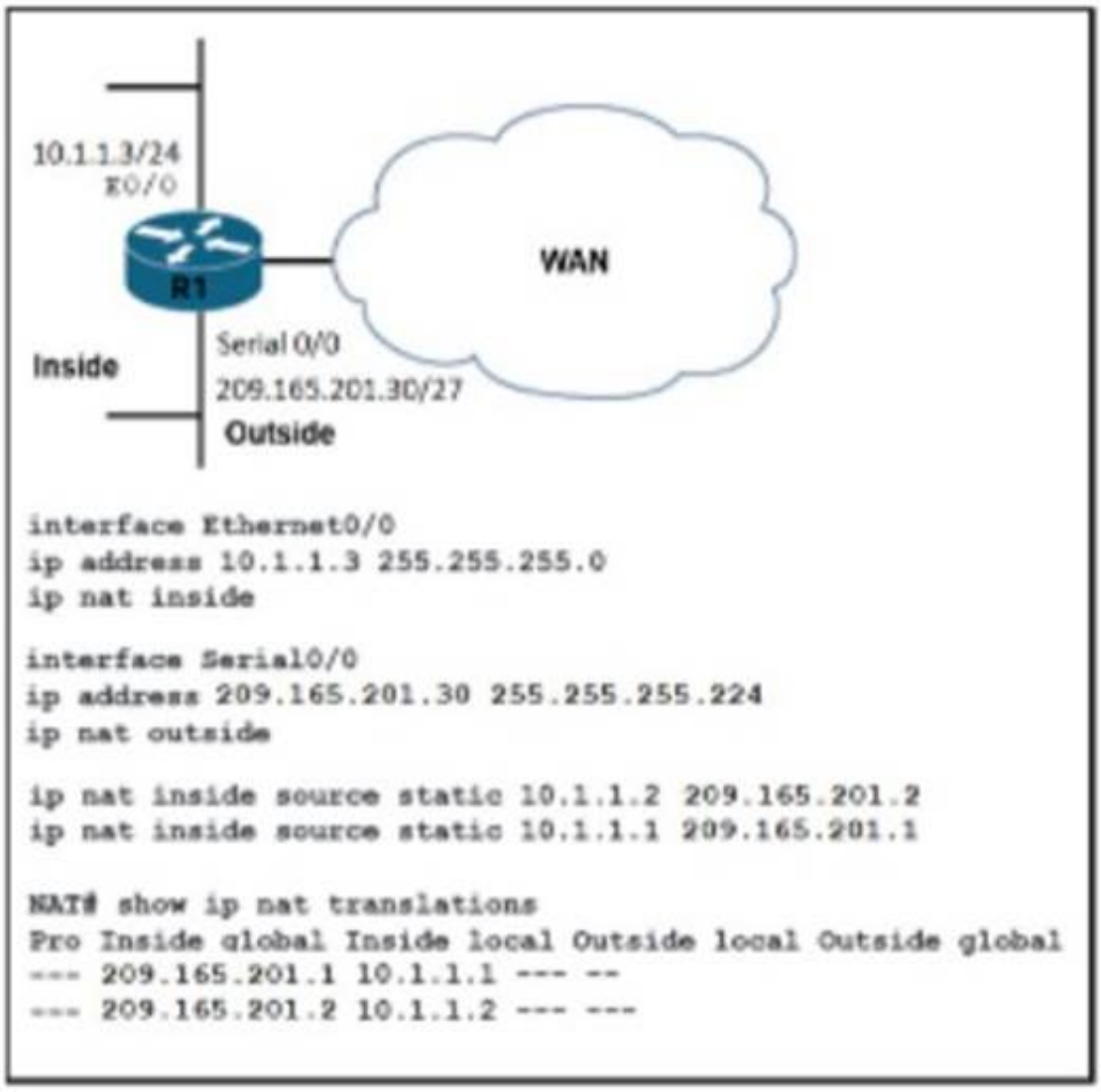
Cisco

Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies

NEW QUESTION 1
- (Topic 4)

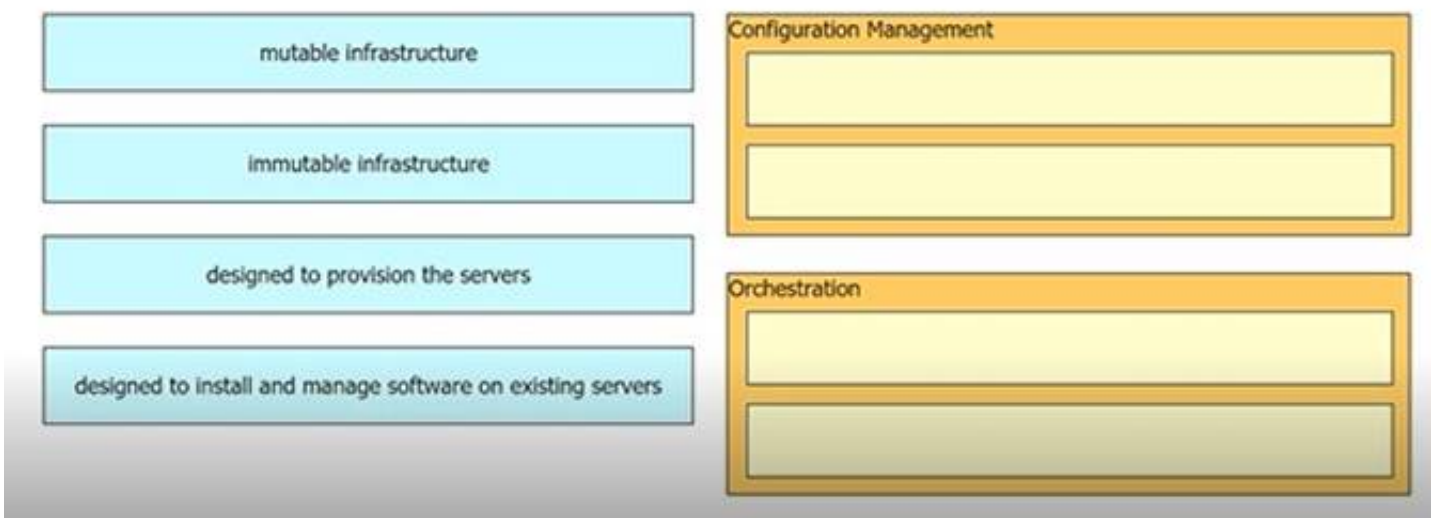


Refer to the exhibit. What are two results of the NAT configuration? (Choose two.)

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

Answer: BC

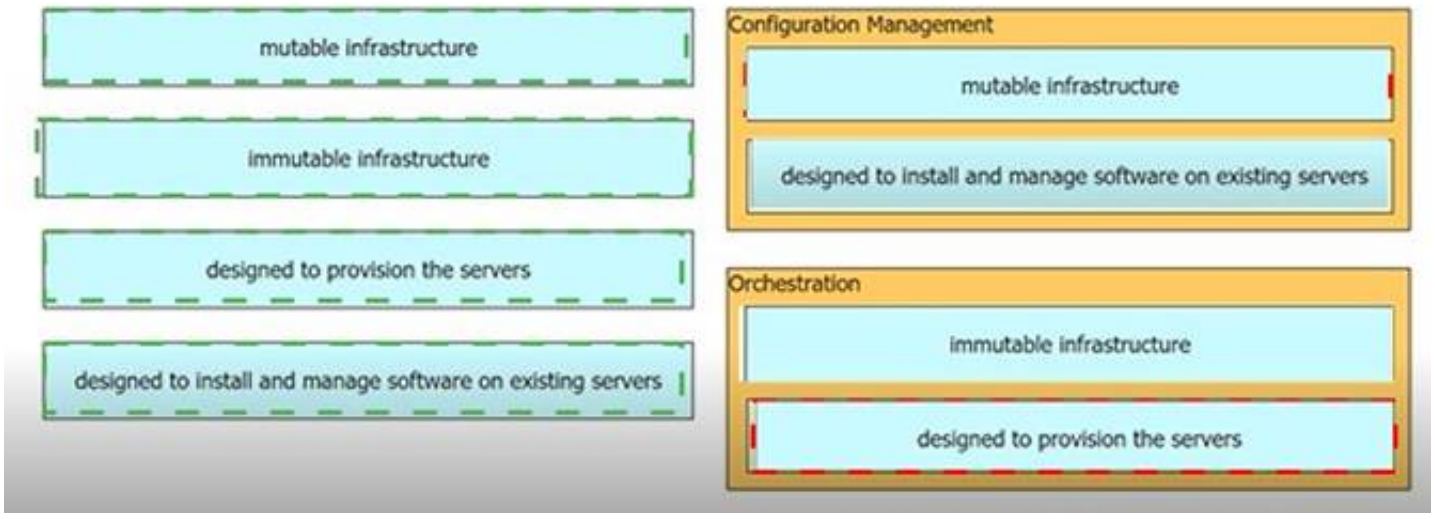
NEW QUESTION 2
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the orchestration tool classifications on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 3
- (Topic 4)
Refer to the exhibit.

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

These commands have been added to the configuration of a switch Which command flags an error if it is added to this configuration?

A. monitor session 1 source interface port-channel 6
B. monitor session 1 source vlan 10
C. monitor session 1 source interface FatEtheret0/1 x
D. monitor session 1 source interface port-channel 7,port-channel8

Answer: B

NEW QUESTION 4
- (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 5
- (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 6
- (Topic 4)
Refer to the exhibit.

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

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

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

DSW1#sh spanning-tree mst

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

!
... output omitted

!
```

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

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

Answer: DE

NEW QUESTION 7
- (Topic 4)

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

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

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

Answer: A

NEW QUESTION 8
- (Topic 4)
An engineer must protect the password for the VTY lines against over-the-shoulder attacks. Which configuration should be applied?

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

Answer: A

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

NEW QUESTION 9
- (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 10
- (Topic 4)
Which JSON script is properly formatted?
A)

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

B)

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

C)

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

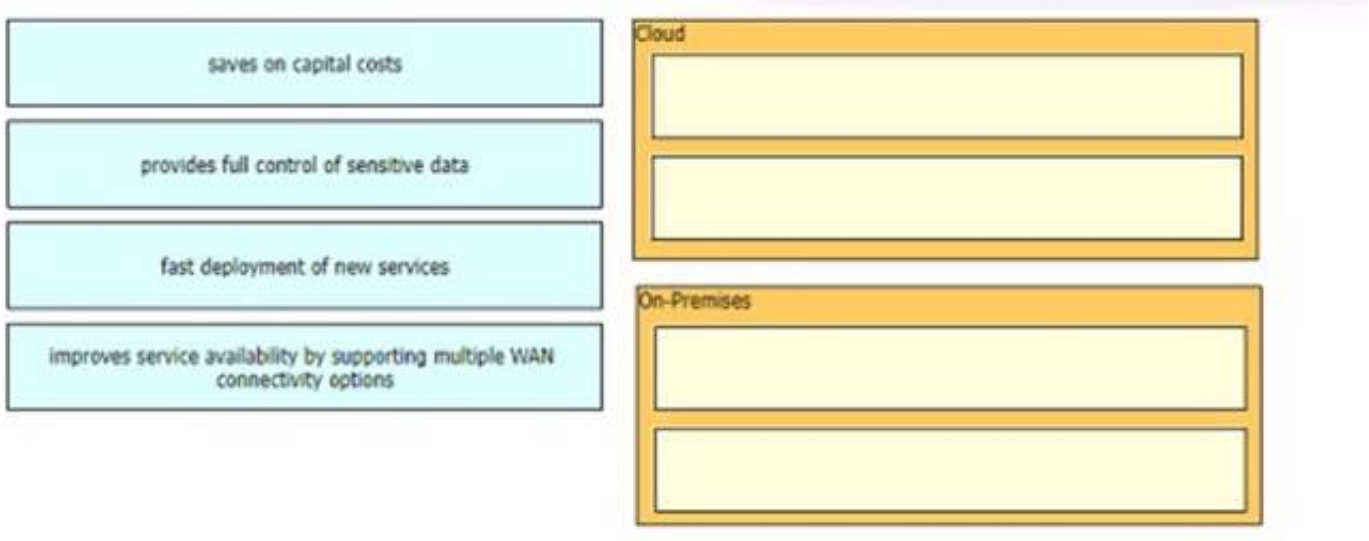
D)

```
[
   "class":{

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

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

Answer: B

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

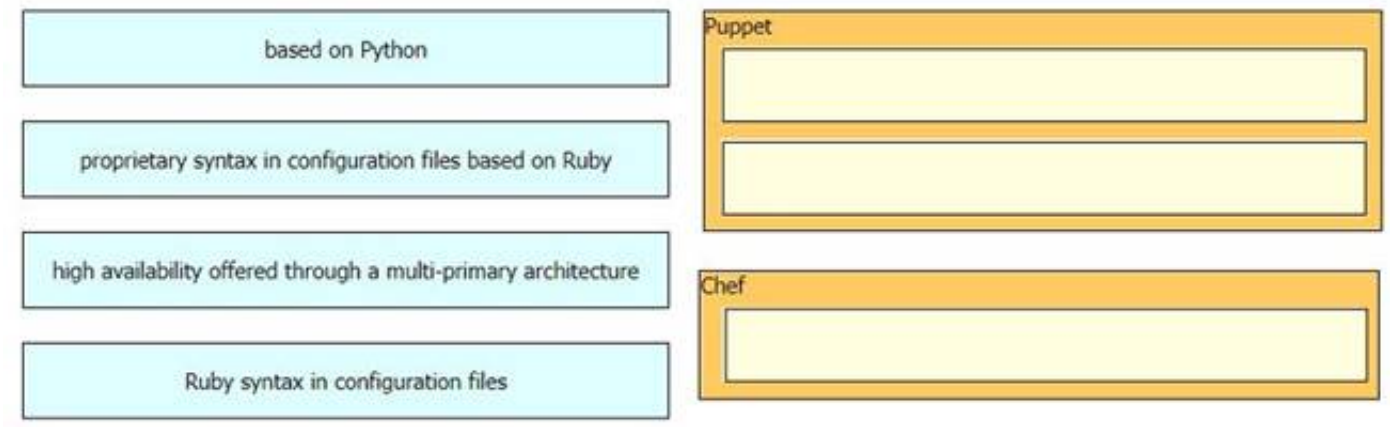


A. Mastered
B. Not Mastered

Answer: A

Explanation:
CLOUD1 and 3ON-PREMISES2 and 4

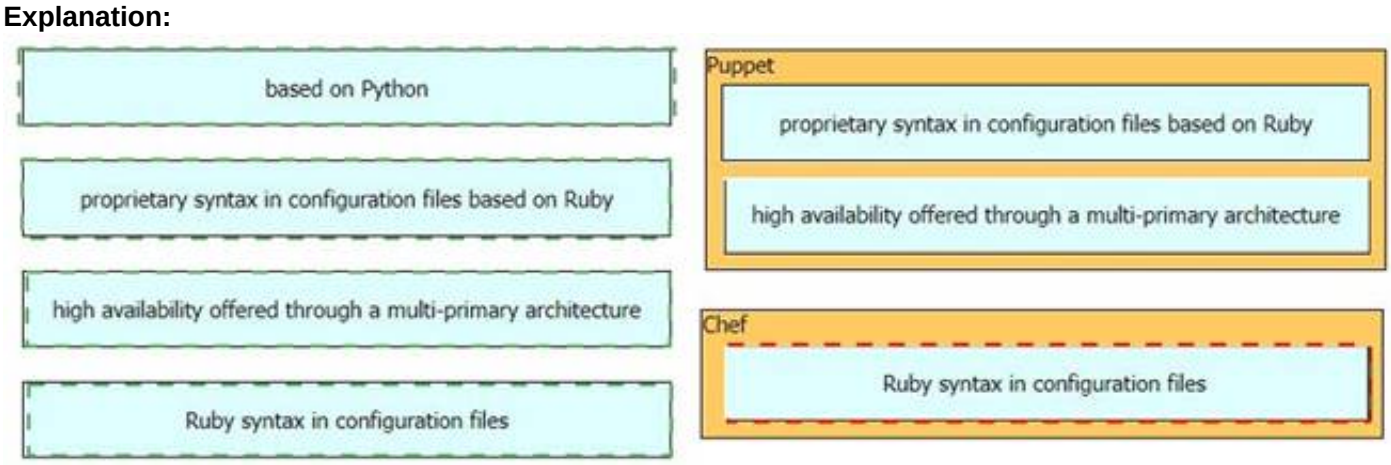
NEW QUESTION 14
DRAG DROP - (Topic 4)
Drag and drop the automation characteristics from the left onto the corresponding tools on the right. Not all options are used.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 18
- (Topic 4)

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

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

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

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

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

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

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

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

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

Answer: BE

NEW QUESTION 23
- (Topic 4)
An engineer must use flexible NetFlow on a group of switches. To prevent overloading of the flow collector, if the flow is idle for 20 seconds, the flow sample should be exported. Which command set should be applied?
A)

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

B)

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

C)

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

D)

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

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

Answer: C

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

NEW QUESTION 25
- (Topic 4)
When does a Cisco StackWise primary switch lose its role?

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

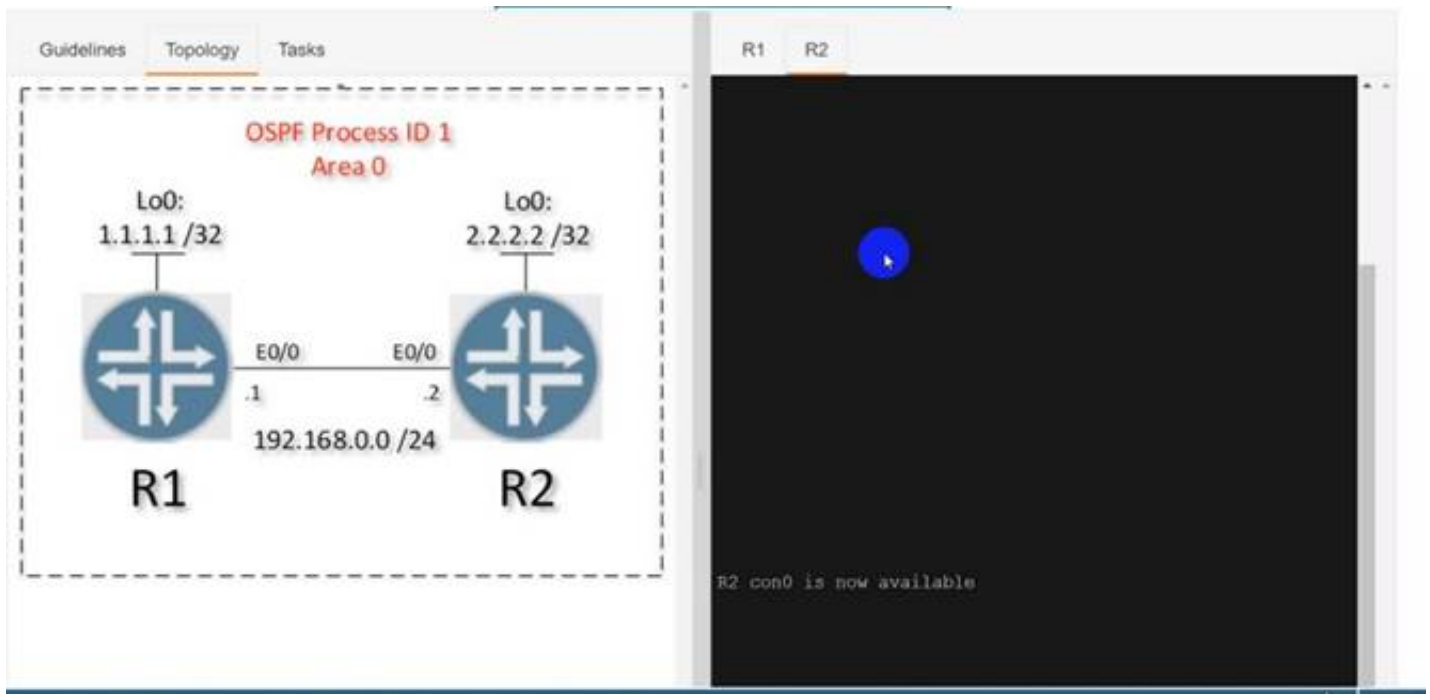
Answer: C

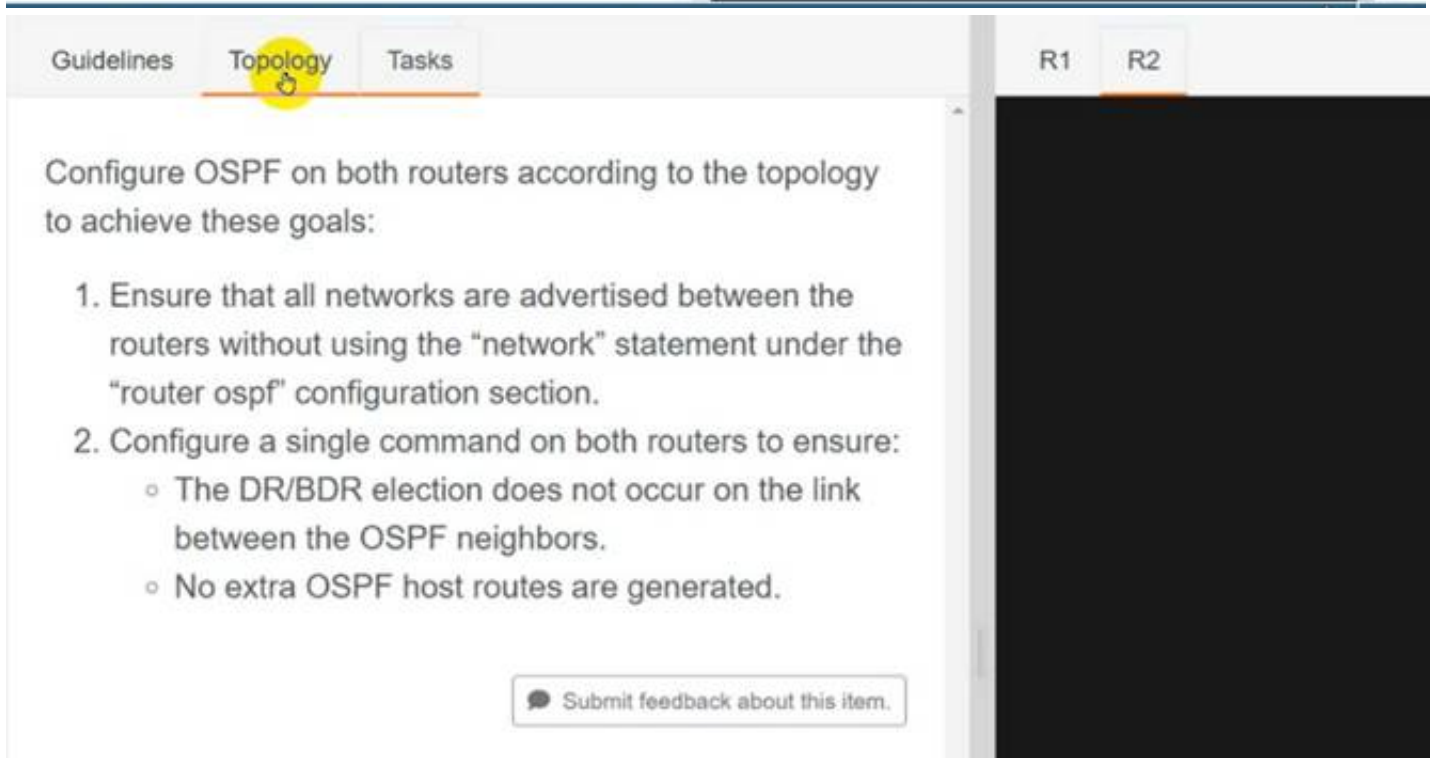
NEW QUESTION 30
- (Topic 4)
In a Cisco StackWise Virtual environment, which planes are virtually combined in the common logical switch?

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

Answer: C

NEW QUESTION 33
SIMULATION - (Topic 4)
Simulation 04





A. Mastered
B. Not Mastered

Answer: A

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

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

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

```
R1#sh ip ospf neighbor

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

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


                Base Topology (MTID 0)


    Area BACKBONE(0)

    Intra-area Route List

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

    First Hop Forwarding Gateway Tree

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

NEW QUESTION 38
- (Topic 4)
How does SSO work with HSRP to minimize network disruptions?

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

Answer: D

NEW QUESTION 40
- (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 45
- (Topic 4)
How does Protocol Independent Multicast function?

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

Answer: C

NEW QUESTION 50
- (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 53
- (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 56
- (Topic 4)
Based on the router's API output in JSON format below, which Python code will display the value of the “hostname" key?

```
{
    "response": [{
        "family": "Switches",
        "macAddress": "00:42:50:62:99:00",
        "hostname": "SwitchIDF14",
        "upTime": "352 days, 6:17:26:10",
        "lastUpdated": "2020-07-12 21:15:29"
    }]
}
```

```
json_data = json.loads(response.text)
print(json_data[response][0][hostname])
```

```
json_data = json.loads(response.text)
print(json_data['response']['family']['hostname'])
```

```
json_data = response.json()
print(json_data['response'][0]['hostname'])
```

```
json_data = response.json()
print(json_data['response'][family][hostname'])
```

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

Answer: B

NEW QUESTION 61
- (Topic 4)
Which behavior can be expected when the HSRP versions is changed from 1 to 2?

A. Each HSRP group reinitializes because the virtual MAC address has changed.
B. No changes occur because version 1 and 2 use the same virtual MAC OUI.
C. Each HSRP group reinitializes because the multicast address has changed.
D. No changes occur because the standby router is upgraded before the active router.

Answer: A

NEW QUESTION 66
- (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 71
- (Topic 2)
Refer to the exhibit.

```
DSW2#sh spanning-tree vlan 10

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

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

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

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

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

Answer: A

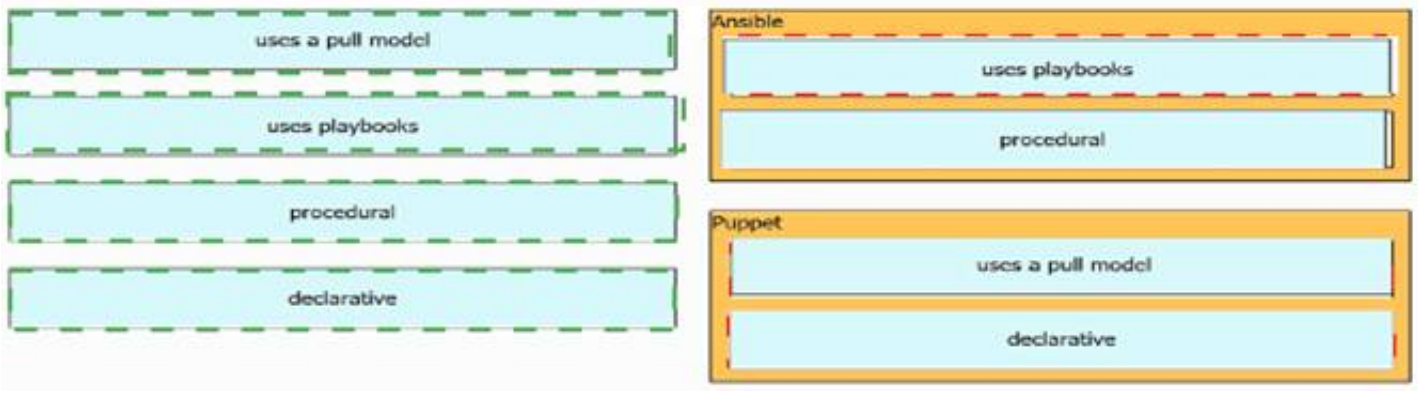
Explanation:
From the output we see DSW2 is running in RSTP mode (in fact Rapid PVST+ mode as Cisco does not support RSTP alone). When a new switch running PVST+ mode is added to the topology, they keep running the old STP instances as RSTP (in fact Rapid PVST+) is compatible with PVST+.

NEW QUESTION 73
DRAG DROP - (Topic 2)
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 78
- (Topic 2)
Refer to the exhibit.

```
DSW1#sh spanning-tree vlan 20

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

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

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

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

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

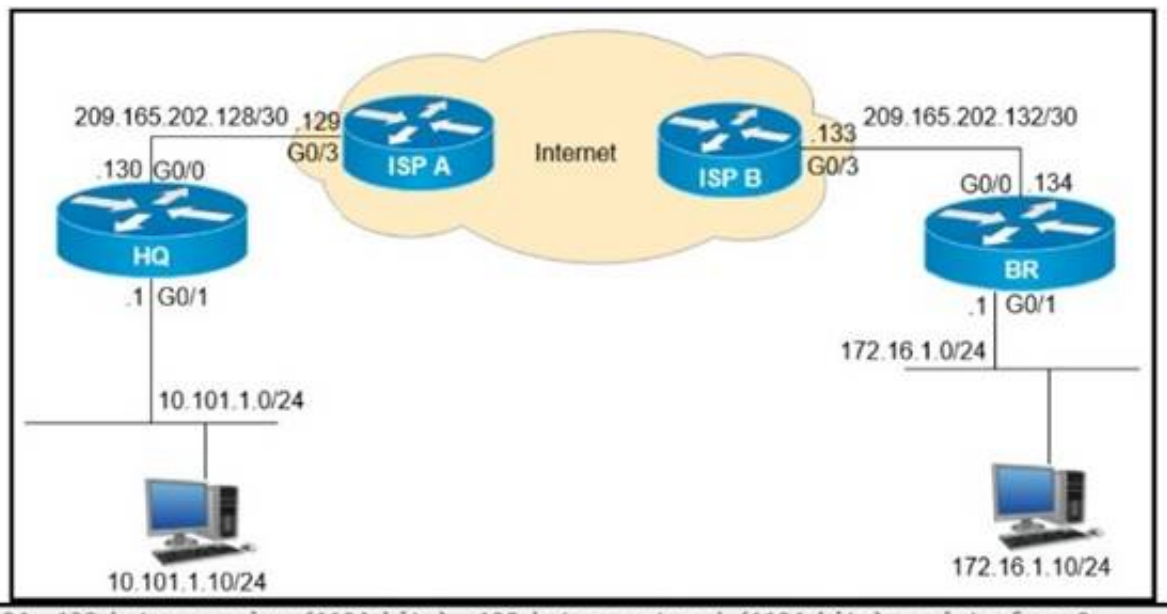
Answer: C

NEW QUESTION 83
- (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 85
- (Topic 2)
Refer to the exhibit.



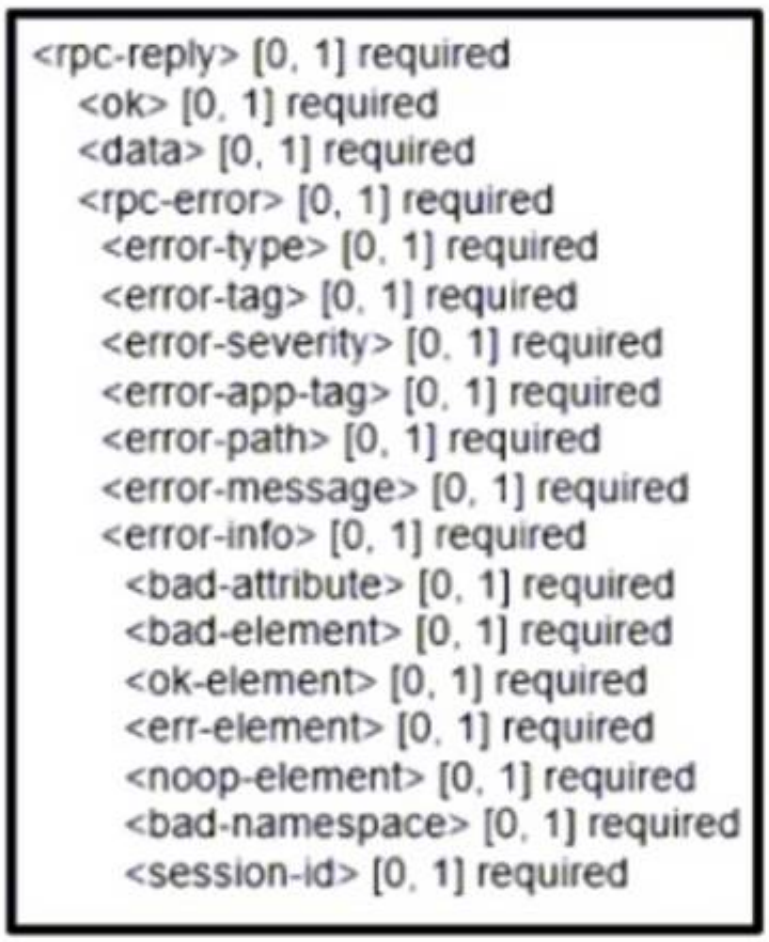

```
> Frame 24: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
> Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 50:00:00:02:00:01 (50:00:00:02:00:01)
> Internet Protocol Version 4, Src: 209.165.202.130, Dst: 209.165.202.134
> Generic Routing Encapsulation (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 89
- (Topic 2)



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 92
- (Topic 2)
AN engineer is implementing a route map to support redistribution within BGP. The route map must configured to permit all unmatched routes. Which action must the engineer perform to complete this task?

