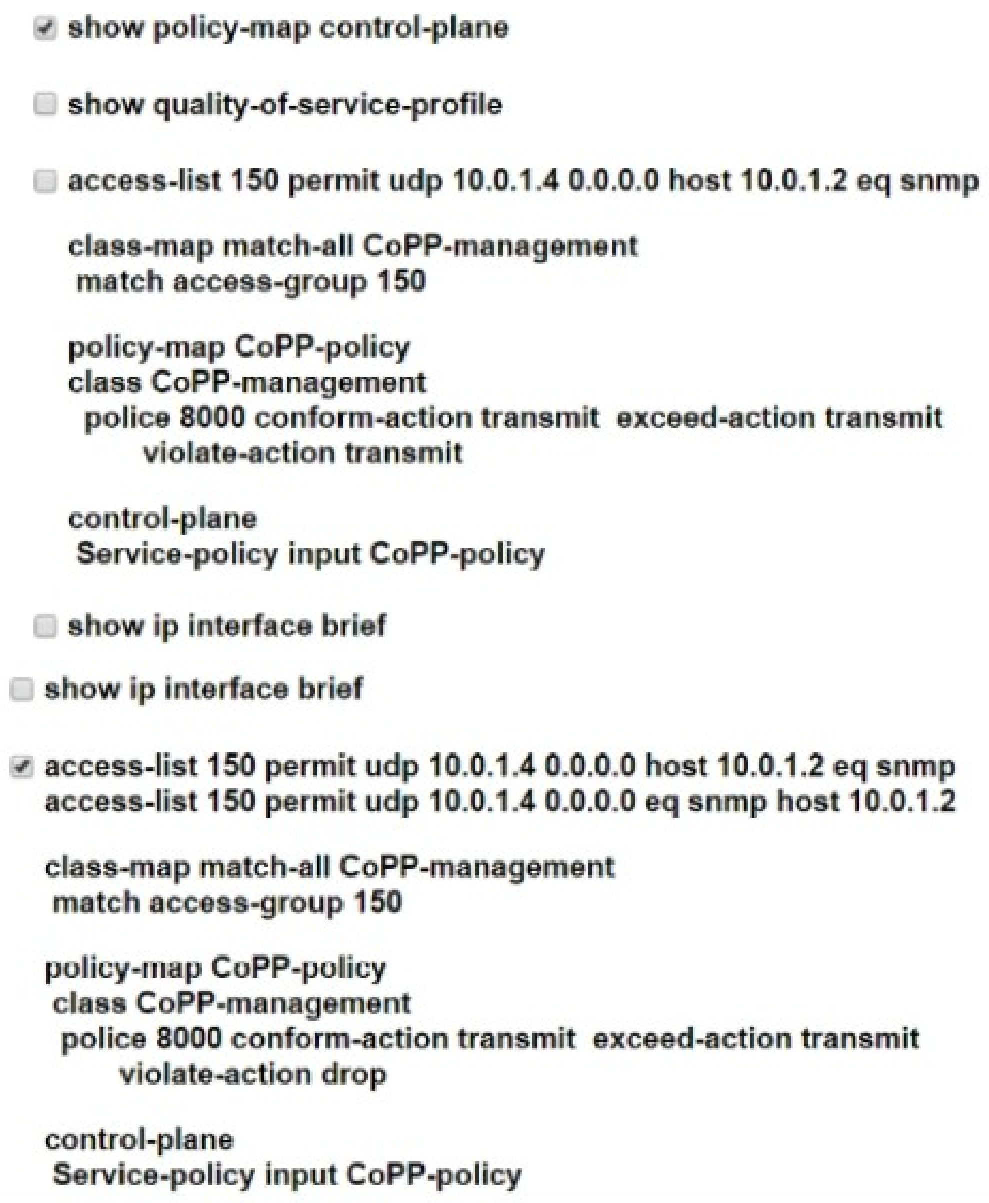
A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

NEW QUESTION 520
- (Topic 2)
Refer to the exhibit.



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



☑ show policy-map control-plane

□ show quality-of-service-profile

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

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

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

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

□ show ip interface brief

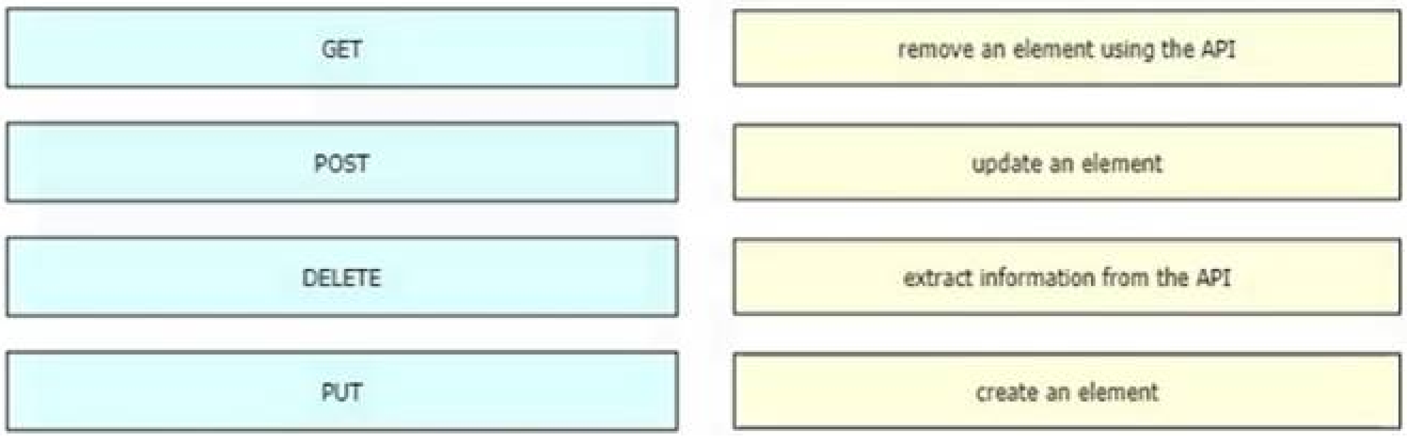
□ show ip interface brief

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

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

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

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

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

Answer: AF

NEW QUESTION 525
DRAG DROP - (Topic 2)
An engineer is working with the Cisco DNA Center API Drag and drop the methods from the left onto the actions that they are used for on the right.

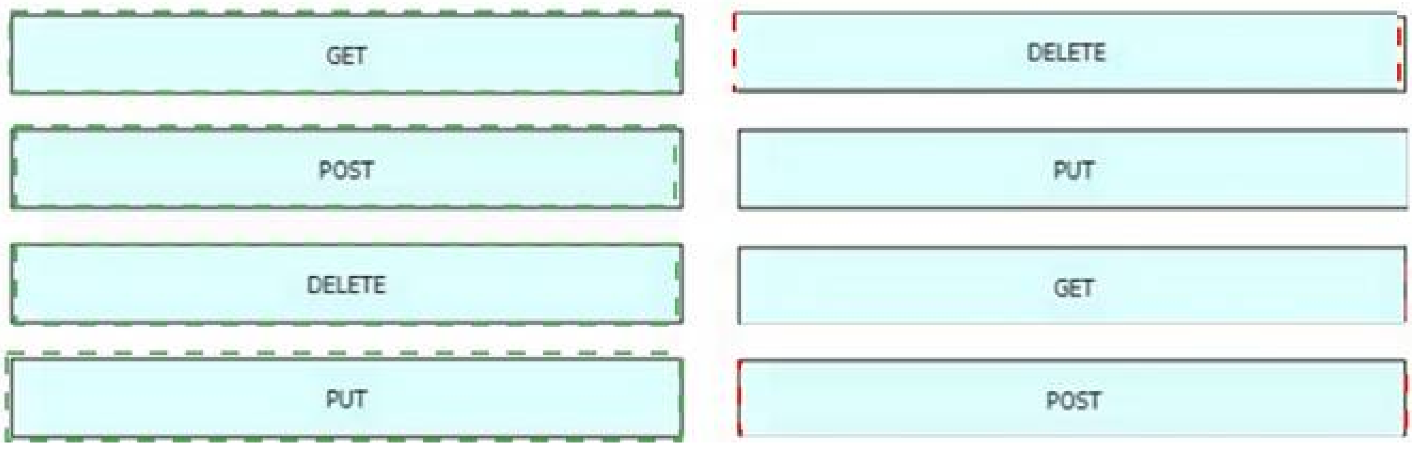


GET	remove an element using the API
POST	update an element
DELETE	extract information from the API
PUT	create an element

A. Mastered
B. Not Mastered

Answer: A

Explanation:

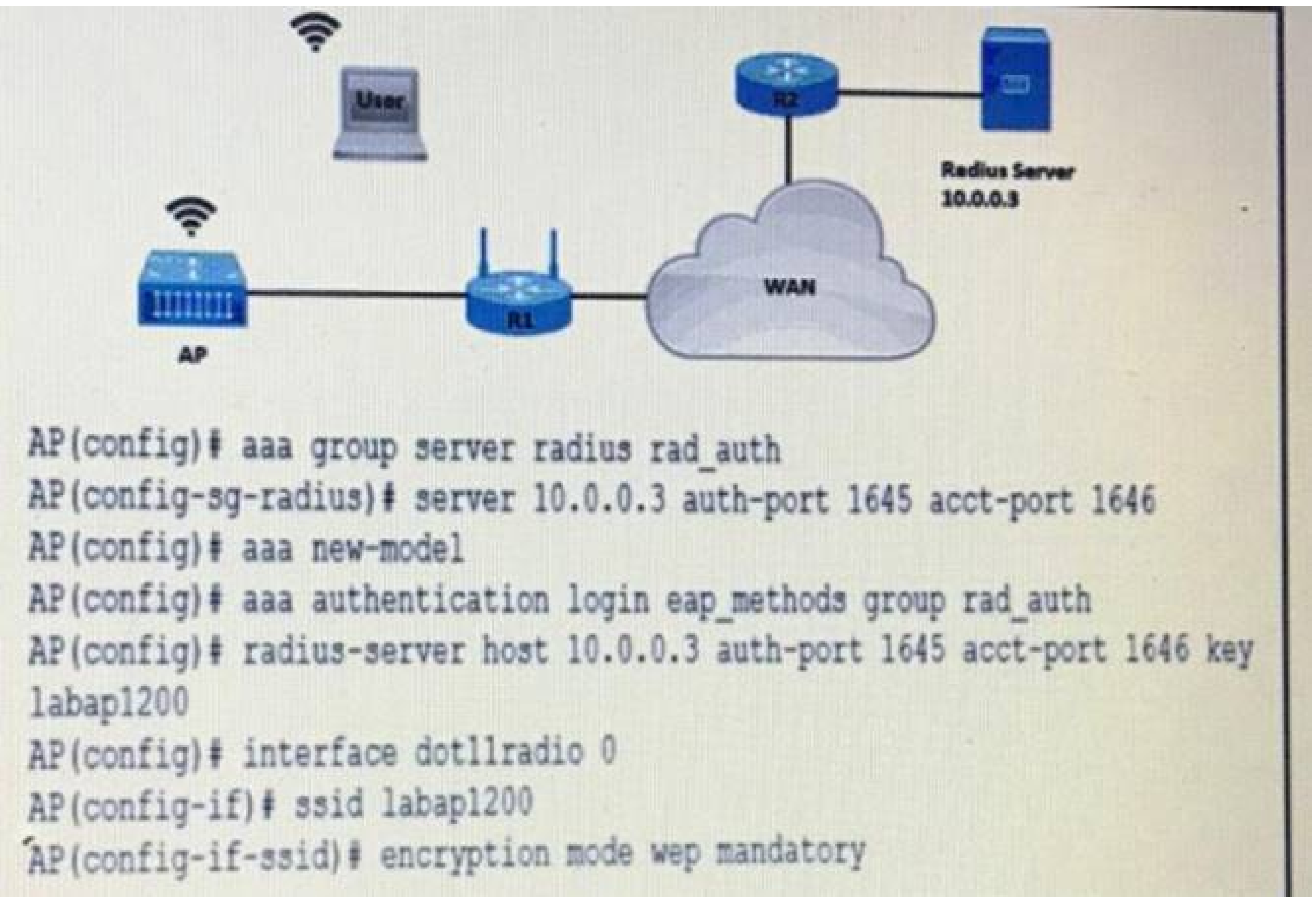


NEW QUESTION 530
- (Topic 2)
What is a VPN in a Cisco SD-WAN deployment?

