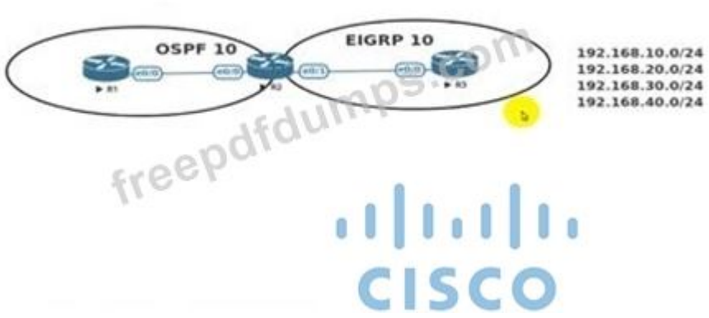
Cisco.300-410.v2023-02-14.q151

Exam Code:	300-410
Exam Name:	Implementing Cisco Enterprise Advanced Routing and Services
Certification Provider:	Cisco
Free Question Number:	151
Version:	v2023-02-14
# of views:	2064
# of Questions views:	1510
https://www.freepdfdumps.com/Cisco.300-410.v2023-02-14.q151.html	

NEW QUESTION: 1
Refer to the exhibit.



An engineer must redistribute networks 192.168.10.0/24 and 192.168.20.0/24 into OSPF from EIGRP. where the metric must be added when traversing through multiple hops to start an external route of 20 The engineer notices that the external metric is fixed and does not add at each hop. Which configuration resolves the issue?

```
R2(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R2(config)#access-list 10 permit 192.168.20.0 0.0.0.255
!
R2(config)#route-map RD permit 10
R2(config-route-map)#match ip address 10
R2(config-route-map)#set metric 20
R2(config-route-map)#set metric-type type-2
!
R2(config)#router ospf 10
R2(config-router)#redistribute eigrp 10 subnets route-map RD

R2(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R2(config)#access-list 10 permit 192.168.20.0 0.0.0.255
!
R2(config)#route-map RD permit 10
R2(config-route-map)#match ip address 10
R2(config-route-map)#set metric 20
R2(config-route-map)#set metric-type type-1
!
R2(config)#router ospf 10
R2(config-router)#redistribute eigrp 10 subnets route-map RD
```

```
R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit 192.168.20.0 0.0.0.255
!
R1(config)#route-map RD permit 10
R1(config-route-map)#match ip address 10
R1(config-route-map)#set metric 20
R1(config-route-map)#set metric-type type-1
!
R1(config)#router ospf 10
R1(config-router)#redistribute eigrp 10 subnets route-map RD

R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit 192.168.20.0 0.0.0.255
!
R1(config)#route-map RD permit 10
R1(config-route-map)#match ip address 10
R1(config-route-map)#set metric 20
R1(config-route-map)#set metric-type type-2
!
R1(config)#router ospf 10
R1(config-router)#redistribute eigrp 10 subnets route-map RD
```

A. Option B
B. Option C
C. Option A
D. Option D
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
Refer to the exhibit.

A network administrator is trying to switch to the privileged EXEC level on R1 but failed. Which configuration resolves the issue?

A. tacass server enable-password Cisco@123

B. tacacs-server enable-password Cisco@123

C. Enable password Cisco@123

D. enable-password Cisco@123

Answer: D (LEAVE A REPLY)

NEW QUESTION: 3

Refer to the exhibit.

Refer to the exhibit. An engineer configured BGP and wants to select the path from 10.77.255.57 as the best path instead of current best path. Which action resolves the issue?

A. Configure AS_PATH prepend for the desired best path

B. Configure higher MED to select as the best path.

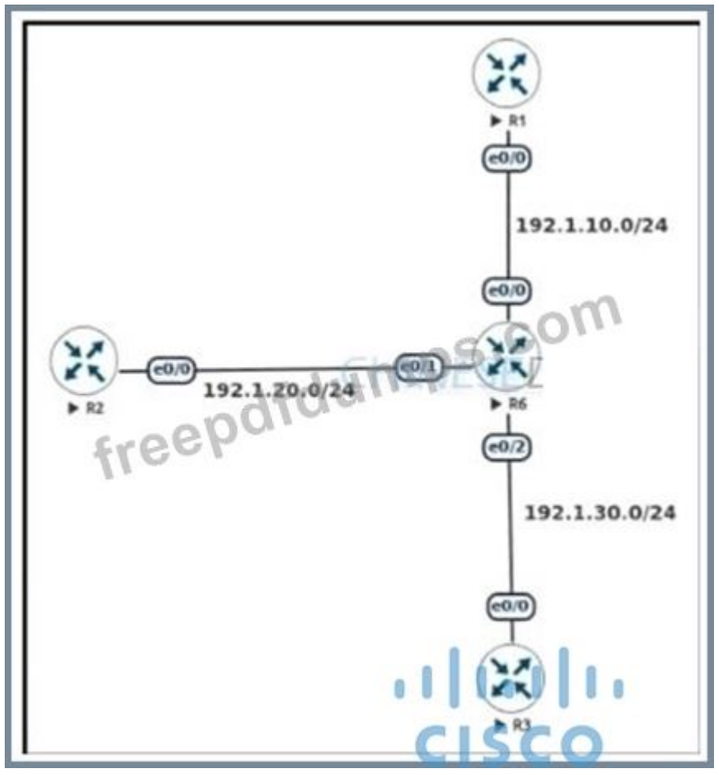
C. Configure lower LOCAL_PREF to select as the best path.

D. Configure AS_PATH prepend for the current best path

Answer: D (LEAVE A REPLY)

NEW QUESTION: 4

Refer to the exhibit.



An engineer must configure DMVPN Phase 3 hub-and-spoke topology to enable a spoke-to-spoke tunnel. Which NHRP configuration meets the requirement on R6?

A. Option C
B. Option D
C. Option A
D. Option B
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
Refer to the exhibit.

```
R2#show running-config | section ospf
 ip ospf l area 1
 ip ospf l area 1
router ospf 1
 log-adjacency-changes
 area i stub no-summary
R2#show ip ospf interface brief
Interface    PID   Area   IP Address/Mask    Cost   State  Nbrs  F/C
Lo0          1     1      10.0.0.2/32        1      Loop   0/0
Fa0/0        1     1      10.10.10.1/30      1      DR     0/1
R2#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 116 bytes
!
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.255.252
 ip mtu 1400
 ip ospf1 area 1
 duplex full
end
```

```
R2#show ip ospf neighbor

Neighbor ID  Pri  State           Dead Time   Address       Interface
10.0.0.1     1    EXSTART/BDR     00:00:37    10.10.10.2    FastEthernet0/0
```

```
R1#show running-config | section ospf
 ip ospf l area o
 ip ospf l area 1
router ospf 1
 log-adjacency-changes
 area 1 stub no-summary
R1#show ip ospf interface brief
Interface    PID   Area   IP Address/Mask    Cost   State  Nbrs  F/C
Lo0          1     0      10.0.0.1/32        1      LOOP   0/0
Lo0          1     1      10.10.10.2/30 Fa/o 1      BDR    0/1
R1#show running-config interface fastEthernet 1/0
Building configuration...

Current configuration : 115 bytes
!
interface FastEthernet1/0
 ip address 10.10.10.2 255.255.255.252
 ip ospf1 area 1
 duplex auto
 speed auto
end
```

```
R1#show ip ospf neighbor

Neighbor ID      Pri  State          Dead Time   Address     Interface
10.10.10.1 R1#   1    EXCHANGE/DR    00:00:39    10.10.10.1  FastEthernet1/0
```

Which action restores OSPF adjacency between R1 and R2?

A. Change the IP MTU of R1 Fa1/0 to 1500

B. Change the IP MTU of R2 Fa0/0 to 1300

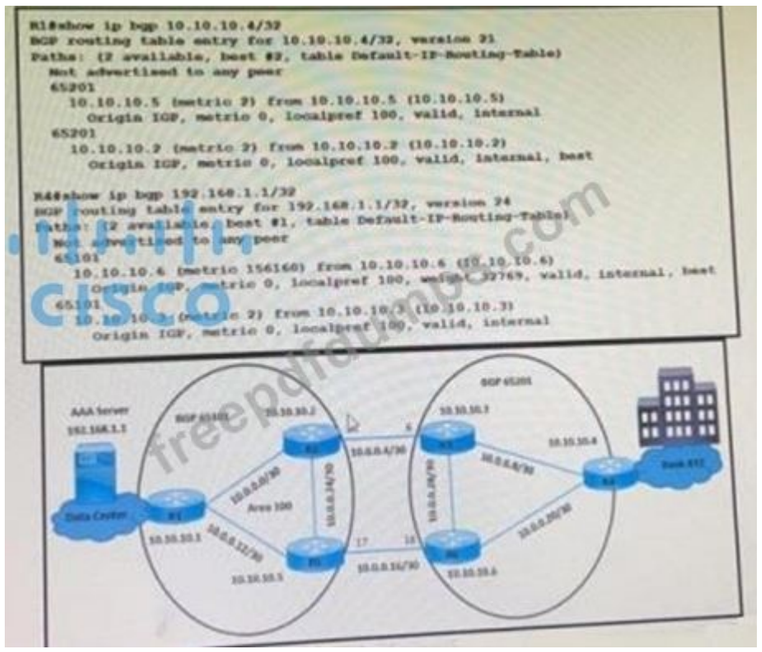
C. Change the IP MTU of R2 Fa0/0 to 1500

D. Change the IP MTU of R1 Fa1/0 to 1300

Answer: (SHOW ANSWER)

NEW QUESTION: 6

Refer to the exhibit.



A customer reports that user traffic of bank XYZ to the AAA server is not using the primary path via the R3-R2 link. The network team observes:

No fiber is cut on links R2 and R3.

As101 and AS 201 routers established BGP peering.

Which configuration resolves the issue?

A)

```
R2(config)#route-map BGP-Path permit 10
R2(config-route-map)# set metric 200
R2(config)#router bgp 65101
R2(config-router)# neighbor 10.10.10.3 route-map BGP-Path out
```

B)

```
R6(config)#router bgp 65201
R6(config-router)#no neighbor 10.10.10.5 weight 32769
```

C)

```
R4(config)#router bgp 65201
R4(config-router)#no neighbor 10.10.10.5 weight 32769
```

D)

```
R1(config)#route-map BGP-Path permit 10
R1(config-route-map)# set local-preference 200
R1(config)#router bgp 65101
R1(config-router)# neighbor 10.10.10.2 route-map BGP-Path out
```

A. Option C

B. Option D

C. Option A

D. Option B

Answer: C (LEAVE A REPLY)

NEW QUESTION: 7

Refer to the exhibit.

```
ip prefix-list DMZ-STATIC seq 5 permit 10.1.1.0/24
!
route-map DMZ permit 10
     match ip addresss prefix-list DMZ-STATIC
!
router ospf 1
network 0.0.0.0 0.0.0.0 area 0
redistribute static route-map DMZ
!
ip route 10.1.1.0 255.255.255.0 10.20.20.1
```


The static route is not present in the routing table of an adjacent OSPF neighbor router. Which action resolves the issue?

A. Configure the next hop of 10.20.20.1 in the prefix list DMZ-STATIC

B. Configure the subnets keyword in the redistribution command

C. Configure a permit 20 statement to the route map to redistribute the static route

D. Configure the next-hop interface at the end of the static router for it to get redistributed

Answer: B (LEAVE A REPLY)

NEW QUESTION: 8

Which two protocols work in the control plane of P routers across the MPLS cloud? (choose two)

A. MPLS OAM

B. ECMP

C. LSP

D. RSVP

E. LDP

Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 9

Which two methods use IPsec to provide secure connectivity from the branch office to the headquarters office? (Choose two.)

A. Virtual Tunnel Interface (VTI)

B. PPPoE

C. MPLS VPN

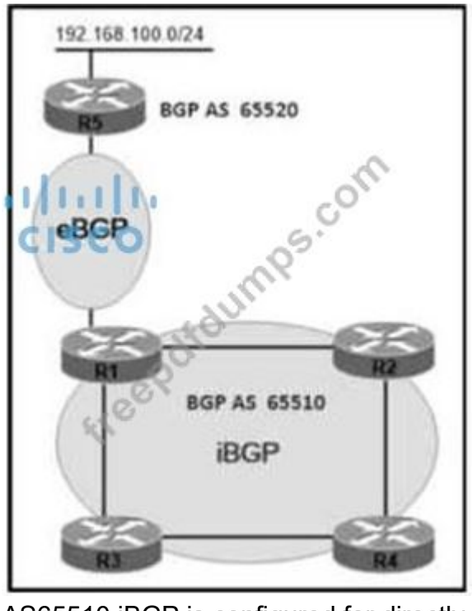
D. DMVPN

E. SSL VPN

Answer: (SHOW ANSWER)

NEW QUESTION: 10

Refer to the exhibit.



AS65510 iBGP is configured for directly connected neighbors. R4 cannot ping or traceroute network 192 168.100.0/24 Which action resolves this issue?

A. Configure R4 as a route reflector server and configure R2 and R3 as route reflector clients.

B. Configure R4 as a route reflector server and configure R1 as a route reflector client

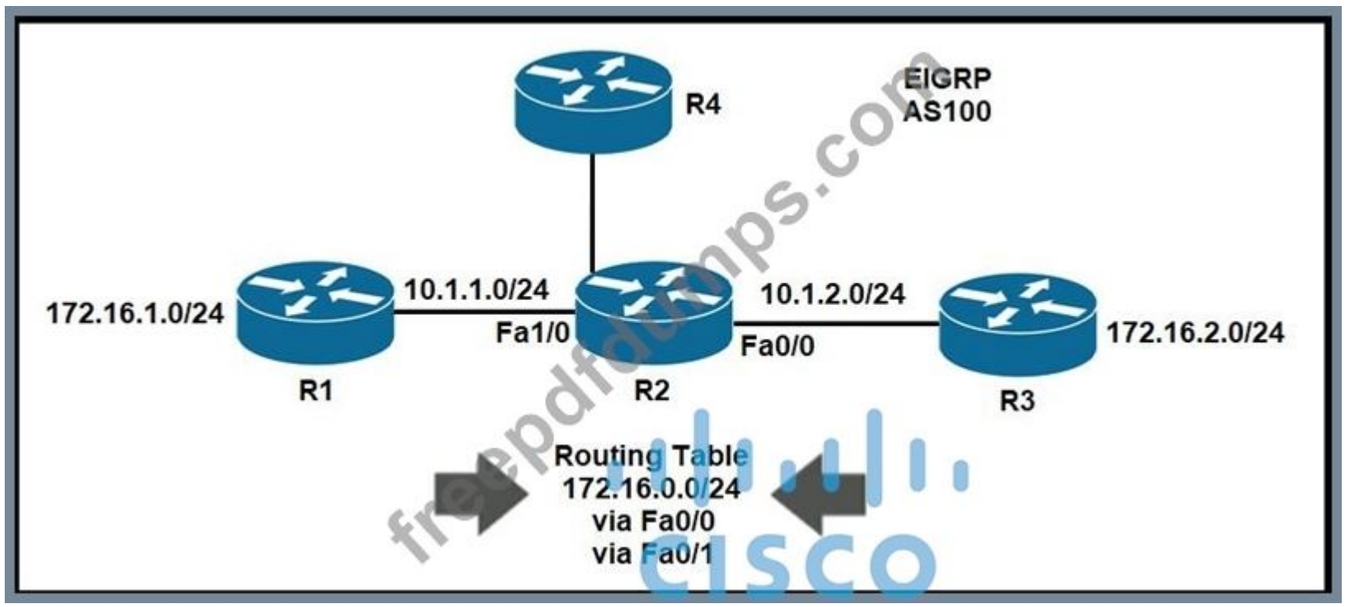
C. Configure R1 as a route reflector server and configure R4 as a route reflector client

D. Configure R1 as a route reflector server and configure R2 and R3 as route reflector clients

Answer: A (LEAVE A REPLY)

NEW QUESTION: 11

Refer to the exhibit.



R4 is experiencing packet drop when trying to reach 172.16.2.7 behind R2. Which action resolves the issue?

A. Insert a /16 floating static route on R2 toward R3 with metric 254

B. Enable auto summarization on all three routers R1, R2, and R3
C. Insert a /24 floating static route on R2 toward R3 with metric 254
D. Disable auto summarization on R2
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12
What are two functions of LDP? (Choose two.)
A. It is defined in RFC 3038 and 3039.
B. It requires MPLS Traffic Engineering.
C. It advertises labels per Forwarding Equivalence Class.
D. It must use Resource Reservation Protocol.
E. It uses Forwarding Equivalence Class
Answer: C,E (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/mpls/configuration/guide/mpls_cg/mp_mpls_overview.pdf

NEW QUESTION: 13
What does IPv6 Source Guard utilize to determine if IPv6 source addresses should be forwarded?
A. ACE
B. ACLS
C. DHCP
D. Binding Table
Answer: (SHOW ANSWER)

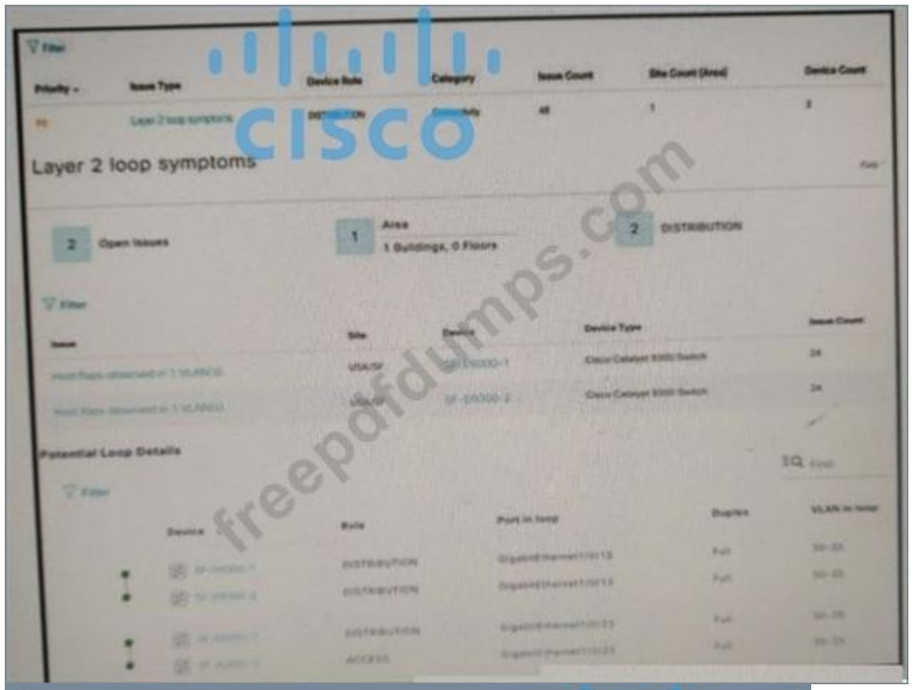
IPv6 source guard is an interface feature between the populated binding table and data traffic filtering. This feature enables the device to deny traffic when it is originated from an address that is not stored in the binding table. IPv6 source guard does not inspect ND or DHCP packets; rather, it works

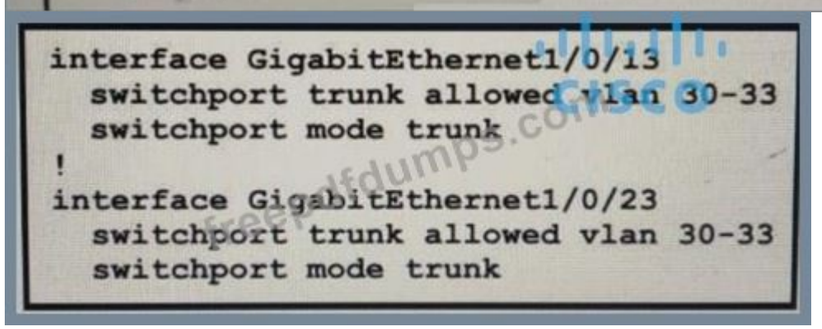
NEW QUESTION: 14
An engineer needs dynamic routing between two routers and is unable to establish OSPF adjacency. The output of the show ip ospf neighbor command shows that the neighbor state is EXSTART/EXCHANGE. Which action should be taken to resolve this issue?
A. match the passwords
B. match the hello timers
C. match the MTUs
D. match the network types
Answer: (SHOW ANSWER)

Neighbors Stuck in Exstart/Exchange State

The problem occurs most frequently when attempting to run OSPF between a Cisco router and another vendor's router. The problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces don't match. If the router with the higher MTU sends a packet larger that the MTU set on the neighboring router, the neighboring router ignores the packet.0 When

NEW QUESTION: 15
Refer to the exhibit.





An engineer identifier a Layer 2 loop using DNAC. Which command fixes the problem in the SF-D9300-1 switch?

A. no spanning-tree uplinkfast

B. spanning-tree loopguard default

C. spanning-tree backbonesfast

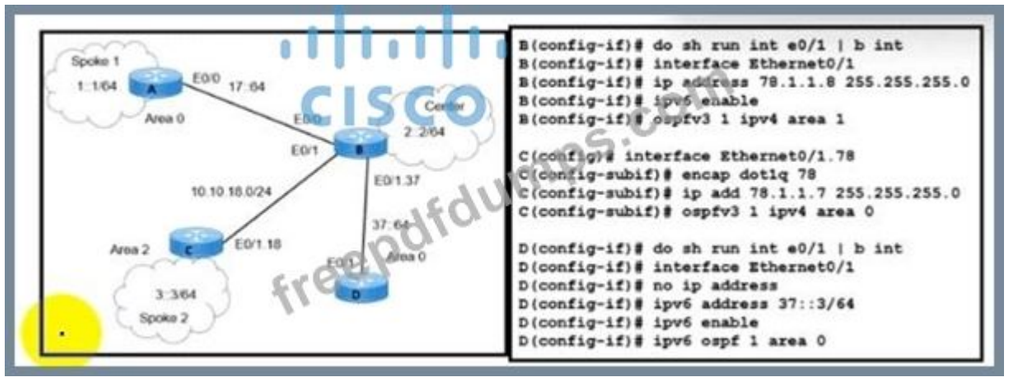
D. spanning-tree portfast bpduguard

Answer: D (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and management/dnacenter/tech_notes/b_dnac_sda_lan_automation_deployment.html

NEW QUESTION: 16

Refer to the exhibit.



Refer to the exhibit. A network engineer receives a report that Spoke 1 users can perform bank transactions with the server located at the Center site, but Spoke 2 users cannot. Which action resolves the issue?

A. Configure OSPFv2 on the routers B and C interfaces

B. Configure encapsulation dot1q 78 on the router C interface.

C. Configure IPv6 on the routers B and C interfaces

D. Configure the Spoke 2 users IP on the router B OSPF domain

Answer: (SHOW ANSWER)

NEW QUESTION: 17

Refer to the exhibit.

A network administrator is trying to access a branch router using TACACS+ username and password credentials, but the administrator cannot log in to the router because the WAN connectivity is down. The branch router has following AAA configuration:

```
aaa new-model
aaa authorization commands 15 default group tacacs+
aaa accounting commands 1 default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
tacacs-server host 10.100.50.99
tacacs-server key CiSco123
```

Which command will resolve this problem when WAN connectivity is down?

A. aaa authentication login console group tacacs+ enable

B. aaa authentication login default group tacacs+ console

C. aaa authentication login default group tacacs+ enable

D. aaa authentication login default group tacacs+ local

Answer: D (LEAVE A REPLY)

NEW QUESTION: 18

A CoPP policy is applied for receiving SSH traffic from the WAN interface on a Cisco ISR4321 router.

However, the SSH response from the router is abnormal and stuck during the high link utilization. The problem is identified as SSH traffic does not match in the ACL. Which action resolves the issue?

A. Rate-limit SSH traffic to ensure dedicated bandwidth.

B. Apply CoPP on the control plane interface.

C. Increase the IP precedence value of SSH traffic to 6.

D. Apply CoPP on the WAN interface inbound direction.

Answer: B (LEAVE A REPLY)

The problem is "SSH traffic does not match in the ACL" and "CoPP policy is applied for receiving SSH traffic from the WAN interface" so we should apply CoPP on the control plane interface instead.

NEW QUESTION: 19

The network administrator configured the router for Control Plane Policing to limit OSPF traffic to be policed to 1 Mbps. Any traffic that exceeds this limit must also be allowed at this point for traffic analysis. The router configuration is:

```
access-list 100 permit ospf any any
!
class-map CM-OSPF
match access-group 100
!
policy-map PM-COPP
class CM-OSPF
police 1000000 conform-action transmit
!
control-plane
service-policy output PM-COPP
```

The Control Plane Policing failed to monitor and police OSPF traffic. Which configuration resolves this issue?

```
no access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit ospf any any
access-list 101 permit tcp any any range 22 23
!
!
class-map CM-MGMT
 no match access-group 100
 match access-group 101
!
control-plane
 no service-policy output PM-COPP
 service-policy input PM-COPP
```

```
No access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit tcp any any range eq 22
access-list 100 permit tcp any any range eq 23
access-list 100 permit ospf any any
!
control-plane
 no service-policy output PM-COPP
 service-policy input PM-COPP
```

```
no access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit ospf any any
access-list 101 permit tcp any any range 22 23
!
!
class-map CM-MGMT
 no match access-group 100
 match access-group 101
```

A. Option D

B. Option C

C. Option B

D. Option A

Answer: D (LEAVE A REPLY)

NEW QUESTION: 20

Refer to Exhibit.

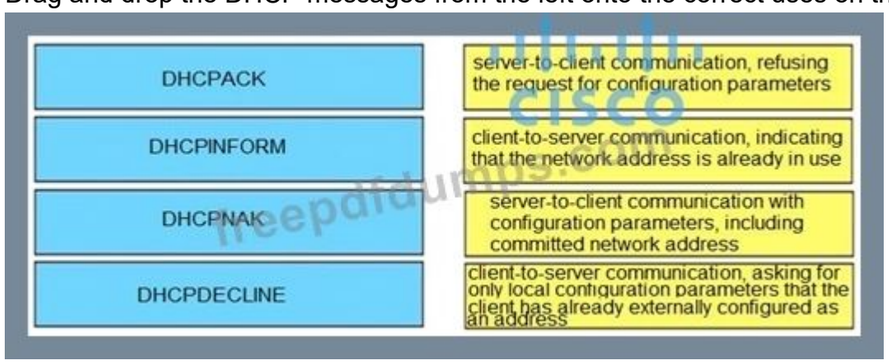
A network administrator added one router in the Cisco DNA Center and checked its discovery and health from the Network Health Dashboard. The network administrator observed that the router is still showing up as unmonitored. What must be configured on the router to mount it in the Cisco DNA Center?

A. Configure router with NetFlow data
B. Configure router with the telemetry data
C. Configure router with routing to reach Cisco DNA Center
D. Configure router with SNMPv2c or SNMPv3 traps
Answer: (SHOW ANSWER)
Unmonitored: Unmonitored devices are devices for which Assurance did not receive any telemetry data during the specified time range.

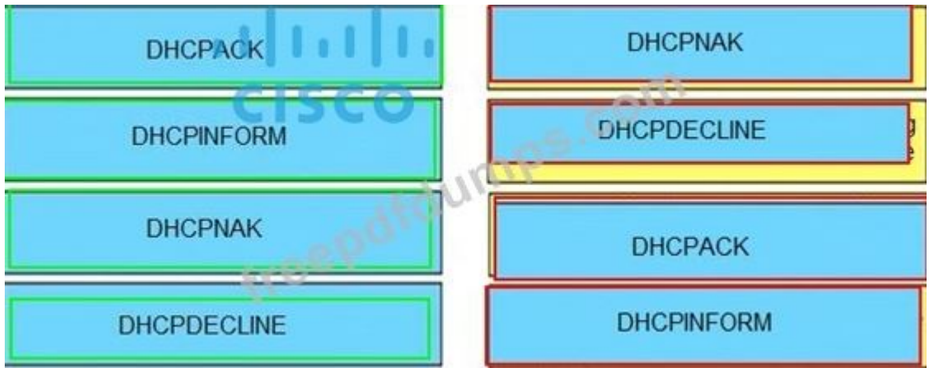
NEW QUESTION: 21
Refer to the exhibit.

An IT staff member comes into the office during normal office hours and cannot access devices through SSH Which action should be taken to resolve this issue?
A. Modify the access list to use the correct IP address.
B. Configure the correct time range.
C. Modify the access list to correct the subnet mask
D. Configure the access list in the outbound direction.
Answer: (SHOW ANSWER)
To ACL should be permit tcp 101 10.1.1.1 0.0.0.0

NEW QUESTION: 22
Drag and drop the DHCP messages from the left onto the correct uses on the right.



Answer:



NEW QUESTION: 23
Which statement about MPLS LDP router ID is true?
A. If not configured, the operational physical interface is chosen as the router ID even if a loopback is configured.
B. The MPLS LDP router ID must match the IGP router ID.
C. The force keyword changes the router ID to the specified address without causing any impact.
D. The loopback with the highest IP address is selected as the router ID.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
Refer to the exhibit.

```
enable secret 5 <password>
username cisco privilege 15 secret 5 <password>
username operator password 7 <password>
line vty 0 4
session-timeout 240
password 7 <password>
transport input telnet
```

Refer to the exhibit. The authentication is not working as desired and the user drops into user-exec mode. Which configuration resolves the issue?

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
!
line vty 0 4
 login authentication default
 authorization exec default
```

```
aaa new-model
aaa authentication login default local
aaa authorization priv default 15
!
line vty 0 4
 login authentication default
 authorization exec priv15
```

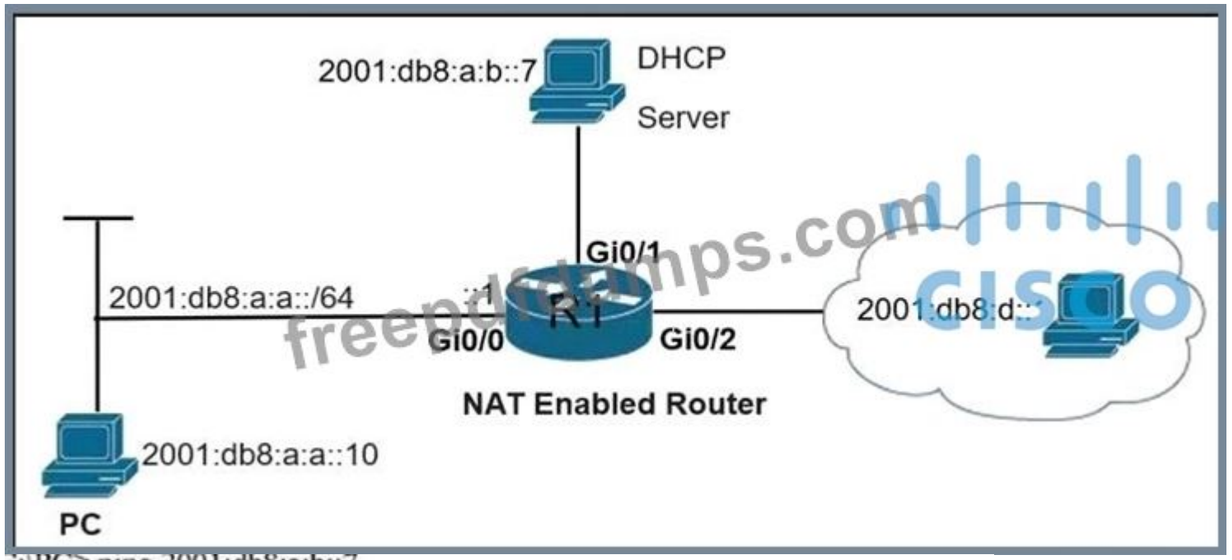
```
aaa new-model
aaa authentication login local
aaa authorization exec local
!
line vty 0 4
 login authentication local
 authorization exec default
```

```
aaa new-model
aaa authentication common-id default local
aaa authorization exec default local
!
line vty 0 4
 login authentication default
 authorization exec default
```

A. Option D
B. Option A

C. Option C
D. Option B
Answer: C (LEAVE A REPLY)

NEW QUESTION: 25
Refer to the exhibit.




