Cisco

Exam Questions 300-410

Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)

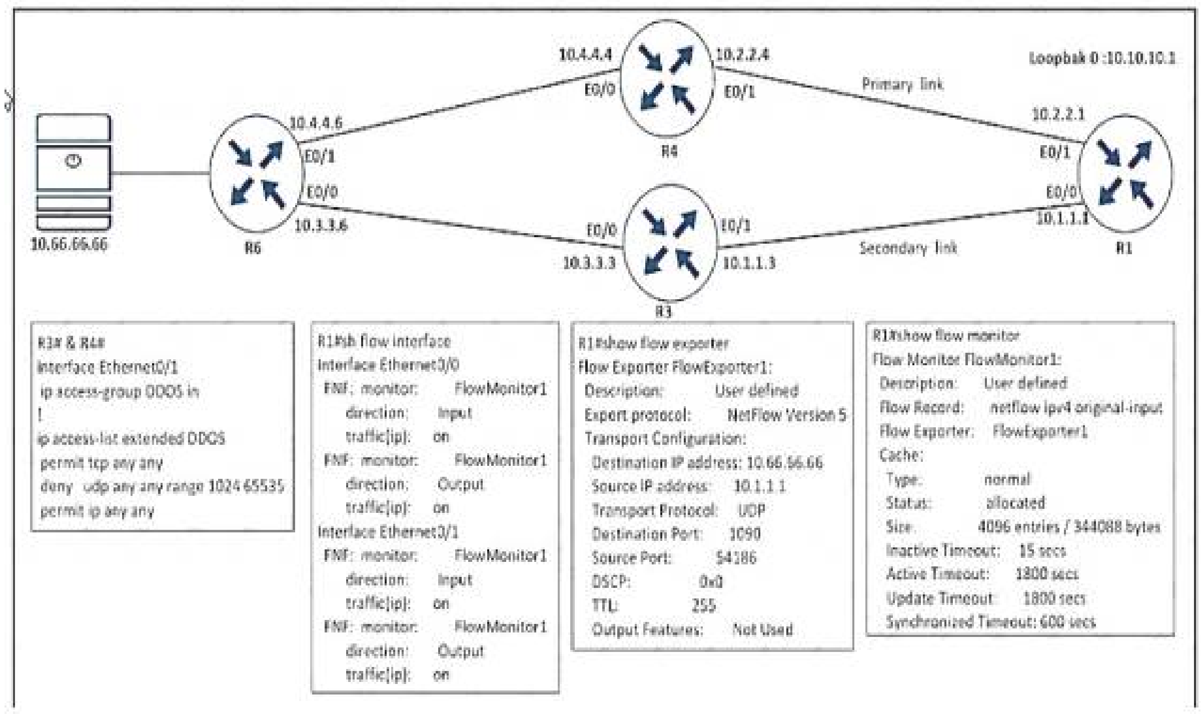
NEW QUESTION 1
- (Exam Topic 3)
A newly installed spoke router is configured for DMVPN with the ip mtu 1400 command. Which configuration allows the spoke to use fragmentation with the maximum negotiated TCP MTU over GRE?

A. ip tcp adjust-mss 1360crypto ipsec fragmentation after-encryption
B. ip tcp adjust-mtu 1360crypto ipsec fragmentation after-encryption
C. ip tcp adjust-mss 1360crypto ipsec fragmentation mtu-discovery
D. ip tcp adjust-mtu 1360crypto ipsec fragmentation mtu-discovery

Answer: A

Explanation:
https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troublesh

NEW QUESTION 2
- (Exam Topic 3)



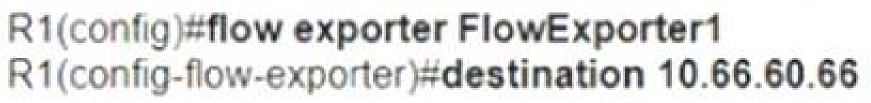
```
R3# & R4#
Interface Ethernet0/1
 ip access-group DDOS in
!
ip access-list extended DDOS
 permit tcp any any
 deny  udp any any range 1024 65535
 permit ip any any
```

```
R1#sh flow interface
Interface Ethernet3/0
 FNF:  monitor:        FlowMonitor1
       direction:      Input
       traffic(ip):    on
 FNF:  monitor:        FlowMonitor1
       direction:      Output
       traffic(ip):    on
Interface Ethernet3/1
 FNF:  monitor:        FlowMonitor1
       direction:      Input
       traffic(ip):    on
 FNF:  monitor:        FlowMonitor1
       direction:      Output
       traffic(ip):    on
```

```
R1#show flow exporter
Flow Exporter FlowExporter1:
 Description:          User defined
 Export protocol:      NetFlow Version 5
 Transport Configuration:
  Destination IP address: 10.66.56.66
  Source IP address:    10.1.1.1
  Transport Protocol:   UDP
  Destination Port:     1090
  Source Port:          54186
  DSCP:                 0x0
  TTL:                  255
  Output Features:      Not Used
```

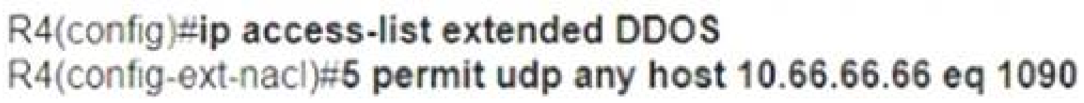
```
R1#show flow monitor
Flow Monitor FlowMonitor1:
 Description:      User defined
 Flow Record:      netflow ipv4 original-input
 Flow Exporter:    FlowExporter1
 Cache:
  Type:            normal
  Status:          allocated
  Size:            4096 entries / 344088 bytes
  Inactive Timeout:   15 secs
  Active Timeout:     1800 secs
  Update Timeout:     1800 secs
  Synchronized Timeout: 600 secs
```

Refer to the exhibit An engineer configured NetFlow but cannot receive the flows from R1 Which two configurations resolve the issue? (Choose two)
A)



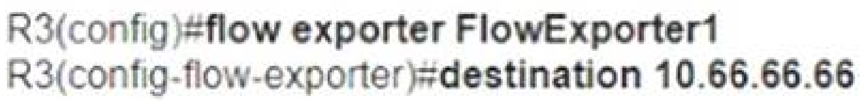
```
R1(config)#flow exporter FlowExporter1
R1(config-flow-exporter)#destination 10.66.60.66
```

B)



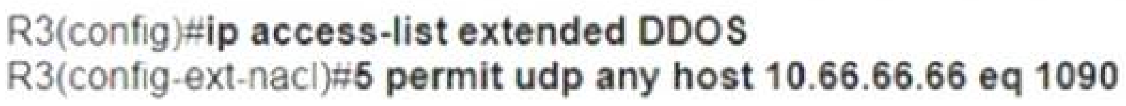
```
R4(config)#ip access-list extended DDOS
R4(config-ext-nacl)#5 permit udp any host 10.66.66.66 eq 1090
```

C)



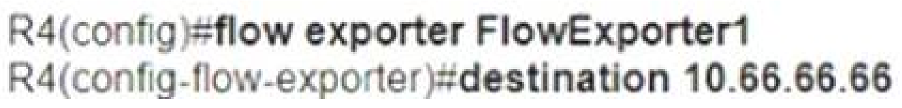
```
R3(config)#flow exporter FlowExporter1
R3(config-flow-exporter)#destination 10.66.66.66
```

D)



```
R3(config)#ip access-list extended DDOS
R3(config-ext-nacl)#5 permit udp any host 10.66.66.66 eq 1090
```

E)

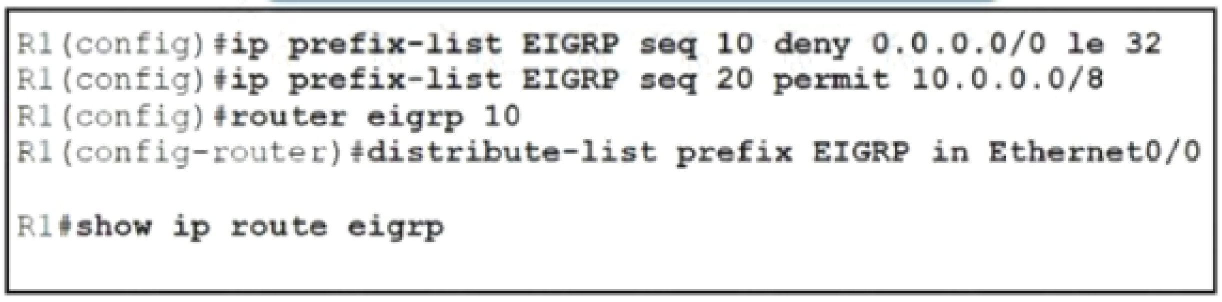


```
R4(config)#flow exporter FlowExporter1
R4(config-flow-exporter)#destination 10.66.66.66
```

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

Answer: BE

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



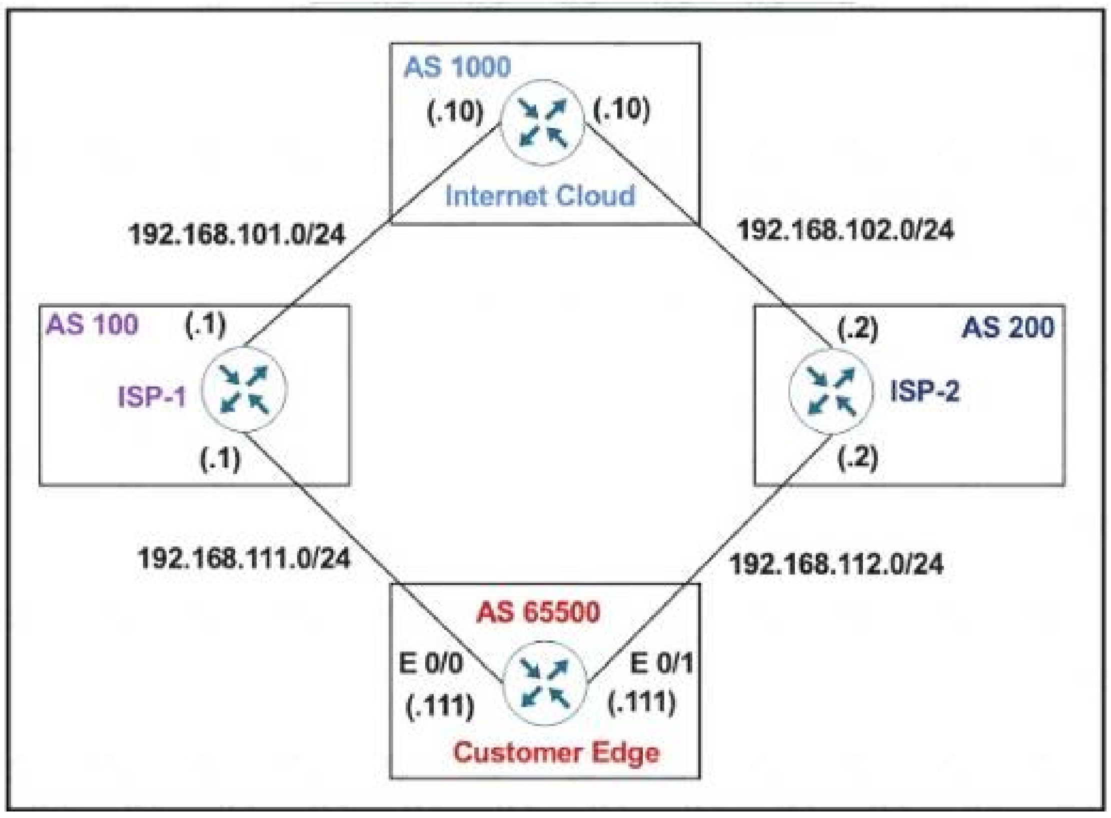
```
R1(config)#ip prefix-list EIGRP seq 10 deny 0.0.0.0/0 le 32
R1(config)#ip prefix-list EIGRP seq 20 permit 10.0.0.0/8
R1(config)#router eigrp 10
R1(config-router)#distribute-list prefix EIGRP in Ethernet0/0

R1#show ip route eigrp
```

A prefix list is created to filter routes inbound to an EIGRP process except for network 10 prefixes After the prefix list is applied no network 10 prefixes are visible in the routing table from EIGRP. Which configuration resolves the issue?

