Cisco

Exam Questions 350-401

Implementing and Operating Cisco Enterprise Network Core Technologies

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
- (Topic 4)
Which two security features are available when implementing NTP? (Choose two.)

A. symmetric server passwords
B. dock offset authentication
C. broadcast association mode
D. encrypted authentication mechanism
E. access list-based restriction scheme

Answer: DE

NEW QUESTION 2
- (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 3
- (Topic 4)
Refer to the exhibit.

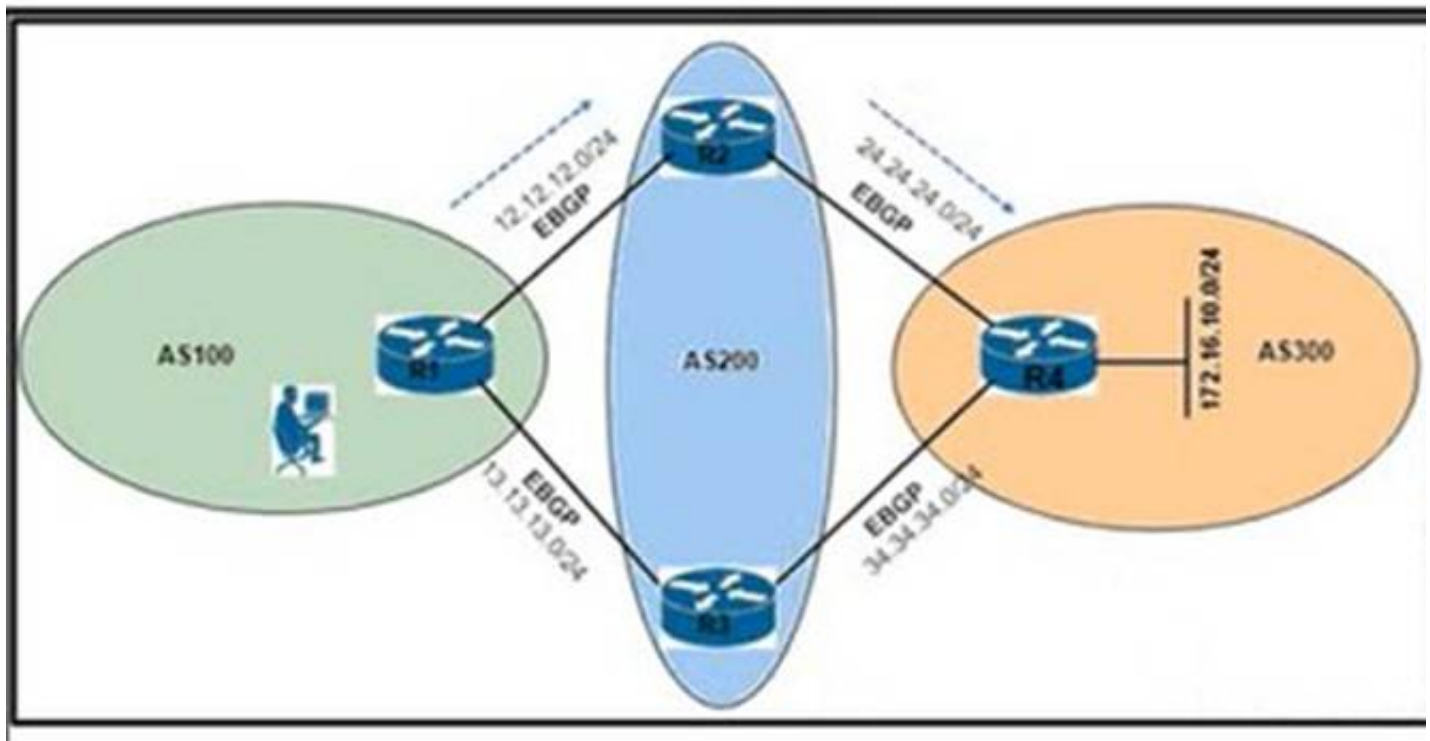
```
Router#show running-config | include aaa
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
aaa session-id common
```

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

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

Answer: B

NEW QUESTION 4
- (Topic 4)




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

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

A)

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

B)

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

C)

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

D)

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

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

Answer: D

NEW QUESTION 5
- (Topic 4)
Which tunnel type al'ows clients to perform a seamless Layer 3 roam between a Cisco AireOS WLC and a Cisco IOS XE WLC?

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

Answer: A

NEW QUESTION 6
- (Topic 4)
A network engineer must configure a switch to allow remote access for all feasible protocols. Only a password must be requested for device authentication and all idle sessions must be terminated in 30 minutes. Which configuration must be applied?

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

line console 0
password cisco
exec-timeout 30 0

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

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

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

Answer: C

NEW QUESTION 7
- (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 8
- (Topic 4)
Which mechanism can be used to enforce network access authentication against an AAA server if the endpoint does not support the 802.1X supplicant functionality?

A. private VLANs

B. port security
C. MAC Authentication Bypass
D. MACsec

Answer: C

NEW QUESTION 9
- (Topic 4)
What is the function of the fabric control plane node in a Cisco SD-Access deployment?

A. It is responsible for policy application and network segmentation in the fabric
B. It performs traffic encapsulation and security profiles enforcement in the fabric
C. It holds a comprehensive database that tracks endpoints and networks in the fabric
D. It provides integration with legacy nonfabric-enabled environments

Answer: C

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

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

Answer: A

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

NEW QUESTION 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 13
- (Topic 4)
Which IP SLA operation requires the IP SLA responder to be configured on the remote end?

A. TCP connect
B. ICMP echo
C. ICMP jitter
D. UDP jitter

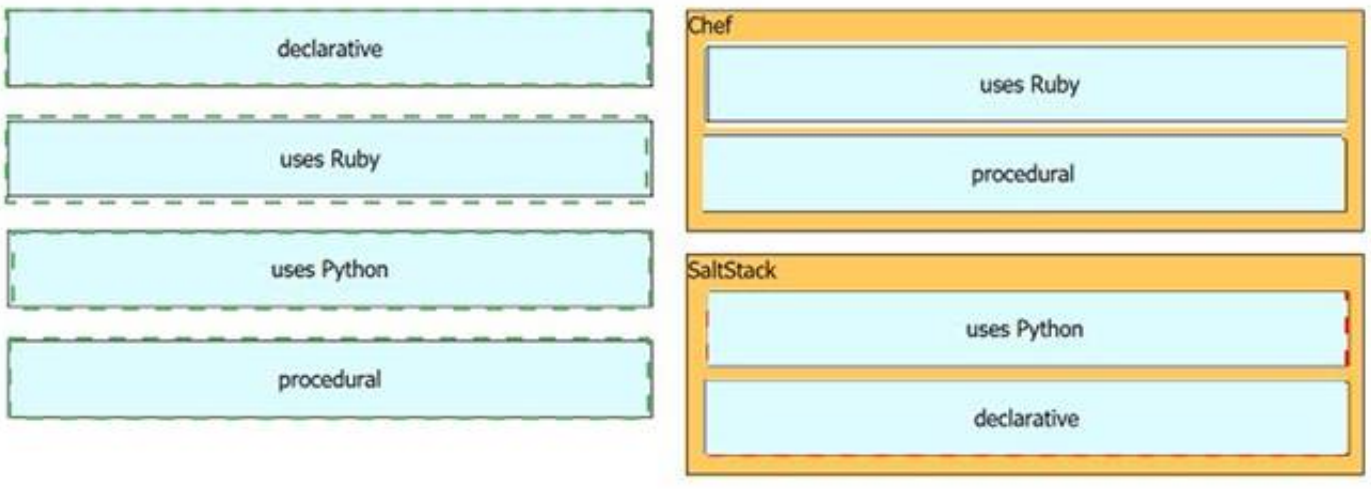
Answer: D

NEW QUESTION 16
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 18

- (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 19
- (Topic 4)
An engineer is connected to a Cisco router through a Telnet session. Which command must be issued to view the logging messages from the current session as soon as they are generated by the router?

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

Answer: D

NEW QUESTION 21
- (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 23
- (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.

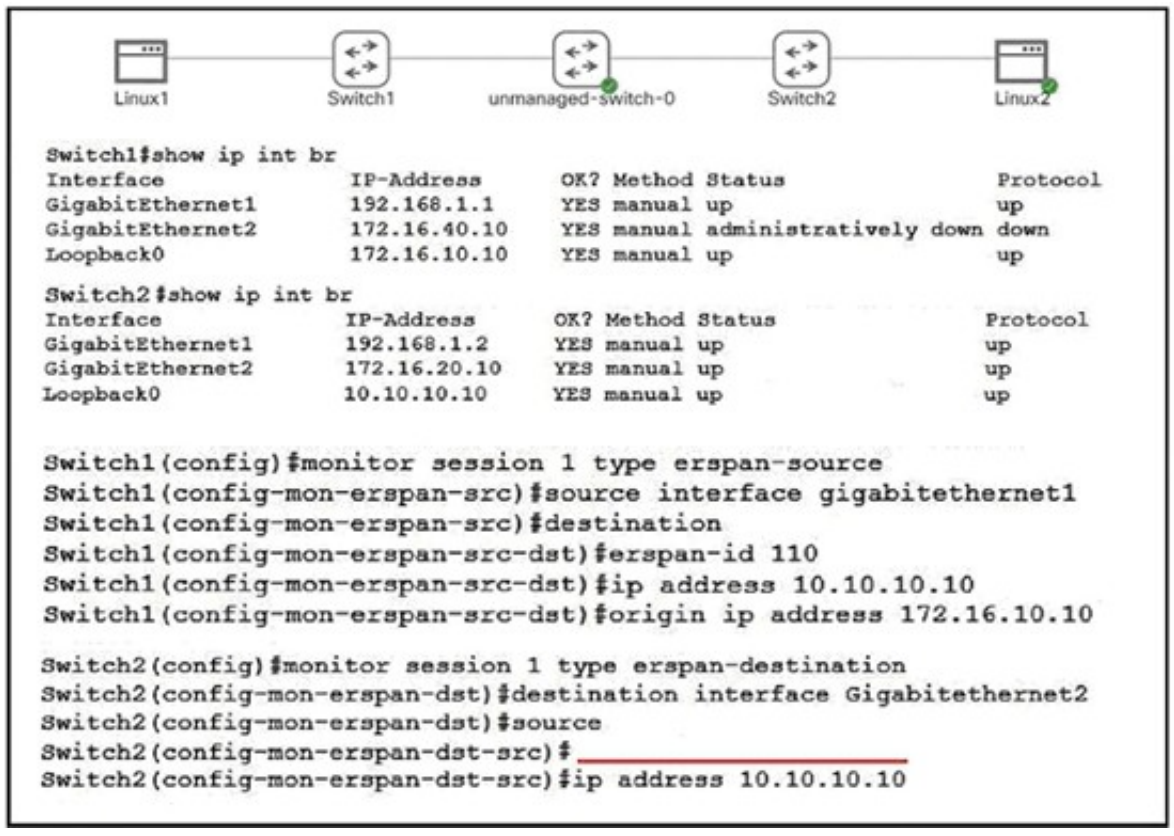
Answer: D

NEW QUESTION 27
- (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 31
- (Topic 4)



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

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

Answer: D

NEW QUESTION 34
- (Topic 4)
An engineer must configure a new WLAN that allows a user to enter a passphrase and provides forward secrecy as a security measure. Which Layer 2 WLAN configuration is required on the Cisco WLC?

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

Answer: C

NEW QUESTION 39
- (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 44
- (Topic 2)
Refer to the exhibit.

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

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

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

Answer: B

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

NEW QUESTION 48
- (Topic 2)
What is a characteristic of Cisco StackWise technology?

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

Answer: C

NEW QUESTION 53
- (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 54
- (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 59
- (Topic 2)
Refer to the exhibit.

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

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

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

Answer: A

NEW QUESTION 61
- (Topic 2)

What does a northbound API accomplish?

A. programmatic control of abstracted network resources through a centralized controller
B. access to controlled network resources from a centralized node
C. communication between SDN controllers and physical switches
D. controlled access to switches from automated security applications

Answer: A

NEW QUESTION 63
- (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
```

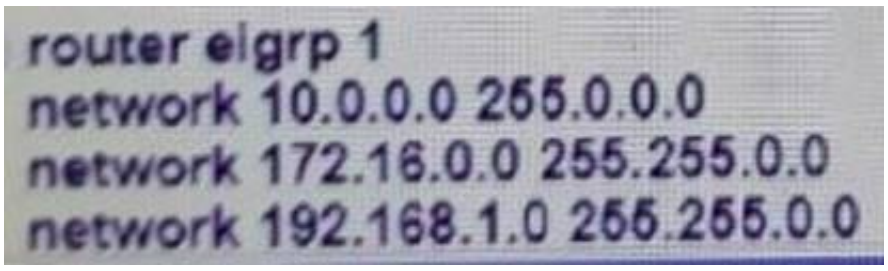
B)

```
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)

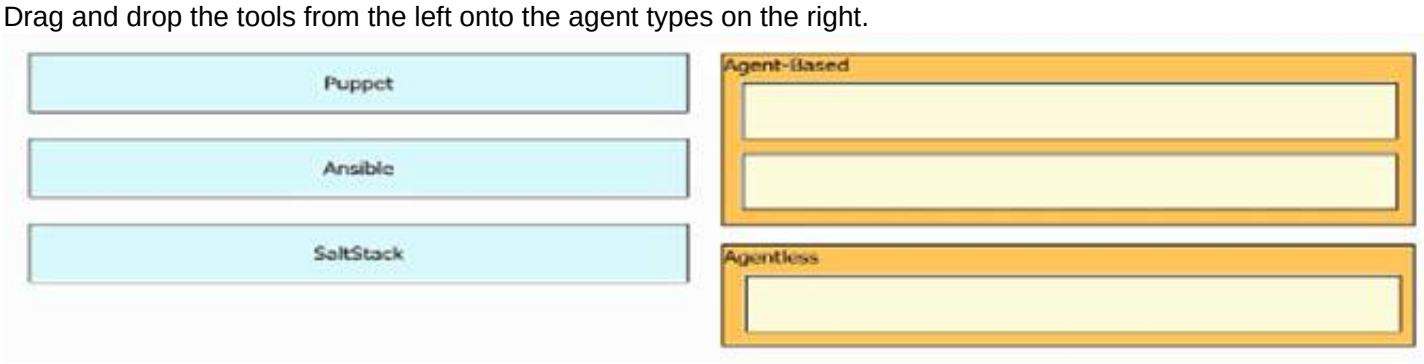


A. Option A
B. Option B
C. Option C
D. Option D

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.

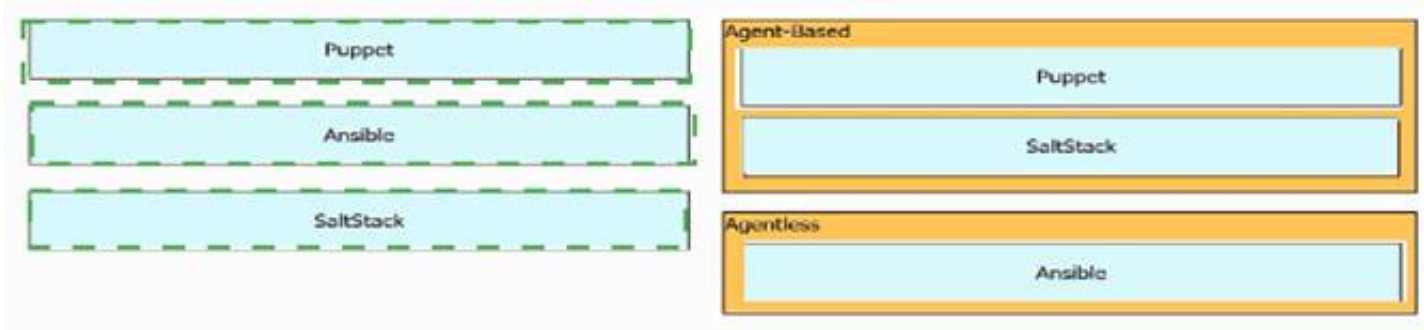
NEW QUESTION 67
DRAG DROP - (Topic 2)
Drag and drop the tools from the left onto the agent types on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 72
- (Topic 2)
Which outcome is achieved with this Python code?

```
client.connect ( ip,  port= 22, username= usr, password= pswd )
stdin,  stdout, stderr = client.exec_command ( 'show ip bgp 192.168.101.0 bestpath\n ' )
print (stdout)
```

A. connects to a Cisco device using SSH and exports the routing table information
B. displays the output of the show command in a formatted way
C. connects to a Cisco device using SSH and exports the BGP table for the prefix
D. connects to a Cisco device using Telnet and exports the routing table information

Answer: C

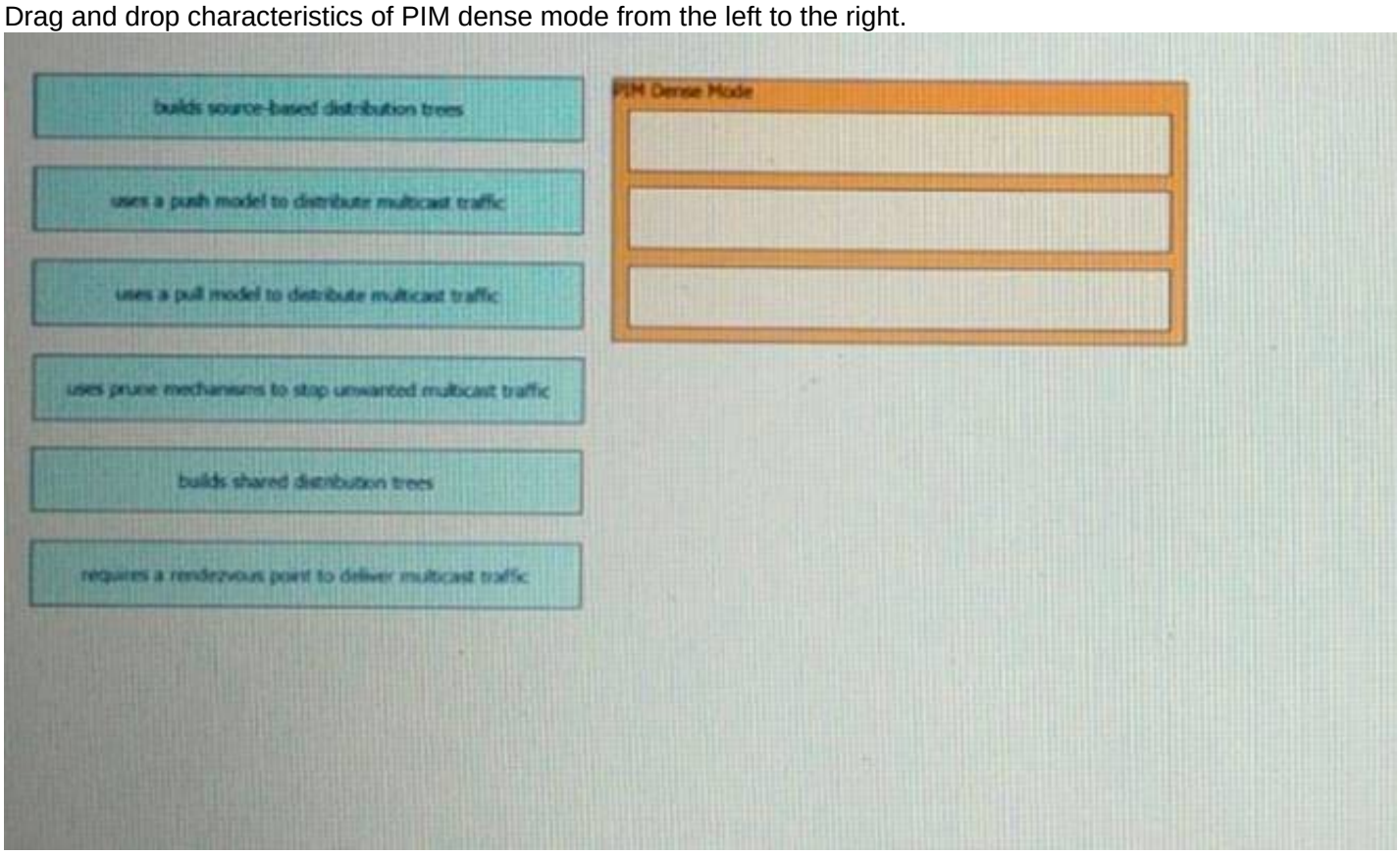
NEW QUESTION 75
- (Topic 2)
What is the function of a control-plane node In a Cisco SD-Access solution?

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

Answer: A

NEW QUESTION 79

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 83
- (Topic 2)
Why would a log file contain a * next to the date?

A. The network device was receiving NTP time when the log messages were recorded.
B. The network device was unable to reach The NTP server when the log messages were recorded
C. The network device is not configured to use NTP.
D. The network device is nor configured to use NTP time stamps for logging

Answer: B

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

```
R1#show ip bgp sum
BGP router identifier 1.1.1.1, local AS number 65001
<output omitted>

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.50.2    4        65002       0       0        1    0    0 00:00:46 Idle (Admin)
```

Which command set changes the neighbor state from Idle (Admin) to Active?
A)

```
R1(config)#router bgp 65002
R1(config-router)#neighbor 192.168.50.2 activate
```

B)

```
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 activate
```

C)

```
R1(config)#router bgp 65001
R1(config-router)#no neighbor 192.168.50.2 shutdown
```

D)

```
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 remote-as 65001
```

A. Option A

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

Answer: C

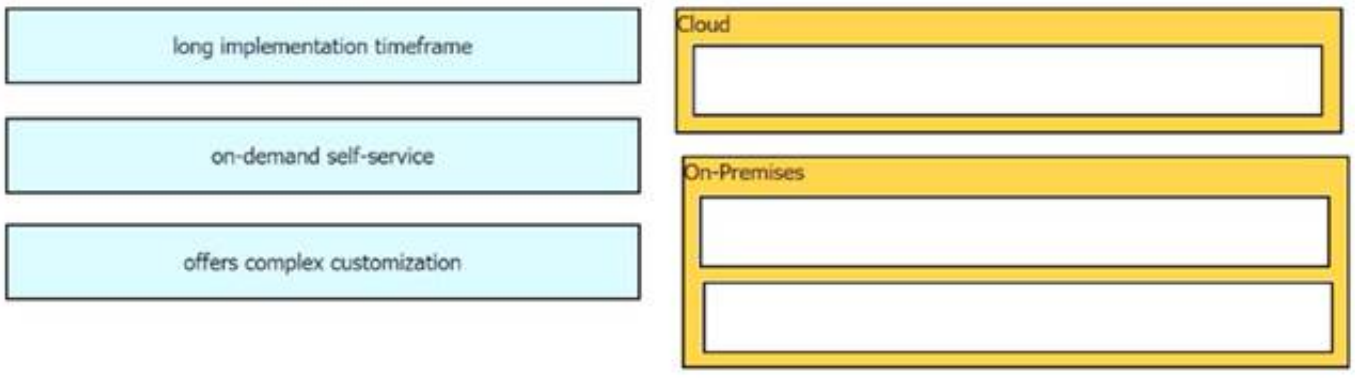
NEW QUESTION 90
- (Topic 2)
What is the structure of a JSON web token?

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

Answer: A

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

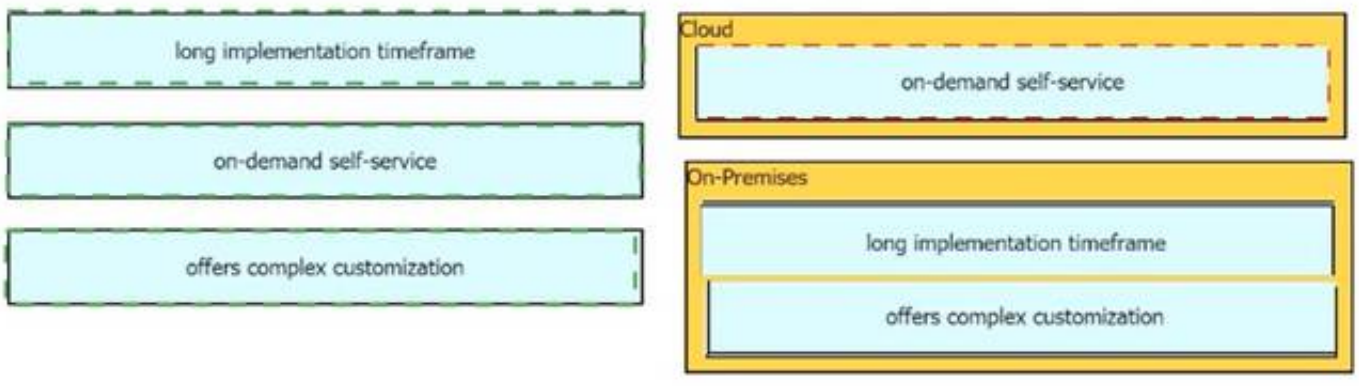
NEW QUESTION 93
DRAG DROP - (Topic 2)
Drag and drop the characteristics from the left onto the deployment models on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

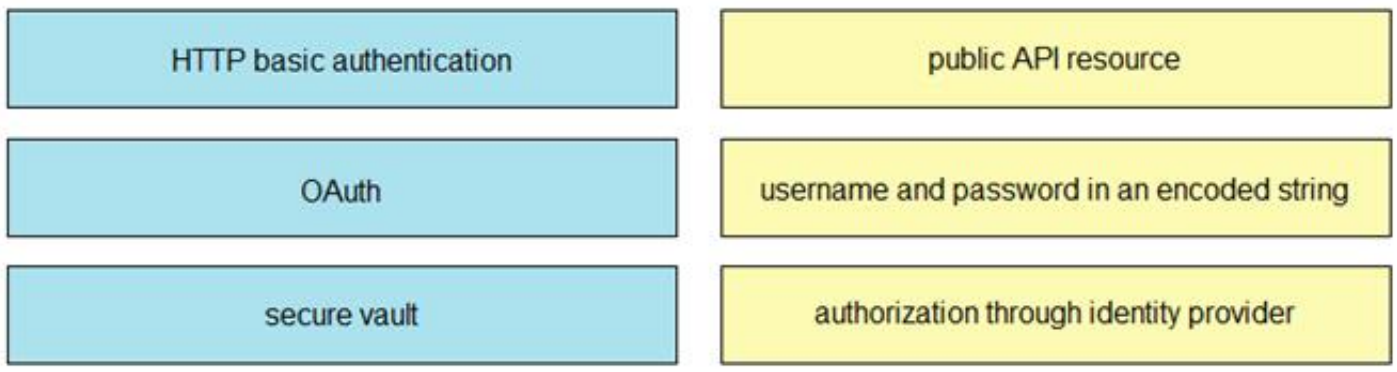


NEW QUESTION 96
- (Topic 2)
What is a characteristic of Cisco DNA Northbound APIs?

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

Answer: C

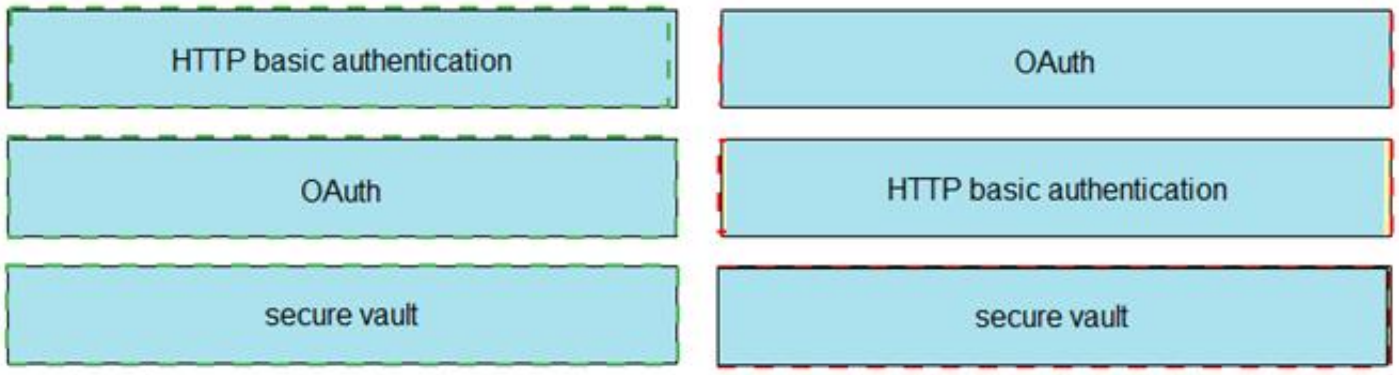
NEW QUESTION 98
DRAG DROP - (Topic 2)
Drag and drop the REST API authentication methods from the left onto their descriptions on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

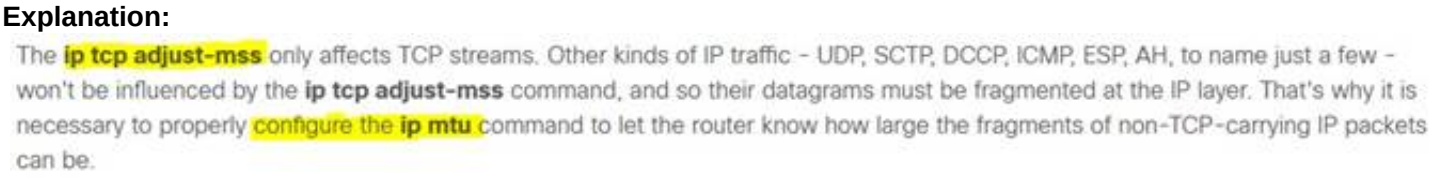


NEW QUESTION 100
- (Topic 2)
Which two GRE features are configured to prevent fragmentation? (Choose two.)