```
C:\PC> ping 2001:db8:a:b::7

Pinging 2001:db8:a:b::7 with 32 bytes of data:
Reply from 2001:db8:a:b::7: time=46ms
Reply from 2001:db8:a:b::7: time=40ms
Reply from 2001:db8:a:b::7: time=40ms
Reply from 2001:db8:a:b::7: time=40ms
Ping statistics for 2001:db8:a:b::7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 40ms, Maximum = 46ms, Average = 41ms

R1# telnet 2001:db8:a:b::7
Trying 2001:DB8:A:B::7 ... Open
User Access Verification
Password:

R1# show ipv6 access-list TSHOOT
IPv6 access list TSHOOT
deny tcp any host 2001:DB8:A:B::7 eq telnet (6 matches) sequence 10
permit tcp host 2001:DB8:A:A::10 host 2001:DB8:A:B::7 eq telnet sequence 20
permit tcp host 2001:DB8:A:A::10 host 2001:DB8:D::1 eq www sequence 30
permit ipv6 2001:DB8:A:A::/64 any (67 matches) sequence 40
```

An engineer is troubleshooting a failed Telnet session from PC to the DHCP server. Which action resolves the issue?

A. Remove sequence 30 and add it back to the IPv6 traffic filter as sequence 5.

B. Remove sequence 10 to add the PC source IP address and add it back as sequence 10.

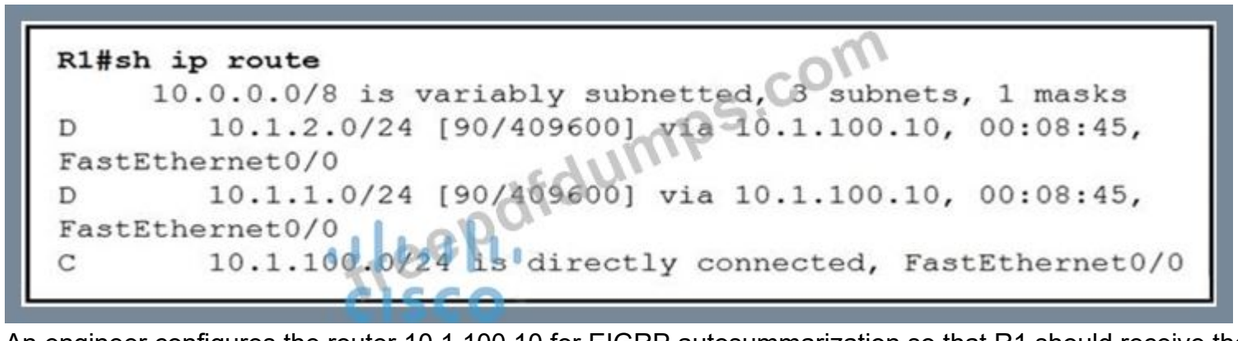
C. Remove sequence 20 and add it back to the IPv6 traffic filter as sequence 5.

D. Remove sequence 20 for sequence 40 in the access list to allow Telnet.

Answer: (SHOW ANSWER)

NEW QUESTION: 26

Refer to the exhibit.



An engineer configures the router 10.1.100.10 for EIGRP autosummarization so that R1 should receive the summary route of 10.0.0.0/8. However, R1 receives more specific /24 routes.

Which action resolves this issue?

A. Router 10.1.100.10 should configure ip route 10.0.0.0 255.0.0.0 null 0 for the routes that are summarized toward R1.

B. Router R1 should configure ip route 10.0.0.0 255.0.0.0 null 0 for the routes that are received on R1.

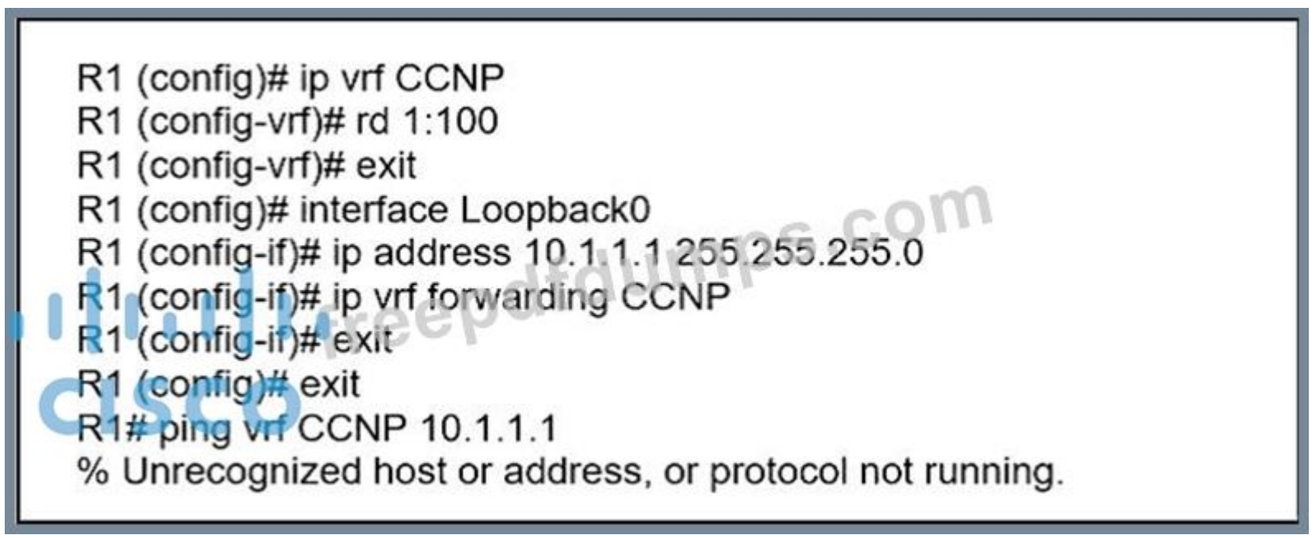
C. Router 10.1.100.10 should configure ip summary address eigrp (AS number) 10.0.0.0 255.0.0.0 for the R1 Fast Ethernet 0/0 connected interface.

D. Router R1 should configure ip summary address eigrp (AS number) 10.0.0.0 255.0.0.0 for the R1 Fast Ethernet 0/0 connected interface.

Answer: C (LEAVE A REPLY)

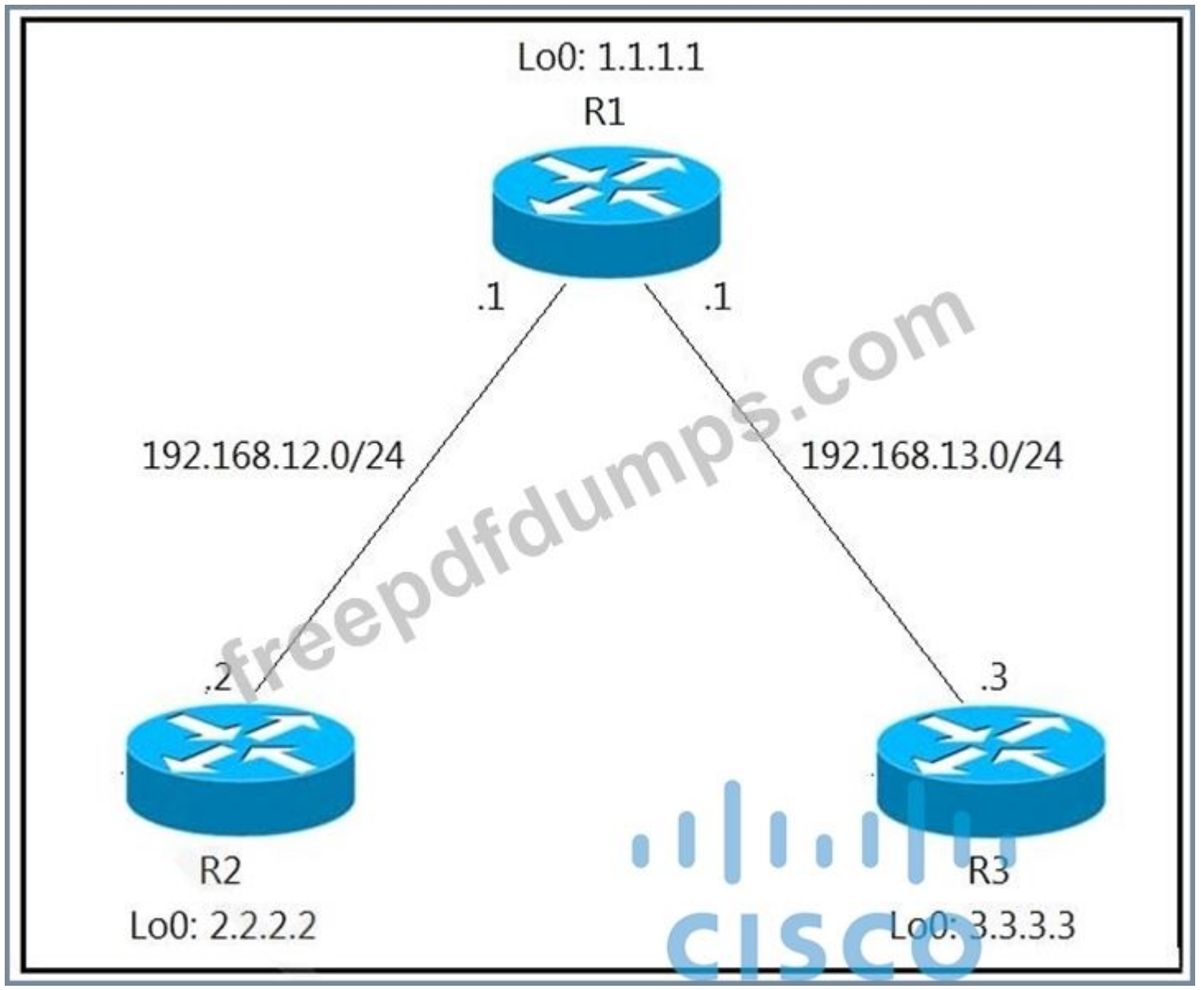
NEW QUESTION: 27

Refer to the exhibit.



Which command must be configured to make VRF CCNP work?
A. interface Loopback0
vrf forwarding CCNP
B. interface Loopback0
ip address 10.1.1.1 255.255.255.0
C. interface Loopback0
ip address 10.1.1.1 255.255.255.0
vrf forwarding CCNP
D. interface Loopback0
ip address 10.1.1.1 255.255.255.0
ip vrf forwarding CCNP
Answer: B (LEAVE A REPLY)
From the exhibit, we learn that the command "ip address 10.1.1.1 255.255.255.0" has been issued before the command "ip vrf forwarding CCNP". But the second command removed the IP address configured in the first command so we have to retype the IP address command.

NEW QUESTION: 28
Refer to the exhibit.



An engineer has configured R1 as EIGRP stub router. After the configuration, router R3 failed to reach to R2 loopback address.

Which action advertises R2 loopback back into the R3 routing table?

A. Add a static route for R2 loopback address in R1 and redistribute it to advertise to R3.

B. Use a leak map on R1 that matches the required prefix and apply it with the distribute list command toward R3.

C. Use a leak map on R3 that matches the required prefix and apply it with the EIGRP stub feature.

D. Add a static null route for R2 loopback address in R1 and redistribute it to advertise to R3.

Answer: (SHOW ANSWER)

The EIGRP stub feature is useful to prevent unnecessary EIGRP queries and to filter some routes that you advertise. What if you want to configure your router as a stub router but still make an exception to some routes that it advertises? That is possible with the leak-map feature. This is how to configure leak-map in this question:

R1

(config)#ip access-list standard R2_L0

R1(config-std-nacl)#permit host 2.2.2.2

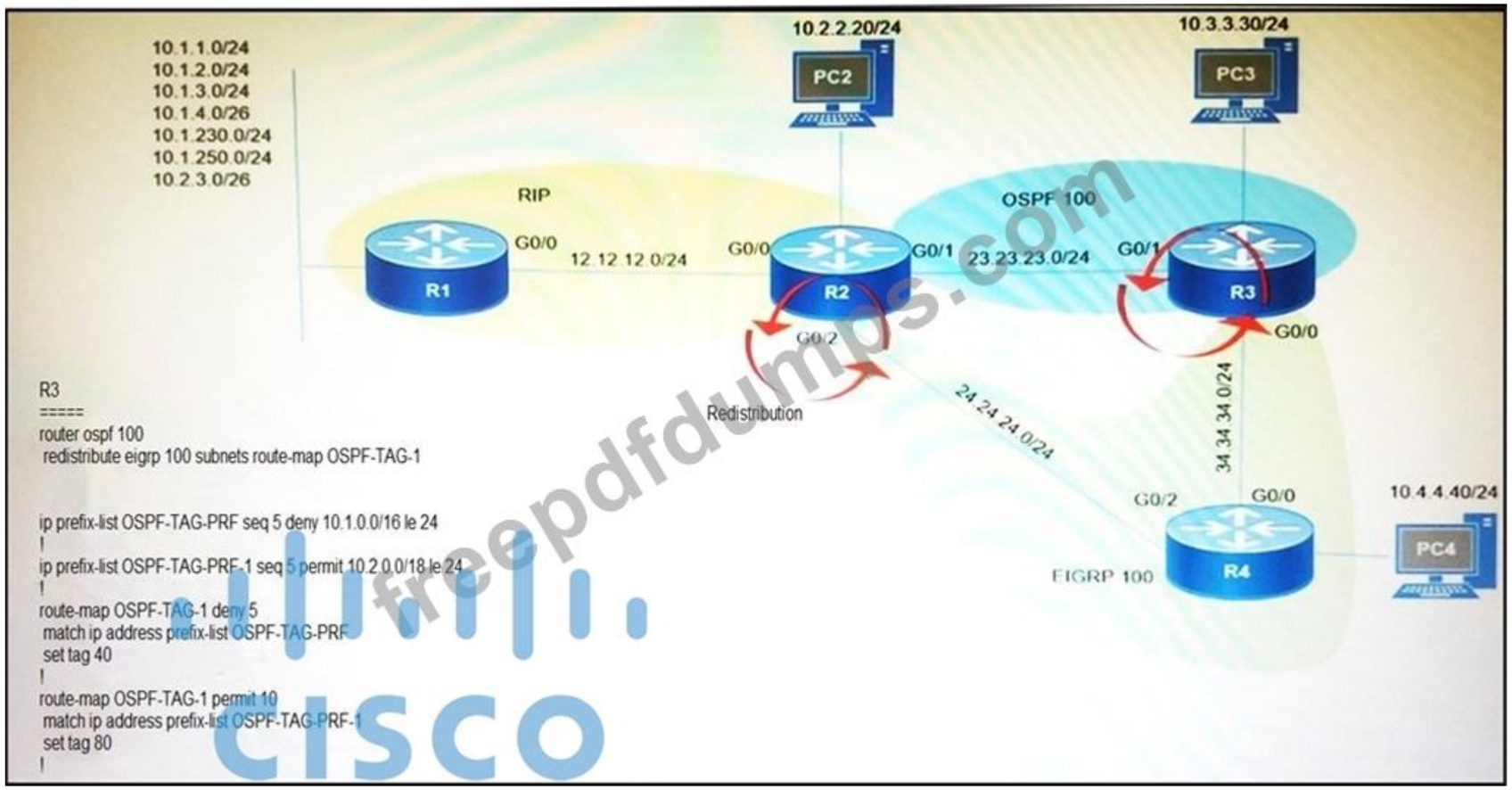
R1(config)#route-map R2_L0_LEAK

R2(config-route-map)#match ip address R2_L0

R1(config)#router eigrp 1

R1(config-router)#eigrp stub leak-map R2_L0_LEAK

NEW QUESTION: 29
Refer to the exhibit.



Which subnet is redistributed from EIGRP to OSPF routing protocols?

A. 10.2.3.0/26

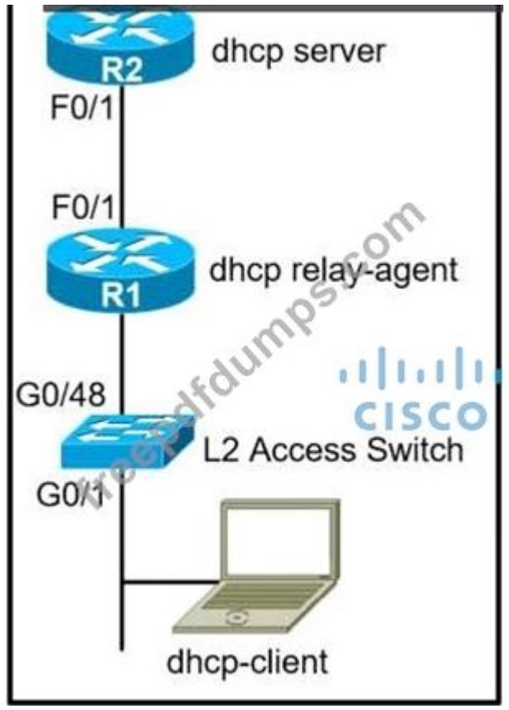
B. 10.2.2.0/24

C. 10.1.4.0/26

D. 10.1.2.0/24

Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
Refer to the exhibit.



The network administrator can see the DHCP discovery packet in R1. but R2 is not replying to the DHCP request. The R1 related interface is configured with the DHCP helper address. If the PC is directly connected to the FaO/1 interface on R2, the DHCP server assigns as IP address from the DHCP pool to the PC. Which two commands resolve this issue? (Choose two.)

A. service dhcp command on R1

B. service dhcp-relay command on R1

C. ip dhcp option 82 command on R2

D. ip dhcp relay information enable command on R1

E. ip dhcp relay information trust-all command on R2

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 31

Which mechanism provides traffic segmentation within a DMVPN network?

A. RSVP

B. BGP

C. MPLS

D. iPsec

Answer: C (LEAVE A REPLY)

To use the DMPVN - Traffic Segmentation Within DMVPN feature you must configure Multiprotocol Label Switching (MPLS) by using the mpls ip command.

Reference:

16/sec-conn-dmvpn-xe-16-book/sec-conn-dmvpn-dmvpn.html

NEW QUESTION: 32
Which security feature can protect DMVPN tunnels?
A. RADIUS
B. TACACS+
C. RTBH
D. IPsec
Answer: D (LEAVE A REPLY)

NEW QUESTION: 33
Which command allows traffic to load-balance in an MPLS Layer 3 VPN configuration?
A. multi-paths eibgp 2
B. multi-paths 2
C. maximum-paths 2
D. Maximum-paths ibgp 2
Answer: D (LEAVE A REPLY)

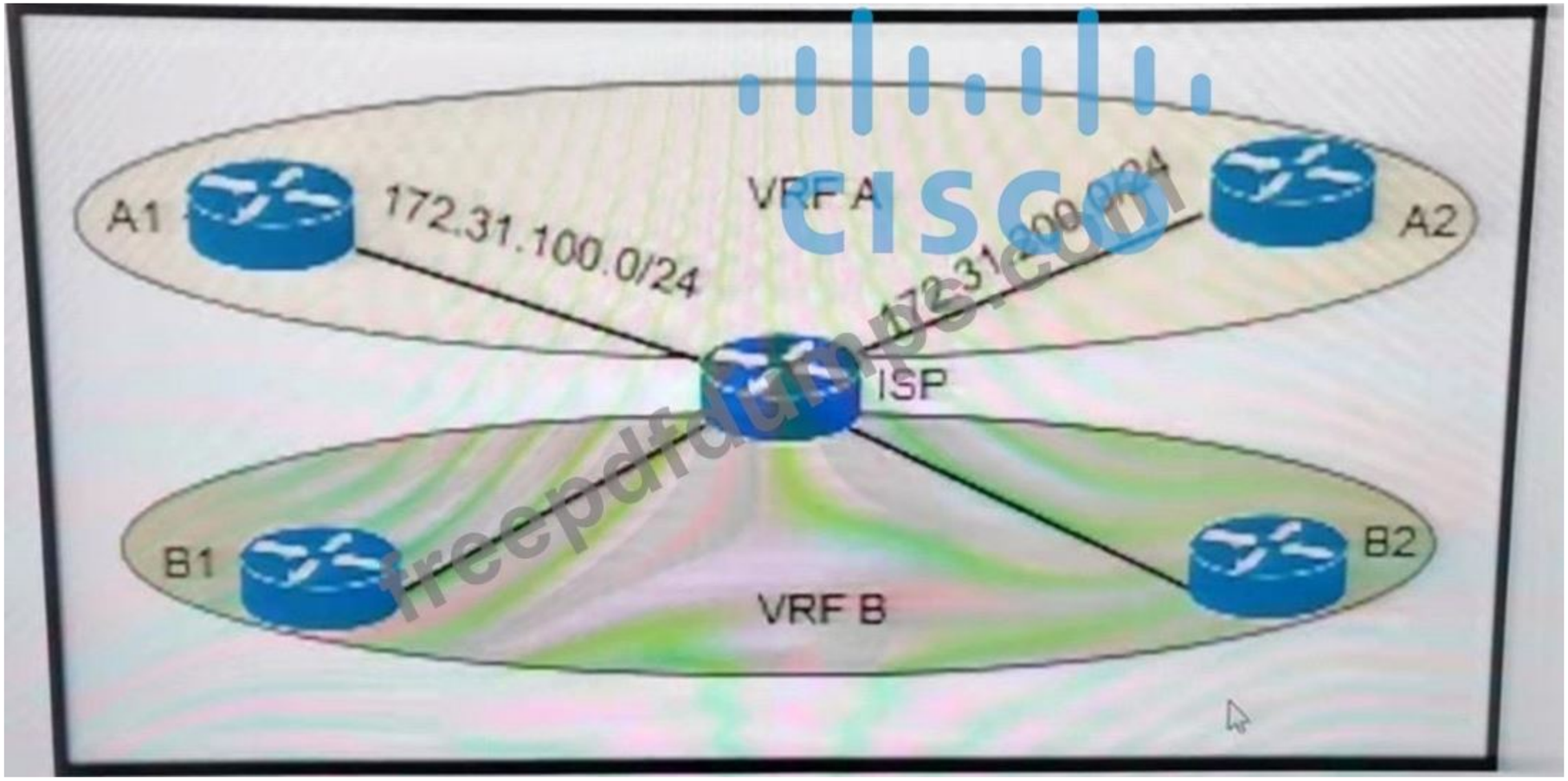
NEW QUESTION: 34
An engineer configured policy-based routing for a destination IP address that does not exist in the routing table. How is the packet treated through the policy for configuring the set ip default next-hop command?
A. Packets are not forwarded to the specific next hop.
B. Packets are forwarded based on the routing table.
C. Packets are forwarded based on a static route.
D. Packets are forwarded to the specific next hop.
Answer: (SHOW ANSWER)
The set ip default next-hop command verifies the existence of the destination IP address in the routing table, and...+ if the destination IP address exists, the command does not policy route the packet, but forwards the packet based on the routing table.+ if the destination IP address does not exist, the command policy routes the packet by sending it to the specified next hop.

NEW QUESTION: 35
A customer reports that traffic is not passing on an EIGRP enabled multipoint interface on a router configured as below:
interface Serial0/0
no ip address
interface Server0/0/0.9 multipoint
ip address 10.1.1.1 255.255.255.248
ip split-horizon eigrp 1
Which action resolves the issue?
A. Enable split horizon

B. Disable split horizon
C. Enable poison reverse
D. Disable poison reverse
Answer: (SHOW ANSWER)

NEW QUESTION: 36
What is a function of IPv6 Source Guard?
A. It works with address glean or ND to find existing addresses.
B. It inspects ND and DHCP packets to build an address binding table.
C. It denies traffic from known sources and allocated addresses.
D. It notifies the ND protocol to inform hosts if the traffic is denied by it.
Answer: A (LEAVE A REPLY)
IPv6 source guard is an interface feature between the populated binding table and data traffic filtering. This feature enables the device to deny traffic when it is originated from an address that is not stored in the binding table. IPv6 source guard does not inspect ND or DHCP packets;rather, it works in conjunction with IPv6 neighbor discovery (ND) inspection or IPv6 address glean, both of which detect existing addresses on the link and store them into the binding table.

NEW QUESTION: 37
Refer to the exhibit. The ISP router is fully configured for customer A and customer B using the VRF-Lite feature. What is the minimum configuration required for customer A to communicate between routers A1 and A2?



A. A1
interface fa0/0
description To->ISP
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.100.1 0.0.0.255 area 0
A2
interface fa0/0
description To->ISP
ip add 172.31.200.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.200.1 0.0.0.255 area 0
B. A1
interface fa0/0

description To->ISP
ip vrf forwarding A
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.100.1 0.0.0.255 area 0
A2
interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.200.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.200.1 0.0.0.255 area 0
C. A1
interface fa0/0
description To->ISP
ip add 172.31.200.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.200.1 0.0.0.255 area 0
A2
interface fa0/0
description To->ISP
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.100.1 0.0.0.255 area 0
D. A1
interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100 vrf A
net 172.31.200.1 0.0.0.255 area 0

A2
interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100 vrf A
net 172.31.200.1 0.0.0.255 area 0
Answer: C (LEAVE A REPLY)
A1 and A2 routers do not know they belong to VRF A.
The two interfaces of ISP (which are connected to A1 & A2) should be configured like this (we only show the configure of one interface):
ISP router:
interface g0/0
description ISP->To_CustomerA
ip vrf forwarding A
ip address 172.31.100.2 255.255.255.0
router ospf 100 vrf A
network 172.31.200.2 0.0.0.255 area 0

NEW QUESTION: 38
Refer to the exhibit.

```
Router# show ip route

     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Ethernet0/0
C    3.0.0.0/8 is directly connected, Serial1/0
O E2 200.1.1.0/24 [110/20] via 2.2.2.2, 00:16:17, Ethernet0/0
O E1 200.2.2.0/24 [110/104] via 2.2.2.2, 00:00:41, Ethernet0/0
     131.108.0.0/24 is subnetted, 2 subnets
O       131.108.2.0 [110/74] via 2.2.2.2, 00:16:17, Ethernet0/0
O IA    131.108.1.0 [110/84] via 2.2.2.2, 00:16:17, Ethernet0/0

Router# show ip bgp

  Network          Next Hop            Metric LocPrf Weight Path
*> 2.2.2.0/24      0.0.0.0                  0         32768 ?
*> 131.108.1.0/24  2.2.2.2                 84         32768 ?
*> 131.108.2.0/24  2.2.2.2                 74         32768 ?
```

The OSPF routing protocol is redistributed into the BGP routing protocol, but not all the OSPF routes are distributed into BGP Which action resolves the issue?
A. Include the word external in the redistribute command
B. Use a route-map command to redistribute OSPF external routes defined in an access list
C. Include the word internal external in the redistribute command

D. Use a route-map command to redistribute OSPF external routes defined in a prefix list.

Answer: C (LEAVE A REPLY)

If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and inter-area routes are redistributed into BGP, by default. You can use the internal keyword along with the redistribute command under router bgp to redistribute OSPF intra- and inter-area routes.

Use the external keyword along with the redistribute command under router bgp to redistribute OSPF external routes into BGP.

-> In order to redistribute all OSPF routes into BGP, we must use both internal and external keywords. The full command would be (suppose we are using OSPF 1):

redistribute ospf 1 match internal external

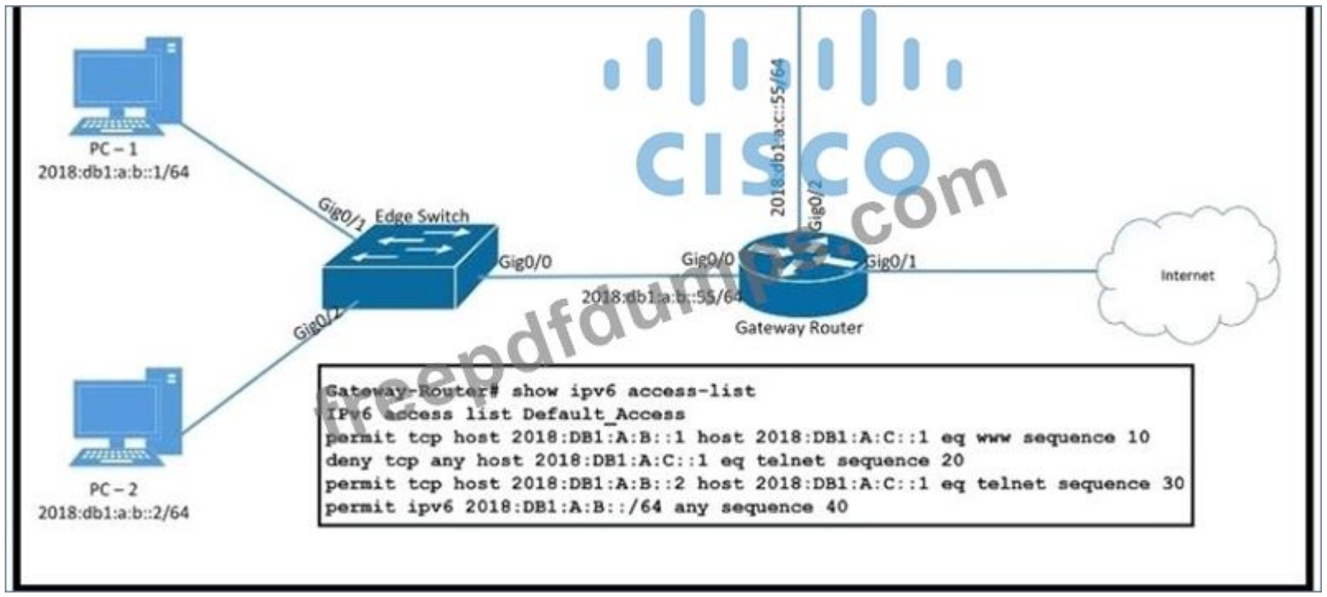
Note: The configuration shows match internal external 1 external 2. This is normal because OSPF automatically appends "external 1 external 2" in the configuration. In other words, keyword external = external 1 external 2. External 1 = O E1 and External 2 = O E2.

Reference:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5242-bgp-ospf-redi s.html

NEW QUESTION: 39

Refer to the exhibit.



PC-2 failed to establish a Telnet connection to the terminal server Which configuration resolves the issue?

A. Option A

B. Option B

C. Option C

D. Option D
Answer: A (LEAVE A REPLY)
In fact in this question both answer A and answer C are correct but we believe answer A is the better choice as it only allows PC-2 to telnet to terminal server. All other hosts are refused to telnet to terminal server via sequence 20.

NEW QUESTION: 40
Refer to the exhibit.

An engineer is trying to add an encrypted user password that should not be visible in the router configuration. Which two configuration commands resolve the issue? (Choose two)
A. username Admin secret Cisco@maedeh motamedi
B. no service password-encryption
C. service password-encryption
D. username Admin password 5 Cisco@maedeh motamedi
E. username Admin password Cisco@maedeh motamedi
F. password encryption aes
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 41

Refer to the exhibit.