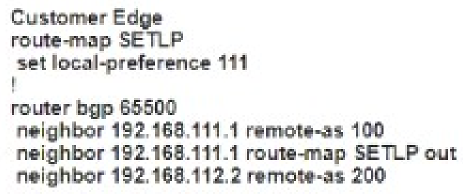
A. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9.
B. ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
C. ip prefix-list EIGRP seq 5 permit 10.0.0.0/8 ge 9 no ip prefix-list EIGRP seq 20 permit 10.0.0.0/8
D. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9 ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32

Answer: C

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

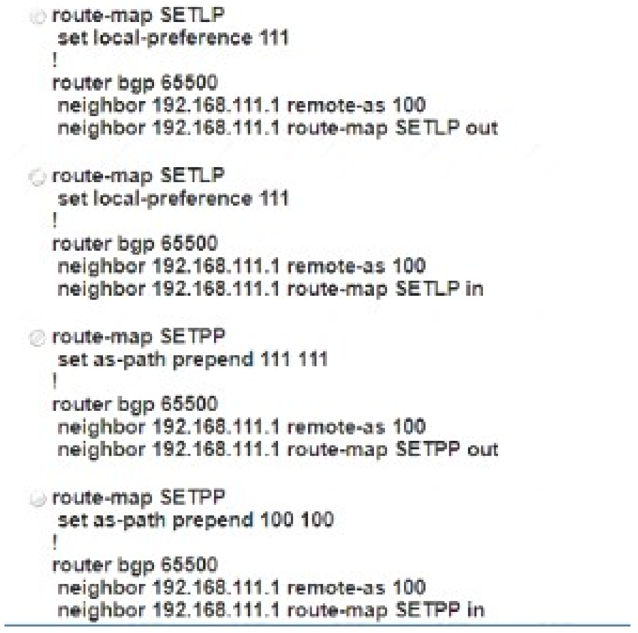


The Customer Edge router (AS 65500) wants to use ASC100 as the preferred ISP for all external routes.



```
Customer Edge
route-map SETLP
 set local-preference 111
!
router bgp 65500
 neighbor 192.168.111.1 remote-as 100
 neighbor 192.168.111.1 route-map SETLP out
 neighbor 192.168.112.2 remote-as 200
```

This configuration failed to send routes to AS 100 as the preferred path. Which set of configuration resolves the issue?



```
○ route-map SETLP
   set local-preference 111
  !
  router bgp 65500
   neighbor 192.168.111.1 remote-as 100
   neighbor 192.168.111.1 route-map SETLP out

○ route-map SETLP
   set local-preference 111
  !
  router bgp 65500
   neighbor 192.168.111.1 remote-as 100
   neighbor 192.168.111.1 route-map SETLP in

○ route-map SETPP
   set as-path prepend 111 111
  !
  router bgp 65500
   neighbor 192.168.111.1 remote-as 100
   neighbor 192.168.111.1 route-map SETPP out

○ route-map SETPP
   set as-path prepend 100 100
  !
  router bgp 65500
   neighbor 192.168.111.1 remote-as 100
   neighbor 192.168.111.1 route-map SETPP in
```

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

Answer: B

NEW QUESTION 5
- (Exam Topic 3)
What must be configured by the network engineer to circumvent AS_PATH prevention mechanism in IP/VPN Hub and Spoke deployment scenarios?

A. Use allows in and as-override at all Pes.
B. Use allowas in and as-override at the PE-Hub.
C. Use Allowas-in the PE_Hub
D. Use as-override at the PE_Hub

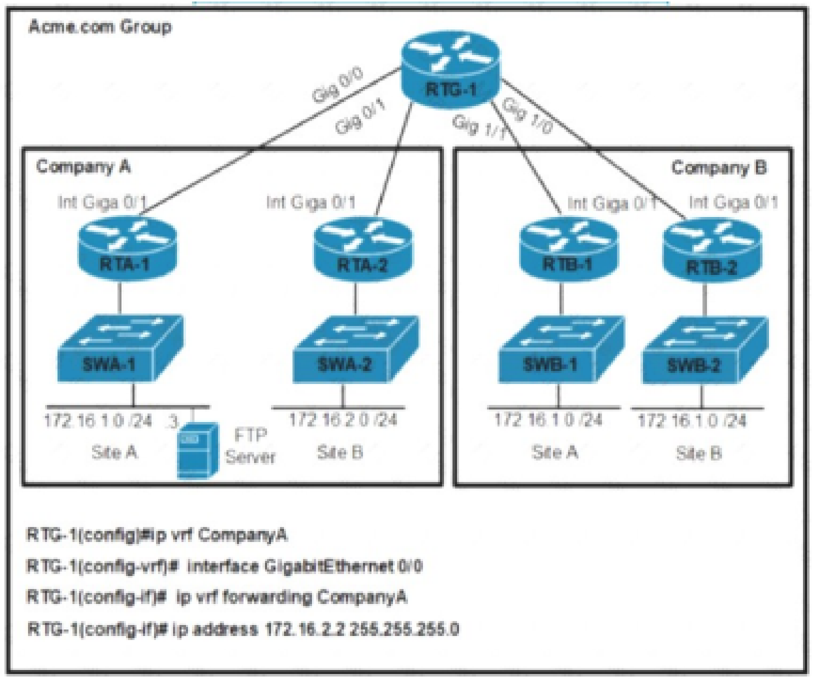
Answer: D

NEW QUESTION 6
- (Exam Topic 3)
An engineer notices that R1 does not hold enough log messages to Identity the root cause during troubleshooting Which command resolves this issue?

A. #logging buffered 4096 critical
B. (config)#logging buffered 16000 informational
C. #logging buffered 16000 critical
D. (config)#logging buffered 4096 informational

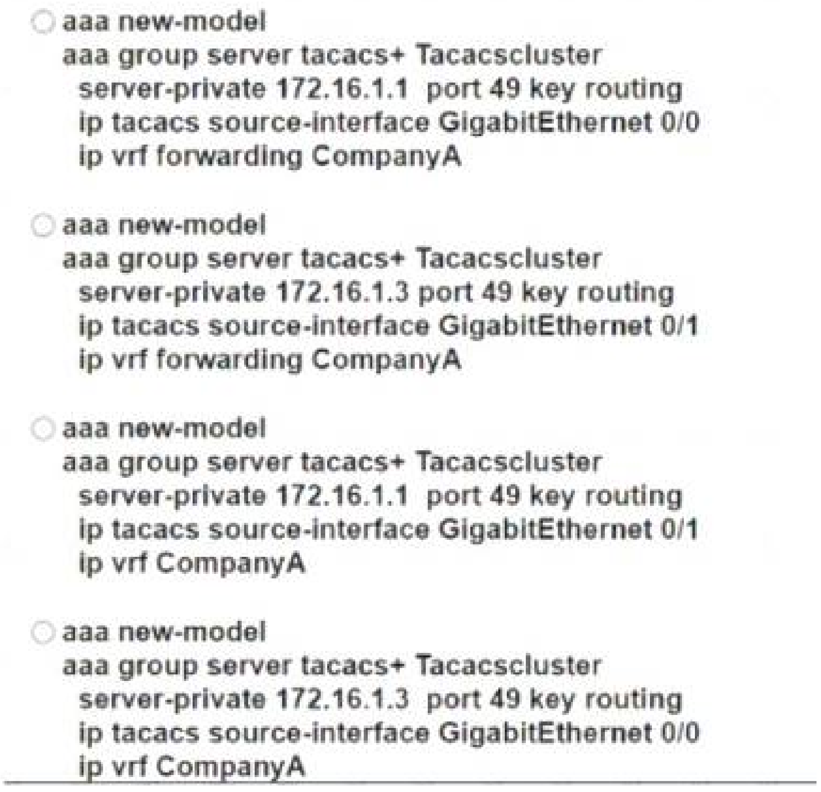
Answer: B

NEW QUESTION 7
- (Exam Topic 3)



```
RTG-1(config)#ip vrf CompanyA
RTG-1(config-vrf)# interface GigabitEthernet 0/0
RTG-1(config-if)# ip vrf forwarding CompanyA
RTG-1(config-if)# ip address 172.16.2.2 255.255.255.0
```

Refer to the exhibit. An engineer must configure a per VRF for TACACS+ for company A. Which configuration on RTG-1 accomplishes the task?



○
```
aaa new-model
aaa group server tacacs+ Tacacscluster
 server-private 172.16.1.1  port 49 key routing
 ip tacacs source-interface GigabitEthernet 0/0
 ip vrf forwarding CompanyA
```

○
```
aaa new-model
aaa group server tacacs+ Tacacscluster
 server-private 172.16.1.3 port 49 key routing
 ip tacacs source-interface GigabitEthernet 0/1
 ip vrf forwarding CompanyA
```

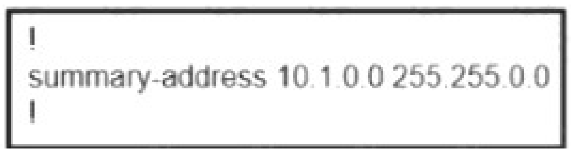
○
```
aaa new-model
aaa group server tacacs+ Tacacscluster
 server-private 172.16.1.1  port 49 key routing
 ip tacacs source-interface GigabitEthernet 0/1
 ip vrf CompanyA
```

○
```
aaa new-model
aaa group server tacacs+ Tacacscluster
 server-private 172.16.1.3  port 49 key routing
 ip tacacs source-interface GigabitEthernet 0/0
 ip vrf CompanyA
```

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

Answer: D

NEW QUESTION 8
- (Exam Topic 3)
Refer to the exhibit.



```
!
summary-address 10.1.0.0 255.255.0.0
!
```

The none area 0 routers in OSPF still receive more specific routes of 10.1.1.0.10.1.2.0.10.1.3.0 from area 1. Which action resolves the issue?

A. Configure route summarization on OSPF-enabled interfaces.
B. Summarize by using the summary-address 10.1.0.0 255.255.252.0 command.
C. Summarize by using the area range command on ABRs
D. Configure the summary-address 10.1.0.0 255.255.252.0 command under OSPF process.

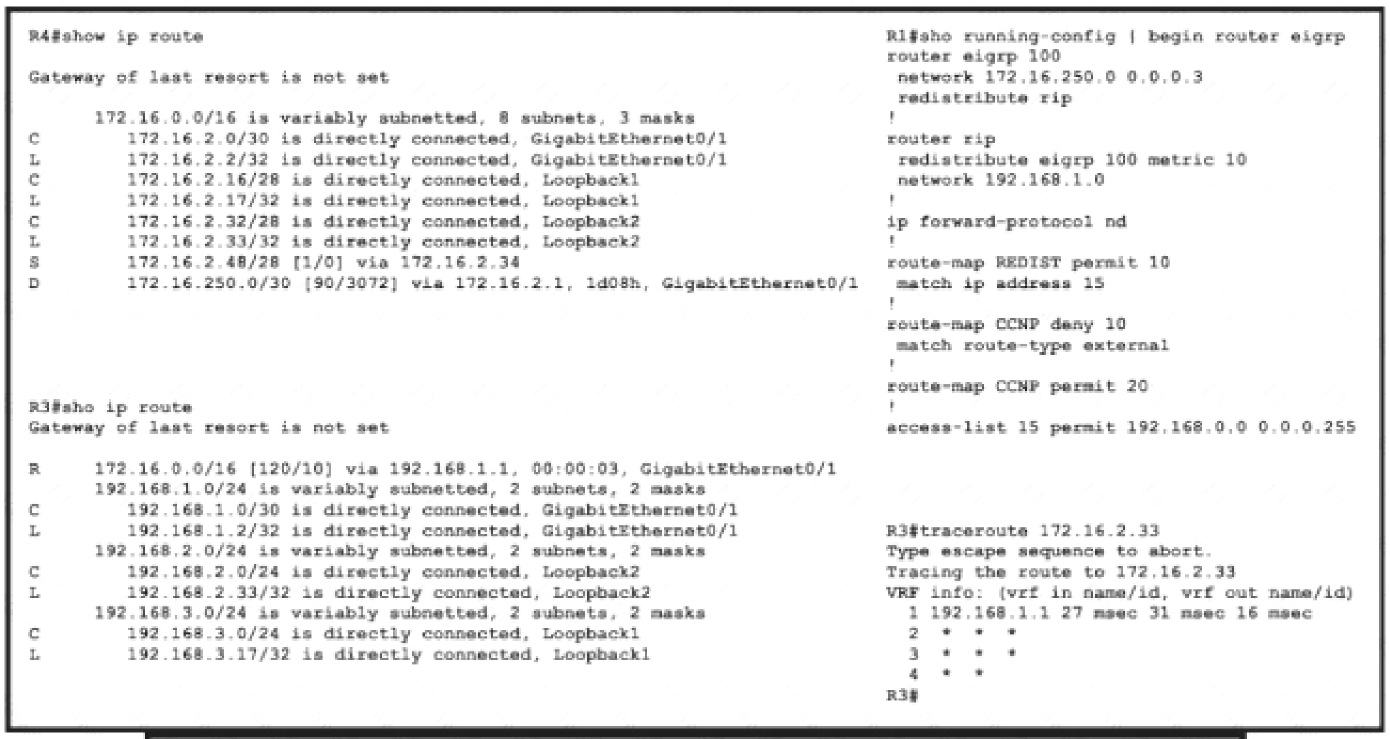
Answer: C

NEW QUESTION 9
- (Exam Topic 3)
The network administrator must implement IPv6 in the network to allow only devices that not only have registered IP addresses but are also connecting from assigned locations. Which security feature must be implemented?