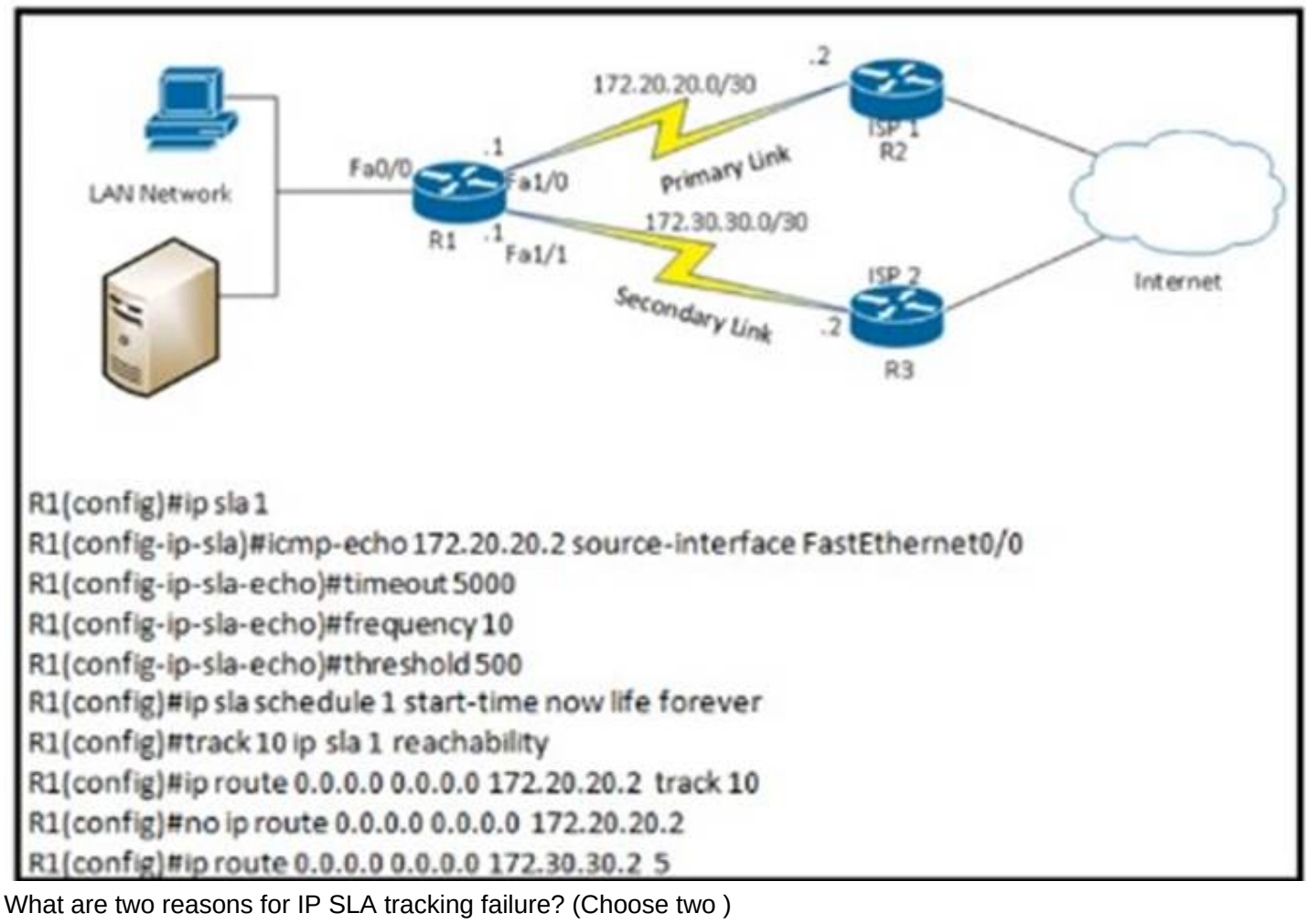
A. TCP MSS
B. PMTUD
C. DF bit Clear
D. MTU ignore
E. IP MTU
F. TCP window size

Answer: AE

Explanation:


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

NEW QUESTION 101
- (Topic 2)
Refer to the exhibit.




```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 172.20.20.2 source-interface FastEthernet0/0
R1(config-ip-sla-echo)#timeout 5000
R1(config-ip-sla-echo)#frequency 10
R1(config-ip-sla-echo)#threshold 500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track 10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2  track 10
R1(config)#no ip route 0.0.0.0 0.0.0.0 172.20.20.2
R1(config)#ip route 0.0.0.0 0.0.0.0 172.30.30.2 5
```

What are two reasons for IP SLA tracking failure? (Choose two)

A. The destination must be 172 30 30 2 for icmp-echo
B. A route back to the R1 LAN network is missing in R2.
C. The source-interface is configured incorrectly.
D. The default route has the wrong next hop IP address
E. The threshold value is wrong

Answer: BE

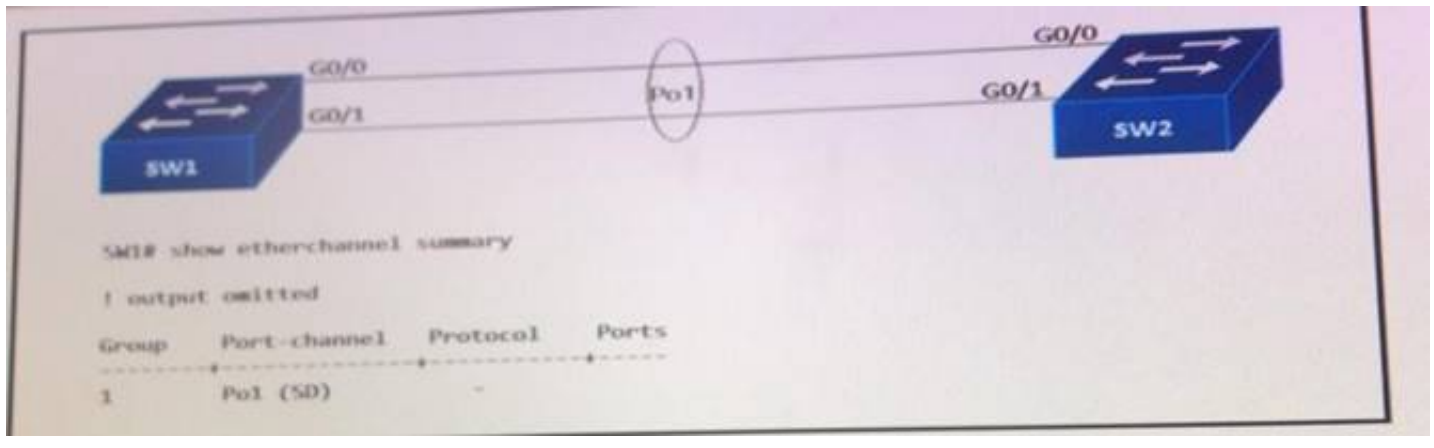
NEW QUESTION 106
- (Topic 2)
How are map-register messages sent in a LISP deployment?

A. egress tunnel routers to map resolvers to determine the appropriate egress tunnel router
B. ingress tunnel routers to map servers to determine the appropriate egress tunnel router
C. egress tunnel routers to map servers to determine the appropriate egress tunnel router
D. ingress tunnel routers to map resolvers to determine the appropnate egress tunnel router

Answer: C

Explanation:
During operation, an Egress Tunnel Router (ETR) sends periodic Map- Register messages to all its configured map servers.

NEW QUESTION 109
- (Topic 2)
Refer to the exhibit.



After an engineer configures an EtherChannel between switch SW1 and switch SW2, this error message is logged on switch SW2.

```
SW2#
09:45:32: %PM-4-ERR_DISABLE: channel-misconfig error detected on Gi0/0, putting Gi0/0 in err-disable state
09:45:32: %PM-4-ERR_DISABLE: channel-misconfig error detected on Gi0/1, putting Gi0/1 in err-disable state
```

Based on the output from SW1 and the log message received on Switch SW2, what action should the engineer take to resolve this issue?

A. Configure the same protocol on the EtherChannel on switch SW1 and SW2.
B. Connect the configuration error on interface Gi0/1 on switch SW1.
C. Define the correct port members on the EtherChannel on switch SW1.
D. Correct the configuration error on interface Gi0/0 switch SW1.

Answer: A

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

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

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

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

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

B)

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

C)

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

D)

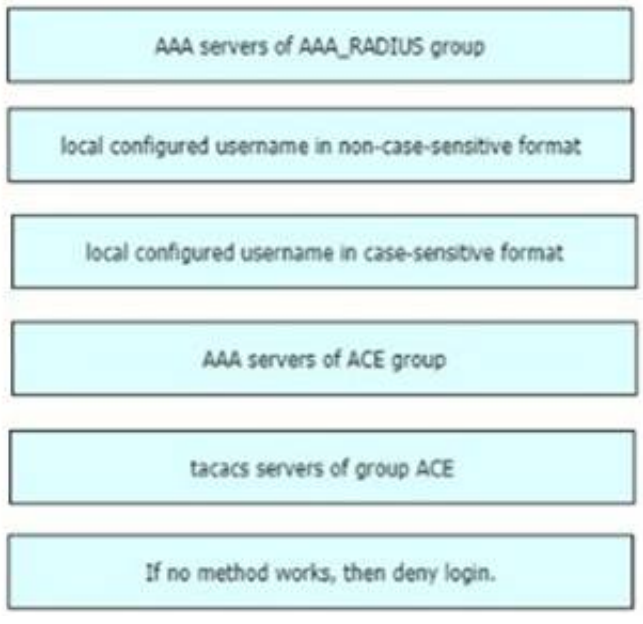
```
R1(config)#interface Gi0/1
R1(config-if)#ip ospf 1 area 0
R1(config-if)#no shutdown
```

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

Answer: C

NEW QUESTION 114
DRAG DROP - (Topic 2)
An engineer creates the configuration below. Drag and drop the authentication methods from the left into the order of priority on the right. Not all options are used.

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 118
- (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 121
- (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 125
- (Topic 2)
A network monitoring system uses SNMP polling to record the statistics of router interfaces The SNMP queries work as expected until an engineer installs a new interface and reloads the router After this action, all SNMP queries for the router fail What is the cause of this issue?

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

Answer: B

NEW QUESTION 128
- (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 133
- (Topic 2)
By default, which virtual MAC address does HSRP group 16 use?

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

Answer: B

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

NEW QUESTION 138
- (Topic 2)
Which technology uses network traffic telemetry, contextual information, and file reputation to provide insight into cyber threats?

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

Answer: C

NEW QUESTION 140
- (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 142
- (Topic 1)

What is the function of a fabric border node in a Cisco SD-Access environment?

A. To collect traffic flow information toward external networks
B. To connect the Cisco SD-Access fabric to another fabric or external Layer 3 networks
C. To attach and register clients to the fabric
D. To handle an ordered list of IP addresses and locations for endpoints in the fabric.

Answer: B

NEW QUESTION 145
- (Topic 1)
Which two operational models enable an AP to scan one or more wireless channels for rouge access points and at the same time provide wireless services to clients? (Choose two.)

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

Answer: DE

NEW QUESTION 149
- (Topic 1)
In cisco SD_WAN, which protocol is used to measure link quality?

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

Answer: B

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

NEW QUESTION 154
- (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 157
- (Topic 1)
Which JSON syntax is valid?
A)

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

B)

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

C)

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

D)

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

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

Answer: C

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

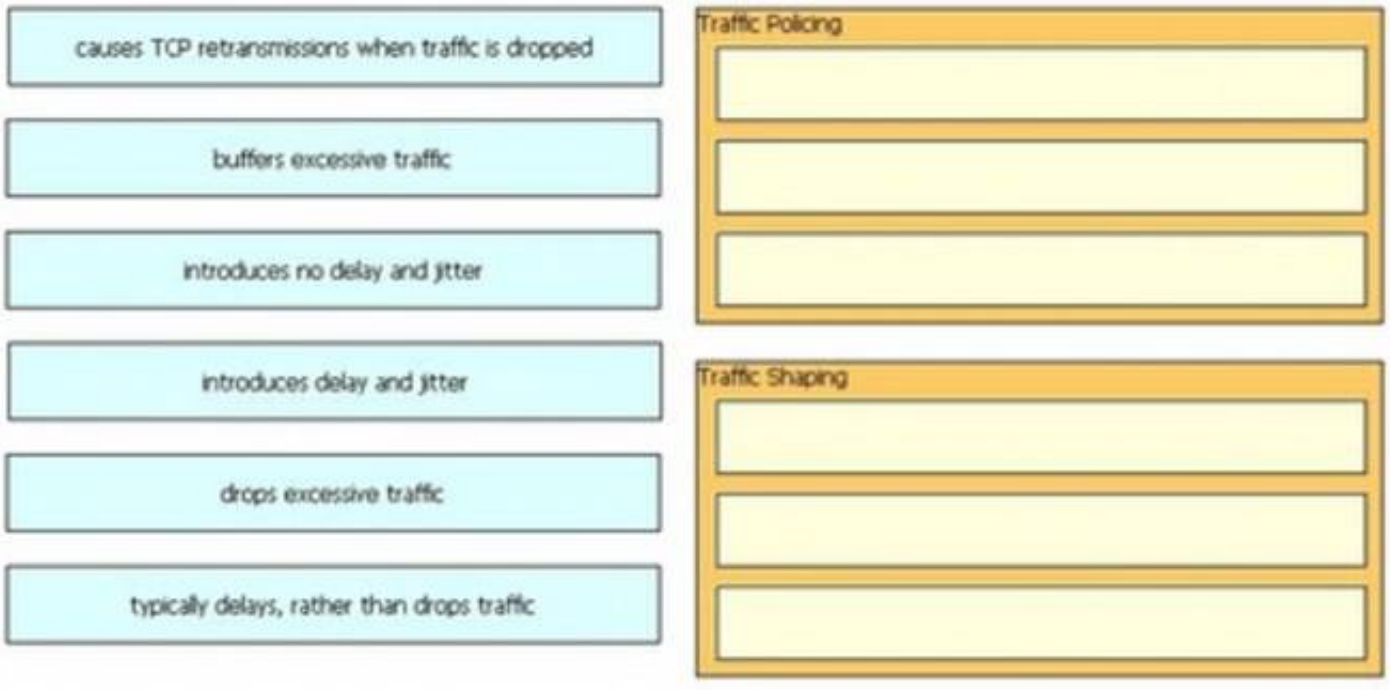
NEW QUESTION 161
- (Topic 1)
In a wireless Cisco SD-Access deployment, which roaming method is used when a user moves from one access point to another on a different access switch using a single WLC?

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

Answer: B

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

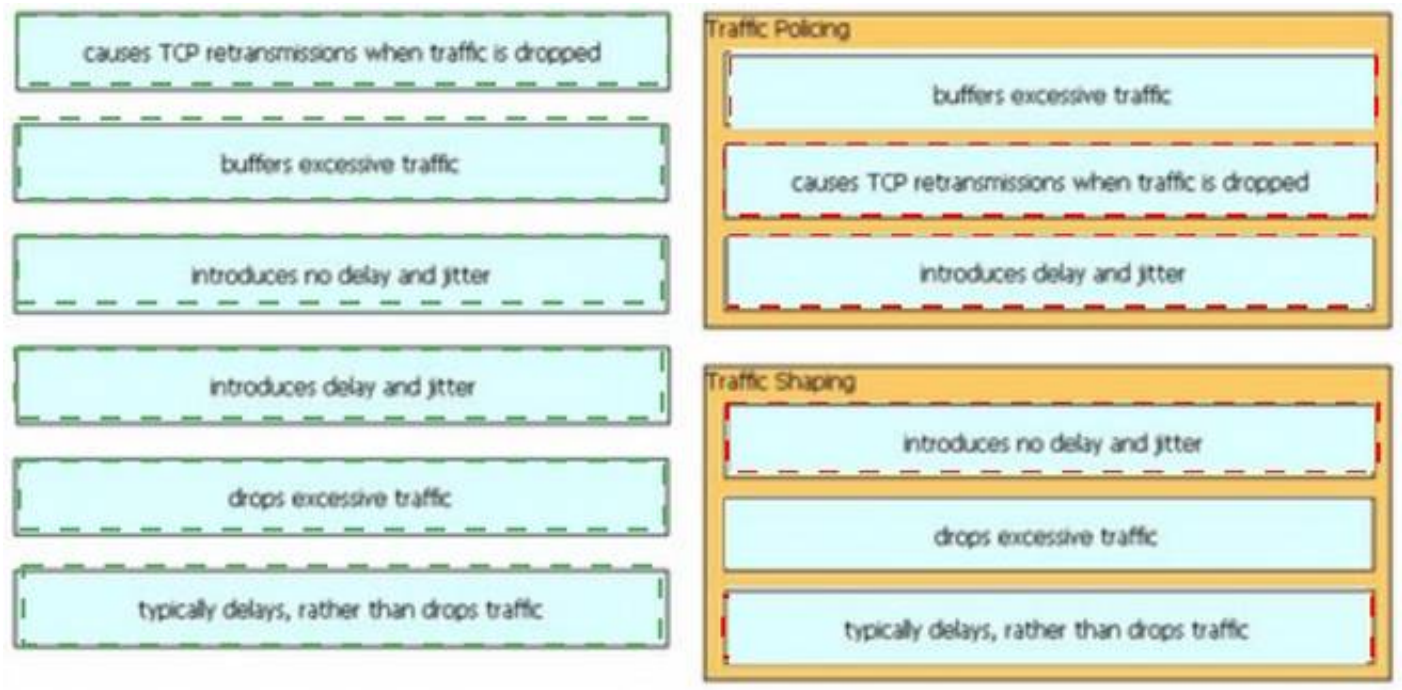
NEW QUESTION 163
DRAG DROP - (Topic 1)
Drag and drop the descriptions from the left onto the QoS components on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

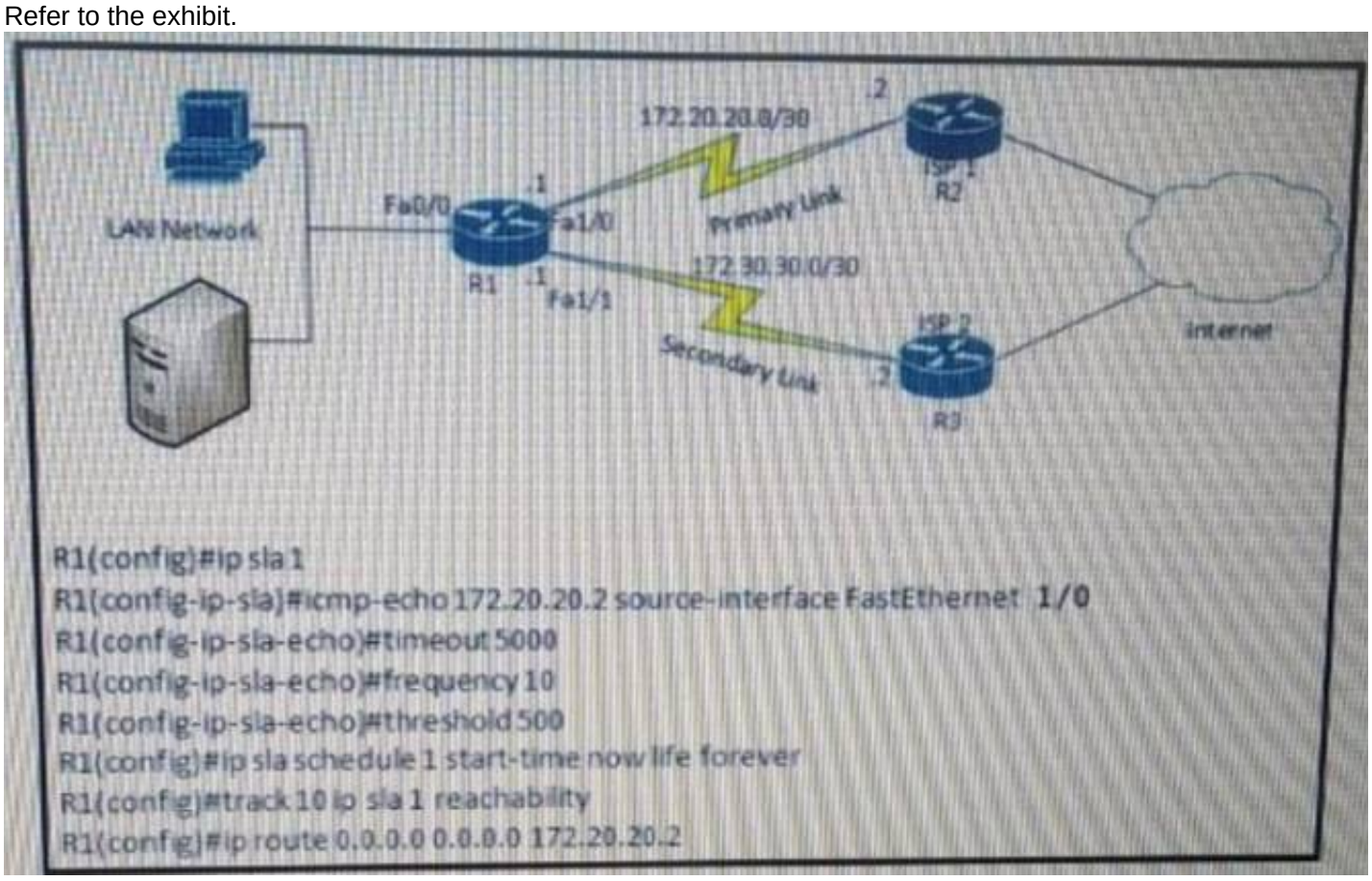


NEW QUESTION 166
- (Topic 1)
After a redundant route processor failure occurs on a Layer 3 device, which mechanism allows for packets to be forwarded from a neighboring router based on the most recent tables?

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

Answer: D

NEW QUESTION 167
- (Topic 1)
Refer to the exhibit.



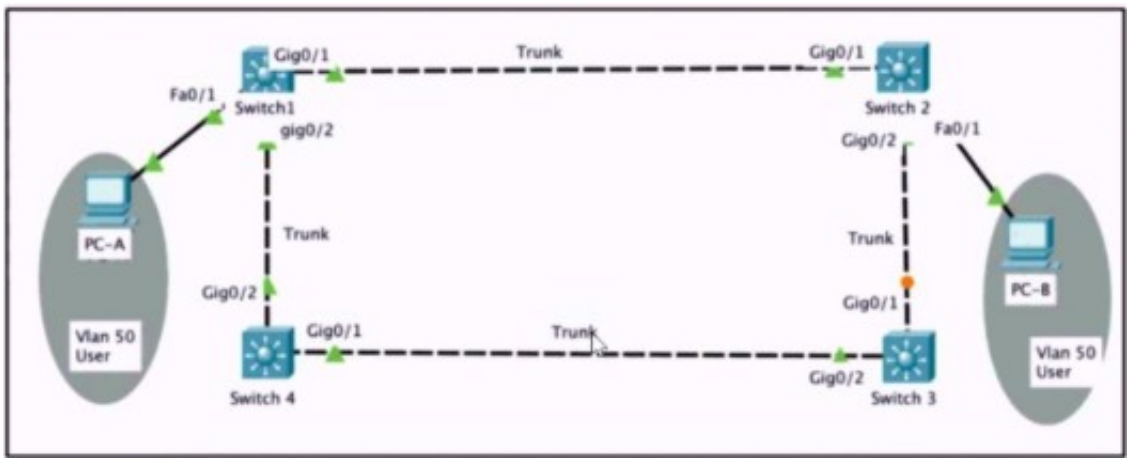
After implementing the configuration 172.20.20.2 stops replaying to ICMP echoes, but the default route fails to be removed. What is the reason for this behavior?

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

Answer: C

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

NEW QUESTION 168
- (Topic 1)



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

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

A)

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

B)

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

C)

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

D)

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

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

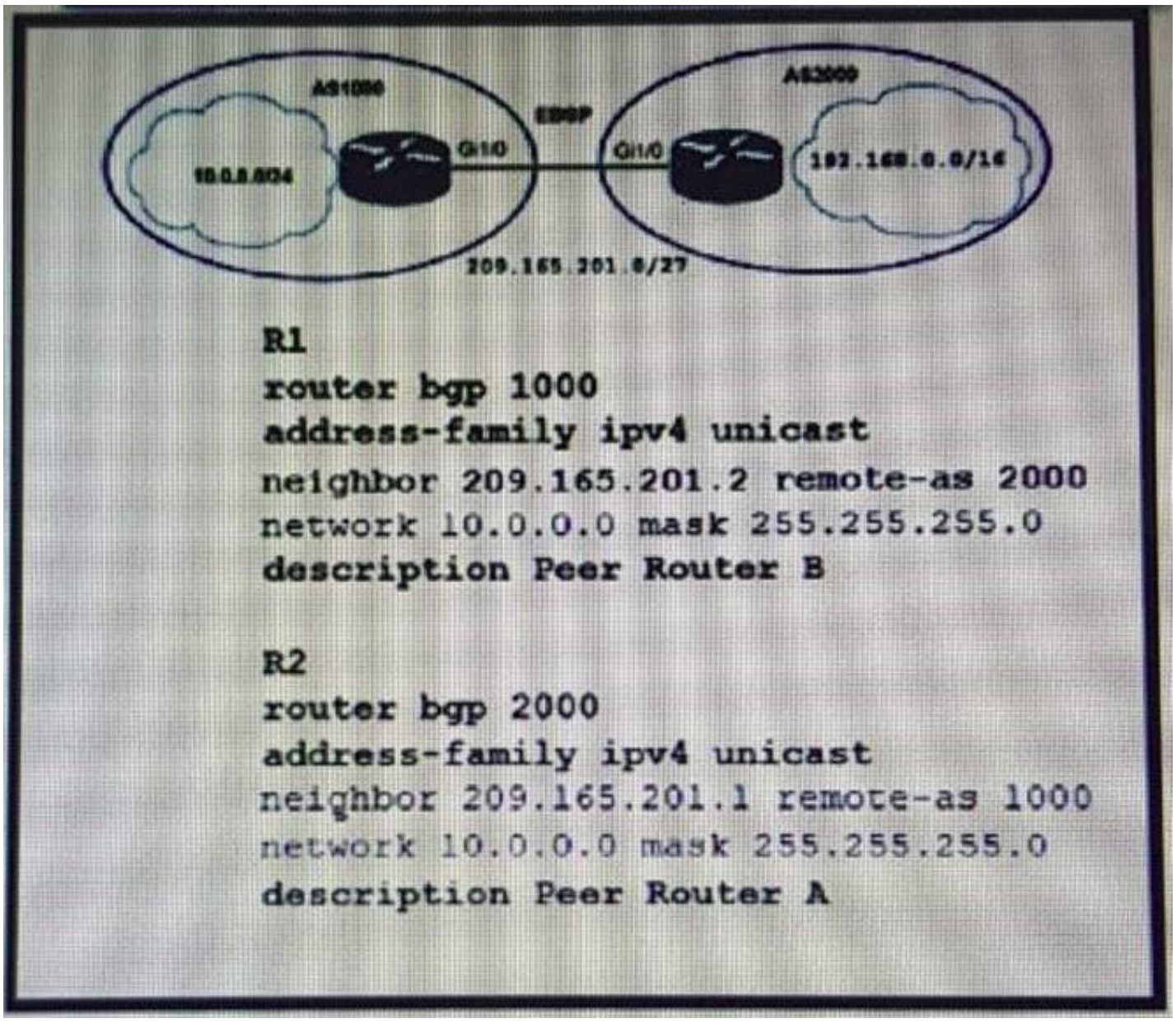
Answer: D

NEW QUESTION 170
- (Topic 1)
Which congestion queuing method on Cisco IOS based routers uses four static queues?

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

Answer: A

NEW QUESTION 175
- (Topic 1)



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

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

Answer: BC

NEW QUESTION 177
- (Topic 1)
When a wireless client roams between two different wireless controllers, a network connectivity outage is experience for a period of time. Which configuration issue would cause this problem?

A. Not all of the controllers in the mobility group are using the same mobility group name.
B. Not all of the controllers within the mobility group are using the same virtual interface IP address.
C. All of the controllers within the mobility group are using the same virtual interface IP address.
D. All of the controllers in the mobility group are using the same mobility group name.

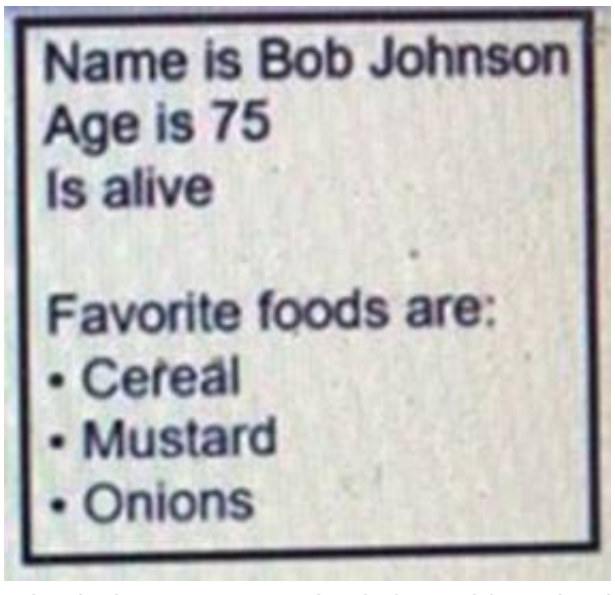
Answer: B

NEW QUESTION 181
- (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 182
- (Topic 1)
Refer to the exhibit.