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

Answer: D

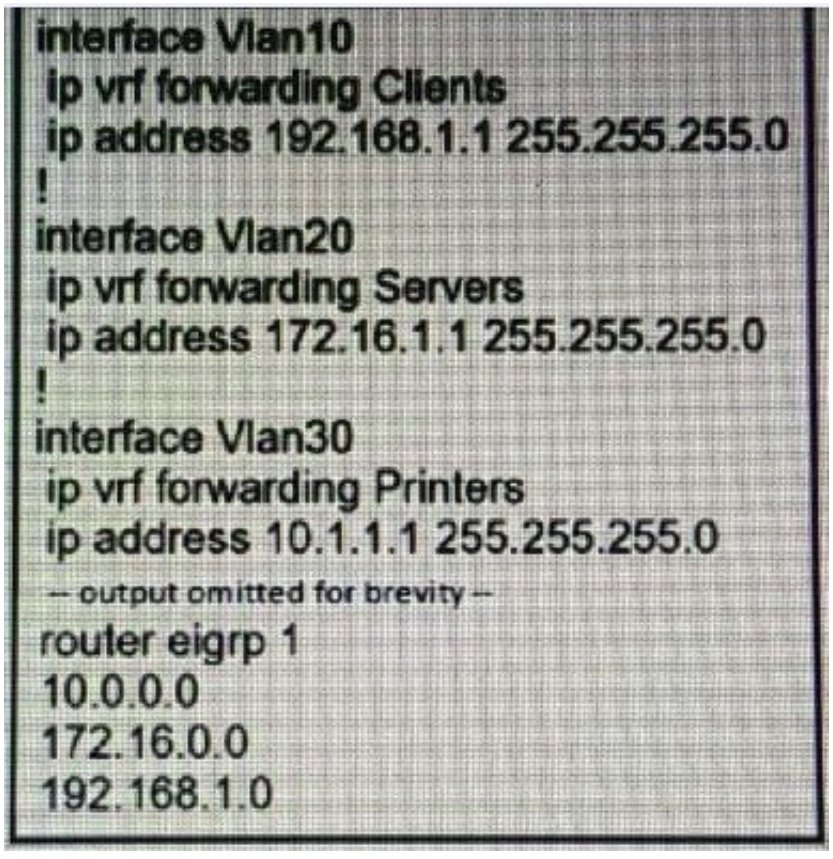
NEW QUESTION 94
- (Topic 2)
In a Cisco SD-WAN solution, which two functions are performed by OMP? (Choose two.)

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

Answer: AB

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

NEW QUESTION 98
- (Topic 2)


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

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

A)

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

B)

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

C)

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

D)

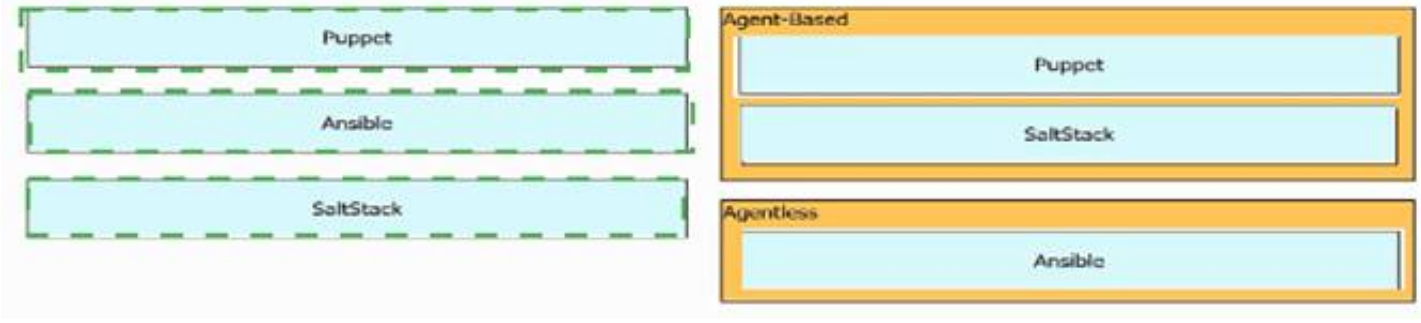
```
router eigrp 1
network 10.0.0.0 255.0.0.0
network 172.16.0.0 255.255.0.0
network 192.168.1.0 255.255.0.0
```

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

Answer: C

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

NEW QUESTION 99
DRAG DROP - (Topic 2)
Drag and drop the tools from the left onto the agent types on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

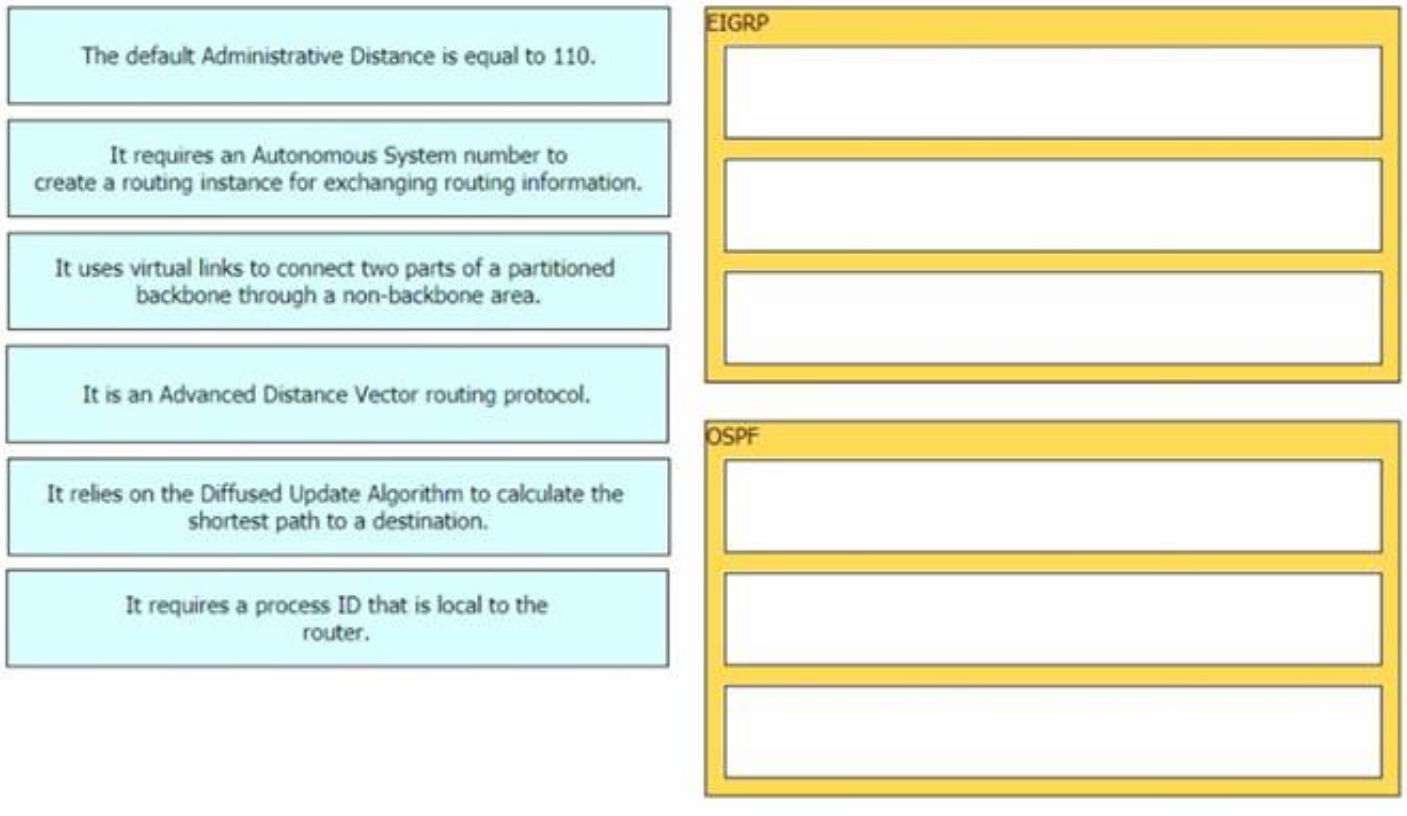
NEW QUESTION 102
- (Topic 2)
Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

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

Answer: D

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

NEW QUESTION 106
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the routing protocols they describe on the right.

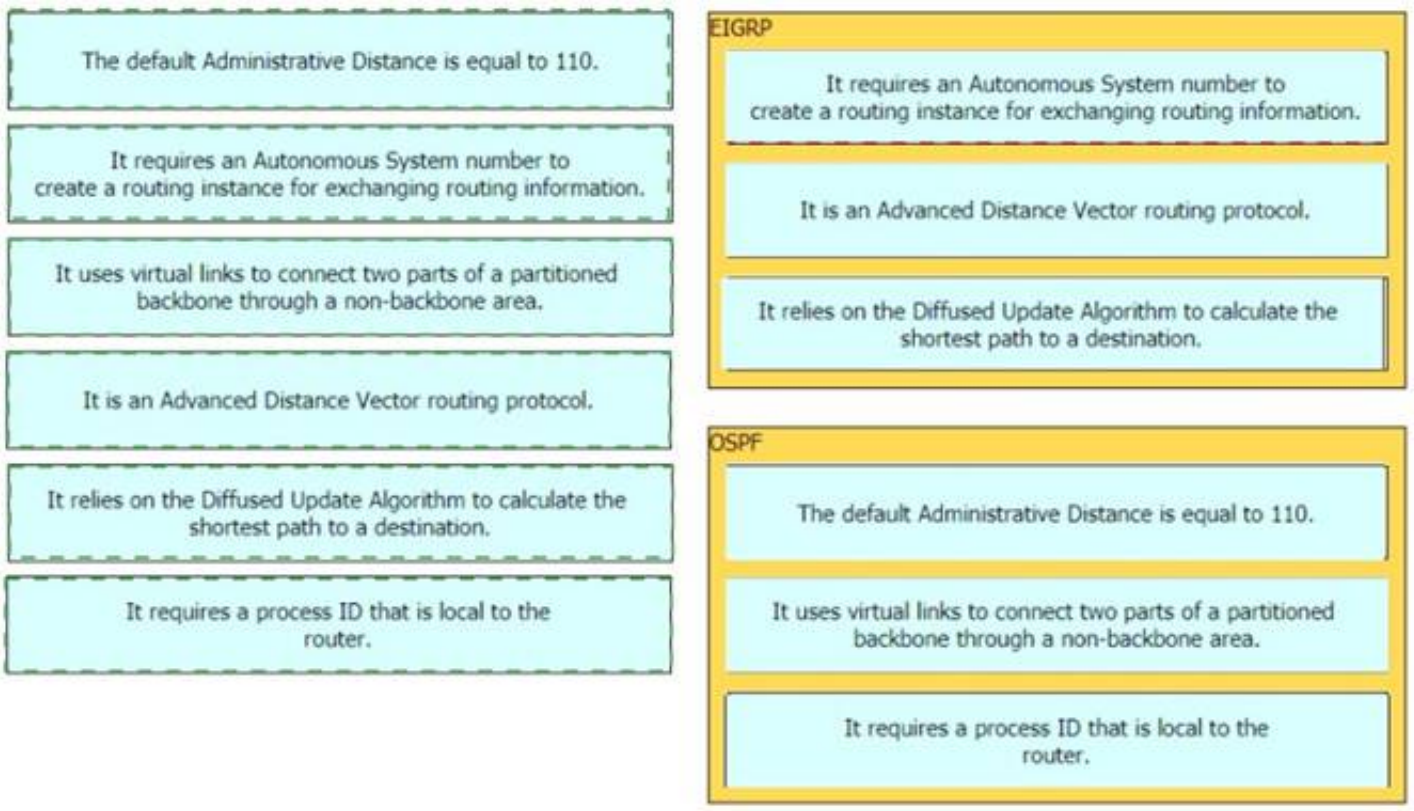


A. Mastered

B. Not Mastered

Answer: A

Explanation:



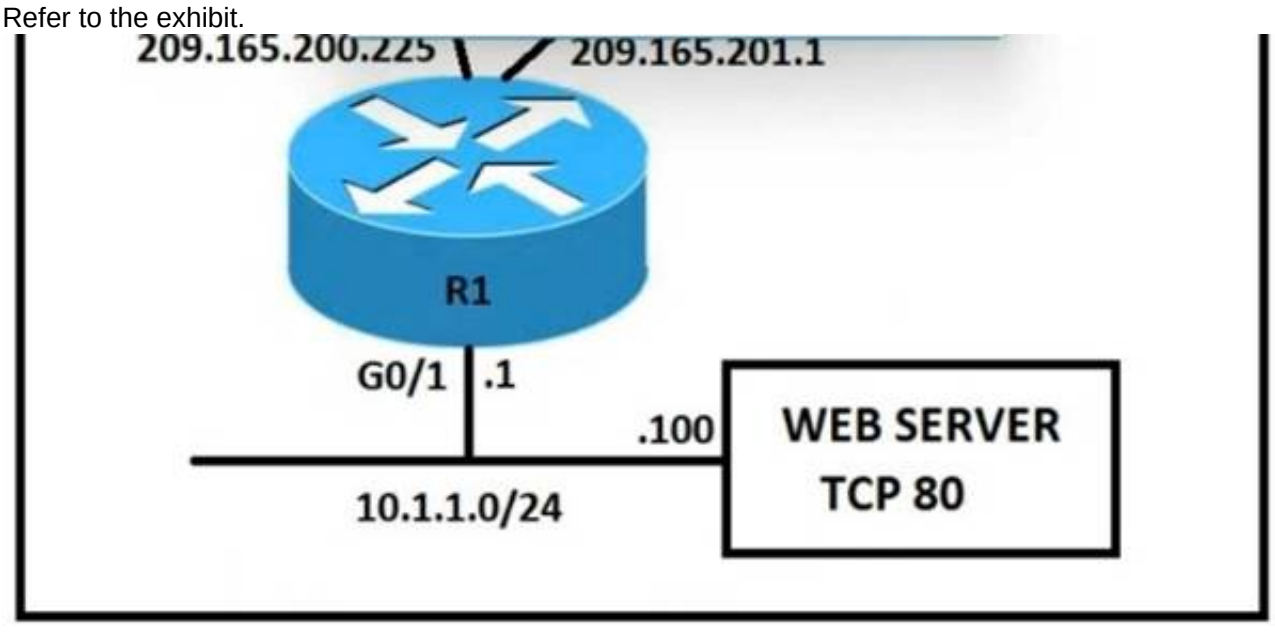
NEW QUESTION 108
- (Topic 2)
What is the difference between a RIB and a FIB?

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

Answer: D

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

NEW QUESTION 111
- (Topic 2)
Refer to the exhibit.



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

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

Answer: B

NEW QUESTION 115
- (Topic 2)
Refer to the exhibit.

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

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

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

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

B)

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

C)

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

D)

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

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

Answer: C

NEW QUESTION 119
- (Topic 2)
An engineer configures GigabitEthernet 0/1 for VRRP group 115. The router must assume the primary role when it has the highest priority in the group. Which command set is required to complete this task?

```
interface GigabitEthernet0/1
ip address 10.10.10.2 255.255.255.0
vrrp 115 ip 10.10.10.1
vrrp 115 authentication 406530697

Router(config-if)# vrrp 115 priority 100

Router(config-if)# standby 115 priority 100
Router(config-if)# standby 115 preempt

Router(config-if)# vrrp 115 track 1 decrement 10
Router(config-if)# vrrp 115 preempt

Router(config-if)# vrrp 115 track 1 decrement 100
Router(config-if)# vrrp 115 preempt
```

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

Answer: C

NEW QUESTION 123

- (Topic 2)
Refer to the exhibit.

An engineer is troubleshooting an application running on Apple phones. The application Is receiving incorrect QoS markings. The systems administrator confirmed that ail configuration profiles are correct on the Apple devices. Which change on the WLC optimizes QoS for these devices?

A. Enable Fastlane
B. Set WMM to required
C. Change the QoS level to Platinum
D. Configure AVC Profiles

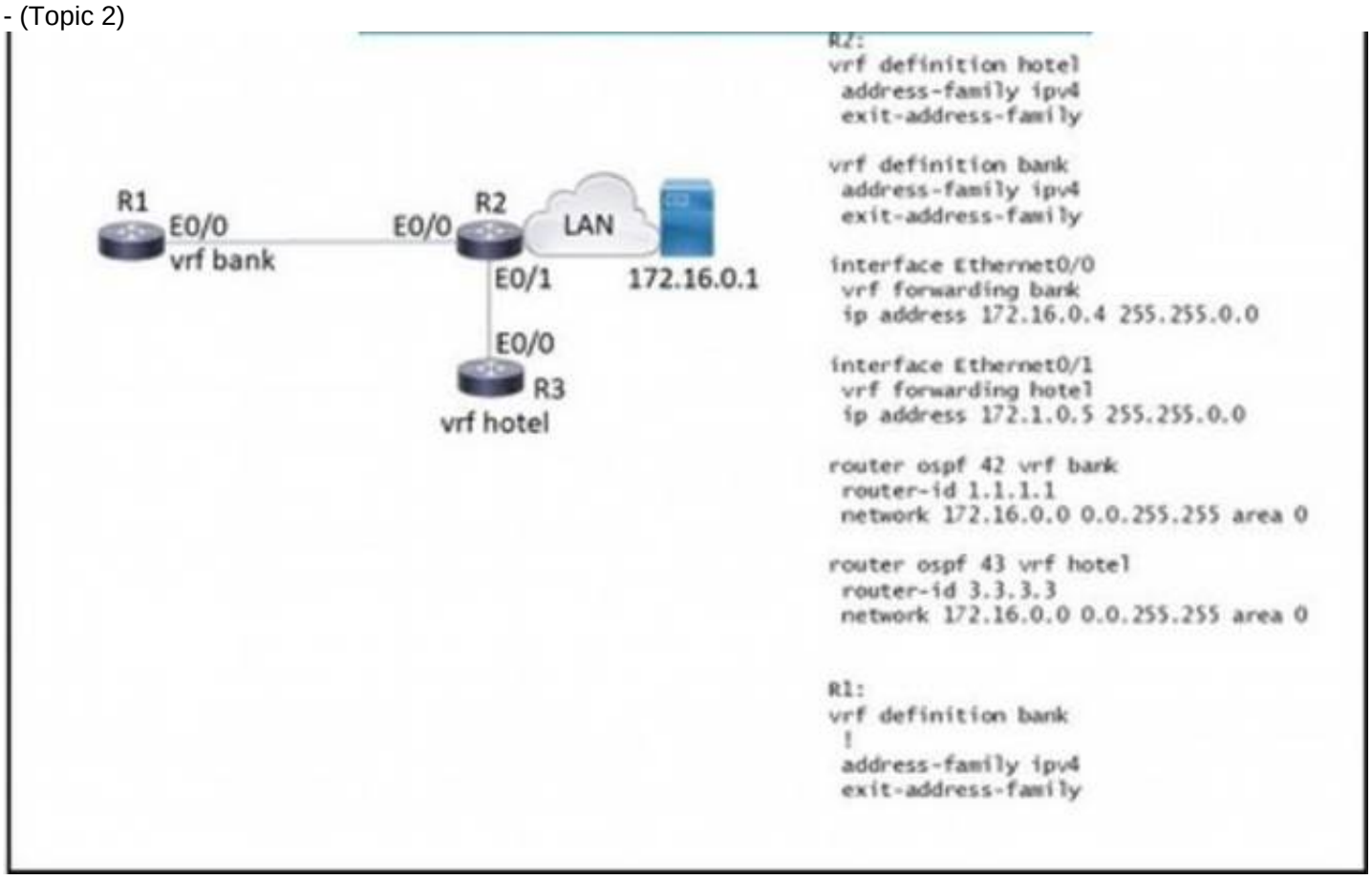
Answer: C

NEW QUESTION 128
- (Topic 2)
When firewall capabilities are considered, which feature is found only in Cisco next- generation firewalls?

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

Answer: A

NEW QUESTION 132
- (Topic 2)



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 134
- (Topic 2)
Which two actions, when applied in the LAN network segment, will facilitate Layer 3 CAPWAP discovery for lightweight AP? (Choose two.)

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

Answer: CE

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

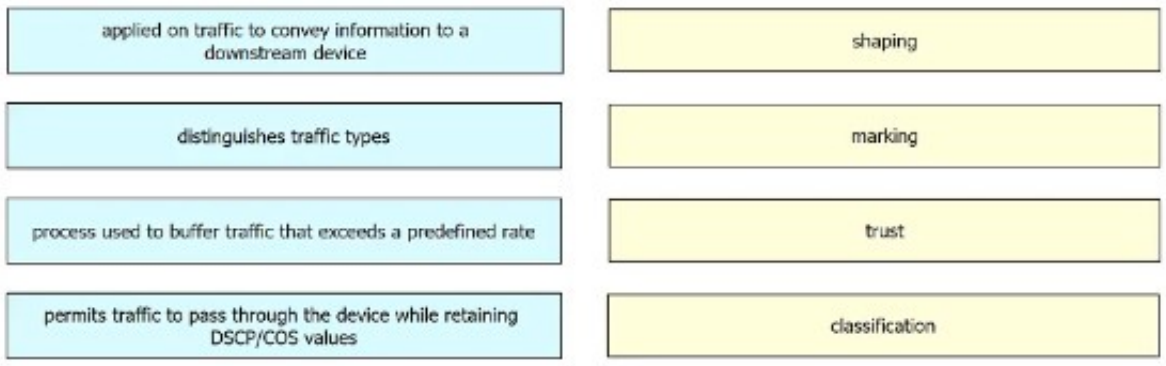
NEW QUESTION 137
- (Topic 2)
An engineer must create an EEM applet that sends a syslog message in the event a change happens in the network due to trouble with an OSPF process. Which action should the engineer use?

```
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

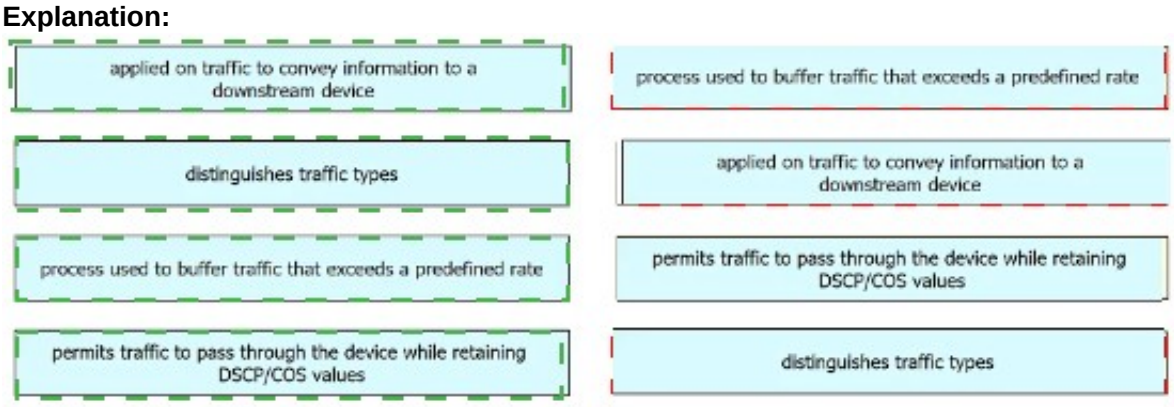
NEW QUESTION 140
DRAG DROP - (Topic 2)
Drag and drop the descriptions from the left onto the QoS components they describe on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 145
- (Topic 2)
A customer wants to use a single SSID to authenticate IoT devices using different passwords. Which Layer 2 security type must be configured in conjunction with Cisco ISE to achieve this requirement?

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

Answer: D

NEW QUESTION 150
- (Topic 2)
Refer to the exhibit.

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

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

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

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

D. Interface GigabitEthernet2 is configured with IP address 10.10.10.1/24

Answer: D

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