A. IPv6 Snooping
B. IPv6 Destination Guard
C. IPv6 Prefix Guard
D. IPv6 Router Advertisement Guard

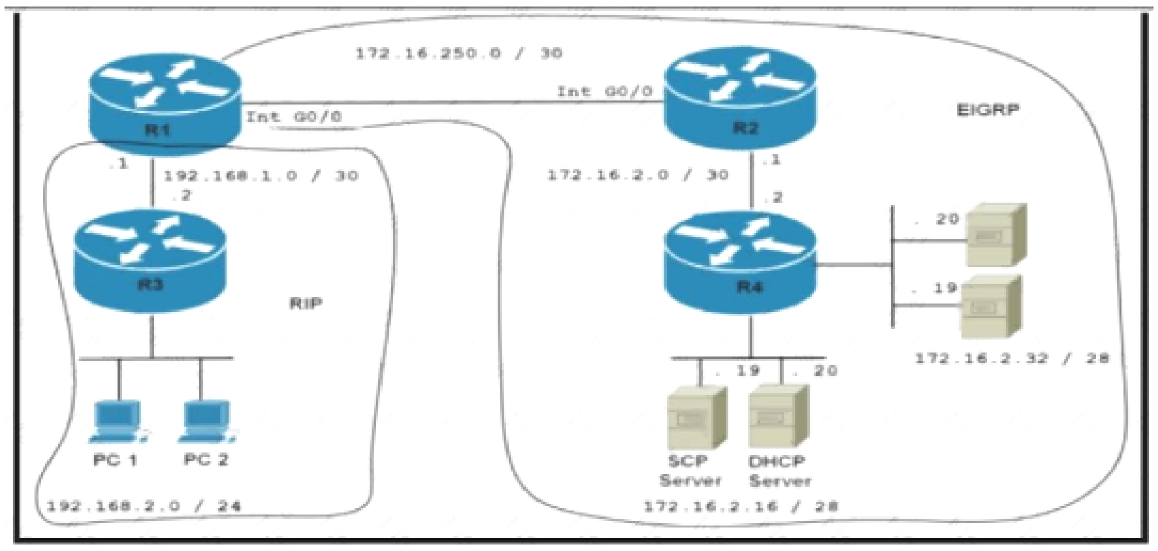
Answer: A

NEW QUESTION 10
- (Exam Topic 3)

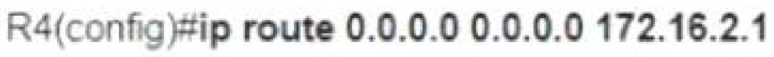


```
R4#show ip route

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
C        172.16.2.0/30 is directly connected, GigabitEthernet0/1
L        172.16.2.2/32 is directly connected, GigabitEthernet0/1
C        172.16.2.16/28 is directly connected, Loopback1
L        172.16.2.17/32 is directly connected, Loopback1
C        172.16.2.32/28 is directly connected, Loopback2
L        172.16.2.33/32 is directly connected, Loopback2
S        172.16.2.48/28 [1/0] via 172.16.2.34
D        172.16.250.0/30 [90/3072] via 172.16.2.1, 1d08h, GigabitEthernet0/1




R3#sho ip route
Gateway of last resort is not set

R     172.16.0.0/16 [120/10] via 192.168.1.1, 00:00:03, GigabitEthernet0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0/1
L        192.168.1.2/32 is directly connected, GigabitEthernet0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Loopback2
L        192.168.2.33/32 is directly connected, Loopback2
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Loopback1
L        192.168.3.17/32 is directly connected, Loopback1
```

```
R1#sho running-config | begin router eigrp
router eigrp 100
 network 172.16.250.0 0.0.0.3
 redistribute rip
!
router rip
 redistribute eigrp 100 metric 10
 network 192.168.1.0
!
ip forward-protocol nd
!
route-map REDIST permit 10
 match ip address 15
!
route-map CCNP deny 10
 match route-type external
!
route-map CCNP permit 20
!
access-list 15 permit 192.168.0.0 0.0.0.255



R3#traceroute 172.16.2.33
Type escape sequence to abort.
Tracing the route to 172.16.2.33
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.1 27 msec 31 msec 16 msec
  2  *  *  *
  3  *  *  *
  4  *  *
R3#
```

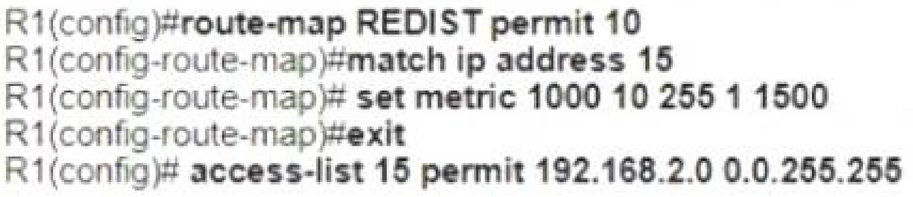


Refer to the exhibit Users from the 192 168.2.0/24 network cannot connect to the 172.16 2 32/28 network Which configuration resolves the issue'?
A)



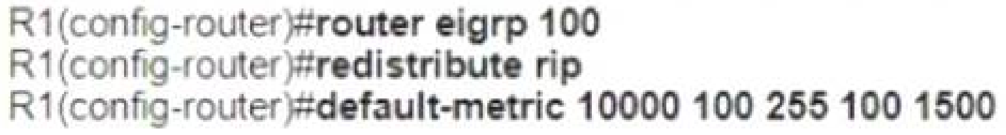
```
R4(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.1
```

B)



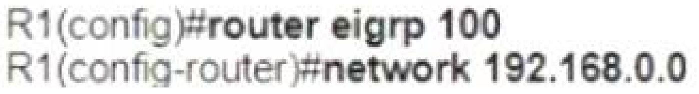
```
R1(config)#route-map REDIST permit 10
R1(config-route-map)#match ip address 15
R1(config-route-map)# set metric 1000 10 255 1 1500
R1(config-route-map)#exit
R1(config)# access-list 15 permit 192.168.2.0 0.0.255.255
```

C)



```
R1(config-router)#router eigrp 100
R1(config-router)#redistribute rip
R1(config-router)#default-metric 10000 100 255 100 1500
```

D)



```
R1(config)#router eigrp 100
R1(config-router)#network 192.168.0.0
```

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

Answer: A

NEW QUESTION 10
- (Exam Topic 3)
Refer to the exhibit.
A network administrator is troubleshooting OSPF adjacency issue by going through the console logs in the router, but due to an overwhelming log message stream it is impossible to capture the problem Which two commands reduce console log messages to relevant OSPF neighbor problem details so that the issue can be resolved? (Choose two)

A. debug condition interface
B. debug condition ip
C. debug condition ospf neighbor
D. debug condition session-id ADJCHG
E. debug condition all

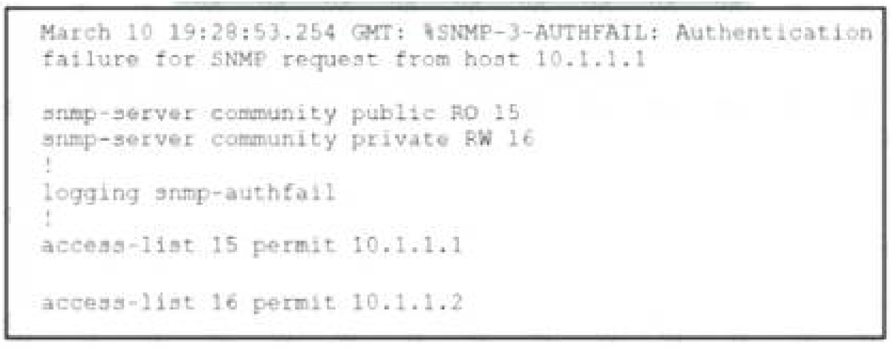
Answer: AD

NEW QUESTION 12
- (Exam Topic 3)
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: C

NEW QUESTION 14
- (Exam Topic 3)



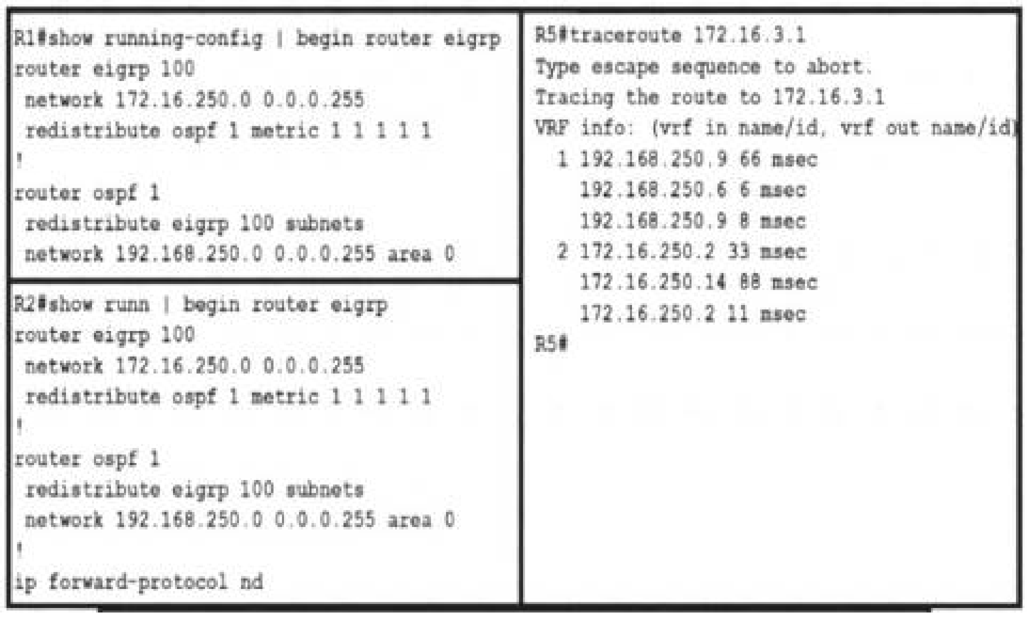
```
March 10 19:28:53.254 GMT: %SNMP-3-AUTHFAIL: Authentication
failure for SNMP request from host 10.1.1.1

snmp-server community public RO 15
snmp-server community private RW 16
!
logging snmp-authfail
!
access-list 15 permit 10.1.1.1

access-list 16 permit 10.1.1.2
```

Refer to the exhibit Which action resolves the issue?