```
aaa new-model
aaa group server radius RADIUS-SERVERS
aaa authentication login default group RADIUS-SERVERS local
aaa authentication enable default group RADIUS-SERVERS enable
aaa authorization exec default group RADIUS-SERVERS if-authenticated
aaa authorization network default group RADIUS-SERVERS if-authenticated
aaa accounting send stop-record authentication failure
aaa session-id common
!
line con 0
logging synchronous
stopbits 1
line vty 0 4
logging synchronous
transport input ssh
```


A network administrator successfully logs in to a switch using SSH from a (RADIUS server When the network administrator uses a console port to access the switch the RADIUS server returns shell:priv-lvl=15" and the switch asks to enter the enable command \ the command is entered, it gets rejected. Which command set is used to troubleshoot and reserve this issue?

A. line con 0
aaa authorization console priv15
!
line vty 0 4
authorization exec

B. line con 0
aaa authorization console
!
line vty 0 4
authorization exec

C. line con 0
aaa authorization console
authorization exec
!
line vty 0 4
transport input ssh

D. line con 0
aaa authorization console
authorization priv15
!
line vty 0 4

transport input ssh
Answer: C (LEAVE A REPLY)

NEW QUESTION: 42
Refer to the exhibit.

```
!-- ACL for CoPP Routing class-map
!
access-list 120 permit tcp any gt 1024 eq bgp log
access-list 120 permit tcp any bgp gt 1024 established
access-list 120 permit tcp any gt 1024 eq 639
access-list 120 permit tcp any eq 639 gt 1024 established
access-list 120 permit tcp any eq 646
access-list 120 permit udp any eq 646
access-list 120 permit ospf any
access-list 120 permit ospf any host 224.0.0.5
access-list 120 permit ospf any host 224.0.0.6
access-list 120 permit eigrp any
access-list 120 permit eigrp any host 224.0.0.10
access-list 120 permit udp any any eq pim-auto-rp
```

The control plane is heavily impacted after the CoPP configuration is applied to the router. Which command removal lessens the impact on the control plane?

A. access-list 120 permit ospf any
B. access-list 120 permit udp any any eq pim-auto-rp
C. access-list 120 permit tcp any gt 1024 eq bgp log
D. access-list 120 permit eigrp any host 224.0.0.10
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
Refer to the exhibit.

```
BRANCH-RTR#

router eigrp 100
 network 10.4.31.0 0.0.0.7
 network 10.100.100.1 0.0.0.0
 distribute-list route-map FILTER-IN in FastEthernet0/0
 eigrp router-id 10.100.100.1
!
ip prefix-list 102 seq 10 permit 10.1.1.100/32
!
route-map FILTER-IN deny 10
 match ip address prefix-list 102
!
```

A junior engineer updated a branch router configuration. Immediately after the change, the engineer receives calls from the help desk that branch personnel cannot reach any network destinations.
Which configuration restores service and continues to block 10.1.1.100/32?

A. route-map FILTER-IN deny 5

B. ip prefix-list 102 seq 15 permit 0.0.0.0/32 le 32

C. ip prefix-list 102 seq 5 permit 0.0.0.0/32 le 32

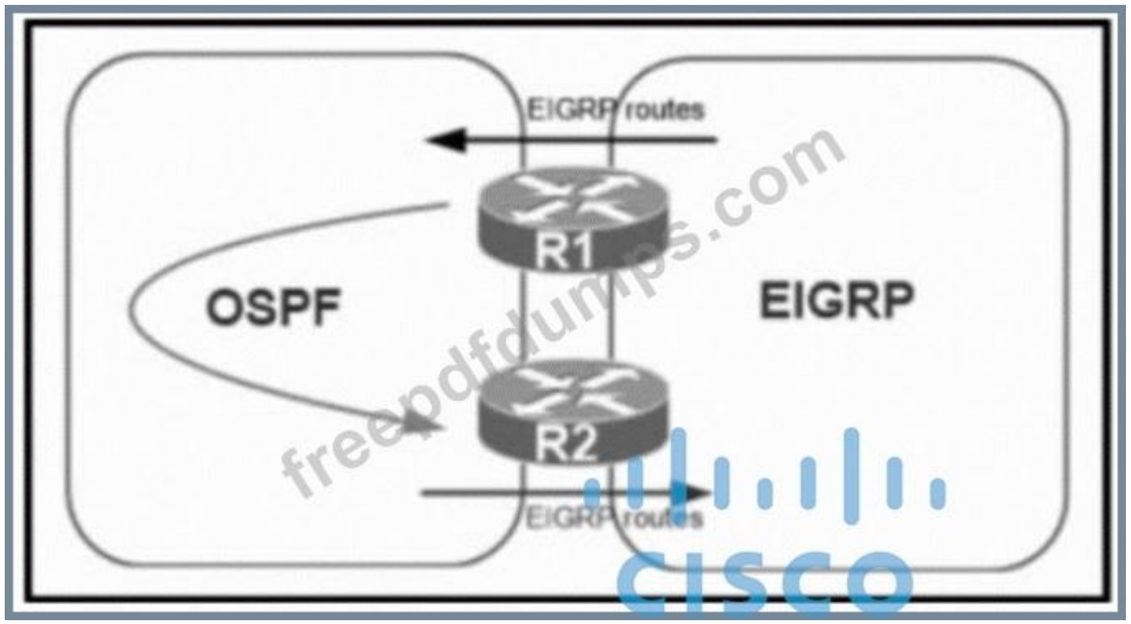
D. route-map FILTER-IN permit 20

Answer: D (LEAVE A REPLY)

By using "deny" keyword in a route-map, we can filter out the prefix specified in the prefix-list.
But there is an implicit "deny all" statement in the prefix-list so we must permit other prefixes with "permit" keyword in the route-map.

NEW QUESTION: 44

Refer to the exhibit.



Refer to the exhibit. A network administrator configured mutual redistribution on R1 and R2 routers, which caused instability in the network. Which action resolves the issue?

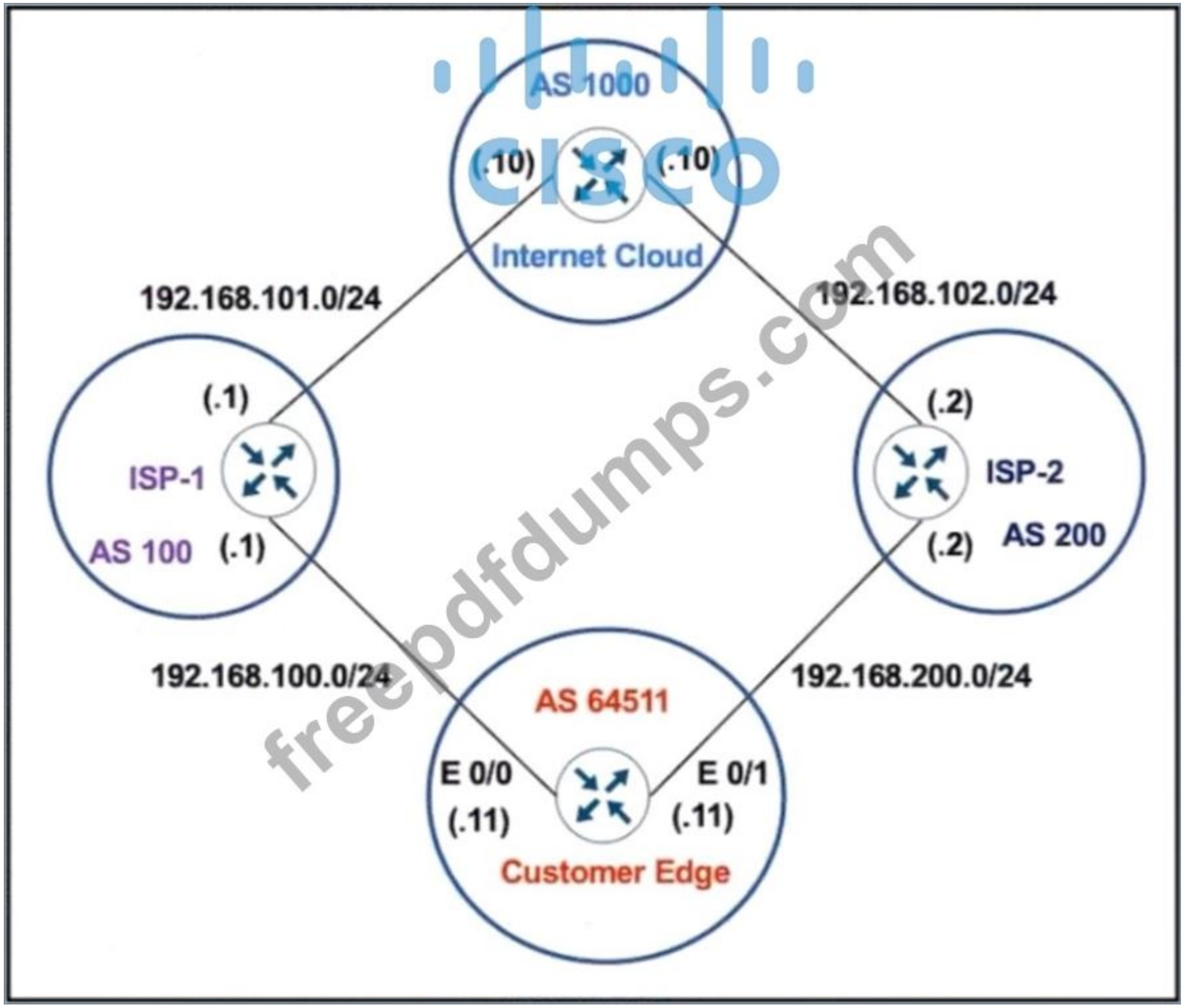
A. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag on R2 to deny when redistributing OSPF into EIGRP.

B. Apply a prefix list of EIGRP network routes in OSPF domain on R1 to propagate back into the EIGRP routing domain.

C. Advertise summary routes of EIGRP to OSPF and deny specific EIGRP routes when redistributing into OSPF.
D. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag on R2 to allow when redistributing OSPF into EIGRP.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 45
Refer to the exhibit.
A network engineer receives a fault ticket about traffic drops from BANK SITE to BANK Users can reach BANK SITE Y from router RA as a source.
Routers RB and RD are acting as route reflectors.
Which configuration resolves the issue?
A. RC(config)#router bgp 65201
RC(config-router)#neighbor 10.10.10.4 route-reflector-client
B. RB(config)router bgp 65201
RB(config-router)#neighbor 10.10.10.3 route-reflector-client
C. RF(config)#router bgp 65201
RF(config-router)#neighbor 10.10.10.6 route-reflector-client
D. RC(config)#router bgp 65201
RC(config-router)#neighbor 10.10.10.2 route-reflector-client
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Refer to the exhibit.



The network administrator has configured the Customer Edge router (AS 64511) to send only summarized routes toward ISP-1 (AS 100) and ISP-2 (AS 200).

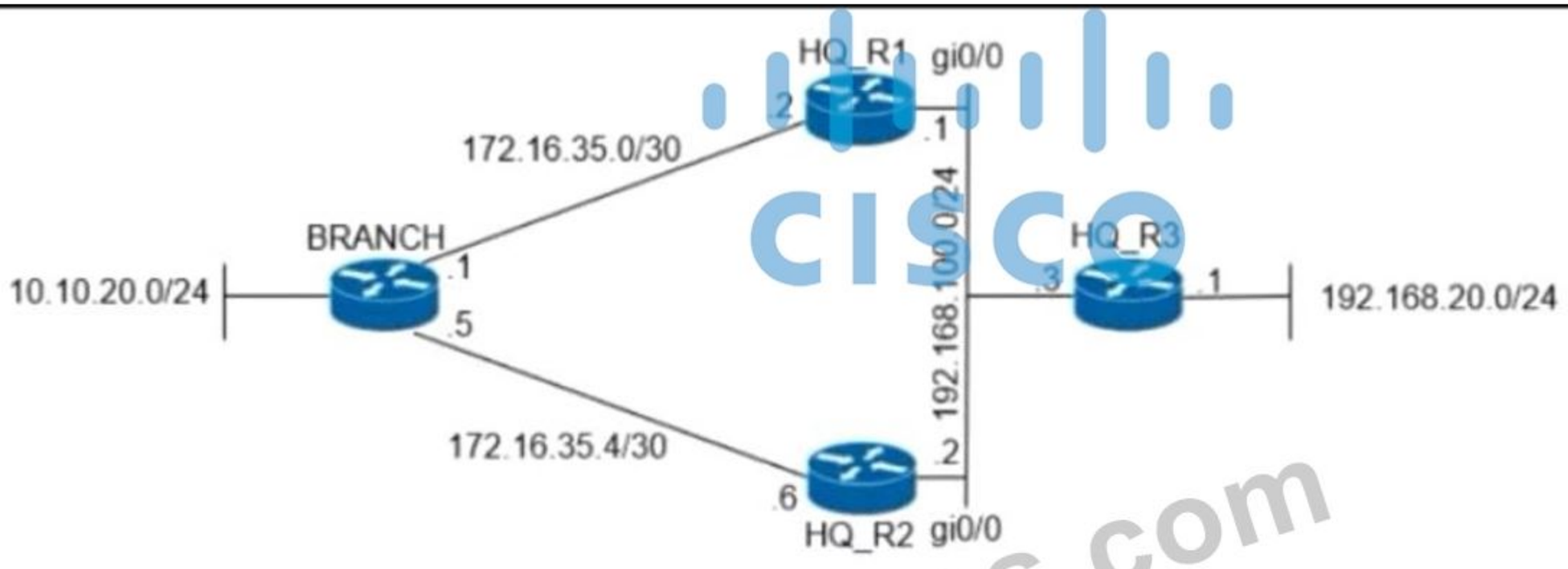
router bgp 64511
network 172.16.20.0 mask 255.255.255.0
network 172.16.21.0 mask 255.255.255.0
network 172.16.22.0 mask 255.255.255.0
network 172.16.23.0 mask 255.255.255.0
aggregate-address 172.16.20.0 255.255.252.0

After this configuration. ISP-1 and ISP-2 continue to receive the specific routes and the summary route. Which configuration resolves the issue?

A. router bgp 64511

aggregate-address 172.16.20.0 255.255.252.0 summary-only
B. router bgp 64511
neighbor 192.168.100.1 summary-only
neighbor 192.168.200.2 summary-only
C. interface E 0/0
ip bgp suppress-map BLOCK_SPECIFIC
!
interface E 0/1
ip bgp suppress-map BLOCK_SPECIFIC
!
ip prefix-list PL_BLOCK_SPECIFIC permit 172.16.20.0/22 ge 24
!
route-map BLOCK_SPECIFIC permit 10
match ip address prefix-list PL_BLOCK_SPECIFIC
D. ip prefix-list PL_BLOCK_SPECIFIC deny 172.16.20.0/22 ge 22
ip prefix-list PL BLOCK SPECIFIC permit 172.16.20.0/22
!
route-map BLOCK_SPECIFIC permit 10
match ip address prefix-list PL_BLOCK_SPECIFIC
!
router bgp 64511
aggregate-address 172.16.20.0 255 255.252.0 suppress-map BLOCKSPECIFIC
Answer: A (LEAVE A REPLY)
When the aggregate-address command is used within BGP routing, the aggregated address is advertised, along with the more specific routes. The exception to this rule is through the use of the summary-only command. The "summary-only" keyword suppresses the more specific routes and announces only the summarized route.

NEW QUESTION: 47
Refer to the exhibit.




```
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.2 track 1
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.6 5
!
BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 172.16.35.2
BRANCH(config-ip-sla)# timeout 200
BRANCH(config-ip-sla)# frequency 5
!
BRANCH(config)# ip sla schedule 1 life forever start-time now
!
BRANCH(config)# track 1 ip sla 1 reachability
```


An engineer has successfully set up a floating static route from the BRANCH router to the HQ network using HQ_R1 as the primary default gateway When the g0/0 goes down on HQ_R1, the branch network cannot reach the HQ network 192.168.20.0/24. Which set of configurations resolves the issue?

A. BRANCH(config)# ip sla 1

BRANCH(config-ip-sla)# icmp-echo 192.168.100.2
B. BRANCH(config)# Ip sla 1
BRANCH(config-ip-sta)# Icmp-echo 192.168.100.1
C. HQ R3(config)# Ip sla responder
HQ R3(config)# Ip sla responder Icmp-echo 172.16.35.5
D. HQ_R3(config)# ip sla responder
HQ_R3(config)# ip sla responder icmp-echo 172.16.35.1
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
Refer to the exhibit.

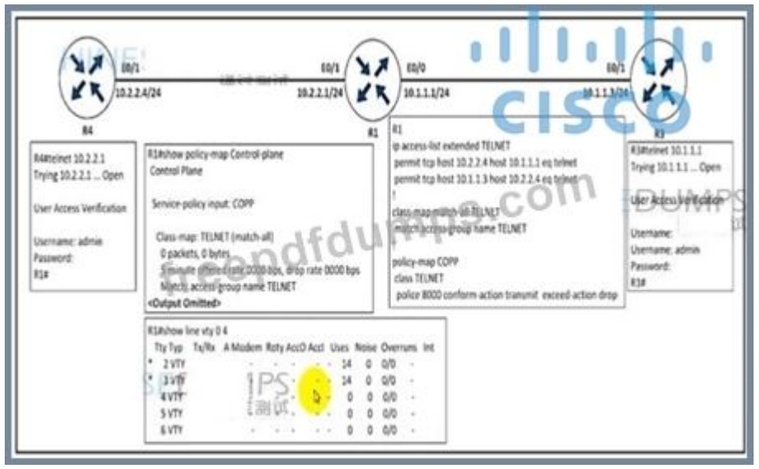
```
R1#show policy-map control-plane
 Control Plane

      Service-policy output:  CoPP

       Class-map: SNMP-Out (match-all)
         124 packets, 3693 bytes
         5 minute offered rate 0000 bps, drop rate 0000 bps
         Match: access-group name SNMP
         police:
             cir 8000 bps, bc 1500 bytes
           conformed 0 packets, 0 bytes; actions:
             transmit
           exceeded 0 packets, 0 bytes; actions:
             drop
           conformed 0000 bps, exceeded 0000 bps

       Class-map: class-default (match-any)
         10 packets, 1003 bytes
         5 minute offered rate 0000 bps, drop rate 0000 bps
         Match: any
R1#show ip access-list SNMP
Extended IP access list SNMP
        10 permit udp any eq snmp any
```

R1 is being monitored using SNMP and monitoring devices are getting only partial information. What action should be taken to resolve this issue?
A. Modify the CoPP policy to increase the configured CIR limit for SNMP.
B. Modify the CoPP policy to increase the configured exceeded limit for SNMP.
C. Modify the access list to include snmptrap.
D. Modify the access list to add a second line to allow udp any any eq snmp
Answer: D (LEAVE A REPLY)

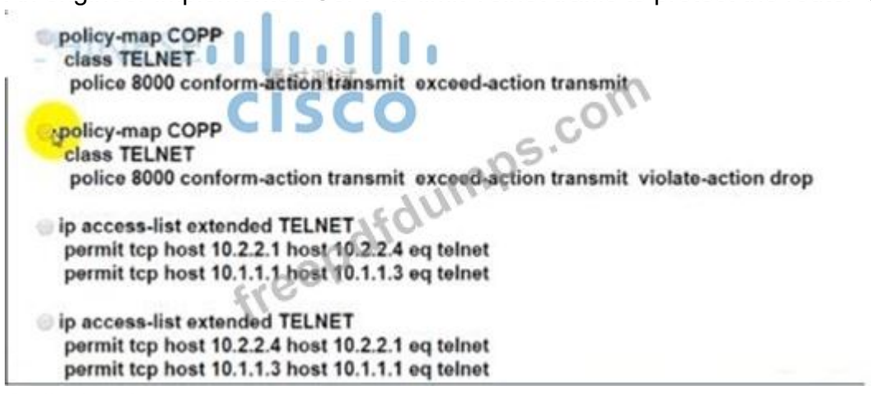
NEW QUESTION: 49
What is a limitation of IPv6 RA Guard?
A. It is not supported in hardware when TCAM is programmed
B. It does not offer protection in environments where IPv6 traffic is tunneled.

C. It cannot be configured on a switch port interface in the ingress direction
D. Packets that are dropped by IPv6 RA Guard cannot be spanned
Answer: B (LEAVE A REPLY)
Restrictions for IPv6 RA Guard
The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
This feature can be configured on a switch port interface in the ingress direction.
This feature supports host mode and router mode.
This feature is supported only in the ingress direction; it is not supported in the egress direction.
This feature is not supported on EtherChannel and EtherChannel port members.
This feature is not supported on trunk ports with merge mode.
This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of PVLANs, primary VLAN features are inherited and merged with port features.
Packets dropped by the IPv6 RA Guard feature can be spanned.
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16-10/ip6f-xe-16-10-book/ip6-ra-guard.html#GUID-589AF00C-7499-439F-AD23-51005D61CAB7

NEW QUESTION: 50
Refer to the exhibit.



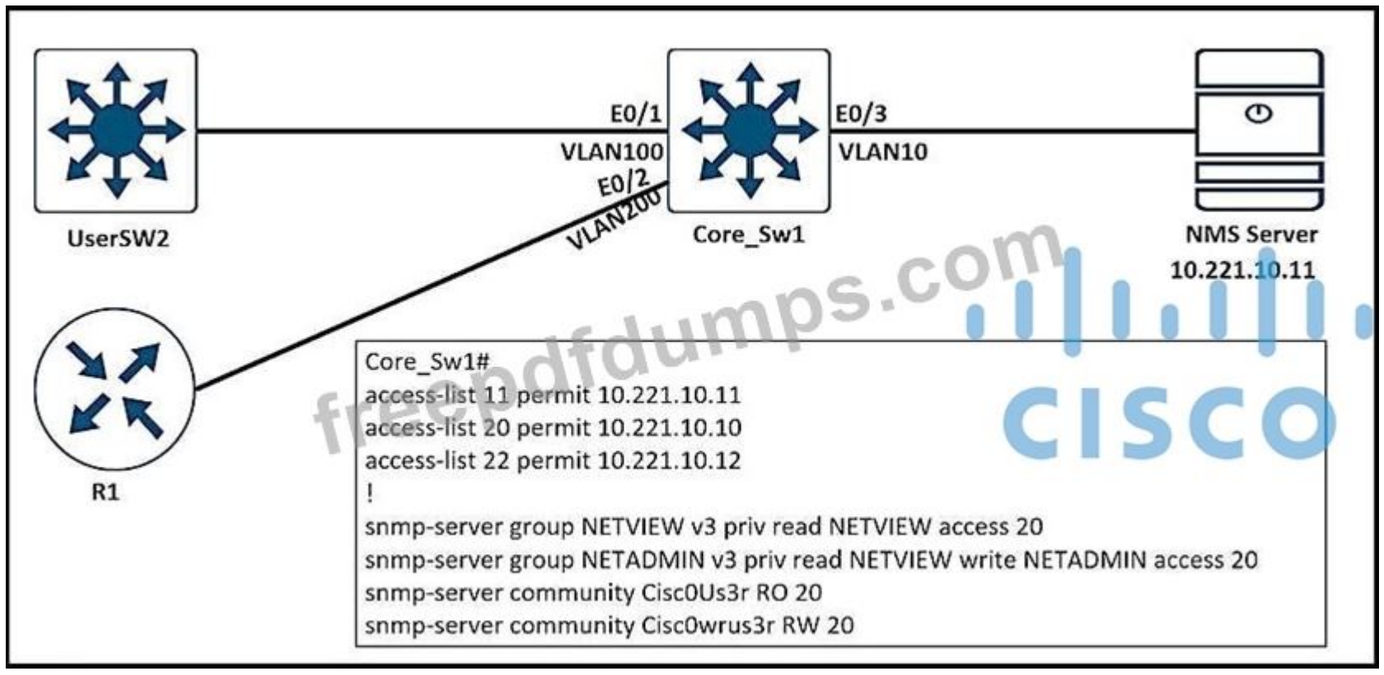
An engineer implemented CoPP to limit Telnet traffic to protect the router CPU. It was noticed that the Telnet traffic did not pass through CoPP Which configuration resolves the issue?



A. Option A

B. Option D
C. Option C
D. Option B
Answer: (SHOW ANSWER)

NEW QUESTION: 51
Refer to the exhibit.

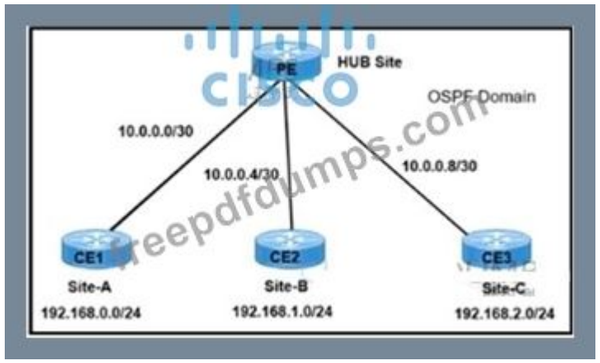


A. access-list 20 permit 10.221.10.11
B. snmp-server group NETVIEW v2c priv read NETVIEW access 20
C. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22
D. access-list 20 permit 10.221.10.12
Answer: A (LEAVE A REPLY)

NEW QUESTION: 52
A customer is running an mGRE DMVPN tunnel over WAN infrastructure between hub and spoke sites. The existing configuration allows NHRP to add spoke routers automatically to the multicast NHRP mappings. The customer is migrated the network from IPv4 to the IPv6 addressing scheme for those spokes' routers that support IPv6 and can run DMVPN tunnel over the IPv6 network. Which configuration must be applied to support IPv4 and IPv6 DMVPN tunnel on spoke routers?
A. Tunnel mode ipv6ip 6to4
B. Tunnel mode ipv6ip 6rd
C. Tunnel mode ipv6ip auto-tunnel
D. Tunnel mode ipv6ip isatap
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53

Refer to the exhibit.



A network engineer must establish communication between three different customer sites with these requirements:

Site-A: must be restricted to access to any users at Site-B or Site-C.

Site-B and Site-C must be able to communicate between sites and share routes using OSPF.

```
PE interface configuration
interface FastEthernet0/0
 ip vrf forwarding Site-A
!
interface FastEthernet0/1
 ip vrf forwarding SharedSites
!
interface FastEthernet0/2
 ip vrf forwarding SharedSites
```

Which configuration meets the requirements?

```
PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config)#router ospf 10 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 1

PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config)#router ospf 10 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0

PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config)#router ospf 20 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0

PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config)#router ospf 20 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 1
```

A. Option D

B. Option A

C. Option C

D. Option B

Answer: C (LEAVE A REPLY)

NEW QUESTION: 54

Refer to the exhibit.

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 198.51.100.1 2 name ISP2
```

The administrator noticed that the connection was flapping between the two ISPs instead of switching to ISP2 when the ISP1 failed. Which action resolves the issue?

A. Include a valid source-interface keyword in the icmp-echo statement.

B. Reference the track object 1 on the default route through ISP2 instead of ISP1.

C. Modify the static routes to refer both to the next hop and the outgoing intertace.

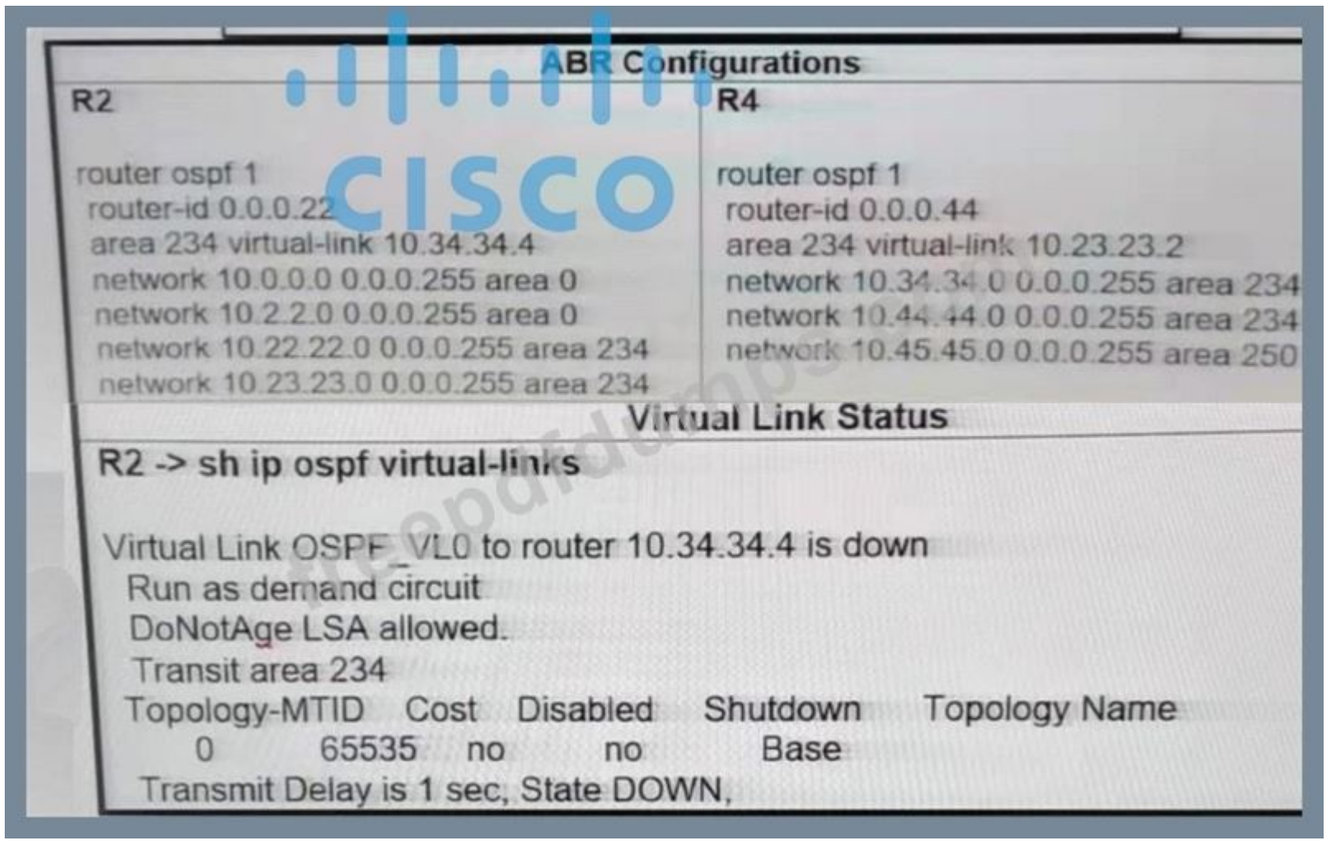
D. Modify the threshold to match the administrative distance of the ISP2 route.