A. common exchange point between two different services
B. attribute to identify a set of services offered in specific places in the SD-WAN fabric
C. virtualized environment that provides traffic isolation and segmentation in the SD-WAN fabric
D. virtual channel used to carry control plane information

Answer: C

NEW QUESTION 535
- (Topic 2)
Refer to the exhibit.



```
AP(config)# aaa group server radius rad_auth
AP(config-sg-radius)# server 10.0.0.3 auth-port 1645 acct-port 1646
AP(config)# aaa new-model
AP(config)# aaa authentication login eap_methods group rad_auth
AP(config)# radius-server host 10.0.0.3 auth-port 1645 acct-port 1646 key
labap1200
AP(config)# interface dot11radio 0
AP(config-if)# ssid labap1200
AP(config-if-ssid)# encryption mode wep mandatory
```

A company requires that all wireless users authenticate using dynamic key generation. Which configuration must be applied?

A. AP(config-if-ssid)# authentication open wep wep_methods
B. AP(config-if-ssid)# authentication dynamic wep wep_methods
C. AP(config-if-ssid)# authentication dynamic open wep_dynamic
D. AP(config-if-ssid)# authentication open eap eap_methods

Answer: D

NEW QUESTION 536
- (Topic 2)
A network administrator is implementing a routing configuration change and enables routing debugs to track routing behavior during the change. The logging output on the terminal is interrupting the command typing process. Which two actions can the network administrator take to minimize the possibility of typing commands incorrectly? (Choose two.)

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

Answer: CD

NEW QUESTION 541
- (Topic 2)
What are two benefits of implementing a Cisco SD-WAN architecture? (Choose two)

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

Answer: CD

Explanation:

The top SD-WAN benefits are:
+ Increased bandwidth at a lower cost
+ Centralized management across branch networks
+ Full visibility into the network
+ Providing organizations with more connection type options and vendor selection when building a network.
Reference: https://www.sdxcentral.com/networking/sd-wan/definitions/sd-wan-technology/
-> We can provision endpoints (vEdges) through a centralized router vManage -> Answer D is correct.
Answer A is not correct as we can use different kind of connections on SD-WAN: MPLS,
LTE, 4G, xDSL, Internet connections…
Application-Aware Routing policy is configured in vManage as a centralized data policy that maps the service- side application(s) to specific SLA requirements. The centralized policies provisioned in vSmart controller is pushed to relevant WAN Edge devices for enforcement. The defined policy consists of match- action pairs, where the match statement defines the application-list or the type of traffic to match, and the action statement defines the SLA action the WAN Edge devices must enforce for the specified traffic.
Reference: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan- application-awarerouting-deploy-guide.html

NEW QUESTION 545
- (Topic 4)
A company recently decided to use RESTCONF instead of NETCONF and many of their NETCONF scripts contain the operation <edit-config>(operation=”create”).Which RESTCONF operation must be used to replace these statements?

A. POST
B. GET
C. PUT
D. CREATE

Answer: A

NEW QUESTION 549
- (Topic 4)
Why would an architect use an OSPF virtual link?

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

Answer: D

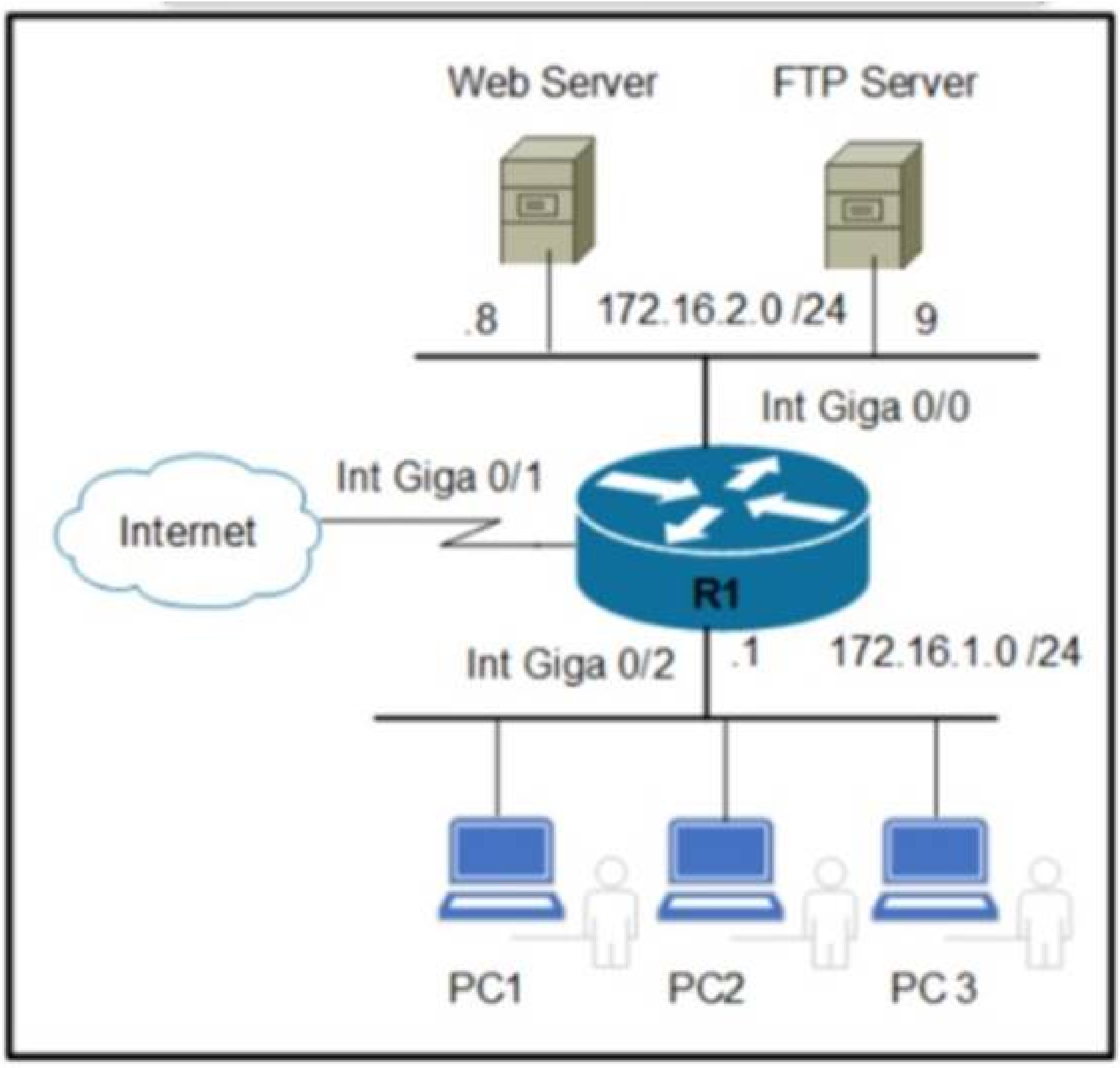
Explanation:
A virtual link is a logical connection between two OSPF routers that belong to different areas but share a common border with a transit area. A virtual link allows an OSPF router to participate in the backbone area (Area 0) even if it is not physically connected to it. This way, the OSPF network can maintain connectivity and routing consistency across all areas. A virtual link is configured between the OSPF router IDs of the two routers that need to be connected to the backbone area123.
Option A is incorrect because a stub area is an area that does not receive external routes from other autonomous systems or other OSPF areas. A stub area can only transit traffic to and from the backbone area, and it cannot be used as a transit area for a virtual link12. Option B is incorrect because a virtual link does not change the IP address space of the networks that it connects. A virtual link is transparent to the IP layer and only affects the OSPF routing protocol. To connect two networks that have overlapping private IP address space, other solutions such as NAT or VPN are required12.
Option C is incorrect because a virtual link cannot merge two existing Area 0s through a nonbackbone area. A virtual link can only extend an existing Area 0 through a nonbackbone area. If there are two separate Area 0s in an OSPF network, they cannot be merged by a virtual link, and the network is considered to be partitioned. A partitioned network can cause routing loops and inconsistencies, and it should be
avoided12. References: 1: Configure OSPF Connection in a Virtual Link
Environment, 2: How to configure OSPF Virtual Link, 3: Understand OSPF Areas and Virtual Links

NEW QUESTION 552
- (Topic 4)
How do cloud deployments compare to on-premises deployments?

A. Cloud deployments provide a better user experience across world regions, whereas on- premises deployments depend upon region-specific conditions
B. Cloud deployments are inherently unsecur
C. whereas a secure architecture is mandatory for on-premises deployments.
D. Cloud deployments mandate a secure architecture, whereas on-premises deployments are inherently unsecure.
E. Cloud deployments must include automation infrastructure, whereas on-premises deployments often lack the ability for automation.

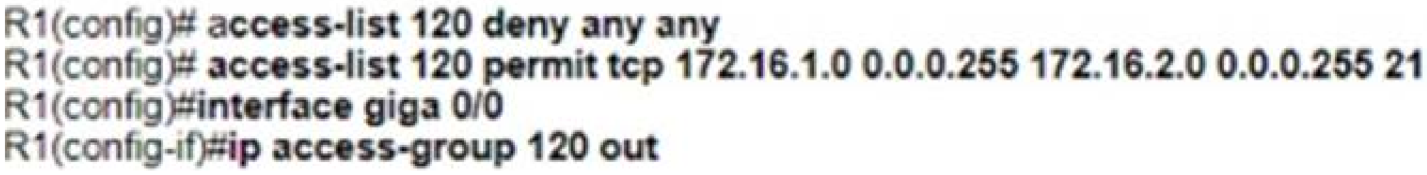
Answer: B

NEW QUESTION 554
- (Topic 4)



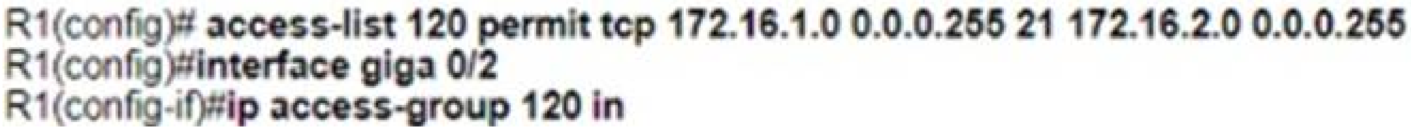
Refer to the exhibit. An engineer must allow the FTP traffic from users on 172.16.1.0 /24 to 172.16.2.0 /24 and block all other traffic. Which configuration must be applied?