A. Configure host IP address in access-list 16
B. Configure SNMPv3 on the router
C. Configure SNMP authentication on the router
D. Configure a valid SNMP community string

Answer: D

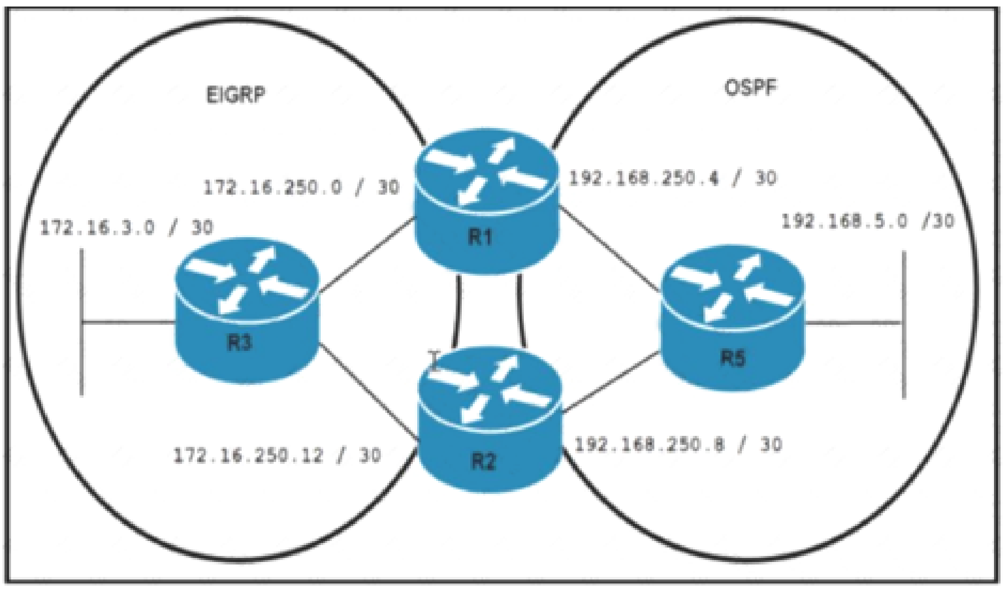
NEW QUESTION 15
- (Exam Topic 3)



```
R1#show running-config | begin router eigrp
router eigrp 100
 network 172.16.250.0 0.0.0.255
 redistribute ospf 1 metric 1 1 1 1 1
!
router ospf 1
 redistribute eigrp 100 subnets
 network 192.168.250.0 0.0.0.255 area 0
```

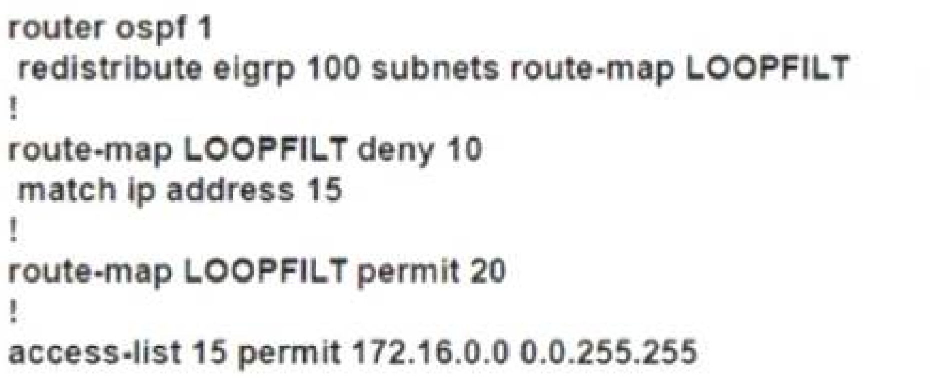
```
R2#show runn | begin router eigrp
router eigrp 100
 network 172.16.250.0 0.0.0.255
 redistribute ospf 1 metric 1 1 1 1 1
!
router ospf 1
 redistribute eigrp 100 subnets
 network 192.168.250.0 0.0.0.255 area 0
!
ip forward-protocol nd
```

```
R5#traceroute 172.16.3.1
Type escape sequence to abort.
Tracing the route to 172.16.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.250.9 66 msec
    192.168.250.6 6 msec
    192.168.250.9 8 msec
  2 172.16.250.2 33 msec
    172.16.250.14 88 msec
    172.16.250.2 11 msec
R5#
```



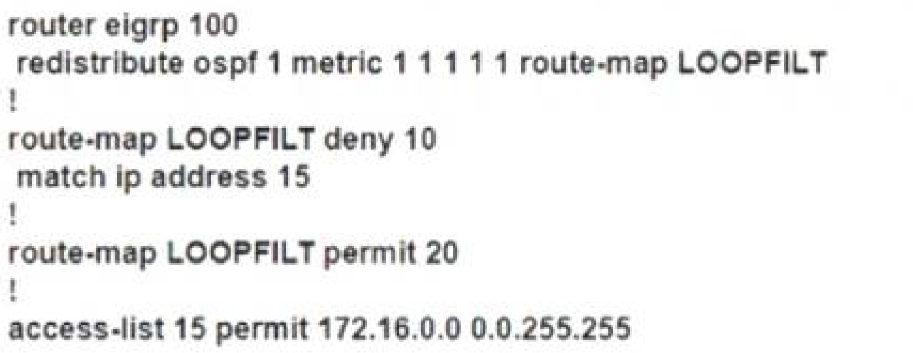
Refer to the exhibit. An engineer Is troubleshooting a routing loop on the network to reach the 172.16.3.0/16 from the OSPF domain. Which configuration on router R1 resolves the Issue?

A)



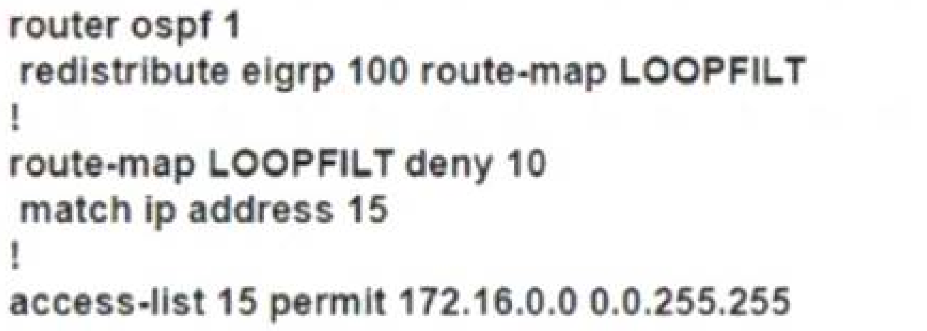
```
router ospf 1
 redistribute eigrp 100 subnets route-map LOOPFILT
!
route-map LOOPFILT deny 10
 match ip address 15
!
route-map LOOPFILT permit 20
!
access-list 15 permit 172.16.0.0 0.0.255.255
```

B)



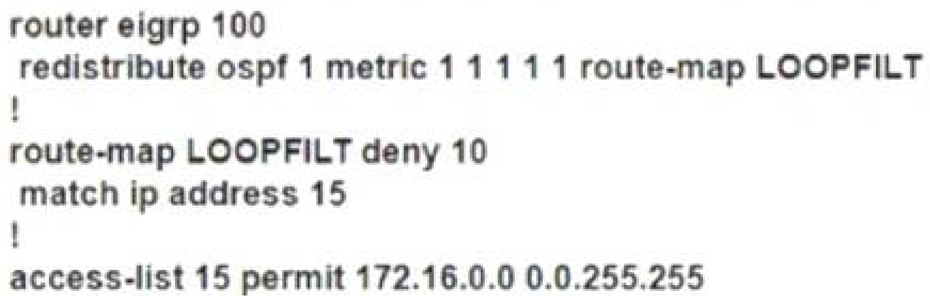
```
router eigrp 100
 redistribute ospf 1 metric 1 1 1 1 1 route-map LOOPFILT
!
route-map LOOPFILT deny 10
 match ip address 15
!
route-map LOOPFILT permit 20
!
access-list 15 permit 172.16.0.0 0.0.255.255
```

C)



```
router ospf 1
 redistribute eigrp 100 route-map LOOPFILT
!
route-map LOOPFILT deny 10
 match ip address 15
!
access-list 15 permit 172.16.0.0 0.0.255.255
```

D)

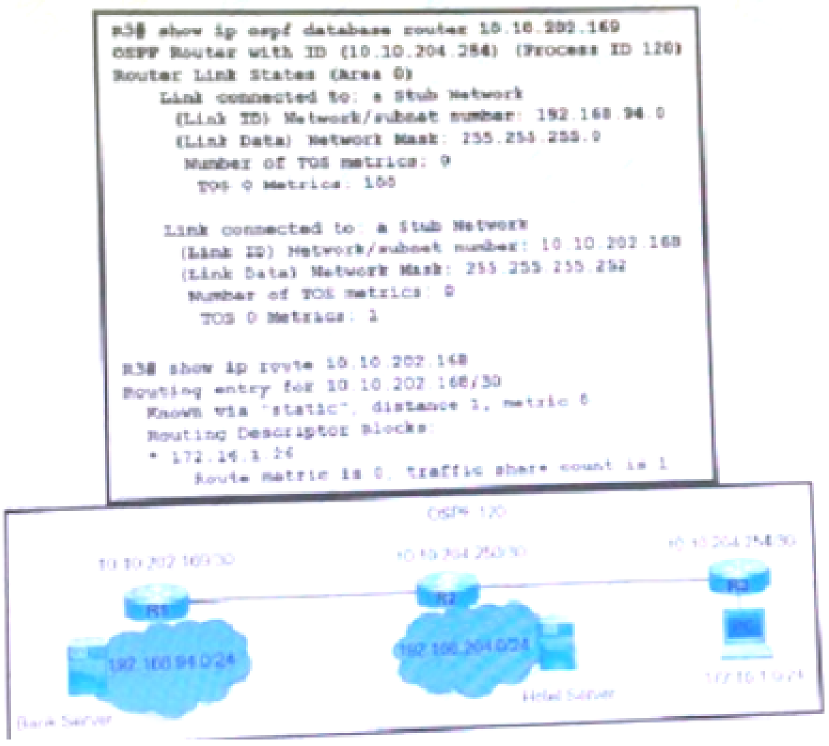


```
router eigrp 100
 redistribute ospf 1 metric 1 1 1 1 1 route-map LOOPFILT
!
route-map LOOPFILT deny 10
 match ip address 15
!
access-list 15 permit 172.16.0.0 0.0.255.255
```

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

Answer: C

NEW QUESTION 19
- (Exam Topic 3)
Refer to the exhibit.



```
R3# show ip ospf database router 10.10.202.169
OSPF Router with ID (10.10.204.254) (Process ID 120)
Router Link States (Area 0)
    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 192.168.94.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
       TOS 0 Metrics: 100

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 10.10.202.168
     (Link Data) Network Mask: 255.255.255.252
      Number of TOS metrics: 0
       TOS 0 Metrics: 1

R3# show ip route 10.10.202.168
Routing entry for 10.10.202.168/30
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 172.16.1.26
      Route metric is 0, traffic share count is 1
```

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. Allow stub network 10.10.202.168/30 on router R3 OSPF.
B. Decrease the AD to 5 OSPF route 192.168.94.0 on R1.
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.

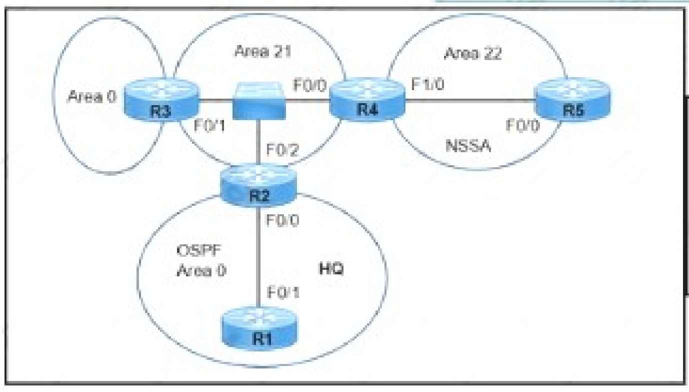
Answer: A

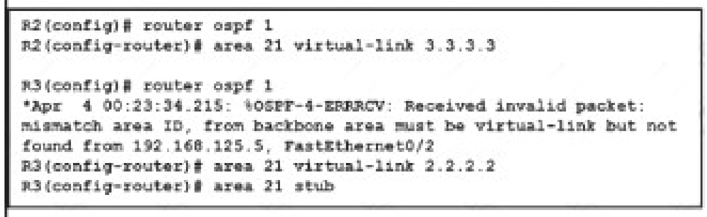
NEW QUESTION 24
- (Exam Topic 3)
What are the two prerequisites to enable BFD on Cisco routers? (Choose two)

A. A supported IP routing protocol must be configured on the participating routers.
B. OSPF Demand Circuit must run BFD on all participating routers.
C. ICMP must be allowed on all participating routers.
D. UDP port 1985 must be allowed on all participating routers.
E. Cisco Express Forwarding and IP Routing must be enabled on all participating routers.