Answer: A (LEAVE A REPLY)

https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-withdefault- routes-using-I.html

NEW QUESTION: 55

Refer to the exhibit.



The network administrator configured the network to connect two disjointed networks and ail the connectivity is up except the virtual link which causes area 250 to be unreachable. Which two configurations resolve this issue? (Choose two.)

A. R2
router ospf 1
router-id 10.23.23.2

B. R2
router ospf 1
no area area 234 virtual-link 10.34.34.4
area 0 virtual-link 0.0.0.44

C. R4
router ospf 1
no area 234 virtual-link 10.23.23.2
area 234 virtual-link 0.0.0.22

D. R2
router ospf 1
no area 234 virtual-link 10.34.34.4
area 234 virtual-link 0.0.0.44

E. R4
router ospf 1
no area area 234 virtual-link 10.23.23.2

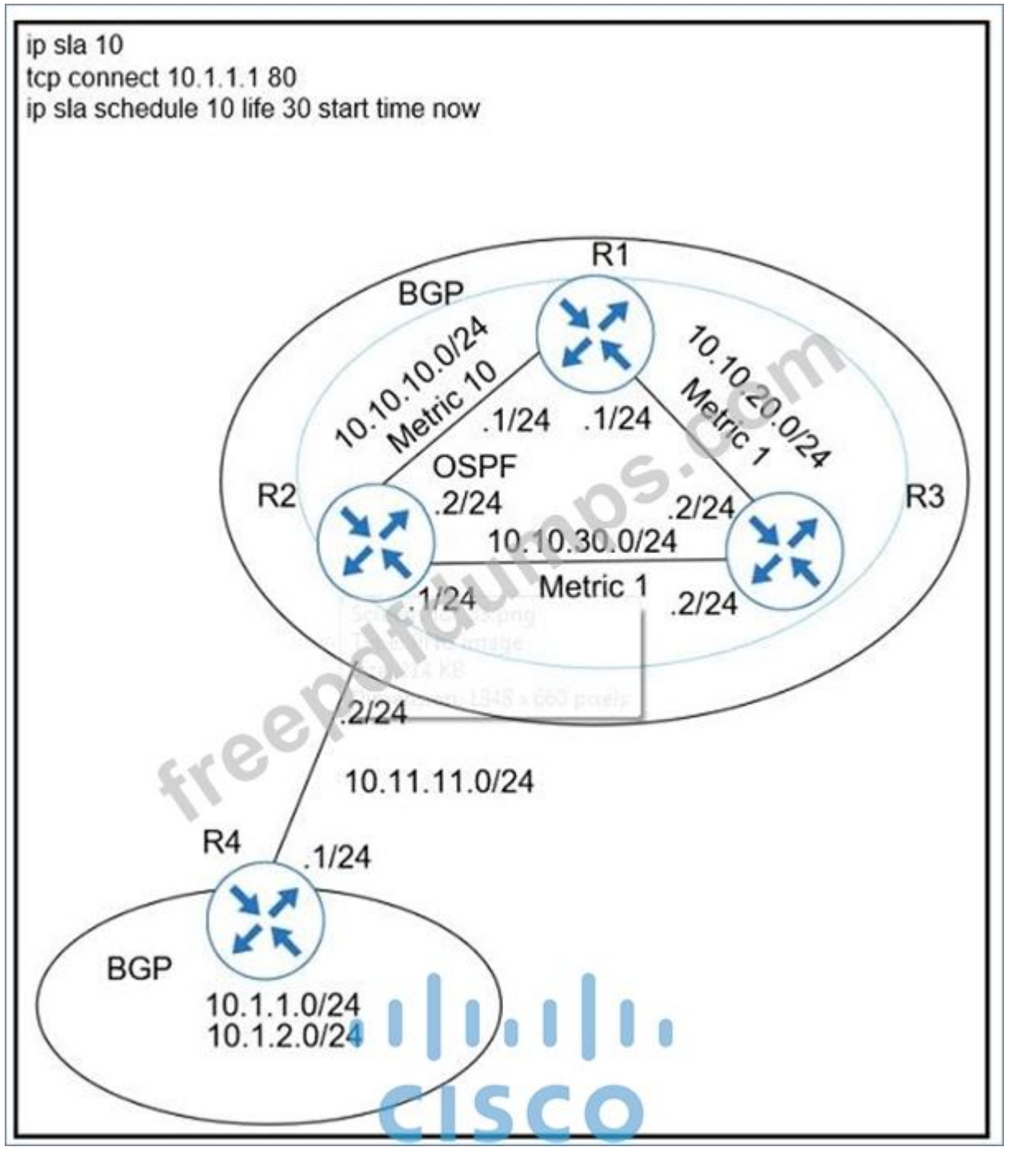
area 0 virtual-link 0.0.0.22
Answer: C,D (LEAVE A REPLY)
Reference:
An important thing to remember when configuring virtual-link is we need to configure the OSPF router ID and NOT the IP address of the ABR. Therefore in this question we have to use the command "area
234 virtual-link 0.0.0.44" on R2 and "area 234 virtual-link 0.0.0.22" on R4.

NEW QUESTION: 56
Refer to the exhibit.

```
snmp-server community ciscotest1
snmp-server host 192.168.1.128 ciscotest
snmp-sever enable traps bgp
```

Network operations cannot read or write any configuration on the device with this configuration from the operations subnet. Which two configurations fix the issue? (Choose two.)
A. Modify access list 1 and allow operations subnet in the access list.
B. Modify access list 1 and allow SNMP in the access list.
C. Configure SNMP rw permission in addition to community ciscotest.
D. Configure SNMP rw permission in addition to version 1.
E. Configure SNMP rw permission in addition to community ciscotest 1.
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 57
Refer to the exhibit.



A user has set up an IP SLA probe to test if a non-SLA host web server on IP address 10.1.1.1 accepts HTTP sessions prior to deployment. The probe is failing. Which action should the network administrator recommend for the probe to succeed?

A. Modify the ip sla schedule frequency to forever.

B. Re-issue the ip sla schedule command.

C. Add icmp-echo command for the host.

D. Add the control disable option to the tcp connect.

Answer: (SHOW ANSWER)

NEW QUESTION: 58

Refer to the exhibit.

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 198.51.100.1 name ISP2 track 1
```

An administrator configures a router to stop using a particular default route if the DNS server 8.8.8.8 is not reachable through that route. However, this configuration did not work as desired and the default route still works even if the DNS server 8.8.8 8 is unreachable. Which two configuration changes resolve the issue? (Choose two.)

A. Use a separate IP SLA probe and track object for every static route

B. Use a separate track object to reference the existing IP SLA 1 probe for every static route.

C. Reference the proper exit interfaces along with the next hops in both static default routes.

D. Associate every IP SLA probe with the proper WAN address of the router.

E. Configure two static routes for the 8.8.8.8/32 destination to match the IP SLA probe for each ISP.

Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 59

Refer to the exhibit.

```
config t
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow exporter EXPORTER-1
  destination 172.16.10.2
  transport udp 90
  exit
!
flow monitor FLOW-MONITOR-1
  record v4_r1
  exit
!
ip cef
!
interface Ethernet0/0.1
  ip address 172.16.6.2 255.255.255.0
  ip flow monitor FLOW-MONITOR-1 input
!
```

Why is the remote NetFlow server failing to receive the NetFlow data?

A. The destination of the flow exporter is not reachable.

B. The flow monitor is applied in the wrong direction.

C. The flow exporter is configured but is not used.

D. The flow monitor is applied to the wrong interface.

Answer: (SHOW ANSWER)

NEW QUESTION: 60

Refer to the exhibit.

```
R1#sh ip route
     10.0.0.0/8 is variably subnetted, 3 subnets, 1 masks
D       10.1.2.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
D       10.1.1.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
C       10.1.100.0/24 is directly connected, FastEthernet0/0
```

Although summarization is configured for R1 to receive 10.0.0.0/8. more specific routes are received by R1. How should the 10.0.0.0/8 summary route be received from the neighbor, attached to R1 via Fast Ethernet0/0 interface?

A. The summarization condition is not met Router 10 1 100.10 requires a route for 10 0.0.0/8 that points to null 0

B. R1 should configure the ip summary-address eigrp <AS number> 10.0.0.0.255.0.0.0 command under the Fast Ethernet 0/0 interface.

C. The summarization condition is not met. The network 10.1.100.0/24 should be changed to 172.16.0.0/24.

D. R1 should configure the ip summary-address eigrp <AS number> 10.0.0.0 0.0.0.255 command under the Fast Ethernet 0/0 interface.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 61

What is the role of a route distinguisher via a VRF-Lite setup implementation?

A. It extends the IP address to identify which VFP instance it belongs to.

B. It enables multicast distribution for VRF-Lite setups to enhance EGP routing protocol capabilities

C. It manages the import and export of routes between two or more VRF instances

D. It enables multicast distribution for VRF-Lite setups to enhance IGP routing protocol capabilities

Answer: A (LEAVE A REPLY)

NEW QUESTION: 62

What is an advantage of using BFD?

A. It has sub-second failure detection for layer 1 and layer 3 problems.

B. It detects local link failure at layer 1 and updates routing table.

C. It detects local link failure at layer 2 and updates routing protocols.
D. It has sub-second failure detection for layer 1 and layer 2 problems.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 63
Refer to the exhibit.

An engineer is troubleshooting failed access by contractors to the business application server via Telnet or HTTP during the weekend. Which configuration resolves the issue?
A)
R1
time-range Contractor
no periodic weekdays 8:00 to 16:30
periodic daily 8:00 to 16:30
B)
R4
time-range Contractor
no periodic weekdays 17:00 to 23:59
periodic daily 8:00 to 16:30
C)
R4
no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor
D)
R1
no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor
A. Option
B. Option
C. Option
D. Option
Answer: C (LEAVE A REPLY)

NEW QUESTION: 64
What is a function of the IPv6 DHCP Guard feature for DHCP messages?
A. All client messages are always switched regardless of the device role.

B. If the device is configured as a DHCP server, no message is switched.
C. Only access lists are supported for matching traffic.
D. It blocks only DHCP request messages.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 65
What does the MP-BGP OPEN message contain?
A. the version number and the AS number to which the router belongs
B. MPLS labels and the IP address of the router that receives the message
C. NLRI, path attributes, and IP addresses of the sending and receiving routers
D. IP routing information and the AS number to which the router belongs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 66
What are two characteristics of IPv6 Source Guard? (Choose two.)
A. requires IPv6 snooping on Layer 2 access or trunk ports
B. used in service provider deployments to protect DDoS attacks
C. requires the user to configure a static binding
D. requires that validate prefix be enabled
E. recovers missing binding table entries
Answer: D,E (LEAVE A REPLY)
IPv6 Source Guard uses the IPv6 First-Hop Security Binding Table to drop traffic from unknown sources or bogus IPv6 addresses not in the binding table. The switch also tries to recover from lost address information, querying DHCPv6 server or using IPv6 neighbor discovery to verify the source IPv6 address after dropping the offending packet(s).

NEW QUESTION: 67
A network administrator added a new spoke site with dynamic IP on the DMVPN network. Which configuration command passes traffic on the DMVPN tunnel from the spoke router?
A. ip nhrp registration dynamic
B. ip nhrp registration no-unique
C. ip nhrp registration ignore
D. ip nhrp registration no-registration
Answer: B (LEAVE A REPLY)

NEW QUESTION: 68
Refer to the exhibit.

An engineer configured IP SLA on R1 to avoid the ISP link flapping problem. but it is not working as designed IP SLA should wait 30 seconds before switching traffic to a secondary connection and then revert to the primary link after waning 20 seconds, when the primary link is available and stabilized. Which configuration resolves the issue?

A. R1(config)#ip sla 700
R1(config-ip-sla)#delay down 30 up 20

B. R1(config)#ip sla 700
R1(config-ip-sla)#delay down 20 up 30

C. R1(config)#track 700 ip sla 700
R1(config-track)#delay down 30 up 20

D. R1(config)#track 700 ip sla 700
R1(config-track)#delay down 20 up 30

Answer: C (LEAVE A REPLY)

"wait 30 seconds before switching traffic to a secondary connection" -> delay down 30
"then revert to the primary link after waiting 20 seconds" -> up 20
Under the track object, you can specify delays so we have to configure delay under "track 700 ip sla 700" (not under "ip sla 700").

NEW QUESTION: 69

An administrator attempts to download the pack NBAR2 file using TFTP from the CPE router to another device over the Gi0/0 interface. The CPE is configured as below:

The transfer fails. Which action resolves the issue?

A. Make the permit udp any eq tftp any entry the last entry in the WAN ACL.

B. Change the WAN ACL to permit the UDP port 69 to allow TFTP

C. Shorten the file name to the 8+3 naming convention.

D. Change the WAN ACL to permit the entire UDP destination port range

Answer: A (LEAVE A REPLY)

NEW QUESTION: 70

What is a prerequisite for configuring BFD?

A. All routers in the path between two BFD endpoints must have BFD enabled.

B. To use BFD with BGP, the timers 3 9 command must first be configured in the BGP routing process.

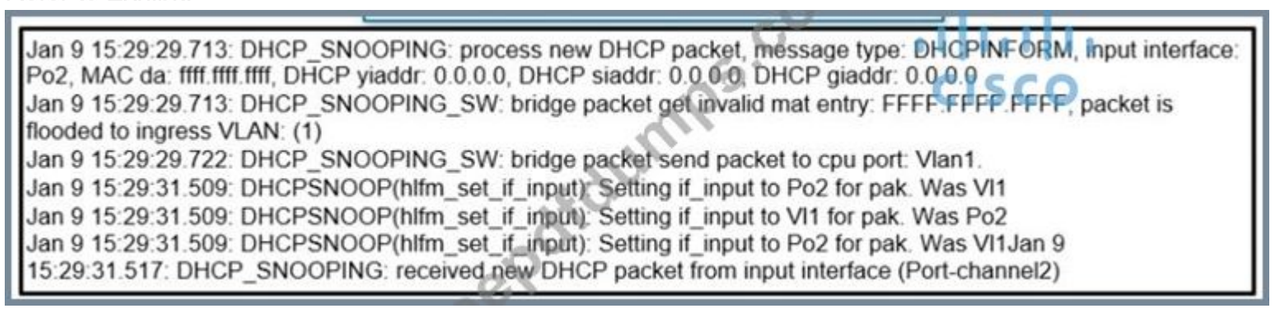
C. Jumbo frame support must be configured on the router that is using BFD.

D. Cisco Express Forwarding must be enabled on all participating BFD endpoints.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 71

Refer to Exhibit.



A network administrator enables DHCP snooping on the Cisco Catalyst 3750-X switch and configures the uplink port (Port-channel2) as a trusted port. Clients are not receiving an IP address, but when DHCP snooping is disabled, clients start receiving IP addresses. Which global command resolves the issue?

A. ip dhcp relay information trust portchannel2

B. ip dhcp snooping trust

C. ip dhcp snooping

D. No ip dhcp snooping information option

Answer: (SHOW ANSWER)

NEW QUESTION: 72

Refer to the exhibit.

R1 is configured with uRPF, and ping to R1 is failing from a source present in the R1 routing table via the GigatxtEthernet 0/0 interface. Which action resolves the issue?

A. Add a floating static route to the source on R1 to the GigabitEthernet 0/1 interface

B. Enable Cisco Express Forwarding to ensure that uRPF is functioning correctly

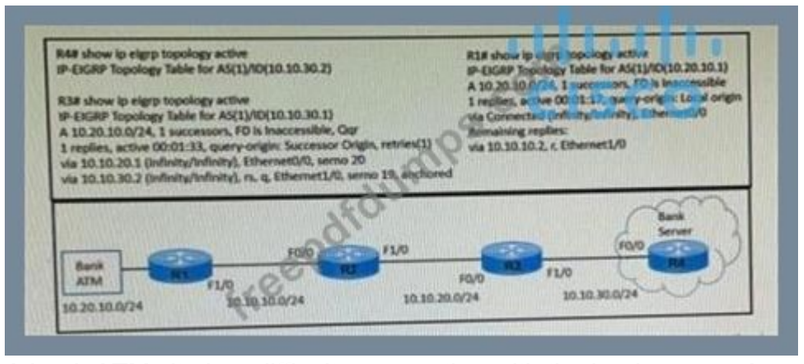
C. Remove the access list from the interface GigabrtEthernet 0/0

D. Modify the uRPF mode from strict to loose

Answer: D (LEAVE A REPLY)

NEW QUESTION: 73

Refer to the exhibit.



A bank ATM site has difficulty connecting with the bank server. A network engineer troubleshoots the issue and finds that R4 has no active route to the bank ATM site. Which action resolves the issue?

A. EIGRP peering between R3 and R4 to be fixed.

B. EIGRP peering between R1 and R2 to be fixed.

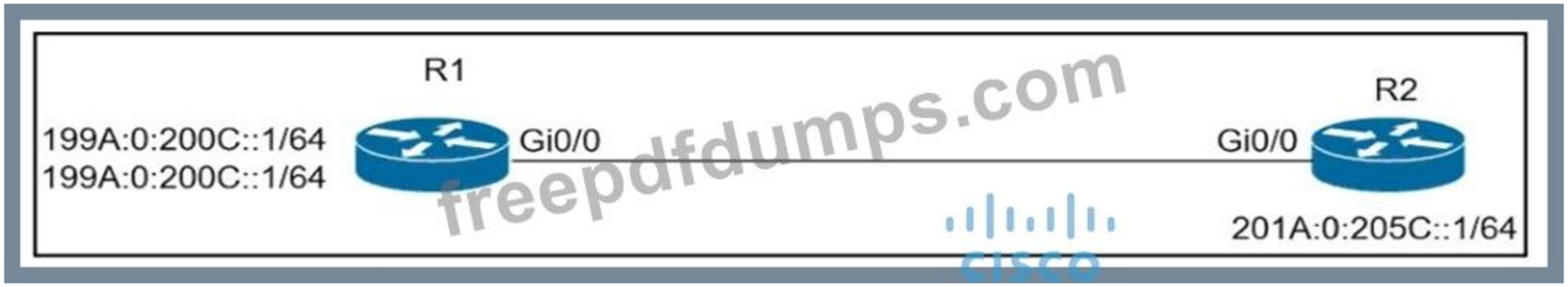
C. Advertise 10.10.30.0/24 subnet in R1 EIGRP AS.

D. Advertise 10.10.30.0/24 subnet in R3 EIGRP AS.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 74

Refer to the exhibit.



Which configuration denies Telnet traffic to router 2 from 198A:0:200C::1/64?

A)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
 ipv6 traffic-filter Deny_Telnet in
!
```

B)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
 ipv6 access-map Deny_Telnet in
!
```

C)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
 ipv6 access-map Deny_Telnet in
!
```

D)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
 ipv6 traffic-filter Deny_Telnet in
!
```

A. Option C

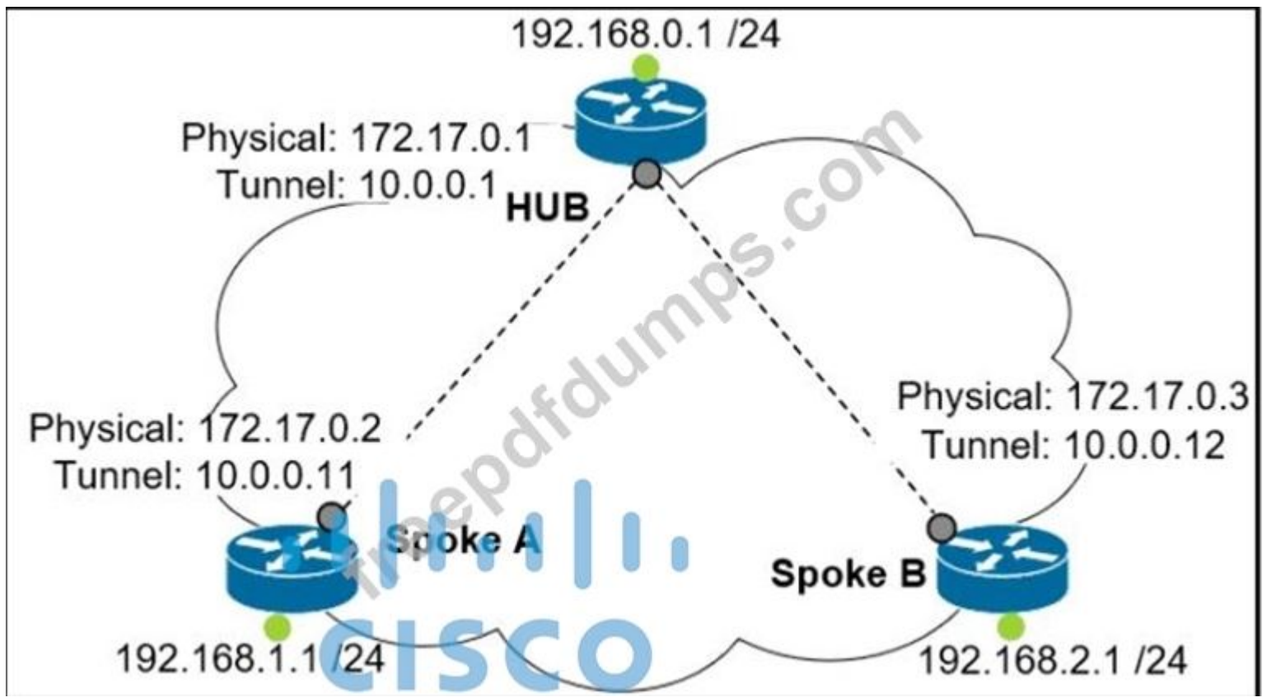
B. Option B

C. Option D

D. Option A

Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
Refer to the exhibit.



Which interface configuration must be configured on the spoke A router to enable a dynamic DMVPN tunnel with the spoke B router?

A.
```
interface Tunnel0
description mGRE – DMVPN Tunnel
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel destination FastEthernet 0/0
tunnel mode gre multipoint
```

B.
```
interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source FastEthernet 0/0
tunnel mode gre multipoint
ip nhrp nhs 10.0.0.1
ip nhrp map 10.0.0.1 172.17.0.1
```

```
interface Tunnel0
ip address 10.1.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source 1.1.1.10
ip nhrp map 10.0.0.11 172.17.0.2
tunnel mode gre
```

```
interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast static
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel mode gre multipoint
```

A. Option C
B. Option D
C. Option A
D. Option B
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
Refer to the exhibit.

```
R1#show run | begin line
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synohronous
 transport preferred telnet
 transport output none
 stopbits 0 4
line vty 0 4
 login
 transport referred telnet
 transport input none
 transport output telnet
R1#

R1#ssh -1 cisco 192.168.12.2
% ssh connections not permitted from this terminal
R1#
```

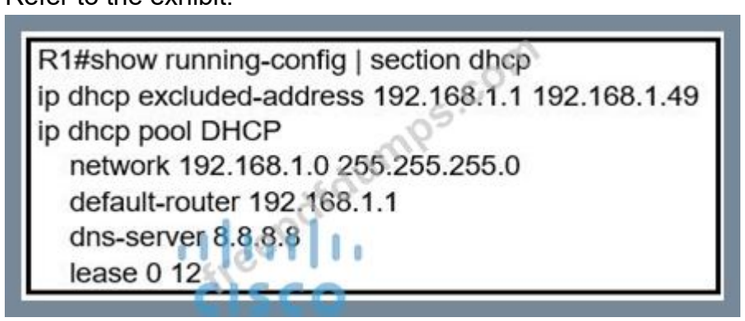
An engineer receives this error message when trying to access another router m-band from the serial interface connected to the console of R1. Which configuration is needed on R1 to resolve this issue?

```
R1(config)#line console 0
R1(config-line)# transport preferred ssh

R1(config)#line vty 0
R1(config-line)# transport output ssh

R1(config)#line vty 0
R1(config-line)# transport output ssh
R1(config-line)# transport preferred ssh

R1(config)#line console 0
R1(config-line)# transport output ssh
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: (SHOW ANSWER)
https://community.cisco.com/t5/other-network-architecture/out-of-band-router-access/td-p/333295 The "transport output none" command prevents any protocol connection made from R1. Therefore our SSH connection to 192.168.12.2 was refused. In order to fix this problem we can configure "transport output ssh" under "line console 0" of R1.

Note: The parameter "-l" specifies the username to log in as on the remote machine.

NEW QUESTION: 77
Refer to the exhibit.



Users report that IP addresses cannot be acquired from the DHCP server. The DHCP server is configured as shown. About 300 total nonconcurrent users are using this DHCP server, but none of them are active for more than two hours per day. Which action fixes the issue within the current resources?
A. Modify the subnet mask to the network 192.168.1.0 255.255.254.0 command in the DHCP pool
B. Configure the DHCP lease time to a smaller value
C. Configure the DHCP lease time to a bigger value
D. Add the network 192.168.2.0 255.255.255.0 command to the DHCP pool
Answer: B (LEAVE A REPLY)

NEW QUESTION: 78
Refer to the exhibit.

Router Configuration:

```
ip vrf customer_a
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
!
interface FastEthernet0.1
 encapsulation dot1Q 2
 ip vrf forwarding customer_a
 ip address 192.168.4.1 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 !
router ospf 2 vrf customer_a
 log-adjacency-changes
 network 192.168.4.0 0.0.0.255 area 0
 !
end
```

The network administrator configured VRF lite for customer A.

The technician at the remote site misconfigured VRF on the router.

Which configuration will resolve connectivity for both sites of customer_a?

A. Option A

B. Option B

C. Option C

D. Option D

Answer: (SHOW ANSWER)

From the exhibit, we learned:

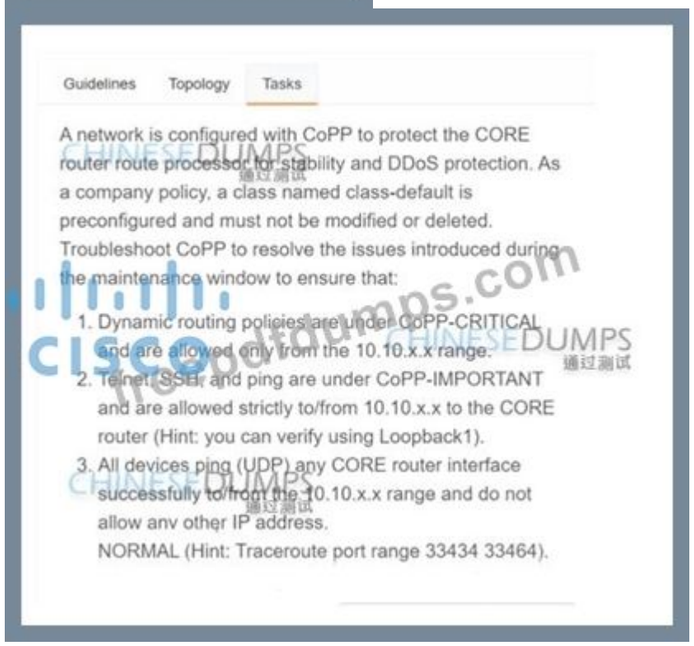
+ VRF customer_a was exported with Route target (RT) of 1:1 so at the remote site it must be imported with the same RT 1:1.

+ VRF customer_a was imported with Route target (RT) of 1:1 so at the remote site it must be exported with the same RT 1:1.

Therefore at the remote site we must configure the command "route-target both 1:1" (which is equivalent to two commands "route-target import 1:1" & "route-target export 1:1".

NEW QUESTION: 79

LAB SIMULATION



WAN


!
!
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
 ip address 172.16.2.2 255.255.255.255
!


WAN
CORE
MGMT
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
 ip address 172.16.2.2 255.255.255.0
!
interface Ethernet0/0
 ip address 10.10.12.2 255.255.255.0
 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 eigrp 101
 network 10.10.0.0 0.0.255.255
 network 172.16.2.0 0.0.0.255
 eigrp router-id 10.10.2.2


!
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 network 172.16.2.0 0.0.0.255
 eigrp router-id 10.10.2.2
!

CORE


!
class-map match-all CoPP-CRITICAL
match access-group 120
class-map match-all CoPP-NORMAL
match access-group 122
class-map match-all CoPP-IMPORTANT
match access-group 121
!
policy-map CoPP
class CoPP-CRITICAL
police 1000000 50000 50000 conform-action transmit exceed
-action drop
class CoPP-IMPORTANT
police 100000 20000 20000 conform-action transmit exceed-
action drop
class CoPP-NORMAL
police 64000 6400 64000 conform-action transmit exceed-ac
tion drop
class class-default
police 8000 1500 1500 conform-action drop exceed-action d
rop
!


interface Ethernet0/0
ip address 10.10.1.1 255.255.255.0
!
interface Ethernet0/0
ip address 10.10.1.1 255.255.255.0
duplex auto
!
interface Ethernet0/1
ip address 10.10.13.1 255.255.255.0
duplex auto
!


interface Ethernet0/1
ip address 10.10.13.1 255.255.255.0
duplex auto
!
interface Ethernet0/2
no ip address
shutdown
duplex auto
!
interface Ethernet0/3
no ip address
shutdown
duplex auto
!
router eigrp 1
network 10.10.0.0 0.0.255.255
eigrp router-id 10.10.1.1
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp


!
!
access-list 120 remark *** ACL for CoPP-Critical ***
access-list 121 remark *** ACL for CoPP-IMPORTANT
access-list 122 remark *** ACL for CoPP-NORMAL
!
control-plane
service-policy input CoPP
!