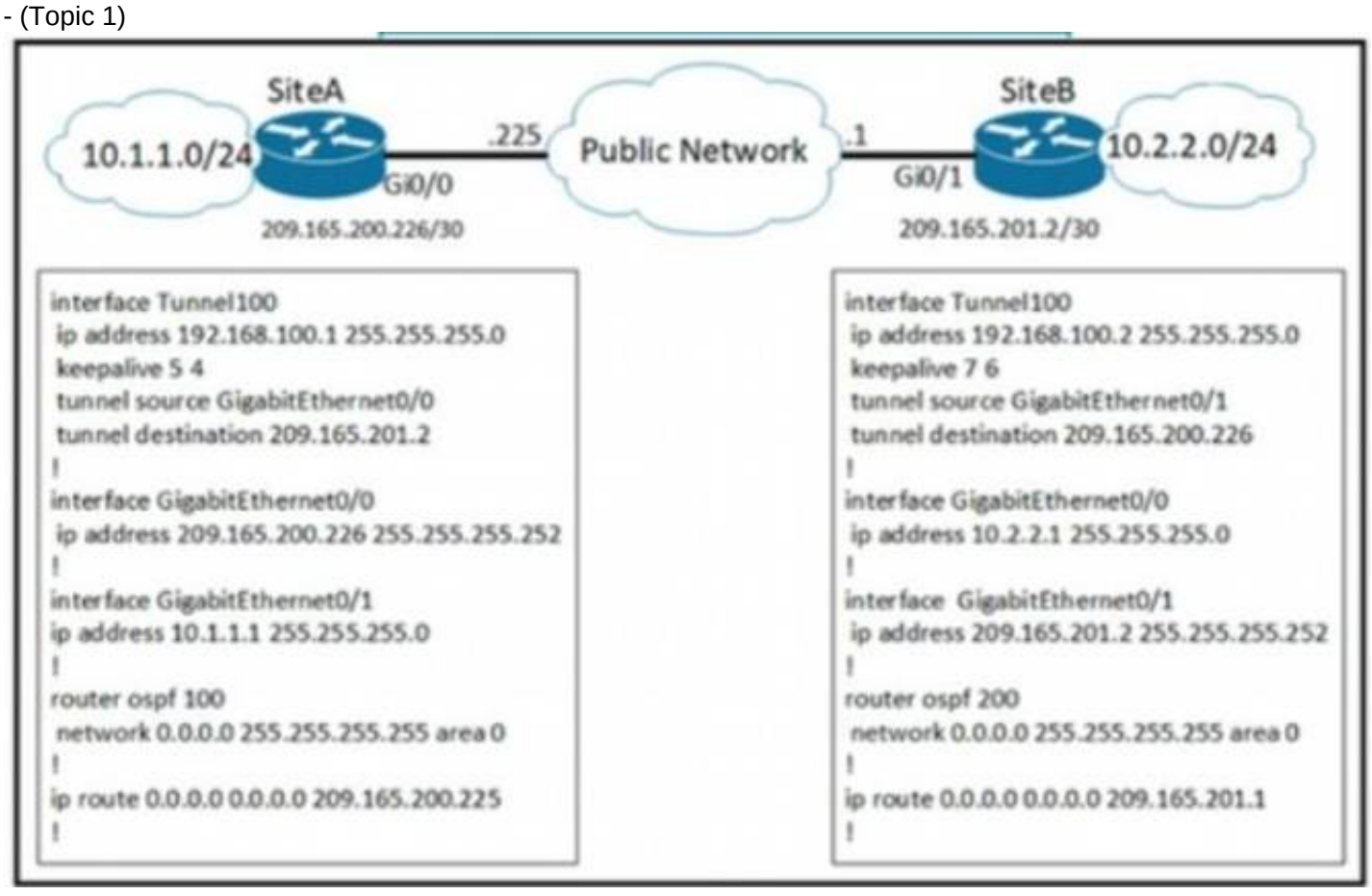


What is the Json syntax that is formed from the data?

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 184
- (Topic 1)

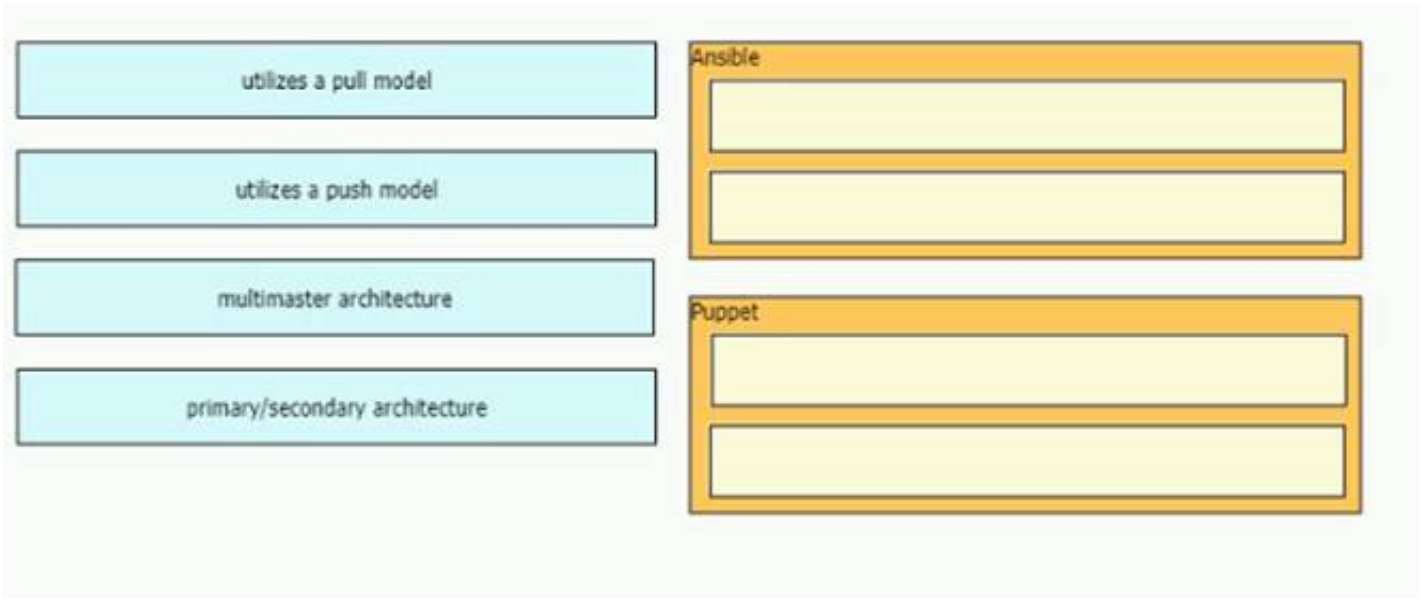


A network engineer configures a new GRE tunnel and enters the show run command. What does the output verify?

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

Answer: B

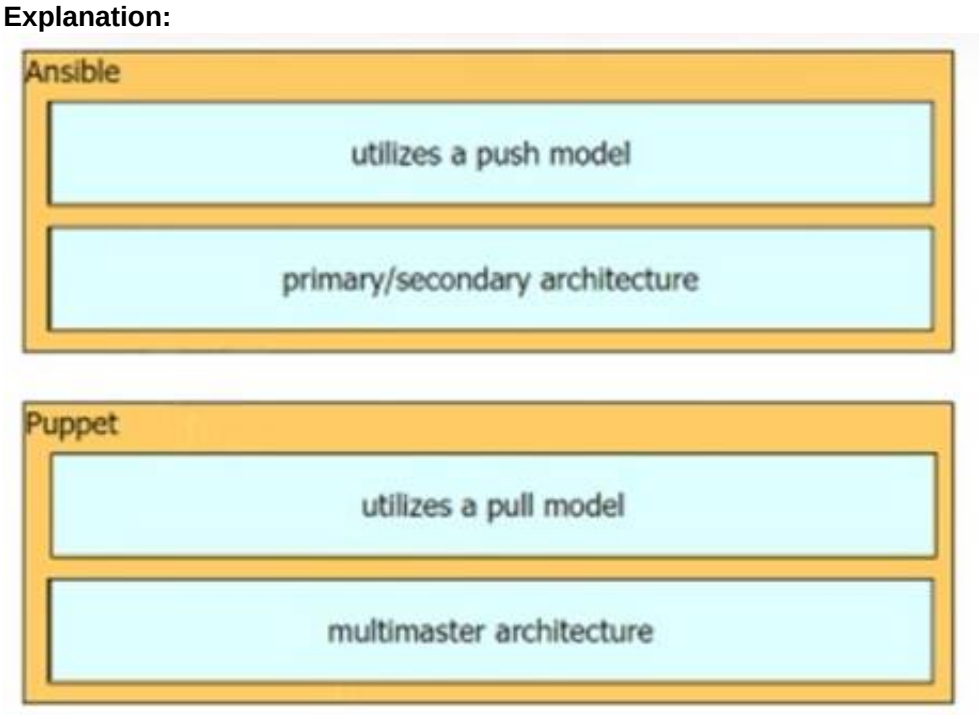
NEW QUESTION 186
DRAG DROP - (Topic 1)
Drag and drop the characteristics from the left onto the orchestration tools they describe on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 190
- (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 191
- (Topic 1)

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

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

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

Answer: B

NEW QUESTION 192
- (Topic 1)
Refer to the exhibit.

```
SW1#sh monitor session all
Session 1
------------

Type                        : Remote Destination Session
Source RSPAN VLAN           : 50

Session 2
------------

Type                        : Local Session
Source Ports                :
       Both                 : Fa0/14
  Destination Ports         : Fa0/15
       Encapsulation        : Native
             Ingress        : Disables
```

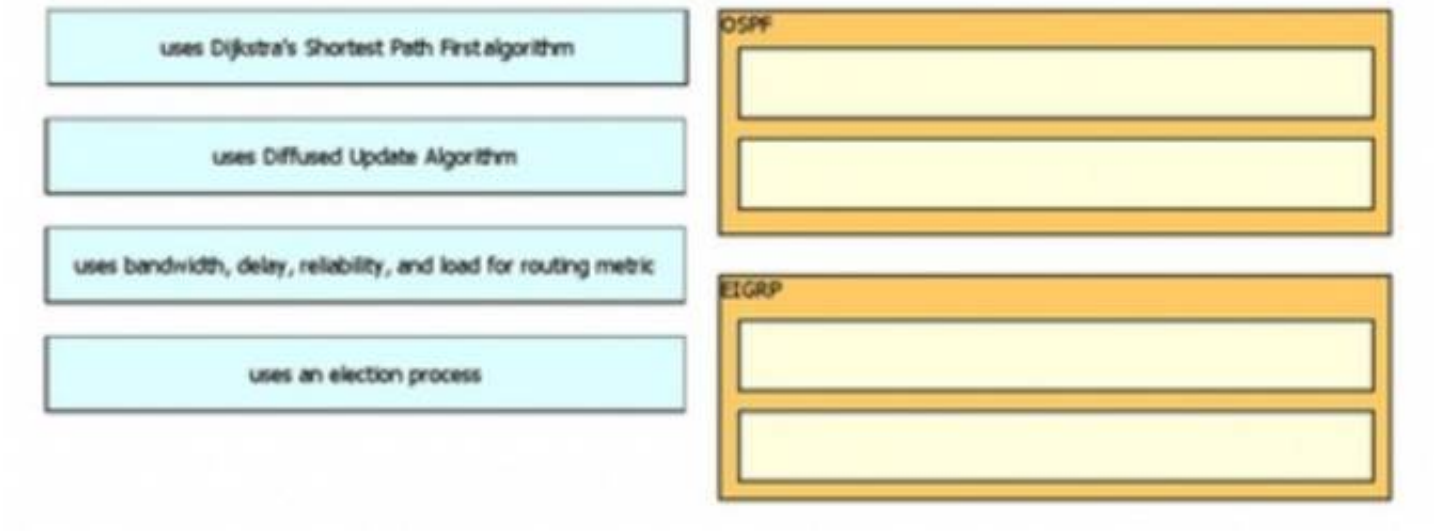
An engineer configures monitoring on SW1 and enters the show command to verify operation. What does the output confirm?

A. SPAN session 1 monitors activity on VLAN 50 of a remote switch
B. SPAN session 2 only monitors egress traffic exiting port FastEthernet 0/14.
C. SPAN session 2 monitors all traffic entering and exiting port FastEthernet 0/15.
D. RSPAN session 1 is incompletely configured for monitoring

Answer: D

Explanation:
SW1 has been configured with the following commands: SW1(config)#monitor session 1 source remote vlan 50 SW1(config)#monitor session 2 source interface fa0/14 SW1(config)#monitor session 2 destination interface fa0/15
The session 1 on SW1 was configured for Remote SPAN (RSPAN) while session 2 was configured for local SPAN. For RSPAN we need to configure the destination port to complete the configuration.
Note: In fact we cannot create such a session like session 1 because if we only configure Source RSPAN VLAN 50 (with the command monitor session 1 source remote vlan 50) then we will receive a Type: Remote Source Session (not Remote Destination Session).

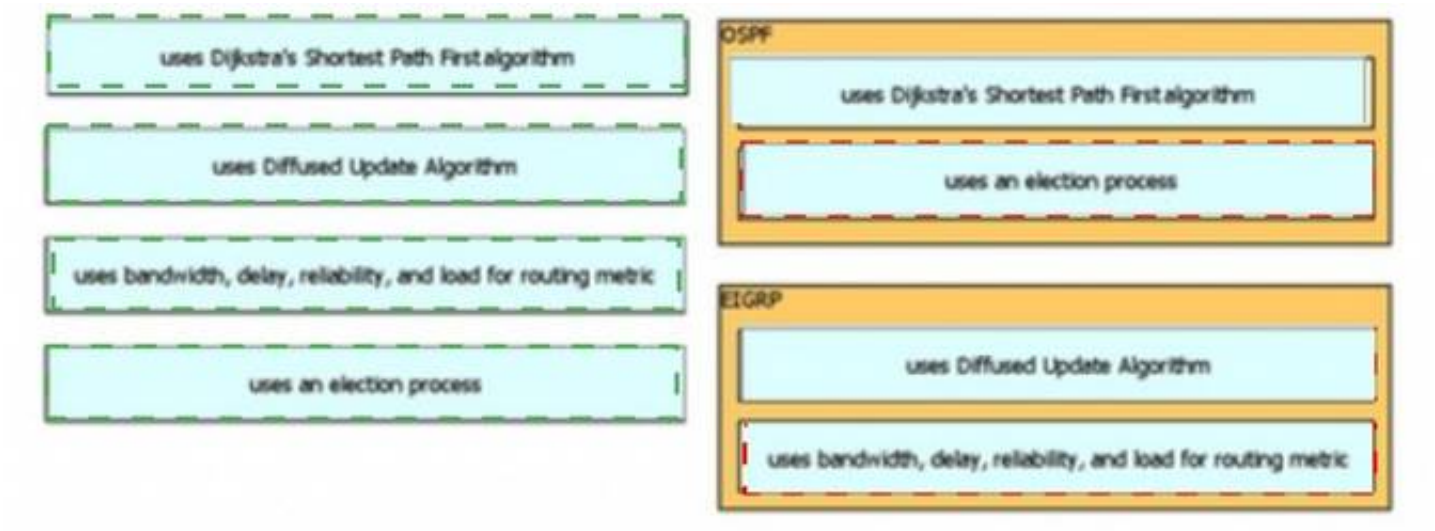
NEW QUESTION 193
DRAG DROP - (Topic 1)
Drag and drop the characteristics from the left onto the protocols they apply to on the right?



A. Mastered
B. Not Mastered

Answer: A

Explanation:

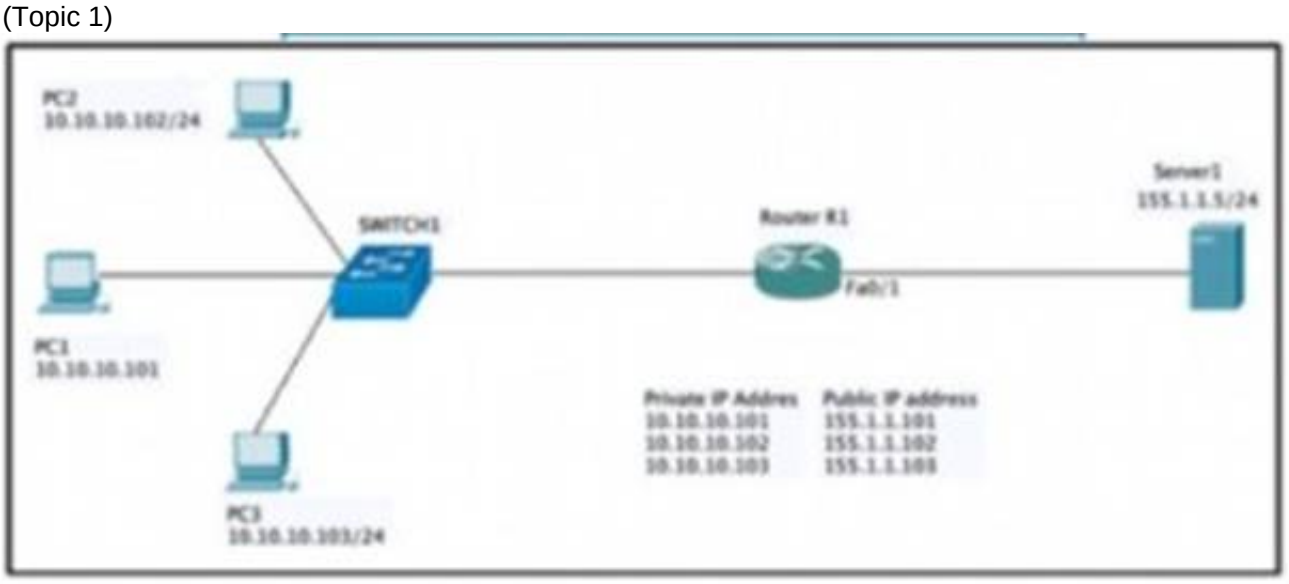


NEW QUESTION 194
- (Topic 1)
Which AP mode allows an engineer to scan configured channels for rogue access points?

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

Answer: B

NEW QUESTION 198
- (Topic 1)



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

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

B)

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

C)

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

D)

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

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

Answer: A

NEW QUESTION 199
- (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 202
- (Topic 1)
Refer to the exhibit.

```
ip sla 10

icmp-echo 192.168.10.20

timeout 500

frequency 3

ip sla schedule 10 life forever start-time now
track 10 ip sla 10 reachability
```

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

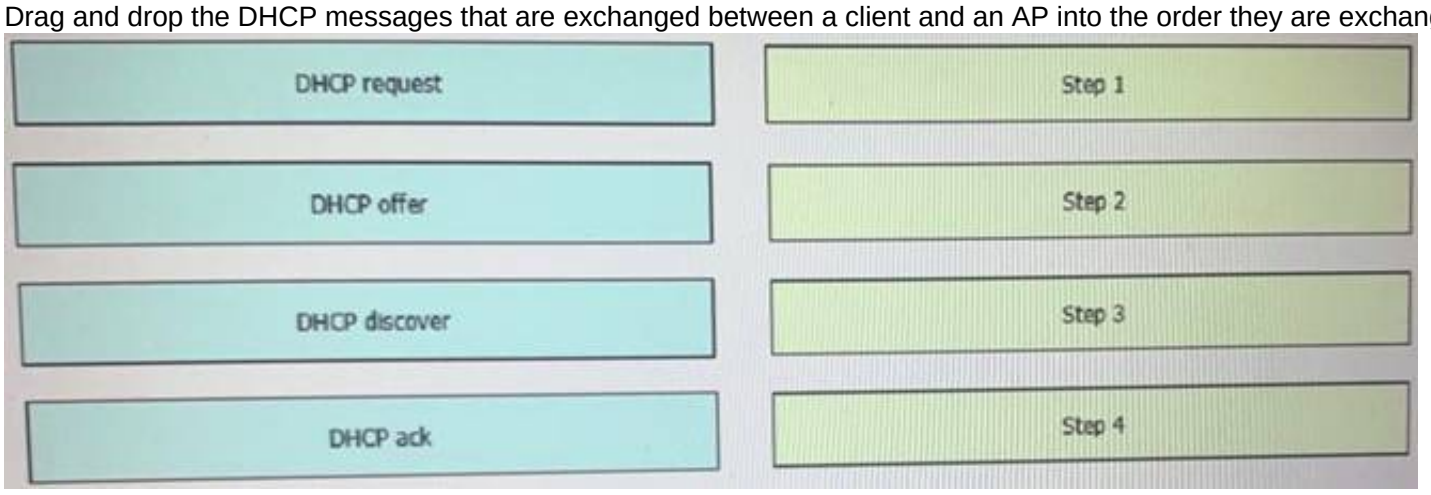
A. event manager applet EEM_IP_SLA event track 10 state down
B. event manager applet EEM_IP_SLA event track 10 state unreachable
C. event manager applet EEM_IP_SLA event sla 10 state unreachable
D. event manager applet EEM_IP_SLA event sla 10 state down

Answer: A

Explanation:
The ip sla 10 will ping the IP 192.168.10.20 every 3 seconds to make sure the connection is still up. We can configure an EEM applet if there is any problem with

this IP SLA via the command event track 10 state down.
Reference: https://www.theroutingtable.com/ip-sla-and-cisco-eem/

NEW QUESTION 206
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 209
- (Topic 1)
How is 802.11 traffic handled in a fabric-enabled SSID?

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

Answer: B

NEW QUESTION 214
- (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 219
- (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 221
- (Topic 1)
Which two threats does AMP4E have the ability to block? (Choose two.)

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

Answer: BC

Explanation:

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

NEW QUESTION 225
- (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 229
- (Topic 1)

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

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

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

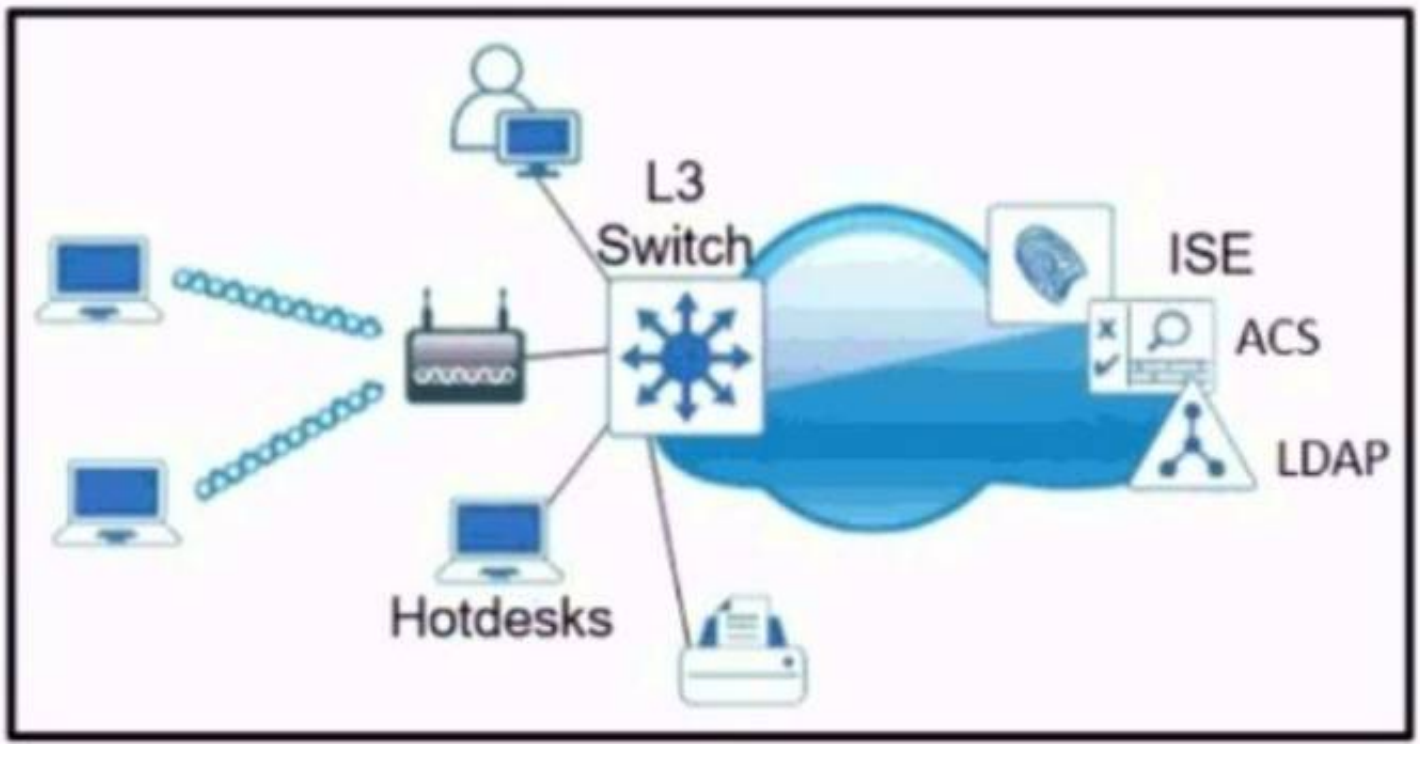
Answer: A

NEW QUESTION 232
- (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 234
- (Topic 1)

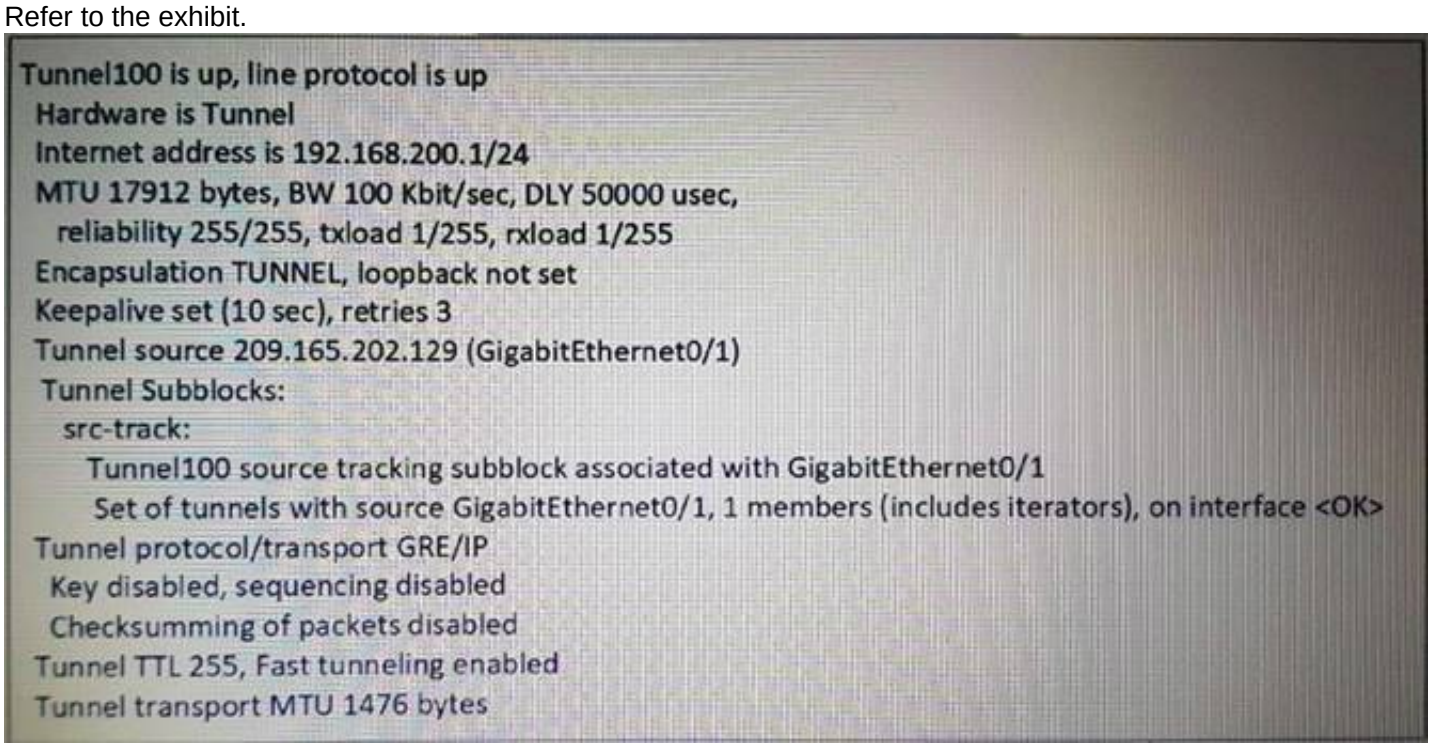


Refer to the exhibit Which single security feature is recommended to provide Network Access Control in the enterprise?

A. MAB
B. 802.1X
C. WebAuth
D. port security sticky MAC

Answer: B

NEW QUESTION 238
- (Topic 1)
Refer to the exhibit.



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 241
- (Topic 1)
Under which network conditions is an outbound QoS policy that is applied on a router WAN interface most beneficial?

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

Answer: A

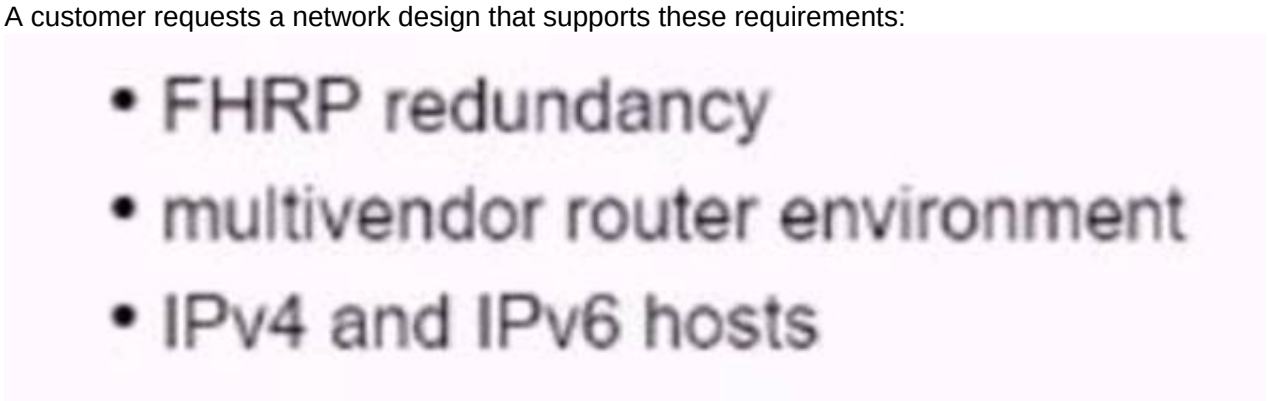
NEW QUESTION 244
- (Topic 1)
Which encryption hashing algorithm does NTP use for authentication?

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

Answer: B

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

NEW QUESTION 245
- (Topic 1)
A customer requests a network design that supports these requirements:



Which protocol does the design include?