```
Switch1#show lacp internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi0/0     SP      hot-sby   20            0x1       0x1     0x1         0x5
Gi0/1     SA      bndl      15            0x1       0x1     0x2         0x3C
```

An engineer attempts to bundle interface Gi0/0 into the port channel, but it does not function as expected. Which action resolves the issue?

A. Configure channel-group 1 mode active on interface Gi0/0.
B. Configure no shutdown on interface Gi0/0
C. Enable fast LACP PDUs on interface Gi0/0.
D. Set LACP max-bundle to 2 on interface Port-channeM

Answer: D

NEW QUESTION 154
- (Topic 2)
What is the wireless received signal strength indicator?

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

Answer: D

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

NEW QUESTION 158
- (Topic 2)
Refer to the exhibit.

Which JSON syntax is derived from this data?
A)

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

B)

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

C)

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

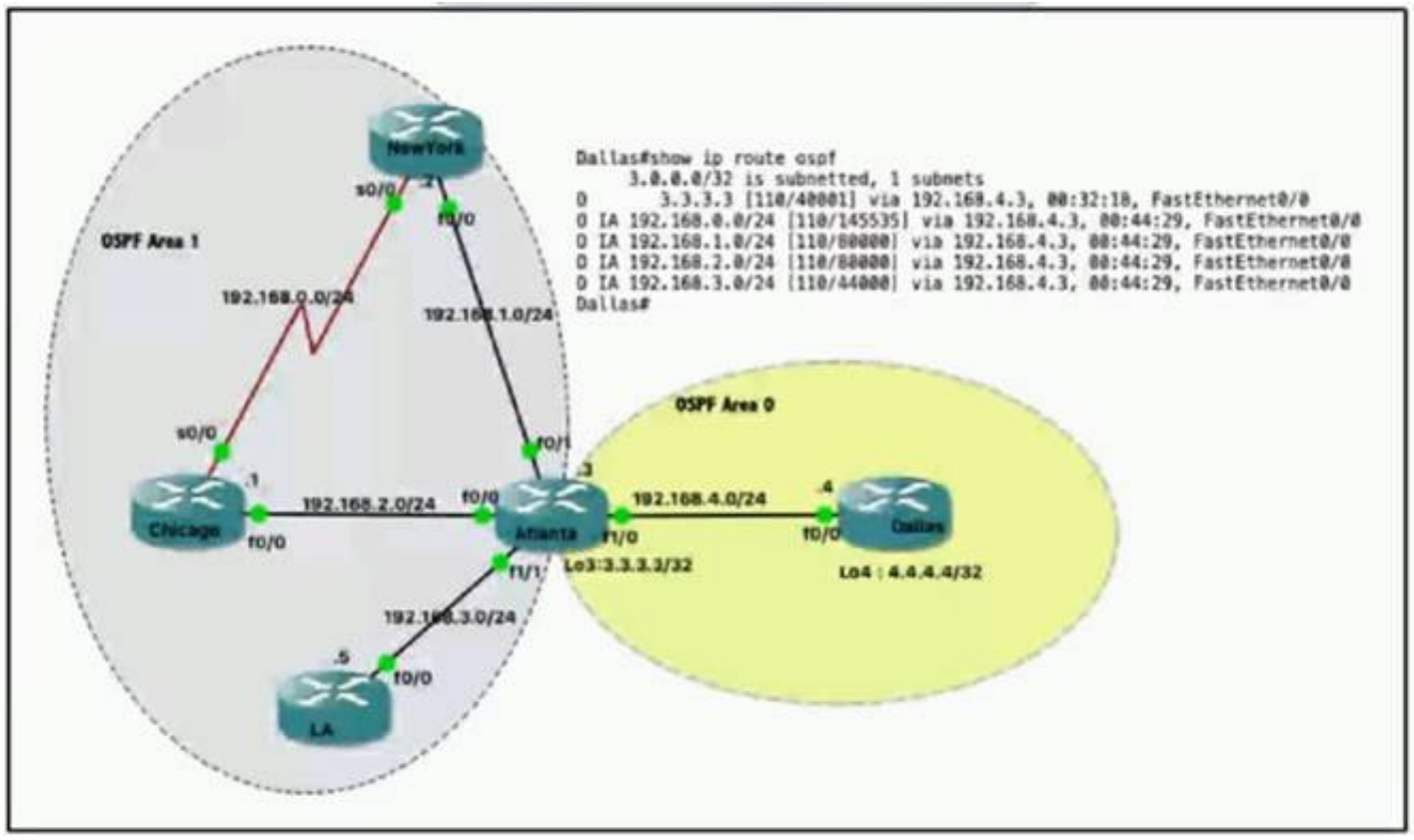
D)

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

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

Answer: D

NEW QUESTION 159
- (Topic 2)
Refer to the exhibit.

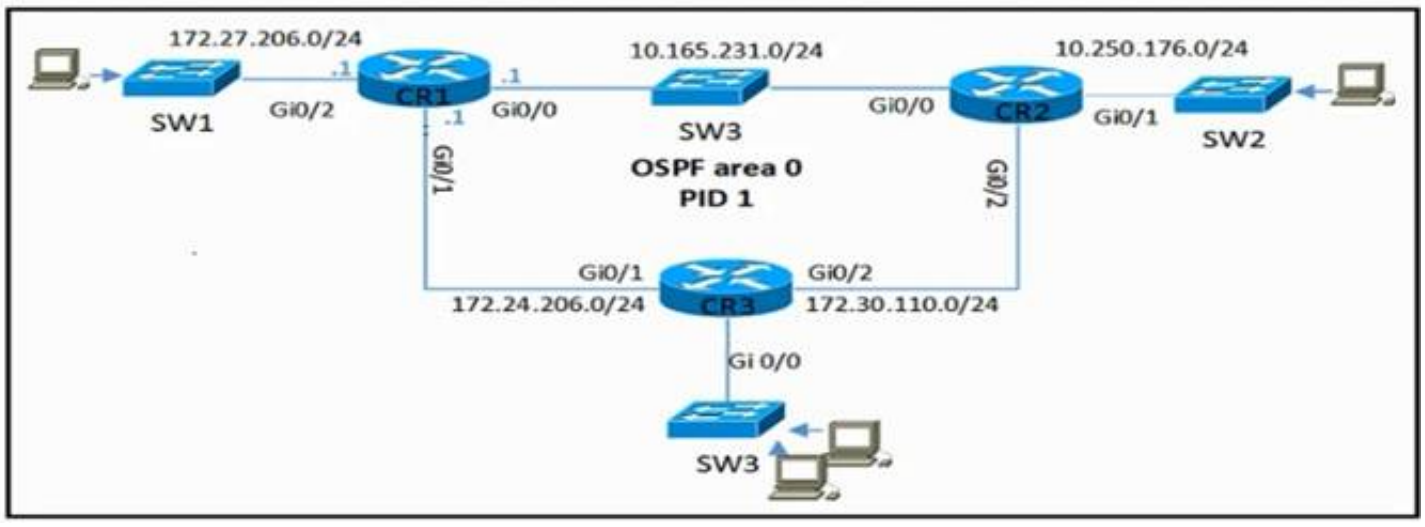


Which command when applied to the Atlanta router reduces type 3 LSA flooding into the backbone area and summarizes the inter-area routes on the Dallas router?

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

Answer: C

NEW QUESTION 163
- (Topic 2)
Refer to the exhibit.



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

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

B)

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

C)

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

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

D)

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

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

Answer: D

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

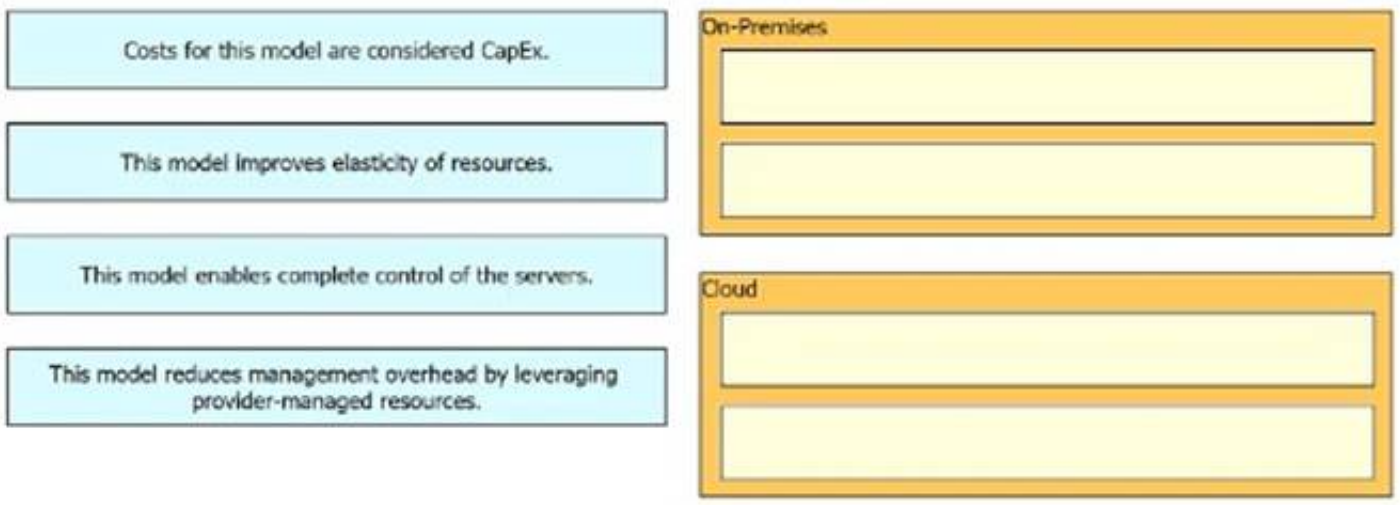
```
logging buffered discriminator Disc1
logging monitor discriminator Disc1
logging host 10.1.55.237 discriminator Disc1
```

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

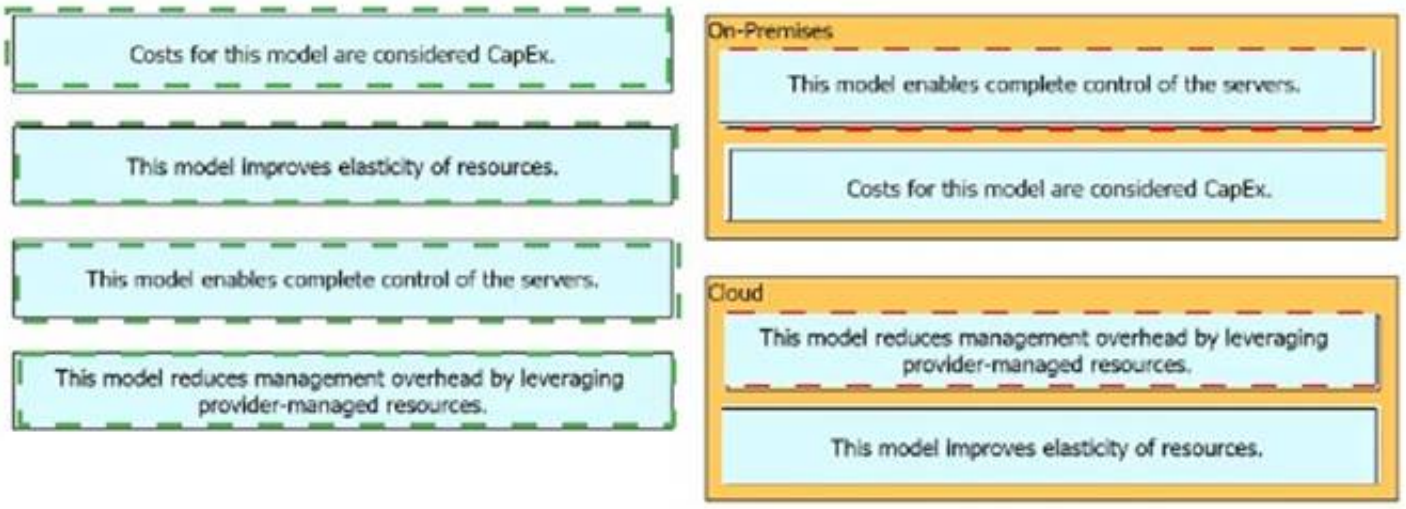
NEW QUESTION 169
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the infrastructure deployment models on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 172
- (Topic 2)
Refer to the exhibit.

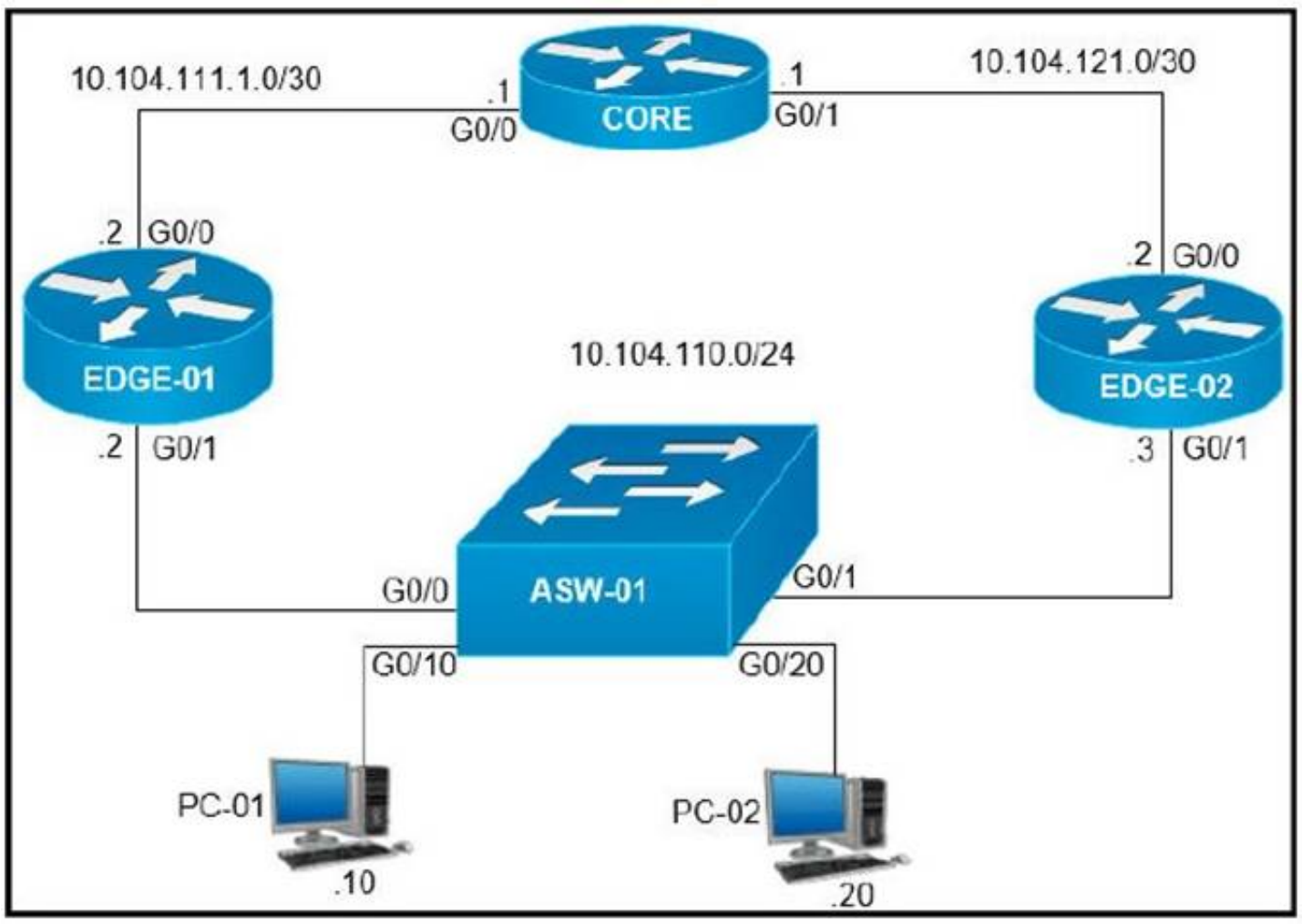
Cisco DNA Center has obtained the username of the client and the multiple devices that the client is using on the network. How is Cisco DNA Center getting these context details?

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

Answer: A

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

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



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

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

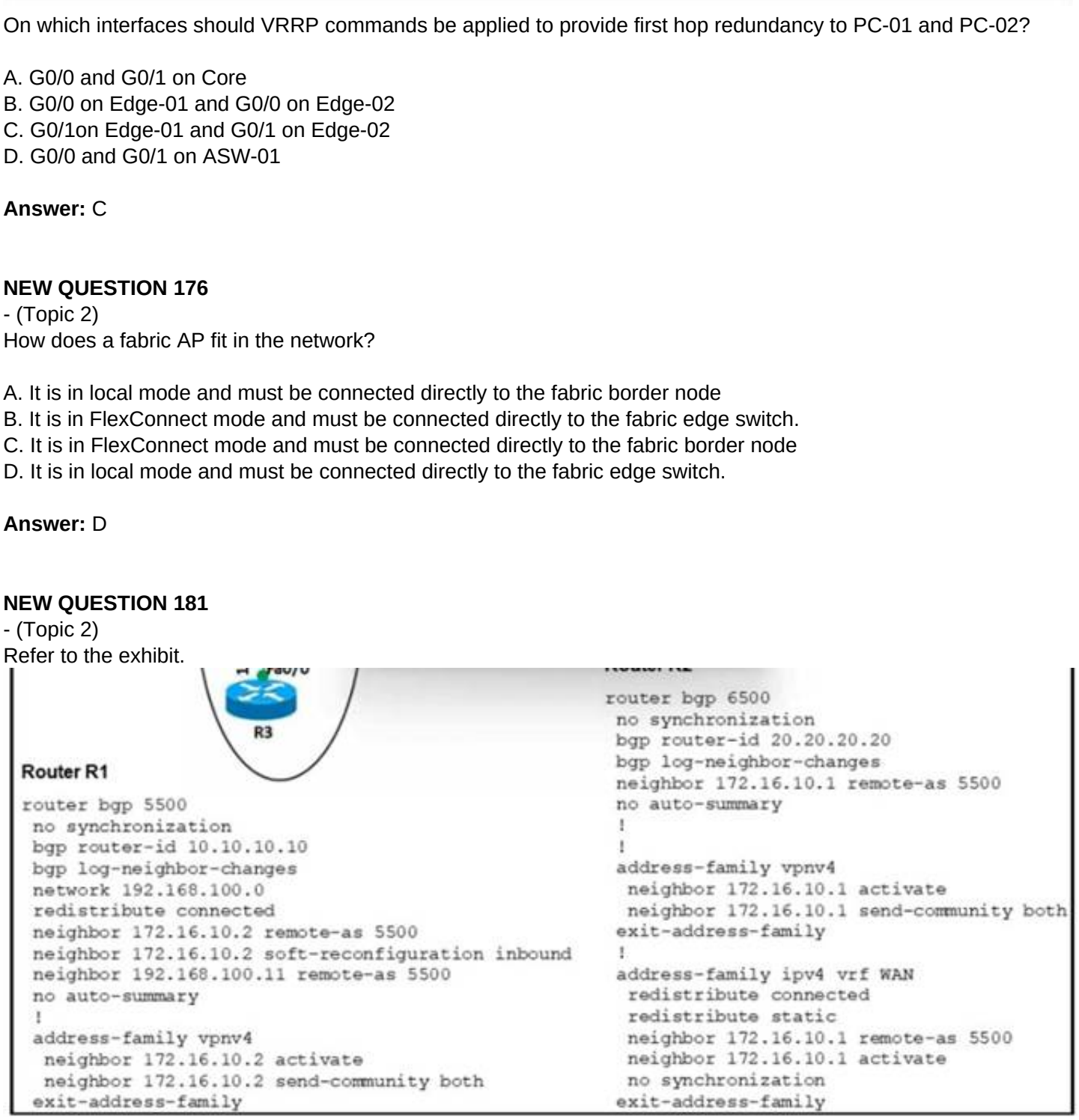
Answer: C

NEW QUESTION 176
- (Topic 2)
How does a fabric AP fit in the network?

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

Answer: D

NEW QUESTION 181
- (Topic 2)
Refer to the exhibit.



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

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

Answer: D

NEW QUESTION 184

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

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

Answer: B

NEW QUESTION 187
- (Topic 1)
Which two mechanisms are available to secure NTP? (Choose two.)

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

Answer: DE

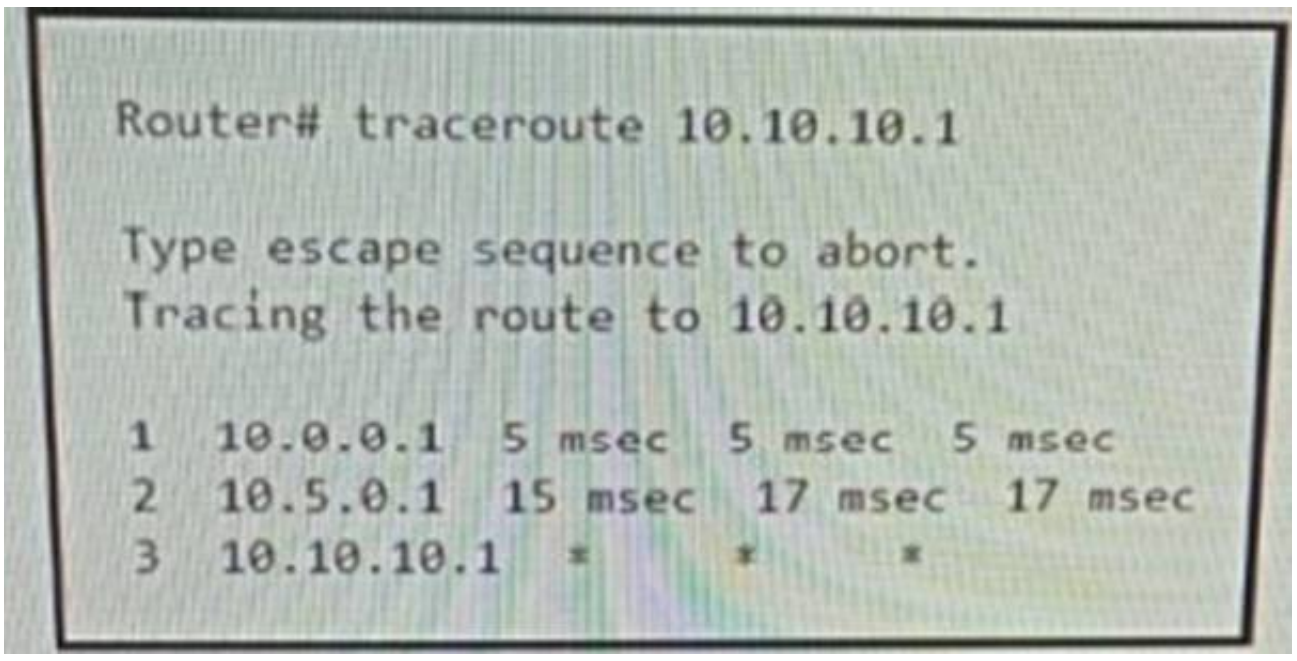
NEW QUESTION 190
- (Topic 1)
Which method of account authentication does OAuth 2.0 within REST APIs?

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 192
- (Topic 1)
Refer to the exhibit.



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

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

Answer: D

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

NEW QUESTION 193
- (Topic 1)

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

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

Answer: B

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

NEW QUESTION 194
- (Topic 1)
which entity is a Type 1 hypervisor?

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

Answer: C

NEW QUESTION 197
- (Topic 1)
What is the centralized control policy in a Cisco SD-WAN deployment?

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

Answer: B

NEW QUESTION 199
- (Topic 1)
How does Cisco Trustsec enable more access controls for dynamic networking
environments and data centers?

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

Answer: C

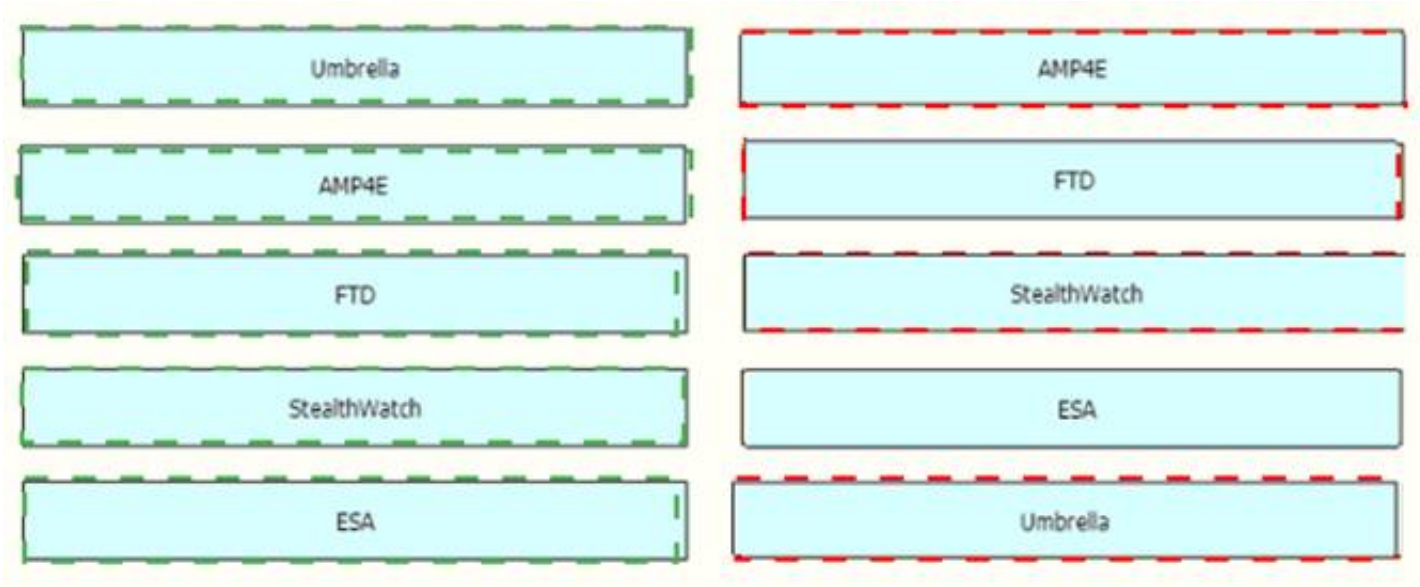
Explanation:
The Cisco TrustSec solution simplifies the provisioning and management of network access control through the use of software-defined segmentation to classify network traffic and enforce policies for more flexible access controls. Traffic classification is based on endpoint identity, not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

NEW QUESTION 204
DRAG DROP - (Topic 1)
Drag and drop the threat defense solutions from the left onto their descriptions on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

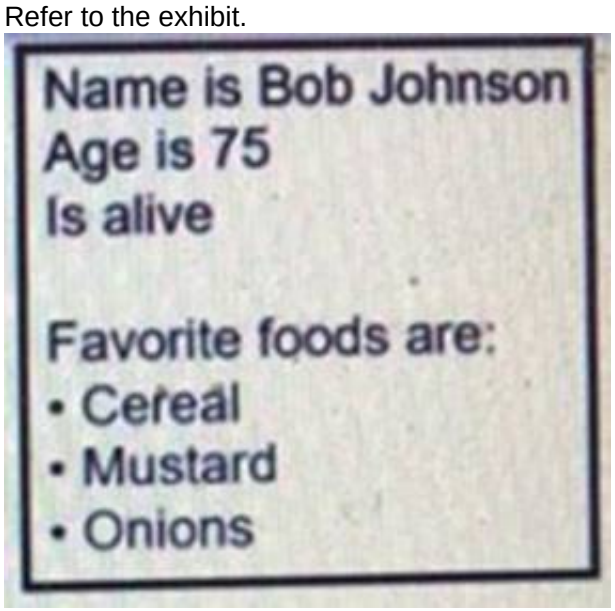


NEW QUESTION 207
- (Topic 1)
An engineer configures HSRP group 37. The configuration does not modify the default virtual MAC address. Which virtual MAC address does the group use?

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 211
- (Topic 1)
Refer to the exhibit.



What is the Json syntax that is formed from the data?

A. {Name: Bob Johnson, Age: 75, Alive: true, Favorite Foods: [Cereal, Mustard, Onions]}
B. {"Name": "Bob Johnson", "Age": 75, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "Onions"]}
C. {"˜Name': "˜Bob Johnson', "˜Age': 75, "˜Alive': True, "˜Favorite Foods': "˜Cereal', "˜Mustard', "˜Onions'}
D. {"Name": "Bob Johnson", "Age": Seventyfive, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "Onions"]}

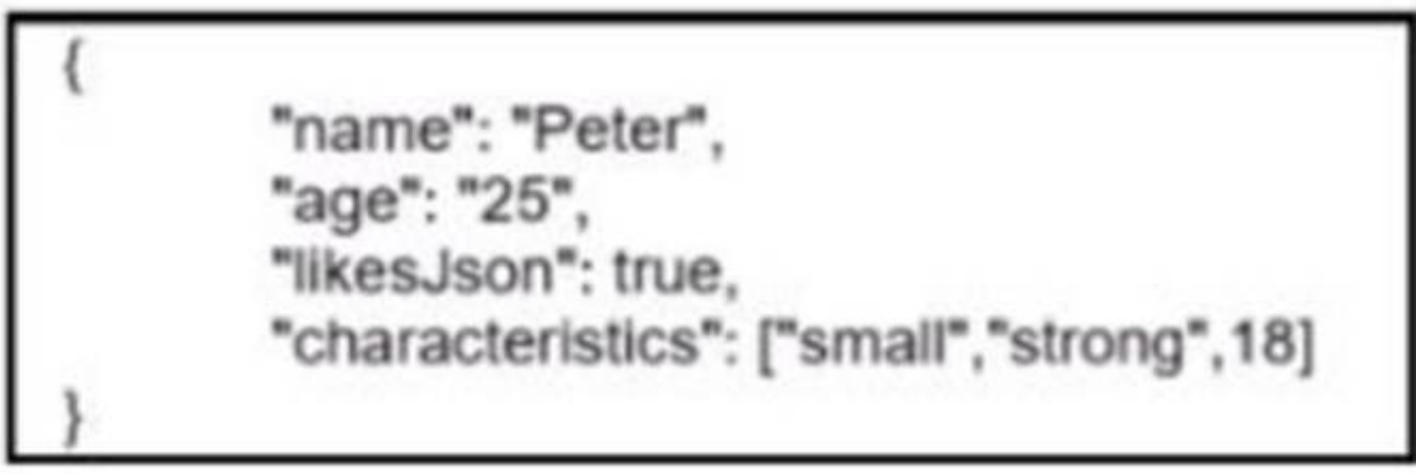
Answer: B

NEW QUESTION 216
- (Topic 1)
When configuration WPA2 Enterprise on a WLAN, which additional security component configuration is required?

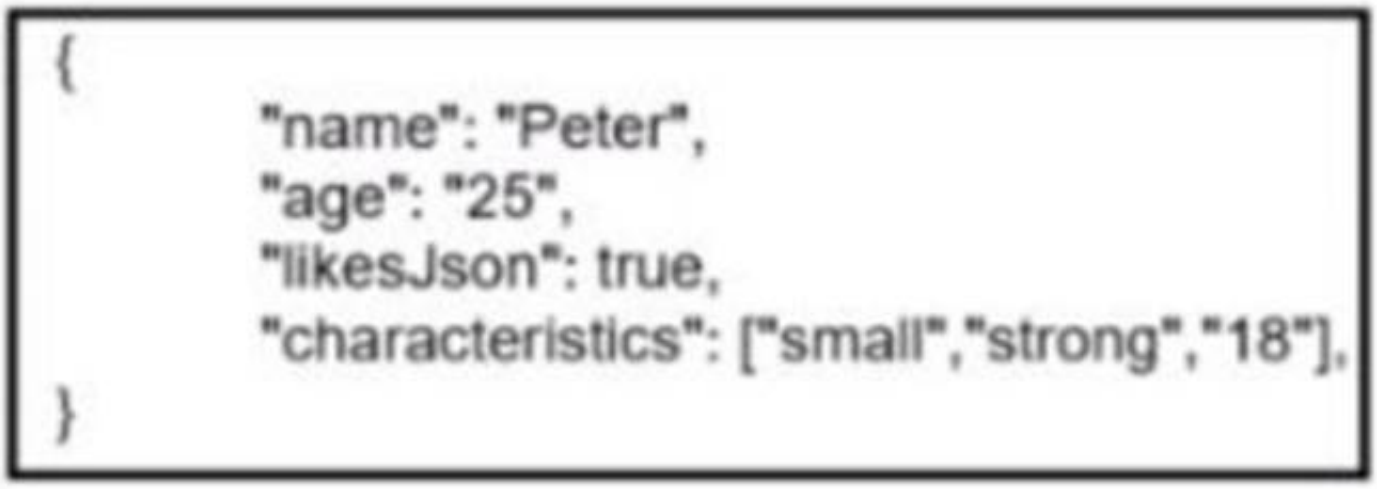
A. NTP server
B. PKI server
C. RADIUS server
D. TACACS server

Answer: C

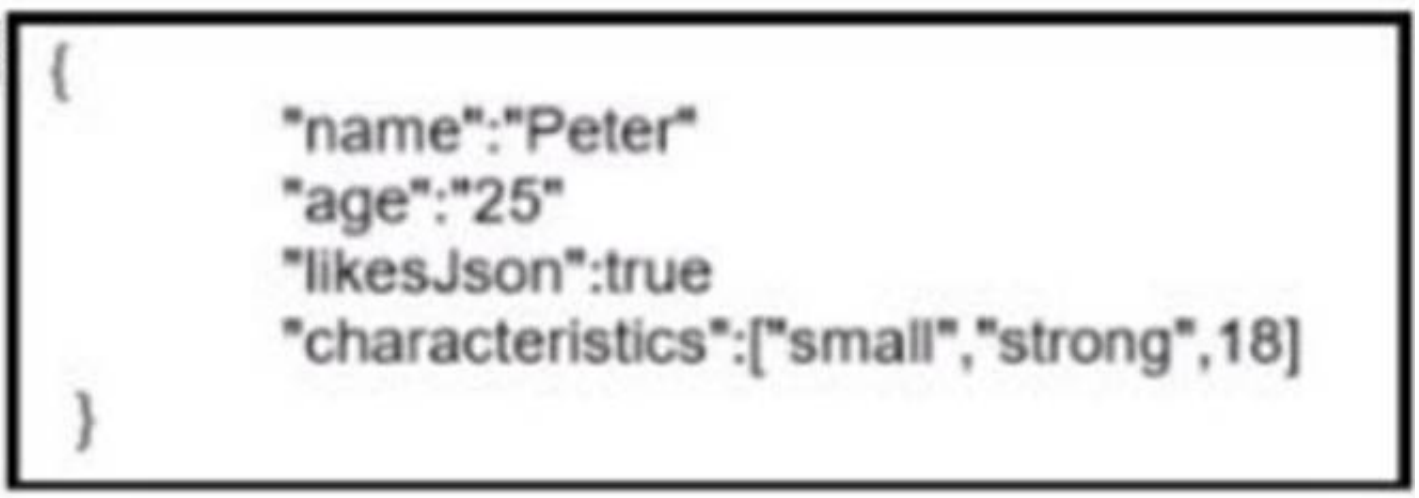
NEW QUESTION 218
- (Topic 1)
Which data is properly formatted with JSON?
A)



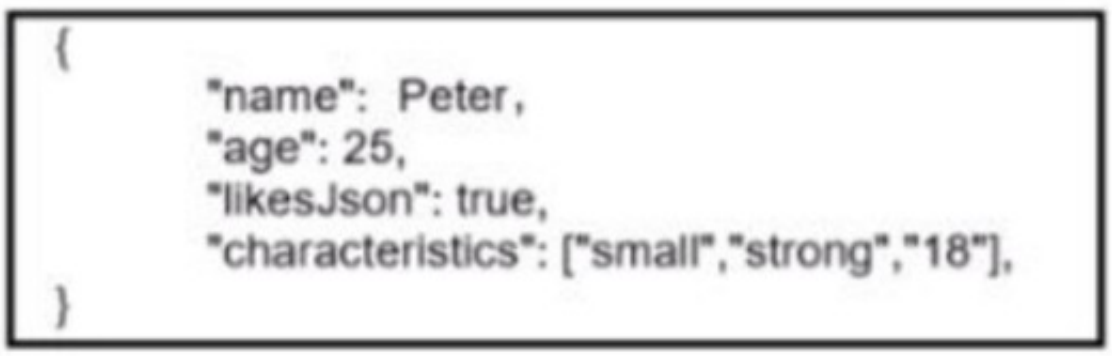
B)



C)



D)



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

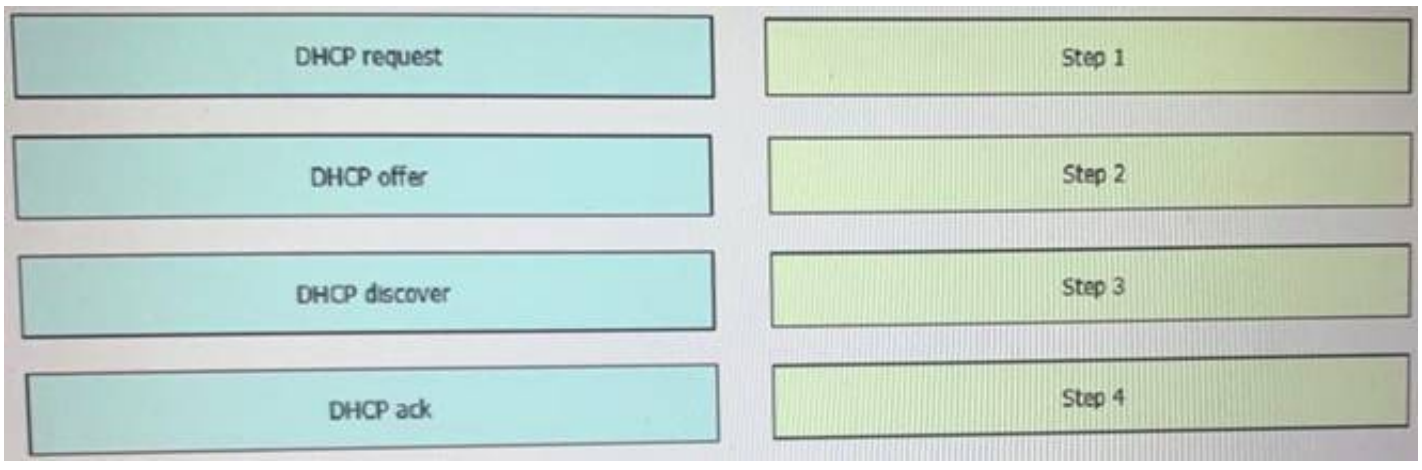
Answer: A

NEW QUESTION 219
- (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 220
DRAG DROP - (Topic 1)
Drag and drop the DHCP messages that are exchanged between a client and an AP into the order they are exchanged on the right.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 221
- (Topic 1)
What are two differences between the RIB and the FIB? (Choose two.)

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

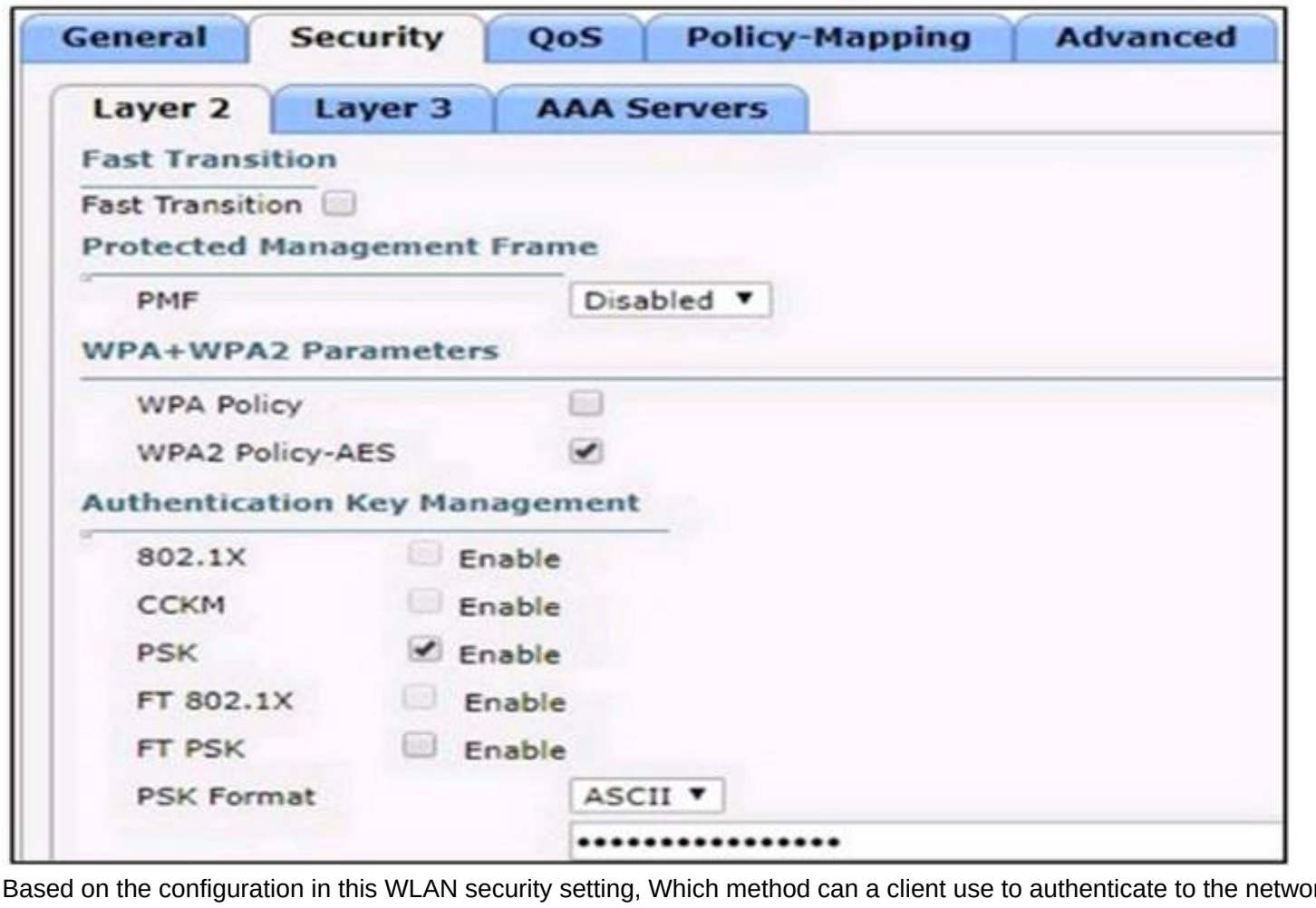
Answer: BE

NEW QUESTION 224
- (Topic 1)
In a Cisco SD-Access solution, what is the role of the Identity Services Engine?

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

Answer: A

NEW QUESTION 228
- (Topic 1)
Refer to the exhibit.



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

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

Answer: A

NEW QUESTION 229
- (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 234
- (Topic 1)
If the noise floor is -90 dBm and wireless client is receiving a signal of -75 dBm, what is the SNR?

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

Answer: A

NEW QUESTION 237
- (Topic 1)
What is one fact about Cisco SD-Access wireless network deployments?

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

Answer: C

NEW QUESTION 240
- (Topic 1)
Refer to the exhibit.

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

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

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

B)

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

C)

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

D)

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

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

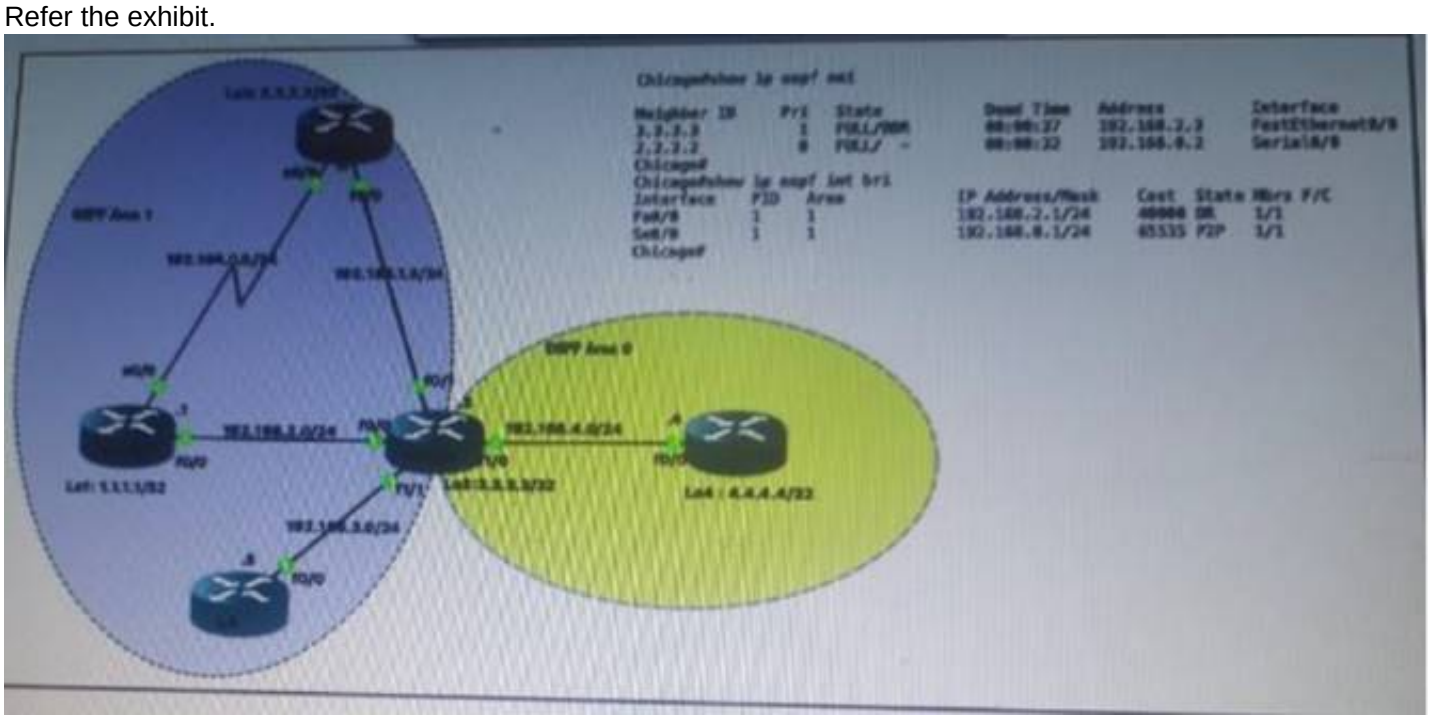
Answer: B

NEW QUESTION 244
- (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 249
- (Topic 1)
Refer the exhibit.



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

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

Answer: B

NEW QUESTION 250
- (Topic 1)

Refer to the exhibit.

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

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

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

Answer: C

NEW QUESTION 254
- (Topic 1)
A customer has recently implemented a new wireless infrastructure using WLC-5520 at a site directly next to a large commercial airport. Users report that they intermittently lose WI- FI connectivity, and troubleshooting reveals it is due to frequent channel changes. Which two actions fix this issue? (Choose two)

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

Answer: AE

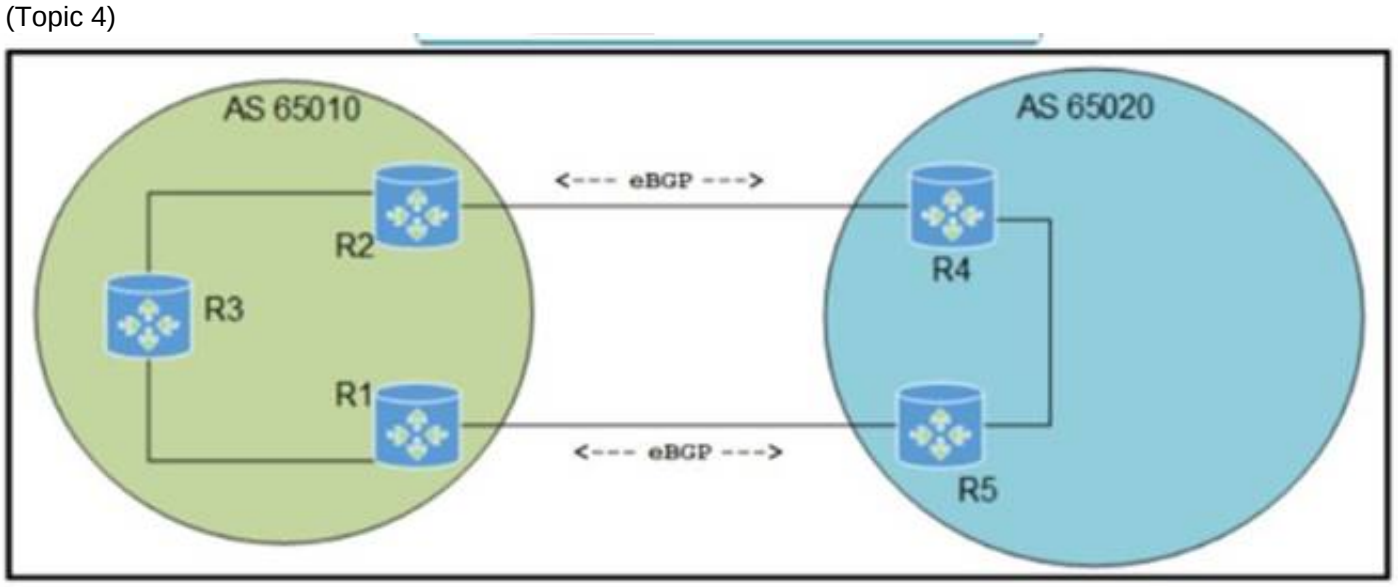
NEW QUESTION 257
- (Topic 4)
A network administrator is designing a new network for a company that has frequent power spikes. The company wants to ensure that employees can the best solution for the administrator to recommend?

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

Answer: D

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

NEW QUESTION 258
- (Topic 4)



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

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

B)

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

C)

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

D)

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

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

Answer: C

NEW QUESTION 260
- (Topic 4)
What is a characteristic of a traditional WAN?

A. low complexity and high overall solution scale
B. centralized reachability, security, and application policies
C. operates over DTLS and TLS authenticated and secured tunnels
D. united data plane and control plane

Answer: D

NEW QUESTION 261
- (Topic 4)
What is a client who is running 802.1x for authentication reffered to as?

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

Answer: A

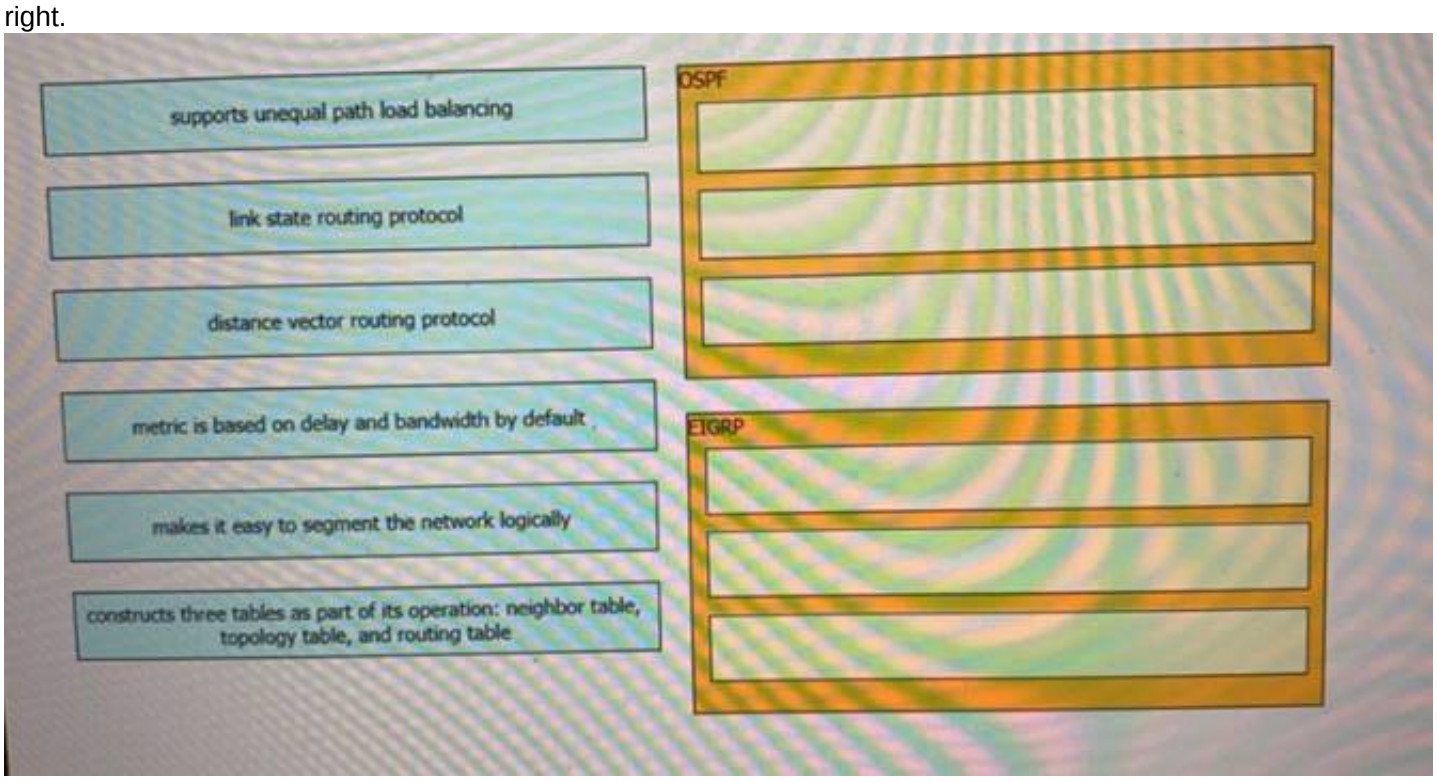
NEW QUESTION 266
- (Topic 4)
Which of the following security methods uses physical characteristics of a person to authorize access to a location?

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

Answer: B

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

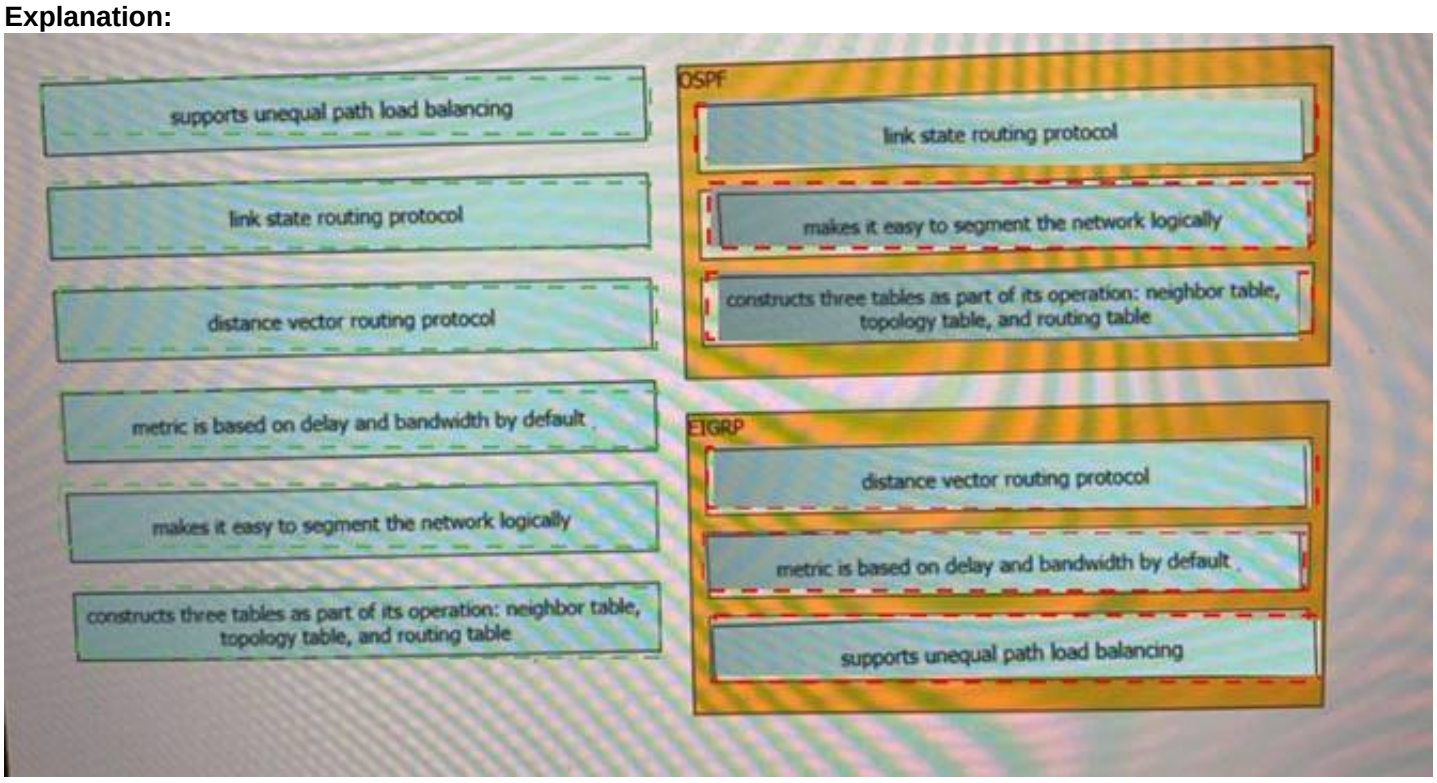
NEW QUESTION 268
DRAG DROP - (Topic 4)
Drag the drop the description from the left onto the routing protocol they describe on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 270
- (Topic 4)
Which device, in a LISP routing architecture, receives and de-encapsulates LISP traffic for endpoints within a LISP-capable site?

A. MR
B. ETR
C. OMS
D. ITR

Answer: B

NEW QUESTION 275
- (Topic 4)
Which action limits the total amount of memory and CPU that is used by a collection of VMs?

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

Answer: A

NEW QUESTION 279
- (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 281
- (Topic 4)
An engineer receives a report that an application exhibits poor performance. On the switch where the server is connected, this syslog message is visible:
SW_MATM4-MACFLAP_N0HF: Host 0054.3831.8253 in vlan 14 is flapping between port GUAM and port Gi1/0/2.
What is causing the problem?

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

Answer: B

NEW QUESTION 282
- (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 287
- (Topic 4)