A)



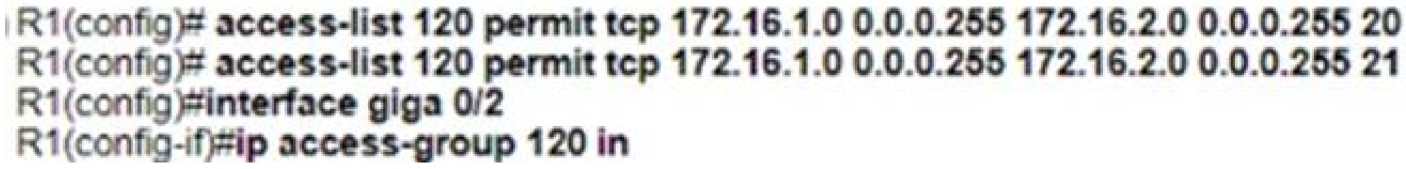
```
R1(config)# access-list 120 deny any any
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21
R1(config)#interface giga 0/0
R1(config-if)#ip access-group 120 out
```

B)



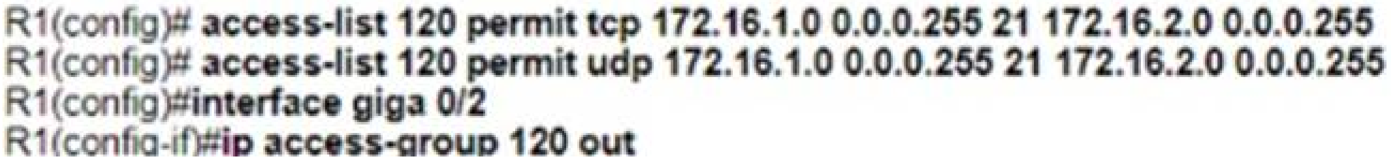
```
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 in
```

C)



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

D)

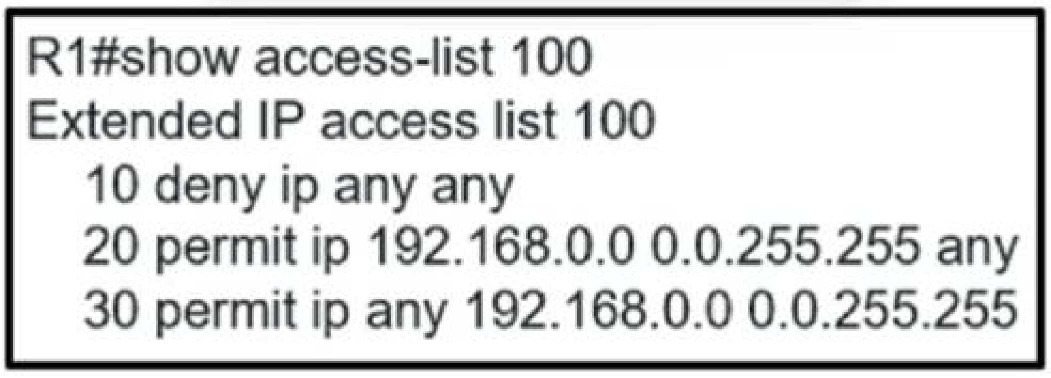


```
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)# access-list 120 permit udp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 out
```

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

Answer: B

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



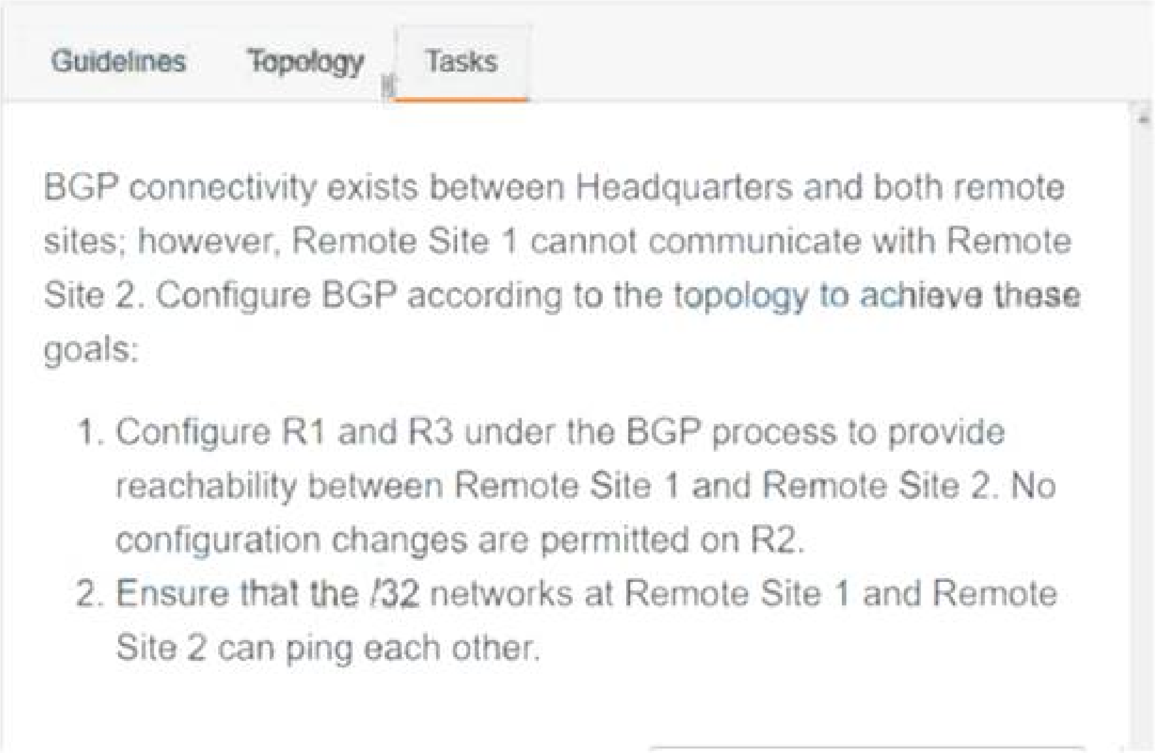
```
R1#show access-list 100
Extended IP access list 100
   10 deny ip any any
   20 permit ip 192.168.0.0 0.0.255.255 any
   30 permit ip any 192.168.0.0 0.0.255.255
```

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

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

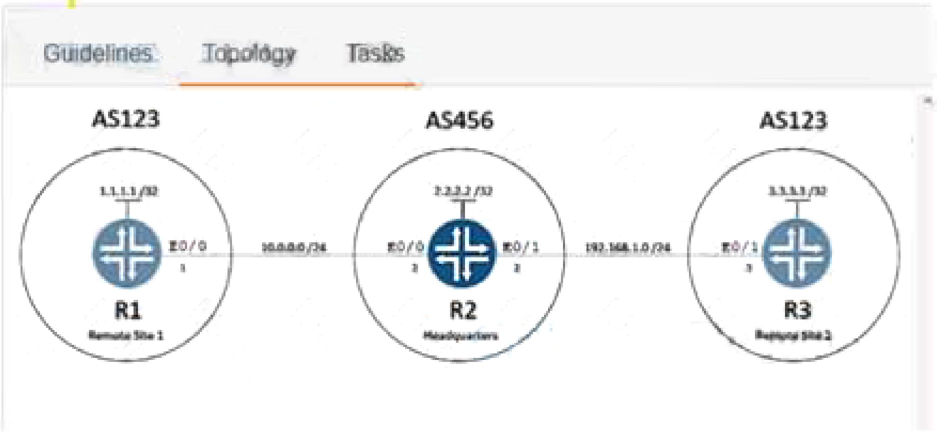
Answer: A

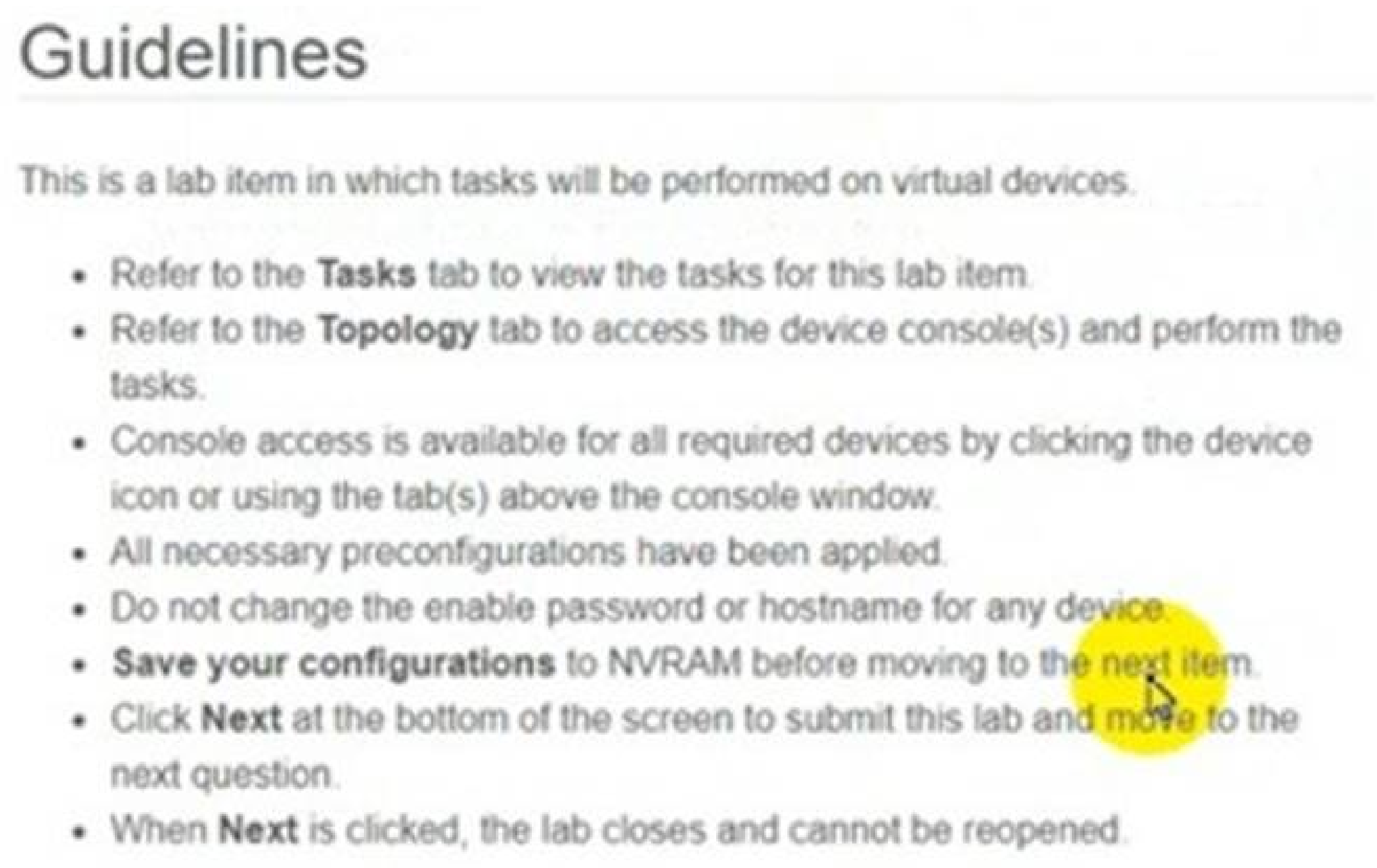
NEW QUESTION 558
SIMULATION - (Topic 4)
Simulation 01
BGP connectivity exists between Headquarters and both remote sites; however, Remote Site 1 cannot communicate with Remote Site 2. Configure BGP according to the topology to
goals:
* 1. Configure R1 and R3 under the BGP process to provide reachability between Remote Site 1 and Remote Site 2. No configuration changes are permitted on R2.
* 2. Ensure that the /32 networks at Remote Site 1 and Remote Site 2 can ping each other.



BGP connectivity exists between Headquarters and both remote sites; however, Remote Site 1 cannot communicate with Remote Site 2. Configure BGP according to the topology to achieve these goals:

1. Configure R1 and R3 under the BGP process to provide reachability between Remote Site 1 and Remote Site 2. No configuration changes are permitted on R2.
2. Ensure that the /32 networks at Remote Site 1 and Remote Site 2 can ping each other.