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

Answer: D

NEW QUESTION 248
- (Topic 1)

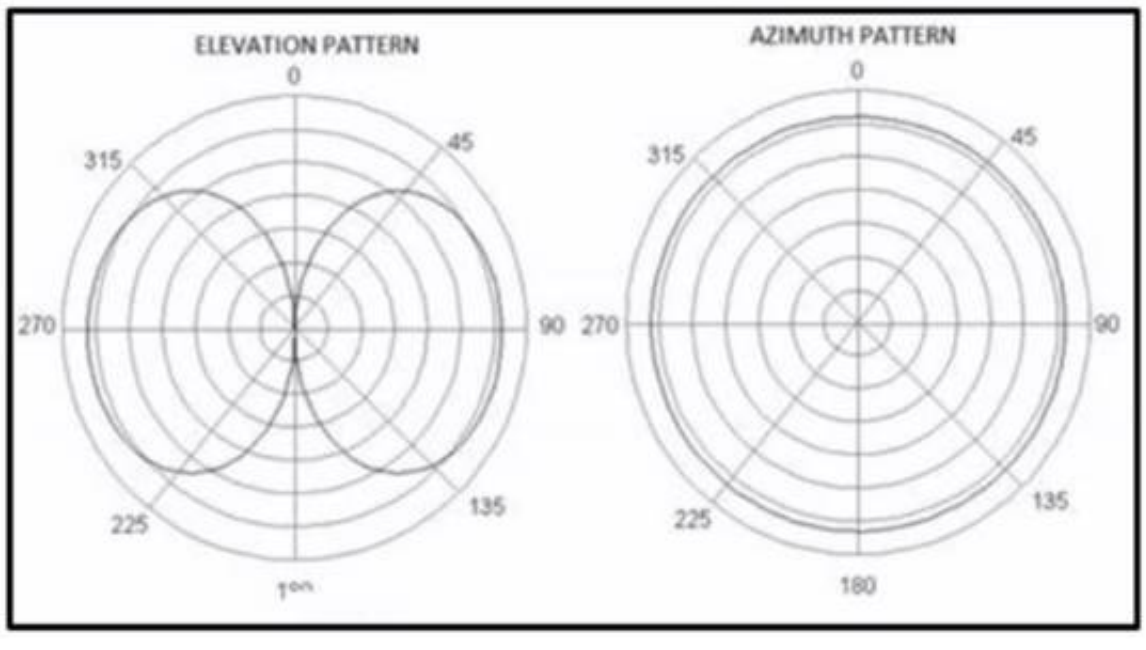

```
{
  "response": [
    {
      "family": "Routers",
      "interfaceCount": "12",
      "lineCardCount": "9",
      "platformId": "ASR1001-X",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Reachable",
      "hostname": "RouterASR-1",
      "macAddress": "00:c8:8b:80:bb:00",
    },
    {
      "family": "Switches and Hubs",
      "interfaceCount": "41",
      "lineCardCount": "2",
      "platformId": "C9300-24UX",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Authentication Failed",
      "hostname": "cat9000-1",
      "macAddress": "f8:7b:20:67:62:80",
    },
    {
      "family": "Switches and Hubs",
      "interfaceCount": "50",
      "lineCardCount": "2",
      "platformId": "WS-C3850-48U-E",
      "reachabilityFailureReason": "",
      "reachabilityStatus": "Unreachable",
      "hostname": "cat3850-1",
      "macAddress": "cc:d8:c1:15:d2:80",
    }
  ],
  "version": "1.0"
}
```


What does the cisco DNA REST response indicate?

A. Cisco DNA Center has the Incorrect credentials for cat3850-1
B. Cisco DNA Center is unable to communicate with cat9000-1
C. Cisco DNA Center has the incorrect credentials for cat9000-1
D. Cisco DNA Center has the Incorrect credentials for RouterASR-1

Answer: C

NEW QUESTION 251
- (Topic 4)
Refer to the exhibit.



Which antenna emits this radiation pattern?

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

Answer: A

NEW QUESTION 252
- (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 257
- (Topic 4)
Which configuration protects the password for the VTY lines against over-the-shoulder attacks?

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

Answer: B

NEW QUESTION 258
- (Topic 4)
An engineer is configuring RADIUS-Based Authentication with EAP MS-CHAPv2 is configured on a client device.
Which outer method protocol must be configured on the ISE to support this authentication type?

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

Answer: D

NEW QUESTION 263
- (Topic 4)
Why would a small or mid-size business choose a cloud solution over an on-premises solution?

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

Answer: C

NEW QUESTION 266
- (Topic 4)
In which way are EIGRP and OSPF similar?

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

Answer: C

NEW QUESTION 271
- (Topic 4)
What is stateful switchover?

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

Answer: D

NEW QUESTION 274
- (Topic 4)

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

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

Answer: B

NEW QUESTION 276
- (Topic 4)
What do Chef and Ansible have in common?

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

Answer: B

NEW QUESTION 277
- (Topic 4)
What is a characteristics of traffic shaping?

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

Answer: B

NEW QUESTION 280
- (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 285
- (Topic 4)
What is difference between TCAM and the MAC address table?

A. TCAM is used to make Lalyer 2 forwarding decisions CAM is used to build routing tables.
B. The MAC address table supports partial matches .TCAM requires an exact match.
C. The MAC address table is contained in CAM.ACL and QoS information is stored in TCAM.
D. Router prefix lookups happens in CAM.MAC address table lookups happen in TCAM.

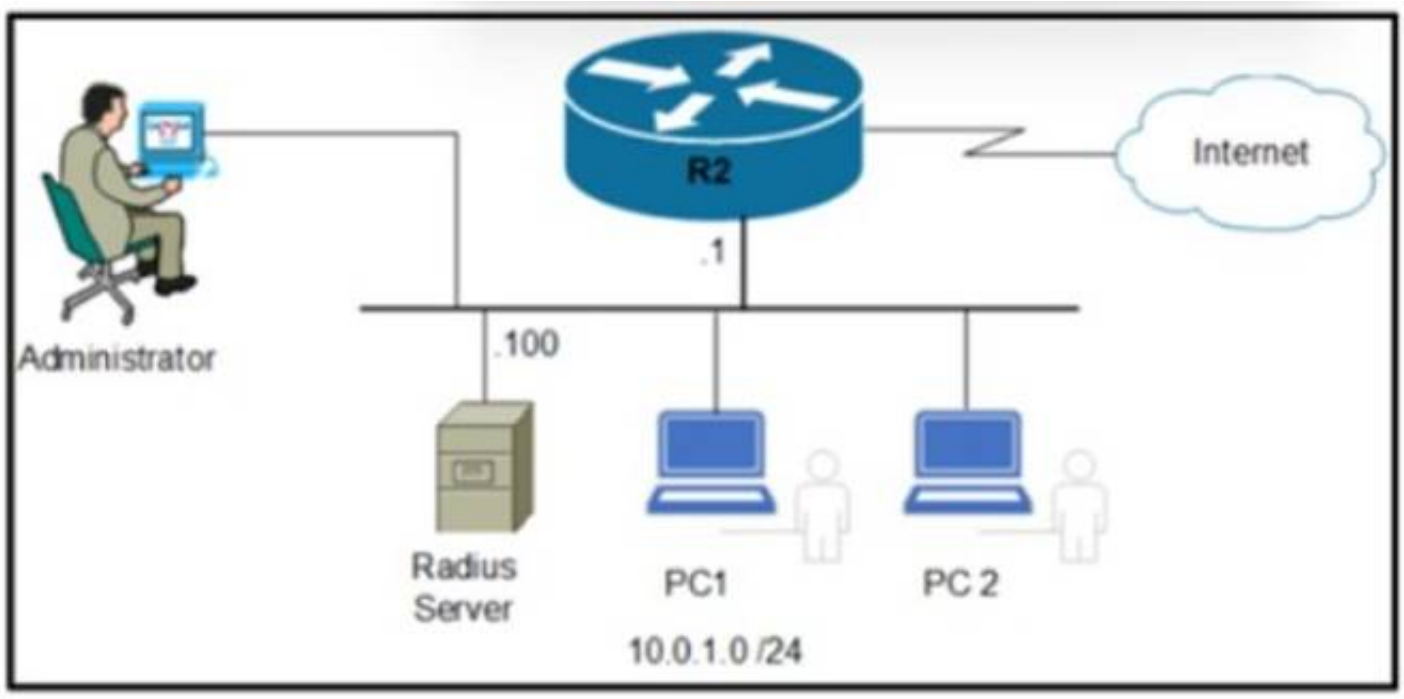
Answer: D

NEW QUESTION 286
- (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 291
- (Topic 4)



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

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

B)

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

C)

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

D)

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

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

Answer: A

NEW QUESTION 296
- (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 297
- (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.

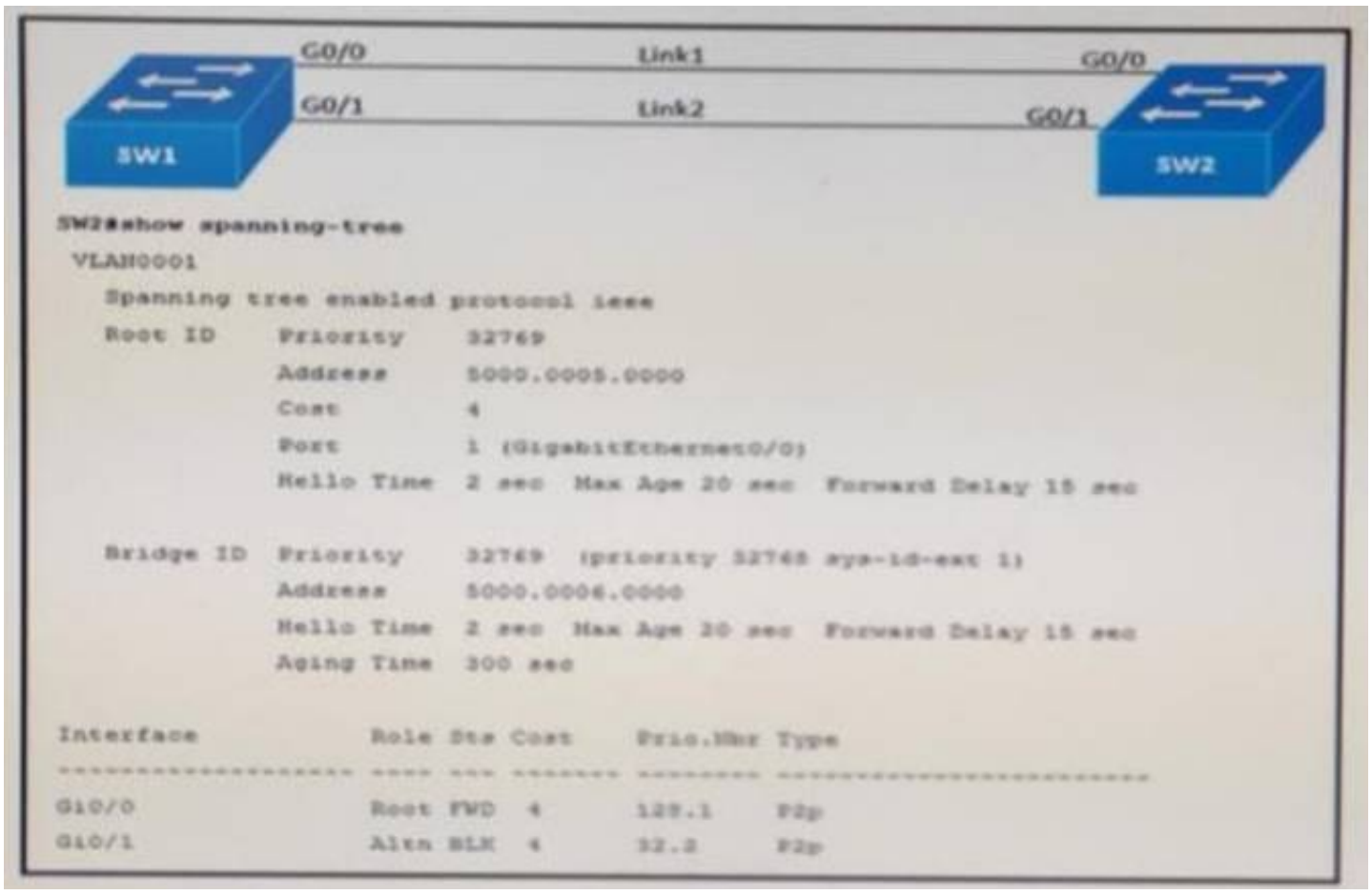
Answer: A

NEW QUESTION 300
- (Topic 4)
How is traffic classified when using Cisco TrustSec technology?

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

Answer: D

NEW QUESTION 305
- (Topic 4)

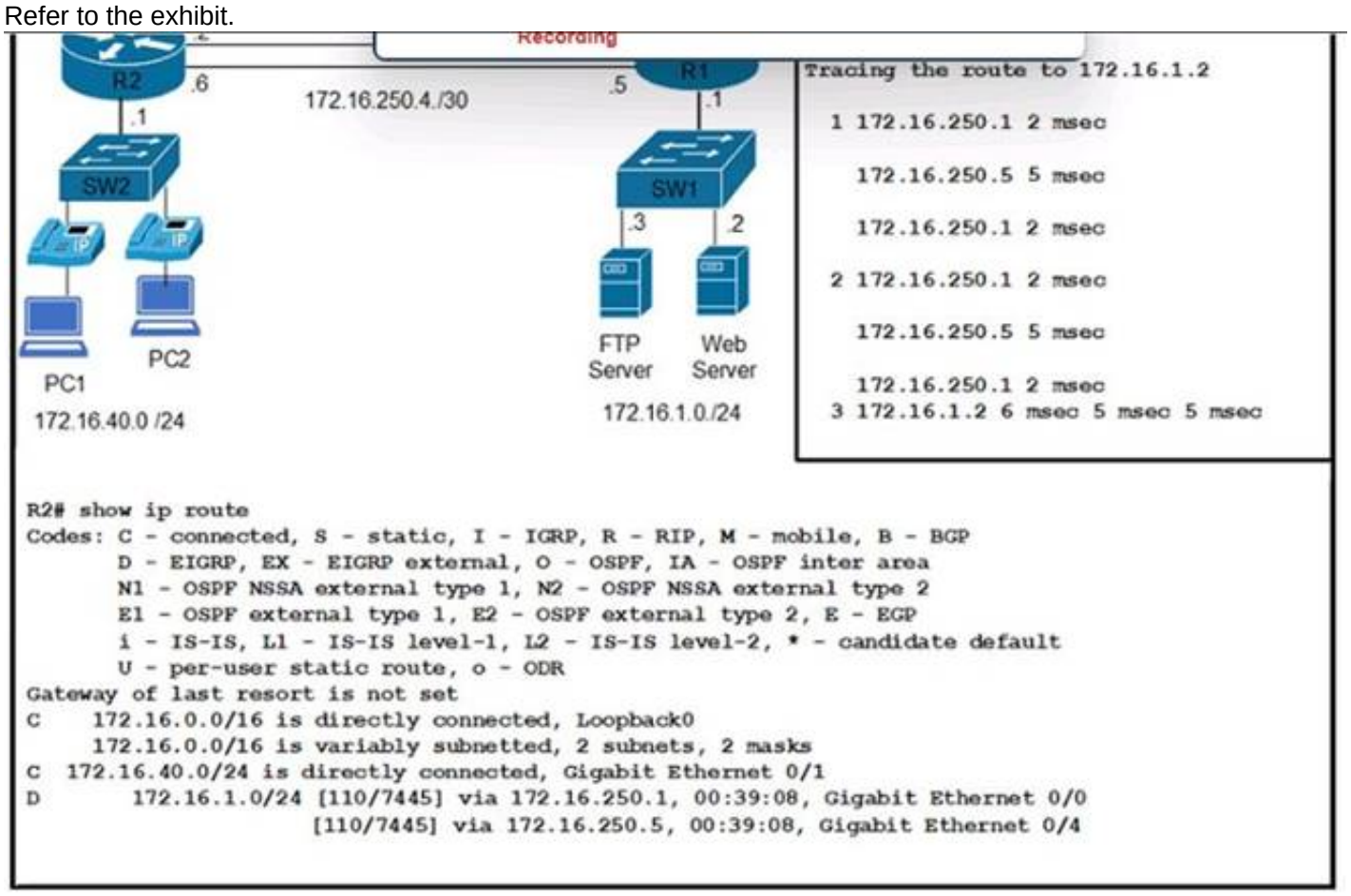


Refer to the exhibit. Link 1 uses a copper connection and link 2 uses a fiber connection. The fiber port must be the primary port for all forwarding. The output of the show spanning- tree command on SW2 shows that the fiber port is blocked by Spanning Tree. After entering the spanning-tree port-priority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

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

Answer: D

NEW QUESTION 308
- (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.

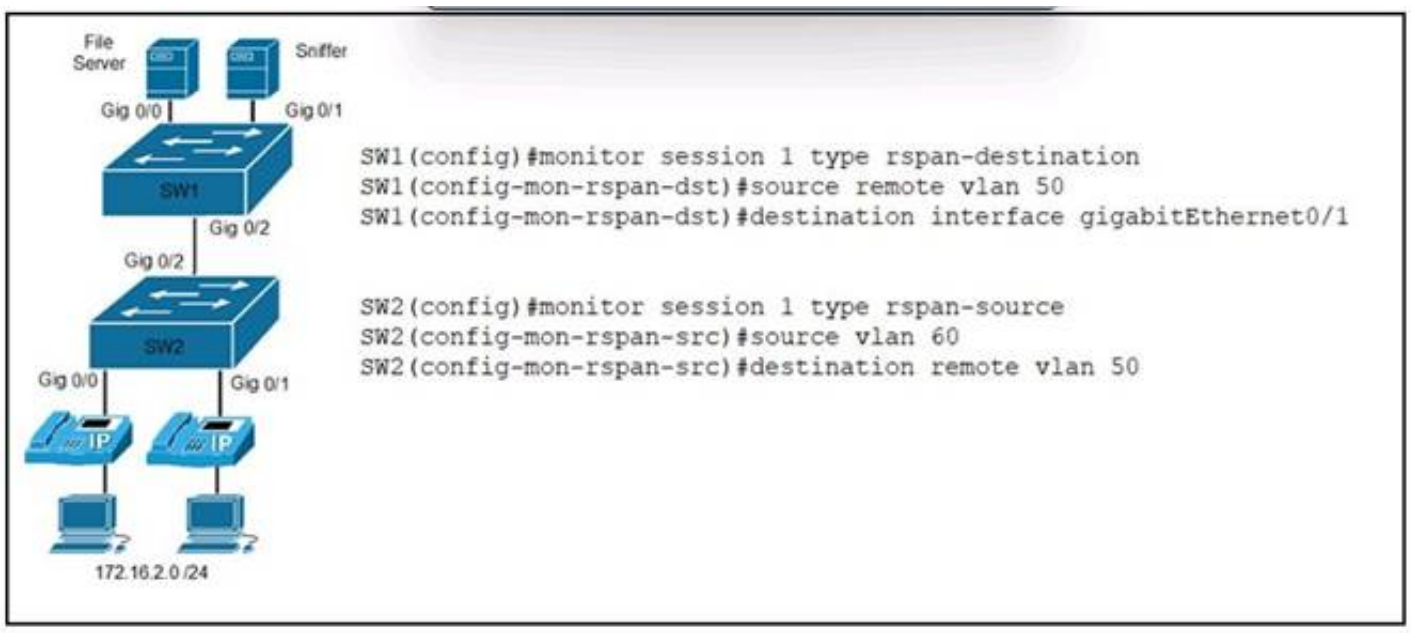
NEW QUESTION 309
- (Topic 4)
By default, which virtual MAC address does HSRP group 15 use?

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 313
- (Topic 4)
Refer to the exhibit.



An engineer must send the 172.16.2.0 /24 user traffic to a packet capture tool to troubleshoot an issue. Which action completes the configuration?

A. Encrypt the traffic between the users and the monitoring servers.
B. Disable the spanning tree protocol on the monitoring server VLAN.
C. Enable the Cisco Discovery Protocol on the server interfaces.
D. Define the remote span VLAN on SW1 and SW2.

Answer: D

Explanation:
This is because the remote span VLAN is used to transport the mirrored traffic from the source switch to the destination switch, where the monitoring server is connected. The remote span VLAN must be defined on both switches and must not be used for any other purpose. The source of this answer is the Cisco ENCOR v1.1 course, module 6, lesson 6.2: Implementing SPAN, RSPAN, and ERSPAN.

NEW QUESTION 315
- (Topic 4)
Which unit of measure is used to measure wireless RF SNR?

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

Answer: C

NEW QUESTION 316
- (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 319
- (Topic 4)
Which JSON script is properly formatted?
A)

```
[
    "Session":{

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

B)

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

C)

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

D)

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

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

Answer: A

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

NEW QUESTION 321
- (Topic 4)
What is an advantage of utilizing data models in a multivendor environment?

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

Answer: C

NEW QUESTION 326
- (Topic 4)
A customer has a wireless network deployed within a multi-tenant building. The network provides client access, location-based services, and is monitored using Cisco DNA Center. The security department wants to locate and track malicious devices based on threat signatures. Which feature is required for this solution?

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

Answer: B

NEW QUESTION 331
- (Topic 4)
Which QoS feature uses the IP Precedence bits in the ToS field of the IP packet header to partition traffic into different priority levels?

A. marking
B. shaping
C. policing
D. classification

Answer: D

NEW QUESTION 333
- (Topic 4)
A customer has a pair of Cisco 5520 WLCs set up in an SSO cluster to manage all APs. Guest traffic is anchored to a Cisco 3504 WLC located in a DMZ. Which action is needed to ensure that the EoIP tunnel remains in an UP state in the event of failover on the SSO cluster?

A. Configure back-to-back connectivity on the RP ports.

B. Enable default gateway reachability check.
C. Use the same mobility domain on all WLCs.
D. Use the mobility MAC when the mobility peer is configured.

Answer: B

NEW QUESTION 334
- (Topic 4)
A technician needs to find the MAC address of a connecting router. Which of the following commands should the technician use?

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

Answer: A

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

NEW QUESTION 339
- (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 343
- (Topic 4)
Which two methods are used to assign security group tags to the user in a Cisco Trust Sec architecture? (Choose two)

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

Answer: CE

NEW QUESTION 348
- (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 352
- (Topic 4)
How do stratum levels relate to the distance from a time source?

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

Answer: C

NEW QUESTION 354
- (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 355
- (Topic 4)
Which device is responsible for finding EID-to-RLOC mappings when traffic is sent to a LISP-capable site?

A. map server
B. map resolver
C. ingress tunnel router
D. egress tunnel router

Answer: C

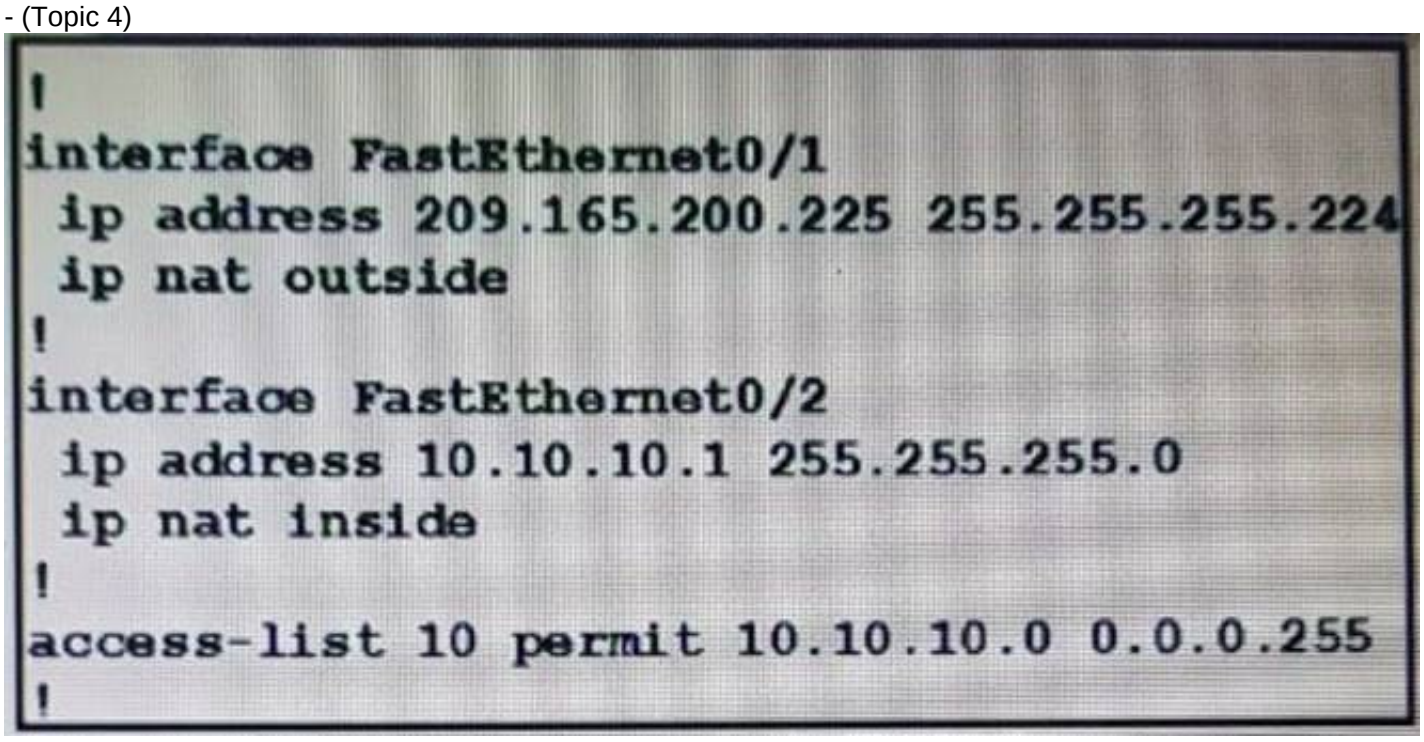
NEW QUESTION 357
- (Topic 4)
Which of the following should a junior security administrator recommend implementing to mitigate malicious network activity?

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 362
- (Topic 4)

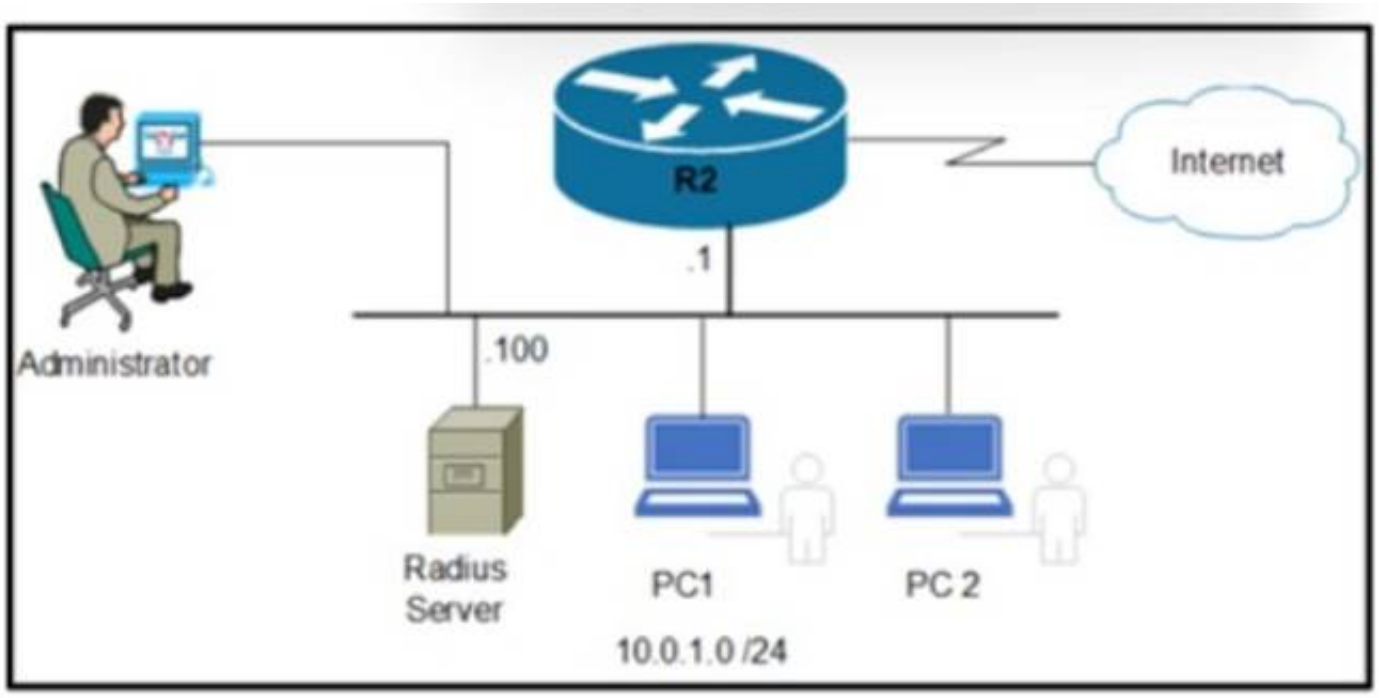


Refer to the exhibit. Which command allows hosts that are connected to FastEthernet0/2 to access the Internet?

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

Answer: A

NEW QUESTION 363
- (Topic 4)



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

```
<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
  <cisco-ia:reset xmlns:cisco-ia="http://cisco.com/yang/cisco-ia">
  <cisco-ia:reinitialize>true</cisco-ia:reinitialize>
  </cisco-ia:reset>
</rpc>
```

```
<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
 <get>
  <filter type="subtree">
   <ncm:netconf-state xmlns:ncm="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">
    <ncm:capabilities/>
   </ncm:netconf-state>
  </filter>
 </get>
</rpc>
```

```
<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
  <cisco-ia:save-config xmlns:cisco-ia="http://cisco.com/yang/cisco-ia"/>
</rpc>
```

```
<?xml version="1.0" encoding="utf-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">
  <cisco-ia:sync-from xmlns:cisco-ia="http://cisco.com/yang/cisco-ia"></cisco-ia:sync-from>
</rpc>
```

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

Answer: C

NEW QUESTION 367
- (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 370
- (Topic 4)
What does the Cisco DNA Center Authentication API provide?

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

Answer: B

NEW QUESTION 375
- (Topic 4)
Which technology enables a redundant supervisor engine to take over when the primary supervisor engine fails?

A. NSF
B. graceful restart
C. SSO
D. FHRP

Answer: C

NEW QUESTION 377
- (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#
```

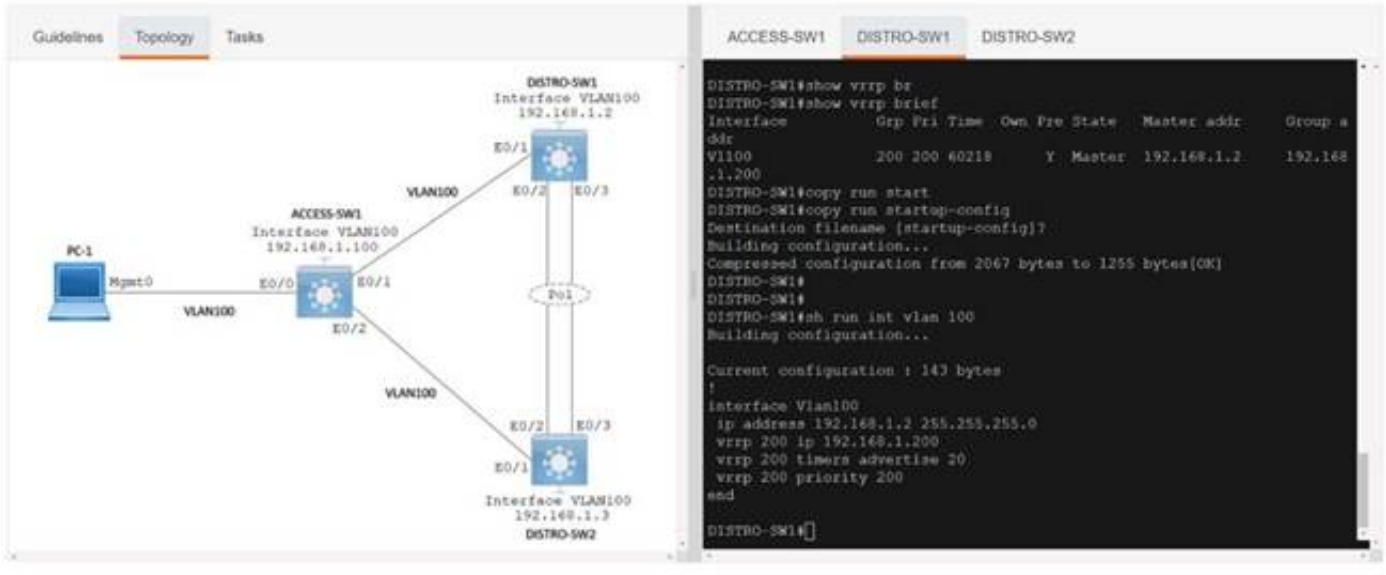
Which result Is achieved by the CoPP configuration?