Answer: CE

NEW QUESTION 28
- (Exam Topic 3)





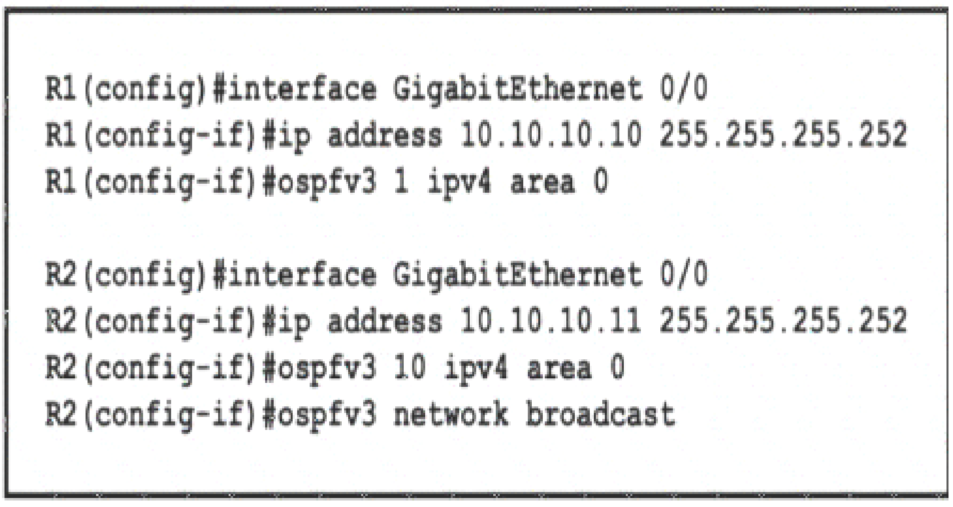
```
R2(config)# router ospf 1
R2(config-router)# area 21 virtual-link 3.3.3.3

R3(config)# router ospf 1
*Apr  4 00:23:34.215: %OSPF-4-ERRRCV: Received invalid packet:
mismatch area ID, from backbone area must be virtual-link but not
found from 192.168.125.5, FastEthernet0/2
R3(config-router)# area 21 virtual-link 2.2.2.2
R3(config-router)# area 21 stub
```

Refer to the exhibit. A network engineer is troubleshooting a failed link between R2 and R3 No traffic loss is reported from router R5 to HQ Which command fixes the separated backbone?

A. R2(config-router)#no area 21 stub
B. R2(config_router)#area 21 virtual-link 192.168.125.5
C. R3(config-router)#area 21 virtual-link 192.168.125.5
D. R3(config-router)#no area 21 stub

Answer: D

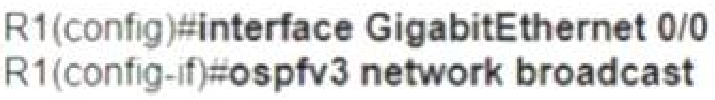
NEW QUESTION 33
- (Exam Topic 3)



```
R1(config)#interface GigabitEthernet 0/0
R1(config-if)#ip address 10.10.10.10 255.255.255.252
R1(config-if)#ospfv3 1 ipv4 area 0

R2(config)#interface GigabitEthernet 0/0
R2(config-if)#ip address 10.10.10.11 255.255.255.252
R2(config-if)#ospfv3 10 ipv4 area 0
R2(config-if)#ospfv3 network broadcast
```

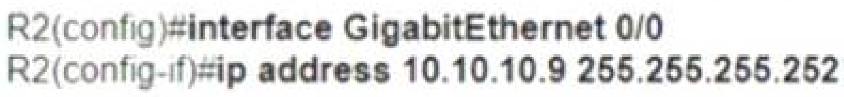
Refer to the exhibit An engineer is troubleshooting an OSPF adjacency issue between directly connected routers R1 and R2 Which configuration resolves the issue?

A)



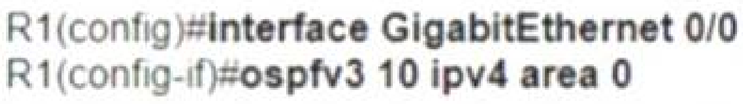
```
R1(config)#interface GigabitEthernet 0/0
R1(config-if)#ospfv3 network broadcast
```

B)



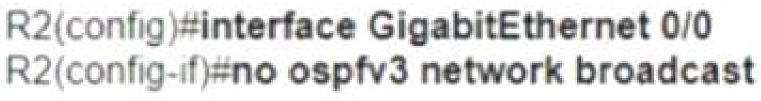
```
R2(config)#interface GigabitEthernet 0/0
R2(config-if)#ip address 10.10.10.9 255.255.255.252
```

C)



```
R1(config)#interface GigabitEthernet 0/0
R1(config-if)#ospfv3 10 ipv4 area 0
```

D)

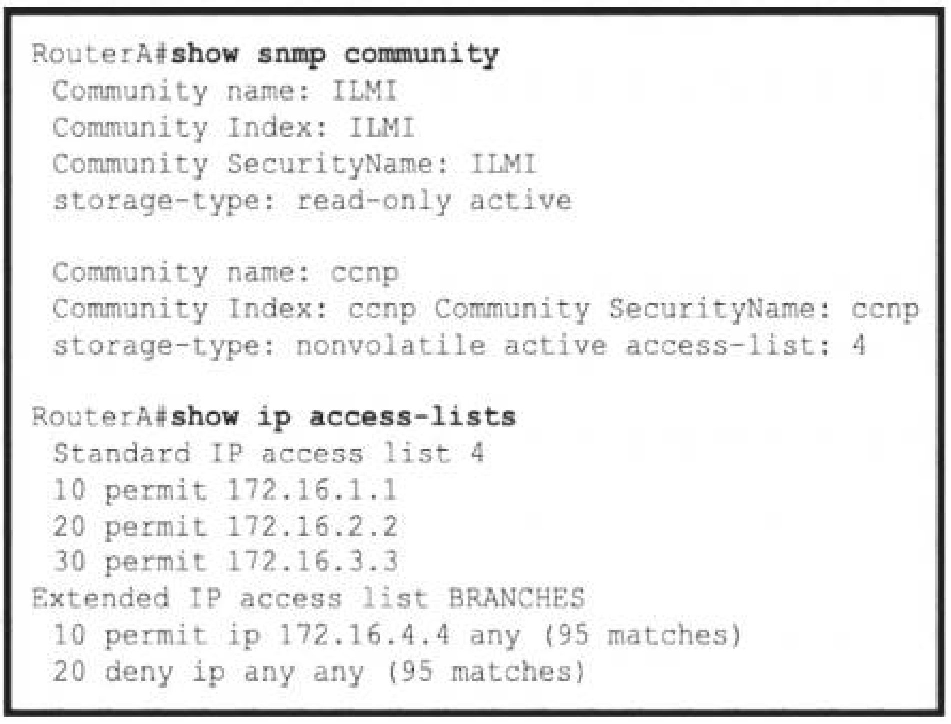


```
R2(config)#interface GigabitEthernet 0/0
R2(config-if)#no ospfv3 network broadcast
```

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

Answer: B

NEW QUESTION 37
- (Exam Topic 3)



```
RouterA#show snmp community
 Community name: ILMI
 Community Index: ILMI
 Community SecurityName: ILMI
 storage-type: read-only active

 Community name: ccnp
 Community Index: ccnp Community SecurityName: ccnp
 storage-type: nonvolatile active access-list: 4

RouterA#show ip access-lists
 Standard IP access list 4
 10 permit 172.16.1.1
 20 permit 172.16.2.2
 30 permit 172.16.3.3
Extended IP access list BRANCHES
 10 permit ip 172.16.4.4 any (95 matches)
 20 deny ip any any (95 matches)
```

Refer to the exhibit The SNMP server with IP address 172.16 4 4 cannot access host router A Which configuration command on router A resolves the issue?

A. snmp-server community ccnp
B. access-list 4 permit 172.16.4.0 0.0.0.3
C. access-list 4 permit host 172.16.4.4
D. snmp-server host 172.16.4.4 ccnp

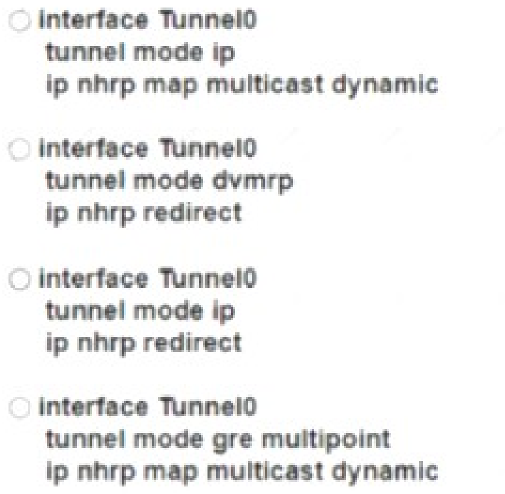
Answer: D

NEW QUESTION 38
- (Exam Topic 3)
configuration on the hub router meets this requirement?

A. interface Tunnel0tunnel mode gre multipoint
B. interface Tunnel0 tunnel mode dvmrp
C. interface Tunnel0 tunnel mode ipsec ipv4
D. interface Tunnel0 tunnel mode ip

Answer: A

NEW QUESTION 43
- (Exam Topic 3)
A company Is redesigning WAN infrastructure so that all branch sites must communicate via the head office and the head office can directly communicate with each site independently. The network engineer must configure the head office router by considering zero-touch technology when adding new sites in the same WAN infrastructure. Which configuration must be applied to the head office router to meet this requirement?

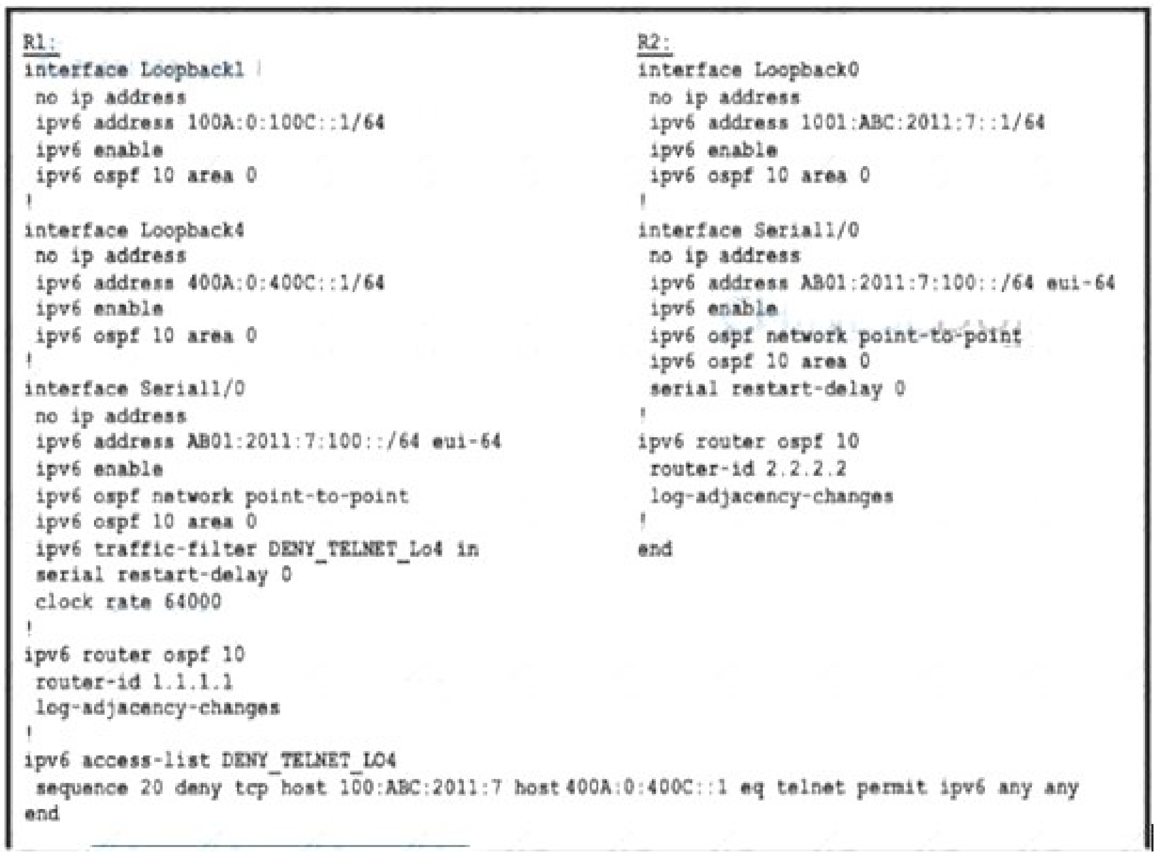


```
○ interface Tunnel0
   tunnel mode ip
   ip nhrp map multicast dynamic

○ interface Tunnel0
   tunnel mode dvmrp
   ip nhrp redirect

○ interface Tunnel0
   tunnel mode ip
   ip nhrp redirect

○ interface Tunnel0
   tunnel mode gre multipoint
   ip nhrp map multicast dynamic
```