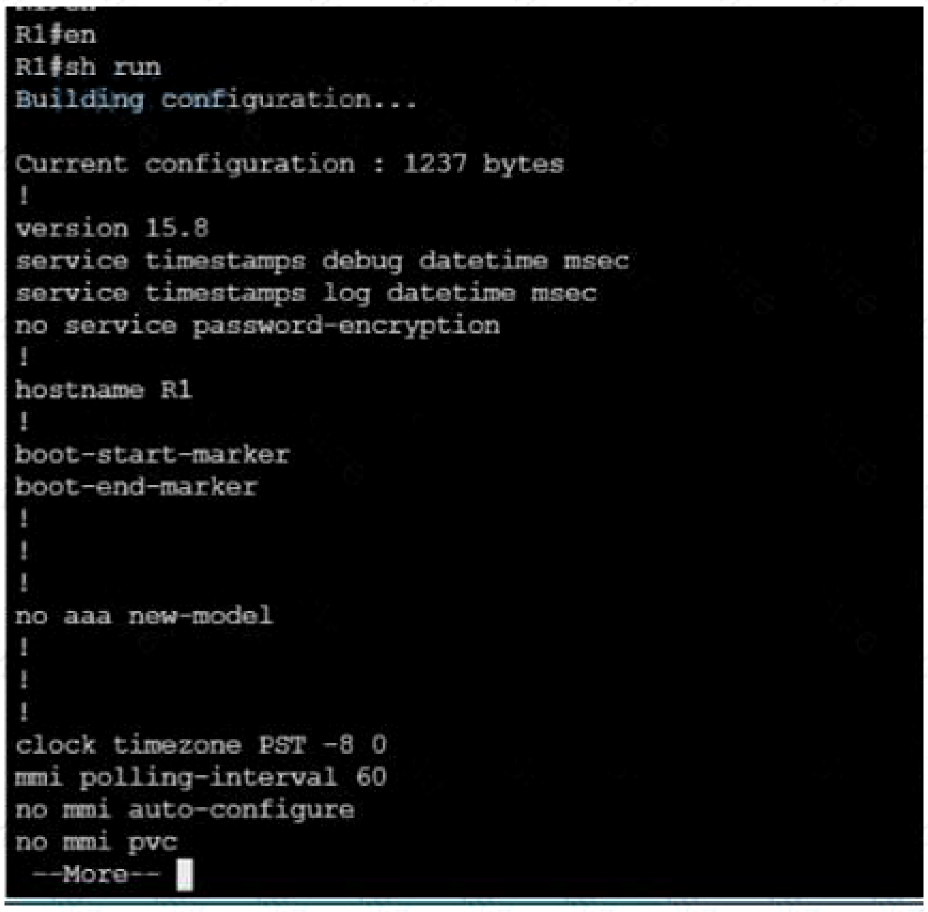


Guidelines

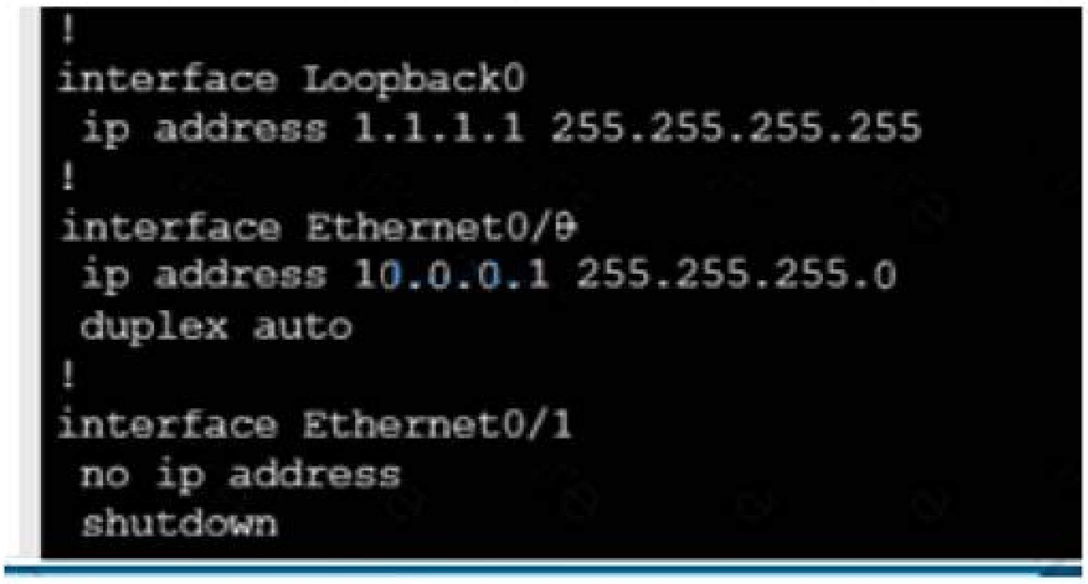
This is a lab item in which tasks will be performed on virtual devices.

- Refer to the **Tasks** tab to view the tasks for this lab item.
- Refer to the **Topology** tab to access the device console(s) and perform the tasks.
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- All necessary preconfigurations have been applied.
- Do not change the enable password or hostname for any device.
- **Save your configurations** to NVRAM before moving to the next item.
- Click **Next** at the bottom of the screen to submit this lab and move to the next question.
- When **Next** is clicked, the lab closes and cannot be reopened.

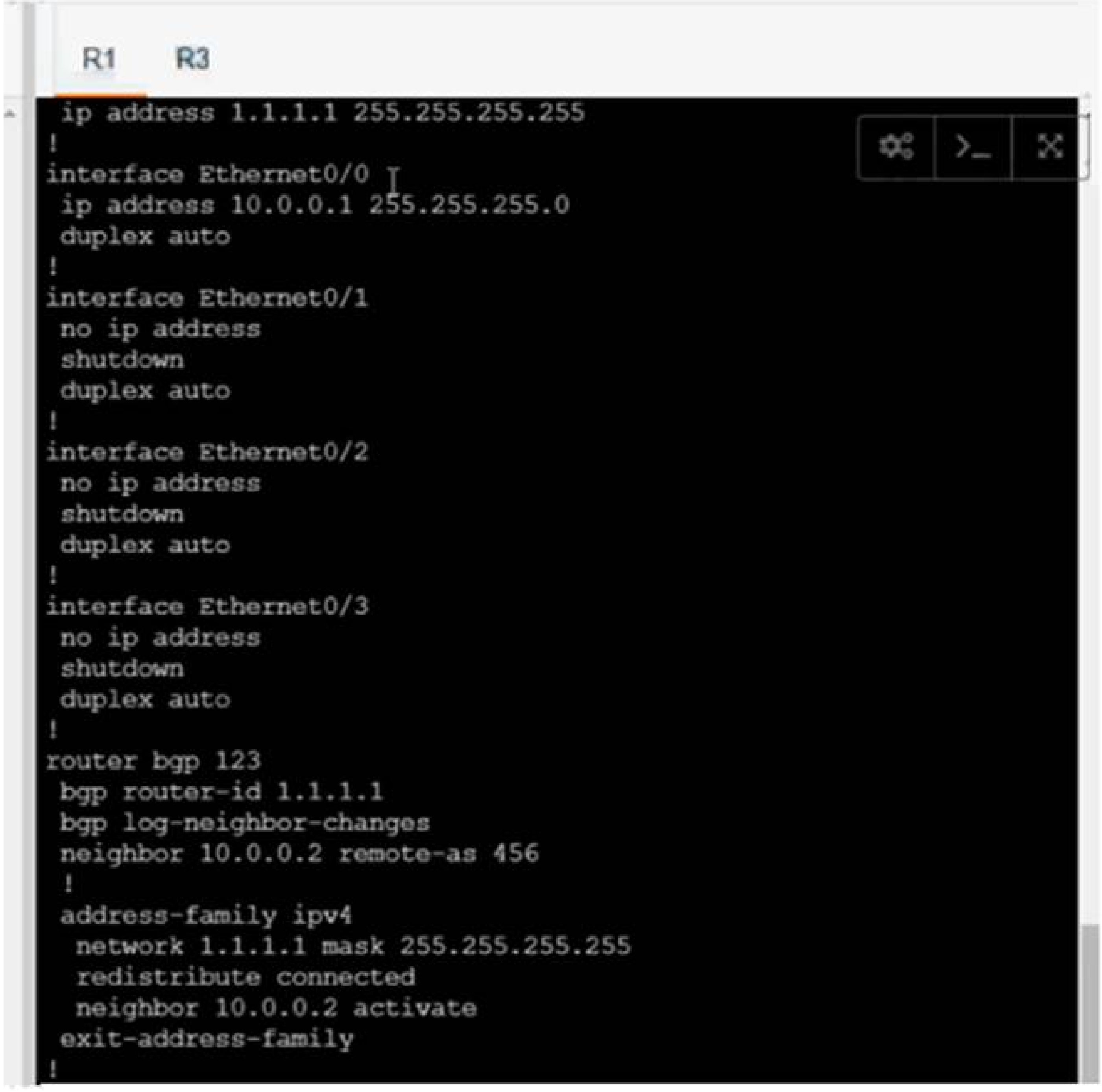
R1



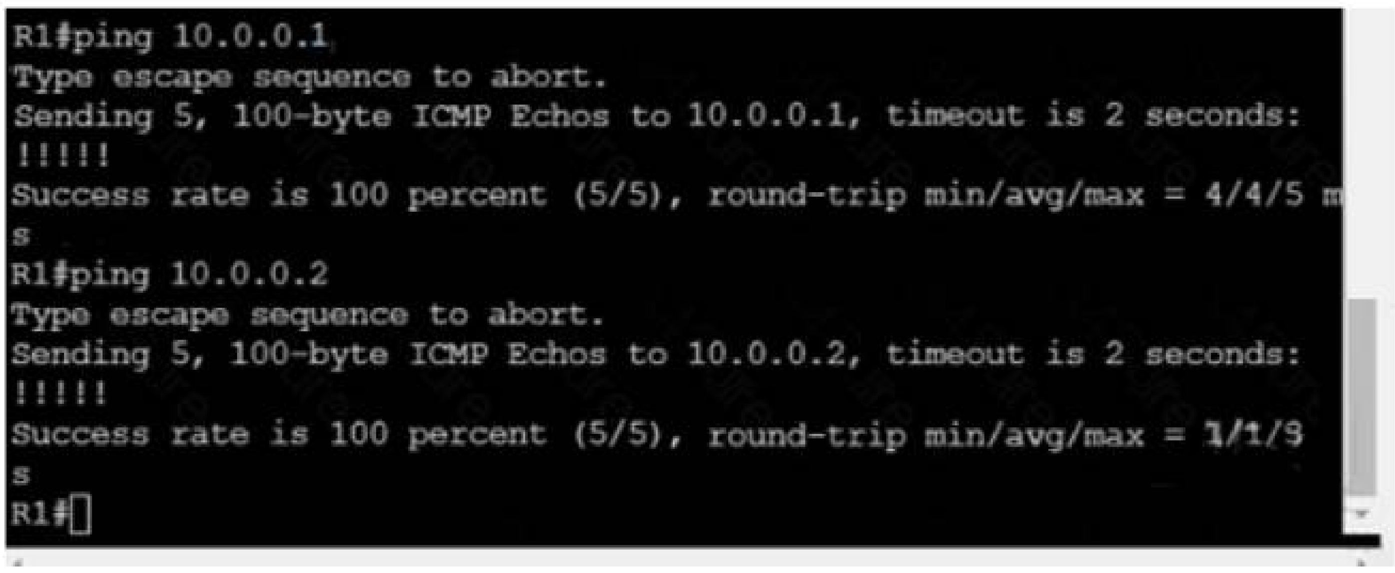
```
R1#en
R1#sh run
Building configuration...

Current configuration : 1237 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
 --More--
```



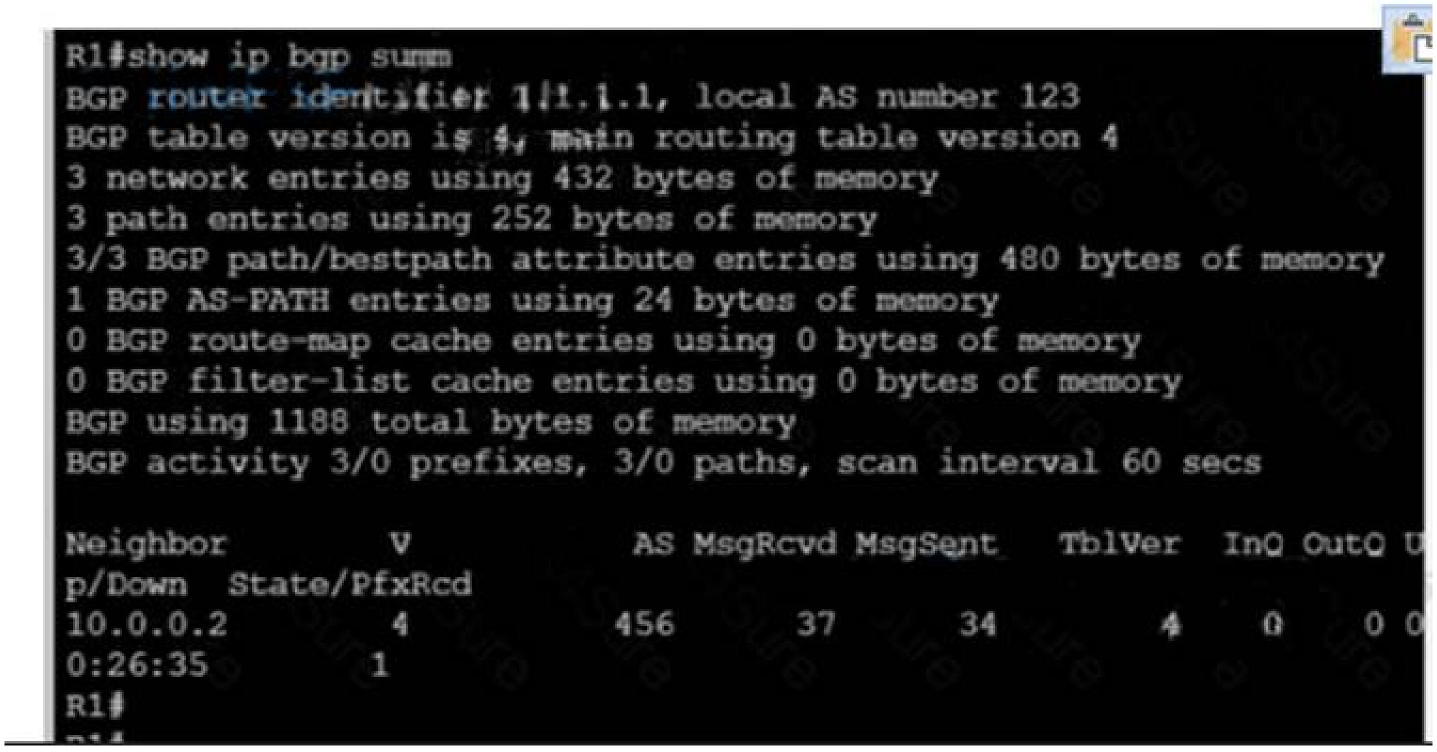
```
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
```