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 380
SIMULATION - (Topic 4)
Simulation 10

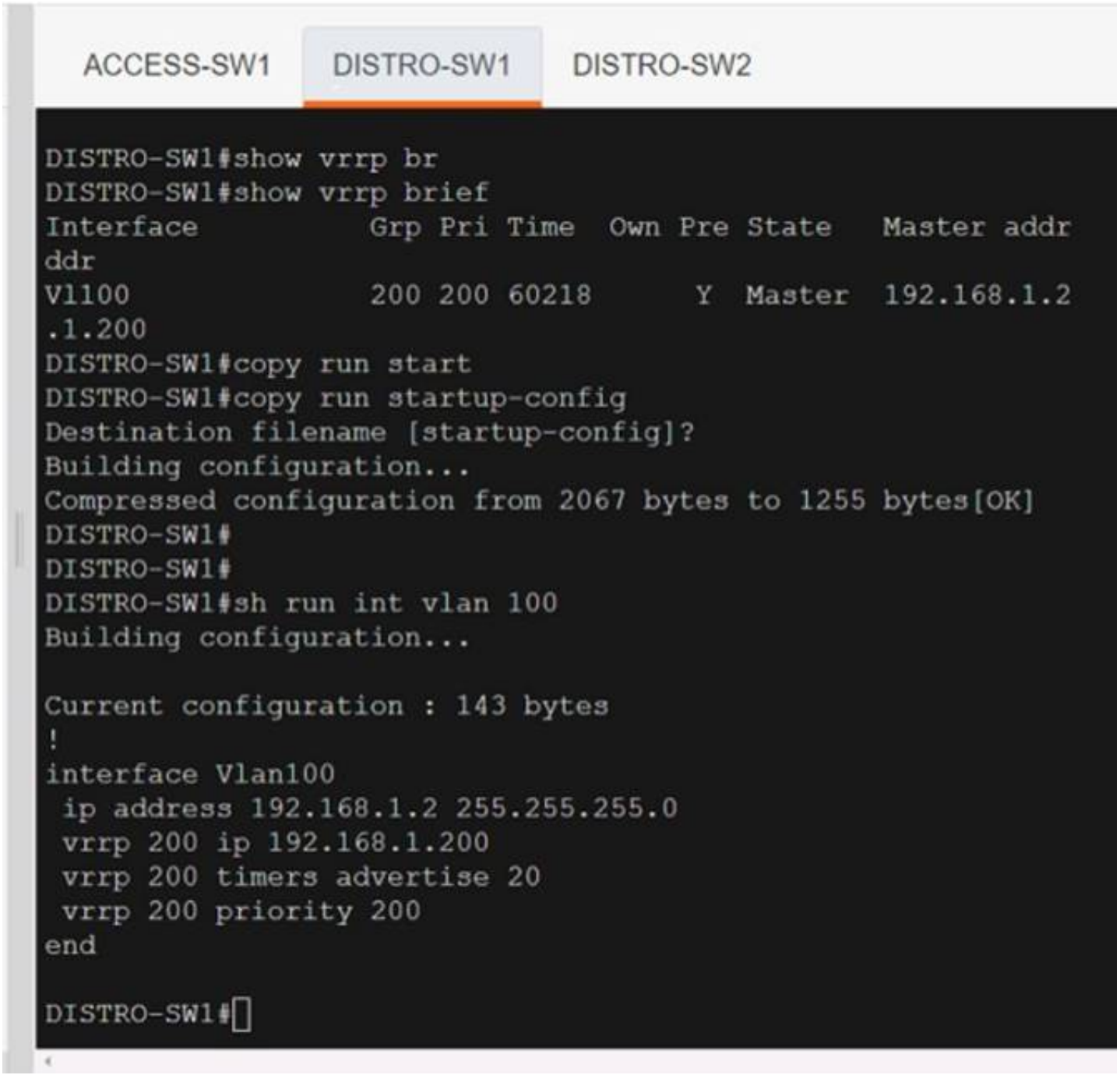


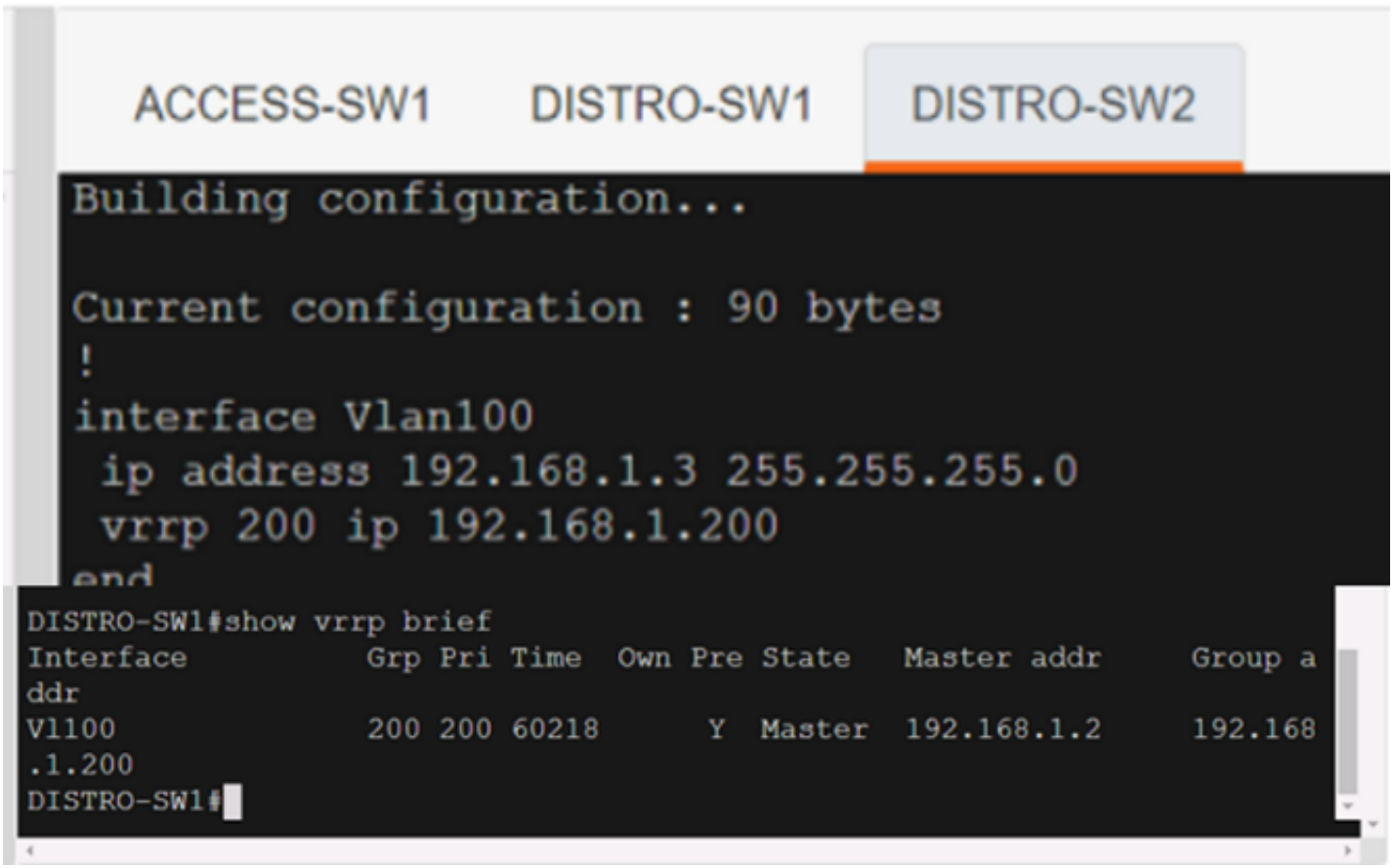
A. Mastered

B. Not Mastered

Answer: A

Explanation:





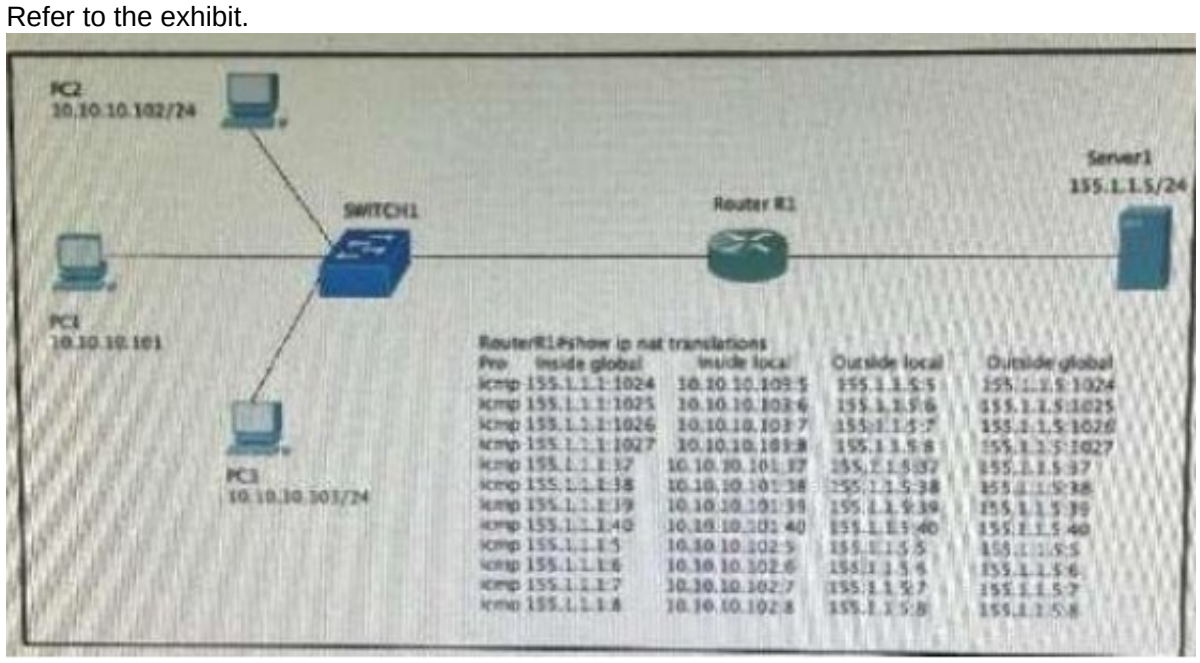
NEW QUESTION 384
- (Topic 4)
Users have reported an issue connecting to a server over the network. A workstation was recently added to the network and configured with a shared USB printer. Which of the following is most likely causing the issue?

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 389
- (Topic 4)
Refer to the exhibit.



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

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

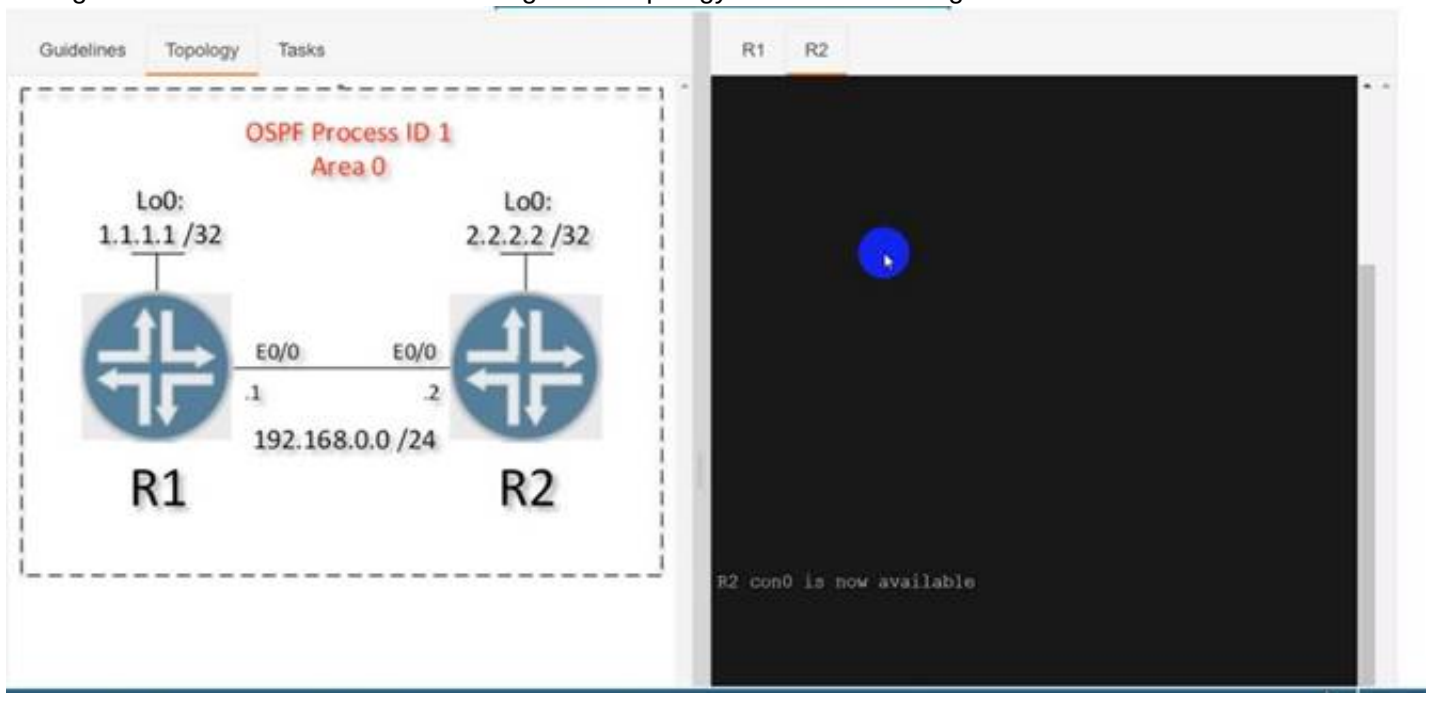
Answer: A

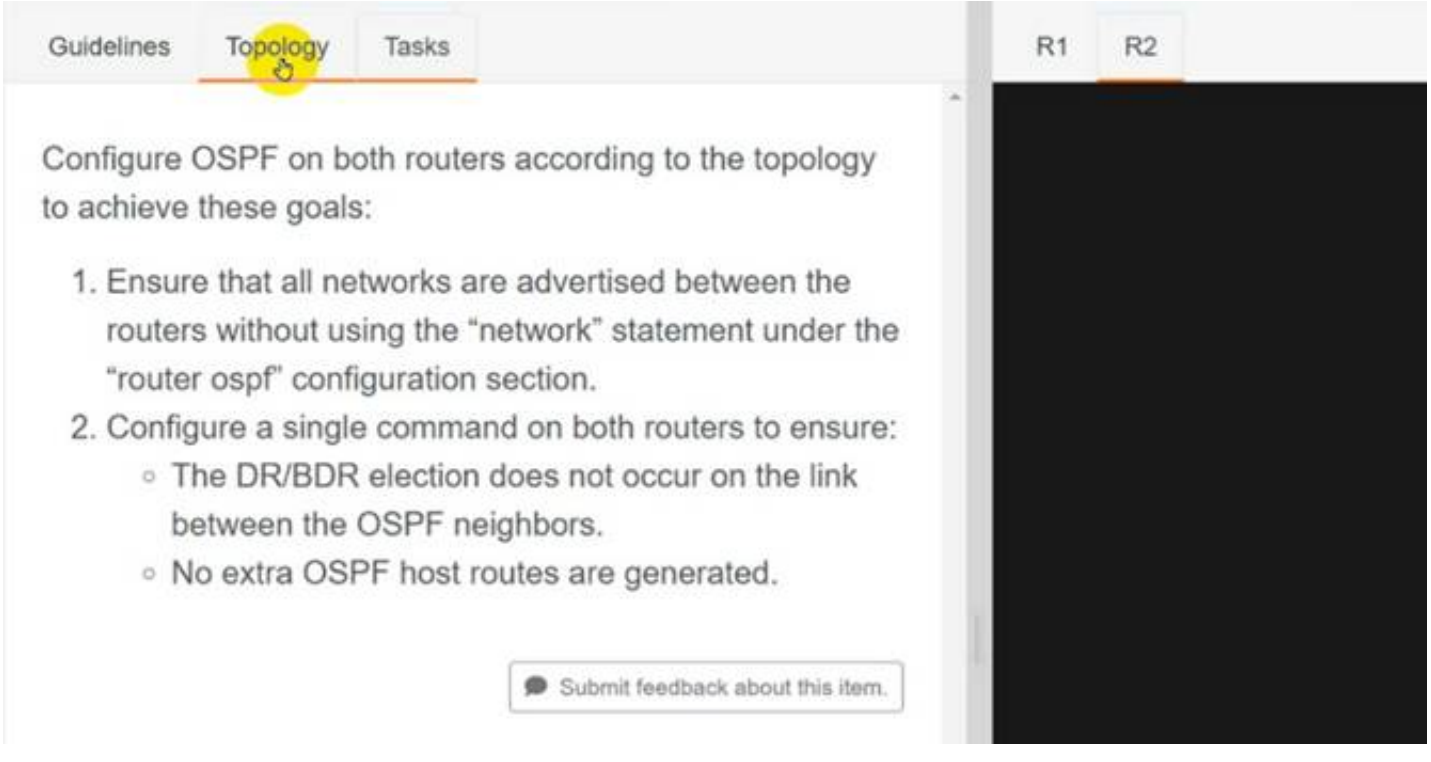
NEW QUESTION 393
- (Topic 4)
Which two new security capabilities are introduced by using a next-generation firewall at the Internet edge? (Choose two.)

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

Answer: DE

NEW QUESTION 394
SIMULATION - (Topic 4)
Simulation 04
Configure OSPF on both routers according to the topology to achieve these goals:





A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

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

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

```
R1#sh ip ospf neighbor

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

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


                Base Topology (MTID 0)


    Area BACKBONE(0)

    Intra-area Route List

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

    First Hop Forwarding Gateway Tree

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

NEW QUESTION 397
- (Topic 4)
Which function is performed by vSmart in the Cisco SD-WAN architecture?

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

Answer: B

NEW QUESTION 399
- (Topic 4)
Which of the following attacks becomes more effective because of global leakages of users' passwords?

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

Answer: A

Explanation:

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

NEW QUESTION 404
- (Topic 4)
An engineer must configure a multicast UDP jitter operation. Which configuration should be applied?
A)

```
Router(config)#ip sla 1
Router(config)#udp-jitter 192.0.2.115  65051 num-packets 20
```

B)

```
Router(config)#ip sla 1
Router(config)#udp jitter 10.0.0.1  source-ip 192.168.1.1
```

C)

```
Router(config)#ip sla 1
Router(config)#udp-jitter 192.0.2.115  65051
```

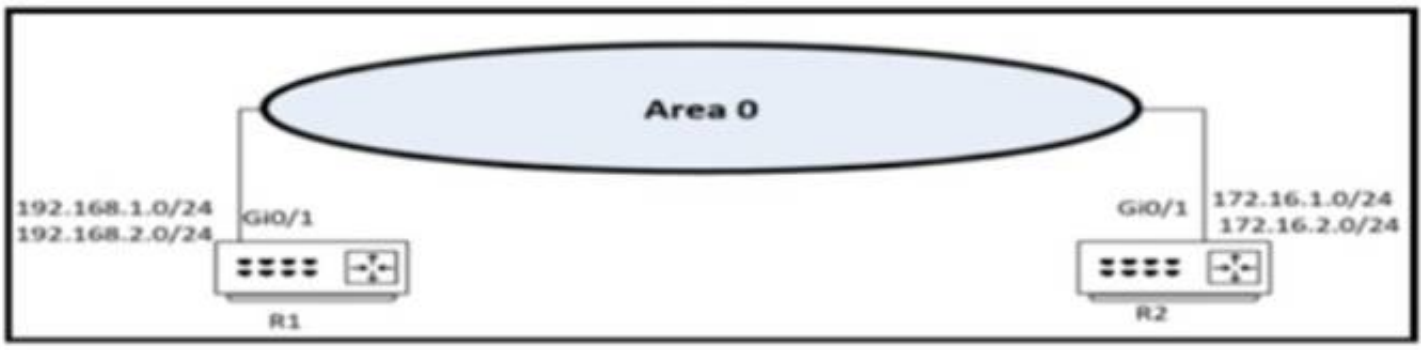
D)

```
Router(config)#ip sla 1
Router(config)#udp jitter 239.1.1.1 65051 end-point list List source-ip 192.168.1.1
```

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

Answer: D

NEW QUESTION 409
- (Topic 4)



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

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

B)

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

C)

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

D)

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

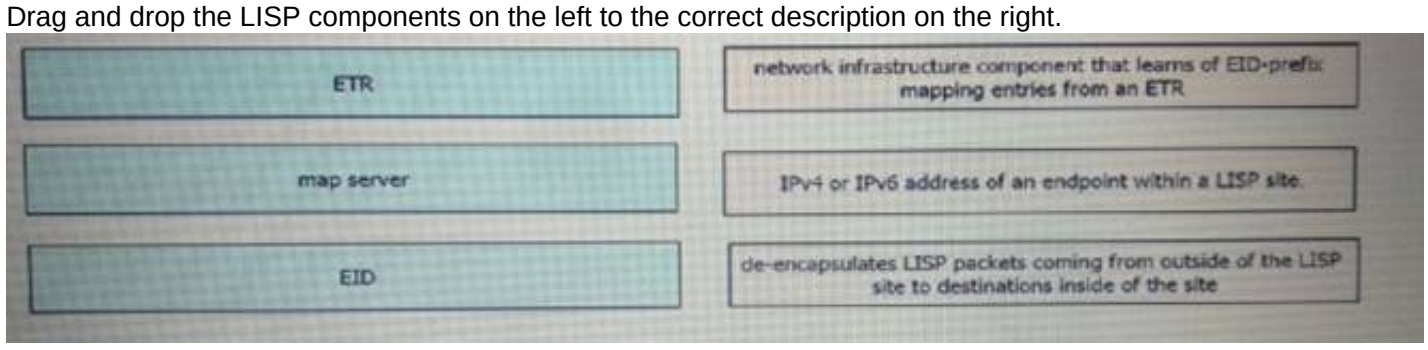
E)

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

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

Answer: CD

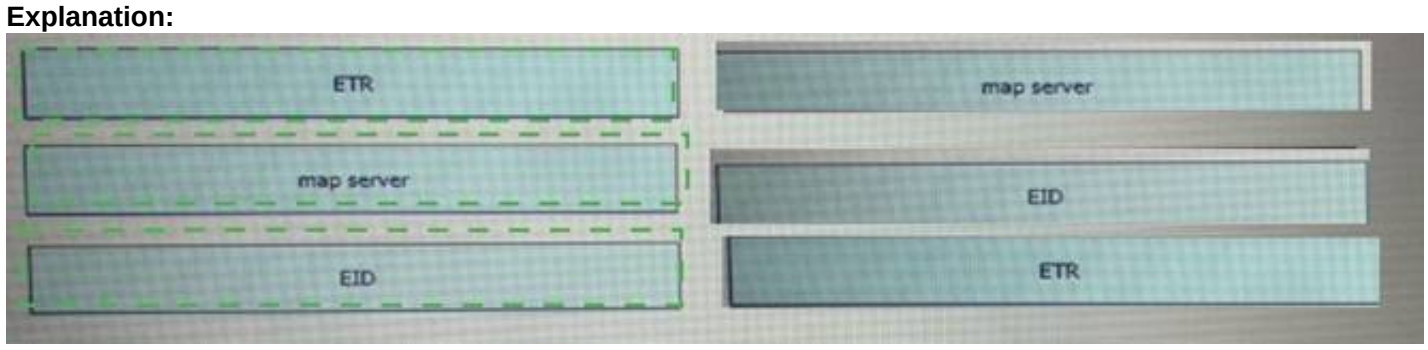
NEW QUESTION 412
DRAG DROP - (Topic 4)
Drag and drop the LISP components on the left to the correct description on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 417
- (Topic 4)
High bandwidth utilization is occurring on interface Gig0/1 of a router. An engineer must identify the flows that are consuming the most bandwidth. Cisco DNA Center is used as a flow exporter and is configured with the IP address 192.168.23.1 and UDP port 23000. Which configuration must be applied to set NetFlow data export and capture on the router?
A)

```
R1(config)# ip flow-export version 9
R1(config)# ip flow-export destination 192.168.23.1 23000
R1(config)# interface Gig0/1
R1(config-if)# ip flow-top-talkers
```

B)

```
R1(config)# ip flow-export
R1(config)# ip flow-export destination 192.168.23.1
R1(config)# interface Gig0/1
R1(config-if)# collect counter bytes
R1(config-if)# collect counter packets
```

C)