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

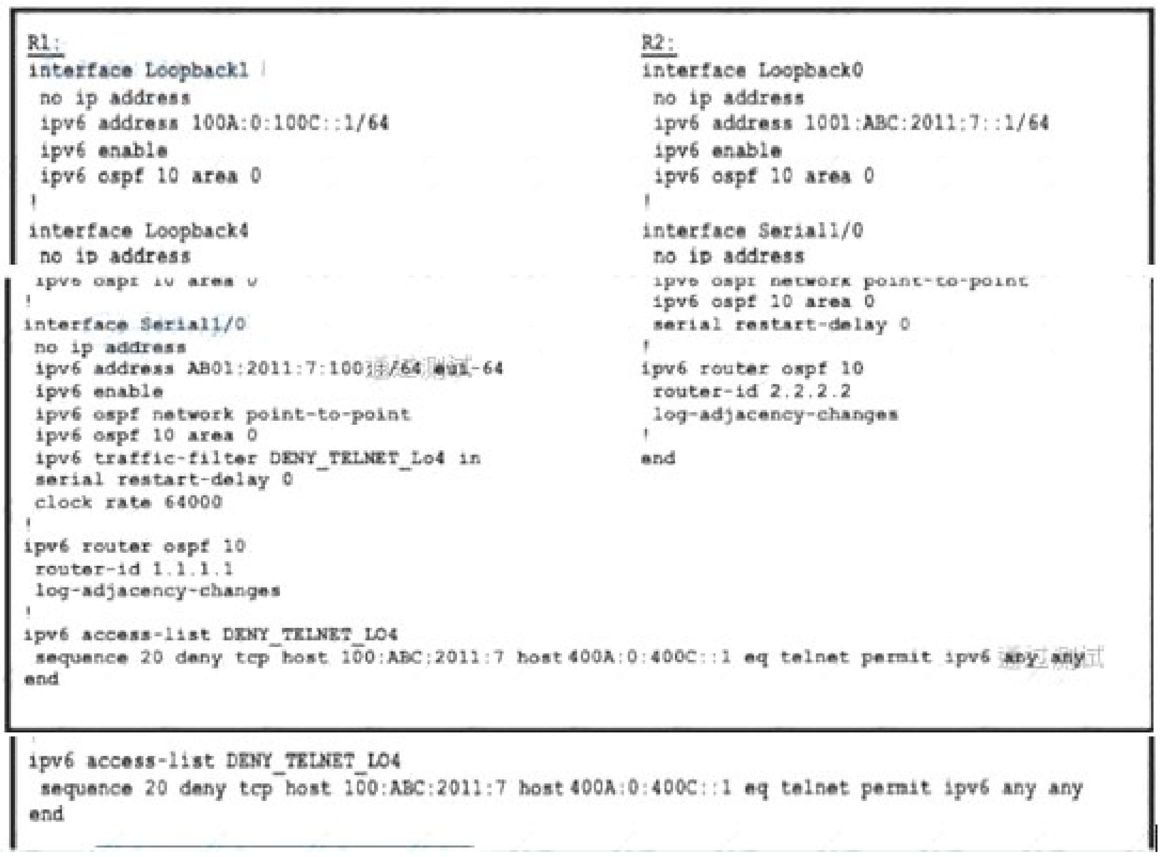
Answer: D

NEW QUESTION 46
- (Exam Topic 3)



```
R1:
interface Loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
interface Loopback4
 no ip address
 ipv6 address 400A:0:400C::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
interface Serial1/0
 no ip address
 ipv6 address AB01:2011:7:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 10 area 0
 ipv6 traffic-filter DENY_TELNET_Lo4 in
 serial restart-delay 0
 clock rate 64000
!
ipv6 router ospf 10
 router-id 1.1.1.1
 log-adjacency-changes
!
ipv6 access-list DENY_TELNET_LO4
 sequence 20 deny tcp host 100:ABC:2011:7 host 400A:0:400C::1 eq telnet permit ipv6 any any
end
```

```
R2:
interface Loopback0
 no ip address
 ipv6 address 1001:ABC:2011:7::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
interface Serial1/0
 no ip address
 ipv6 address AB01:2011:7:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 10 area 0
 serial restart-delay 0
!
ipv6 router ospf 10
 router-id 2.2.2.2
 log-adjacency-changes
!
end
```



```
R1:                                                R2:
interface Loopback1                                interface Loopback0
 no ip address                                      no ip address
 ipv6 address 100A:0:100C::1/64                     ipv6 address 1001:ABC:2011:7::1/64
 ipv6 enable                                        ipv6 enable
 ipv6 ospf 10 area 0                                ipv6 ospf 10 area 0
!                                                  !
interface Loopback4                                interface Serial1/0
 no ip address                                      no ip address
 ipv6 ospf 10 area 0                                ipv6 ospf network point-to-point
!                                                   ipv6 ospf 10 area 0
interface Serial1/0                                 serial restart-delay 0
 no ip address                                     !
 ipv6 address AB01:2011:7:100::/64 eui-64          ipv6 router ospf 10
 ipv6 enable                                        router-id 2.2.2.2
 ipv6 ospf network point-to-point                   log-adjacency-changes
 ipv6 ospf 10 area 0                               !
 ipv6 traffic-filter DENY_TELNET_Lo4 in            end
 serial restart-delay 0
 clock rate 64000
!
ipv6 router ospf 10
 router-id 1.1.1.1
 log-adjacency-changes
!
ipv6 access-list DENY_TELNET_LO4
 sequence 20 deny tcp host 100:ABC:2011:7 host 400A:0:400C::1 eq telnet permit ipv6 any any
end
```

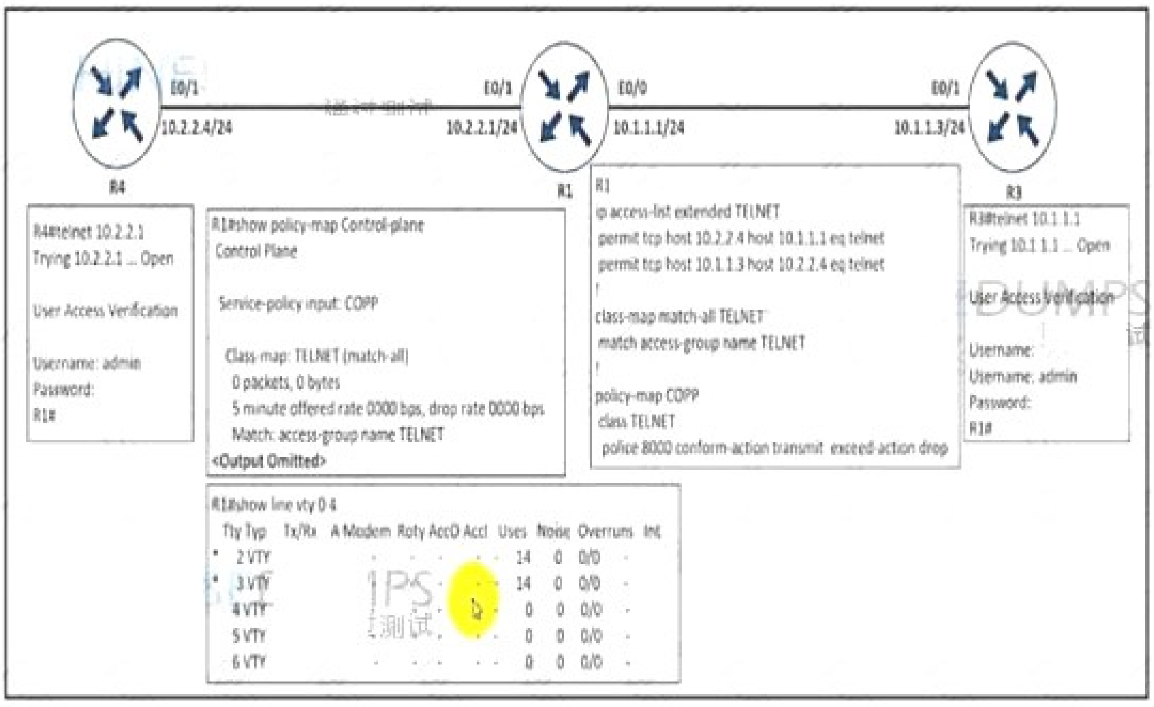
```
ipv6 access-list DENY_TELNET_LO4
 sequence 20 deny tcp host 100:ABC:2011:7 host 400A:0:400C::1 eq telnet permit ipv6 any any
end
```

Refer to the exhibit. An engineer implemented an access list on R1 to allow anyone to Telnet except R2 Loopback0 to R1 Loopback4 How must sequence 20 be replaced on the R1 access list to resolve the issue?

A. sequence 20 permit tcp host 1001 ABC:2011:7:: 1 host 400A:0:400C::1 eq telnet
B. sequence 20 deny tcp host 400A:0:400C::1 host 1001 :ABC:2011:7::1 eq telnet
C. sequence 20 deny tcp host 1001:ABC:2011:7::1 host 400A:0:400C::1 eq telnet
D. sequence 20 permit tcp host 400A:0:400C::1 host 1001ABC:2011:7::1 eq telnet

Answer: C

NEW QUESTION 51
- (Exam Topic 3)
Refer to the exhibit.



```
R4#telnet 10.2.2.1
Trying 10.2.2.1 ... Open

User Access Verification

Username: admin
Password:
R1#
```

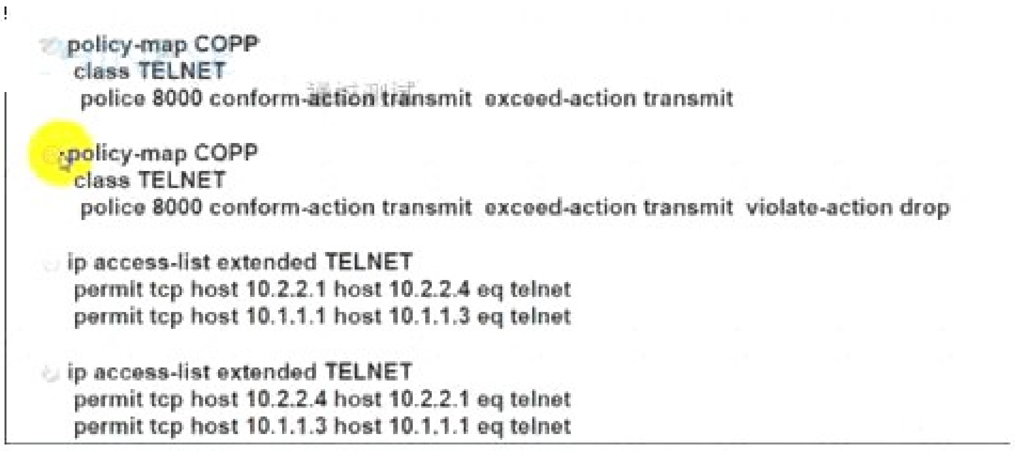
```
R1#show policy-map Control-plane
 Control Plane

  Service-policy input: COPP

   Class-map: TELNET (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: access-group name TELNET
<Output Omitted>
```

```
R1
ip access-list extended TELNET
 permit tcp host 10.2.2.4 host 10.1.1.1 eq telnet
 permit tcp host 10.1.1.3 host 10.2.2.4 eq telnet
!
class-map match-all TELNET
 match access-group name TELNET
!
policy-map COPP
 class TELNET
  police 8000 conform-action transmit  exceed-action drop
```

```
R3#telnet 10.1.1.1
Trying 10.1.1.1 ... Open

User Access Verification

Username:
Username: admin
Password:
R1#
```

```
R1#show line vty 0 4
   Tty Typ    Tx/Rx   A Modem  Roty AccO AccI  Uses  Noise  Overruns  Int
*    2 VTY             -    -    -    -    -     14      0      0/0     -
*    3 VTY             -    -    -    -    -     14      0      0/0     -
     4 VTY             -    -    -    -    -      0      0      0/0     -
     5 VTY             -    -    -    -    -      0      0      0/0     -
     6 VTY             -    -    -    -    -      0      0      0/0     -
```