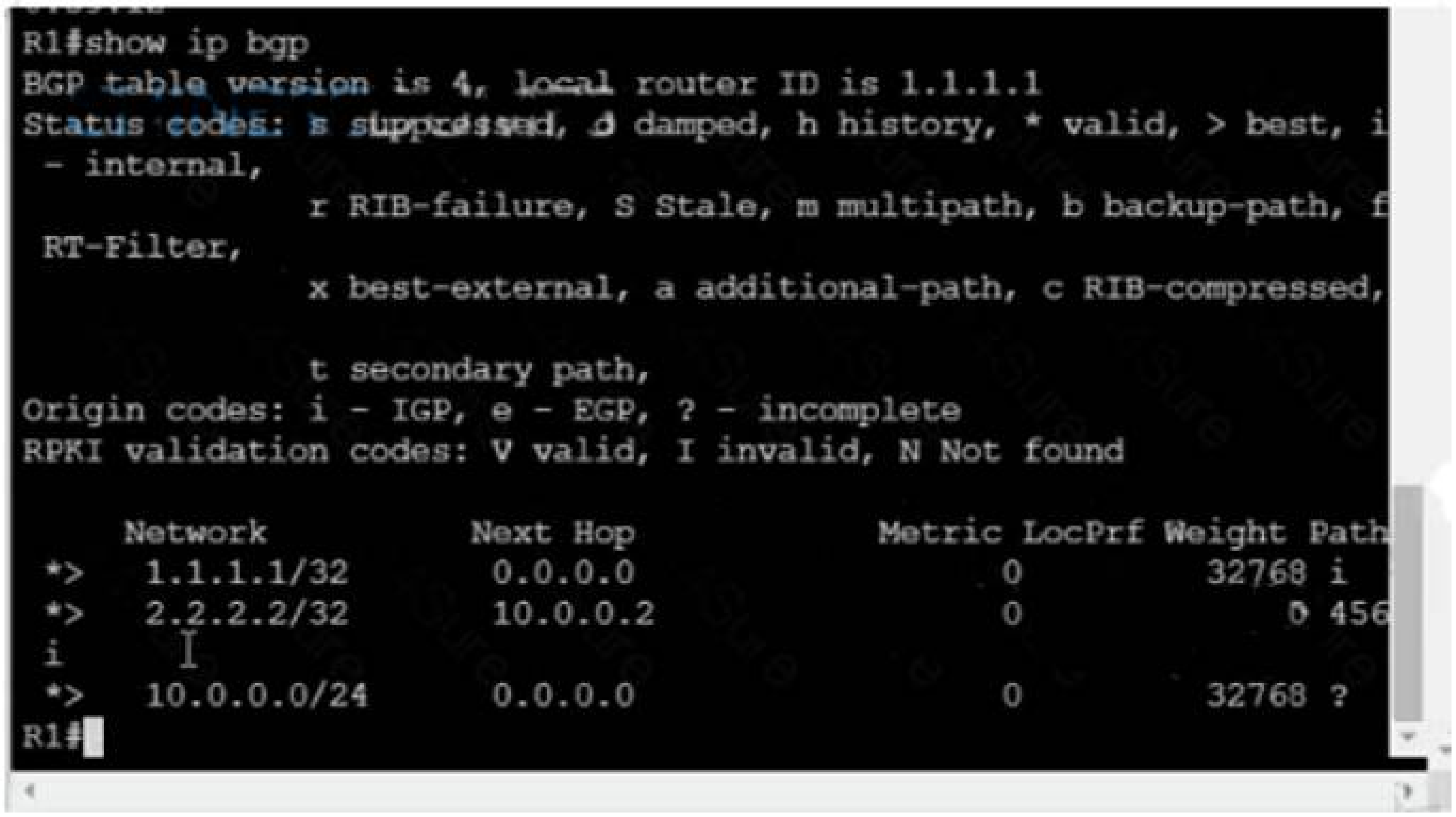
```
 ip address 1.1.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router bgp 123
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 neighbor 10.0.0.2 remote-as 456
 !
 address-family ipv4
  network 1.1.1.1 mask 255.255.255.255
  redistribute connected
  neighbor 10.0.0.2 activate
 exit-address-family
!
```



```
R1#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 m
s
R1#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3
s
R1#
```

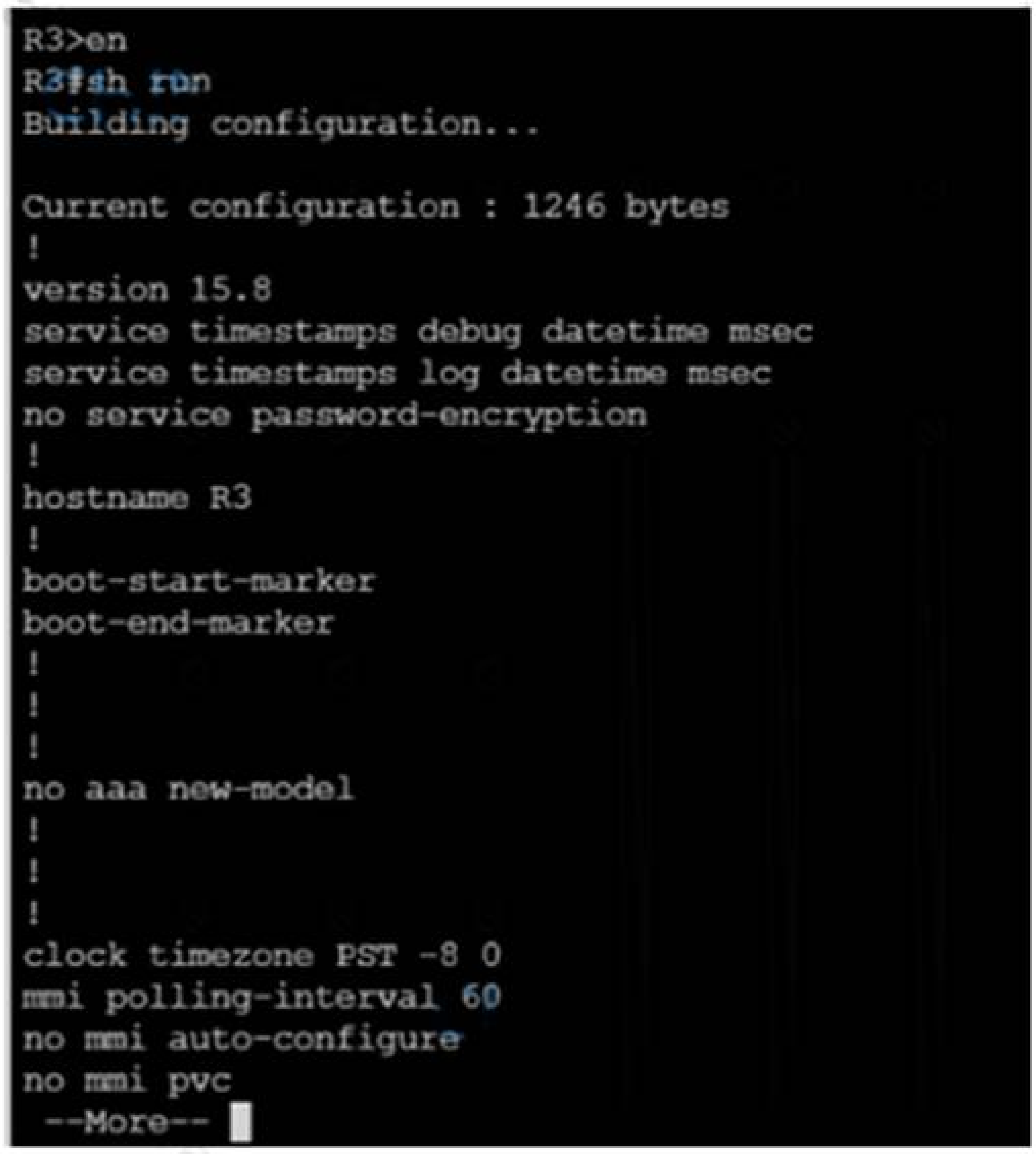


```
R1#show ip bgp summ
BGP router identifier 1.1.1.1, local AS number 123
BGP table version is 4, main routing table version 4
3 network entries using 432 bytes of memory
3 path entries using 252 bytes of memory
3/3 BGP path/bestpath attribute entries using 480 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1188 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ U
p/Down  State/PfxRcd
10.0.0.2        4          456      37      34        4    0    0 0
0:26:35        1
R1#
```

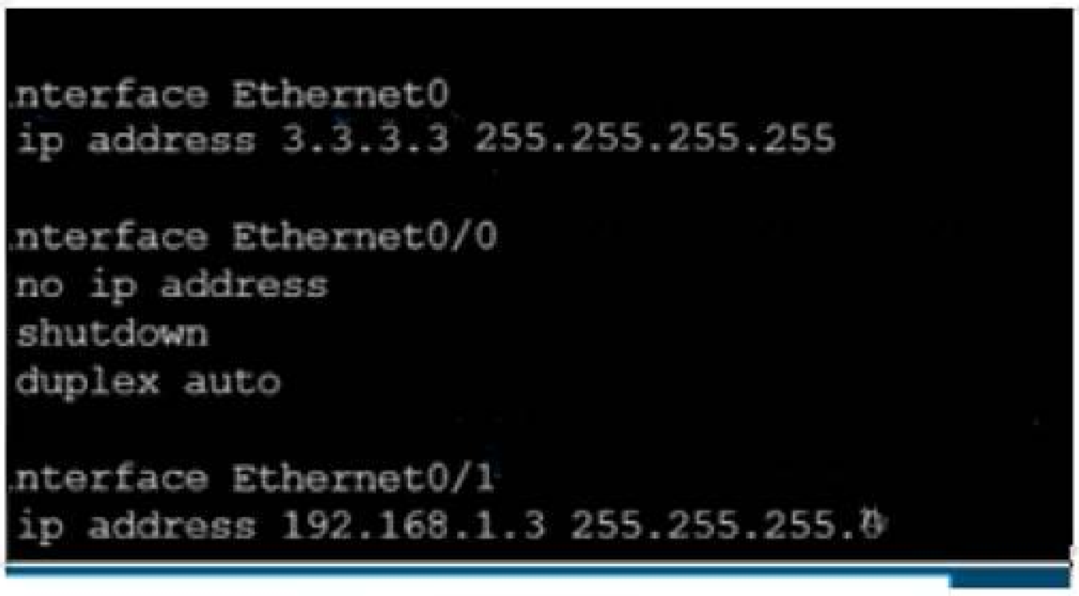


```
R1#show ip bgp
BGP table version is 4, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i
 - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f
 RT-Filter,
              x best-external, a additional-path, c RIB-compressed,

              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>   1.1.1.1/32       0.0.0.0                  0         32768 i
 *>   2.2.2.2/32       10.0.0.2                 0             0 456
 i
 *>   10.0.0.0/24      0.0.0.0                  0         32768 ?
R1#
```