```
R1(config)# ip flow-export
R1(config)# ip flow-export destination 192.168.23.1 23000
R1(config)# interface Gig0/1
R1(config-if)# ip flow monitor
```

D)

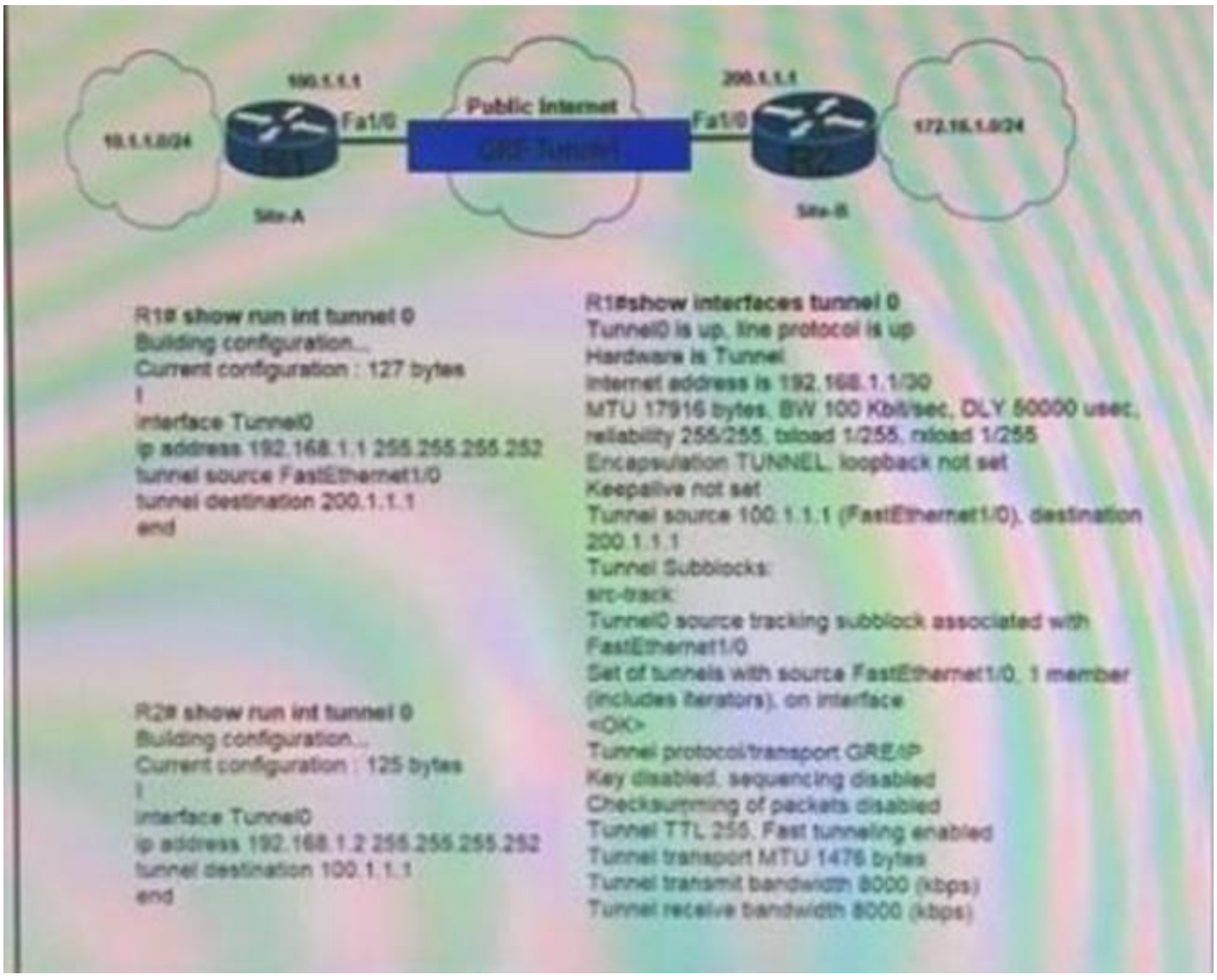
```
R1(config)# ip flow-export version 9
R1(config)# ip flow-export destination 192.168.23.1 23000
R1(config)# interface Gig0/1
R1(config-if)# ip flow ingress
R1(config-if)# ip flow egress
```

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

Answer: A

Explanation:
Option A is the correct configuration to set NetFlow data export and capture on the router. This option enables NetFlow data export to the Cisco DNA Center with the IP address 192.168.23.1 and UDP port 23000, and also enables the ip flow-top-talkers command on the interface Gig0/1. The ip flow-top-talkers command displays the top talkers (the source and destination pairs that are consuming the most bandwidth) on the interface, based on the NetFlow statistics collected by the router12.
Option B is incorrect because it does not enable the ip flow-top-talkers command on the interface Gig0/1, which is required to identify the flows that are consuming the most bandwidth. The collect counter bytes command is used to specify the fields to be collected by Flexible NetFlow, which is a different feature from NetFlow3.
Option C is incorrect because it does not specify the UDP port for the NetFlow data export destination, which is required to send the NetFlow packets to the Cisco DNA Center. The default UDP port for NetFlow is 9996, which does not match the port configured on the Cisco DNA Center4.
Option D is incorrect because it does not enable NetFlow data export on the router, which is required to send the NetFlow statistics to the Cisco DNA Center. The ip flow-export source command is used to specify the source IP address of the NetFlow packets, but it does not enable the NetFlow data export feature4.
References: 1: ip flow-top-talkers, 2: Capture NetFlow data, 3: collect counter bytes, 4: ip flow-export destination

NEW QUESTION 422
- (Topic 4)
Refer to the exhibit.



Which GRE tunnel configuration command is missing on R2?

A. tunnel source 192.181.2
B. tunnel source 172.16.1.0
C. tunnel source 200.1.1.1
D. tunnel destination 200.1.1.1

Answer: C

NEW QUESTION 425
- (Topic 4)
How does a Type 1 hypervisor function?

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

Answer: B

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

NEW QUESTION 427
- (Topic 2)
What does the Cisco DNA Center use to enable the delivery of applications through a network and to yield analytics for innovation?

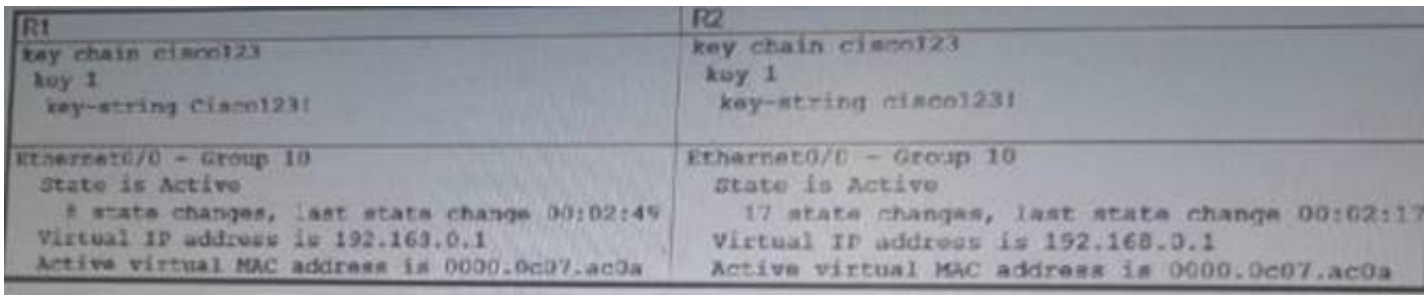
A. process adapters
B. Command Runner
C. intent-based APIs
D. domain adapters

Answer: C

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

NEW QUESTION 432

- (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.

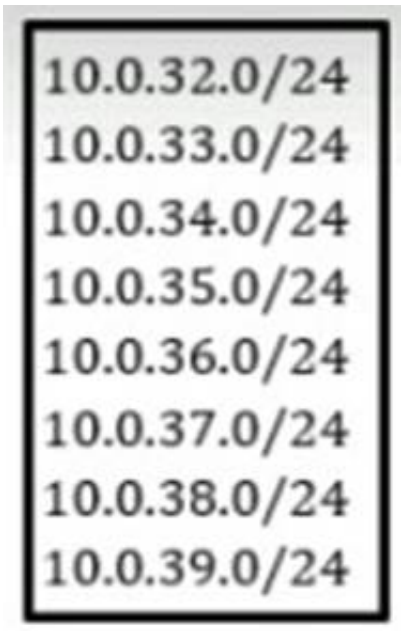
NEW QUESTION 433
- (Topic 2)
An engineer must create a new SSID on a Cisco 9800 wireless LAN controller. The client has asked to use a pre-shared key for authentication Which profile must the engineer edit to achieve this requirement?

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 435
- (Topic 2)
Refer to the exhibit.

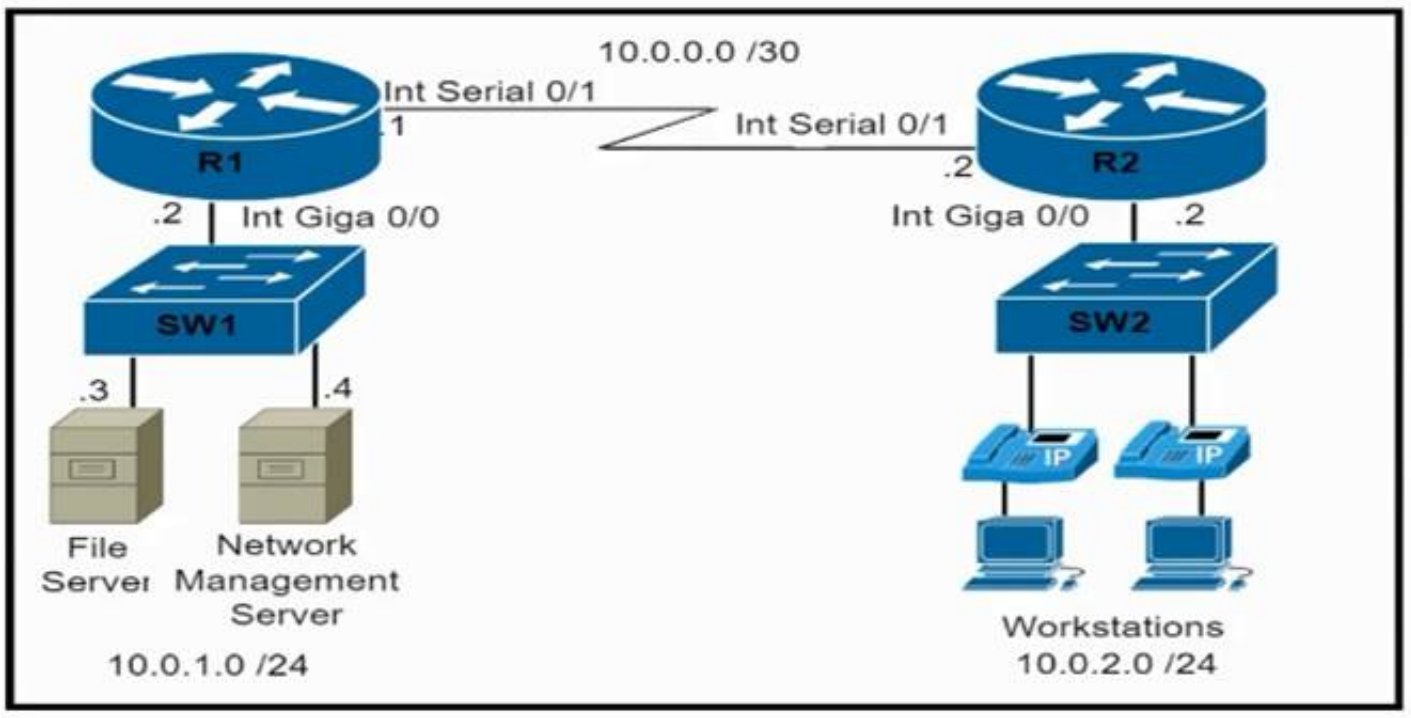


An engineer must permit traffic from these networks and block all other traffic An informational log message should be triggered when traffic enters from these prefixes Which access list must be used?

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 436
- (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

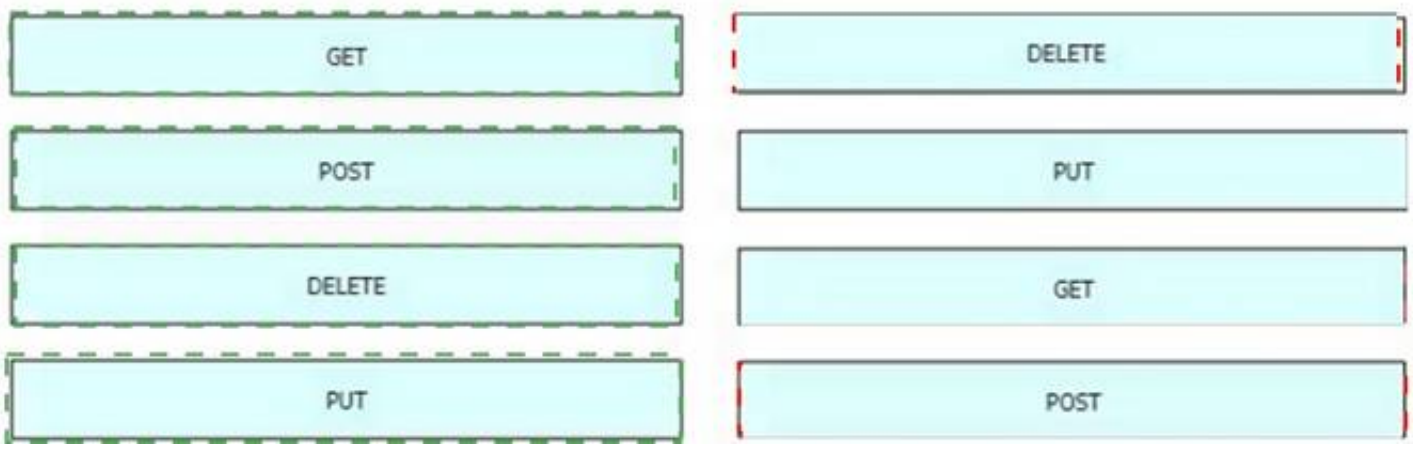
Answer: AF

NEW QUESTION 440
DRAG DROP - (Topic 2)
An engineer is working with the Cisco DNA Center API Drag and drop the methods from the left onto the actions that they are used for on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 444
- (Topic 2)

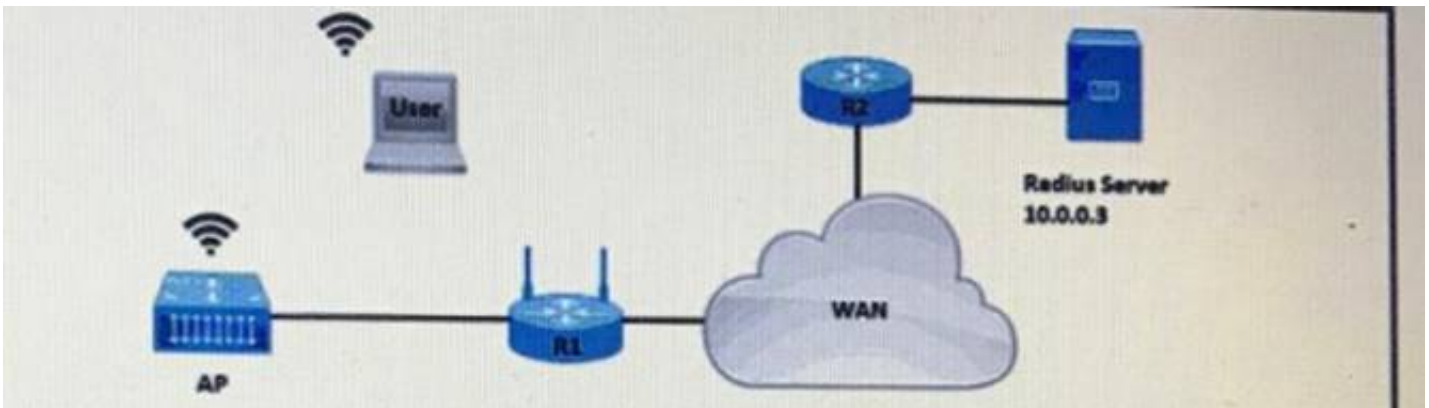
```
RP/0/0/CPU0:R2#debug isis adjacencies
RP/0/0/CPU0:Apr 2 20:57:00.421 : isis[1010]: RECV P2P IIH (L2)
from GigabitEthernet0/0/0/0 SNPA fa16.3ebe.a7bc: System ID R2,
Holdtime 30, length 1429
RP/0/0/CPU0:Apr 2 20:57:01.761 : isis[1010]: SEND P2P IIH (L1)
on GigabitEthernet0/0/0/0: Holdtime 30s, Length 41
```

Refer to the exhibit. A network operator is attempting to configure an IS-IS adjacency between two routers, but the adjacency cannot be established. To troubleshoot the problem, the operator collects this debugging output. Which interfaces are misconfigured on these routers?

A. The peer router interface is configured as Level 1 only, and the R2 interface is configured as Level 2 only
B. The R2 interface is configured as Level 1 only, and the Peer router interface is configured as Level 2 only
C. The R2 interface is configured as point-to-point, and the peer router interface is configured as multipoint.
D. The peer router interface is configured as point-as-point, and the R2 interface is configured as multipoint.

Answer: C

NEW QUESTION 445
- (Topic 2)
Refer to the exhibit.




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

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

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

Answer: D

NEW QUESTION 447
- (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 450
- (Topic 2)
What are two benefits of implementing a Cisco SD-WAN architecture? (Choose two)

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

Answer: CD

Explanation:

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

NEW QUESTION 451
- (Topic 4)
Reter to the exhibit.

A client requests a new SSID that will use web-based authentication and external RADIUS servers. Which Layer 2 security mode must be selected?

A. WPA + WPA2
B. WPA2 + WPA3
C. Static WEP
D. None

Answer: A

NEW QUESTION 452
- (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

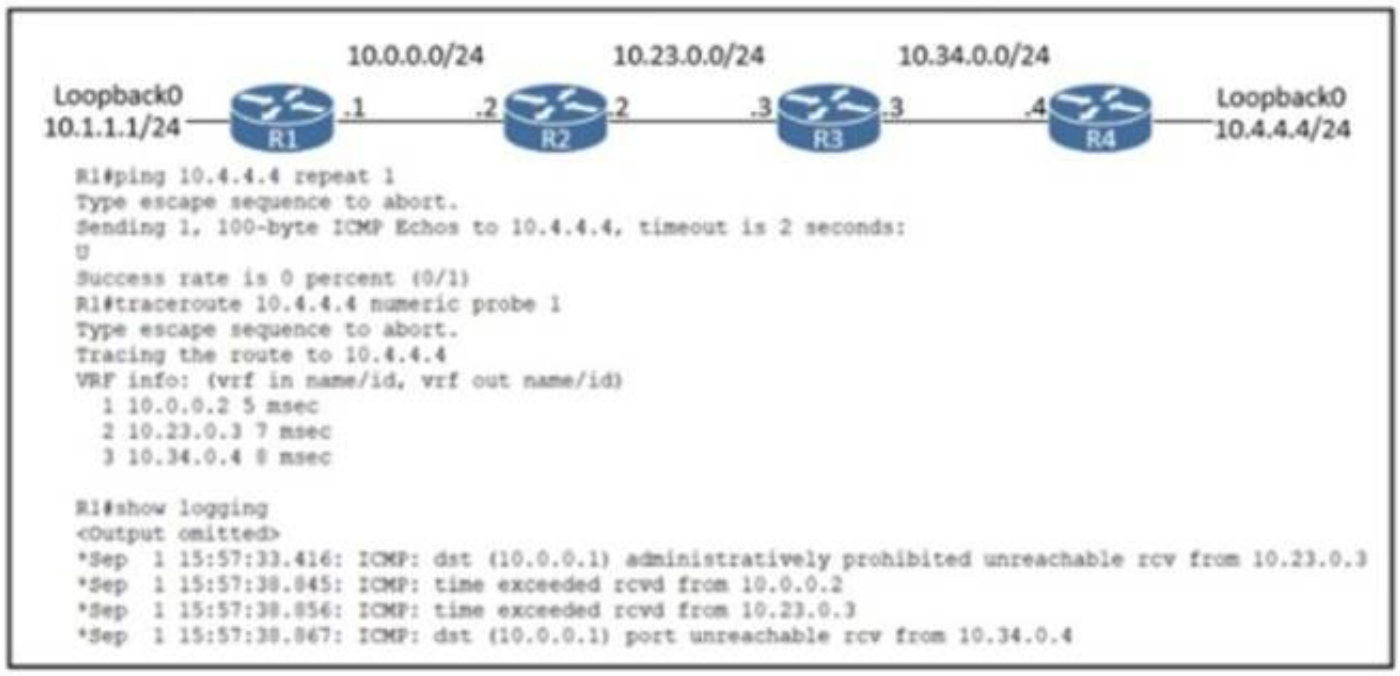
NEW QUESTION 455
- (Topic 4)

Refer to the exhibit. Clients report that they cannot connect to this SSID using the provided PSK. Which action will resolve this issue?

A. Apply the correct interface to this WLAN.
B. Apply the changes this SSID.
C. Select the PSK under authentication key management.
D. Define the correct Radio Policy.

Answer: A

NEW QUESTION 457
- (Topic 4)

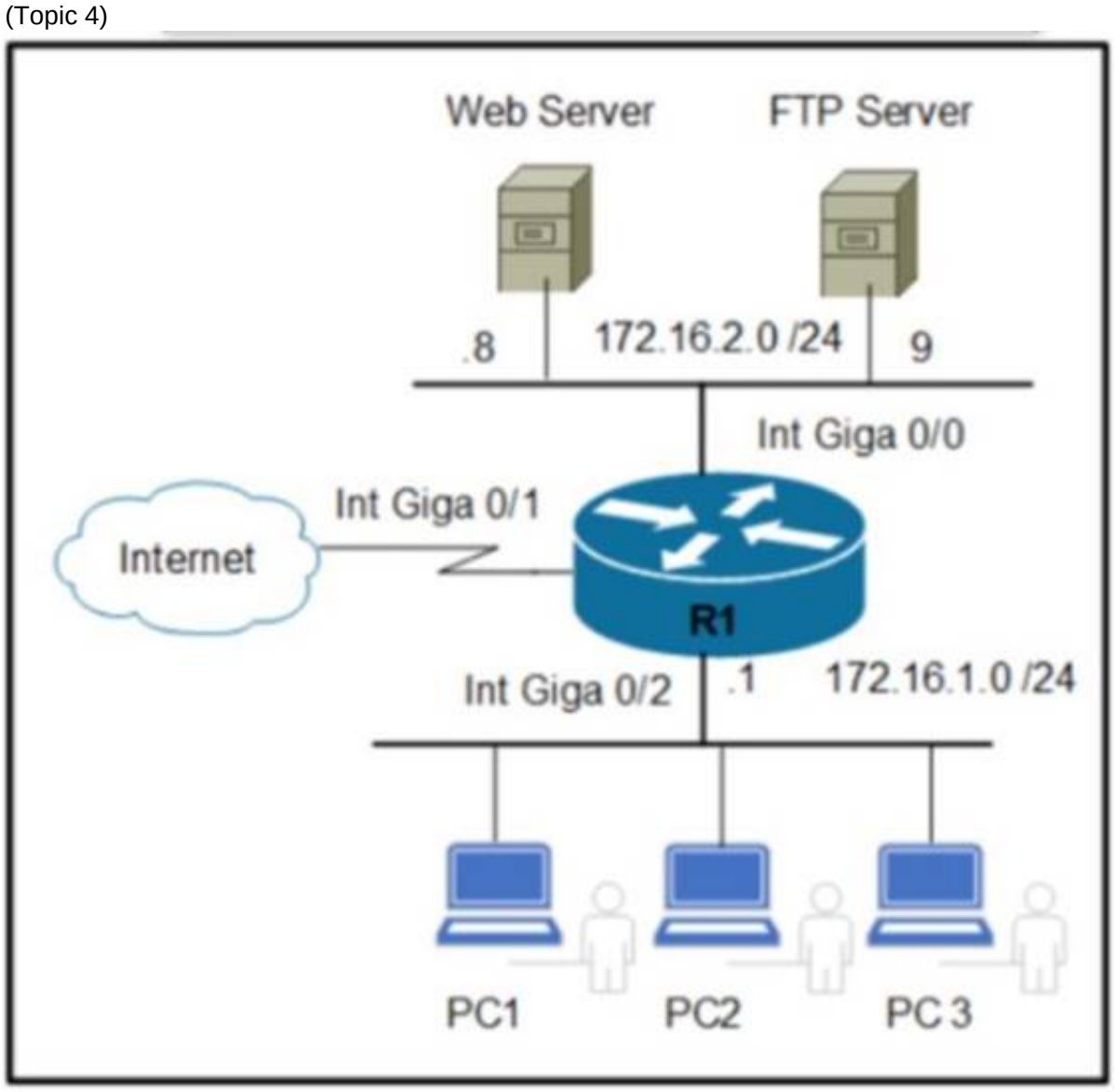


Refer to the exhibit. What is the cause of the communication failure between R1 and R4?

A. R1 is configured with the no ip unreachables command.
B. R2 is denying ICMP
C. R4 is denying ICMP.
D. R3 is denying ICMP.

Answer: A

NEW QUESTION 459
- (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

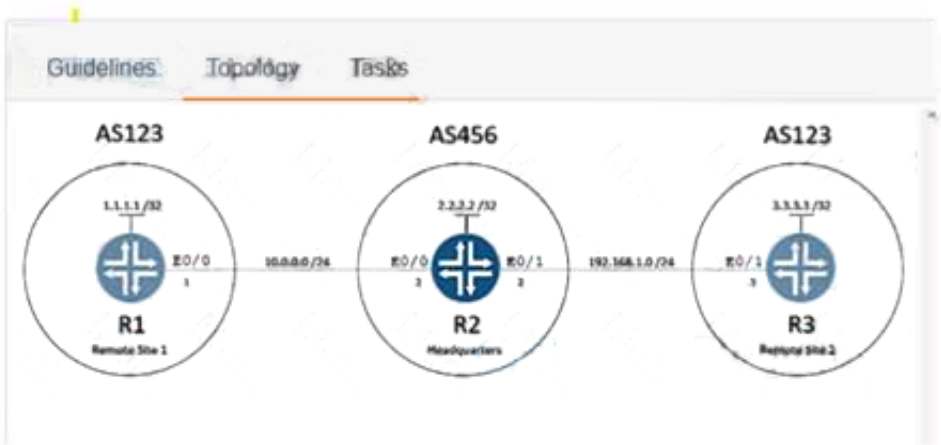
Answer: B

NEW QUESTION 462
- (Topic 4)
In a wireless network environment, what is calculated using the numencal values of the transmitter power level, cable loss, and antenna gain?

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

Answer: A

NEW QUESTION 463
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#
```