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?



```
!
policy-map COPP
 class TELNET
  police 8000 conform-action transmit  exceed-action transmit

policy-map COPP
 class TELNET
  police 8000 conform-action transmit  exceed-action transmit  violate-action drop

ip access-list extended TELNET
 permit tcp host 10.2.2.1 host 10.2.2.4 eq telnet
 permit tcp host 10.1.1.1 host 10.1.1.3 eq telnet

ip access-list extended TELNET
 permit tcp host 10.2.2.4 host 10.2.2.1 eq telnet
 permit tcp host 10.1.1.3 host 10.1.1.1 eq telnet
```

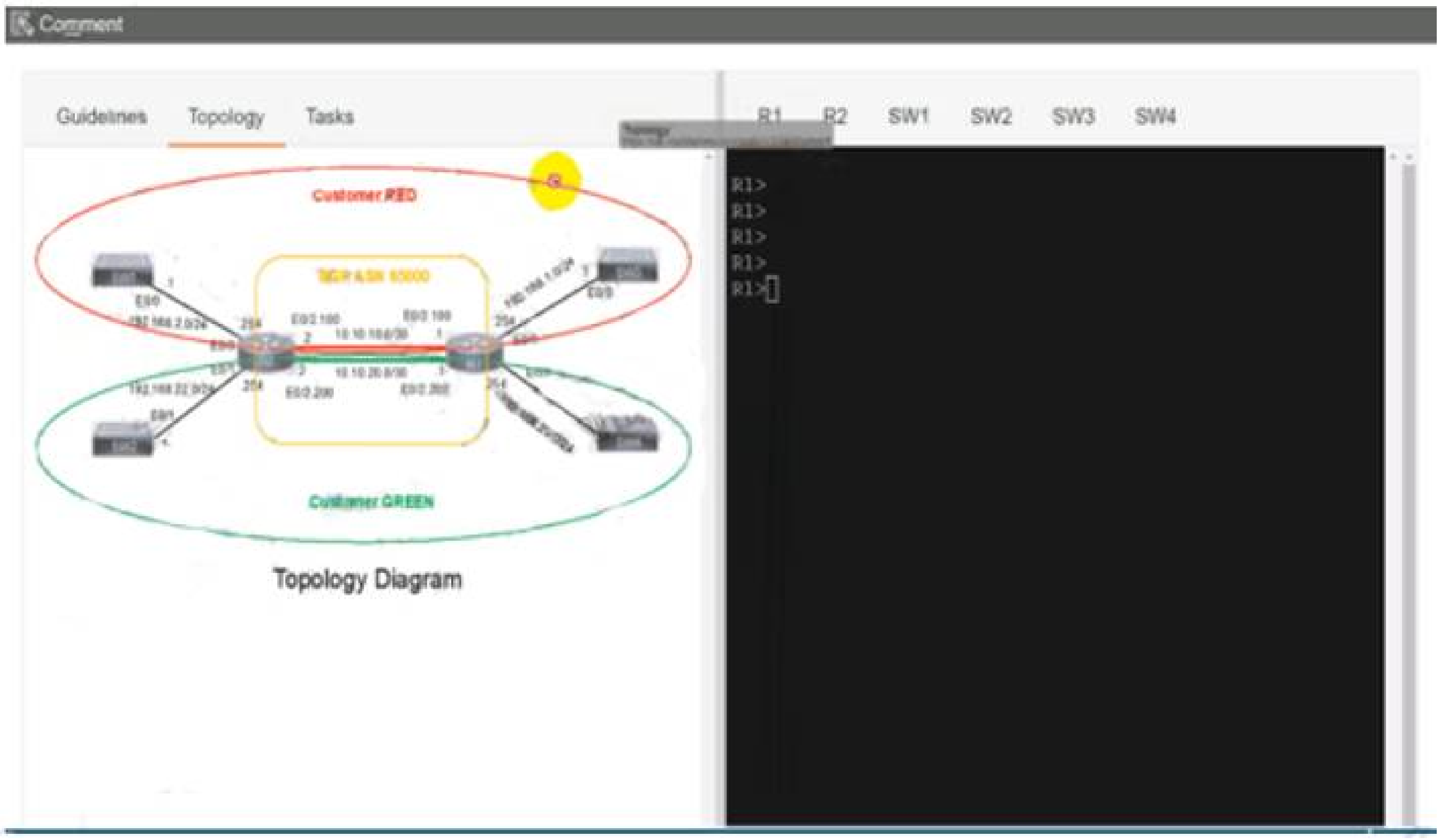
A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

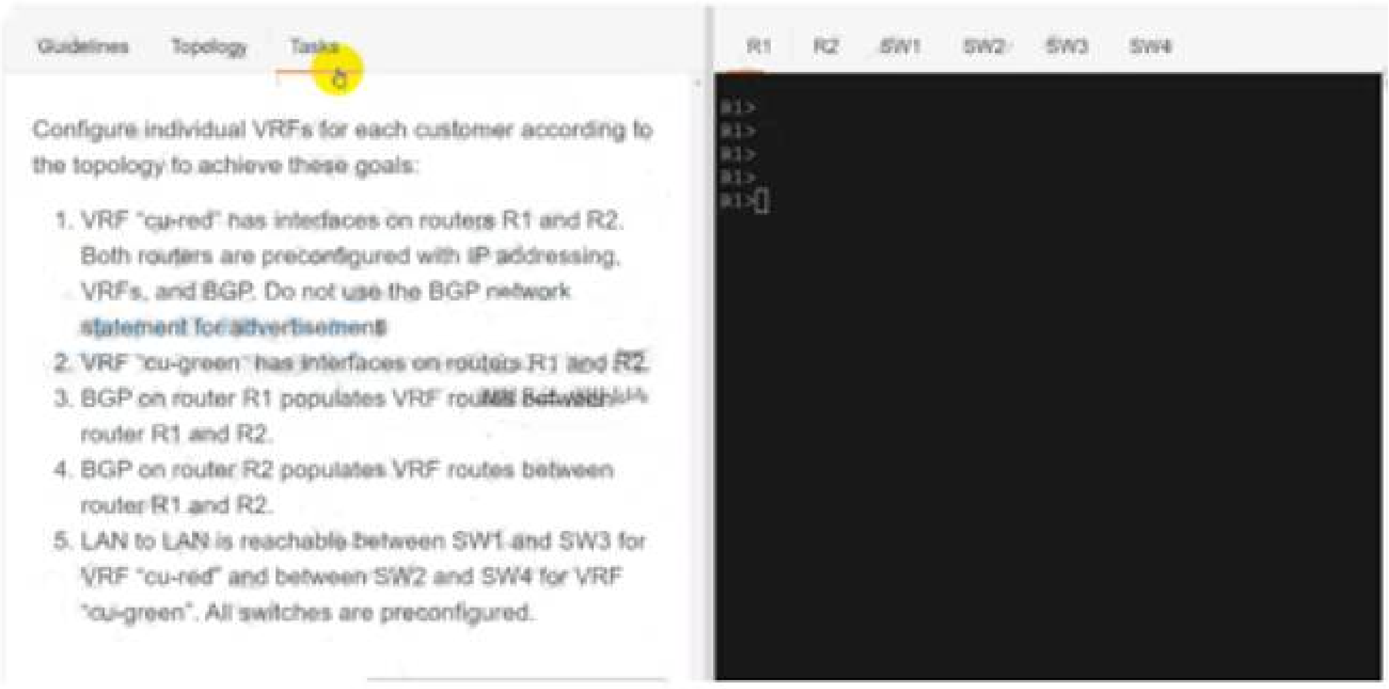
NEW QUESTION 53

- (Exam Topic 3)

Configure individual VRFs for each customer according to the topology to achieve these goals :



```
R1>
R1>
R1>
R1>
R1>
```

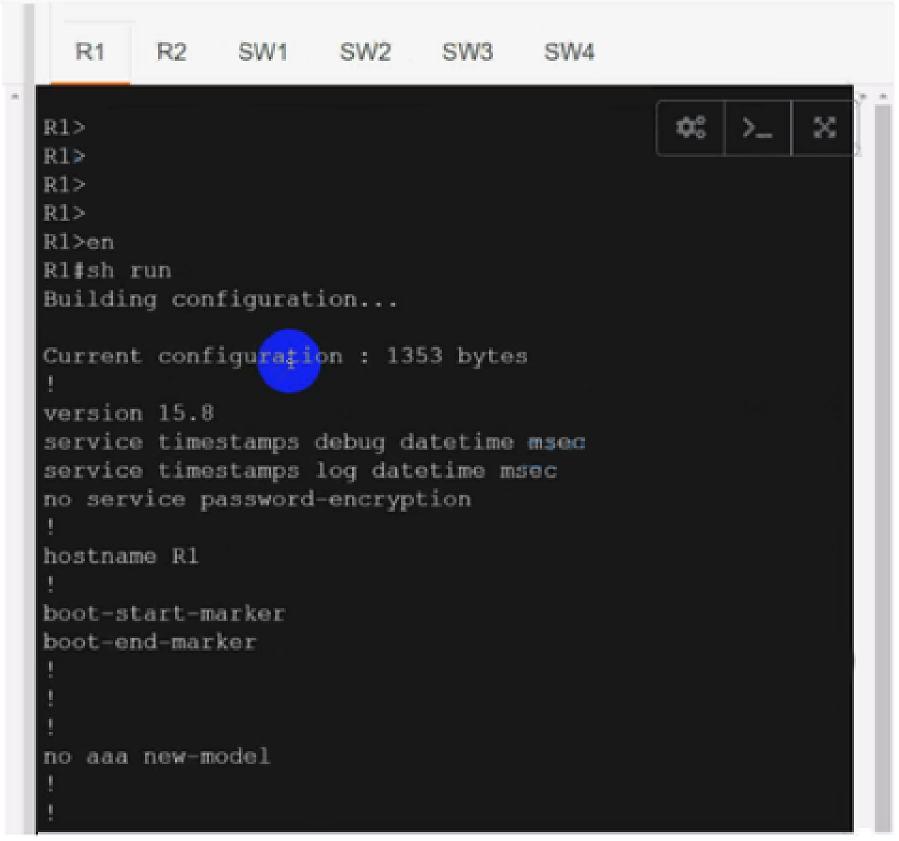


Configure individual VRFs for each customer according to the topology to achieve these goals:

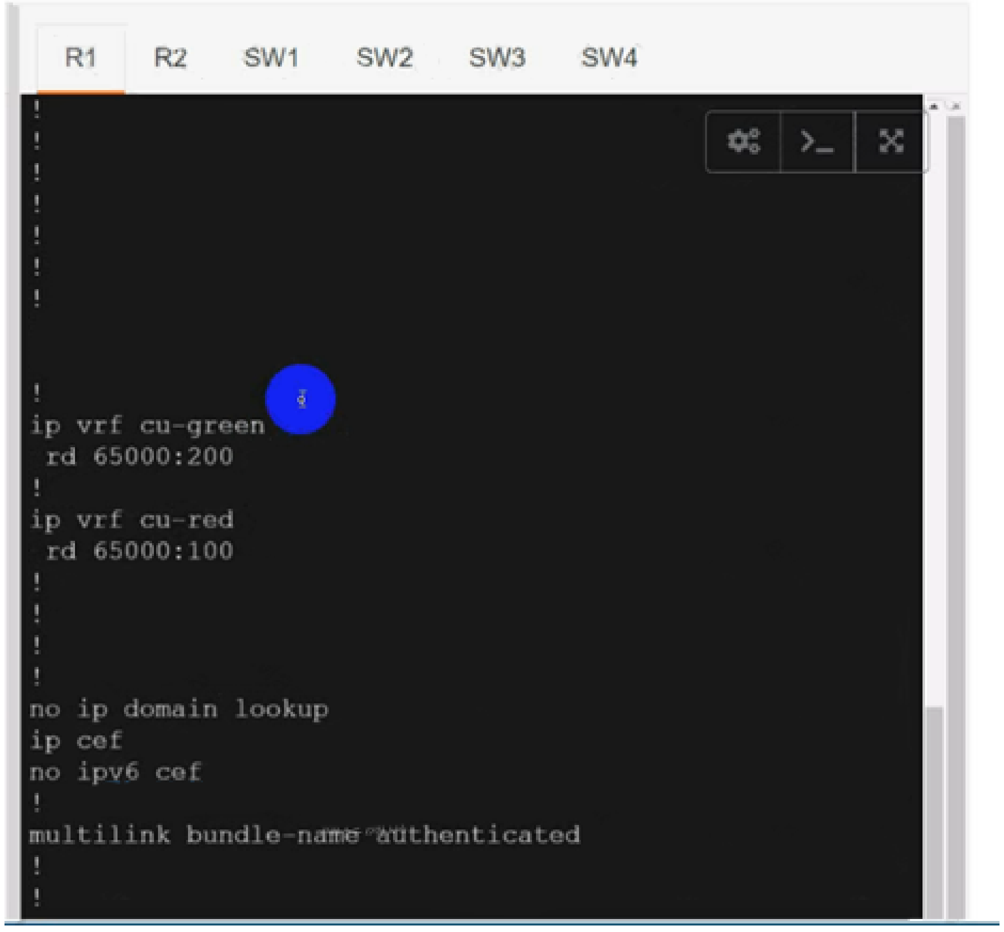
1. VRF "cu-red" has interfaces on routers R1 and R2. Both routers are preconfigured with IP addressing, VRFs, and BGP. Do not use the BGP network statement for advertisement
2. VRF "cu-green" has interfaces on routers R1 and R2.
3. BGP on router R1 populates VRF routes between router R1 and R2.
4. BGP on router R2 populates VRF routes between router R1 and R2.
5. LAN to LAN is reachable between SW1 and SW3 for VRF "cu-red" and between SW2 and SW4 for VRF "cu-green". All switches are preconfigured.

```
R1>
R1>
R1>
R1>
R1>
```