```
monitor session 11 type erspan-source
source interface GigabitEthernet3
destination
erspan-id 12
ip address 10.10.10.10
origin ip address 10.100.10.10
```

Refer to the exhibit. Which command set completes the ERSPAN session configuration?

monitor session 12 type erspan-destination
destination interface GigabitEthernet4
source
erspan-id 12
ip address 10.10.10.10

monitor session 11 type erspan-destination
destination interface GigabitEthernet4
source
erspan-id 12
ip address 10.100.10.10

monitor session 11 type erspan-destination
destination interface GigabitEthernet4
source
erspan-id 11
ip address 10.10.10.10

monitor session 12 type erspan-destination
destination interface GigabitEthernet4
source
erspan-id 11
ip address 10.10.10.10

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

Answer: A

NEW QUESTION 292
DRAG DROP - (Topic 4)
Drag and drop the code snippets from the bottom onto the blanks in the Python script to print the device model to the screen and write JSON data to a file Not all options are used

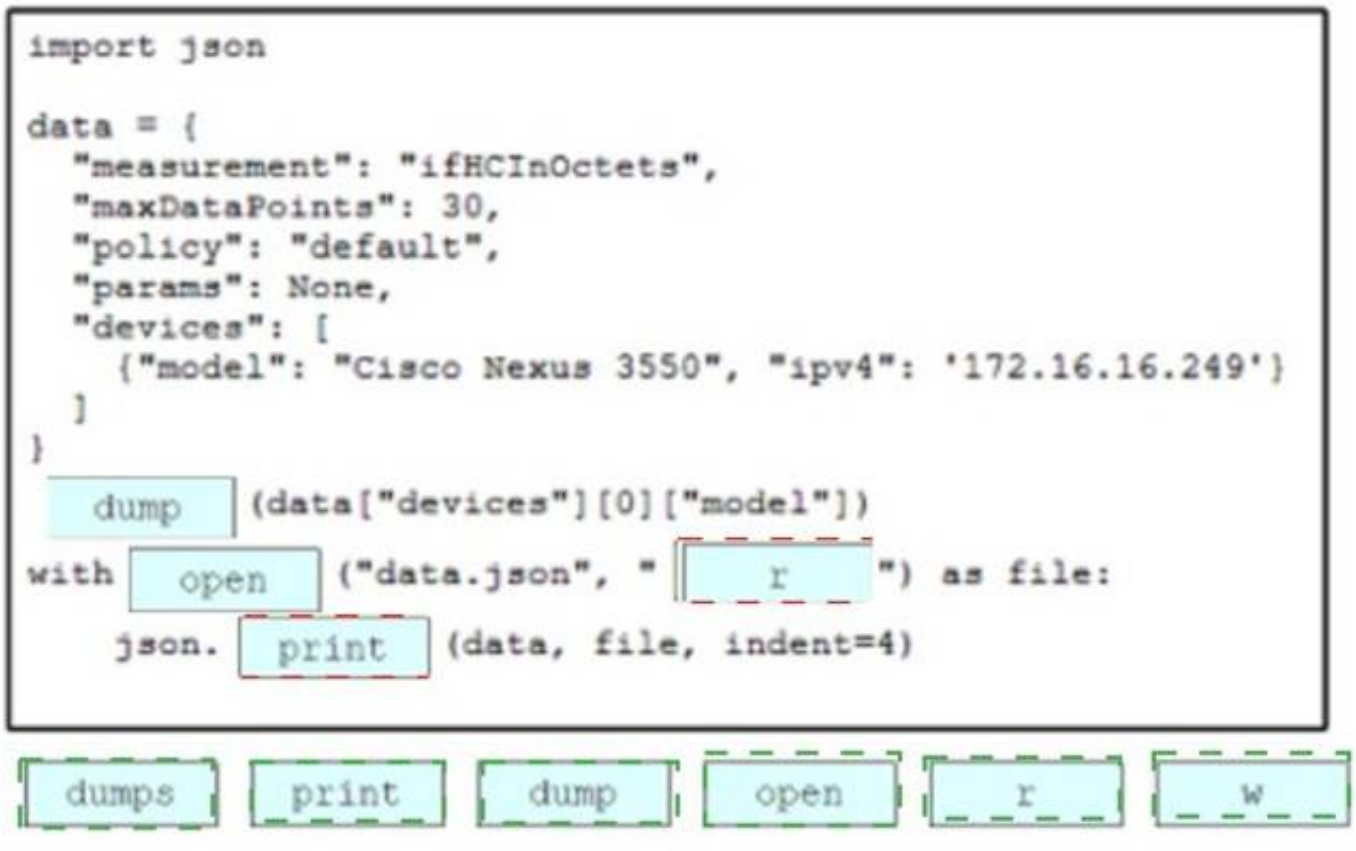
```
import json