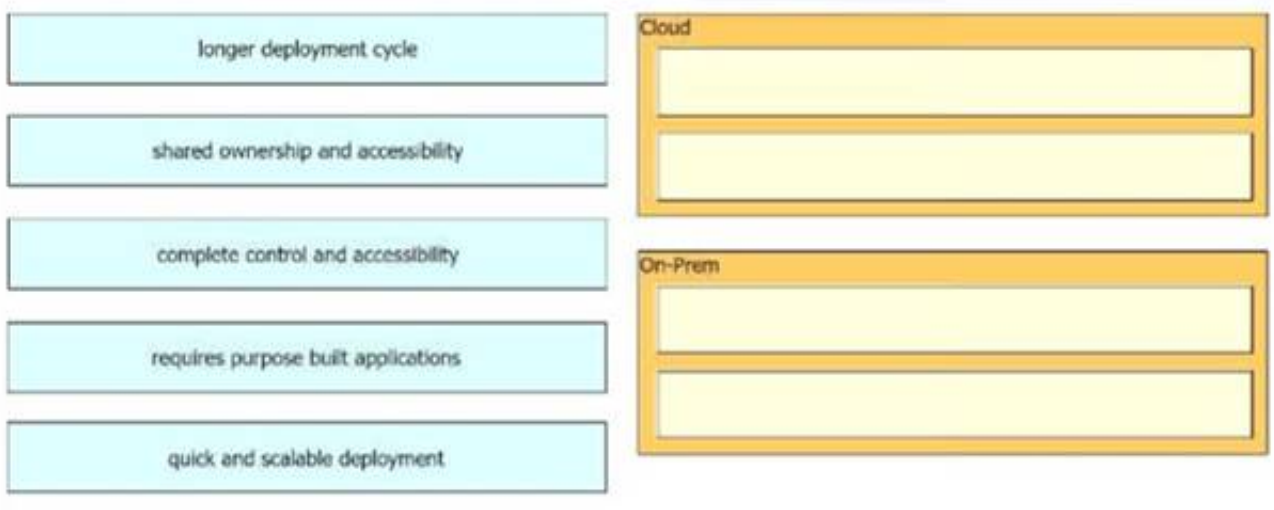
```
R3#show ip bgp
BGP table version is 4, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i
 - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f
 RT-Filter,
              x best-external, a additional-path, c RIB-compressed,

              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

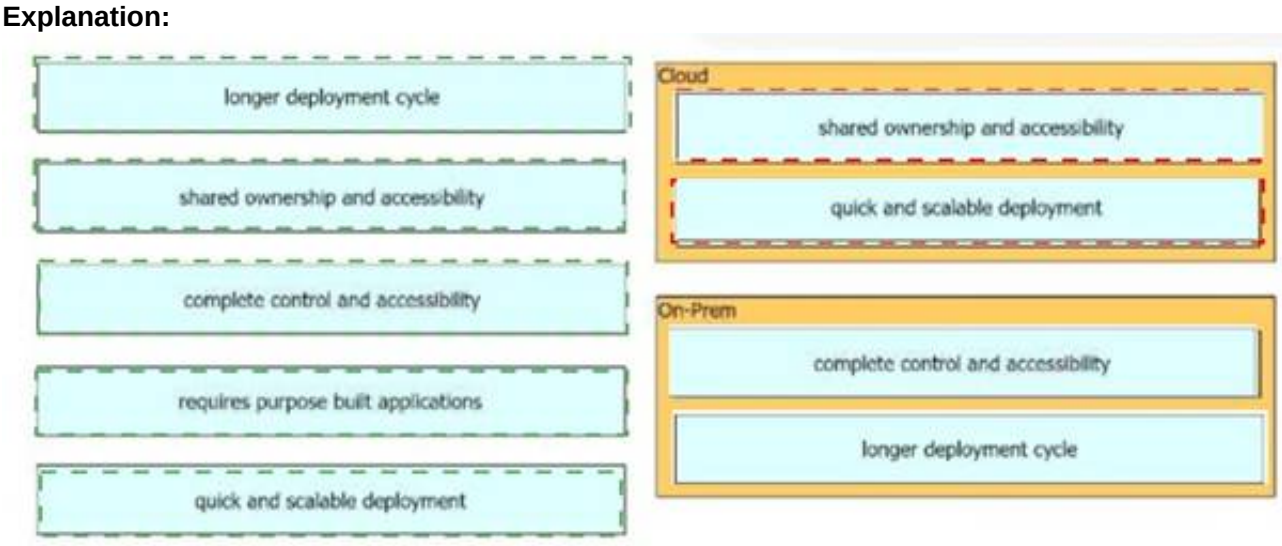
NEW QUESTION 468
DRAG DROP - (Topic 4)
Drag and drop the characteristics from the left onto the deployment models on the right Not all options are used.



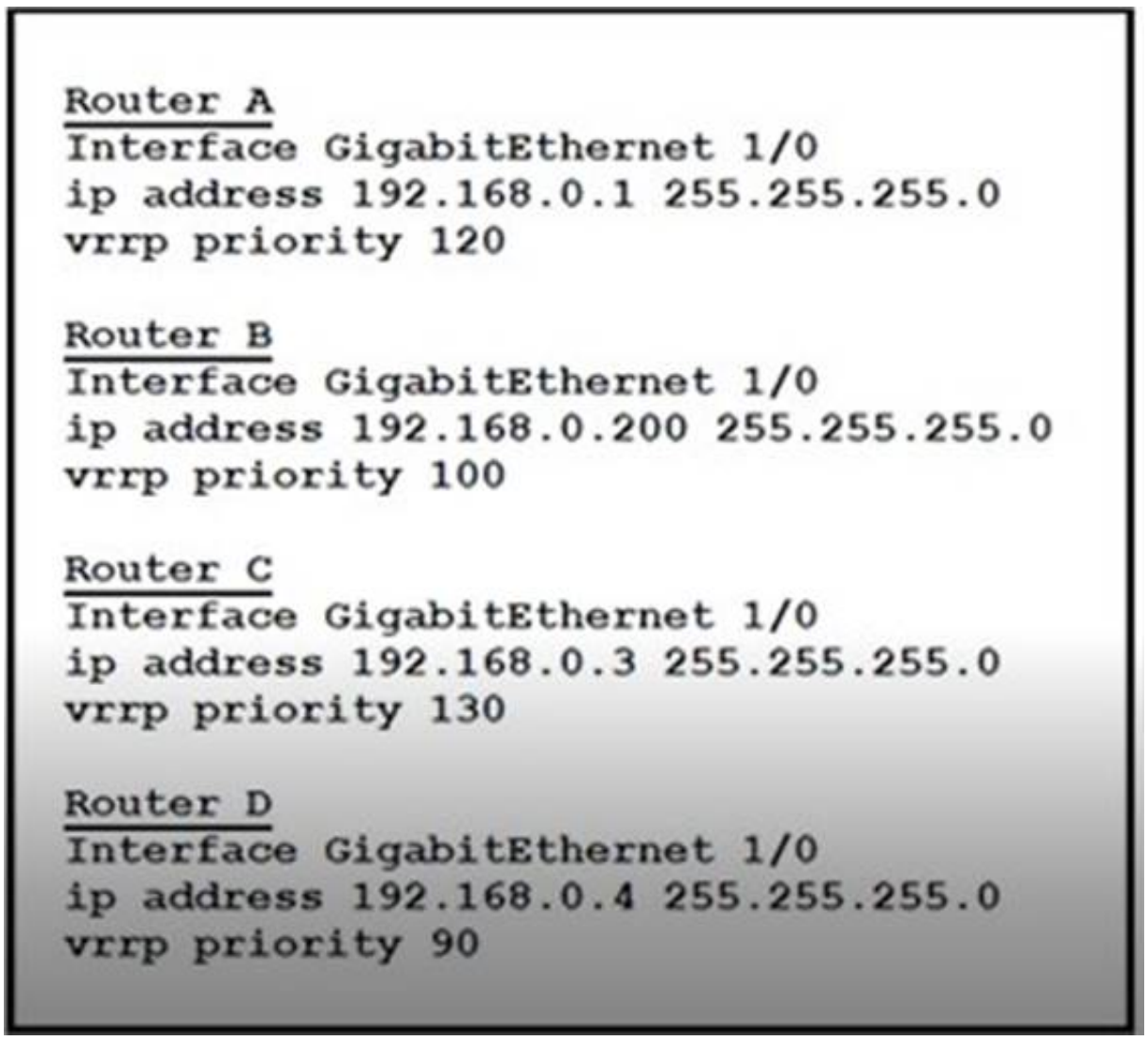
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 469
- (Topic 4)



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

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

Answer: C

NEW QUESTION 471
- (Topic 4)
Which of the following are examples of Type 2 hypervisors? (Choose three.)

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

Answer: BCE

NEW QUESTION 476
- (Topic 4)
What is a characteristics of VXLAN?

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

Answer: C

NEW QUESTION 480
- (Topic 4)
How do OSPF and EIGKP compare?

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

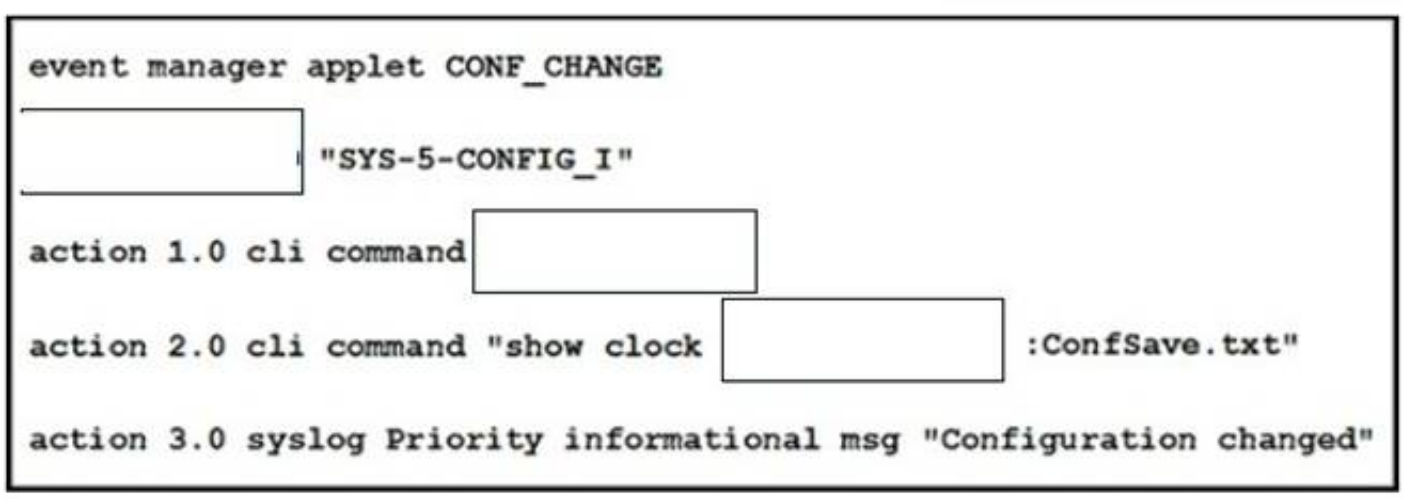
Answer: D

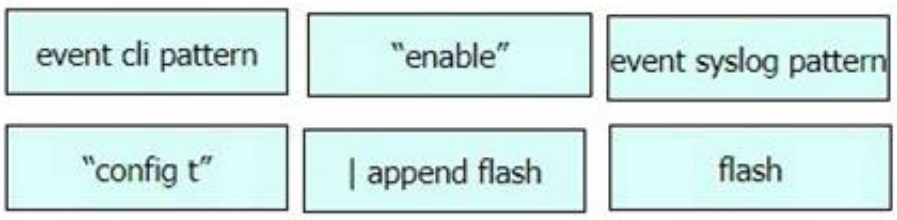
NEW QUESTION 482
- (Topic 4)
Why would a customer implement an on-premises solution instead of a cloud solution?

A. On-premises Offers greater compliance for government regulations than cloud
B. On-premises offers greater scalability than cloud.
C. On-premises oilers shorter deployment time than cloud.
D. On-premises is more secure man cloud.

Answer: D

NEW QUESTION 485
DRAG DROP - (Topic 4)
Drag and drop the snippets onto the blanks within the code to create an EEM script that adds an entry to a locally stored text file with a timestamp when a configuration change is made. Not all options are used.

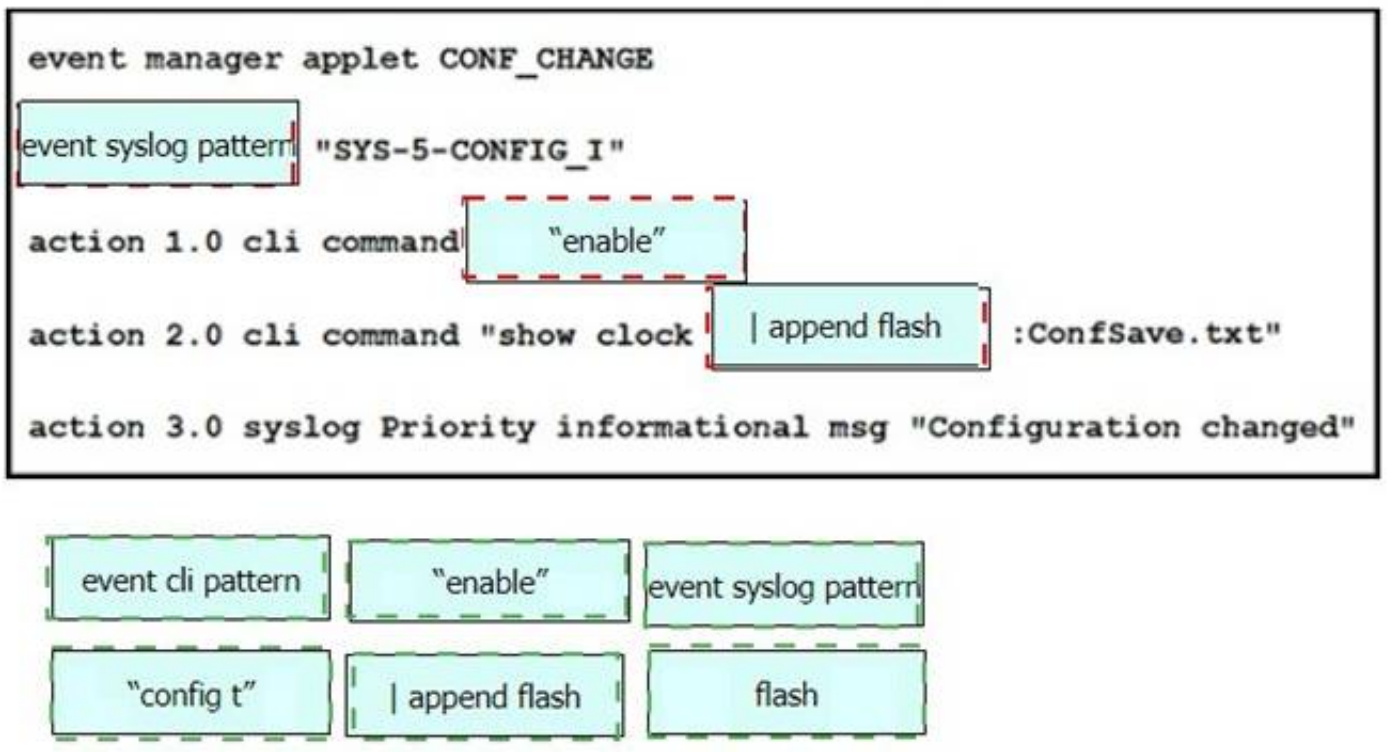




A. Mastered
B. Not Mastered

Answer: A

Explanation:



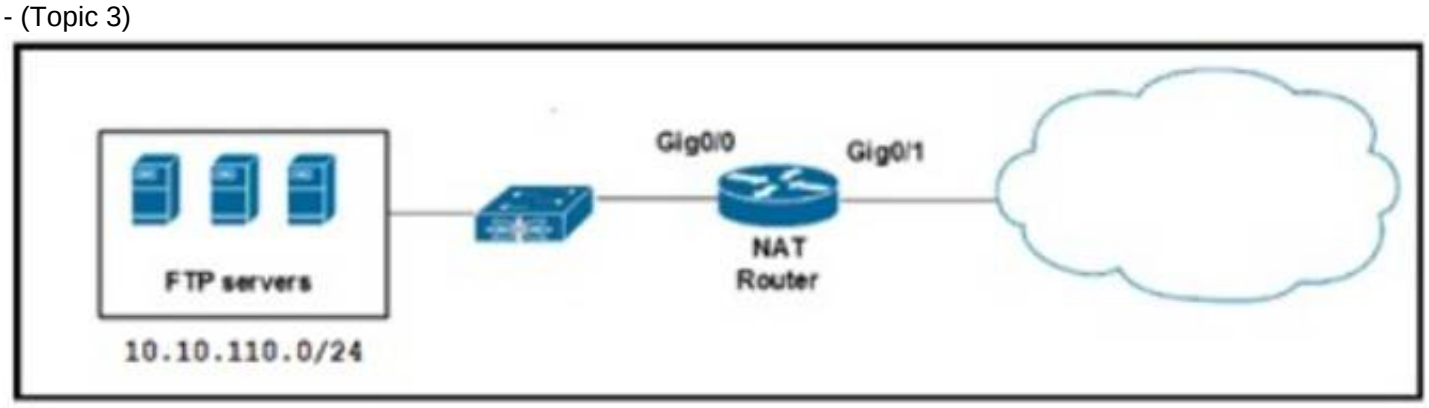
NEW QUESTION 488
DRAG DROP - (Topic 3)
Drag and drop the characteristics from the left onto the orchestration tools that they describe on the right.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 493
- (Topic 3)



Refer to the exhibit. A network engineer must load balance traffic that comes from the NAT Router and is destined to 10.10.110.10, to several FTP servers. Which two commands sets should be applied? (Choose two).
A)

```
interface gig0/0
ip address 10.10.110.1 255.255.255.0
ip nat inside
Interface gig0/1
ip address 172.16.1.1 255.255.255.252
ip nat outside
```

B)

```
ip nat pool ftp-pool 10.10.110.2 10.10.110.9 netmask 255.255.255.0
access-list 23 permit 10.10.110.10
ip nat inside destination-list 23 pool ftp-pool
```

C)

```
ip nat pool ftp-pool 10.10.110.2 10.10.110.9 netmask 255.255.255.0 type rotary
access-list 23 permit 10.10.110.10
ip nat inside destination-list 23 pool ftp-pool
```

D)

```
ip nat pool ftp-pool 10.10.110.2 10.10.110.9 netmask 255.255.255.0 type rotary
access-list 23 permit 10.10.110.10
ip nat outside destination-list 23 pool ftp-pool
```

E)

```
interface gig0/0
ip address 10.10.110.1 255.255.255.0
ip nat outside
Interface gig0/1
ip address 172.16.1.1 255.255.255.252
ip nat inside
```

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

Answer: AC

NEW QUESTION 494
- (Topic 3)

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

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

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

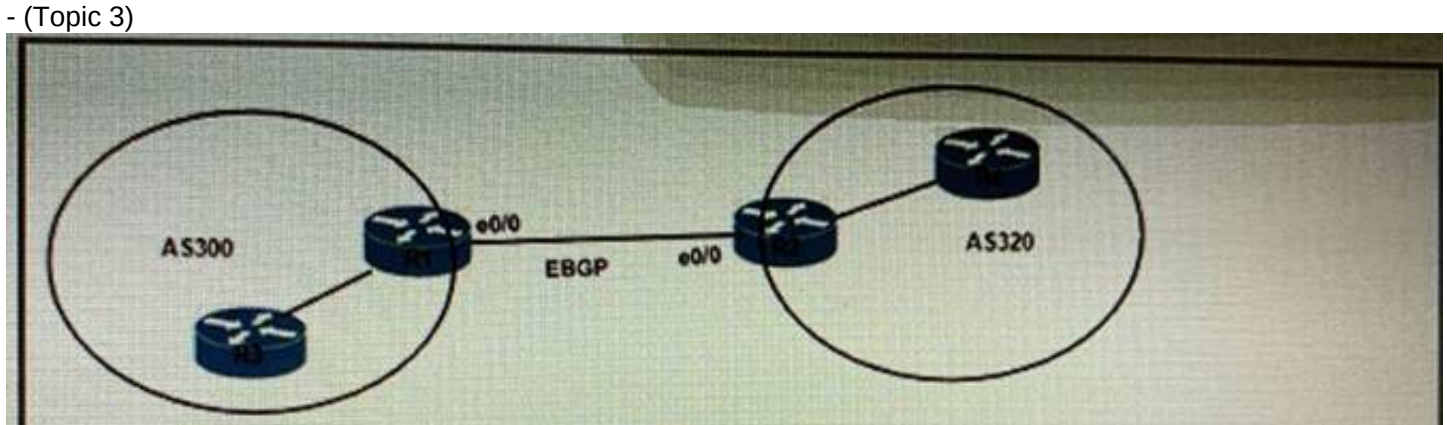
Answer: D

NEW QUESTION 499
- (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

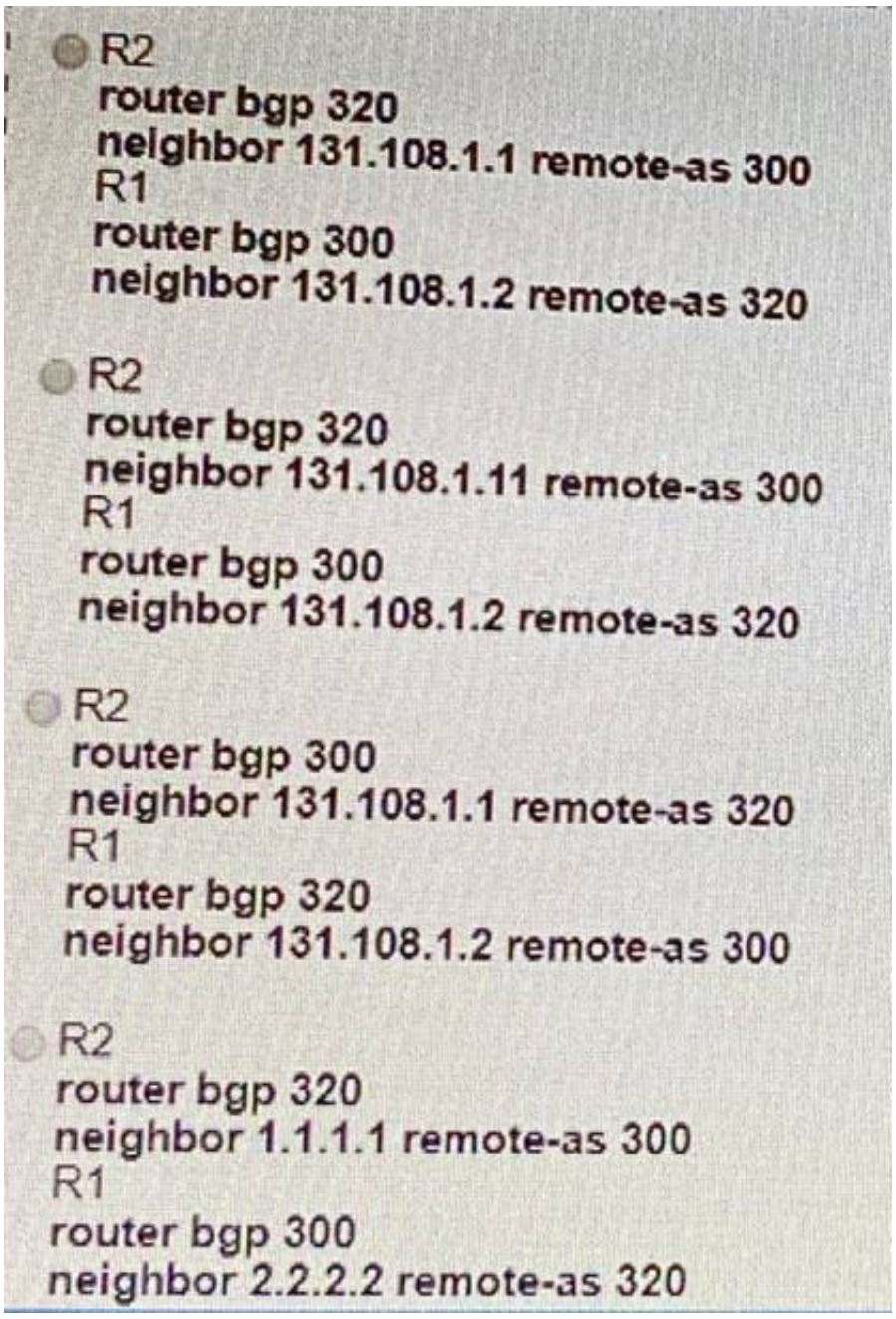
Answer: B

NEW QUESTION 500
- (Topic 3)




```
R2#debug ip bgp
BGP debugging is on
R2#
Nov 28 13:25:12: BGP: 131.108.1.11 open active, local address 131.108.1.2
Nov 28 13:25:42: BGP: 131.108.1.11 open failed: Connection timed out;
remote host not responding
```

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



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

Answer: A

NEW QUESTION 505
- (Topic 3)
Which type of tunnel Is required between two WLCs to enable Intercontroller roaming?

A. mobility
B. LWAPP
C. CAPWAP
D. iPsec

Answer: A

NEW QUESTION 509
- (Topic 3)
Refer to the exhibit.

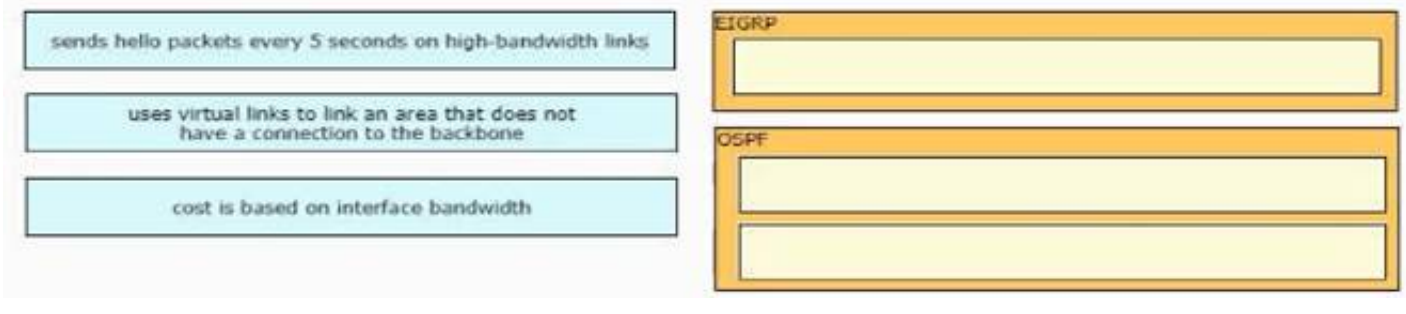

```
Switch1#show run interface Gi0/0          Switch2#show run interface Gi0/0
!                                         !
interface GigabitEthernet0/0              interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q      negotiation auto
 switchport mode trunk                     channel-group 1 mode active
 negotiation auto                         end
 channel-group 1 mode active
end

Switch1#show run interface Gi0/1          Switch2#show run interface Gi0/1
!                                         !
interface GigabitEthernet0/1              interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q      negotiation auto
 switchport mode trunk                     channel-group 1 mode passive
 negotiation auto                         end
 channel-group 1 mode passive
end
```

The port channel between the switches does not work as expected. Which action resolves the issue?

A. Interface Gi0/0 on Switch2 must be configured as passive.
B. Interface Gi0/1 on Switch1 must be configured as desirable.
C. interface Gi0/1 on Switch2 must be configured as active.
D. Trucking must be enabled on both Interfaces on Switch2.

Answer: C

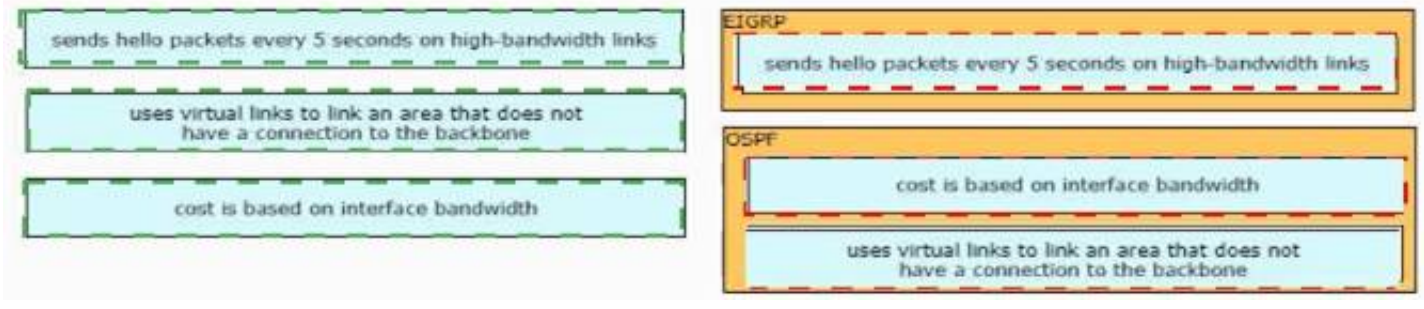
NEW QUESTION 510
DRAG DROP - (Topic 3)
Drag and drop the characteristics from the left onto the routing protocols they describe on the right.



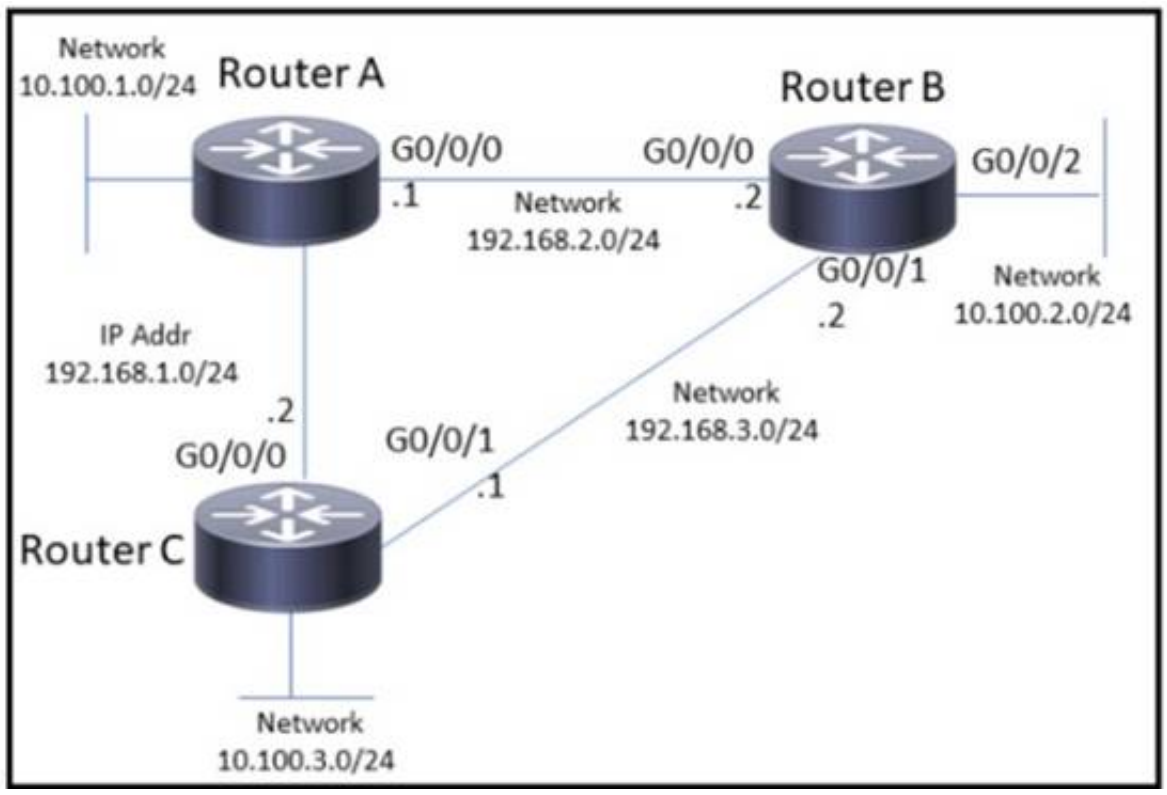
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 513
- (Topic 3)
Refer to the exhibit. A network engineer must block Telnet traffic from hosts in the range of 10.100 2.248 to 10.100.2 255 to the network 10.100.3.0 and permit everything else. Which configuration must the engineer apply'?



A)

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

B)

```
RouterB(config)# access-list 101 deny icmp 10.100.2.0 0.0.0.248 10.100.2.0 0.0.0.248
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

C)