MGMT


WAN
CORE
MGMT
interface Loopback0
ip address 10.10.3.3 255.255.255.255
!
interface Loopback通过测试
ip address 172.16.3.3 255.255.255.0
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface Ethernet0/1
ip address 10.10.13.3 255.255.255.0
duplex auto
!
interface Ethernet0/2
no ip address
shutdown
duplex auto
!
interface Ethernet0/3
no ip address
shutdown
duplex auto
!
!
router eigrp 101
network 10.10.0.0 0.0.255.255
network 172.16.3.0 0.0.0.255
eigrp router-id 10.10.3.3
CHINESEDUMPS
通过测试
freepdfdumps.com
CISCO

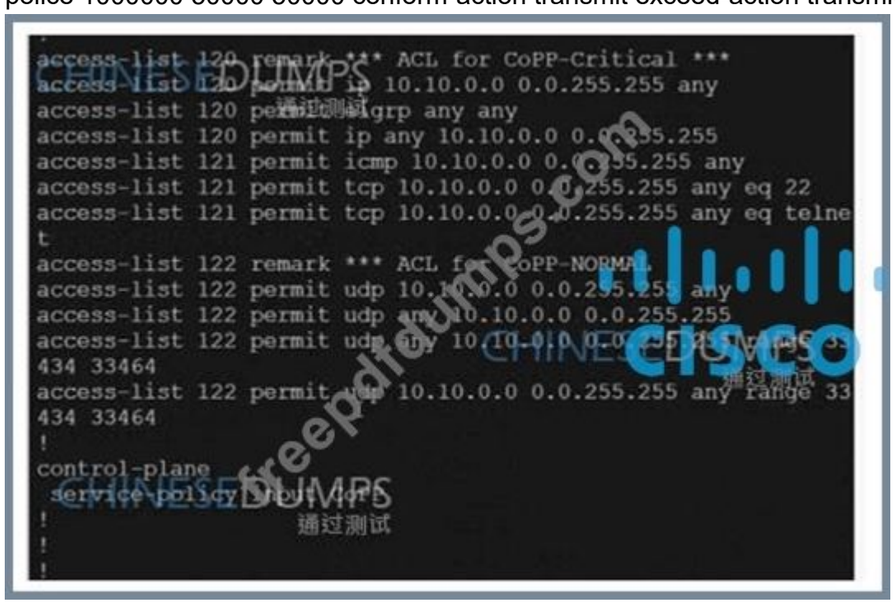
Answer:

CORE

policy-mao CoPP

class CoPP-CRITICAL

police 1000000 50000 50000 conform-action transmit exceed-action transmit



CORE# Copy run start

TESTING: -

CORE

MGMT

NEW QUESTION: 80

How does an MPLS Layer 3 VPN function?

A. set of sites use multiprotocol BGP at the customer site for aggregation

B. multiple customer sites interconnect through service provider network to create secure tunnels between customer edge devices

C. set of sites interconnect privately over the Internet for security

D. multiple customer sites interconnect through a service provider network using customer edge to provider edge connectivity

Answer: D (LEAVE A REPLY)

A Multiprotocol Label Switching(MPLS) Layer 3 Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers.

Reference:

https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-5/lxvpn/configuration/g uide/b-l3vpn-cg-asr9000-65x/b-l3vpn-cg-asr9000-65x_chapter_010.pdf

NEW QUESTION: 81

Refer to the exhibit.

```
P 172.29.0.0/16, 1 successors, FD is 307200, serno 2
        via 192.168.254.2 (307200/281600), FastEthernet0/1
        via 192.168.253.2 (410200/352300), FastEthernet0/0
```

When the FastEthemet0/1 goes down, the route to 172.29.0 0/16 via 192.168.253 2 is not installed in the RIB. Which action resolves the issue?

A. Configure reported distance greater than the feasible distance

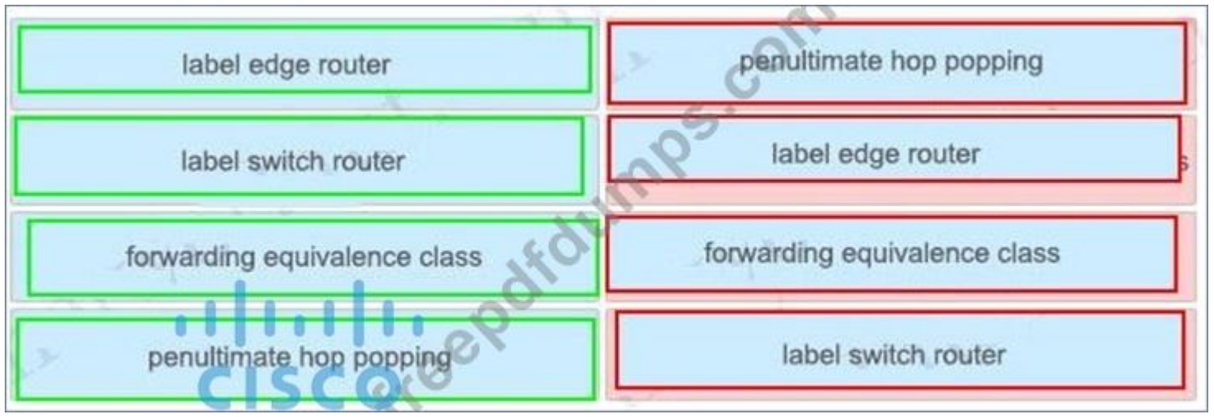
B. Configure feasible distance greater than the successor's feasible distance.

C. Configure reported distance greater than the successor's feasible distance.

D. Configure feasible distance greater than the reported distance
Answer: (SHOW ANSWER)

NEW QUESTION: 82
Drag and drop the MPLS concepts from the left onto the descriptions on the right.

Answer:



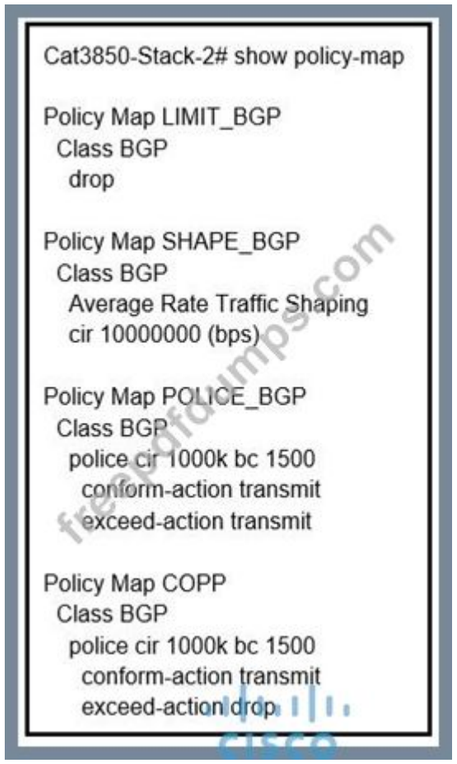
NEW QUESTION: 83
What is a role of route distinguishers in an MPLS network?
A. Route distinguishers make a unique VPNv4 address across the MPLS network
B. Route distinguishers are used for label bindings.
C. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.
D. Route distinguishers define which prefixes are imported and exported on the edge router
Answer: A (LEAVE A REPLY)

NEW QUESTION: 84
The network administrator configured CoPP so that all routing protocol traffic toward the router CPU is limited to 1 mbps. All traffic that exceeds this limit must be dropped. The router is running BGP and OSPF Management traffic for Telnet and SSH must be limited to 500kbps.
access-list 100 permit tcp any any eq 179
access-list 100 permit tcp any any range 22 23
access-list 100 permit ospf any any

!
class-map CM-ROUTING
match access-group 100
class-map CM-MGMT
match access-group 100
!
policy-map PM-COPP
class CM-ROUTING
police 1000000 conform-action transmit
class CM-MGMT
police 500000 conform-action transmit
!
control-plane
service-policy output PM-COPP
No traffic is filtering through CoPP,which is resulting in high CPU utilization,which configuration resolves the issue ?
A. no access-list 100access-list 100 permit tcp any any eq 179
access-list 100 permit ospf any any
access-list 101 Permit tcp any any range 22 23
!
class-map CM-MGMT
no match access-group 100
match access-group 101
B. control-plane
no service-policy output PM-COPP
service-policy input PM-COPP
C. No access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit tcp any any range eq 22
access-list 100 permit tcp any any range eq 23
access-list 100 permit ospf any any
D. no access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit ospf any any
access-list 101 Permit tcp any any range 22 23
!
class-map CM-MGMT
no match access-group 100
Answer: (SHOW ANSWER)
match access-group 101
!
control-plane

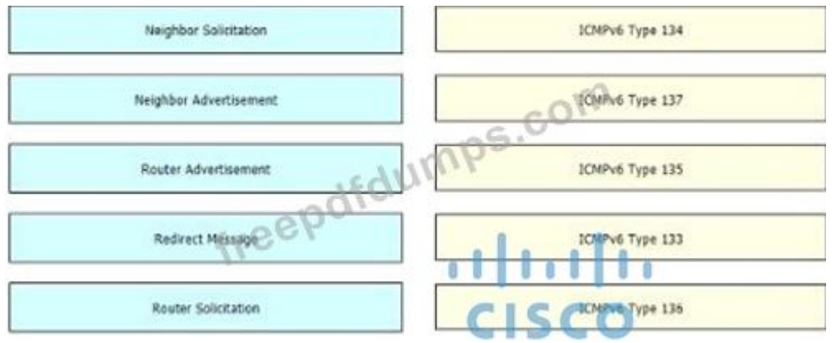
no service-policy output PM-COPP
service-policy input PM-COPP

NEW QUESTION: 85
Refer to the exhibit.

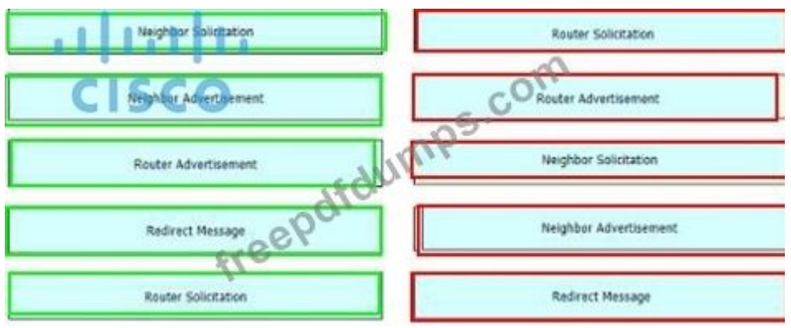


Which control plane policy limits BGP traffic that is destined to the CPU to 1 Mbps and ignores BGP traffic that is sent at higher rate?
A. policy-map POLICE_BGP
B. policy-map COPP
C. policy-map LIMIT_BGP
D. policy-map SHAPE_BGP
Answer: (SHOW ANSWER)

NEW QUESTION: 86
Drag and drop the ICMPv6 neighbor discovery messages from the left onto the correct packet types on the right.

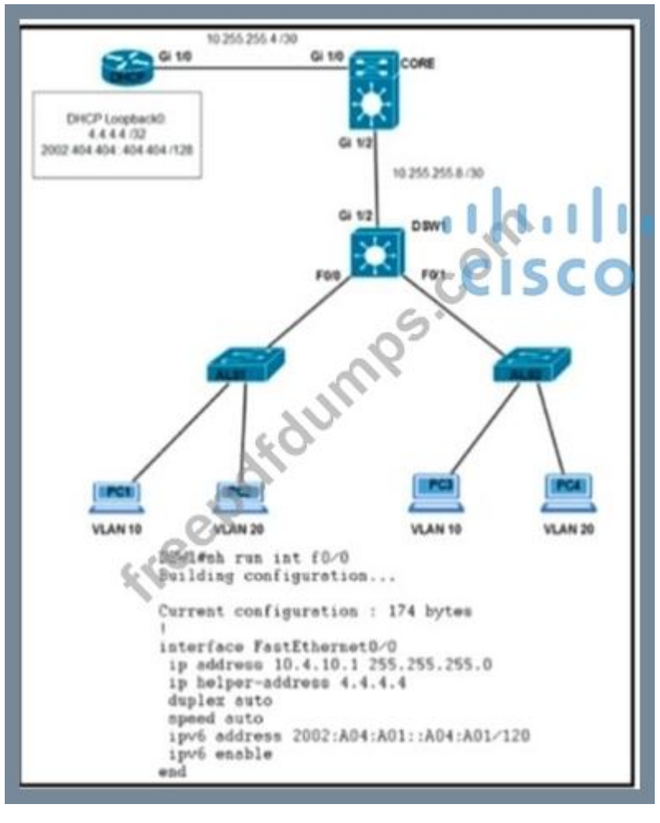


Answer:



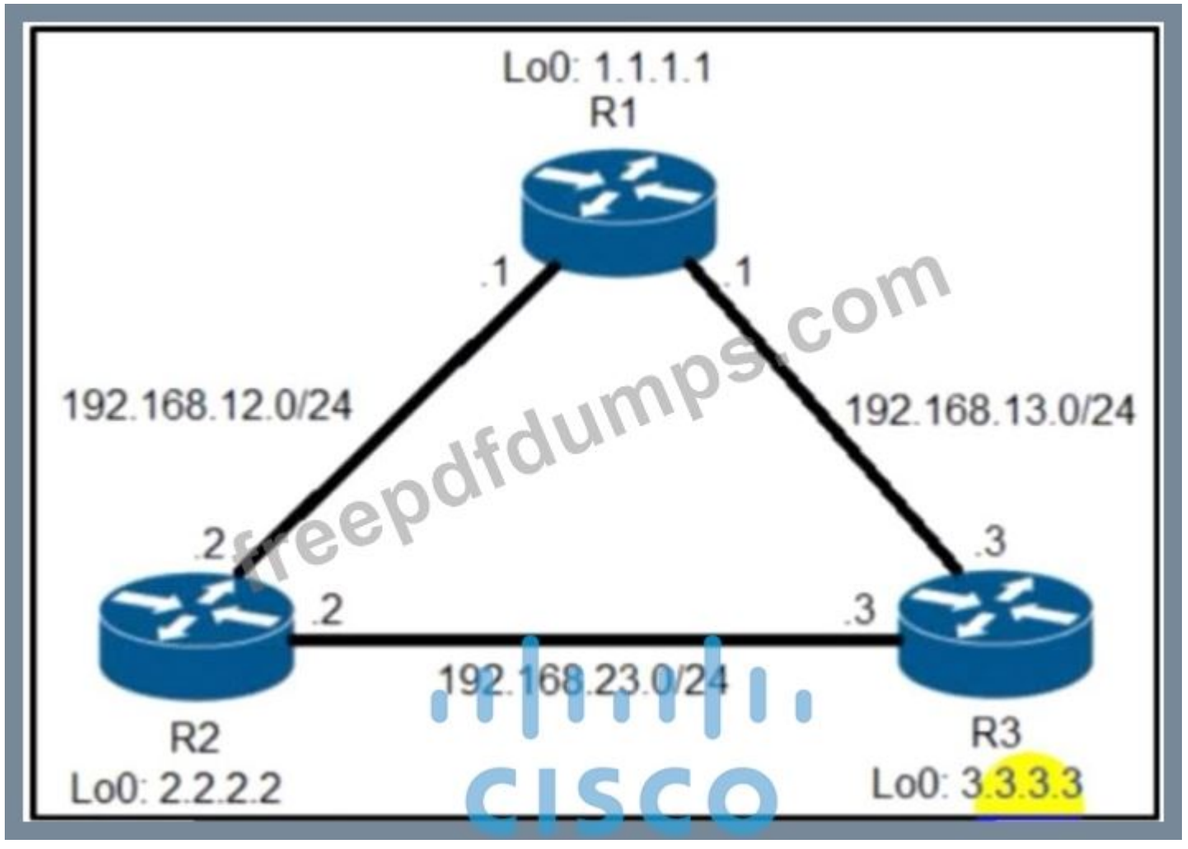
NEW QUESTION: 87

Clients on ALS2 receive IPv4 and IPv6 addresses but clients on ALS1 receive only IPv4 addresses and not IPv6 addresses. Which action on DSW1 allows clients on ALS1 to receive IPv6 addresses?



A. Option A
B. Option B
C. Option C
D. Option D
Answer: B (LEAVE A REPLY)
https://community.cisco.com/t5/networking-documents/stateful-dhcpv6-relay-configuration-example/ta-p/3149338

NEW QUESTION: 88
Refer to the exhibit.



Refer to the exhibit. R2 has two paths to reach 192.168.13.0/24. but traffic is sent only through R3. Which action allows traffic to use both paths?

A. Configure the bandwidth 2000 command under interface FastEthernet0/0 on R2.

B. Configure the variance 4 command under the EIGRP process on R2.

C. Configure the delay 1 command under interface FastEthernet0/0 on R2.

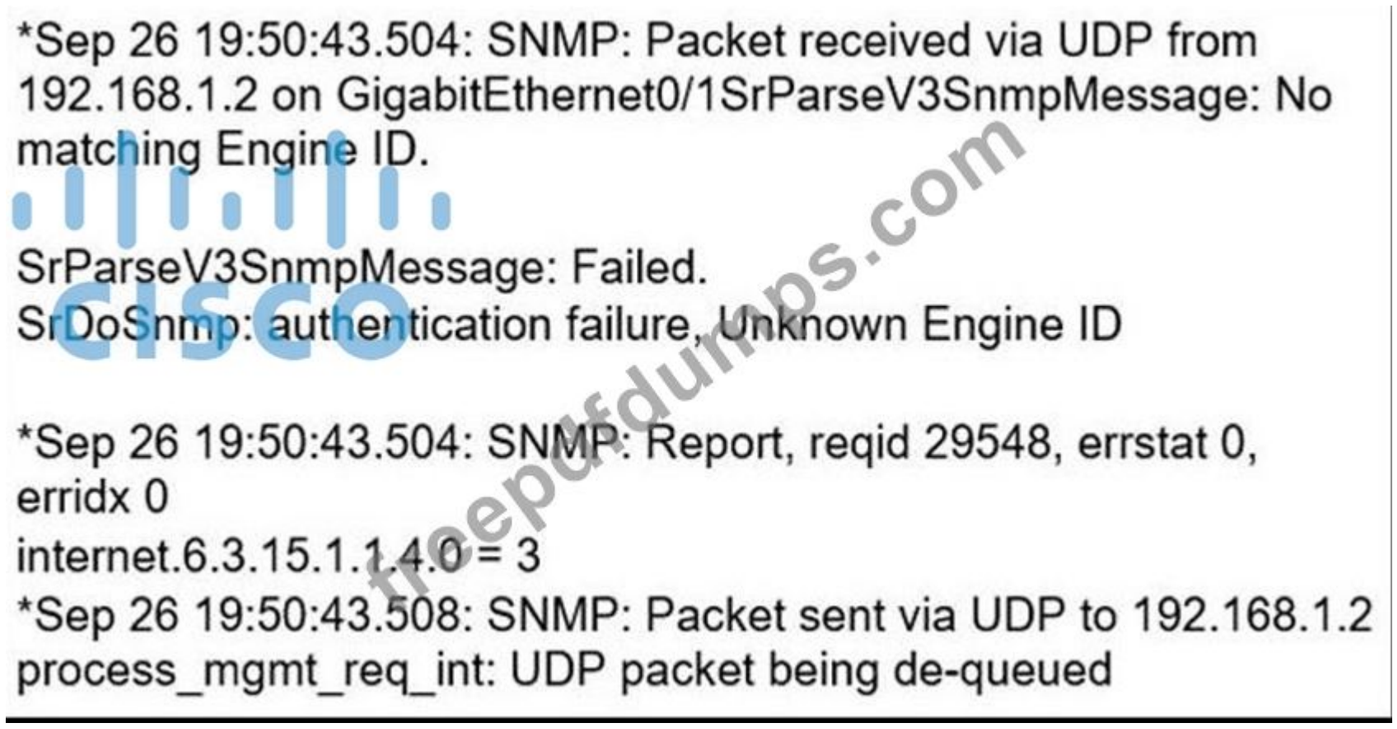
D. Configure the variance 2 command under the EIGRP process on R2

Answer: B (LEAVE A REPLY)

From the output of the "show ip eigrp topology ..." command, we notice network 192.168.13.0/24 was learned via two routes:+ From 192.168.23.3 (R3) with FD = 1075200 and AD = 281600+ From 192.168.12.1 (R1) with FD = 2611200 and AD = 281600 From the output of the "show ip route ..." command, we learned that the best (and chosen) path is via 192.168.23.3 (R3).

To use both paths (called unequal cost load balancing) with EIGRP, the second path via R1 must satisfy the feasibility condition. The feasibility condition states that, theAdvertised Distance (AD) of a route must be lower than the feasible distance of the current successor route.
In this case, the second path satisfies the feasible condition as its AD (281600) is smaller than the FD (1075200) of the best path. Therefore we can configure loadbalancing with "variance" command.
In other words, EIGRP will install all paths with metric < variance * best_metric into the local routing table, provided that it meets the feasibility condition to preventrouting loop. Therefore we can calculate the variance > metric / best_metric = 2611200 / 1075200 =2.4.
So with a variance greater than 2 (and must be an integer), we can load balance traffic to network 192.168.13.0/24.

NEW QUESTION: 89
Refer to the exhibit.



Which two commands provide the administrator with the information needed to resolve the issue? (Choose two.)
A. Show snmp user
B. debug snmp packet
C. showsnmpv3 user
D. debug snmpv3 engine-id
E. debug snmp engine-id
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Exhibit:

```
policy-map COPP-7600
 class COPP-CRITICAL-7600
  police cir 2000000 bc 62500
  conform-action transmit
  exceed-action transmit
  !
 class class-default
  police cir 200000 bc 6250
  conform-action transmit
  exceed-action drop
!
class-map match-all COPP-CRITICAL-7600
  match access-group name COPP-CRITICAL-7600
!
ip access-list extended COPP-CRITICAL-7600
  permit ip any any eq http
  permit ip any any eq https
```


BGP is flapping after the Copp policy is applied. What are the two solutions to fix the issue? (Choose two)

A. Configure BGP in the COPP-CRITICAL-7600 ACL

B. Configure a higher value for CIR under the default class to allow more packets during peak traffic

C. Configure a higher value for CIR under the class COPP-CRITICAL-7600

D. Configure a three-color policer instead of two-color policer under class COPP-CRITICAL-7600

E. Configure IP CEF to CoPP policy and BGP to work

Answer: A,B (LEAVE A REPLY)

The policy-map COPP-7600 only rate-limit HTTP & HTTPS traffic (based on the ACL conditions) so any BGP packets will be processed in the class "class-default", which drops exceeded BGP packets. Therefore we have two ways to solve this problem:

+ Add BGP to the ACL with the statement "permit tcp any any eq bgp"

+ Configure higher value for CIR in default class as 2Mbps is too low for web traffic (http & https)

NEW QUESTION: 91

Which two protocols can cause TCP starvation? (Choose two)

A. TFTP

B. HTTPS

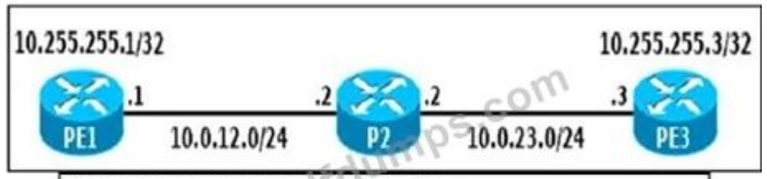
C. SNMP

D. FTP

E. SMTP

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 92
Refer to the exhibit.




```
PE1# show run | sec router bgp
router bgp 65000
 bgp log-neighbor-changes
 neighbor 10.255.255.3 remote-as 65000
 neighbor 10.255.255.3 update-source Loopback0
```

```
1/1/1 ms
PE1# debug ip tcp transactions
PE1# debug ip icmp

[...snip...]
*Feb 22 14:04:12.374: TCP: sending SYN, seq 379810712, ack 0
*Feb 22 14:04:12.374: TCP0: Connection to 10.255.255.3:179,
advertising MSS 1460
*Feb 22 14:04:12.374: TCP0: state was CLOSED -> SYNSENT [21381 -
> 10.255.255.3(179)]
*Feb 22 14:04:12.375: ICMP: dst (10.255.255.1) administratively
prohibited unreachable rcv from 10.0.12.2
*Feb 22 14:04:12.375: TCP0: ICMP destination unreachable
received
*Feb 22 14:04:12.375: Released port 21381 in Transport Port
Agent for TCP IP type 1 delay 240000
*Feb 22 14:04:12.375: TCP0: state was SYNSENT -> CLOSED [21381 -
> 10.255.255.3(179)]
*Feb 22 14:04:12.375: TCB 0xE35A92B8 destroyed
```

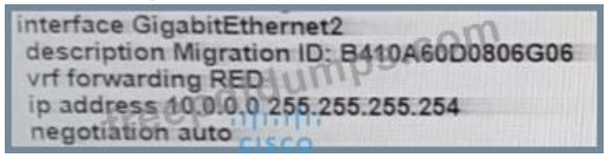
Refer to the exhibit. The administrator is troubleshooting a BGP peering between PE1 and PE3 that is unable to establish Which action resolves the issue?
A. Remove the traffic filtering rules on P2 blocking the BGP communication between PE1 and PE3
B. Ensure that the PE3 loopback address is used as a source for BGP peering to PE1
C. P2 must have a route to PE3 to establish a BGP session to PE1
D. Disable sending ICMP unreachables on P2 to allow PE1 to establish a session with PE3
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
An engineer failed to run diagnostic commands on devices using Cisco DNA Center. Which action in Cisco DNA Center resolves the issue?
A. Enable Secure Shell
B. Enable APIs
C. Enable Command Runner

D. Enable CDP
Answer: C (LEAVE A REPLY)

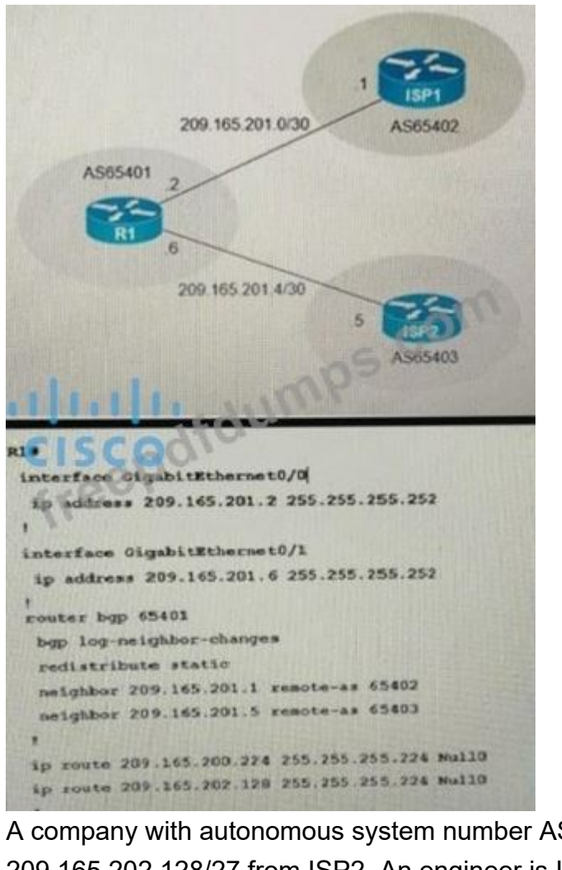
NEW QUESTION: 94
How does an MPLS Layer 3 VPN differentiate the IP address space used between each VPN?
A. by RD
B. by address family
C. byRT
D. by MP-BGP
Answer: (SHOW ANSWER)

NEW QUESTION: 95
An engineer is implementing a coordinated change with a server team. As part of the change, the engineer must configure interlace GigabitEthernet2 in an existing VRF "RED" then move the interface to an existing VRF "BLUE" when the server team is ready. The engineer configured interface GigabitEthemet2 in VRF "RED"



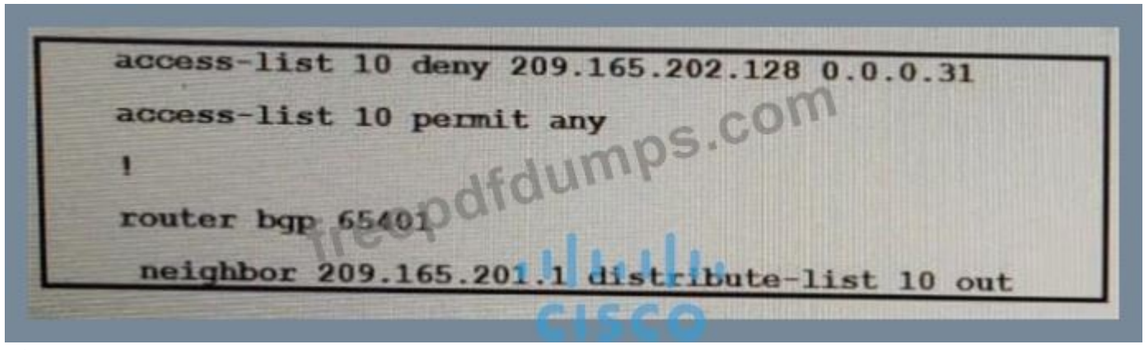
Which configuration completes the change?
A. interface GigabitEthernet2
no ip address
vrf forwarding BLUE
B. interface GigabitEthernet2
no vrf forwarding RED
vrf forwarding BLUE
ip address 10.0.0.0 255.255.255.254
C. interface GigabitEthernet2
no vrf forwarding RED
vrf forwarding BLUE
D. interface GigabitEthernet2
no ip address
ip address 10.0.0.0 255.255.255.254
vrf forwarding BLUE
Answer: B (LEAVE A REPLY)
When assigning an interface to a VRF, the IP address will be removed so we have to reassign the IP address to that interface.

NEW QUESTION: 96
Refer to the exhibit.

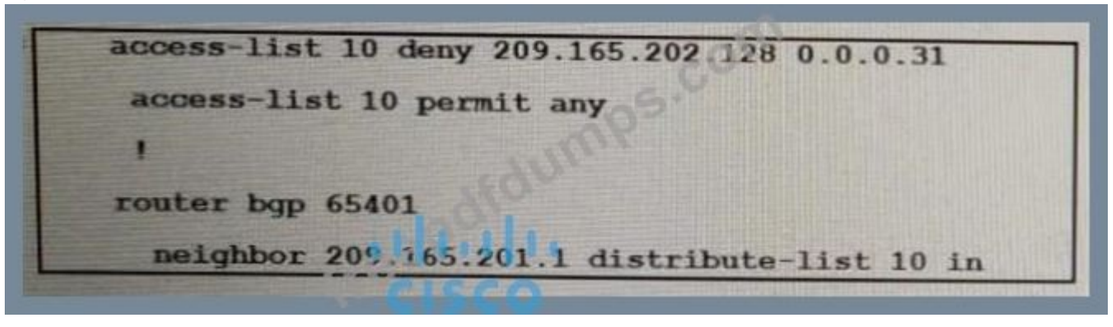


A company with autonomous system number AS65401 has obtained IP address block 209.165.200.224/27 fro, ARIN. The company needed more IP addresses and was assigned block 209.165.202.128/27 from ISP2. An engineer is ISP1 reports they are receiving ISP2 routes from AS65401. Which configuration onR1 resolves the issue?