data = {
  "measurement": "ifHCInOctets",
  "maxDataPoints": 30,
  "policy": "default",
  "params": None,
  "devices": [
    {"model": "Cisco Nexus 3550", "ipv4": '172.16.16.249'}
  ]
}
 [      ](data["devices"][0]["model"])
with [      ]("data.json", " [      ]") as file:
    json. [      ](data, file, indent=4)
```

dumps | print | dump | open | r | w

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 296
- (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 297
- (Topic 4)
An engineer must configure GigabitEthernet 0/0 for VRRP group 65. The rouler must assume the primary rote when it has the highest priority in the group. Which command set must be applied?
A)

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

B)

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

C)

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

D)

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

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

Answer: D

NEW QUESTION 302
- (Topic 4)
A script contains the statement "while loop != 999:" Which value terminates the loop?

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

Answer: A

NEW QUESTION 303
- (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 304
- (Topic 4)

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

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

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

Answer: B

NEW QUESTION 306
- (Topic 4)
A network engineer wants to configure console access to a router without using AAA so that the privileged exec mode is entered directly after a user provides the correct login credentials. Which action achieves this goal?

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

Answer: C

NEW QUESTION 311
- (Topic 4)
Which function does a virtual switch provide?

A. CPU context switching (or multitasking between virtual machines

B. RAID storage for virtual machines
C. emulation of power for virtual machines.
D. connectivity between virtual machines

Answer: D

Explanation:
This is because a virtual switch is a software-based switch that operates at the data link layer of the OSI model and provides connectivity between virtual machines that are running on the same physical host or different hosts. A virtual switch can also connect virtual machines to external networks, such as the Internet or a local area network, by using physical network adapters on the host. A virtual switch can perform the same functions as a physical switch, such as learning MAC addresses, forwarding frames, and applying VLANs. The source of this answer is the Cisco ENCOR v1.1 course, module 9, lesson 9.1: Implementing Network Virtualization.

NEW QUESTION 313
- (Topic 4)
An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?

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

Answer: B

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

NEW QUESTION 315
- (Topic 4)

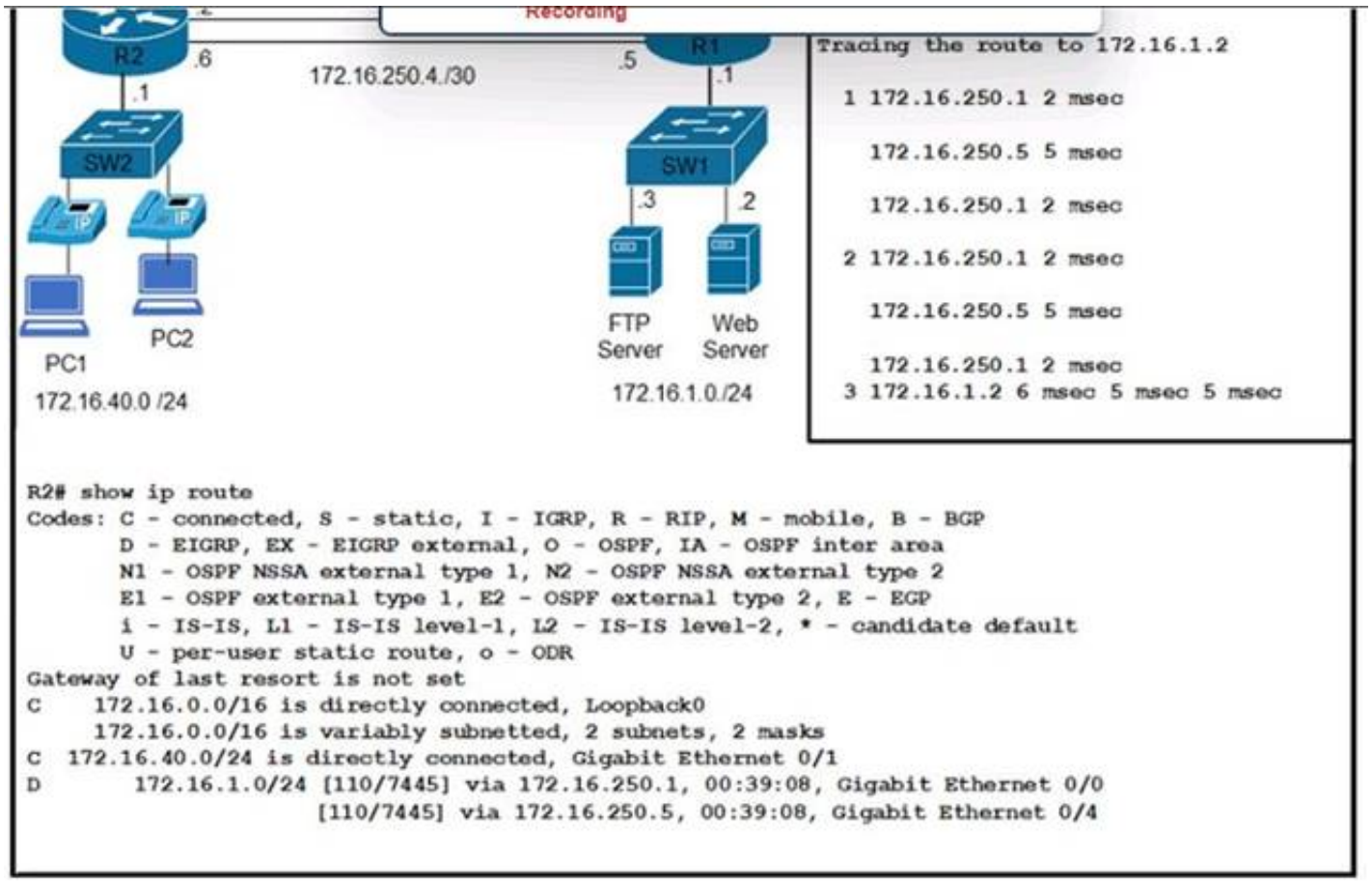
```
list = [1, 2, 3, 4]
list[3] = 10
print(list)
```

Refer to the exhibit. What is the value of the variable list after the code is run?

A. [1, 2, 10]
B. [1, 2, 3, 10]
C. [1, 2, 10, 4]
D. [1, 10, 10, 10]

Answer: B

NEW QUESTION 318
- (Topic 4)
Refer to the exhibit.



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

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

Answer: C

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

NEW QUESTION 320
- (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 321
- (Topic 4)
If AP power level is increased from 25 mW to 100 mW. what is the power difference in dBm?

A. 6 dBm
B. 14 dBm
C. 17 dBm
D. 20 dBm

Answer: D

NEW QUESTION 325
- (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 328
- (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 333
- (Topic 4)
In lhe Cisco DNA Center Image Repository, what is a golden image?

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

Answer: B

NEW QUESTION 337
- (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 341
- (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 346
- (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

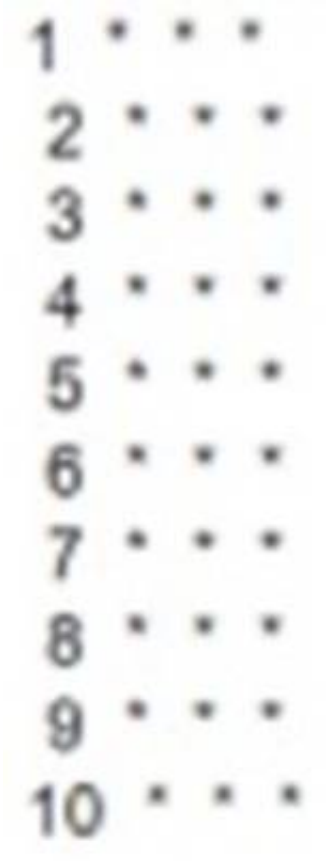
Answer: C

NEW QUESTION 349
- (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 354
- (Topic 4)
A firewall address of 192 166.1.101 can be pinged from a router but, when running a traceroute to It, this output is received



What is the cause of this issue?

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

Answer: D

NEW QUESTION 355
- (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 359
- (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 364
- (Topic 4)
Which of the following should a junior security administrator recommend implementing to mitigate malicious network activity?

A. Intrusion prevention system
B. Load balancer
C. Access logging

D. Endpoint encryption

Answer: A

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

NEW QUESTION 366
- (Topic 4)

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

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

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

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

Answer: C

NEW QUESTION 370
- (Topic 4)

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

Refer to Ihe exhibit. An engineer must update the existing configuation to achieve these resu ts:
• Only administrators from the 192.168 1.0.'?4 subnet can access the vty lines.
* Access to the vty lines using clear-text protocols is prohibited. Which command set should be appled?
A)

```
access-list 1 permit 192.168.1.0 255.255.255.0
 line vty 0 15
 access-class 1 in
 transport input telnet rlogin
```

B)

```
access-list 1 permit 192.168.1.0 0.0.0.255
 line vty 0 15
 access-class 1 in
line vty 0 15
 access-class 1 in
 transport input none
```

C)

```
access-list 1 permit 192.168.1.0 0.0.0.255
 line vty 0 15
 access-class 1 in
 transport input ssh
```

D)

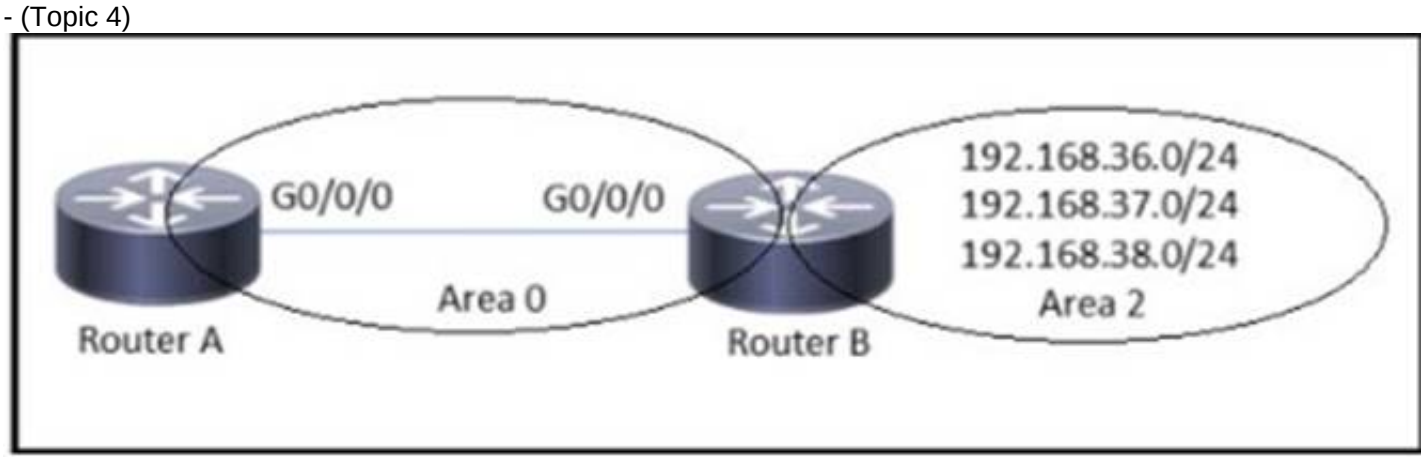
```
access-list 1 permit 192.168.1.0 0.0.0.255
 line vty 0 15
 access-class 1 in
```

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

Answer: B

Explanation:
Option B is the correct command set to update the existing configuration to achieve the desired results. The configuration steps are as follows12:
? Define a standard access list that permits only the administrators from the 192.168.1.0/24 subnet to access the vty lines. In this case, the access list is named ADMIN and it allows any host with an IP address in the range of 192.168.1.1 to 192.168.1.254 to access the vty lines: ip access-list standard ADMIN and permit 192.168.1.0 0.0.0.255.
? Apply the access list to the vty lines using the access-class command. This command restricts incoming and outgoing connections between a particular vty and the addresses in the access list. In this case, the access list ADMIN is applied to the vty lines 0 to 15 in the inbound direction, which means that only the hosts that match the access list can initiate a connection to the vty lines: line vty 0 15 and access-class ADMIN in.
? Disable the clear-text protocols such as Telnet for the vty lines using the transport input command. This command specifies which protocols are allowed for incoming connections. In this case, only SSH is allowed for the vty lines, which is a secure protocol that encrypts the data between the client and the server: transport input ssh.
Option A is incorrect because it does not apply the access list to the vty lines, which is required to restrict the access to the administrators from the 192.168.1.0/24 subnet. Without the access-class command, any host can attempt to connect to the vty lines12.
Option C is incorrect because it does not disable the clear-text protocols for the vty lines, which is required to prohibit the access to the vty lines using unsecure protocols. Without the transport input ssh command, both Telnet and SSH are allowed for the vty lines by default12.
Option D is incorrect because it uses an extended access list instead of a standard access list, which is not recommended for controlling access to the vty lines. An extended access list requires more configuration and processing than a standard access list, and it cannot be applied directly to the vty lines. It has to be applied to each interface that can be used to access the vty lines, which increases the complexity and the possibility of errors12. References: 1: Controlling Access to a Virtual Terminal Line, 2: Configuring Secure Shell

NEW QUESTION 375
- (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 376
- (Topic 4)
Refer to the exhibit.

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

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

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

Answer: C

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

NEW QUESTION 380
- (Topic 4)
A company's office has publicly accessible meeting rooms equipped with network ports. A recent audit revealed that visitors were able to access the corporate network by plugging personal laptops into open network ports. Which of the following should the company
implement to prevent this in the future?

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

Answer: D

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

NEW QUESTION 384
- (Topic 4)
What does a YANG model provide?

A. standardized data structure independent of the transport protocols

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

Answer: D

NEW QUESTION 388
- (Topic 4)

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

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

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

B)

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

C)

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

D)

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

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

Answer: C

NEW QUESTION 389
- (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

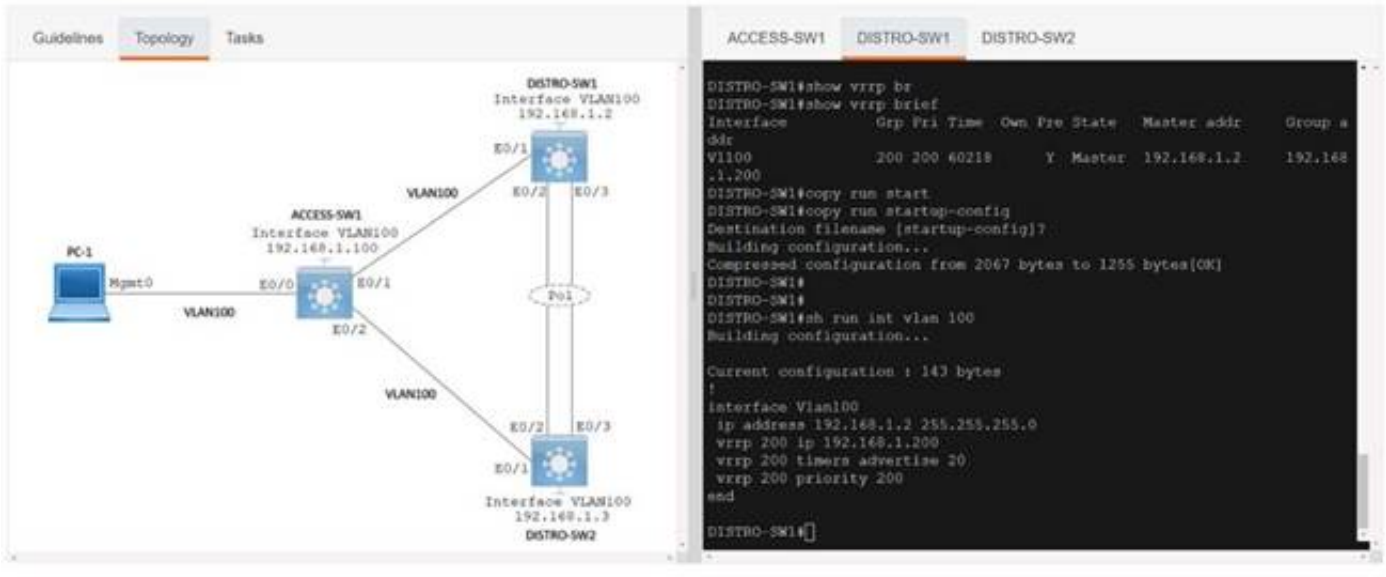
Explanation:
This is because the CoPP configuration shown in the exhibit applies a service policy to the control plane of the router, which is responsible for processing the routing protocols, management protocols, and other control traffic. The service policy uses a class map that matches the access 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 392
- (Topic 4)
Which language defines the structure or modelling of data for NETCONF and RESTCONF?

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

Answer: C

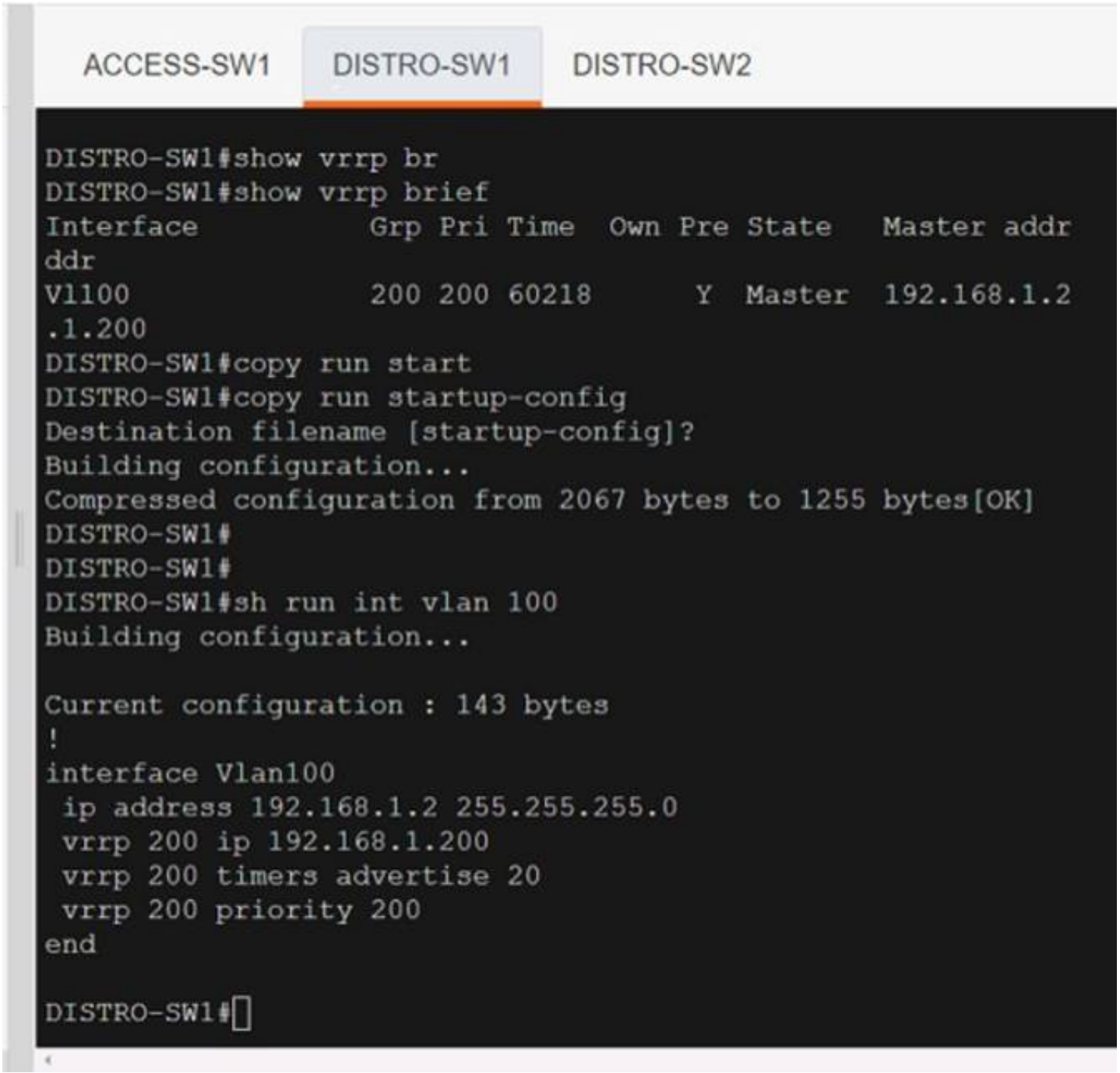
NEW QUESTION 394
SIMULATION - (Topic 4)
Simulation 10

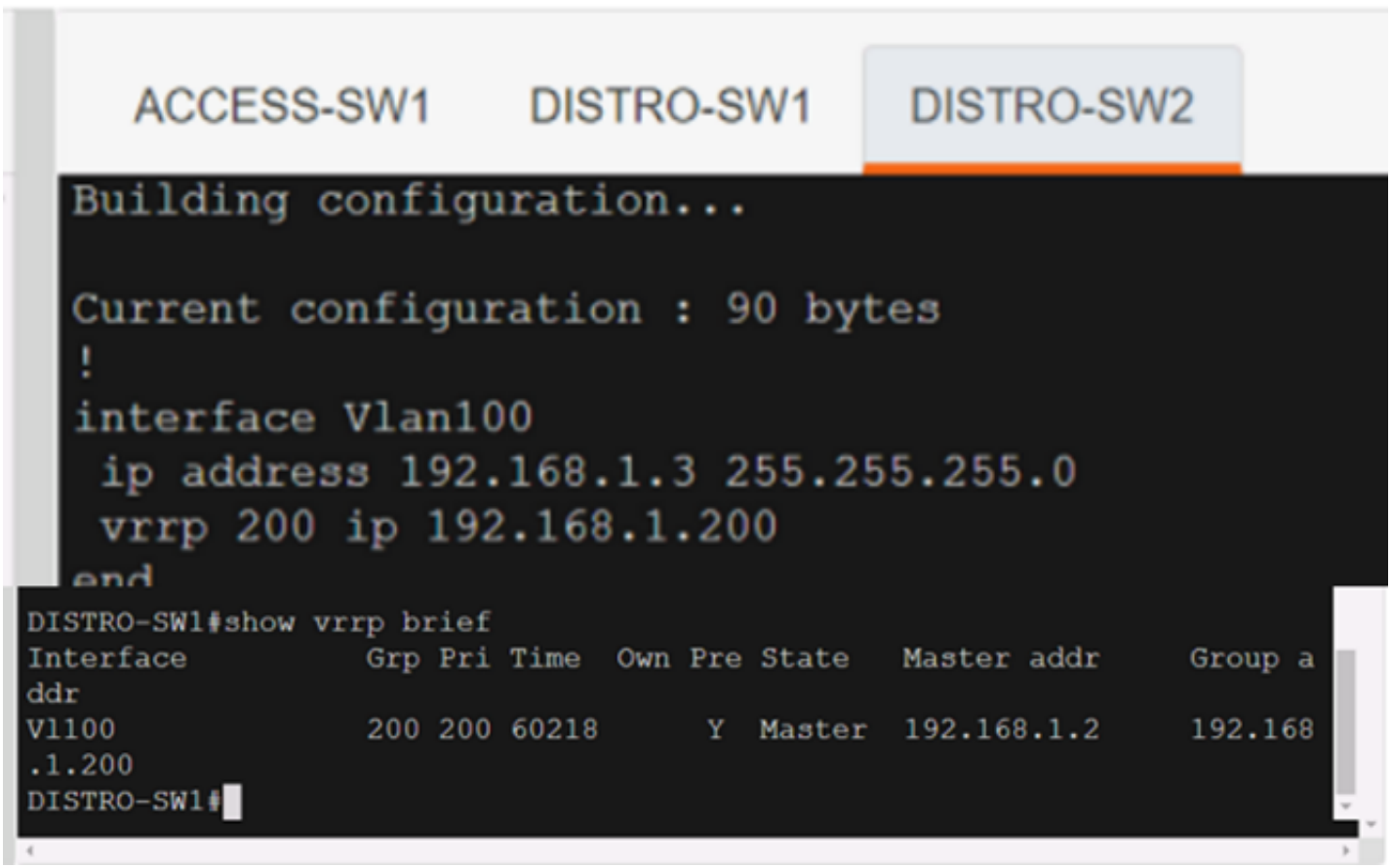


A. Mastered
B. Not Mastered

Answer: A

Explanation:





NEW QUESTION 395
- (Topic 4)
What is a characteristic of the Cisco DMA Center Template Editor feature?

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

Answer: D

Explanation:
This is because the Cisco DNA Center Template Editor feature is a tool that allows the network administrator to create and deploy configuration templates to

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

NEW QUESTION 400
- (Topic 4)
Refer to the exhibit. What is the result of this Python code?

A. 1
B. 7
C. 7.5

Answer: D

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

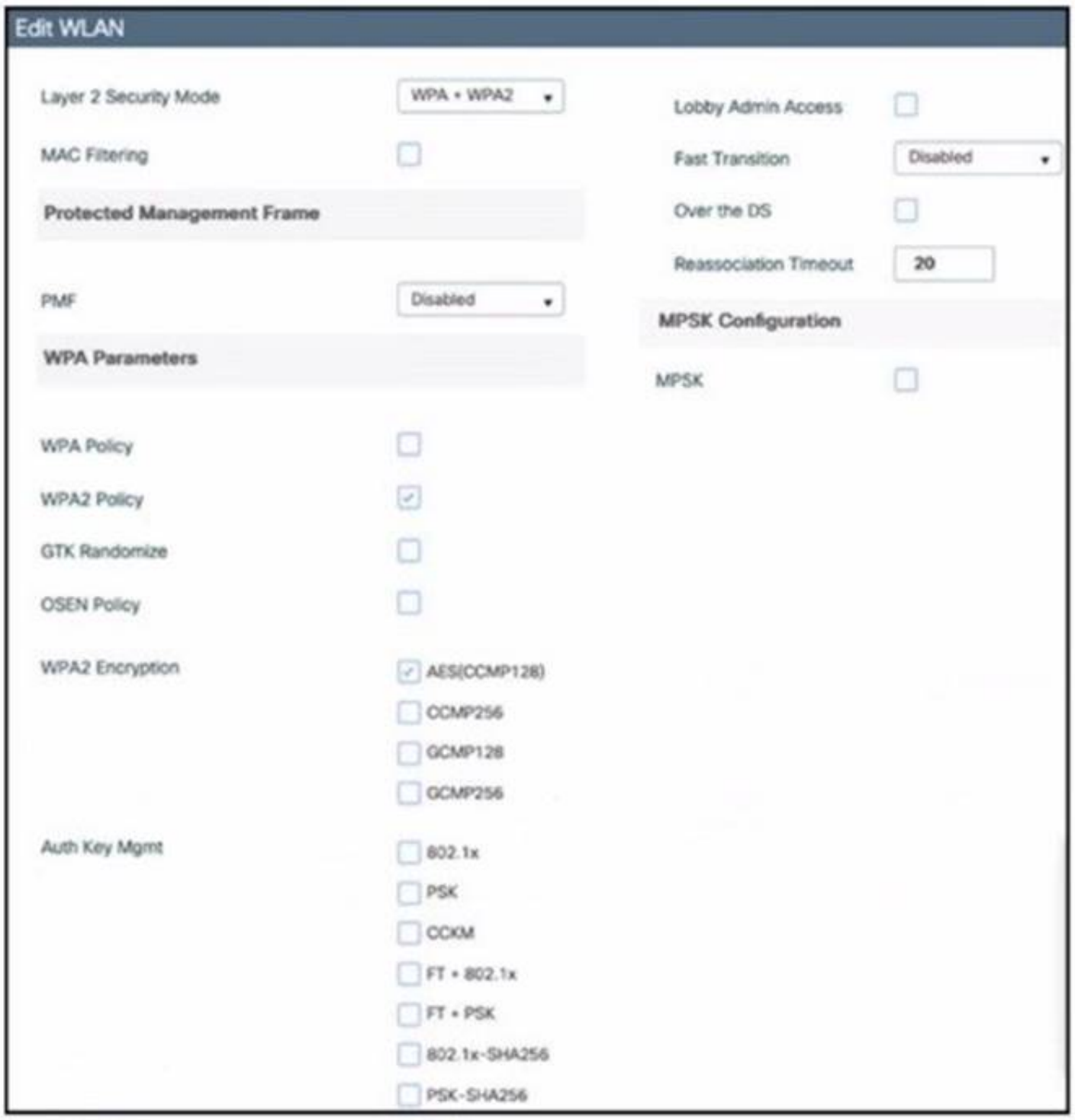
NEW QUESTION 401
- (Topic 4)
Users have reported an issue connecting to a server over the network. A workstation was recently added to the network and configured with a shared USB printer. Which of the following is most likely causing the issue?

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

Answer: D

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

NEW QUESTION 402
- (Topic 4)
Refer to the exhibit.



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

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

Answer: A

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

NEW QUESTION 406
- (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 408
DRAG DROP - (Topic 4)
An engineer plans to use Python to convert text files that contain device information lo JSON. Drag and drop the code snippets from the bottom onto the blanks in the code to construct the request. Not all options are used.

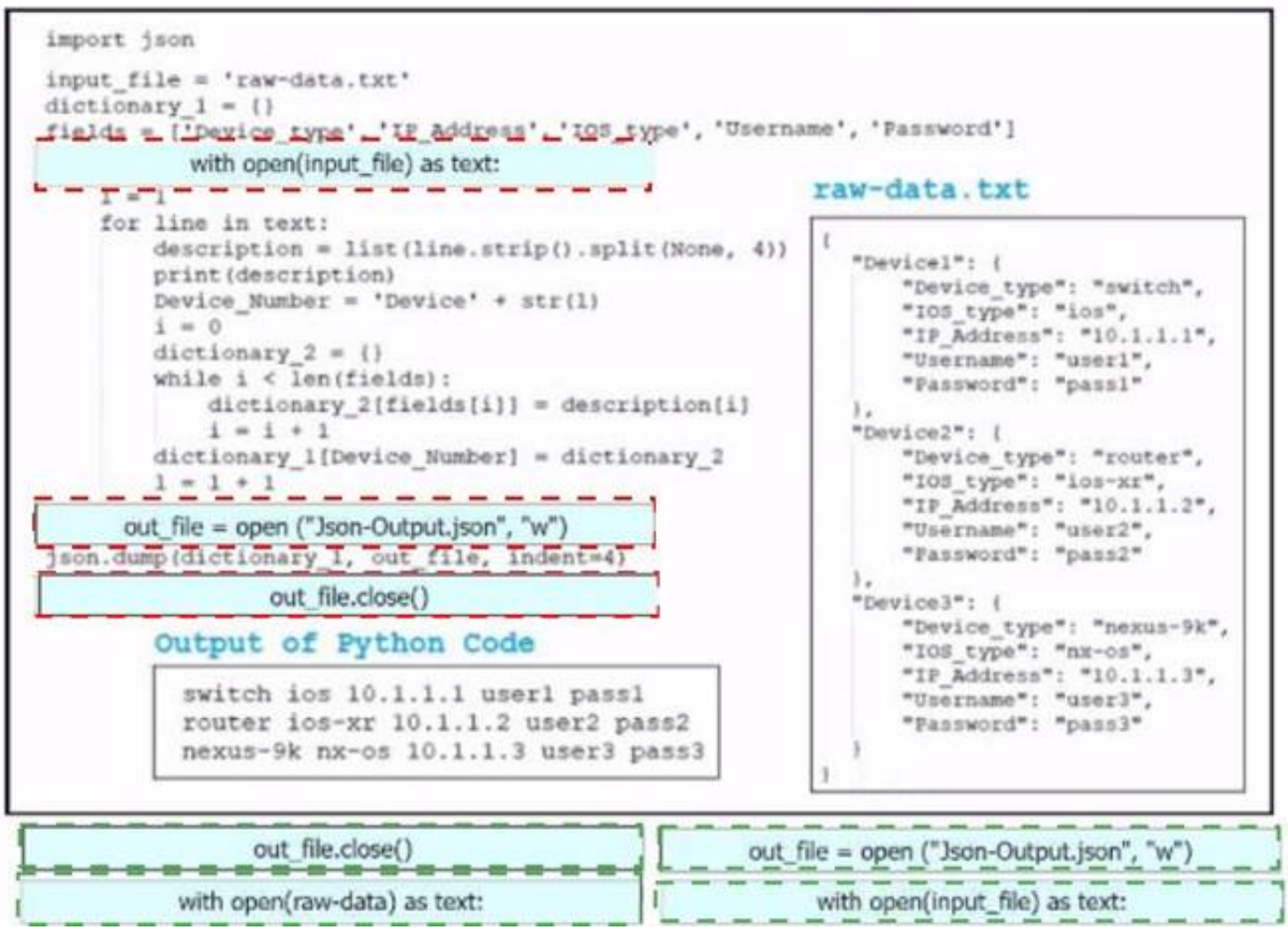
```
import json
input_file = 'raw-data.txt'
dictionary_1 = {}
fields = ['Device_type', 'IP_Address', 'IOS_type', 'Username', 'Password']
                                                    raw-data.txt
    l = 1                                           {
    for line in text:                                 "Device1": {
        description = list(line.strip().split(None, 4))      "Device_type": "switch",
        print(description)                                    "IOS_type": "ios",
        Device_Number = 'Device' + str(l)                     "IP_Address": "10.1.1.1",
        i = 0                                                 "Username": "user1",
        dictionary_2 = {}                                     "Password": "pass1"
        while i < len(fields):                            },
            dictionary_2[fields[i]] = description[i]      "Device2": {
            i = i + 1                                         "Device_type": "router",
        dictionary_1[Device_Number] = dictionary_2             "IOS_type": "ios-xr",
        l = l + 1                                             "IP_Address": "10.1.1.2",
                                                              "Username": "user2",
                                                              "Password": "pass2"
json.dump(dictionary_1, out_file, indent=4)               },
                                                          "Device3": {
Output of Python Code                                         "Device_type": "nexus-9k",
                                                              "IOS_type": "nx-os",
switch ios 10.1.1.1 user1 pass1                               "IP_Address": "10.1.1.3",
router ios-xr 10.1.1.2 user2 pass2                            "Username": "user3",
nexus-9k nx-os 10.1.1.3 user3 pass3                           "Password": "pass3"
                                                          }
                                                    }
```

out_file.close()
out_file = open ("Json-Output.json", "w")
with open(raw-data) as text:
with open(input_file) as text:

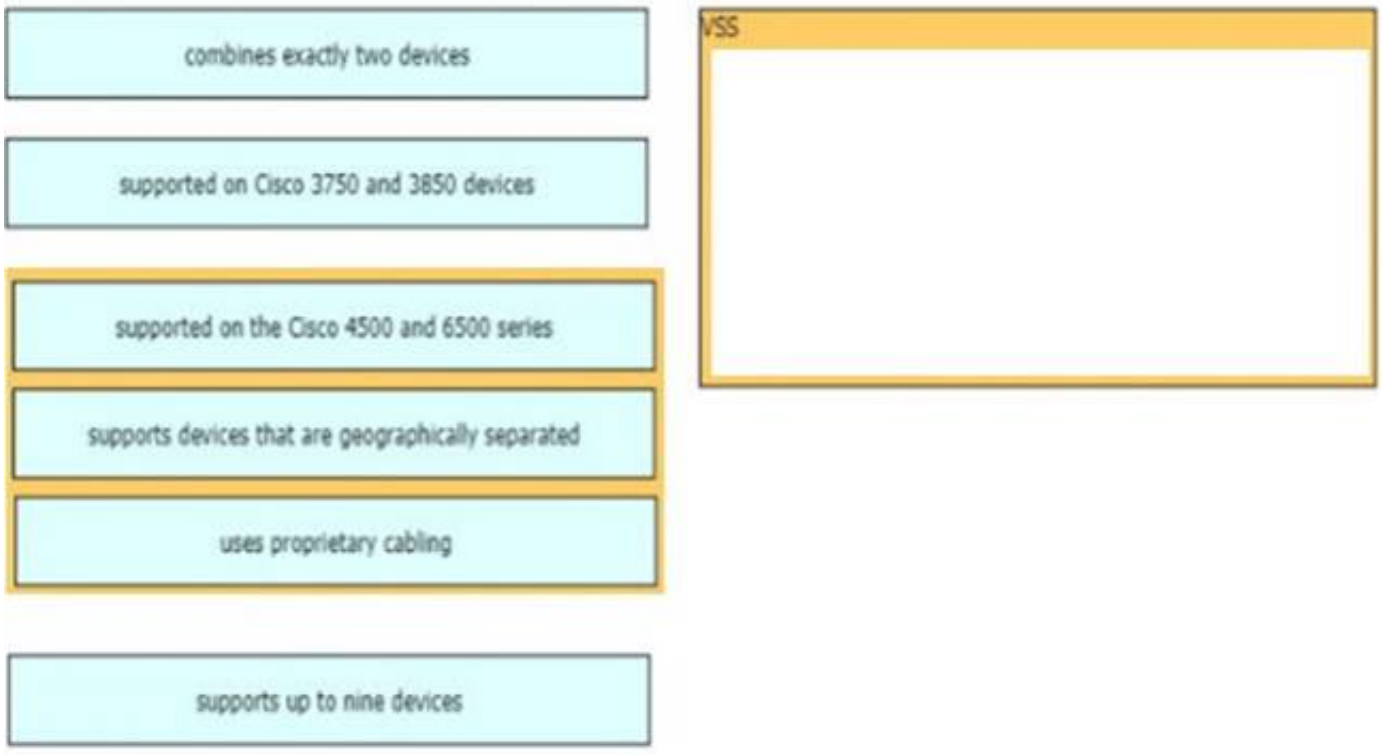
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 409
DRAG DROP - (Topic 4)
Drag and drop the description of the VSS technology from the left to the right. NOT all options are used.

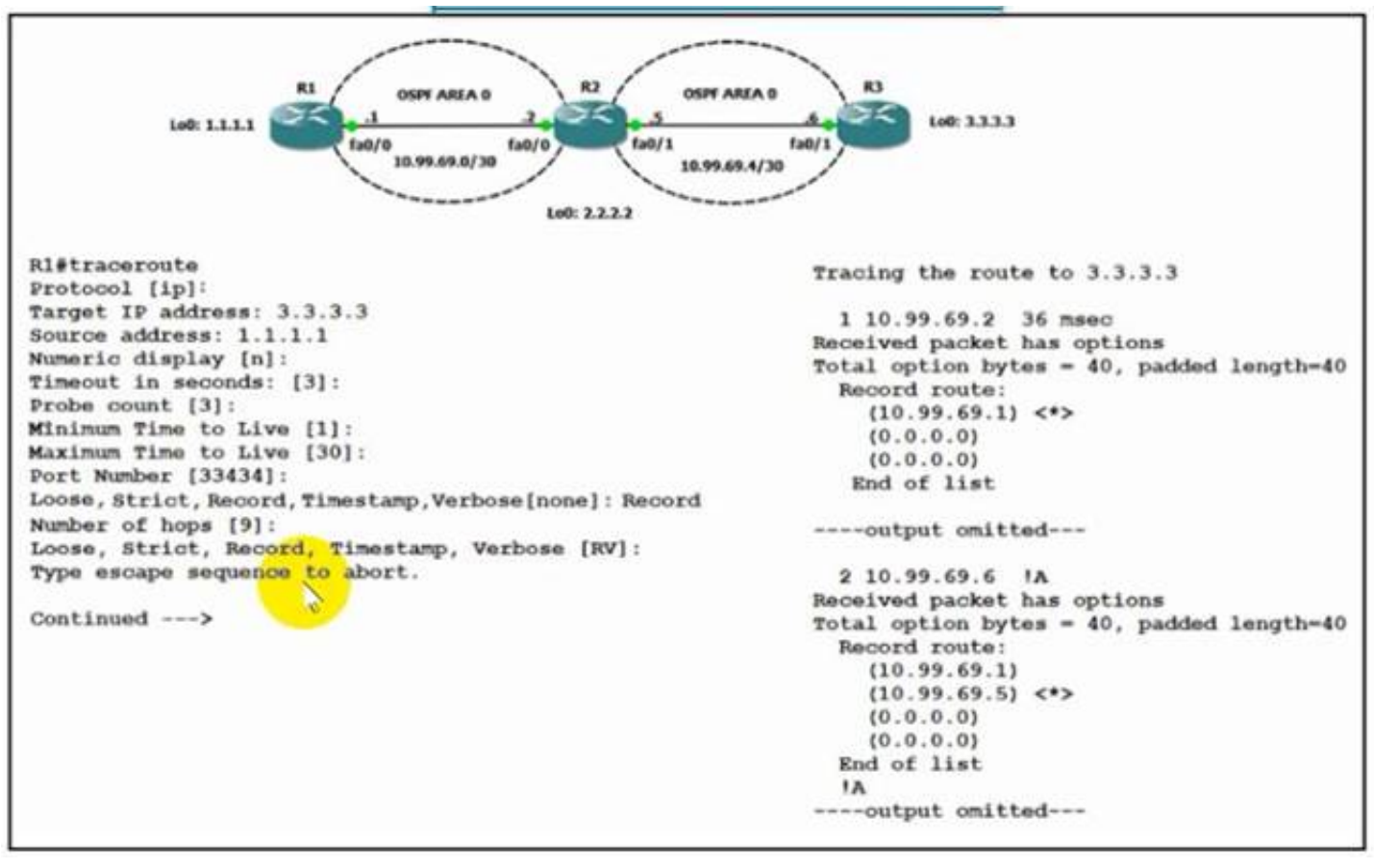


A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 413
- (Topic 4)
Refer to the exhibit.



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 415
SIMULATION - (Topic 4)
Simulation 02
Configure HSRP between DISTRO-SW1 and DISTRO-SW2 on VLAN 100 for hosts connected to ACCESS-SW1 to achieve these goals:
* 1. Configure group number 1 using the virtual IP address of 192.168.1.1/24.
* 2. Configure DlSTRO-SW1 as the active router using a priority value of 110 and DISTRO- SW2 as the standby router.
* 3. Ensure that DISTRO-SW2 will take over the active role when DISTRO-SW1 goes down, and when DISTRO-SW1 recovers, it automatically resumes the active role.

Copyment

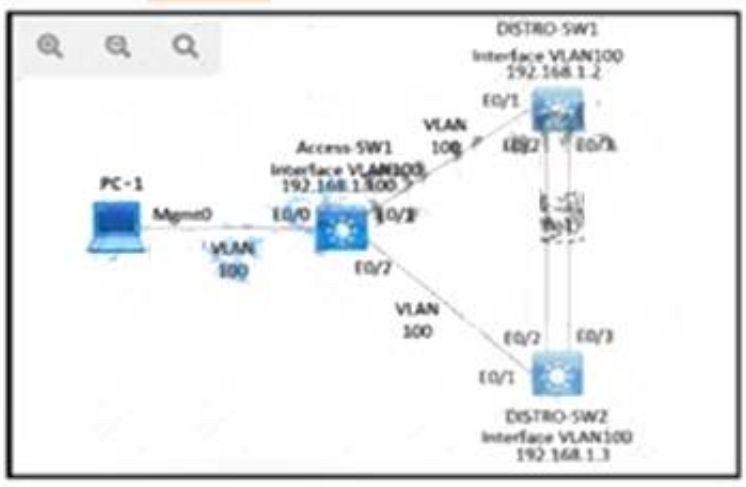
Guidelines Topology Tasks

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

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

DISTRO-SW1 DISTRO-SW2

DISTRO-SW1>



Guidelines Topology Tasks

DISTRO-SW1 DISTRO-SW2

DISTRO-SW1>

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

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

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

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