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

D)

```
RouterB(config)# access-list 101 permit tcp 10.100.2.0 0.0.0.252 10.100.3.0 0.0.0.255
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

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

Answer: C

NEW QUESTION 515
- (Topic 3)
What does the number in an NTP stratum level represent?

A. The number of hops it takes to reach the master time server.
B. The number of hops it takes to reach the authoritative time source.
C. The amount of offset between the device clock and true time.
D. The amount of drift between the device clock and true time.

Answer: B

NEW QUESTION 518
- (Topic 3)
Which resource is able to be shared among virtual machines deployed on the same physical server?

A. applications
B. disk
C. VM configuration file
D. operating system

Answer: B

NEW QUESTION 522

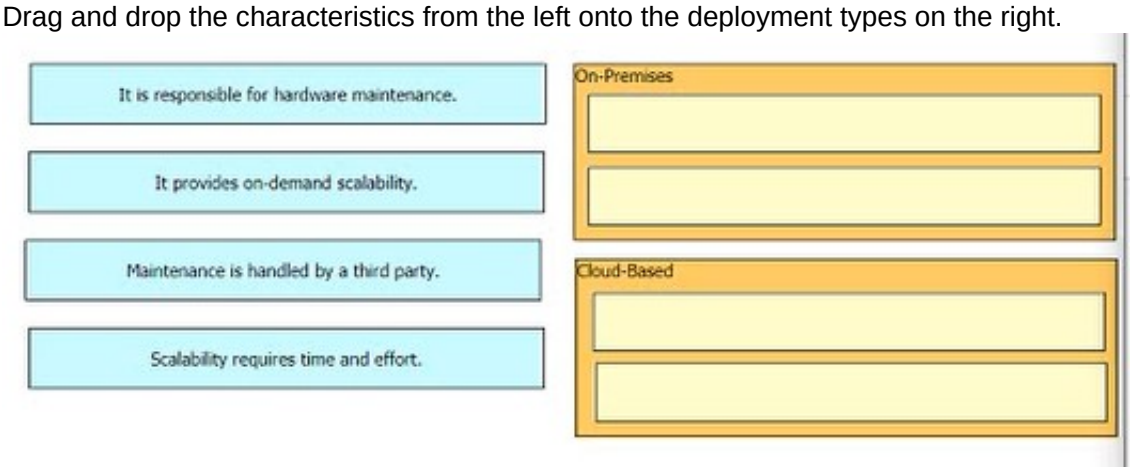
- (Topic 3)
Which IPv4 packet field carries the QoS IP classification marking?

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

Answer: D

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

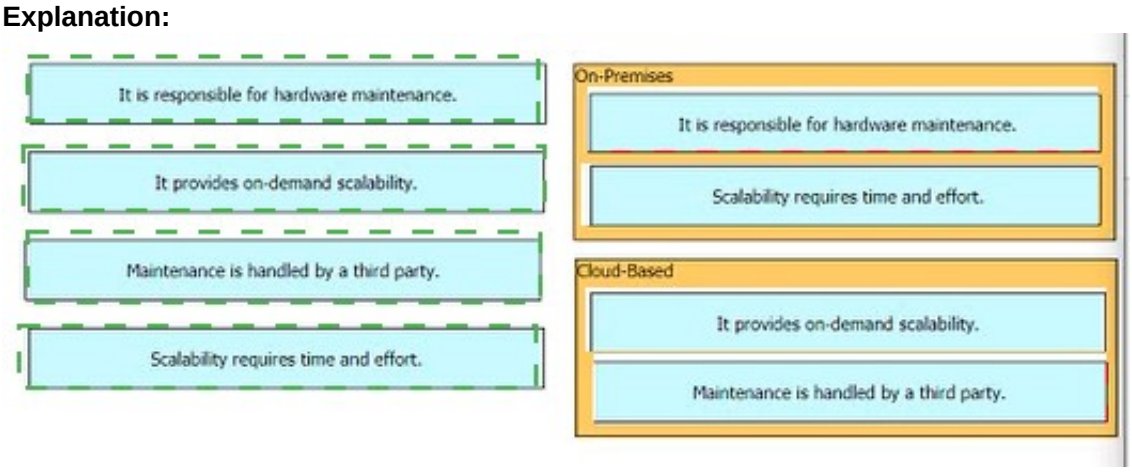
NEW QUESTION 524
DRAG DROP - (Topic 3)
Drag and drop the characteristics from the left onto the deployment types on the right.



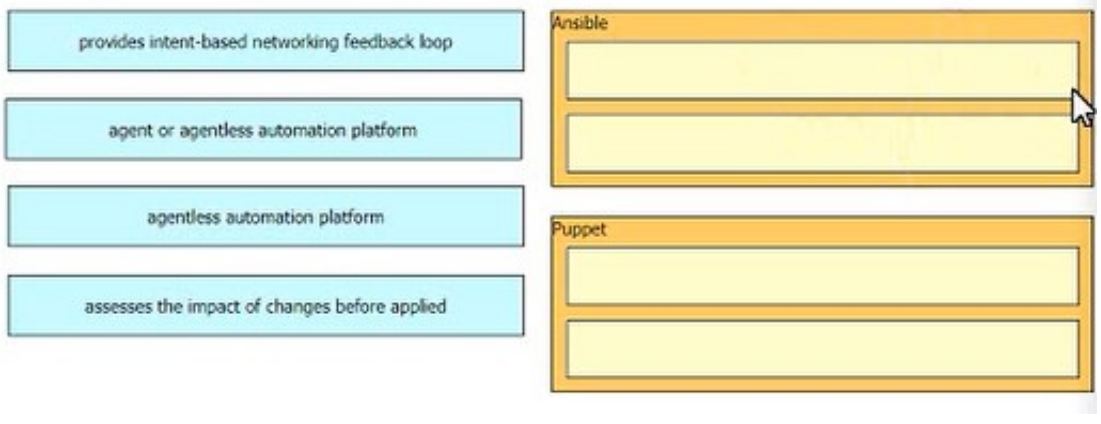
A. Mastered
B. Not Mastered

Answer: A

Explanation:



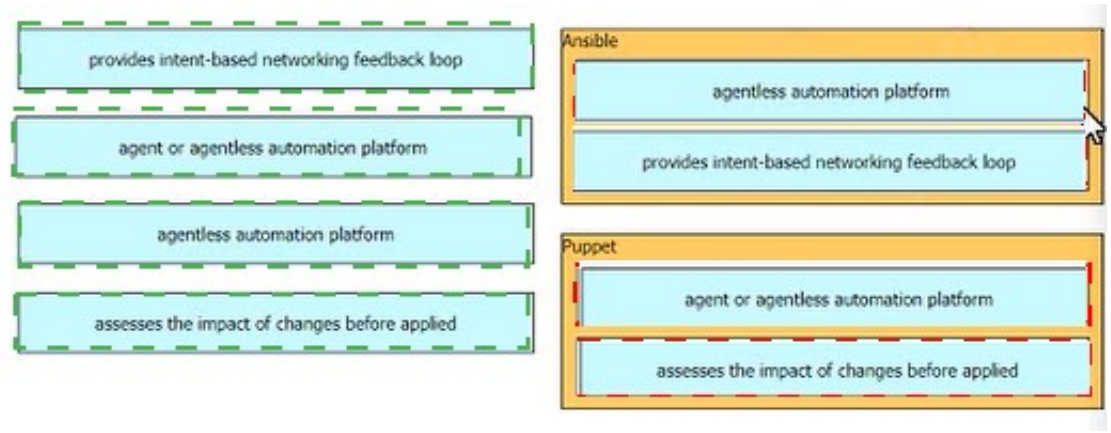
NEW QUESTION 527
DRAG DROP - (Topic 3)
Drag and drop the automation characteristics from the left onto the appropriate tools on the right.



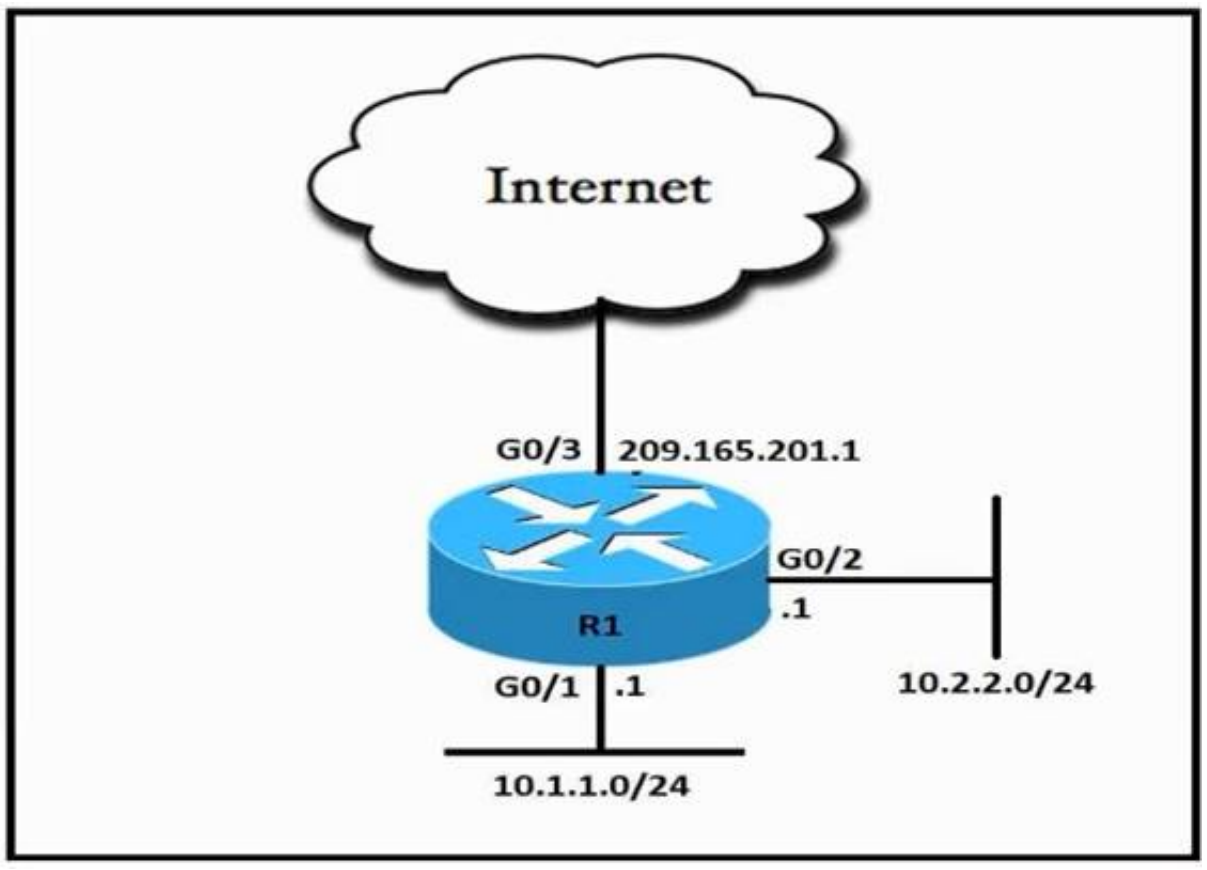
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 530
- (Topic 3)
Refer to the exhibit.



An engineer must allow all users in the 10.2.2.0/24 subnet to access the Internet. To conserve address space the public Interface address of 209 165 201.1 must be used for all external communication. Which command set accomplishes these requirements?
A)

```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/2 overload
```

B)

```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 209.165.201.1
```

C)

```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/3
```

D)

```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/3 overload
```

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

Answer: D

NEW QUESTION 531
- (Topic 3)
A network engineer is configuring OSPF on a router. The engineer wants to prevent having a route to 177.16.0.0/16 learned via OSPF. In the routing table and configures a prefix list using the command ip prefix-list OFFICE seq S deny 172.16.0.0/16. Winch two identical configuration commands must be applied to accomplish the goal? (Choose two.)

A. distribute-list prefix OFFICE in under the OSPF process
B. Ip prefix-list OFFICE seq 10 permit 0.0.0.0/0 Ie 32
C. ip prefix-list OFFICE seq 10 permit 0.0.0.0/0 ge 32
D. distribute-list OFFICE out under the OSPF process
E. distribute-list OFFICE in under the OSPF process

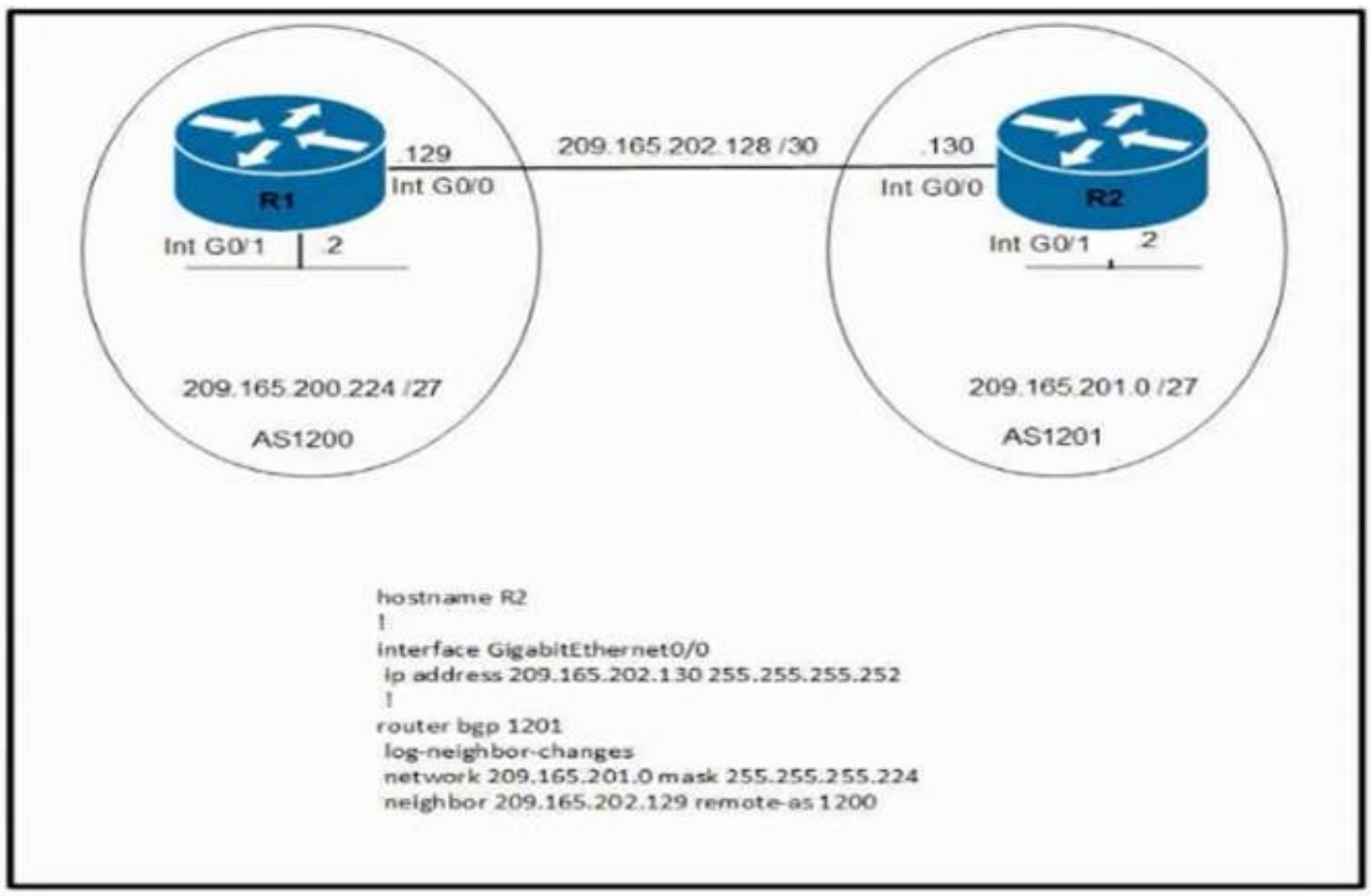
Answer: AB

NEW QUESTION 534
- (Topic 3)
How do EIGRP metrics compare to OSPF metrics?

A. EIGRP metrics are based on a combination of bandwidth and packet loss, and OSPF metrics are based on interface bandwidth.
B. EIGRP uses the Dijkstra algorithm, and OSPF uses The DUAL algorithm
C. The EIGRP administrative distance for external routes is 170. and the OSPF administrative distance for external routes is undefined
D. The EIGRP administrative distance for external routes is 170. and the OSPF administrative distance for external routes is 110

Answer: A

NEW QUESTION 537
- (Topic 3)
Refer to the exhibit.



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

A)

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

B)

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

C)

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

D)

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

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

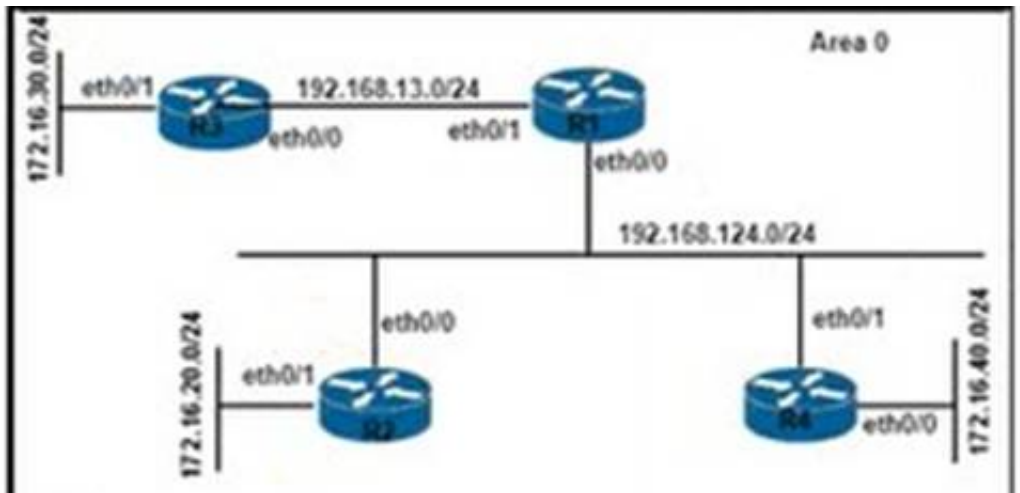
Answer: A

NEW QUESTION 539
- (Topic 3)
Which component transports data plane traffic across a Cisco SD-WAN network?

A. vSmart
B. vManage
C. cEdge
D. vBond

Answer: D

NEW QUESTION 540
- (Topic 3)



R2

```
interface ethernet0/0
ip address 192.168.124.2 255.255.255.0
!
interface ethernet0/1
ip address 172.16.20.2 255.255.255.0
!
interface loopback0
ip address 2.2.2.2 255.255.255.255
!
router ospf 1
router-id 0.0.0.2
network 2.2.2.2 0.0.0.0 area 0
network 172.16.20.0 0.0.0.255 area 0
network 192.168.0.0 0.0.255.255 area 0
```

Refer to the exhibit. An attacker can advertise OSPF fake routes from 172.16.20.0 network to the OSPF domain and black hole traffic. Which action must be taken to avoid this attack and still be able to advertise this subnet into OSPF?

A. Configure 172.16.20.0 as a stub network.
B. Apply a policy to filter OSPF packets on R2.
C. Configure a passive Interface on R2 toward 172.16.20.0.
D. Configure graceful restart on the 172.16.20.0 interface.

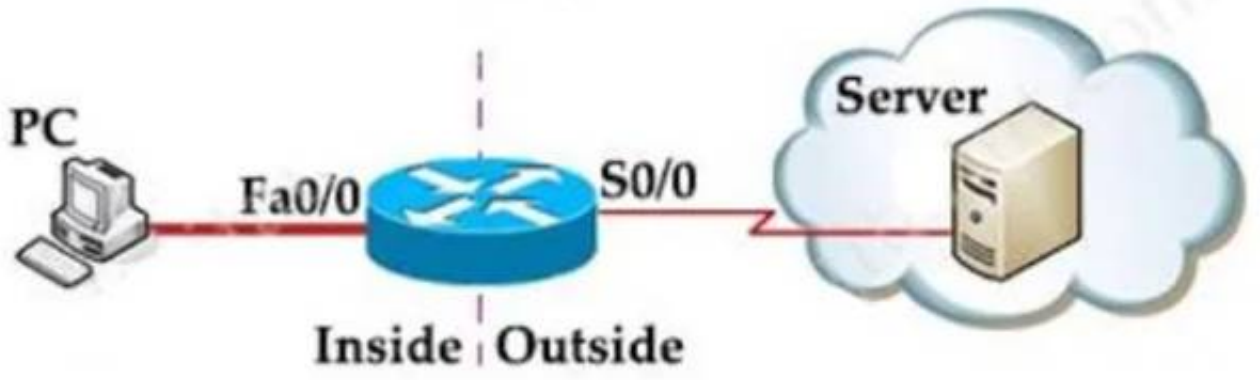
Answer: C

NEW QUESTION 541
- (Topic 3)
An engineer must configure an ACL that permits packets which include an ACK in the TCP header Which entry must be included in the ACL?

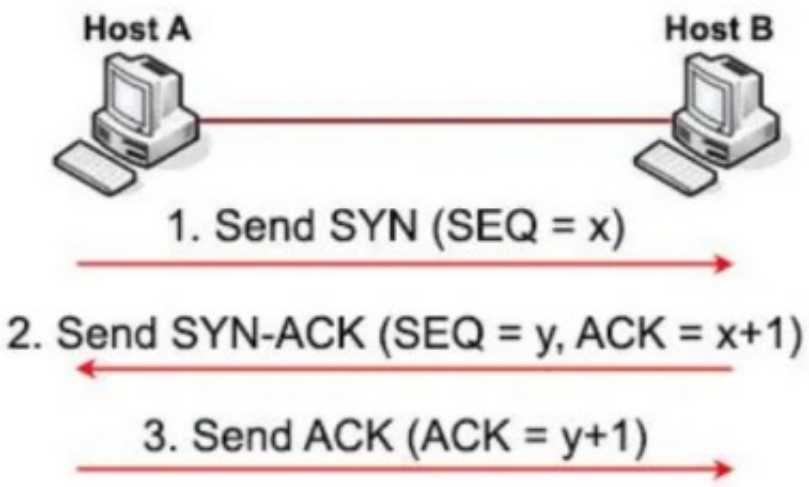
A. access-list 10 permit ip any any eq 21 tcp-ack
B. access-list 110 permit tcp any any eq 21 tcp-ack
C. access-list 10 permit tcp any any eq 21 established
D. access-list 110 permit tcp any any eq 21 established

Answer: D

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



Suppose you only want to allow the hosts inside your company to telnet to an outside server but not vice versa, you can simply use an "established" access-list like this: access-list 100 permit tcp any any established
access-list 101 permit tcp any any eq telnet
!
interface S0/0
ip access-group 100 in ip access-group 101 out
Note: Suppose host A wants to start communicating with host B using TCP. Before they can send real data, a three-way handshake must be established first. Let's see how this process takes place:



* 1. First host A will send a SYN message (a TCP segment with SYN flag set to 1, SYN is short for SYNchronize) to indicate it wants to setup a connection with host B. This message includes a sequence (SEQ) number for tracking purpose. This sequence number can be any 32-bit number (range from 0 to 232) so we use ”x” to represent it.
* 2. After receiving SYN message from host A, host B replies with SYN-ACK message (some books may call it SYN/ACK or SYN, ACK message. ACK is short for ACKnowledge). This message includes a SYN sequence number and an ACK number:
+ SYN sequence number (let‘s called it “y”) is a random number and does not have any relationship with Host A‘s SYN SEQ number.
+ ACK number is the next number of Host A‘s SYN sequence number it received, so we represent it with “x+1. It means I received your part. Now send me the next part (x + 1)”.
The SYN-ACK message indicates host B accepts to talk to host A (via ACK part). And ask if host A still wants to talk to it as well (via SYN part).
* 3. After Host A received the SYN-ACK message from host B, it sends an ACK message with ACK number “y+1” to host B. This confirms host A still wants to talk to host B.

NEW QUESTION 543
- (Topic 3)
Which two Cisco SD-WAN components exchange OMP information?

A. vAnaiytlcs
B. vSmart
C. WAN Edge
D. vBond
E. vManage

Answer: BC

NEW QUESTION 547
- (Topic 3)
A company requires a wireless solution to support its mam office and multiple branch locations. All sites have local Internet connections and a link to the main office lor corporate connectivity. The branch offices are managed centrally. Which solution should the company choose?

A. Cisco United Wireless Network
B. Cisco DNA Spaces
C. Cisco Catalyst switch with embedded controller
D. Cisco Mobility Express

Answer: B

NEW QUESTION 549
- (Topic 3)
Refer to the exhibit.

```
flow monitor FLOW-MONITOR-1
 record netflow ipv6 original-input
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet 0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
!
```

What is the effect of introducing the sampler feature into the Flexible NetFlow configuration on the router?

A. NetFlow updates to the collector are sent 50% less frequently.
B. Every second IPv4 packet is forwarded to the collector for inspection.
C. CPU and memory utilization are reduced when compared with what is required for full NetFlow.
D. The resolution of sampling data increases, but it requires more performance from the router.

Answer: C

NEW QUESTION 553
- (Topic 3)
Refer to the exhibit.

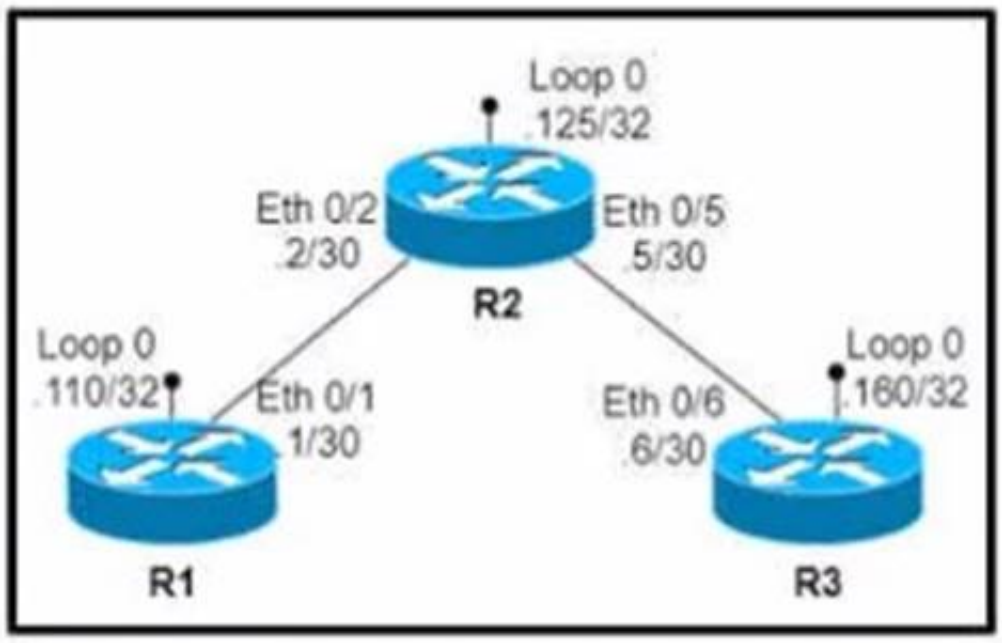
```
enable secret cisco

aaa new-model

tacacs server ise-1
address 10.1.1.1
key cisco123!

tacacs server ISE-2
address 10.2.2.1
key cisco123!

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

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

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

Answer: A

NEW QUESTION 554
- (Topic 3)
Refer to the exhibit.



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

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

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

B)

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

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

C)

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

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

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

D)

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

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

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

Answer: D

NEW QUESTION 555
- (Topic 3)
What is one benefit of adopting a data modeling language?

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

Answer: B

NEW QUESTION 559
- (Topic 3)
Which definition describes JWT in regard to REST API security?

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

Answer: D

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

NEW QUESTION 560
- (Topic 3)
Reter to the exhibit.

```
*Jun 28 19:14:50.462: %IPNAT-4-ADDR_ALLOC_FAILURE: Address allocation failed for 10.0.3.1,
pool NAT might be exhausted
*Jun 28 19:14:50.462: NAT: translation failed (A), dropping packet s=10.0.3.1 d=203.0.113.8

CPE# show ip nat translation
Pro Inside global     Inside local   Outside local      Outside global
tcp 198.51.100.5:61082 10.0.1.1:61082 203.0.113.8:23     203.0.113.8:23
--- 198.51.100.5      10.0.1.1       ---                ---
tcp 198.51.100.6:15350 10.0.2.1:15350 203.0.113.8:23     203.0.113.8:23
--- 198.51.100.6      10.0.2.1       ---                ---

CPE# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 234  Misses: 0
CEF Translated packets: 234, CEF Punted packets: 7
Expired translations: 2
Dynamic mappings:
-- Inside Source
[id: 1] access-list NAT pool NAT refcount 4
 pool NAT: id 1, netmask 255.255.255.0
    start 198.51.100.5 end 198.51.100.6
    type generic, total addresses 2, allocated 2 (100%), misses 7
nat-limit statistics:
 max entry: max allowed 0, used 0, missed 0
Outside global interfaces count: 1
```

An administrator troubleshoots intermittent connectivity from internal hosts to an external public server. Some internal hosts can connect to the server while others receive an ICMP Host Unreachable message and these hosts change over time. What is the cause of this issue?

A. The translator does not use aOdress overloading
B. The NAT ACL does not match alt internal hosts
C. The NAT ACL and NAT pool share the same name
D. The NAT pool netmask rs excessively wide

Answer: B

NEW QUESTION 563
- (Topic 3)
An engineer must configure an EXEC authorization list that first checks a AAA server then a local username. If both methods fail, the user is denied. Which configuration should be applied?

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

Answer: D

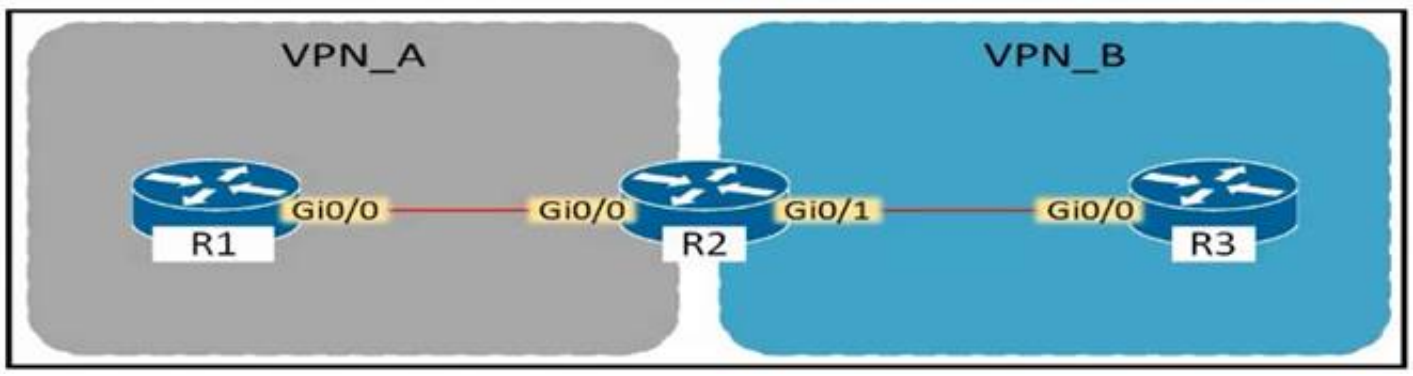
NEW QUESTION 567
- (Topic 3)
In a Cisco SD-Access wireless architecture which device manages endpoint ID to edge node bindings?

A. fabric control plane node
B. fabric wireless controller
C. fabric border node
D. fabric edge node

Answer: A

Explanation:
SD-Access Wireless Architecture Control Plane Node –A Closer Look Fabric Control-Plane Node is based on a LISP Map Server / Resolver
Runs the LISP Endpoint ID Database to provide overlay reachability information
+ A simple Host Database, that tracks Endpoint ID to Edge Node bindings (RLOCs)+ Host Database supports multiple types of Endpoint ID (EID), such as IPv4 /32, IPv6 /128* or MAC/48+ Receives prefix registrations from Edge Nodes for wired clients, and from Fabric
mode WLCs for wireless clients+ Resolves lookup requests from FE to locate Endpoints+ Updates Fabric Edge nodes, Border nodes with wireless client mobility and RLOC information

NEW QUESTION 572
- (Topic 3)
Refer to The exhibit.



Assuming that R1 is a CE router, which VRF is assigned to Gi0/0 on R1?

A. VRF VFN_A
B. VRF VPN_B
C. management VRF
D. default VRF

Answer: D

NEW QUESTION 577
- (Topic 3)
Refer to the exhibit.

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# description source1
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/4 - 8 tx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/3
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 100
Device(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
Device(config-mon-erspan-src-dst)# ip prec 5
Device(config-mon-erspan-src-dst)# ip ttl 32
Device(config-mon-erspan-src-dst)# mtu 1700
Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)# vrf 1
Device(config-mon-erspan-src-dst)# no shutdown
Device(config-mon-erspan-src-dst)# end
```

An engineer must configure an ERSPAN session with the remote end of the session 10.10.0.1. Which commands must be added to complete the configuration?
A)

```
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)#no origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)#ip address 10.10.0.1
```

B)

```
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)#no origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)#ip destination address 10.10.0.1
```

C)

```
Device(config)# monitor session 1 type erspan-destination
Device(config-mon-erspan-src)# source
Device(config-mon-erspan-src-dst)#origin ip address 10.1.0.1
```

D)

```
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)#no vrf 1
```

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

Answer: A

Explanation:
Example: Configuring an ERSPAN Source Session on a WAN Interface The following example shows how to configure more than one WAN interface in a single ERSPAN source monitor session. Multiple interfaces have been separated by a commas. monitor session 100 type erspan-source
source interface Serial 0/1/0:0, Serial 0/1/0:6
Example: Configuring an ERSPAN Destination Session
The following example shows how to configure an ERSPAN destination session: monitor session 2 type erspan-destination
destination interface GigabitEthernet1/3/2 destination interface GigabitEthernet2/2/0 source
erspan-id 100
ip address 10.10.0.1

NEW QUESTION 581
.....

Relate Links

100% Pass Your 350-401 Exam with Exambible Prep Materials

https://www.exambible.com/350-401-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/