A)

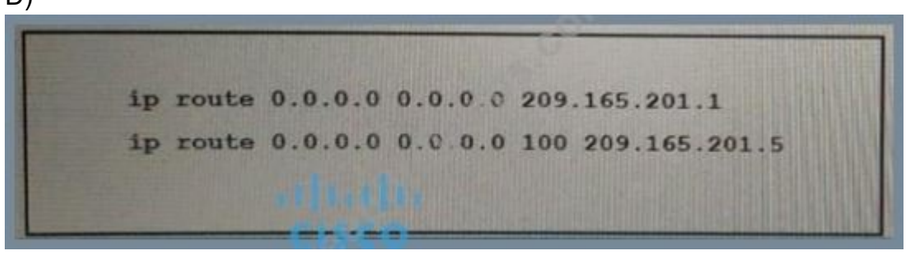


B)



C)

D)



A. Option A

B. Option B

C. Option C

D. Option D

Answer: A (LEAVE A REPLY)

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/23675-27.html

NEW QUESTION: 97

Refer to the exhibit.

```
interface loopback0
ip address 4.4.4.4 255.255.255.0
!
interface FastEthernet1/0
Description **** WAN link ****
ip address 10.0.0.1 255.255.255.0
!
interface FastEthernet1/1
Description **** LAN Network ****
ip address 192.168.1.1 255.255.255.0
!
!
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
network 4.4.4.4 0.0.0.0 area 0
network 10.0.0.1 0.0.0.0 area 0
network 192.168.1.1 0.0.0.0 area 10
!
```

Which set of commands restore reachability to loopback0?

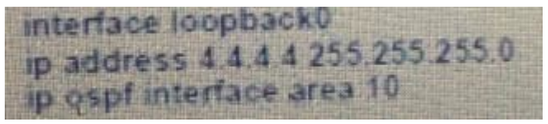
A)

```
interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf network point-to-point
```

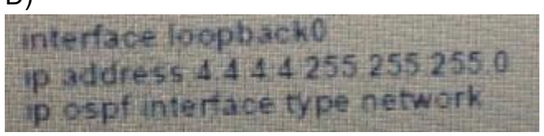
B)

```
interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf network broadcast
```

C)



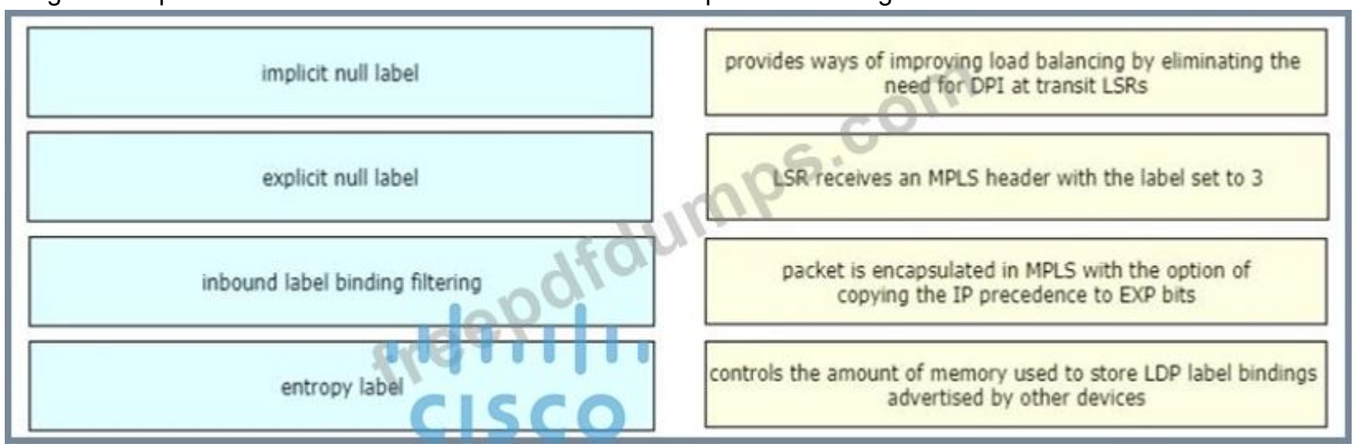
D)



A. Option D
B. Option A
C. Option C
D. Option B
Answer: (SHOW ANSWER)

NEW QUESTION: 98
What is an advantage of implementing BFD?
A. BFD is deployed without the need to run any routing protocol
B. BFD provides faster updates for any flapping route.
C. BFD provides millisecond failure detection
D. BFD provides better capabilities to maintain the routing table
Answer: C (LEAVE A REPLY)

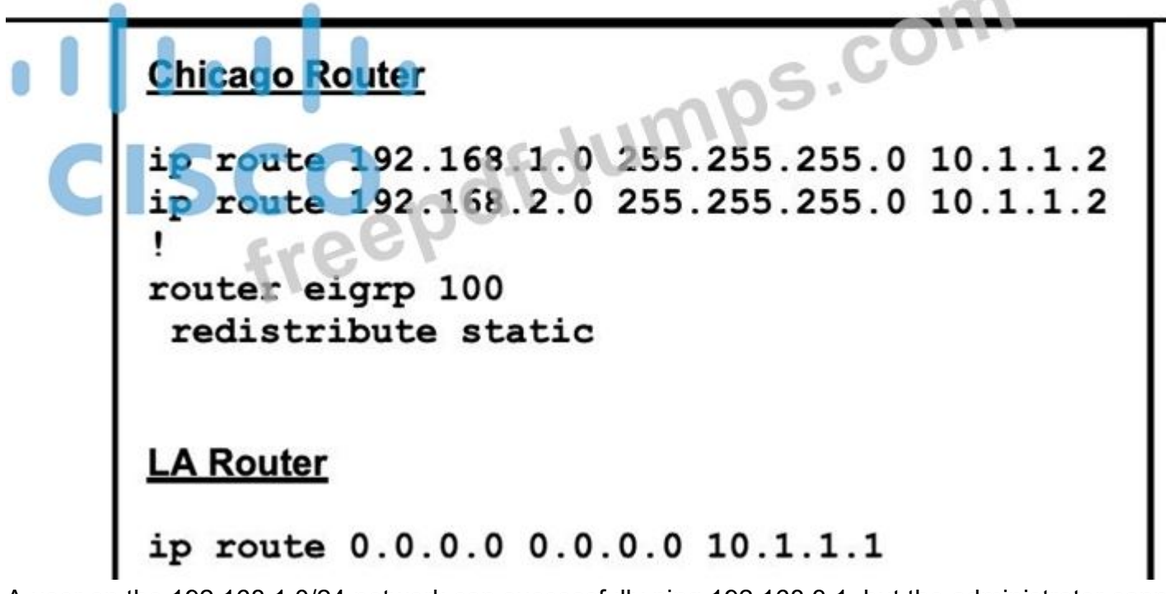
NEW QUESTION: 99
Drag and drop the LDP features from the left onto the descriptions on the right



Answer:

Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/15-sy/mp-ldp-15-sy-boo

NEW QUESTION: 100
Refer to the exhibits.



A user on the 192.168.1.0/24 network can successfully ping 192.168.3.1, but the administrator cannot ping 192.168.3.1 from the LA router. Which set of configurations fixes the issue?
A)

Chicago Router

```
router eigrp 100
 redistribute static metric 10 10 10 10 10
```

B)

Chicago Router

```
router eigrp 100
   redistribute connected
```

C)

Chicago Router

```
ip route 192.168.3.0 255.255.255.0 10.1.2.2
ip route 192.168.4.0 255.255.255.0 10.1.2.2
```

D)

LA Router

```
ip route 192.168.3.0 255.255.255.0 10.1.1.1
ip route 192.168.4.0 255.255.255.0 10.1.1.1
```

A. Option A

B. Option D

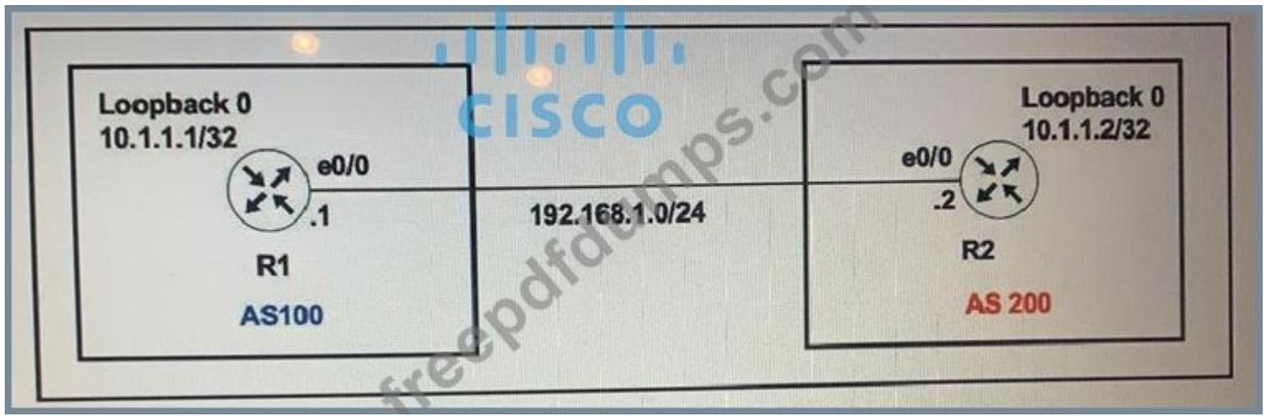
C. Option B

D. Option C

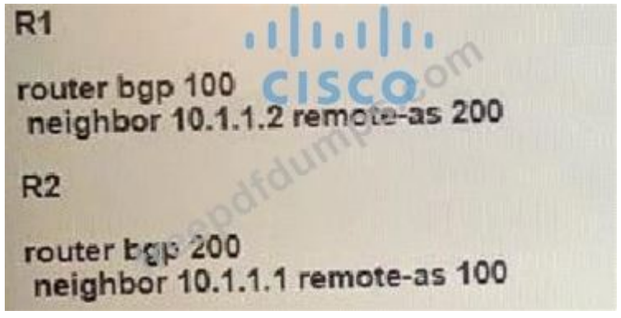
Answer: C (LEAVE A REPLY)

NEW QUESTION: 101

Refer to the exhibit.



The R1 and R2 configurations are:



The neighbor is not coming up. Which two sets of configurations bring the neighbors up? (Choose two.)

A. R2

ip route 10.1.1.1 255.255.255.255 192.168.1.1

!

router bgp 200

neighbor 10.1.1.1 tti-security hops 1

neighbor 10.1.1.1 update-source loopback 0

B. R2

ip route 10.1.1.1 255.255.255.255 192.168.1.1

!

router bgp 200

neighbor 10.1.1.1 disable-connected-check

neighbor 10.1.1.1 update-source loopback 0

C. R2

ip route 10.1.1.2 255.255.255.255 192.168.1.2

!

router bgp 100neighbor 10.1.1.2 ttl-security hops 1

neighbor 10.1.1.2 update-source loopback 0

D. R1

ip route 10.1.1.2 255.255.255.255 192.168.1.2

!

router bgp 100

neighbor 10.1.1.1 ttl-security hops 1

neighbor 10.1.1.2 update-source loopback 0

E. R1

ip route 10.1.1.2 255.255.255.255 192.168.1.2

!

router bgp 100

neighbor 10.1.1.2 disable-connected-check

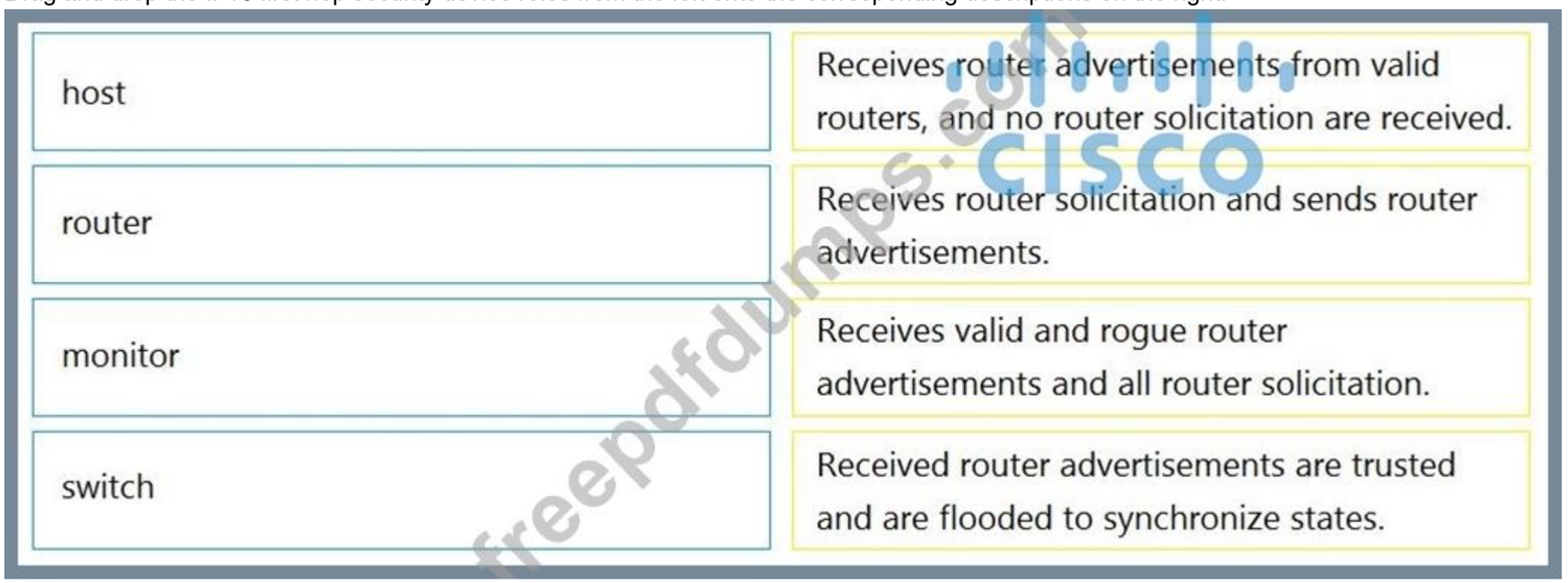
neighbor 10.1.1.2 update-source Loopback0

Answer: B,E (LEAVE A REPLY)

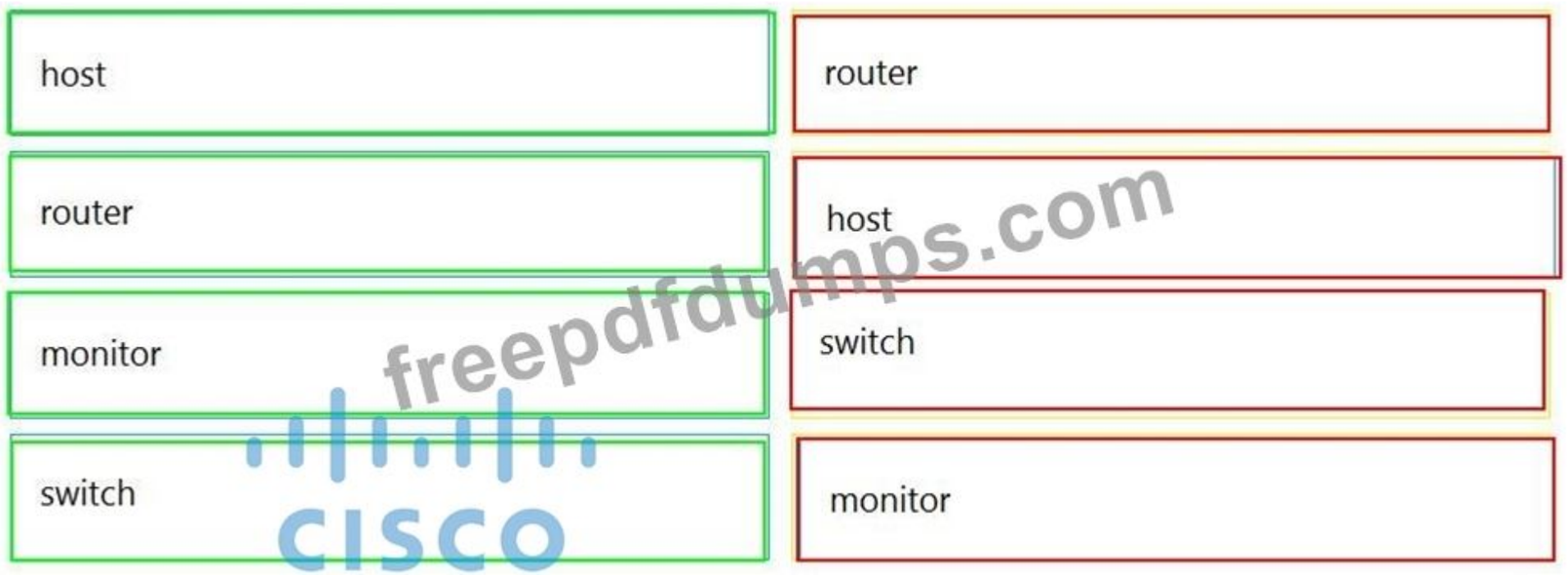
The **neighbor disable-connected-check** command is used to disable the connection verification process for eBGP peering sessions that are reachable by a single hop but are configured on a loopback interface or otherwise configured with a non-directly connected IP address.

NEW QUESTION: 102

Drag and drop the IPv6 first hop security device roles from the left onto the corresponding descriptions on the right.

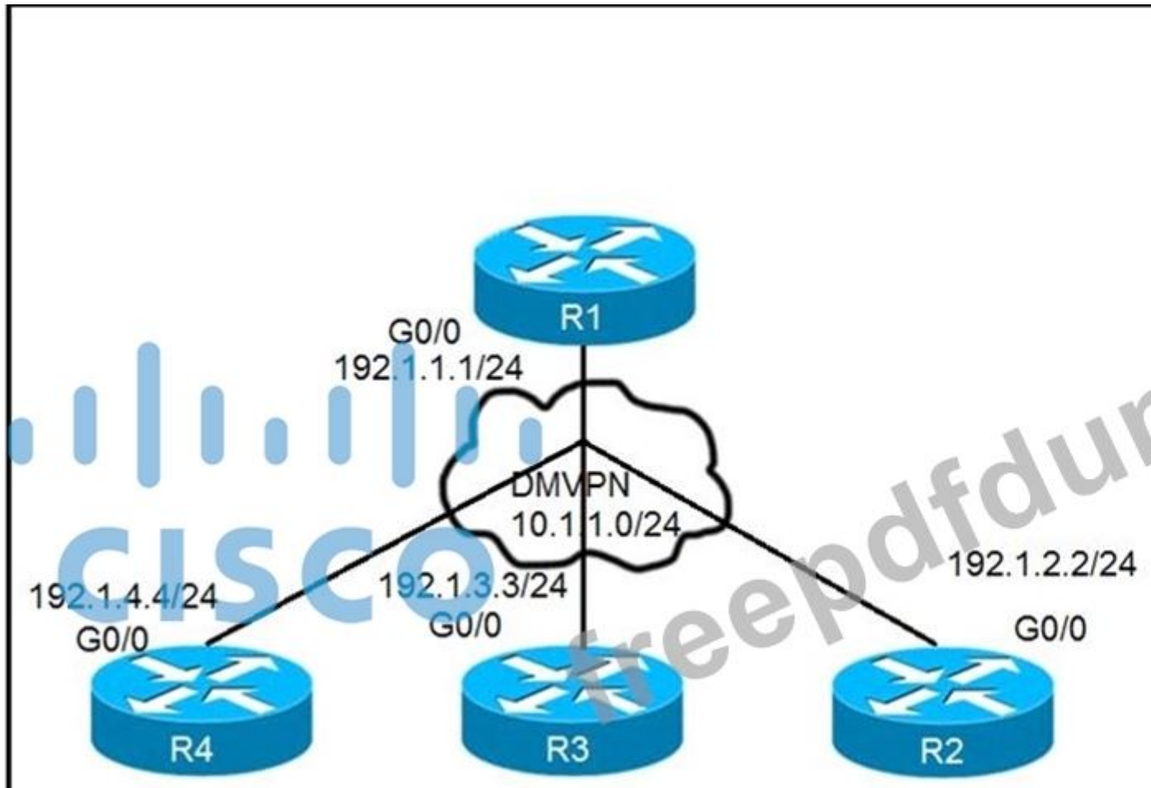


Answer:



Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x_chapter_011011.pdf

NEW QUESTION: 103
Refer to the exhibit.



on R2:
R2(config)# crypto isakmp policy 10
R2(config-isakmp) # hash md5
R2(config-isakmp) # authentication pre-share
R2(config-isakmp) # group 2
R2(config-isakmp)# encryption 3des
R2(config)# crypto isakmp key cisco address 10.1.1.1
R2(config)# crypto ipsec transform-set TSET esp-des esp-md-hmac
R2(cfg-crypto-trans)# mode transport
R2(config)# crypto ipsec profile TST R2 (ipsec-profile) # set transform-set TSET
R2(config)# interface tunnel 123
R2(config-if)# tunnel protection ipsec profile TST

on R3:
R3(config)# crypto isakmp policy 10
R3(config-isakmp) # hash md5
R3(config-isakmp) # authentication pre-share
R3(config-isakmp) # group 2
R3(config-isakmp)# encryption 3des
R3(config)# crypto isakmp key cisco address 10.1.1.1
R3(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R3(cfg-crypto-trans)# mode tunnel
R3(config)# crypto ipsec profile TST R3 (ipsec-profile) + set transform-set TSET
R3(config)# interface tunnel 123
R3(config-if)# tunnel protection ipsec profile TST

After applying IPsec, the engineer observed that the DMVPN tunnel went down, and both spoke-to-spoke and hub were not establishing. Which two actions resolve the issue? (Choose two.)
A. Configure the crypto isakmp key cisco address 192.1.1.1 on R2 and R3
B. Configure the crypto isakmp key cisco address 0.0.0.0 on R2 and R3.
C. Change the mode from mode tunnel to mode transport on R3
D. Change the mode from mode transport to mode tunnel on R2.
E. Remove the crypto isakmp key cisco address 10.1.1.1 on R2 and R3
Answer: A,D (LEAVE A REPLY)
*When using DMVPN with IPSec, it is unnecessary to use tunnel mode. Because DMVPN uses GRE which means that a new IP header is already added by GRE. The GRE encapsulation happens on the tunnel interface before the encryption process takes place.

NEW QUESTION: 104
Refer to the exhibit.

Which action resolves the adjacency issue?

A. Match the hello interval timers.

B. Configure the same EIGRP process IDs.

C. Match the authentication keys.

D. Configure the same autonomous system numbers.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 105

What is an MPLS LDP targeted session?

A. session between neighbors that are connected no more than one hop away

B. LDP session established between LSRs by exchanging TCP hello packets

C. label distribution session between non-directly connected neighbors

D. LDP session established by exchanging multicast hello packets

Answer: (SHOW ANSWER)

NEW QUESTION: 106

An engineer must configure a Cisco router to initiate secure connections from the router to other devices in the network but kept failing. Which two actions resolve the issue? (Choose two.)

A. Configure a source port for the SSH connection to initiate

B. Configure a TACACS+ server and enable it

C. Configure transport input ssh command on the console

D. Configure a domain name

E. Configure a crypto key to be generated

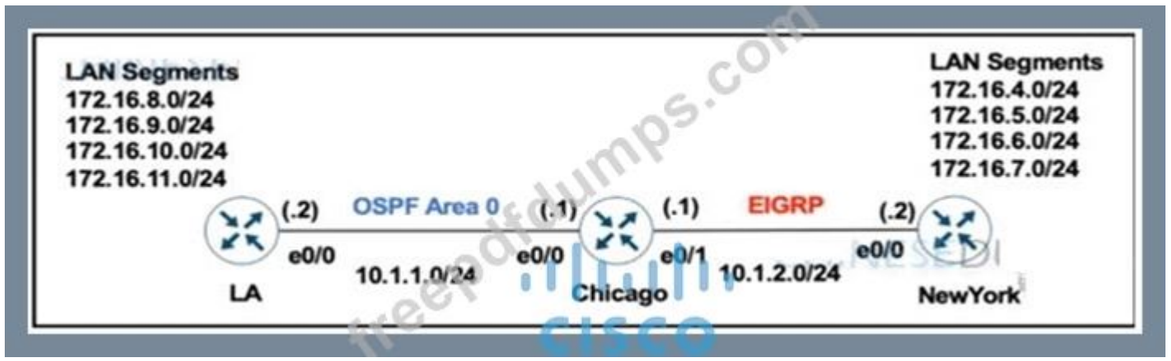
Answer: (SHOW ANSWER)

Follow these guidelines when configuring the switch as an SSH server or SSH client:

+ An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.+ If the SSH server is running on a stack master and the stack master fails, the new stack master uses the RSA key pair generated by the previous stack master

+ If you get CLI error messages after entering the crypto key generate rsa global configuration command, an RSA key pair has not been generated. Reconfigure thehostname and domain, and then enter the crypto key generate rsa command.+ When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the hostname globalconfiguration command.+ When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the ip domain-nameglobal configuration command.+ When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

NEW QUESTION: 107
Refer to the exhibit.



The network administrator configured the Chicago router to mutually redistribute the LA and NewYork routes with OSPF routes to be summarized as a single route in EIGRP using the longest summary mask:

```
router eigrp 100
 redistribute ospf 1 metric 10 10 10 10 10
router ospf 1
 redistribute eigrp 100 subnets
!
interface E 0/0
 ip summary-address eigrp 100 172.16.0.0 255.255.0.0
```

After the configuration, the New York router receives all the specific LA routes but the summary route. Which set of configurations resolves the issue on the Chicago router?

```
interface E 0/1
 ip summary-address eigrp 100 172.16.0.0 255.255.0.0

interface E 0/1
 ip summary-address eigrp 100 172.16.8.0 255.255.252.0

router eigrp 100
 summary-address 172.16.8.0 255.255.252.0

router eigrp 100
 summary-address 172.16.0.0 255.255.0.0
```

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

D. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Refer to the exhibit.

```
R1(config)#ipv6 prefix-list PRE-PEND-PREFIX permit 2001:db8:0:a::/64
R1(config)#route-map PRE-PEND permit 10
R1(config-route-map)#match ipv6 address prefix-list PRE-PEND-PREFIX
R1(config-route-map)#set as-path prepend 65412
R1(config)#router bgp 65412
R1(config-router)#address-family ipv6
R1(config-router-af)#neighbor 2001:db8:0:20::2 route-map PRE-PEND out
```

R1 has a route map configured, which results in a loss of partial IPv6 prefixes for the BGP neighbor, resulting in service degradation. How can the full service be restored?
A. The route map requires a deny 20 statement without set conditions, and this will allow additional prefixes to be advertised.
B. The prefix lit requires all prefixes that R1 is advertising to be added to it, and this will allow additional prefixes to be advertised.
C. The neighbor requires a soft reconfiguration, and this will clear the policy without resetting the BGP TCP connection.
D. The route map requires a permit 20 statement without set conditions, and this will allow additional prefixes to be advertised.
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Refer to the exhibit.

Configuration output:

```
clock timezone PST -8
clock summer-time PDT recurring
service timestamps debug datetime
service timestamps log datetime
logging buffered 16000 debugging
ntp clock-period 17179272
ntp server 161.181.92.152
```

Debug output:

```
router#show clock
14:12:26.312 PDT Thu Apr 27 2019
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#exit

router#
Apr 27 21:12:28: %SYS-5-CONFIG_I: Configured from console by vty0
```

A network administrator configured NTP on a Cisco router to get synchronized time for system and logs from a unified time source The configuration did not work as desired Which service must be enabled to resolve the issue?

A. Enter the service timestamps log datetime localtime global command.

B. Enter the service timestamps log datetime synchronize global command.

C. Enter the service timestamps log datetime console global command.

D. Enter the service timestamps log datetime clock-period global command

Answer: A (LEAVE A REPLY)

If a router is configured to get the time from a Network Time Protocol (NTP) server, the times in the router's log entries may be different from the time on the systemclock if the [localtime] option is not in the service timestamps log command. To solve this issue, add the [localtime] option to the service timestamps log command. Thetimes should now be synchronized between the system clock and the log message timestamps.

NEW QUESTION: 110

Refer to the exhibit.

```
ipv6 access-list INTERNET
 permit ipv6 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA14::/64
 permit tcp 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA13::/64 eq telnet
 permit tcp 2001:DB8:AD59:BA21::/64 any eq http
 permit ipv6 2001:DB8:AD59::/48 any
 deny ipv6 any any log
```

While monitoring VTY access to a router, an engineer notices that the router does not have any filter and anyone can access the router with username and password even though an ACL is configured.

Which command resolves this issue?

A. ipv6 traffic-filter INTERNET in

B. ip access-group INTERNET in

C. ipv6 access-class INTERNET in

D. access-class INTERNET in

Answer: (SHOW ANSWER)

NEW QUESTION: 111

While working with software images, an engineer observes that Cisco DNA Center cannot upload its software image directly from the device. Why is the image not uploading?

A. The device must be resynced to Cisco DNA Center.

B. The software image for the device is in install mode.

C. The device has lost connectivity to Cisco DNA Center.

D. The software image for the device is in bundle mode

Answer: B (LEAVE A REPLY)

Upload Software Images for Devices in Install Mode

The Image Repository page might show a software image as being in Install Mode. When a device is in Install Mode, Cisco DNA Center is unable to upload its software image directly from the device. When a device is in install mode, you must first manually upload the software image to the Cisco DNA Center repository before marking the image as golden, as shown in the following steps.