```
!
interface Vlan100
 ip address 192.168.1.2.255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes2
56-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes2
56-ctr
!
!
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
```

DISTRO-SW2

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

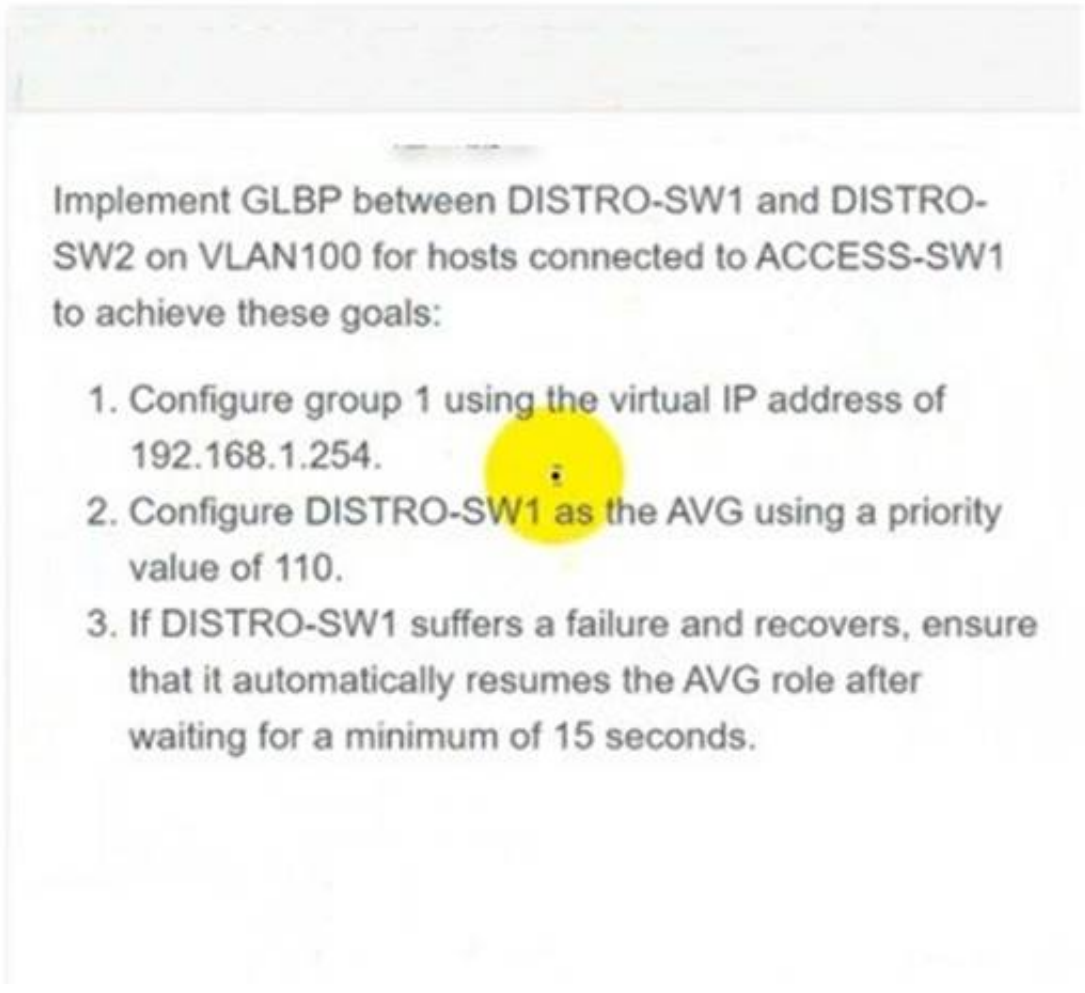
```
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
 channel-group 1 mode passive
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
 channel-group 1 mode passive
!
interface Vlan100
 ip address 192.168.1.3 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes2
56 ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes2
56-ctr
!
```

A. Mastered
B. Not Mastered

Answer: A

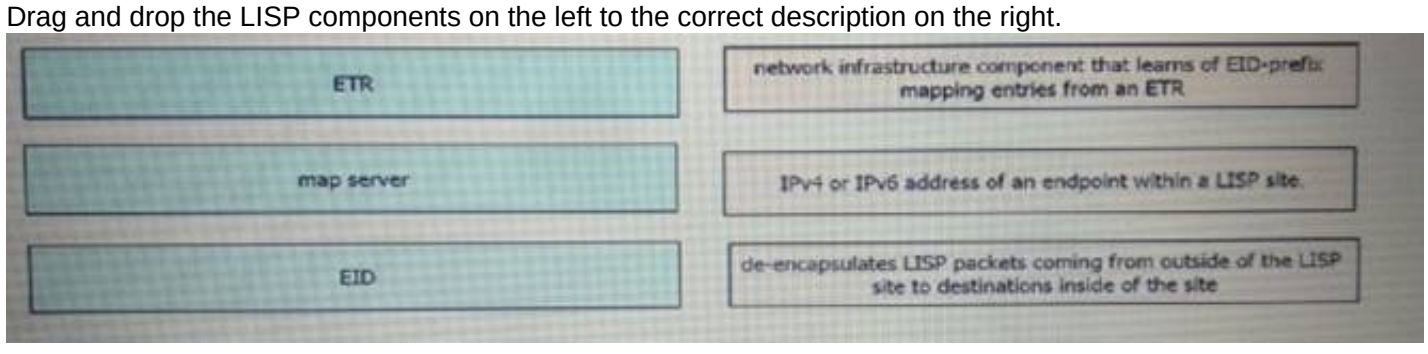
Explanation:
DISTRO-SW1
Sw1

int vlan 100
standby 1 ip 192.168.1.1
standby 1 priority 110
standby 1 preempt copy run start
DISTRO-SW2 SW2
int vlan 100
standby 1 ip 192.168.1.1
standby 1 preempt
copy run start
OR
MINOR CHANGE IN ABOVE HSRP SCENERIO



Description automatically generated
Check the IP address 1.254 check the minimum 15 seconds solution get change.
DISTRO-SW1
Sw1
int vlan 100
glbp 1 ip 192.168.1.254
glbp 1 priority 110
glbp 1 timers 5 15
glbp 1 preempt
copy run start
DISTRO-SW2 SW2
int vlan 100
glbp 1 ip 192.168.1.254
glbp 1 timers 5 15
glbp 1 preempt copy run start

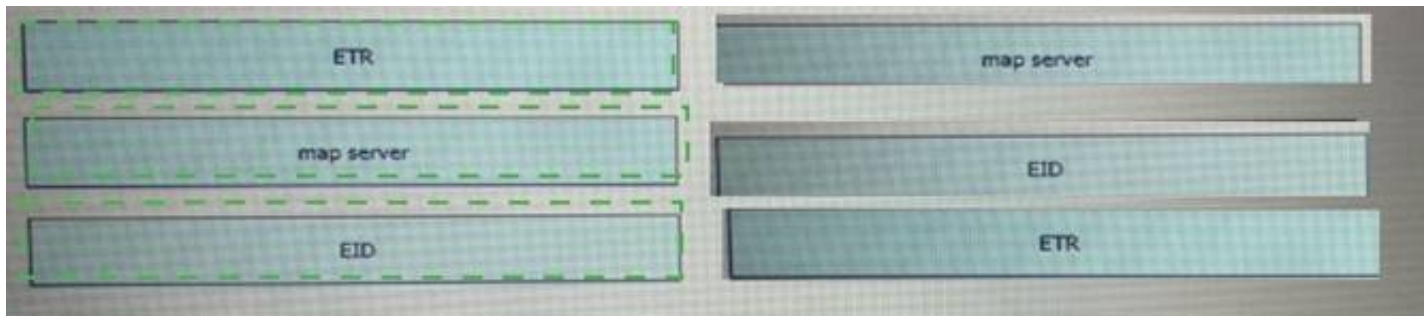
NEW QUESTION 418
DRAG DROP - (Topic 4)
Drag and drop the LISP components on the left to the correct description on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 423
- (Topic 4)
Refer to the exhibit.

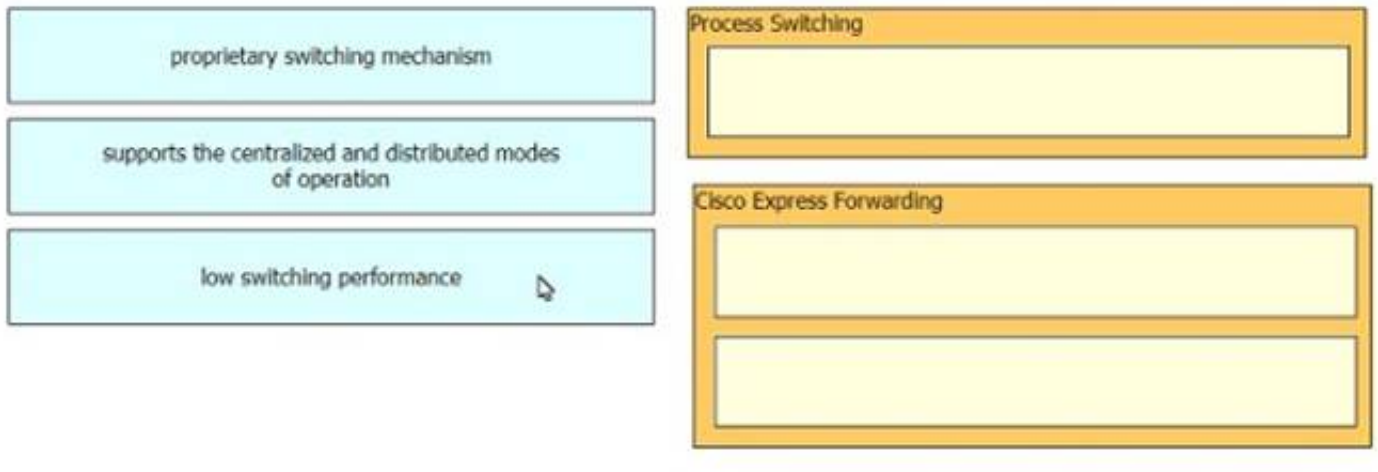
An engineer must assign an IP address of 192.168.1.1/24 to the GigabitEtherenet1 interface. Which two commands must be added to the existing configuration to accomplish this task? (Choose two.)

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

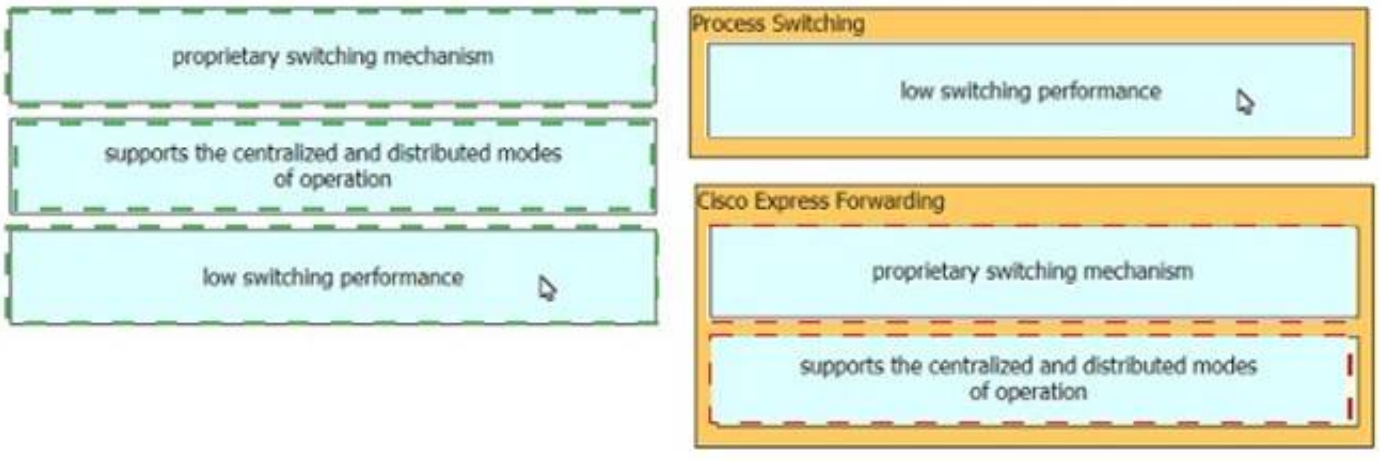
NEW QUESTION 425
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the switching architectures on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

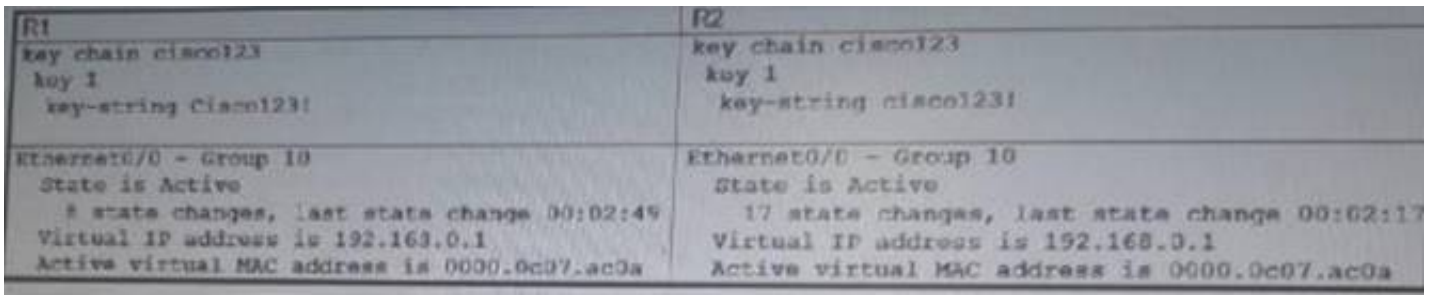


NEW QUESTION 427
- (Topic 4)
By default, which virtual MAC address does HSRP group 41 use?

A. 0c:5e:ac:07:0c:29
B. 00:05:0c:07:ac:41
C. 004:41:73:18:84:29
D. 00:00:0c:07:ac:29

Answer: D

NEW QUESTION 428
- (Topic 2)
Refer to the exhibit.



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

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

Answer: A

Explanation:
The virtual MAC address is 0000.0c07.acXX (XX is the hexadecimal group number) so it is using HSRPv1.
Note: HSRP Version 2 uses a new MAC address which ranges from 0000.0C9F.F000 to 0000.0C9F.FFFF.

NEW QUESTION 433
- (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

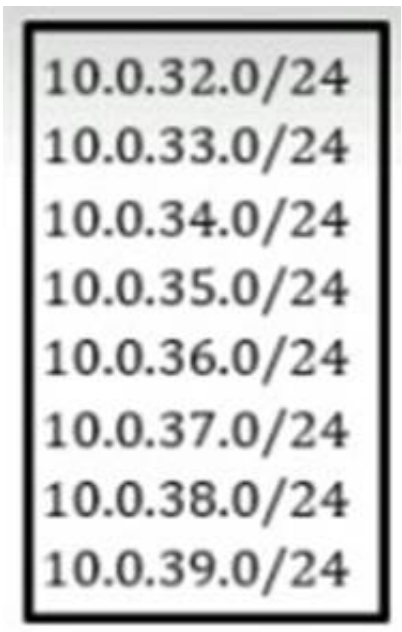
NEW QUESTION 434
- (Topic 2)
An engineer must create a new SSID on a Cisco 9800 wireless LAN controller. The client has asked to use a pre-shared key for authentication Which profile must the engineer edit to achieve this requirement?

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 437
- (Topic 2)
Refer to the exhibit.

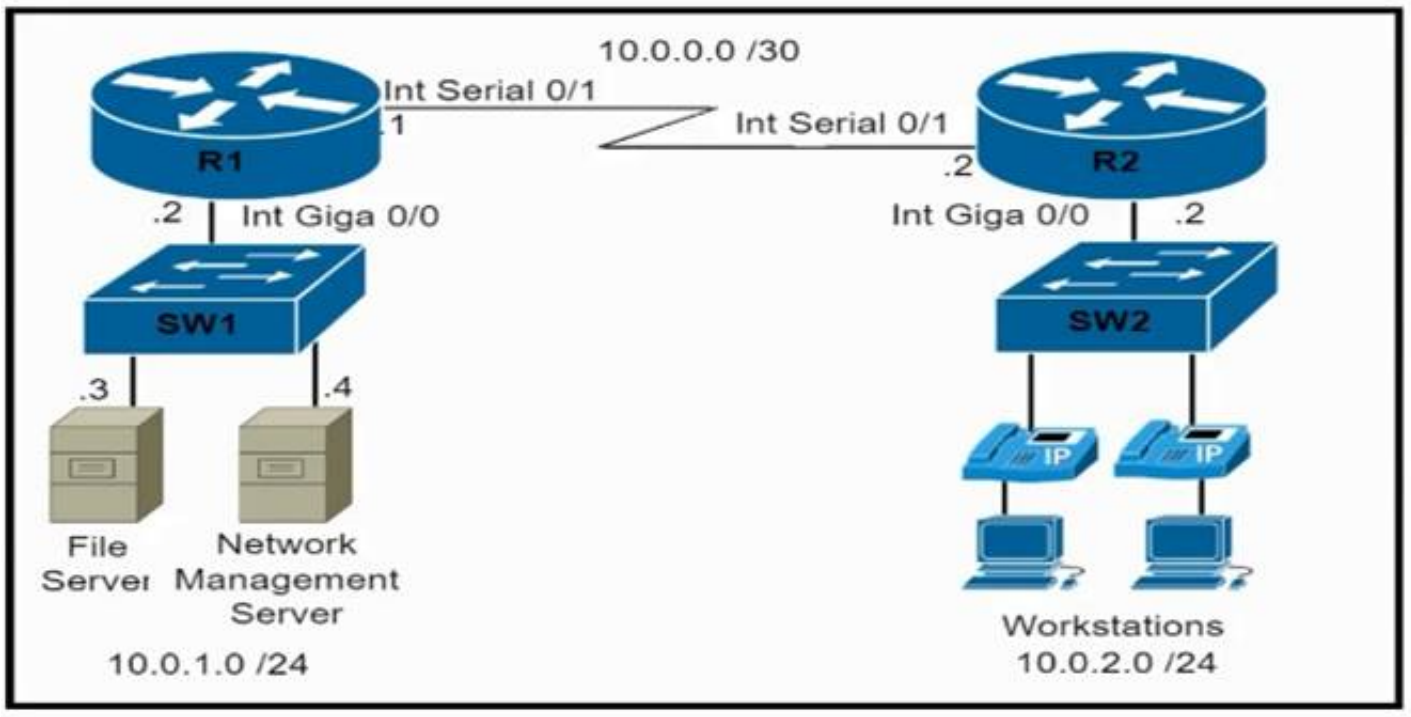


An engineer must permit traffic from these networks and block all other traffic An informational log message should be triggered when traffic enters from these prefixes Which access list must be used?

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 440
- (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.)

- [x] **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**

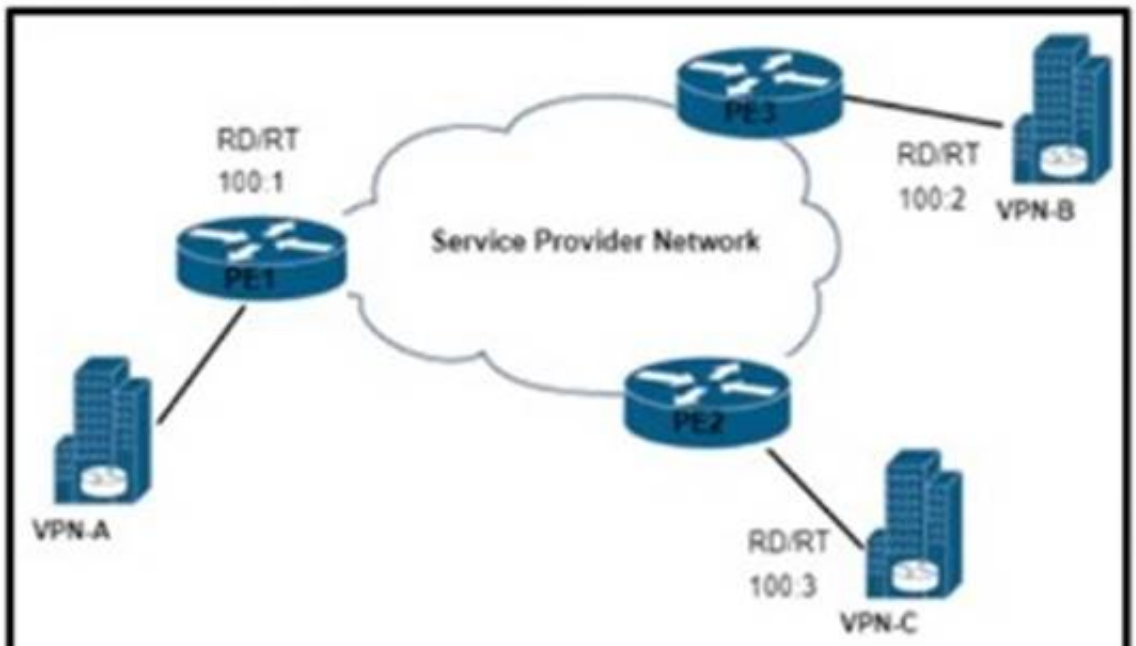
- [x] **access-list 150 permit udp 10.0.1.4 0.0.0.0 host 10.0.1.2 eq snmp**
access-list 150 permit udp 10.0.1.4 0.0.0.0 eq snmp host 10.0.1.2