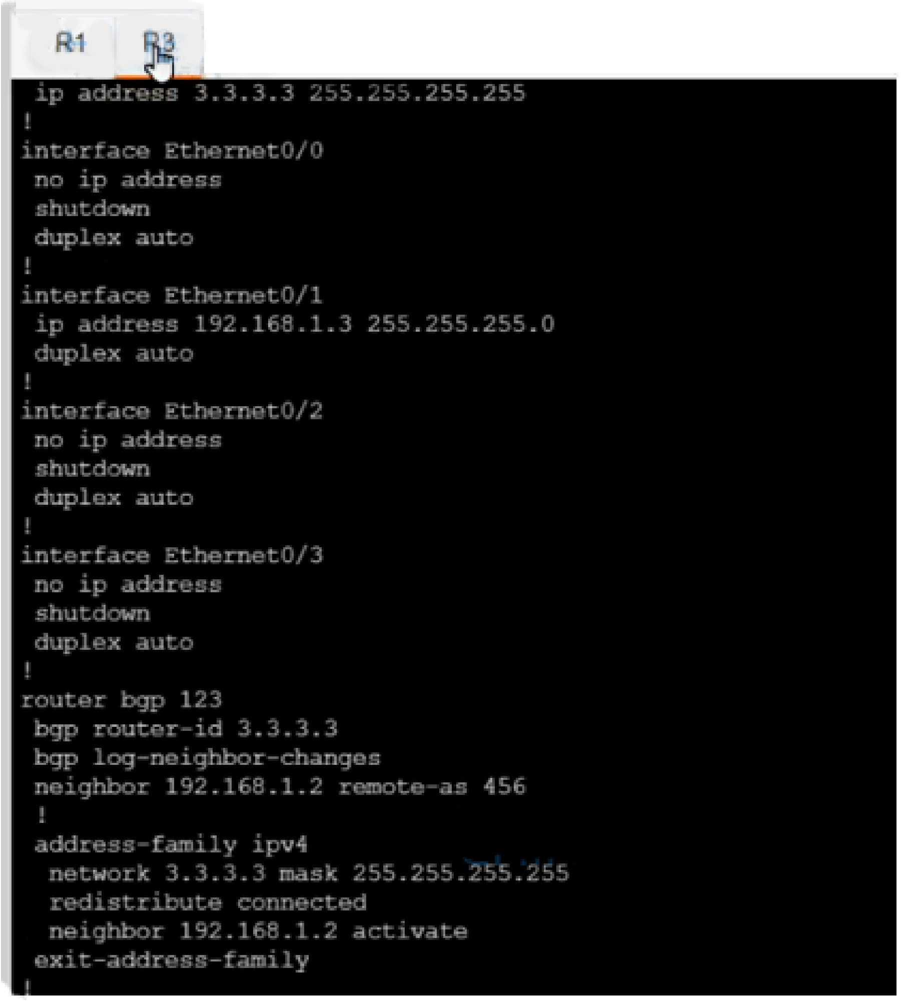
R3



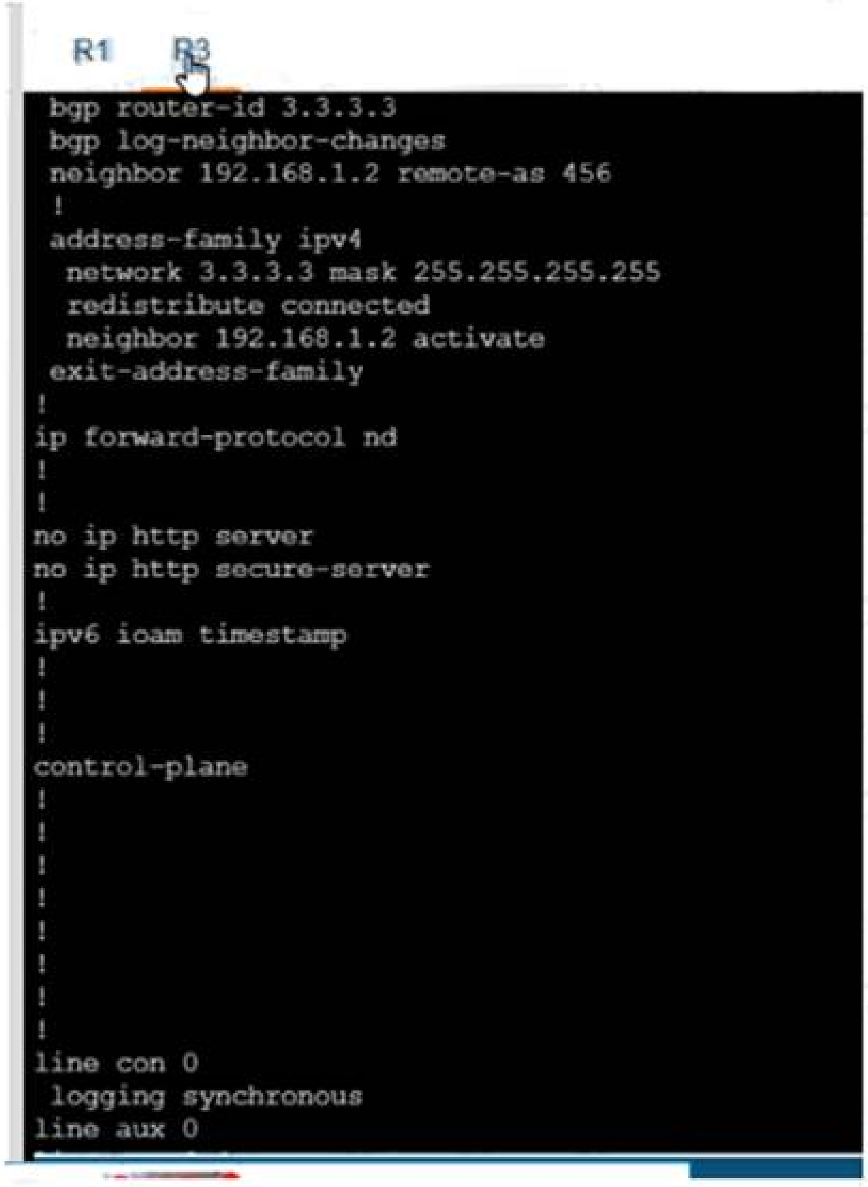
```
R3>en
R3#sh run
Building configuration...

Current configuration : 1246 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
 --More--
```



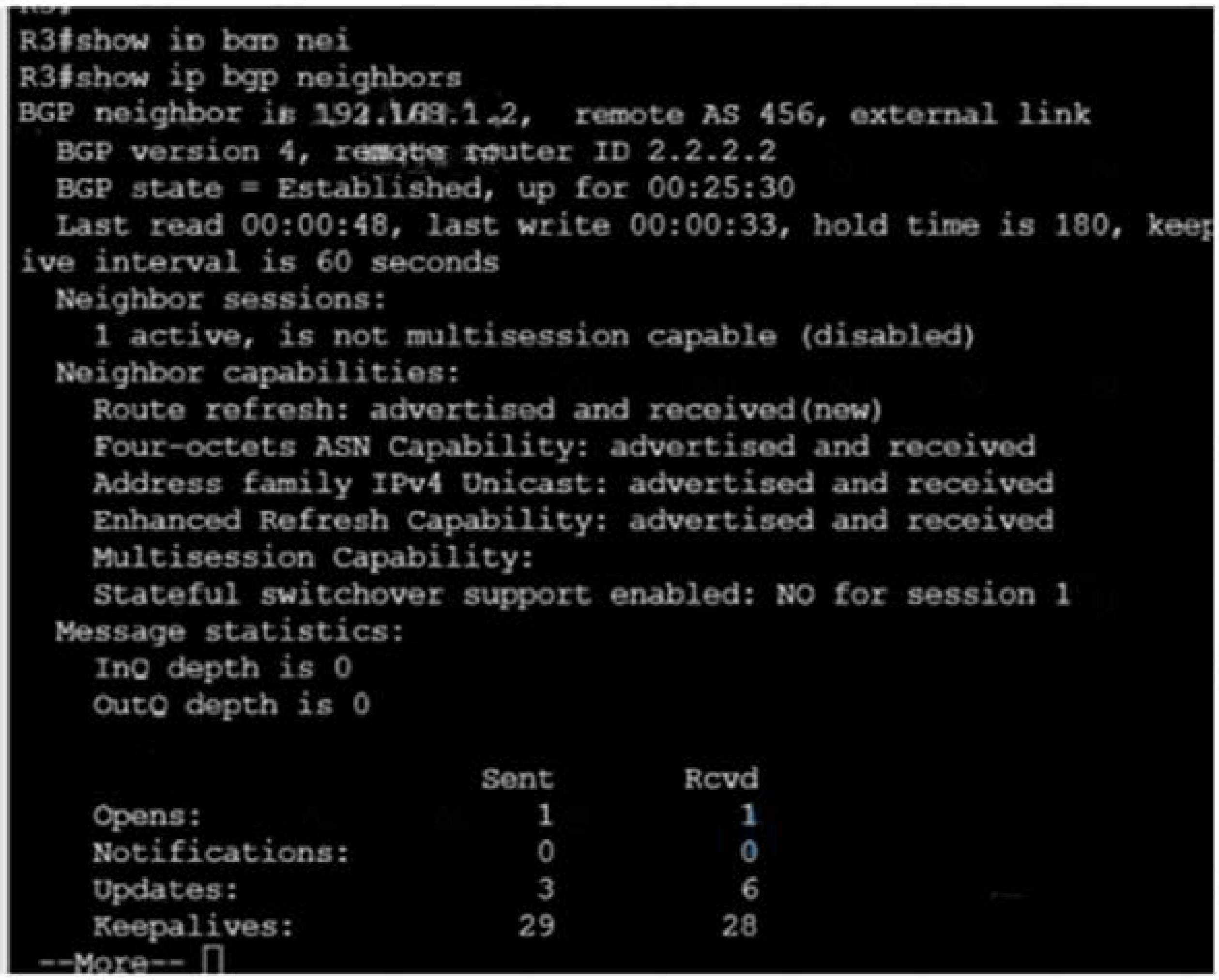
```
nterface Ethernet0
ip address 3.3.3.3 255.255.255.255

nterface Ethernet0/0
no ip address
shutdown
duplex auto

nterface Ethernet0/1
ip address 192.168.1.3 255.255.255.0
```



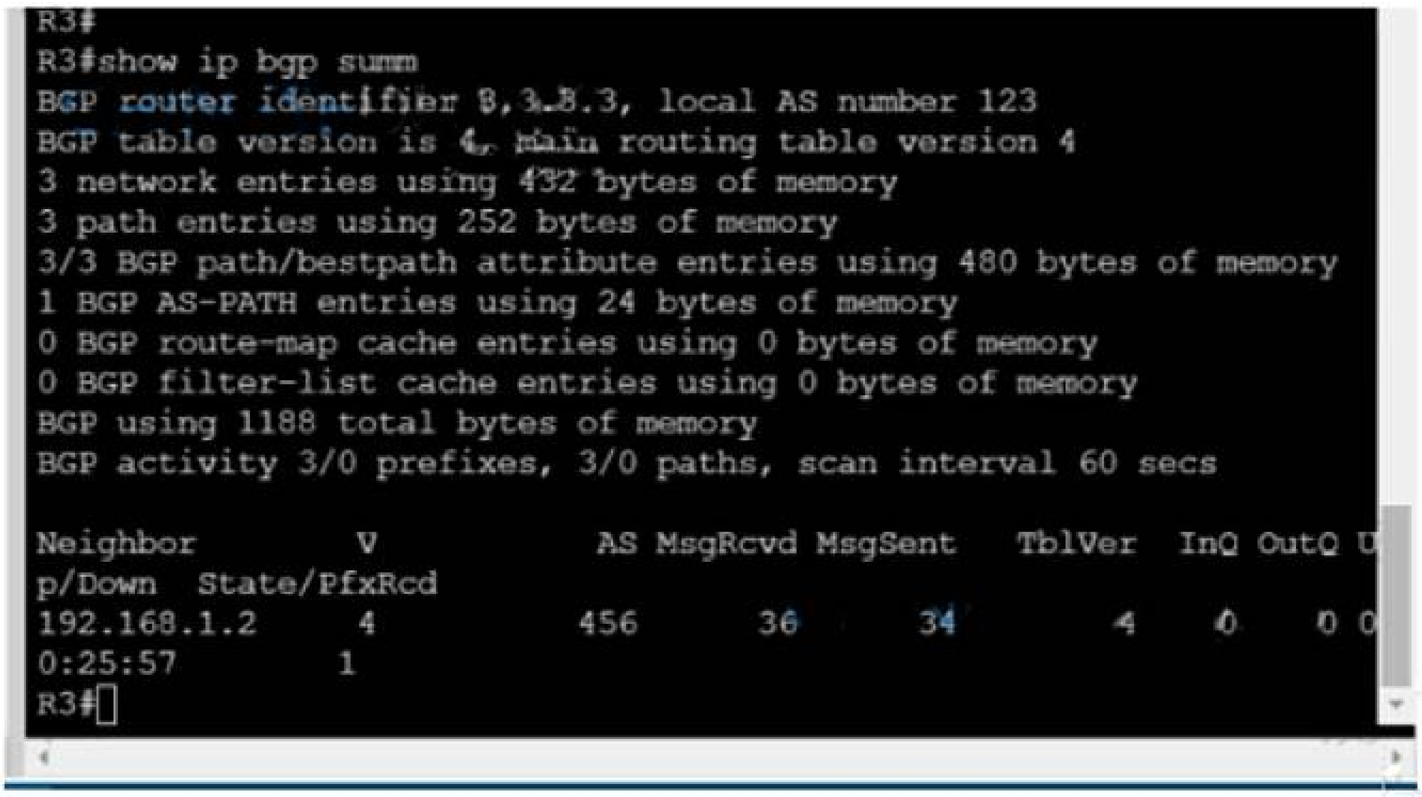
```
 ip address 3.3.3.3 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.1.3 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router bgp 123
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 456
 !
 address-family ipv4
  network 3.3.3.3 mask 255.255.255.255
  redistribute connected
  neighbor 192.168.1.2 activate
 exit-address-family
!
```