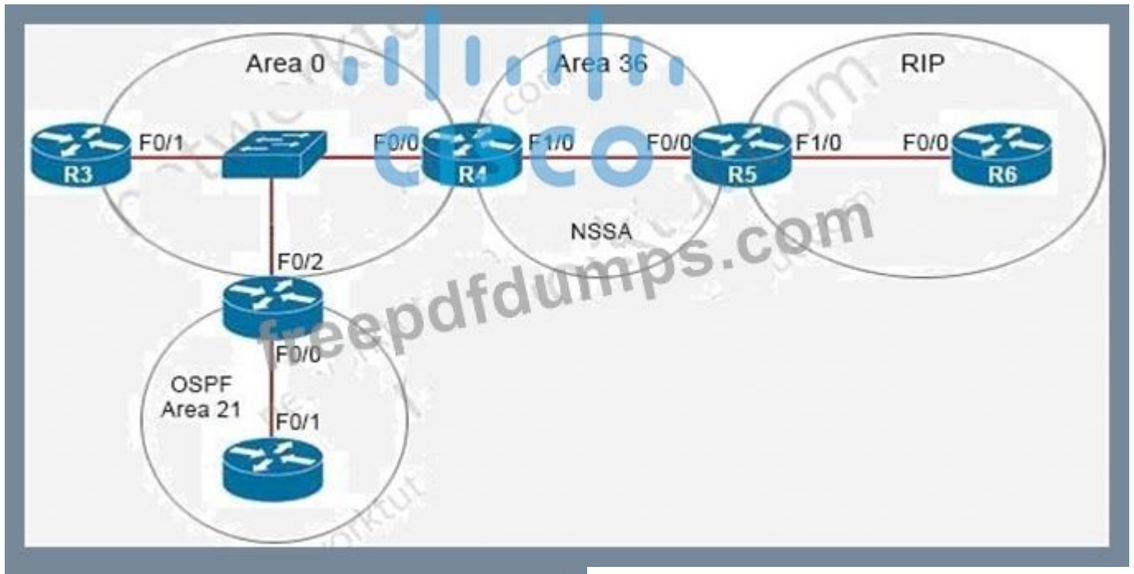
Reference:

dna-center/1-2-10/user_guide/b_cisco_dna_center_ug_1_2_10/

b_dnac_ug_1_2_10_chapter_0100.html

NEW QUESTION: 112

Refer to the exhibit.




```
R5# show ip ospf 1 | begin Area 36
Area 36
Number of interfaces in this area is 2
It is a NSSA area
Area has no authentication
SPF algorithm last executed 00:32:46.376 ago
SFF algorithm executed 13 times
Area ranges are
172.16.0.0/16 Passive Advertise
```

The network engineer configured the summarization of the RIP routes into the OSPF domain on R5 but still sees four different 172.16.0.0/24 networks on R4. Which action resolves the issue?

A. R5(config)#router ospf 1
R5(config-router)#no area
R5(config-router)#summary-address 172.16.0.0 255.255.252.0

B. R4(config)#router ospf 99
R4(config-router)#network 172.16.0.0 0.255.255.255 area 56
R4(config-router)#area 56 range 172.16.0.0 255,255.255.0

C. R4(config)#router ospf 1
R4(config-router)#no area
R4(config-router)#summary-address 172.16.0.0 255.255.252.0

D. R5(config)#router ospf 99
R5(config-router)#network 172.16.0.0 0.255.255.255 area 56
R5(config-router)#area 56 range 172.16.0.0 255.255.255.0

Answer: A (LEAVE A REPLY)

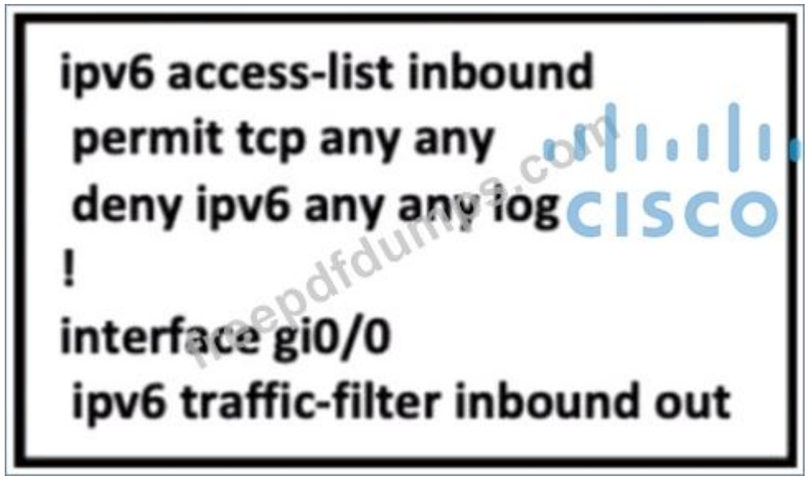
Area 36 is a NSSA so R5 is an ASBR so we can summarize external routes using the "summaryaddress" command. The command "area area-id range" can only be used on ABR so it is not correct. The summarization must be done on the ASBR which is R5, not R4 so the correct answer must be started with "R5(config)#router ospf 1".

Note: The "no area" command is used to remove any existing "area ..." command (maybe "area 56 range ..." command).

NEW QUESTION: 113
What are two MPLS label characteristics? (Choose two.)
A. The label edge router swaps labels on the received packets.
B. An MPLS label is a short identifier that identifies a forwarding equivalence class.
C. Labels are imposed in packets after the Layer 3 header.
D. A maximum of two labels can be imposed on an MPLS packet.
E. LDP uses TCP for reliable delivery of information.
Answer: (SHOW ANSWER)

NEW QUESTION: 114
Which 0S1 model is used to insert an MPLS label?
A. between Layer 2 and Layer 3
B. between Layer 3 and Layer 4
C. between Layer 5 and Layer 6
D. between Layer 1 and Layer 2
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Refer to the exhibit.



Refer to the exhibit. A network administrator configured an IPv6 access list to allow TCP return traffic only, but it is not working as expected. Which changes resolve this issue?
A. ipv6 access-list inbound
permit tcp any any established
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound out
B. ipv6 access-list inbound

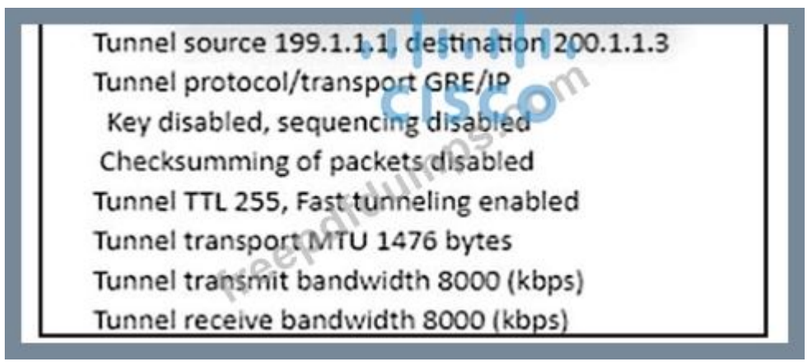
permit tcp any any syn
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound out
C. ipv6 access-list inbound
permit tcp any any syn
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound in
D. ipv6 access-list inbound
permit tcp any any established
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound in
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Refer to the exhibit.

R5 should not receive any routes originated in the EIGRP domain. Which set of configuration changes removes the EIGRP routes from the R5 routing table to fix the issue?
A. R4
route-map O2R deny 10
match tag 111
route-map O2R permit 20
!
router rip
redistribute ospf 1 route-map O2R metric 1

B. R2
route-map E20 deny 20
R4
route-map O2R deny 10
match tag 111
!
router rip
redistribute ospf 1 route-map O2R metric 1
C. R4
route-map O2R permit 10
match tag 111
route-map O2R deny 20
!
router rip
redistribute ospf 1 route-map O2R metric 1
D. R4
route-map O2R deny 10
match tag 111
!
router rip
redistribute ospf 1 route-map O2R metric 1
Answer: A (LEAVE A REPLY)
In this question, routes from EIGRP domain are redistributed into OSPF (with tag 111) then RIPv2 but without any filtering so R5 learns all routes from both EIGRP and OSPF domain. If we only want R5 to learn routes from OSPF domain then we must filter out routes with tag 111 and permit other routes.
The line "route-map O2R permit 20" is important to allow other routes because of the implicit deny all at the end of each route-map.

NEW QUESTION: 117
Refer to the exhibit.



An engineer must establish a point-to-point GRE VPN between R1 and the remote site. Which configuration accomplishes the task for the remote site?
A. Interface Tunnel
lunnel source 199.1.1.1
tunnel destination 200.1.1.3

ip address 192.168.1.1.255.255.255.0
B. Interface Tunnel1
tunnel source 200.1.1.3
tunnel destination 199.1.1.1
ip address 192.168.1.1.255.255.255.0
C. Interface Tunnel1
tunnel source 200.1.1.3
tunnel destination 199.1.1.1
ip address 192.168.1.3.255.255.255.0
D. Interface Tunnel1
tunnel source 199.1.1.1
tunnel destination 200.1.1.3
ip address 192.168.1.3 255.255.255.0
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Refer to the exhibit.

```
Router#show ip route
<output omitted>
Gateway of last resort is not set

      192.168.1.0/32 is subnetted, 1 subnets
O        192.168.1.1 [110/11] via 192.168.12.1, 16:56:40, Ethernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Loopback0
L        192.168.2.2/32 is directly connected, Loopback0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Ethernet0/1
L        192.168.3.1/32 is directly connected, Ethernet0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Ethernet0/0
L        192.168.12.2/32 is directly connected, Ethernet0/0
Router#show running-config | section ospf
router ospf 1
 summary-address 10.0.0.0 255.0.0.0
 redistribute static subnets
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
Router#
```

An engineer is trying to generate a summary route in OSPF for network 10.0.0.0/8, but the summary route does not show up in the routing table. Why is the summary route missing?

A. The summary-address command is used only for summarizing prefixes between areas.

B. The summary route is visible only in the OSPF database, not in the routing table.

C. There is no route for a subnet inside 10.0.0.0/8, so the summary route is not generated.

D. The summary route is not visible on this router, but it is visible on other OSPF routers in the same area.

Answer: C (LEAVE A REPLY)

The -summary-address is only used to create aggregate addresses for OSPF at an autonomous system boundary. It means this command should only be used on the ASBR when you are trying to summarize externally redistributed routes from another protocol domain or you have a NSSA area. But a requirement to create a summarized route is:

-The ASBR compares the summary route's range of addresses with all routes redistributed into OSPF on that ASBR to find any subordinate subnets (subnets that sit inside the summary route range). If at least one subordinate subnet exists, the ASBR advertises the summary route.

NEW QUESTION: 119

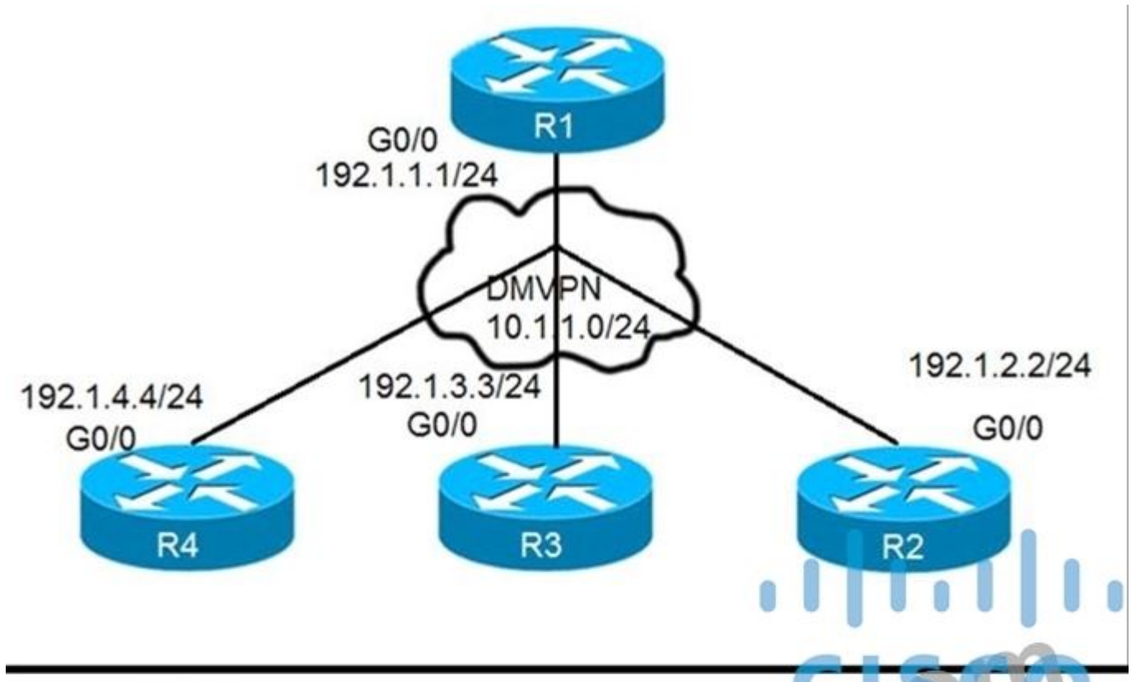
Which two components are required for MPLS Layer 3 VPN configuration? (Choose two)

A. Use OSPF between PE and CE

B. Use MP-BGP for customer routes

C. Use a unique RD per customer VRF
D. Use LDP for customer routes
E. Use pseudowire for Layer 2 routes
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 120
Refer to the exhibits.



On R1:
R1(config)# interface tunnel 1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# tunnel source 192.1.1.1
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# ip nhrp network-id 111

On R2:
R2(config)# interface tunnel 1
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# tunnel source FastEthernet0/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# ip nhrp network-id 222
R2(config-if)# ip nhrp nhs 10.1.1.1
R2(config-if)# ip nhrp map 10.1.1.1 192.1.1.1

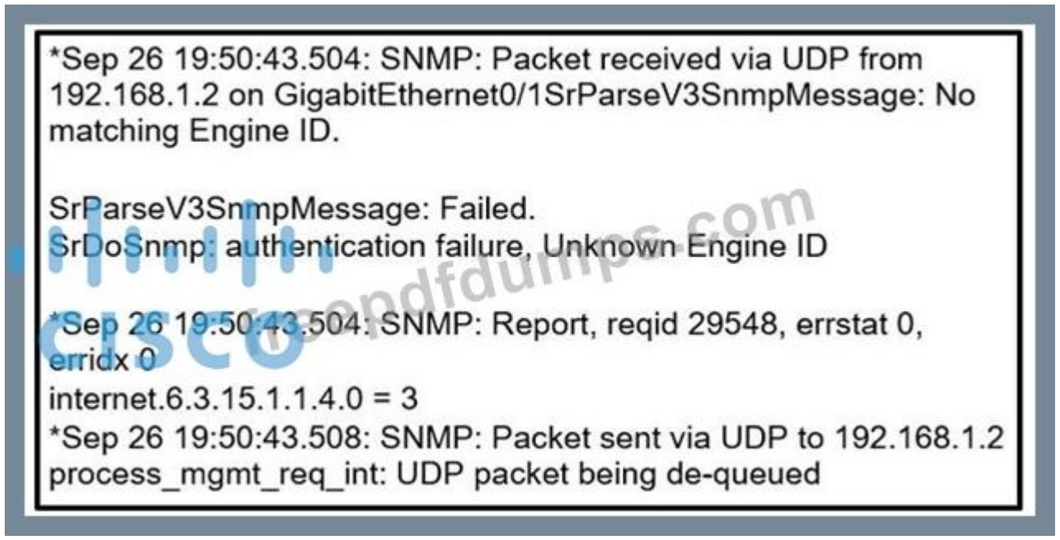
On R3:
R3(config)# interface tunnel 1
R3(config-if)# ip address 10.1.1.3 255.255.255.0
R3(config-if)# tunnel source FastEthernet0/0
R3(config-if)# tunnel mode gre multipoint
R3(config-if)# ip nhrp network-id 333 R3(config-if)# ip nhrp nhs 10.1.1.1
R3(config-if)# ip nhrp map 10.1.1.1 192.1.1.1

On R4: R4(config)# interface tunnel 1
R4(config-if)# ip address 10.1.1.4 255.255.255.0
R4(config-if)# tunnel source FastEthernet0/0
R4(config-if)# tunnel mode gre multipoint
R4(config-if)# ip nhrp network-id 444
R4(config-if)# ip nhrp nhs 10.1.1.1
R4(config-if)# ip nhrp map 10.1.1.1 192.1.1.1

Phase-3 tunnels cannot be established between spoke-to-spoke in DMVPN. Which two commands are missing? (Choose two.)

A. The ip nhrp shortcut commands is missing on the hub router.
B. The ip nhrp shortcut command is missing on the spoke routers.
C. The ip nhrp redirect commands is missing on the hub router.
D. The ip nhrp redirect command is missing on the spoke routers.
E. The ip nhrp map command is missing on the hub router.
Answer: B,C (LEAVE A REPLY)

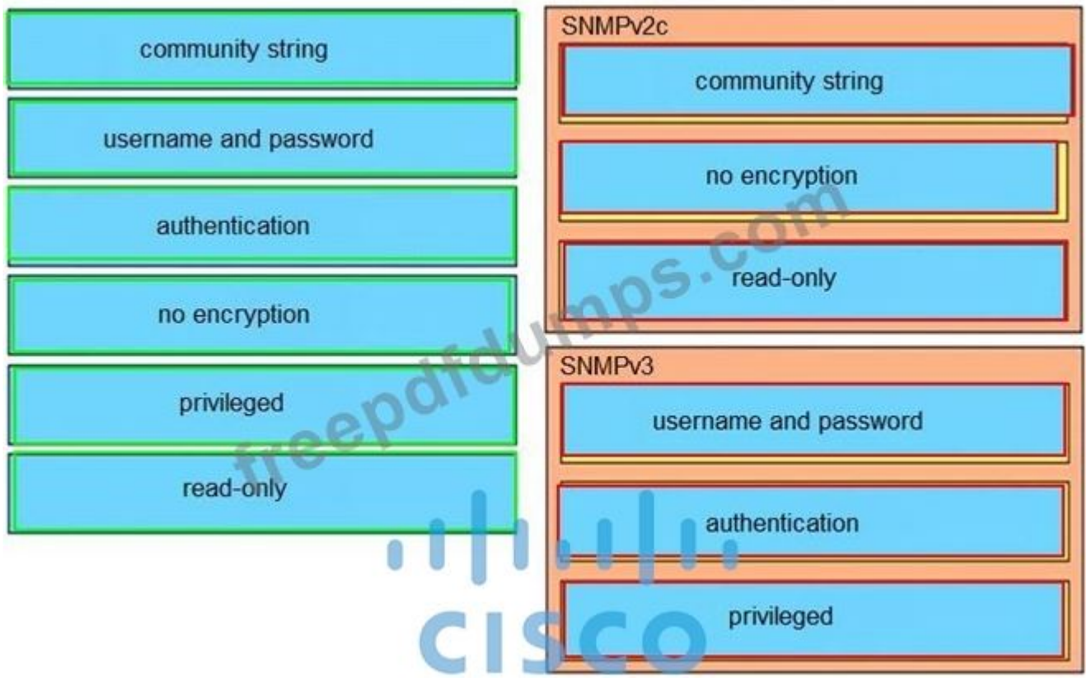
NEW QUESTION: 121
Refer to the exhibit.



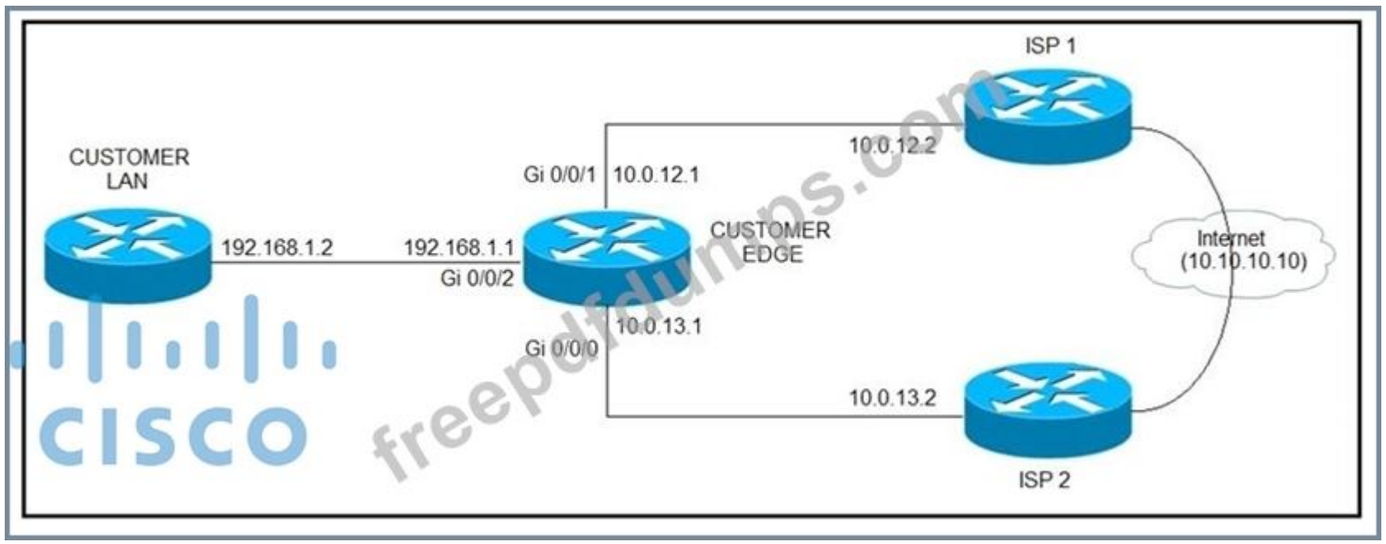
Which two commands provide the administrator with the information needed to resolve the issue? (Choose two.)
A. snmp user
B. debug snmpv3 engine-id
C. debug snmp packet
D. showsnmpv3 user
E. debug snmp engine-id
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 122
Drag and drop the SNMP attributes in Cisco IOS devices from the left onto the correct SNMPv2c or SNMPV3 categories on the right.

Answer:



NEW QUESTION: 123
Refer to the exhibit.



ISP 1 and ISP 2 directly connect to the Internet. A customer is tracking both ISP links to achieve redundancy and cannot see the Cisco IOS IP SLA tracking output on the router console. Which command is missing from the IP SLA configuration?

A. Start-time now

B. Start-time 0

C. Start-time immediately

D. Start-time 00:00

Answer: A (LEAVE A REPLY)

NEW QUESTION: 124

After some changes in the routing policy, it is noticed that the router in AS 45123 is being used as a transit AS router for several service provides. Which configuration ensures that the branch router in AS 45123 advertises only the local networks to all SP neighbors?

A)

```
ip as-path access-list 1 permit  ^45123
!
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

B)

```
ip as-path access-list 1 permit .*
!
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

C)

```
ip as-path access-list 1 permit ^45123$
!
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

D)

```
ip as-path access-list 1 permit ^$
!
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

A. Option A

B. Option B
C. Option C
D. Option D
Answer: (SHOW ANSWER)
By default BGP advertises all prefixes to external BGP neighbors. This means that if you are multi-homed (connected to two or more ISPs) then you might become a transit AS. For example, ISP 2 in AS 200 can send traffic to your router in AS 100 to reach ISP 3 in AS 300 because you advertised prefixes in ISP 3 to ISP 2.
This is what will be seen in the BGP routing table of ISP1:

```
ISP1#show ip bgp
--output omitted--
 Network          Next Hop            Metric LocPrf Weight Path
....
*> 3.3.3.0/24     192.168.12.1                           0 100 300 i
```

NEW QUESTION: 125
Refer to the exhibit.

```
R1#show running-config | include aaa
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login Console local
R1#show running-config | section line
line con 0
 logging synchronous
R1#
```

An engineer is trying to configure local authentication on the console line, but the device is trying to authenticate using TACACS+. Which action produces the desired configuration?
A. Add the aaa authentication login default none command to the global configuration.
B. Replace the capital "C" with a lowercase "c" in the aaa authentication login Console local command.
C. Add the aaa authentication login default group tacacs+ local-case command to the global configuration.
D. Add the login authentication Console command to the line configuration
Answer: D (LEAVE A REPLY)
Reference:
https://community.cisco.com/t5/switching/how-to-define-login-local-for-console-0/td-p/2949493

NEW QUESTION: 126
Refer to Exhibit.

```
ip dhcp excluded-address 172.16.16.1 172.16.16.2
!
ip dhcp pool 0
 network 172.16.16.0 255.255.255.0
 domain-name cisco.com
 dns-server 172.16.16.2
 lease 30


interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.252
 ip access-group 100 in


access-list 100 deny   udp any any
access-list 100 permit ip any any
```

Which two configurations allow clients to get dynamic ip addresses assigned?

A. Configure access-list 100 permit udp any any eq 61 as the first line

B. Configure access-list 100 permit udp any any eq 86 as the first line

C. Configure access-list 100 permit udp any any eq 68 as the first line

D. Configure access-list 100 permit udp any any eq 69 as the first line

E. Configure access-list 100 permit udp any any eq 67 as the first line

Answer: C,E (LEAVE A REPLY)

A DHCP server that receives a DHCPDISCOVER message may respond with a DHCPOFFER message on UDP port 68 (BootP client).

...

In the event that the DHCP server is not on the local subnet, the DHCP server will send the DHCPOFFER, as a unicast packet, on UDP port 67, back to the DHCP/BootPRelay Agent from which the DHCPDISCOVER came.

NEW QUESTION: 127

Refer to the exhibit.

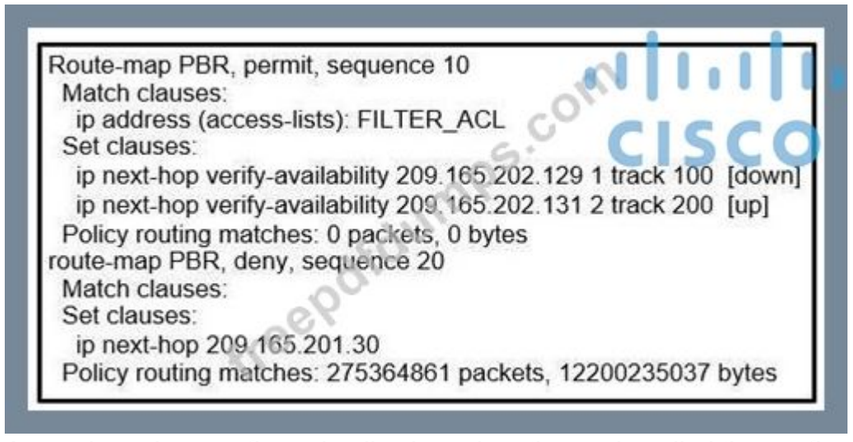
```
CPE# show ntp associations

  address         ref clock       st   when   poll reach  delay
offset   disp
 ~10.1.255.40     .INIT.          16      -     64     0    0.000
0.000 15937.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker,
~ configured

CPE# debug ip icmp
*Feb 20 22:49:32.913: ICMP: dst (10.0.12.1) port unreachable rcv
from 10.1.255.40
*Feb 20 22:50:37.918: ICMP: dst (10.0.12.1) port unreachable rcv
from 10.1.255.40
*Feb 20 22:51:44.951: ICMP: dst (10.0.12.1) port unreachable rcv
from 10.1.255.40
```

An administrator is troubleshooting a time synchronization problem for the router time to another Cisco IOS XE-based device that has recently undergone hardening. Which action resolves the issue?

A. Allow NTP in the ingress ACL on 10.1.255.40 by permitting TCP destined to port 123.

B. Allow NTP in the ingress ACL on 10.1.225.40 by permitting UDP destined to port 123.
C. Ensure that he CPE router has a valid route to 10.1.255. 40 for NTP and rectify if not reachable.
D. NTP service is disabled and must be enabled on 10.1.225.40.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128
Refer to the exhibit.



An engineer has configured policy-based routing and applied the configured to the correct interface. How is the configuration applied to the traffic that matches the access list?
A. It is dropped.
B. It is forwarded using the routing table lookup.
C. It is sent to 209.165.202.129.
D. It is sent to 209.165.202.131.
Answer: (SHOW ANSWER)

NEW QUESTION: 129
A network administrator must optimize the segment size of the TCP packet on the DMVPN IPsec protected tunnel interface, which carries application traffic from the head office to a designated branch. The TCP segment size must not overwhelm the MTU of the outbound link. Which configuration must be applied to the router to improve the application performance?

A. Option C
B. Option B
C. Option D
D. Option A
Answer: A (LEAVE A REPLY)

NEW QUESTION: 130
Refer to the exhibit.

```
ipv6 dhcp pool DHCPPOOL
address prefix 2001:0:1:4::/64 lifetime infinite infinite

interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.240
duplex auto
speed auto
ipv6 address 2001:0:1:4::1/64
ipv6 enable
ipv6 nd ra suppress
ipv6 ospf 1 area 1
ipv6 dhcp server DHCPPOOL
```

Reachability between servers in a network deployed with DHCPv6 is unstable. Which command must be removed from the configuration to make DHCPv6 function?

A. address prefix 2001:0:1:4::/64 lifetime infinite infinite

B. ipv6 nd ra suppress

C. ipv6 address 2001:0:1:4::/64

D. ipv6 dhcp server DHCPPOOL

Answer: B (LEAVE A REPLY)

NEW QUESTION: 131

Refer to Exhibit.

```
Ipv6 unicast-routing
!
Router ospfv3 4
    Router-id 192.168.1.1
 !
Interface E 0/0
 Ipv6 enable
 Ip address 10.1.1.1 255.255.255.0
 Ospfv3 4 area 0 ipv4
 No shut
!
Interface Loopback0
 Ipv6 enable
 Ipv4 172.16.1.1 255.255.255.0
 Ospfv3 4 area 0 ipv4
```

The network administrator configured the branch router for IPv6 on the E0/0 interface. The neighboring router is fully configured to meet requirements, but the neighbor relationship is not coming up. Which action fixes the problem on the branch router to bring the IPv6 neighbors up?

A. Enable the IPv4 address family under the router ospfv3 4 process by using the address-family ipv4 unicast command

B. Disable IPv6 on the E0/0 interface using the no ipv6 enable command
C. Enable the IPv4 address family under the E0/0 interface by using the address-family ipv4 unicast command
D. Disable OSPF for IPv4 using the no ospfv3 4 area 0 ipv4 command under the E0/0 interface
Answer: A (LEAVE A REPLY)
Once again, Cisco changed the IOS configuration commands required for OSPFv3 configuration. The new OSPFv3 configuration uses the "ospfv3" keyword instead of the earlier "ipv6 router ospf" routing process command and "ipv6 ospf" interface commands.
The Open Shortest Path First version 3 (OSPFv3) address families feature enables both IPv4 and IPv6 unicast traffic to be supported. With this feature, users may have two processes per interface, but only one process per address family (AF).