```
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 442
- (Topic 2)
Refer to the exhibit.




```
PE-1#vrf VPN-A
 address-family ipv4 unicast
 import route-target 100:3
 export route-target 100:1
!
PE1# show vrf all detail
VRF VPN-A; RD 1:100; VPN ID not set
Description not set
Interfaces:
 GigabitEthernet0/0/0/0
Address family IPV4 Unicast
 Import VPN route-target communities:
  RT:100:3
 Export VPN route-target communities:
  RT:100:1
 No import route policy
 No export route policy
!
```

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

A)

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

B)

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

C)

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

D)

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

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

Answer: B

NEW QUESTION 444
- (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 447
- (Topic 2)
Refer to the exhibit.

```
R1#show ip bgp
BGP table version is 32, local router ID is 192.168.101.5
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
*    192.168.102.0    192.168.101.18         80             0 64517 i
*                     192.168.101.14         80         80  0 64516 i
*                     192.168.101.10                        0 64515 64515 i
*>                    192.168.101.2                     32768 64513 i
*                     192.168.101.6                      80 0 64514 64514 i
```

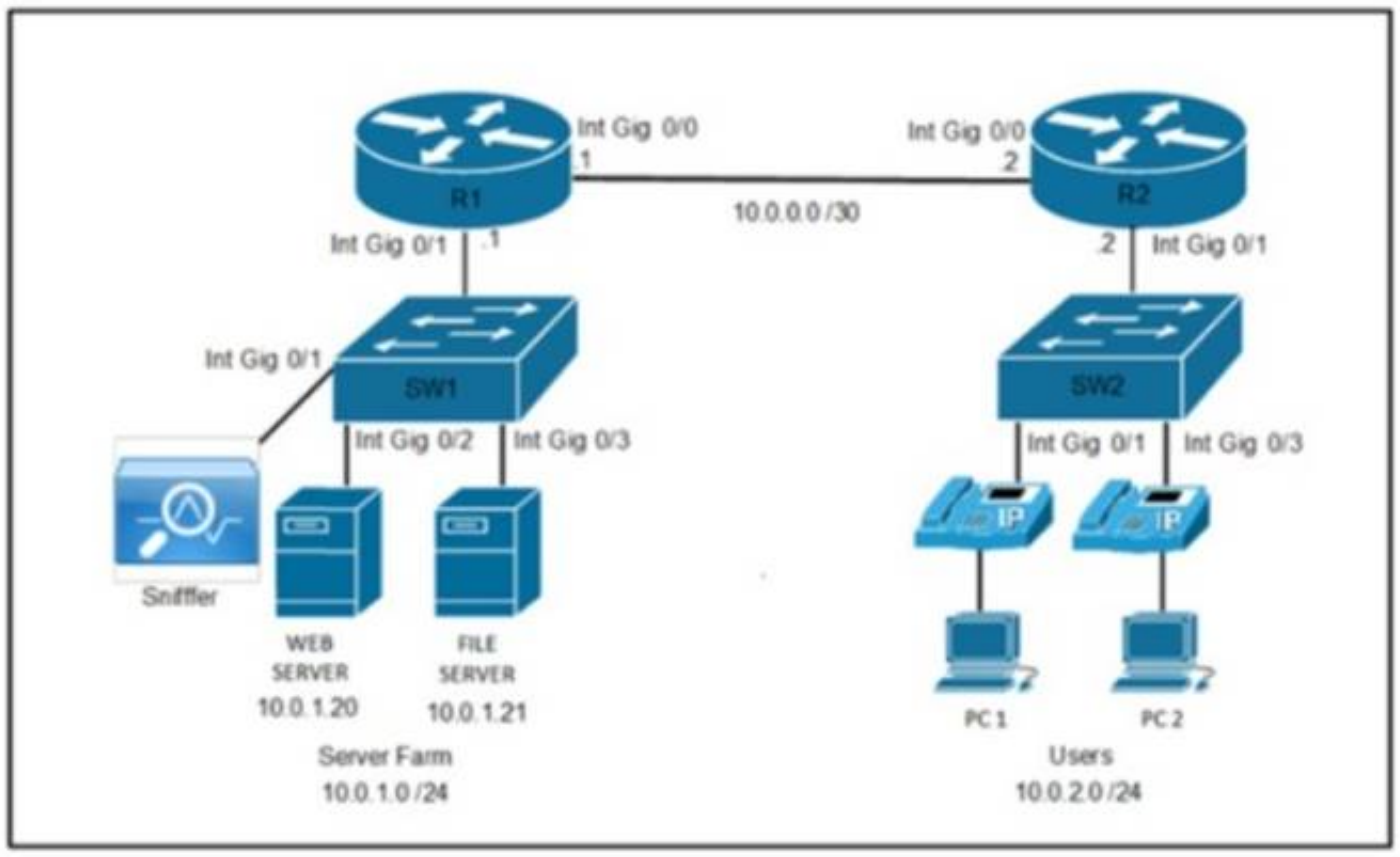
Which IP address becomes the active next hop for 192.168.102 0/24 when 192.168.101.2 fails?

A. 192.168.101.18
B. 192.168.101.6
C. 192.168.101.10
D. 192.168.101.14

Answer: A

Explanation:
The '>' shown in the output above indicates that the path with a next hop of 192.168.101.2 is the current best path.
Path Selection Attributes: Weight > Local Preference > Originate > AS Path > Origin > MED >
External > IGP Cost > eBGP Peering > Router ID
BGP prefers the path with highest weight but the weights here are all 0 (which indicate all routes
that are not originated by the local router) so we need to check the Local Preference.
Answer
'192.168.101.18' path without LOCAL_PREF (LocPrf column) means it has the default value of 100.
Therefore we can find the two next best paths with the next hop of 192.168.101.18 and 192.168.101.10.
We have to move to the next path selection attribute: Originate. BGP prefers the path that the
local router originated (which is indicated with the "next hop 0.0.0.0"). But none of the two best
paths is self-originated.
The AS Path of the next hop 192.168.101.18 is shorter than the AS Path of the next hop 192.168.101.10 then the next hop 192.168.101.18 will be chosen as the next best path.

NEW QUESTION 452
- (Topic 4)



Refer to the exhibit. A network engineer Is troubleshooting an Issue with the file server based on reports of slow file transmissions. Which two commands or command sets are required. In switch SW1 to analyze the traffic from the file server with a packet analyzer? (Choose two.)

A)

```
SW1#show monitor
```

B)

```
SW1(config)# monitor session 1 source interface gigabitethernet0/3
SW1(config)# monitor session 1 destination interface gigabitethernet0/1 encapsulation replicate
```

C)

```
SW1#show ip route
```

D)

```
SW1#show vlan
```

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

Answer: AC

NEW QUESTION 456
- (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 458
- (Topic 4)
Which free application has the ability to make REST calls against Cisco DNA Center?

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

Answer: C

NEW QUESTION 462
- (Topic 4)
Which two results occur if Cisco DNA Center loses connectivity to devices in the SD- Access fabric? (Choose two)

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

Answer: AE

NEW QUESTION 464
- (Topic 4)
A network administrator received reports that a 40Gb connection is saturated. The only server the administrator can use for data collection in that location has a 10Gb connection to the network. Which of the following is the best method to use on the server to determine the source of the saturation?

A. Port mirroring
B. Log aggregation
C. Flow data
D. Packet capture

Answer: C

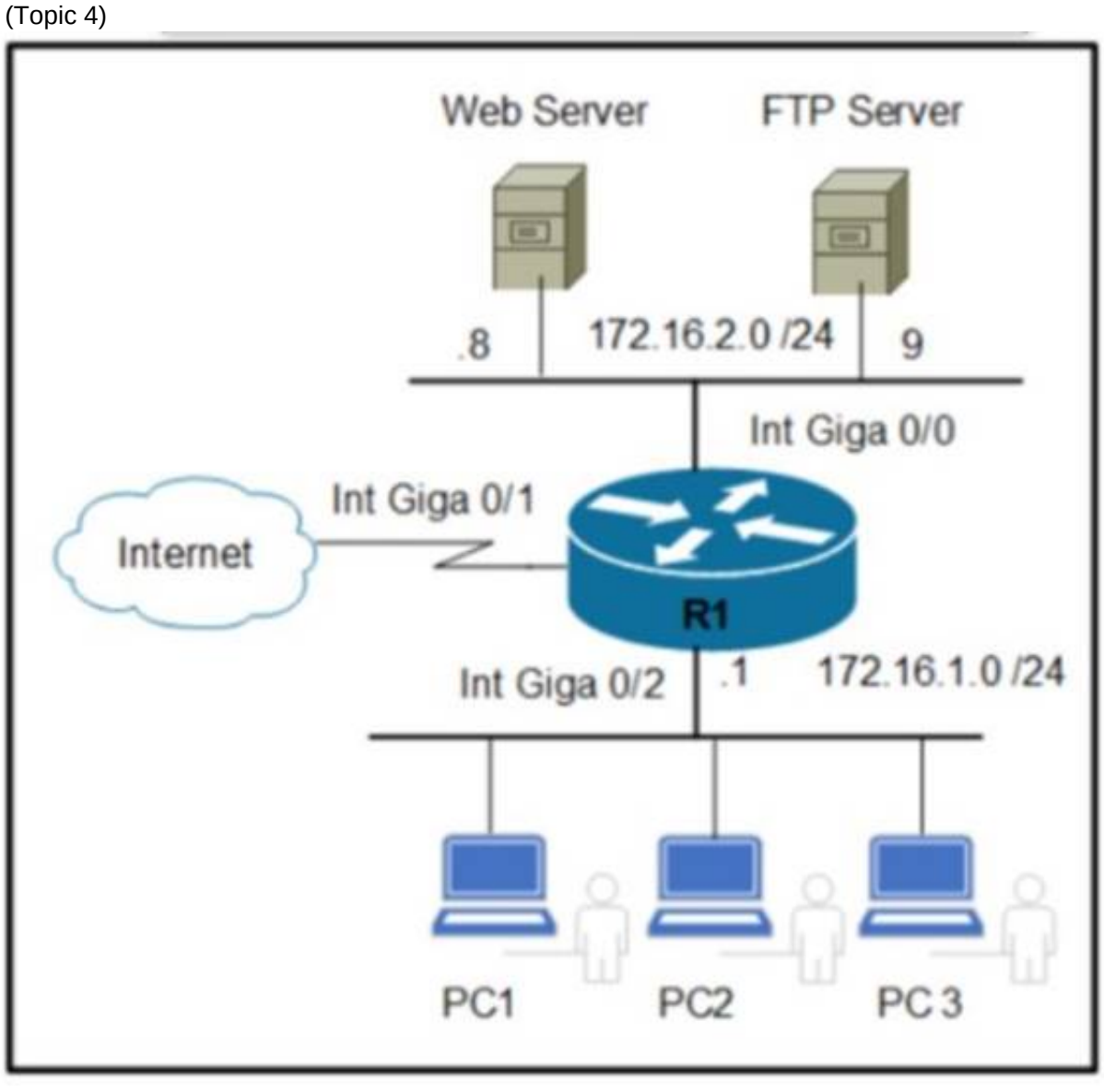
Explanation:
This is because flow data is a method of collecting and analyzing information about the traffic flows on a network. Flow data can provide details such as the source and destination IP addresses, ports, protocols, and bytes transferred for each flow. Flow data can help identify the source of the saturation by showing which hosts and applications are generating or consuming the most bandwidth. Flow data can be collected using protocols such as NetFlow, IPFIX, or sFlow. The source of this answer is the Cisco ENCOR v1.1 course, module 10, lesson 10.1: Implementing NetFlow and IPFIX.

NEW QUESTION 469
- (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 471
- (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
```

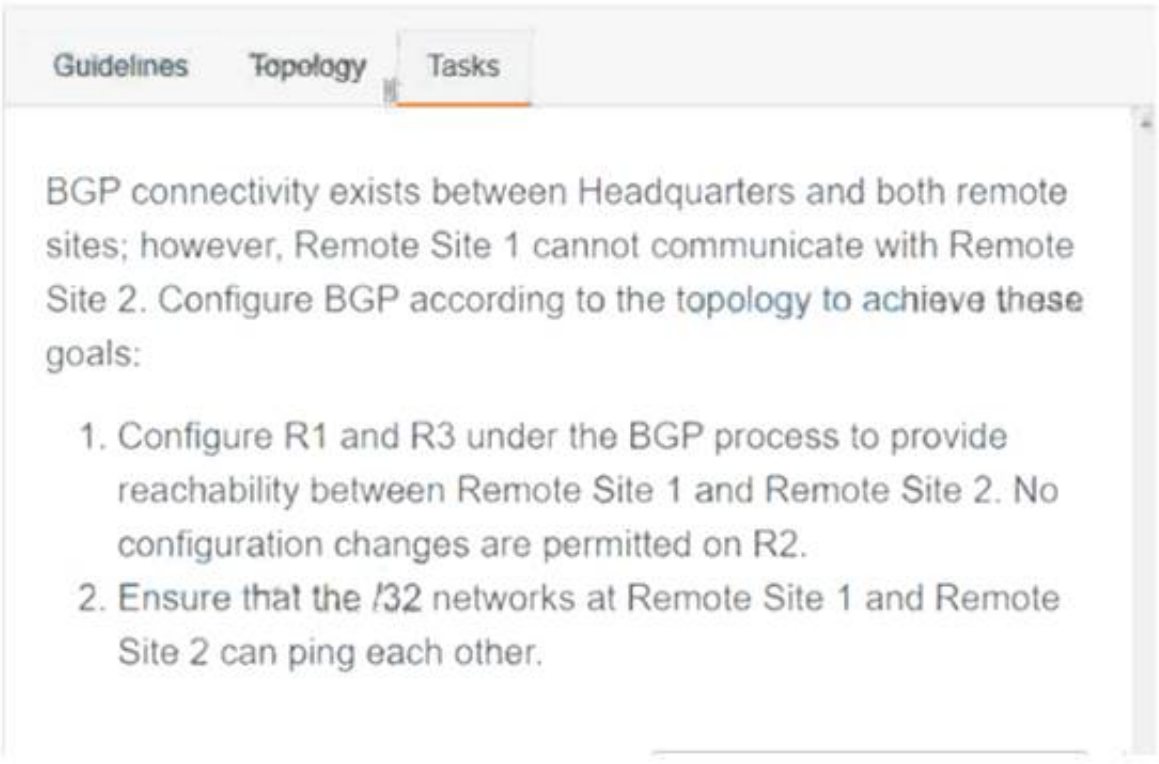
D)

```
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 473
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.



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
```

R1 R3

```
 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
```

R1 R3

```
 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
!
```

R1 R3

```
 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

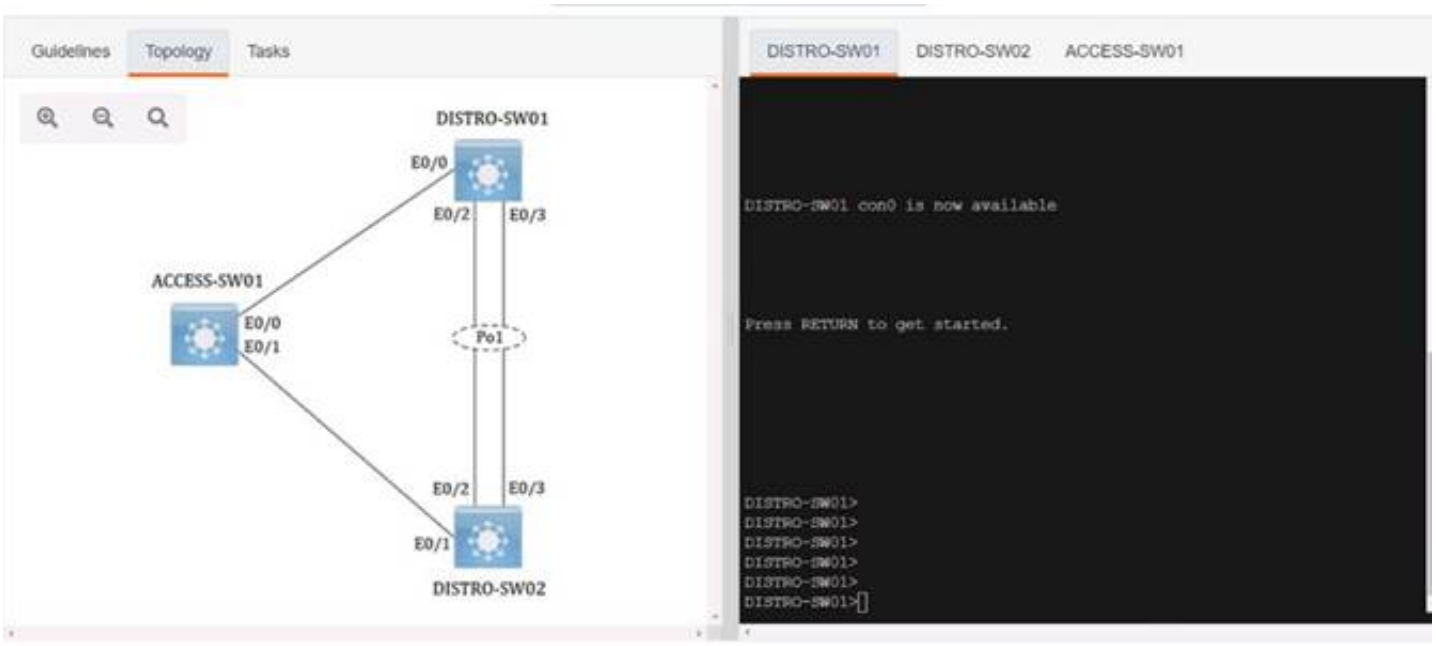
Explanation:
See the solution below in Explanation:
- Solution:
On R1:
R1(config)#router bgp 123
R1(config-router)#address-family ipv4
R1(config-router-af)#neighbor 10.0.0.2 allowas-in
On R3:
R3(config)#router bgp 123
R3(config-router)# address-family ipv4
R3(config-router-af)#neighbor 192.168.1.2 allowas-in
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

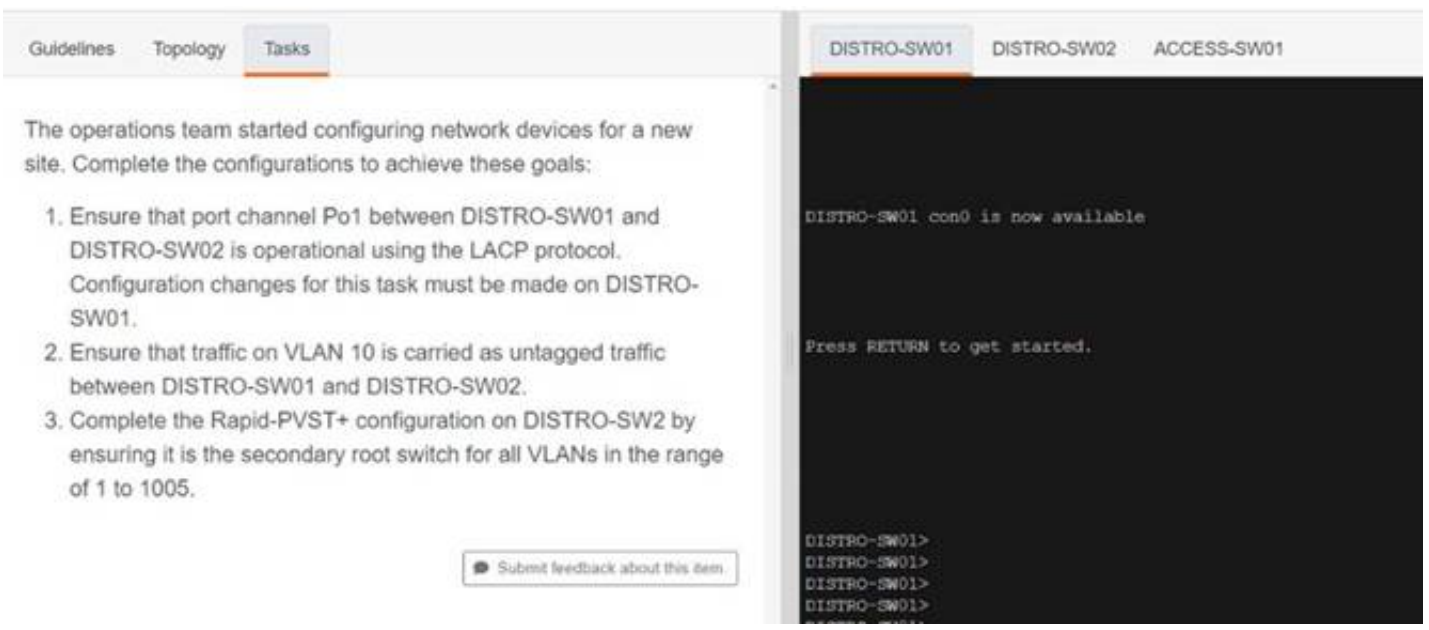
NEW QUESTION 478
- (Topic 4)
What are two characteristics of Cisco SD-Access elements? (Choose two.)

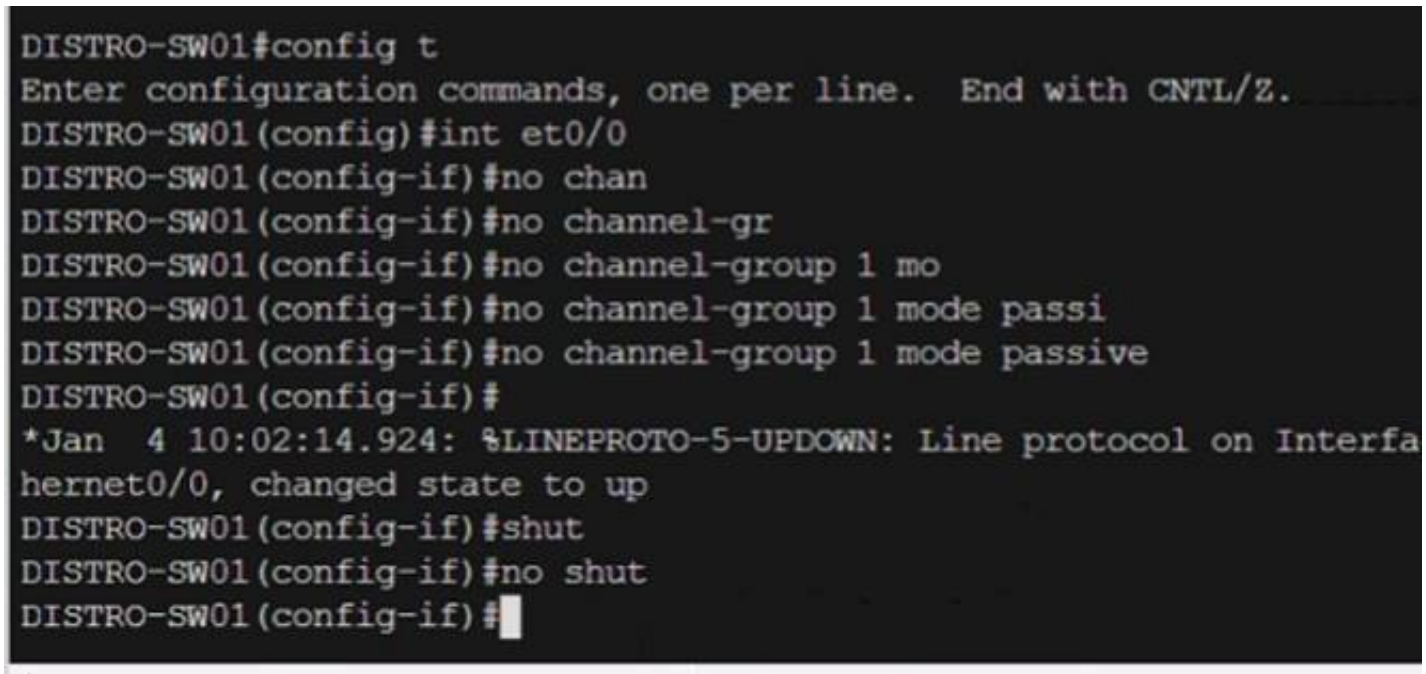
A. The border node is required for communication between fabric and nonfabric devices.
B. Traffic within the fabric always goes through the control plane node.
C. Fabric endpoints are connected directly to the border node.
D. The control plane node has the full RLOC-to-EID mapping database.
E. The border node has the full RLOC-to-EID mapping database.

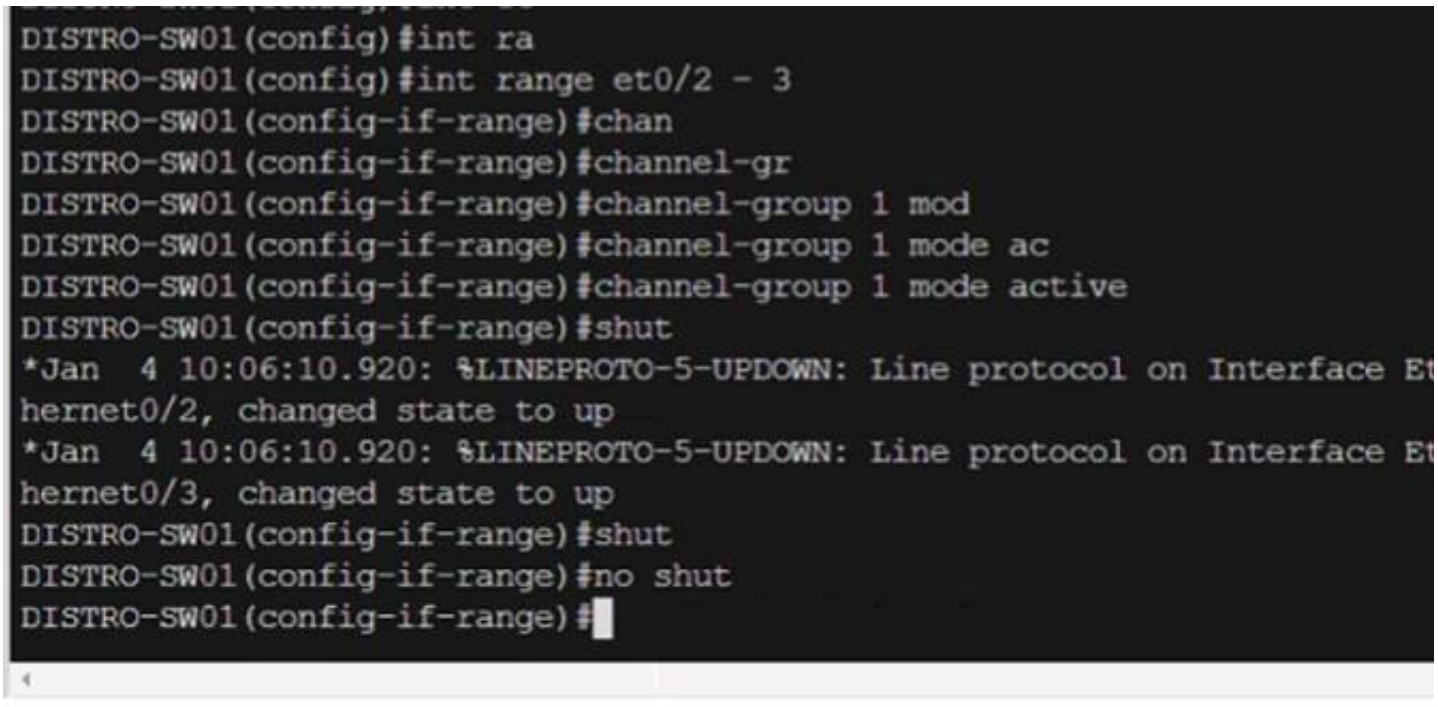
Answer: AD

NEW QUESTION 481
SIMULATION - (Topic 4)
Simulation 06









A. Mastered
B. Not Mastered

Answer: A

Explanation:

Distro-Switch1
Int et0/0
No Channel-group 1 mode passive
Int range et0/2-3
No Channel-group 1 mode passive Channel-group 1 mode active Shut
No shut
Int port 1
Switchport trunk native vlan 10 Copy run start
Distro-Switch2
Int port 1
Switchport trunk native vlan 10 Copy run start
Distro-Switch2
Spanning-tree vlan 1-1005 root secondary Copy run start

NEW QUESTION 483
- (Topic 4)
When a wired client connects to an edge switch in a Cisco SD-Access fabric, which component decides whether the client has access to the network?

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

Answer: C

NEW QUESTION 485
- (Topic 4)
the following system log message is presented after a network administrator configures a GRE tunnel:
%TUN-5-RECURDOWN Interface Tunnel 0 temporarily disabled due to recursive routing Why is tunnel 0 disabled?