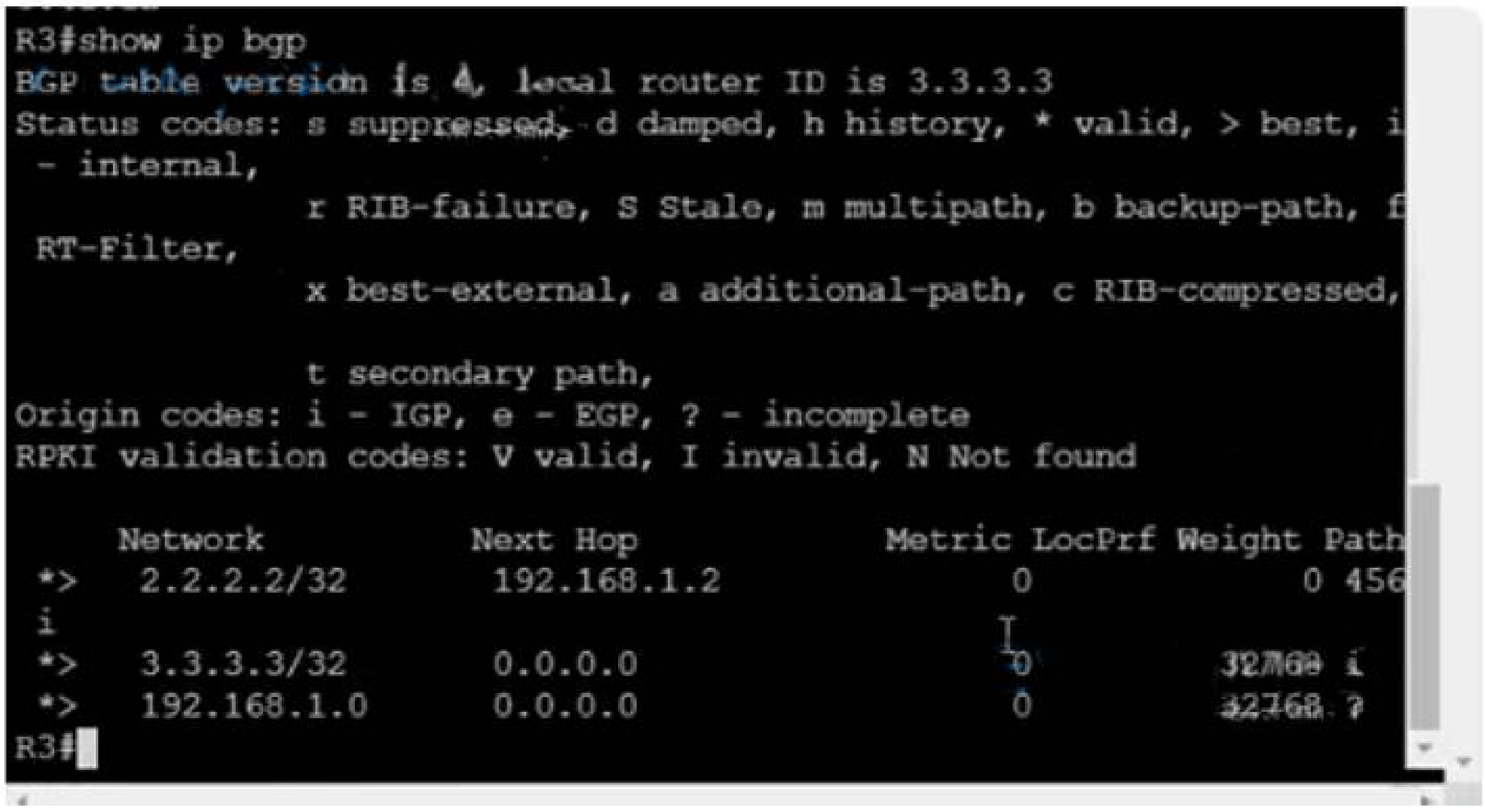
```
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 456
 !
 address-family ipv4
  network 3.3.3.3 mask 255.255.255.255
  redistribute connected
  neighbor 192.168.1.2 activate
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
```



```
R3#show ip bgp nei
R3#show ip bgp neighbors
BGP neighbor is 192.168.1.2,  remote AS 456, external link
  BGP version 4, remote router ID 2.2.2.2
  BGP state = Established, up for 00:25:30
  Last read 00:00:48, last write 00:00:33, hold time is 180, keep
ive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                3          6
    Keepalives:            29         28
 --More--
```



```
R3#
R3#show ip bgp summ
BGP router identifier 3.3.3.3, local AS number 123
BGP table version is 4, main routing table version 4
3 network entries using 432 bytes of memory
3 path entries using 252 bytes of memory
3/3 BGP path/bestpath attribute entries using 480 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1188 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ U
p/Down  State/PfxRcd
192.168.1.2     4          456      36      34        4    0    0 0
0:25:57        1
R3#
```



```
R3#show ip bgp
BGP table version is 4, local router ID is 3.3.3.3
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,

               t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  2.2.2.2/32       192.168.1.2              0             0 456
 i
 *>  3.3.3.3/32       0.0.0.0                  0         32768 i
 *>  192.168.1.0      0.0.0.0                  0         32768 ?
R3#
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
See the solution below in Explanation:
- Solution:

```
On R1:
R1(config)#router bgp 123
R1(config-router)#address-family ipv4
R1(config-router-af)#neighbor 10.0.0.2 allowas-in
On R3:
R3(config)#router bgp 123
R3(config-router)# address-family ipv4
R3(config-router-af)#neighbor 192.168.1.2 allowas-in
VERIFICATION:
R3#sh ip route bgp
Gateway of last resort is not set 1.0.0.0/32 is subnetted, 1 subnets
B 1.1.1.1 [20/0] via 192.168.1.2, 00:01:17 2.0.0.0/32 is subnetted, 1 subnets
B 2.2.2.2 [20/0] via 192.168.1.2, 00:05:06 10.0.0.0/24 is subnetted, 1 subnets
B 10.0.0.0 [20/0] via 192.168.1.2, 00:01:17
Test Ping from R3 to R1:
R3#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
R3#ping 1.1.1.1 source lo0 Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds: Packet sent with a source address of 3.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

NEW QUESTION 561
- (Topic 4)
Which mobility role is assigned to a client in the client table of the new controller after a Layer 3 roam?

A. anchor
B. foreign
C. mobility
D. transparent

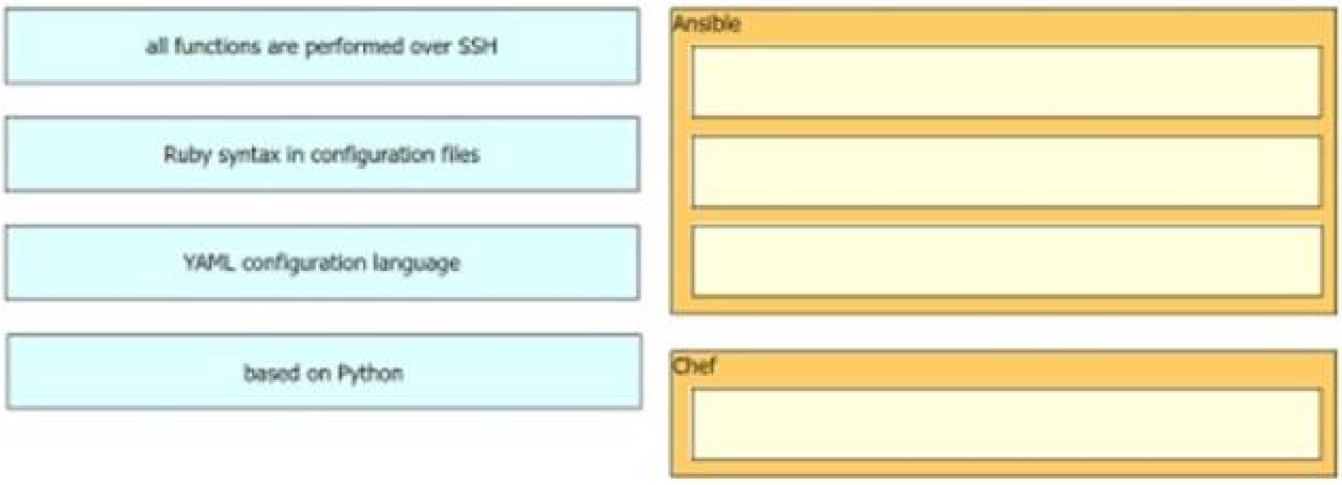
Answer: D

NEW QUESTION 566
- (Topic 4)
In a Cisco SD-Access environment, which function is performed by the border node?

A. Connect uteri and devices to the fabric domain.
B. Group endpoints into IP pools.
C. Provide reachability information to fabric endpoints.
D. Provide connectivity to traditional layer 3 networks.