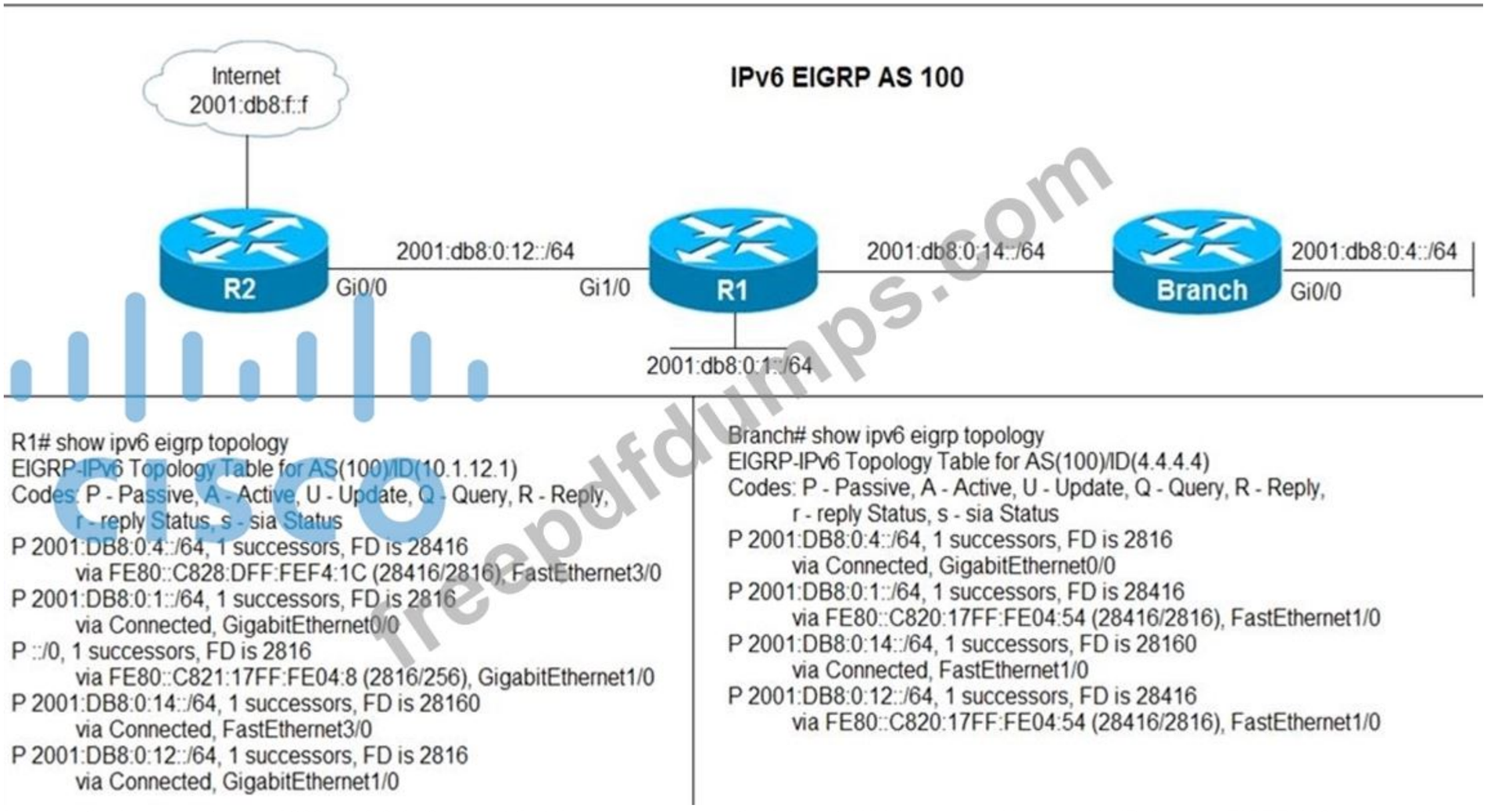
NEW QUESTION: 132
Refer to the exhibit.

```
Router#show access-lists
Standard IP access list 1
        10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, deny, sequence 10
  Match clauses:
        ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
   network 192.168.1.1 0.0.0.0 area o
   network 192.168.12.0 0.0.0.255 area 0
   distribute-list route-map RM-OSPF-DL in
Router#
```

Which two actions should be taken to access the server? (Choose two.)
A. Modify distribute list seq 10 to permit the route to 192.168.2.2.
B. Modify the access list to deny the route to 192.168.2.2.
C. Add a sequence 20 in the route map to permit access list 1.
D. Add a floating static route to reach to 192.168.2.2 with administrative distance higher than OSPF
E. Modify the access list to add a second line of permit ip any

Answer: (SHOW ANSWER)

NEW QUESTION: 133
Refer to the exhibit.



Users in the branch network of 2001:db8:0:4::/64 report that they cannot access the Internet. Which command is issued in IPv6 router EIGRP 100 configuration mode to solve this issue?

A. Issue the eigrp command on R2.

B. Issue the no neighbor stub command on R2.

C. Issue the no eigrp stub command on R1.

D. Issue the eigrp stub command on R1

Answer: (SHOW ANSWER)

NEW QUESTION: 134
The network administrator configured R1 for Control Plane Policing so that the inbound Telnet traffic is policed to 100 kbps. This policy must not apply to traffic coming in from 10.1.1.1/32 and 172.16.1.1/32. The administrator has configured this:

```
access-list 101 permit tcp host 10.1.1.1 any eq 23
access-list 101 permit tcp host 172.16.1.1 any eq 23
!
class-map CoPP-TELNET
match access-group 101
!
policy-map PM-CoPP
class CoPP-TELNET
police 100000 conform transmit exceed drop
!
control-plane
service-policy input PM-CoPP
```


The network administrator is not getting the desired results. Which set of configurations resolves this issue?

A. control-plane
no service-policy input PM-CoPP
!
interface Ethernet 0/0
service-policy input PM-CoPP

B. control-plane
no service-policy input PM-CoPP
service-policy input PM-CoPP

C. no access-list 101
access-list 101 deny tcp host 10,1,1.1 any eq 23
access-list 101 deny tcp host 172,16.1.1 any eq 23
access-list 101 permit ip any any

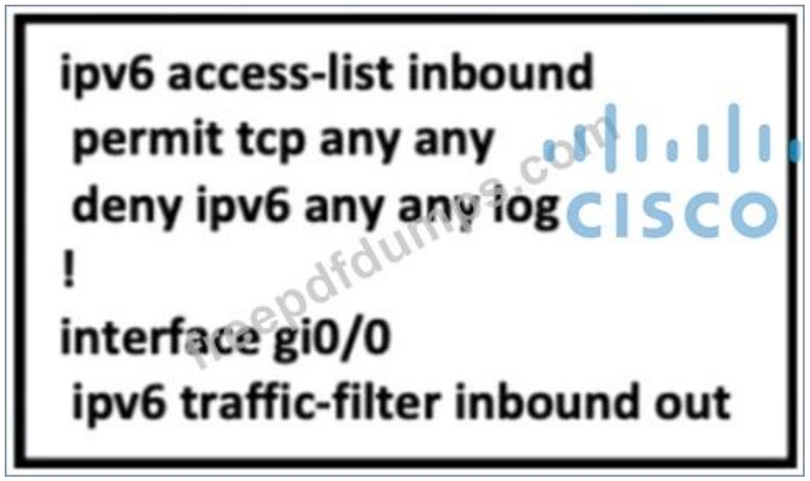
D. no access-list 101
access-list 101 deny tcp host 10,1.1.1 any eq 23
access-list 101 deny tcp host 172.16.1.1 any eq 23
access-list 101 permit ip any any
!

Answer: C (LEAVE A REPLY)

interface E0/0
service-policy input PM-CoPP

Explanation:
Packets that match a deny rule are excluded from that class and cascade to the next class (if one exists) for classification. Therefore if we don't want to CoPP traffic from 10.1.1.1/32 and 172.16.1.1/32, we must "deny" them in the ACL.

NEW QUESTION: 135
Refer to the exhibit.



A network administrator configured an IPv6 access list to allow TCP return frame only, but it is not working as expected. Which changes resolve this issue?

A. Option A

B. Option B

C. Option C

D. Option D
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/122_55_se/configuration/guide/scg3750/swv6acl.html

NEW QUESTION: 136
Which list defines the contents of an MPLS label?
A. 20-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL
B. 32-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL
C. 20-bit label; 3-bit flow label; 1-bit bottom stack; 8-bit hop limit
D. 32-bit label; 3-bit flow label; 1-bit bottom stack; 8-bit hop limit
Answer: (SHOW ANSWER)
The first 20 bits constitute a label, which can have 2^20 values. Next comes 3 bit value called Traffic Class. It was formerly called as experimental (EXP) field. Now it has been renamed to Traffic Class (TC). This field is used for QoS related functions. Ingress router can classify the packet according to some criterion and assign a 3 bit value to this filed. If an incoming packet is marked with some IP Precedence or DSCP value and the ingress router may use such a field to assign an FEC to the packet. Next bit is Stack bit which is called bottom-of-stack bit. This field is used when more than one label is assigned to a packet, as in the case of MPLS VPNs or MPLS TE. Next byte is MPLS TTL field which serves the same purpose as that of IP TTL byte in the IP header

NEW QUESTION: 137
Refer to the exhibit.

```
Ipv6 unicast-routing
!
Router ospfv3 4
    Router-id 192.168.1.1
 !
Interface E 0/0
 Ipv6 enable
 Ip address 10.1.1.1 255.255.255.0
 Ospfv3 4 area 0 ipv4
 No shut
!
Interface Loopback0
 Ipv6 enable
 Ipv4 172.16.1.1 255.255.255.0
 Ospfv3 4 area 0 ipv4
```


The network administrator configured the branch router for IPv6 on the E 0/0 interface The neighboring router is fully configured to meet requirements, but the neighbor relationship is not coming up.
Which action fixes the problem on the branch router to bring the IPv6 neighbors up?

A. Enable the IPv4 address family under the E 0/0 interface by using the address-family Ipv4 unicast command
B. Disable IPv6 on the E 0/0 interface using the no ipv6 enable command
C. Enable the IPv4 address family under the router ospfv3 4 process by using the address-family ipv4 unicast command
D. Disable OSPF for IPv4 using the no ospfv3 4 area 0 ipv4 command under the E 0/0 interface.

Answer: C (LEAVE A REPLY)

Once again, Cisco changed the IOS configuration commands required for OSPFv3 configuration. The new OSPFv3 configuration uses the "ospfv3" keyword instead ofthe earlier "ipv6 router ospf" routing process command and "ipv6 ospf" interface commands.
The Open Shortest Path First version 3 (OSPFv3) address families feature enables both IPv4 and IPv6 unicast traffic to be supported. With this feature, users may havetwo processes per interface, but only one process per address family (AF).

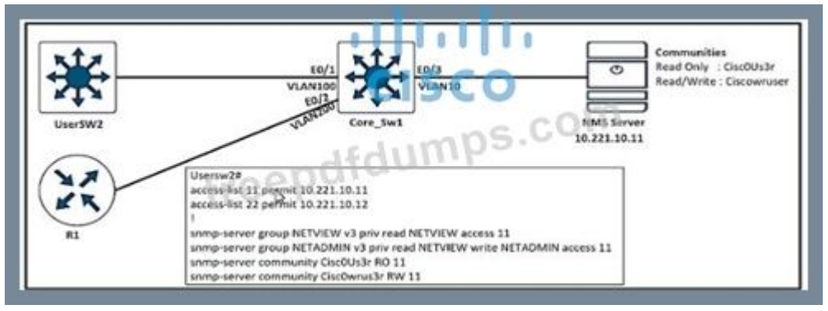
NEW QUESTION: 138

Which two statements about VRF-Lite configurations are true? (Choose two.)

A. They support the exchange of MPLS labels
B. Each customer has its own dedicated TCAM resources
C. They support IS-IS
D. Each customer has its own private routing table.
E. Different customers can have overlapping IP addresses on different VPNs
F. They support a maximum of 512.000 routes

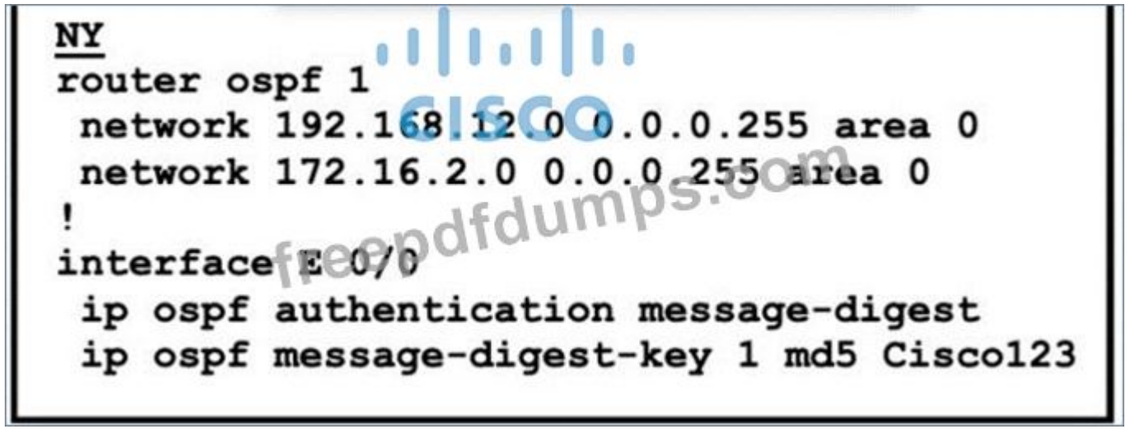
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 139
Refer to the exhibit.



Refer to the exhibit. An engineer configured SNMP Commimes on UserSW2 switch, but the SNMP server cannot upload modified configurations to the switch. Which configuration resolves this issue?
A. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22
B. snmp-server group NETVIEW v2c priv read NETVIEW access 11
C. snmp-server community Ciscowruser RW 11
D. snmp-server community CiscOUs3r RW 11
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140
Refer to the exhibit.

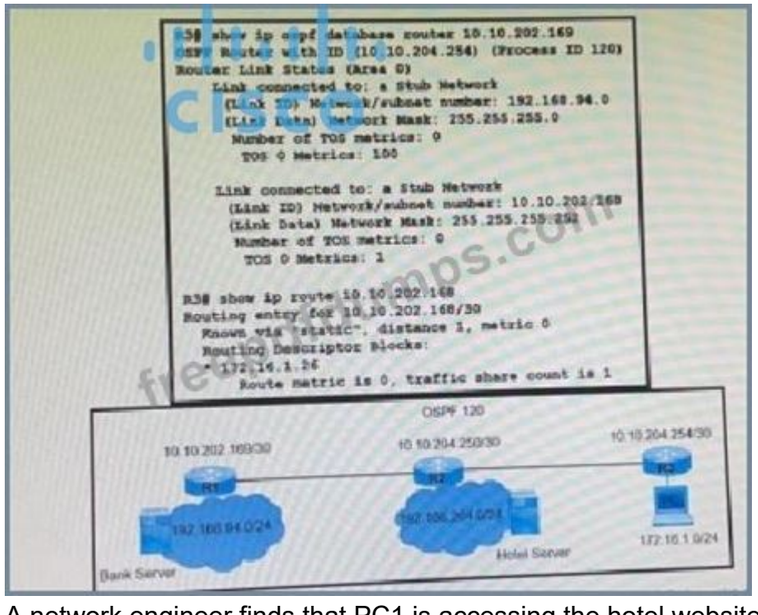


The neighbor relationship is not coming up Which two configurations bring the adjacency up? (Choose two)
A. NY
router ospf 1
area 0 authentication message-digest
B. LA
interface E 0/0
ip ospf message-digest-key 1 md5 Cisco123
C. NY
interface E 0/0
no ip ospf message-digest-key 1 md5 Cisco123

ip ospf authentication-key Cisco123
D. LA
interface E 0/0
ip ospf authentication-key Cisco123
E. LA
router ospf 1
area 0 authentication message-digest
Answer: (SHOW ANSWER)
The configuration on NY router is good for OSPF authentication. So we must enable OSPF authentication on LA router with the following commands:
router ospf 1
area 0 authentication message-digest
interface E0/0
ip ospf message-digest-key 1 md5 Cisco123

NEW QUESTION: 141
Which two solutions are used to overcome a flapping link that causes a frequent label binding exchange between MPLS routers? (Choose two)
A. Create link dampening on links to protect the session.
B. Increase input queue on links to protect the session.
C. Create targeted hellos to protect the session.
D. Increase a hold-timer to protect the session.
E. Increase a session delay to protect the session.
F. When a link flaps (for a short time),
Answer: (SHOW ANSWER)
...
Solution:
+ When LDP session supported by link hello is setup, create a targeted hello to protect the session.
Explanation:
To avoid having to rebuild the LDP session altogether, you can protect it. When the LDP session between two directly connected LSRs is protected, a targeted LDP session is built between the two LSRs. When the directly connected link does go down between the two LSRs, the targeted LDP session is kept up as long as an alternative path exists between the two LSRs.
For the protection to work, you need to enable it on both the LSRs. If this is not possible, you can enable it on one LSR, and the other LSR can accept the targeted LDP Hellos by configuring the command mpls ldp discovery targeted-hello accept.
Reference:
Or from the reference
at https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/TECMPL-3201.pdf Troubleshooting LDP Issues Problem:

NEW QUESTION: 142
Refer to the exhibit.



A network engineer finds that PC1 is accessing the hotel website to do the booking but fails to make payment. Which action resolves the issue?

A. Decrease the AD to 5 OSPF route 192.168.94.0 on R1.

B. Allow stub network 10.10.202.168/30 on router R3 OSPF.

C. Increase the AD to 200 of static route 192.168.94.0 on R3.

D. Configure a reverse route on R1 for PC1 172.16.1.0/24.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 143

Which IGPs are supported by the MPLS LDP autoconfiguration feature?

A. RIPv2 and OSPF

B. OSPF and EIGRP

C. OSPF and ISIS

D. ISIS and RIPv2

Answer: (SHOW ANSWER)

The MPLS LDP Autoconfiguration feature enables you to globally enable Label Distribution Protocol (LDP) on every interface associated with an Interior Gateway Protocol (IGP) instance. This feature is supported on Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) IGPs. It provides

NEW QUESTION: 144

Which transport layer protocol is used to form LDP sessions?

A. UDP

B. SCTP

C. TCP

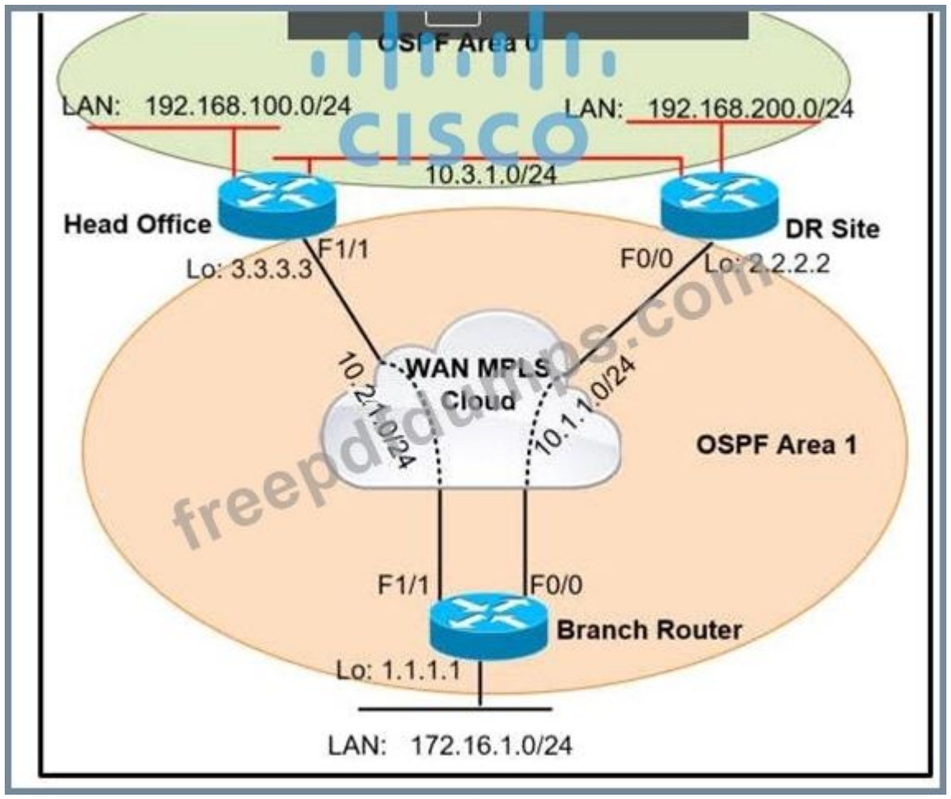
D. RDP

Answer: C (LEAVE A REPLY)

LDP multicasts hello messages to a well-known UDP port (646) in order to discover neighbors. Once the discovery is accomplished, a TCP connection (port 646) is established and the LDP session begins. LDP keepalives ensure the health of the session. Thanks to the LDP session, LDP messages create the label mappings required for a FEC. Withdraw messages are used when FECs need to be torn down.

NEW QUESTION: 145
An engineer received a ticket about a router that has reloaded. The monitoring system graphs show different traffic patterns between logical and physical interfaces when the router is rebooted. Which action resolves the issue?
A. Configure the snmp ifindex persist command on the physical interfaces.
B. Configure the snmp ifindex persist command globally.
C. Clear the logical interfaces with snmp ifindex clear command
D. Trigger a new snmpwalk from the monitoring system to synchronize interface OIDs
Answer: B (LEAVE A REPLY)

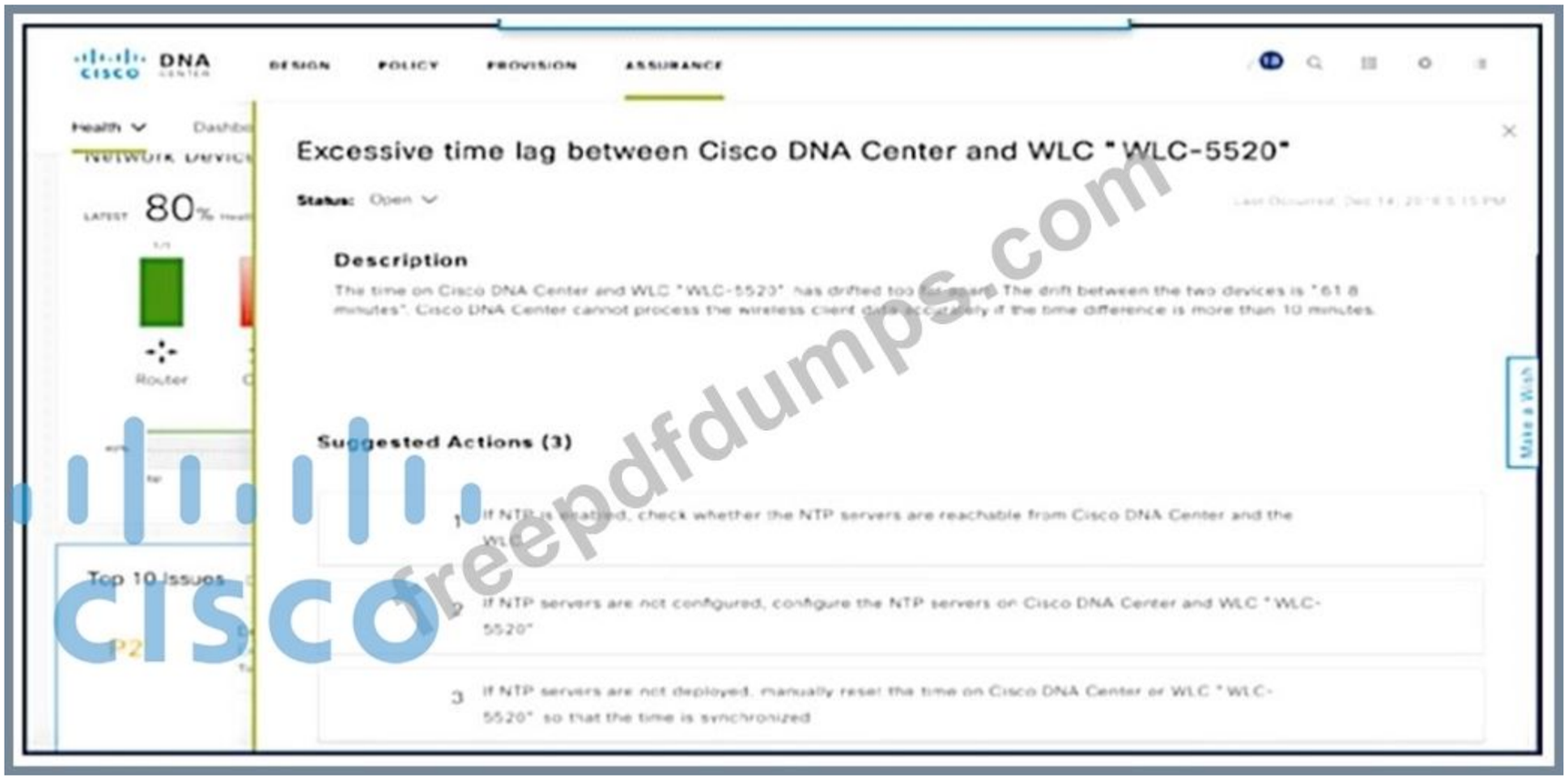
NEW QUESTION: 146
Refer to the exhibit.



A network administrator reviews the branch router console log to troubleshoot the OSPF adjacency issue with the DR router. Which action resolves this issue?
A. Stabilize the DR site flapping link to establish OSPF adjacency.
B. Configure matching hello and dead intervals between sites.
C. Configure the WAN interface for DR site in the related OSPF area.
D. Advertise the branch WAN interface matching subnet for the DR site.
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Which Ipv6 first-hop security feature helps to minimize denial of service attacks?
A. IPv6 Router Advertisement Guard
B. IPv6 Destination Guard
C. DHCPv6 Guard
D. IPv6 MAC address filtering
Answer: (SHOW ANSWER)
The Destination Guard feature helps in minimizing denial-of-service (DoS) attacks. It performs address resolutions only for those addresses that are active on the link,and requires the FHS binding table to be populated with the help of the IPv6 snooping feature.The feature enables the filtering of IPv6 traffic based on the destinationaddress, and blocks the NDP resolution for destination addresses that are not found in the binding table. By default, the policy drops traffic coming for an unknowndestination.

NEW QUESTION: 148
Exhibit:



NTP is configured across the network infrastructure and Cisco DNA Center. An NTP issue was reported on the Cisco DNA Center at 17:15. Which action resolves the issue?
A. Check and resolve reachability between the WLC and the NTP server
B. Reset the NTP server to resolve any synchronization issues tor all devices
C. Check and resolve reachability between Cisco DNA Center and the NTP server
D. Check and configure NTP on the WLC and synchronize with Cisco DNA Center

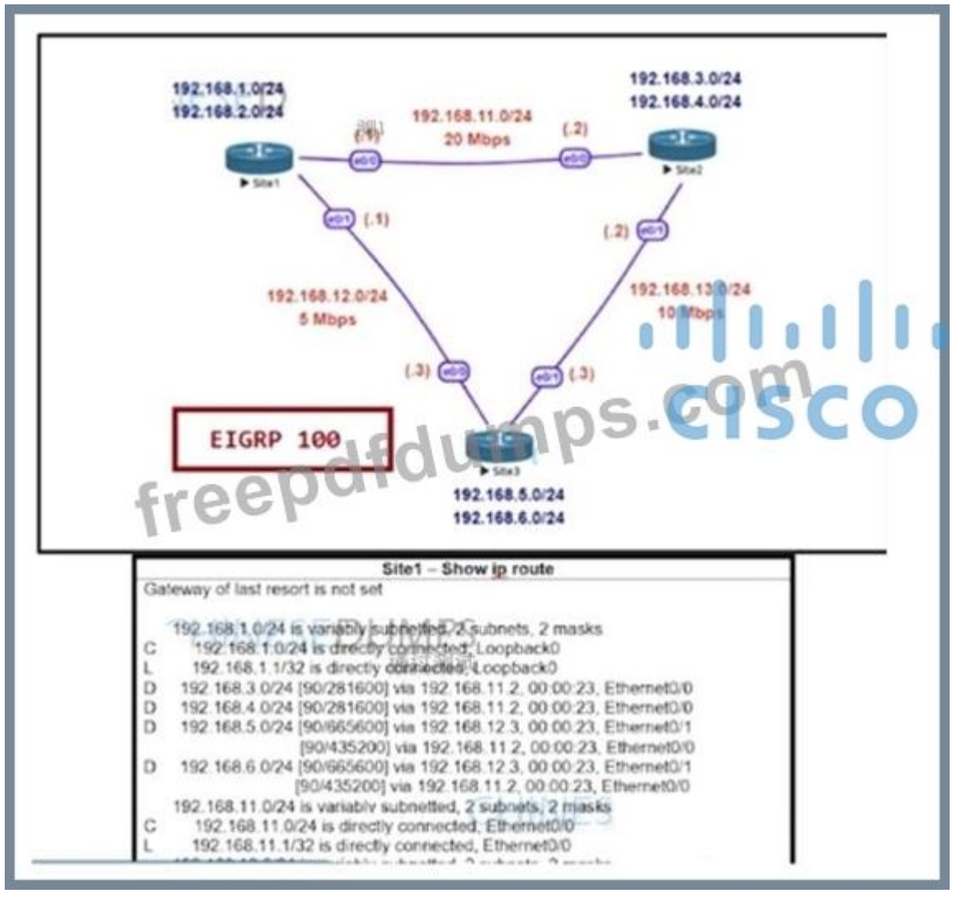
Answer: D (LEAVE A REPLY)
Excessive time lag between Cisco DNA Center and device: The time difference between Cisco DNA Center and the device IP Address has drifted too far apart. CiscoDNA Center cannot process the device data accurately if the time difference is more than 3 minutes.

NEW QUESTION: 149
Which component of MPLS VPNs is used to extend the IP address so that an engineer is able to identify to which VPN it belongs?
A. VPNv4 address family
B. RD
C. RT
D. LDP
Answer: B (LEAVE A REPLY)

- Specify the correct route distinguisher used for that VPN. This is used to extend the IP address so that you can identify which VPN it belongs to.

```
rd <VPN route distinguisher>
```

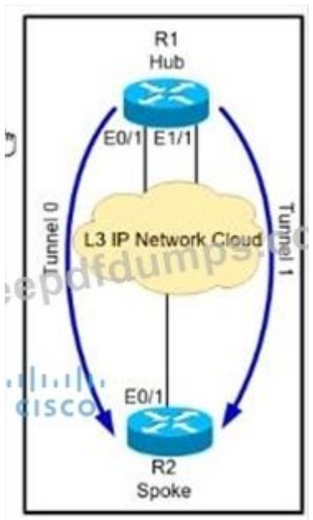
NEW QUESTION: 150
Refer to the exhibit.



Refer to the exhibit. Site1 must perform unequal cost load balancing toward the segments behind Site2 and Site3. Some of the routes are getting load balanced but others are not. Which configuration allows Site1 to load balance toward all the LAN segments of the remote routers?

A. Option C
B. Option A
C. Option B
D. Option D
Answer: D (LEAVE A REPLY)

NEW QUESTION: 151
Refer to the exhibit.



Refer to me exhibit. The hub and spoke are connected via two DMVPN tunnel interfaces The NHRP is configured and the tunnels are detected on the hub and the spoke Which configuration command adds an IPsec profile on both tunnel interfaces to encrypt traffic?

A. tunnel protection ipsec profile DMVPN unique

B. tunnel protection ipsec profile DMVPN multipoint

C. tunnel protection ipsec profile DMVPN shared

D. tunnel protection ipsec profile DMVPN tunnel1

Answer: C (LEAVE A REPLY)

Valid 300-410 Dumps shared by Actual4test.com for Helping Passing 300-410 Exam! Actual4test.com now offer the **newest 300-410 exam dumps**, the Actual4test.com 300-410 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-410 dumps with Test Engine here: https://www.actual4test.com/300-410_examcollection.html (**800** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)