A. Because dynamic routing is not enabled
B. Because the tunnel cannot reach its tunnel destination

C. Because the best path to the tunnel destination is through the tunnel itself
D. Because the router cannot recursively identify its egress forwarding interface

Answer: C

NEW QUESTION 489
- (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 494
- (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

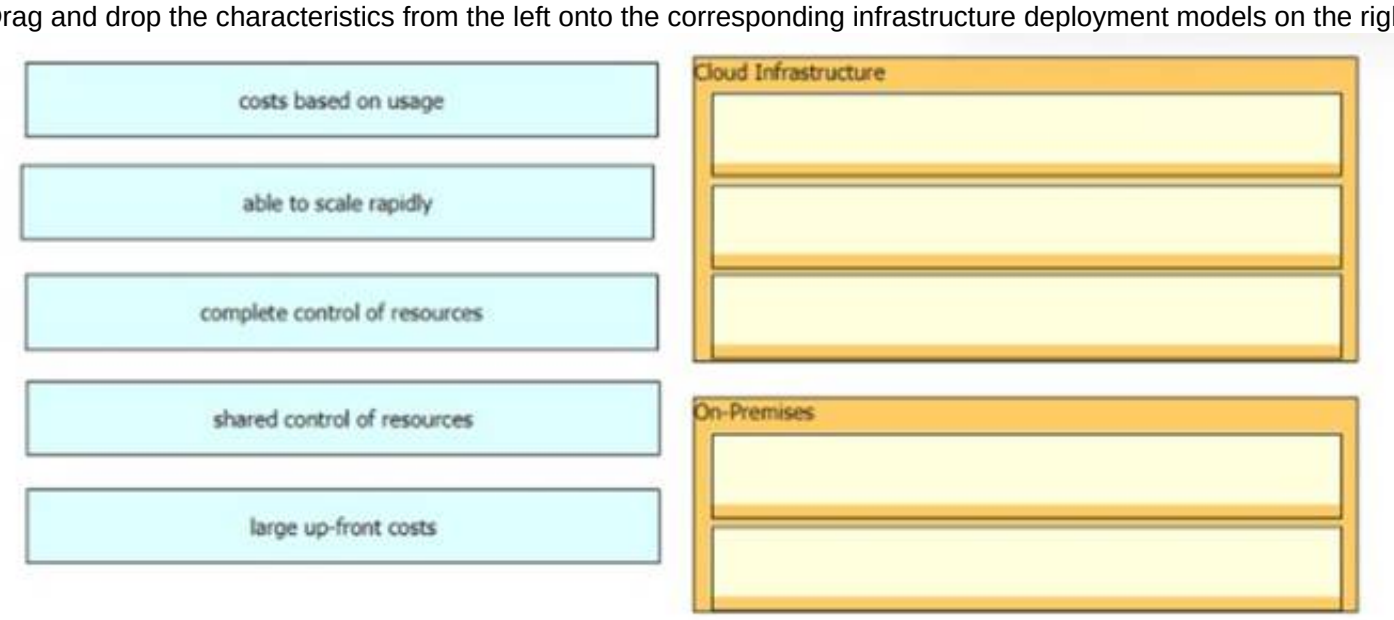
Answer: C

NEW QUESTION 495
- (Topic 4)
In a Cisco SD-Access fabric, which control plane protocol is used for mapping and resolving endpoints?

A. DHCP
B. VXLAN
C. SXP
D. LISP

Answer: D

NEW QUESTION 500
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the corresponding infrastructure deployment models on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
On-premises 3-5

NEW QUESTION 502
DRAG DROP - (Topic 3)
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

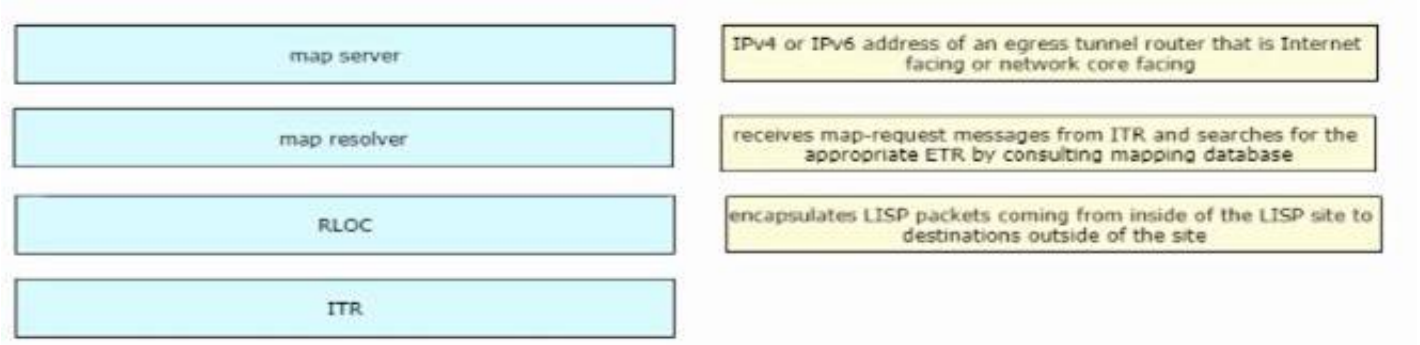
Explanation:
Chef
Communicates using knife tool Procedural
SaltStack
Communicates through SSH Declarative

NEW QUESTION 503
- (Topic 3)
Which two Cisco SD-Access components provide communication between traditional network elements and controller layer? (choose two)

A. network data platform
B. network underlay
C. fabric overlay
D. network control platform
E. partner ecosystem

Answer: BC

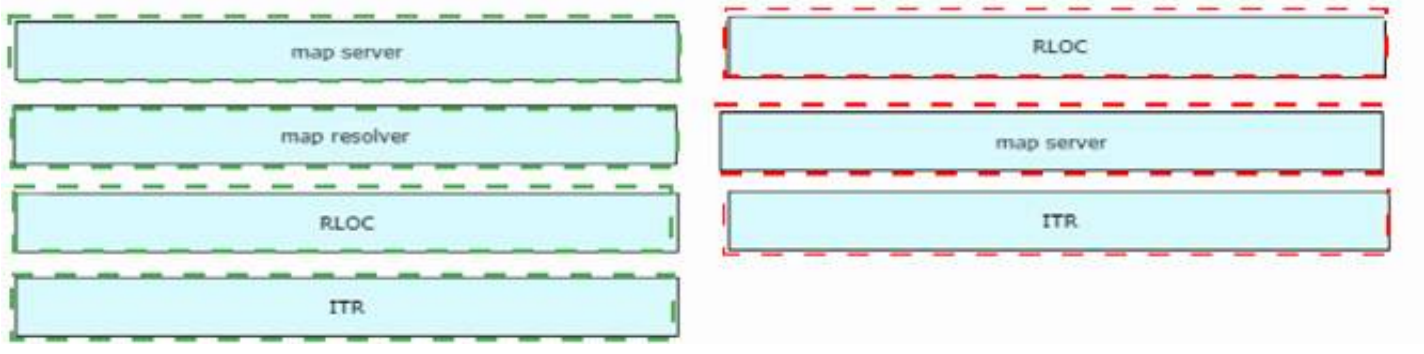
NEW QUESTION 508
DRAG DROP - (Topic 3)
Drag and drop the LISP components on the left to their descriptions on the right. Not all options are used.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

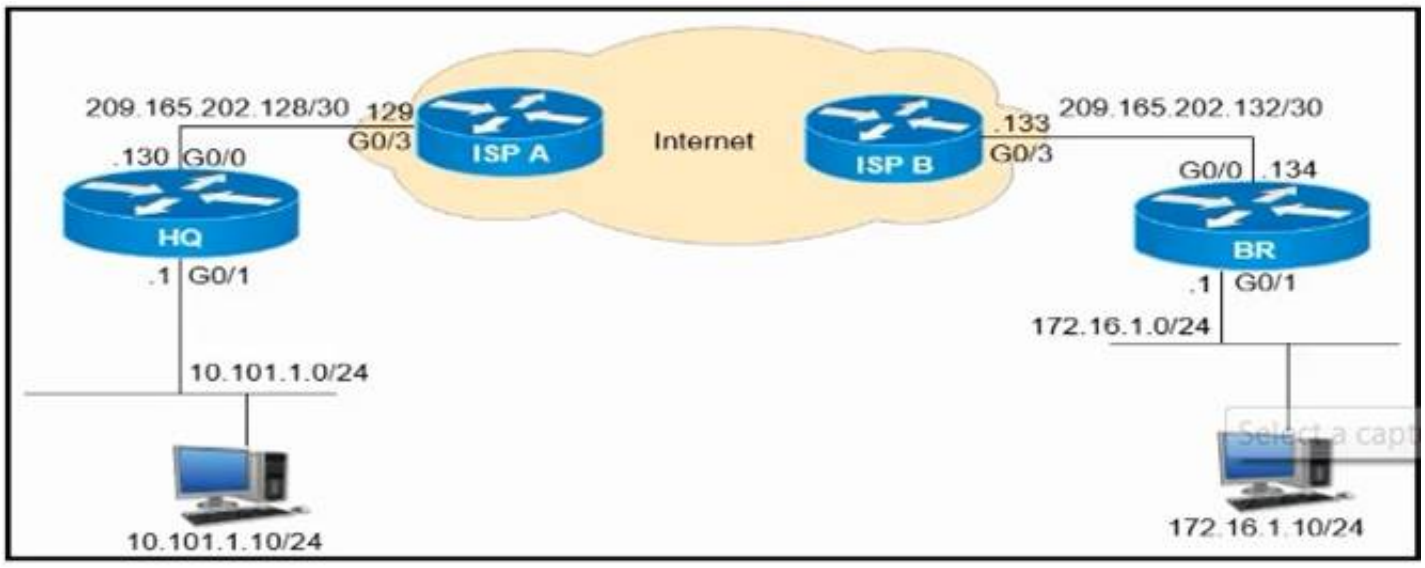


NEW QUESTION 513
- (Topic 3)
Which option must be used to support a WLC with an IPv6 management address and 100 Cisco Aironet 2800 Series access points that will use DHCP to register?

A. 43
B. 52
C. 60
D. 82

Answer: B

NEW QUESTION 518
- (Topic 3)
Refer to the exhibit.



Which configuration must be applied to the HQ router to set up a GRE tunnel between the HQ and BR routers?
A)

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.134
```

B)

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.133
```

C)

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

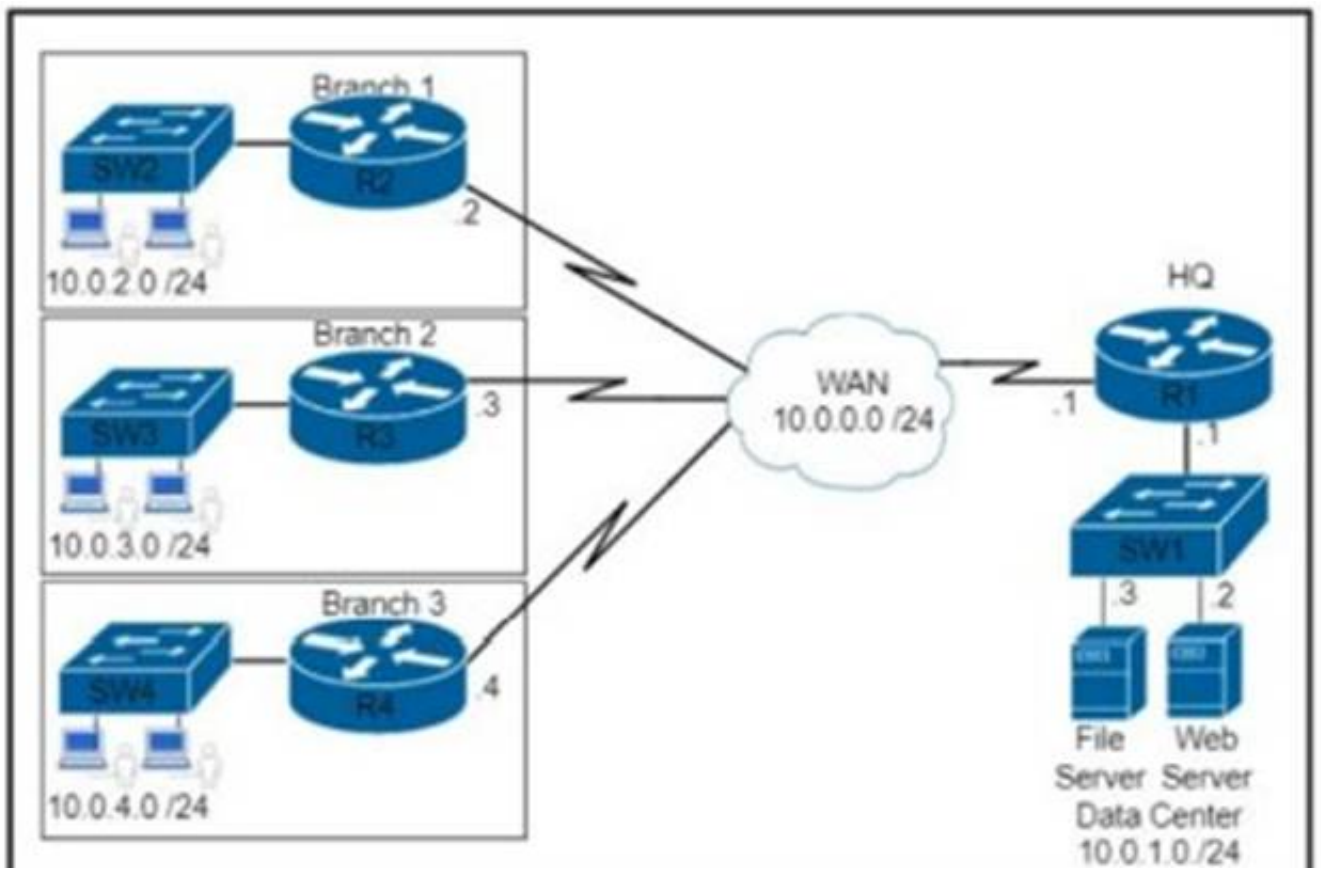
D)

```
interface Tunnel1
 ip address 209.165.202.130 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

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

Answer: A

NEW QUESTION 521
- (Topic 3)
An engineer must configure a router to leak routes between two VRFs Which configuration must the engineer apply?



ip access-list extended acl-to-red
permit ip any 10.1.1.0 0.0.0.255
route-map rm-to-red permit 10
match ip address 50
ip vrf RED
rd 1:1
import ipv4 unicast map rm-to-red

ip access-list extended acl-to-red
permit ip 10.1.1.0 0.0.0.255 any
route-map rm-to-red permit 10
match ip address acl-to-red
ip vrf RED
rd 1:1
import ipv4 unicast map rm-to-red

ip access-list extended acl-to-red
permit ip 10.1.1.0 0.0.0.255 any
route-map rm-to-red permit 10
match ip address acl-to-red
ip vrf RED
rd 1:1
import ipv4 unicast route-map acl-to-red

ip access-list extended acl-to-red
permit ip 10.1.1.0 0.0.0.255 any
route-map rm-to-red permit 10
match ip address acl-to-red
ip vrf RED
rd 1:1

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

Answer: B

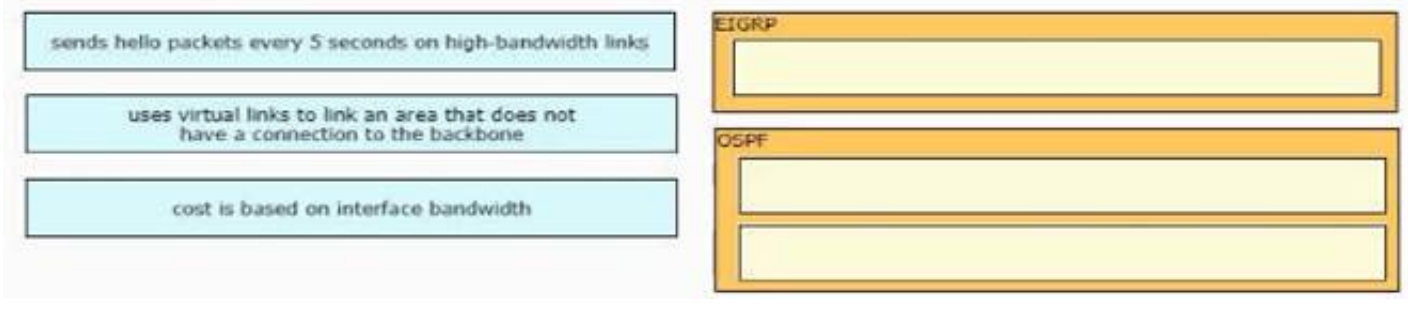
NEW QUESTION 526
- (Topic 3)
A system must validate access rights to all its resources and must not rely on a cached permission matrix. If the access level to a given resource is revoked but is not reflected in the permission matrix, the security is violated. Which term refers to this REST security design principle?

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

Answer: B

Explanation:
A system should validate access rights to all its resources to ensure that they are allowed and should not rely on the cached permission matrix. If the access level to a given resource is being revoked, but that is not being reflected in the permission matrix, it would be violating security.
https://medium.com/strike-sh/rest-security-design-principles-434bd6ee57ea

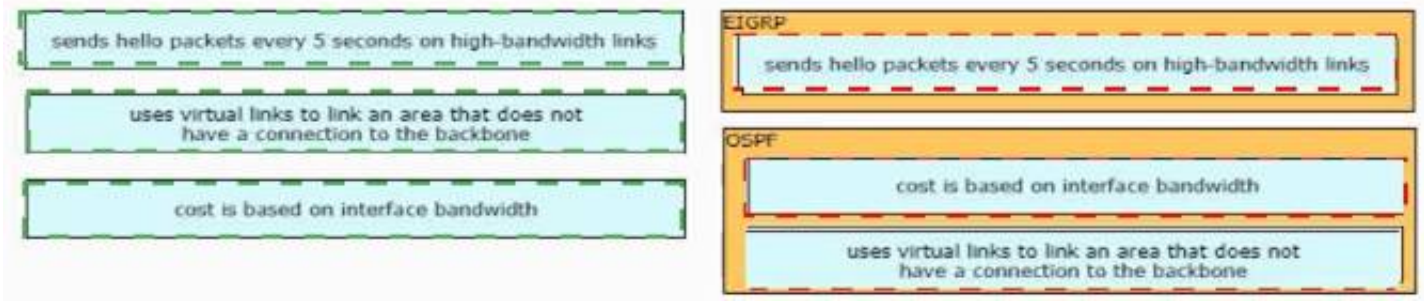
NEW QUESTION 531
DRAG DROP - (Topic 3)
Drag and drop the characteristics from the left onto the routing protocols they describe on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 532
- (Topic 3)
Which two solutions are used for backing up a Cisco DNA Center Assurance database? (Choose two)

A. NFS share
B. non-linux server
C. local server
D. remote server
E. bare metal server

Answer: AE

Explanation:
Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name.To support Assurance data backups, the server must be a Linux-based NFS server that meets the following requirements:– Support NFS v4 and NFS v3.– Cisco DNA Center stores backup copies of Assurance data on an external NFS device and automation data on an external remote sync (rsync) target location.– The remote share for backing up an Assurance database (NDP) must be an NFS share.
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/admin_guide/b_cisco_dna_center_admin_guide_2_1_2/b_cisco_dna_center_admin_guid e_2_1_1_chapter_0110.html

NEW QUESTION 537
- (Topic 3)

```
R1#show ip interface brief | include 192.168.12
FastEthernet0/0    192.168.12.1   YES manual up                    up

R1#ping vrf CUST-A 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1#show ip arp 192.168.12.2
R1#
```

Refer to the exhibit. A network engineer checks connectivity between two routers. The engineer can ping the remote endpoint but cannot see an ARP entry. Why is there no ARP entry?

A. The ping command must be executed in the global routing table.
B. Interface FastEthernet0/0 Is configured in VRF CUST-A, so the ARP entry is also in that VRF.
C. When VRFs are use
D. ARP protocol must be enabled In each VRF.

E. When VRFs are use
F. ARP protocol is disabled in the global routing table.

Answer: B

NEW QUESTION 538
- (Topic 3)
What is an OVF?

A. a package that is similar to an IMG and that contains an OVA file used to build a virtual machine
B. an alternative form of an ISO that Is used to install the base operating system of a virtual machine
C. the third step in a P2V migration
D. a package of files that is used to describe a virtual machine or virtual appliance

Answer: D

NEW QUESTION 540
- (Topic 3)
Refer to the exhibit.

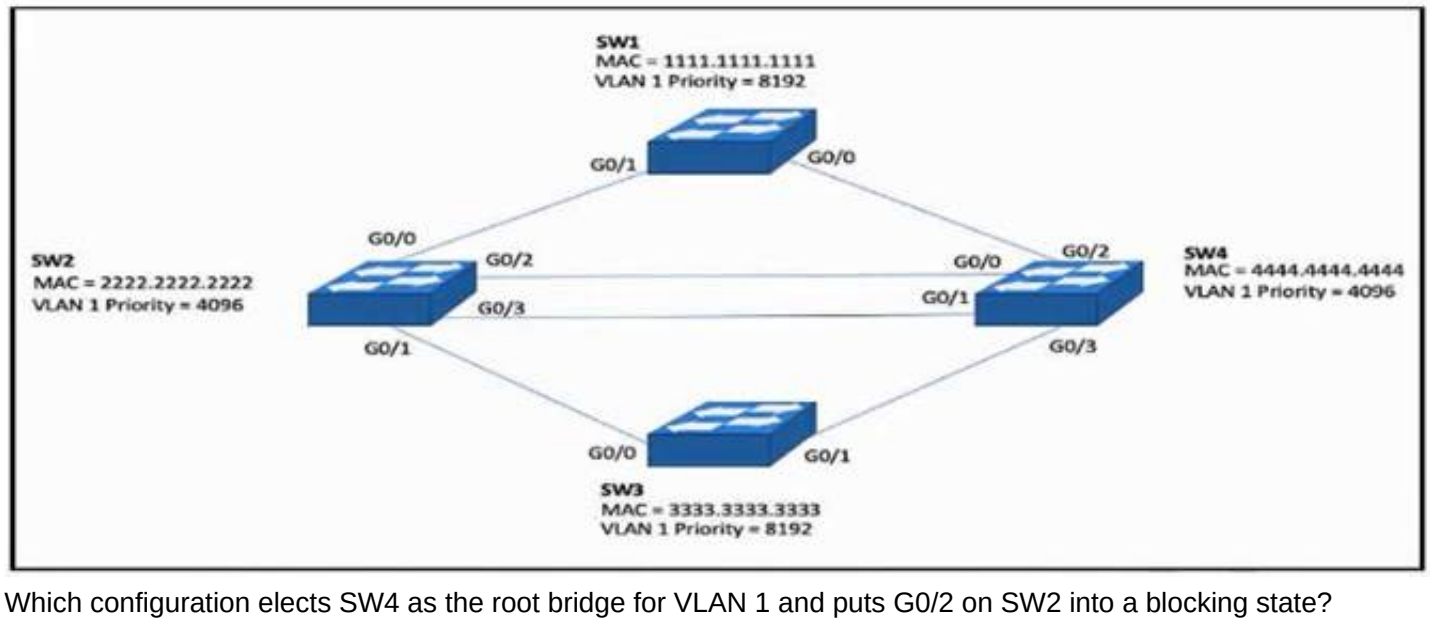
```
Router# show running-config

! lines omitted for brevity


username cisco password 0 cisco

aaa authentication login group1 group radius line
aaa authentication login group2 group radius local
aaa authentication login group3 group radius none

line con 0
password 0 cisco123
login authentication group1
line aux 0
login authentication group3
line vty 0 4
password 0 test123
login authentication group2
```

A network engineer must log in to the router via the console, but the RADIUS servers are not reachable Which credentials allow console access1?

A. the username "cisco" and the password "Cisco"
B. no username and only the password "test123"
C. no username and only the password "cisco123"
D. the username "cisco" and the password “cisco123"

Answer: D

NEW QUESTION 544
- (Topic 3)
Refer the exhibit.



Which configuration elects SW4 as the root bridge for VLAN 1 and puts G0/2 on SW2 into a blocking state?

A)

```
SW4(config)#spanning-tree vlan 1 priority 0
!
SW2(config)#interface G0/2
SW2(config-if)#spanning-tree vlan 1 port-priority 64
```

B)

```
SW4(config)#spanning-tree vlan 1 priority 0
!
SW2(config)#int G0/2
SW2(config-if)#spanning-tree cost 128
```

C)

```
SW4(config)#spanning-tree vlan 1 priority 32768
!
SW2(config)#interface G0/2
SW2(config-if)#spanning-tree vlan 1 port-priority 0
```

D)

```
SW4(config)#spanning-tree vlan 1 priority 32768
!
SW2(config)#int G0/2
SW2(config-if)#spanning-tree cost 128
```

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

Answer: B

NEW QUESTION 547
- (Topic 3)
Which Python snippet should be used to store the devices data structure in a JSON file?

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

A)

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

B)

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

C)

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

D)

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

A. Option A

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

Answer: A

NEW QUESTION 552
- (Topic 3)
Refer to the exhibit.

```
import json
from requests import get

Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

Devices = open("devices.txt", "r")

for Device in Devices.readlines():
  Hostname, IP, Login, Pass = Device.strip().split(",")
  URL = f"https://{IP}/restconf/data/Cisco-IOS-XE-native:native"
  Creds = (Login, Pass)
  Response = get(URL, auth = Creds, headers = Headers, verify = False)
```

How should the script be completed so that each device configuration is saved into a JSON-formatted file under the device name?
A)

Insert after the for loop:

```
with open(f'{Hostname}.json", "w") as OutFile:
  OutFile.write(Response)
```

B)

Insert after the for loop:

```
with open(f'{Hostname}.json", "w") as OutFile:
  OutFile.write(json.dumps(Response.text))
```

C)

Append to the body of the for loop:

```
with open(f'{Hostname}.json", "w") as OutFile:
  OutFile.write(Response.text)
```

D)

Insert immediately before the for loop:

```
with open(f'{Hostname}.json", "w") as OutFile:
  OutFile.write(json.load(Devices))
```

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

Answer: A

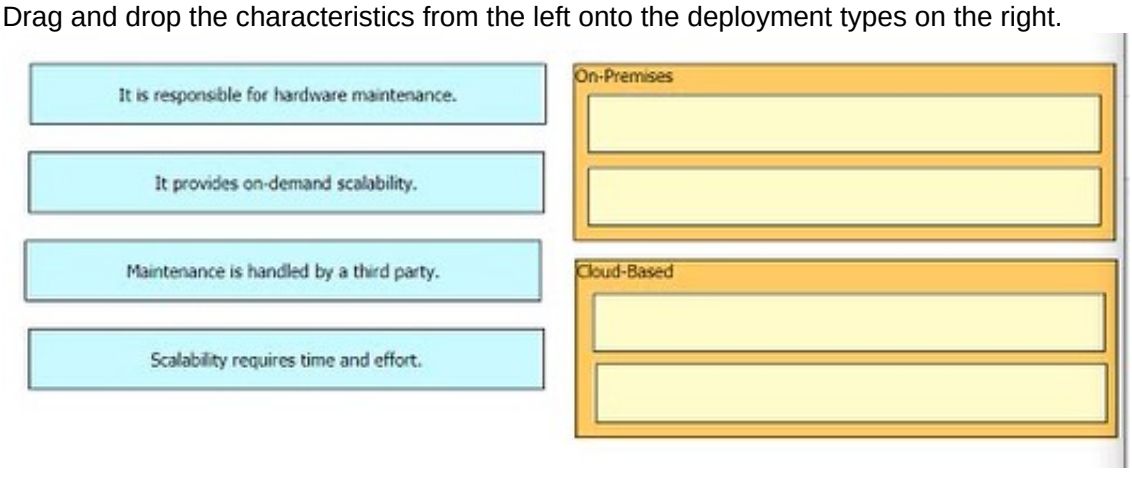
NEW QUESTION 555
- (Topic 3)
What is one main REST security design principle?

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

Answer: A

Explanation:
Separation of Privilege: Granting permissions to an entity should not be purely based on a single condition, a combination of conditions based on the type of resource is a better idea.
https://restfulapi.net/security-essentials/#:~:text=REST%20Security%20Design%20Principles&text=Least%20Privilege%3A%20An%20entity%20should,when%20no%20longer%20in%20use.

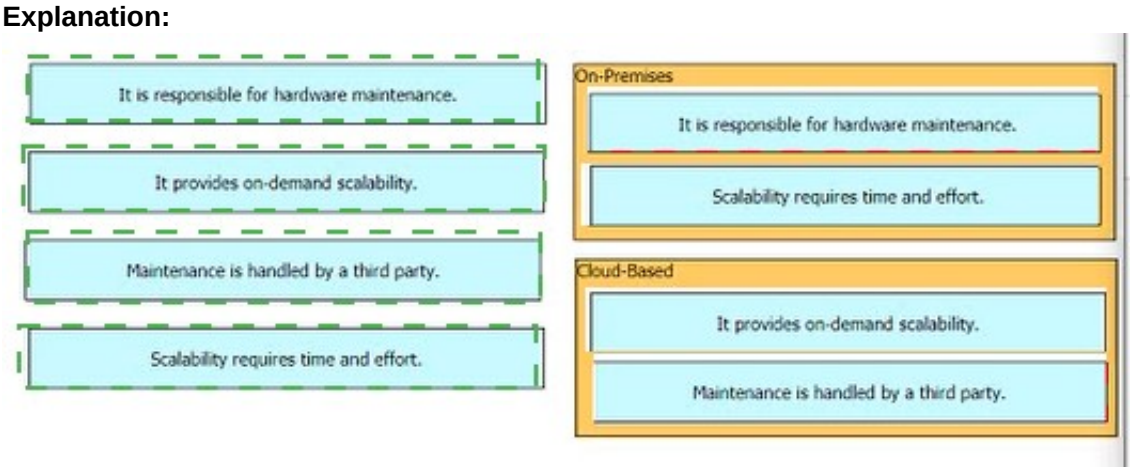
NEW QUESTION 556
DRAG DROP - (Topic 3)
Drag and drop the characteristics from the left onto the deployment types on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 557
- (Topic 3)
Which function does a fabric wireless LAN controller perform In a Cisco SD-Access deployment?

A. manages fabric-enabled APs and forwards client registration and roaming information to the Control Plane Node
B. coordinates configuration of autonomous nonfabric access points within the fabric
C. performs the assurance engine role for both wired and wireless clients
D. is dedicated to onboard clients in fabric-enabled and nonfabric-enabled APs within the fabric

Answer: A

Explanation:
Fabric Enabled WLC:
Fabric enabled WLC is integrated with LISP control plane. This WLC is responsible for AP image /Config, Radio Resource Management, Client Session management and roaming and all other wireless control plane functions.
For WLC Fabric Integration:
? Wireless Client MAC address is used as EID
? It inform about Wireless MAC address with its other information like SGT and Virtual Network Information
? VN information is mapped to VLAN on FEs
? WLC is responsible for updating Host Database tracking DB with roaming information
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design- guide.html#FabricWLC
Both fabric WLCs and non-fabric WLCs provide AP image and configuration management, client session management, and mobility services. Fabric WLCs provide additional services for fabric integration such as registering MAC addresses of wireless clients into the host tracking database of the fabric control plane nodes during wireless client join events and supplying fabric edge node RLOC-association updates to the HTDB during client roam events.

NEW QUESTION 558
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

350-401 Practice Exam Features:

* 350-401 Questions and Answers Updated Frequently

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

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

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