Answer: D

NEW QUESTION 569
FILL IN THE BLANK - (Topic 4)
Drag and drop the automation characteristics from the left onto the corresponding tools on the right.


all functions are performed over SSH
Ruby syntax in configuration files
YAML configuration language
based on Python

Ansible

Chef

A. Mastered
B. Not Mastered

Answer: A

Explanation:
<map><m x1="15" x2="342" y1="18" y2="60" ss="0" a="0" /><m x1="20" x2="343" y1="76" y2="111" ss="0" a="0" /><m x1="19" x2="336" y1="129" y2="169" ss="0" a="0" /><m x1="22" x2="338" y1="186" y2="223" ss="0" a="0" /><m x1="368" x2="682" y1="42" y2="74" ss="1" a="0" /><m x1="362" x2="681" y1="88" y2="124" ss="1" a="0"

/><m x1="366" x2="687" y1="130" y2="167" ss="1" a="0" /><m x1="366" x2="682"
y1="216" y2="251" ss="1" a="0" /><c start="1" stop="3" /><c start="0" stop="0" /><c start="2" stop="1" /><c start="3" stop="2" /></map>

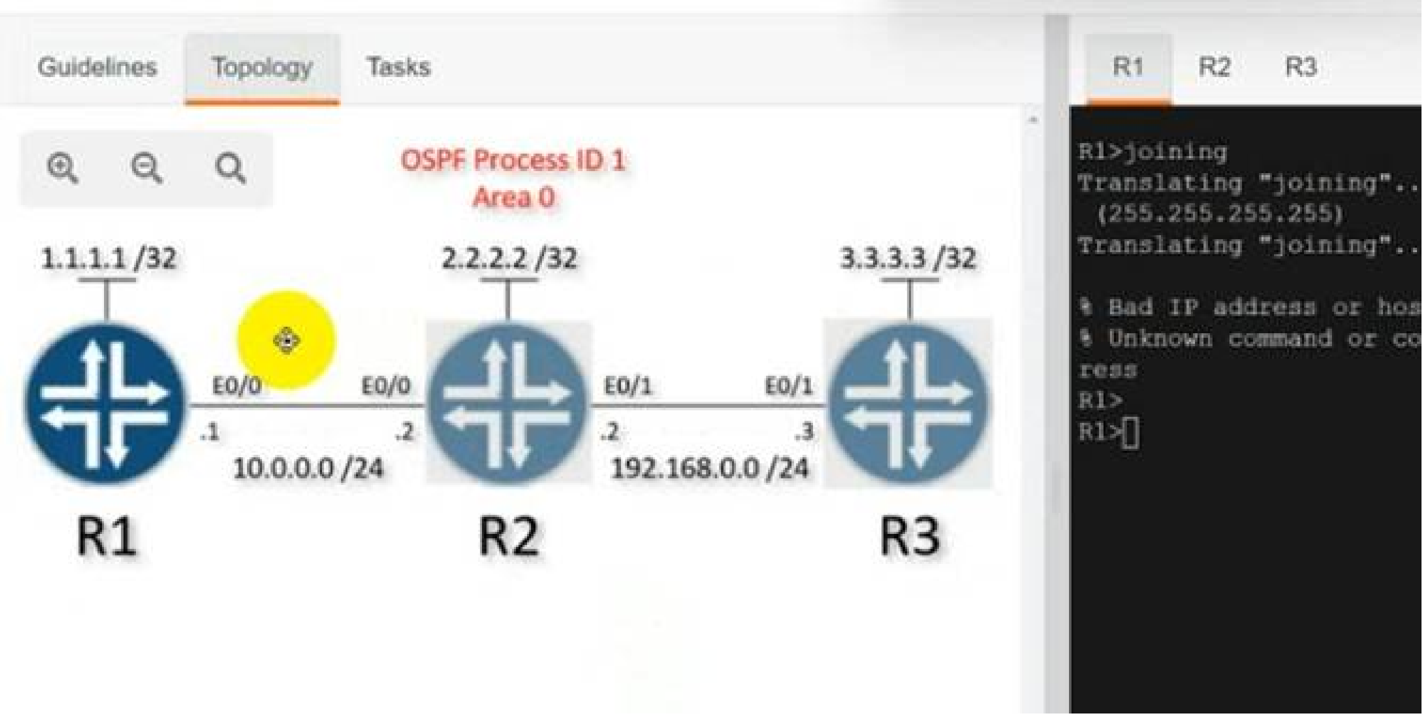
Chef
Ruby syntax in configuration files Ansible
all functions are performed over ssh YAML configuration language Based on Python

NEW QUESTION 571
- (Topic 4)
In a campus network design, what ate two benefits of using BFD tor failure detection? (Choose two.)

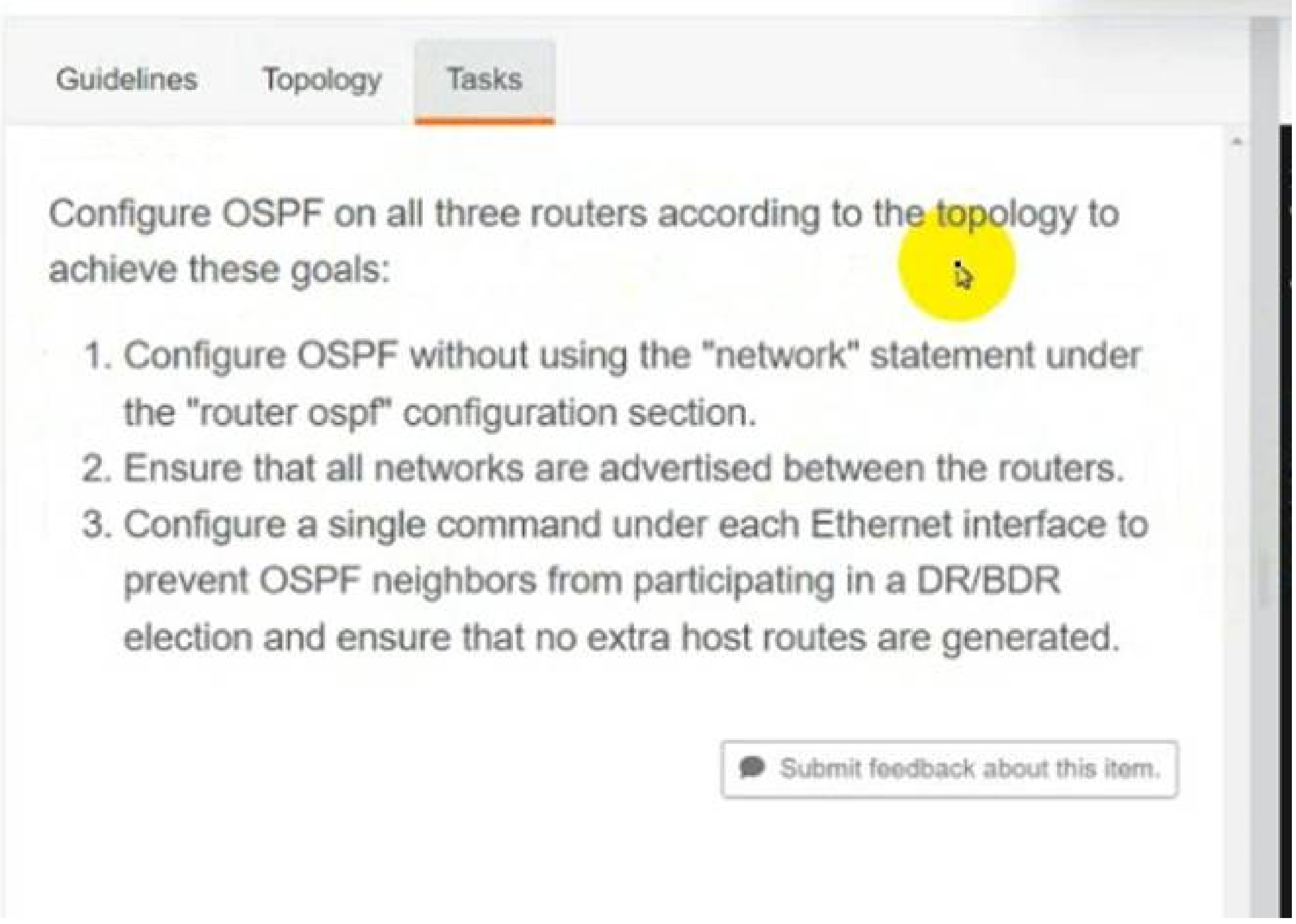
A. BFD provides path failure detection in less than a second.
B. BFD is an efficient way to reduce memory and CPU usage.
C. BFD provides fault tolerance by enabling multiple routers to appear as a single virtual router.
D. BFD speeds up routing convergence time.
E. BFD enables network peers to continue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

Answer: AB

NEW QUESTION 576
SIMULATION - (Topic 4)
Simulation 05



```
R1>joining
Translating "joining"..
 (255.255.255.255)
Translating "joining"..

% Bad IP address or hos
% Unknown command or co
ress
R1>
R1>
```



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

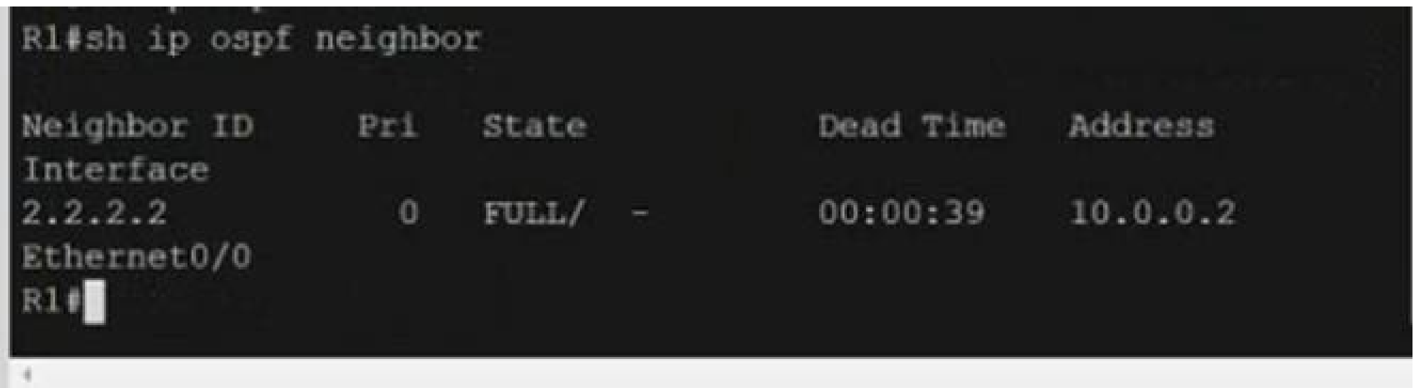
1. Configure OSPF without using the "network" statement under the "router ospf" configuration section.
2. Ensure that all networks are advertised between the routers.
3. Configure a single command under each Ethernet interface to prevent OSPF neighbors from participating in a DR/BDR election and ensure that no extra host routes are generated.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
R1
enable Config t 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
Enable
Config t
Int loop0
Ip ospf 1 area 0
Int et0/0
Ip ospf 1 area 0
Ip ospf network point-to-point
Int et0/1
Ip ospf 1 area 0
Ip ospf network point-to-point
copy run start
R3
Enable Config t Int loop0
Ip ospf 1 area 0
Int et0/1
Ip ospf 1 area 0
Ip ospf network point-to-point
copy run start
Verification:-



```
R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
2.2.2.2           0   FULL/  -        00:00:39    10.0.0.2
Ethernet0/0
R1#
```

NEW QUESTION 578
- (Topic 4)
An engineer is configuring RADIUS-Based Authentication with EAP. MS-CHAPv2 is configured on a client device. Which outer method protocol must be configured on the ISE to support this authentication type?

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

Answer: D

NEW QUESTION 582
- (Topic 4)
How do OSPF and EIGKP compare?

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

Answer: D

NEW QUESTION 586
- (Topic 4)
What is a command-line tool for consuming REST APIs?

A. Postman
B. CURL
C. Firefox
D. Python requests

Answer: B

NEW QUESTION 591
- (Topic 4)
What is the function of vBond in a Cisco SD-WAN deployment?

A. initiating connections with SD-WAN routers automatically
B. pushing of configuration toward SD-WAN routers
C. onboarding of SD-WAN routers into the SD-WAN overlay

D. gathering telemetry data from SD-WAN routers

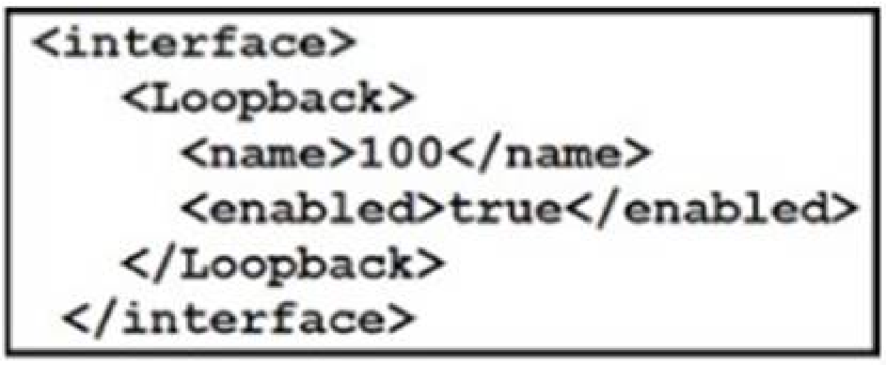
Answer: C

NEW QUESTION 593
- (Topic 4)
An engineer is describing QoS to a client. Which two facts apply to traffic policing? (Choose two.)

A. Policing adapts to network congestion by queuing excess traffic
B. Policing should be performed as close to the destination as possible
C. Policing drops traffic that exceeds the defined rate
D. Policing typically delays the traffic, rather than drops it
E. Policing should be performed as close to the source as possible

Answer: CE

NEW QUESTION 597
- (Topic 3)



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

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

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

Answer: D

NEW QUESTION 599
......