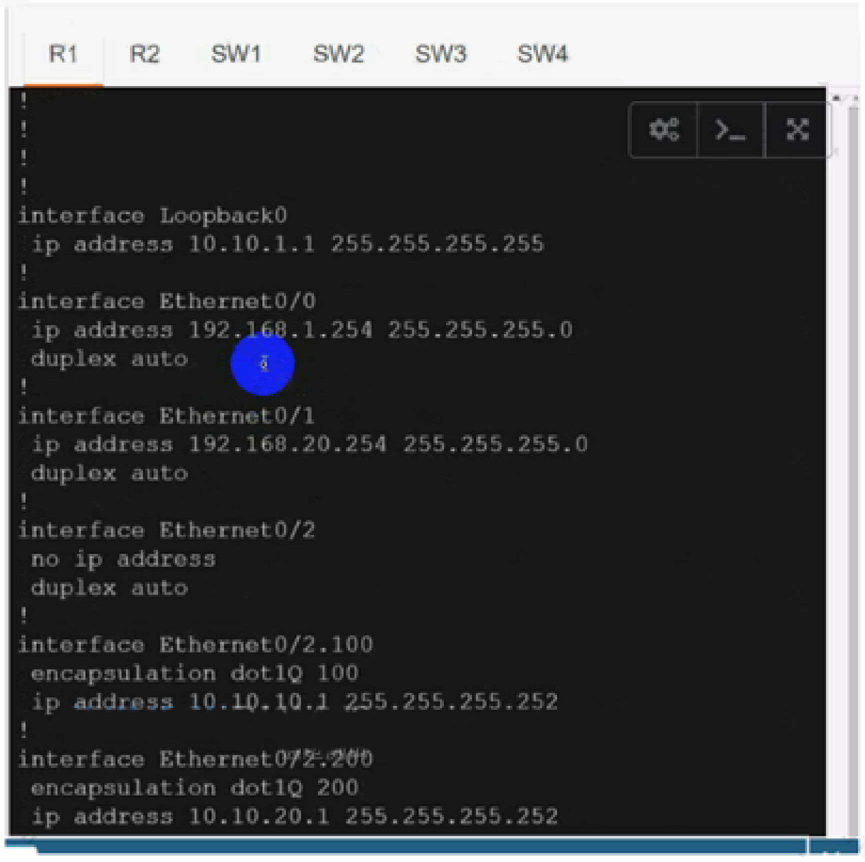
R1



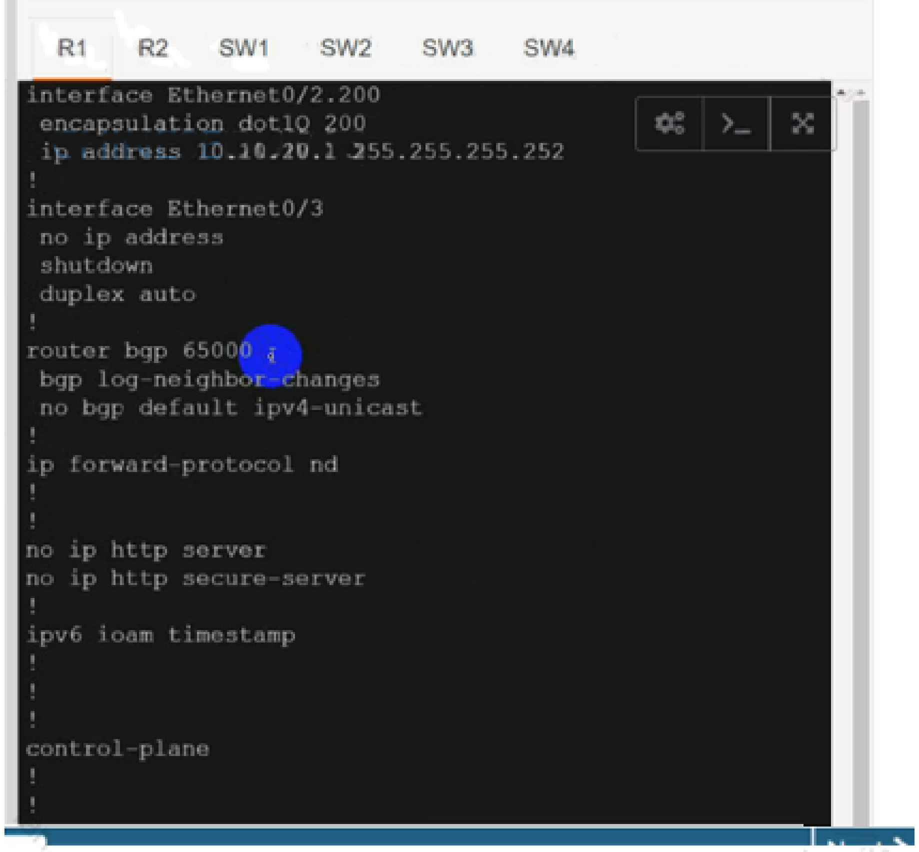
```
R1>
R1>
R1>
R1>
R1>en
R1#sh run
Building configuration...

Current configuration : 1353 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
```



```
!
!
!
!
!
!
!


!
ip vrf cu-green
 rd 65000:200
!
ip vrf cu-red
 rd 65000:100
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
```

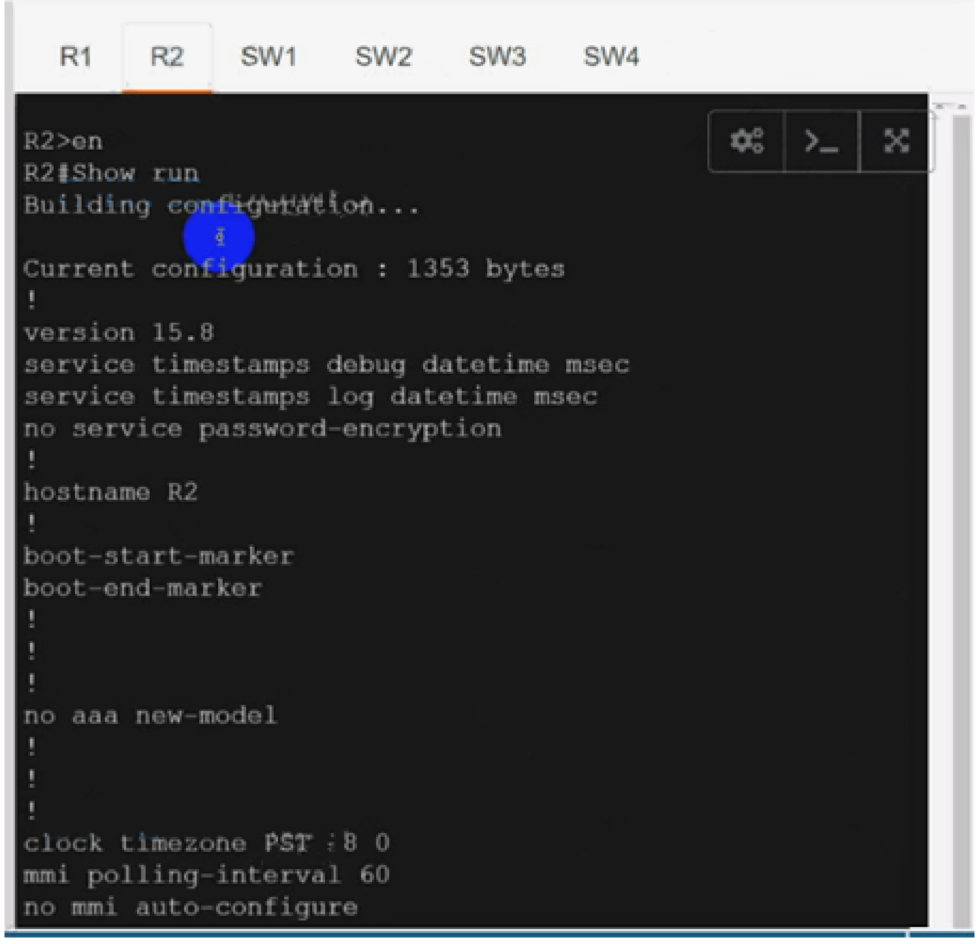


```
!
!
!
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.1.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.20.254 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 duplex auto
!
interface Ethernet0/2.100
 encapsulation dot1Q 100
 ip address 10.10.10.1 255.255.255.252
!
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.1 255.255.255.252
```

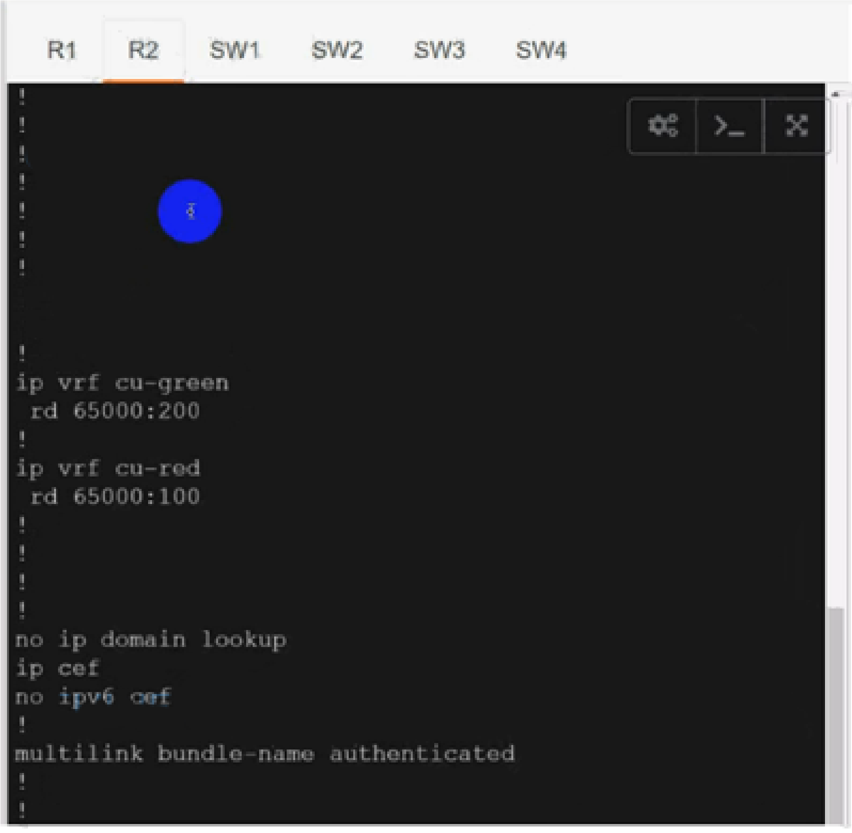


```
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.1 255.255.255.252
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!
```

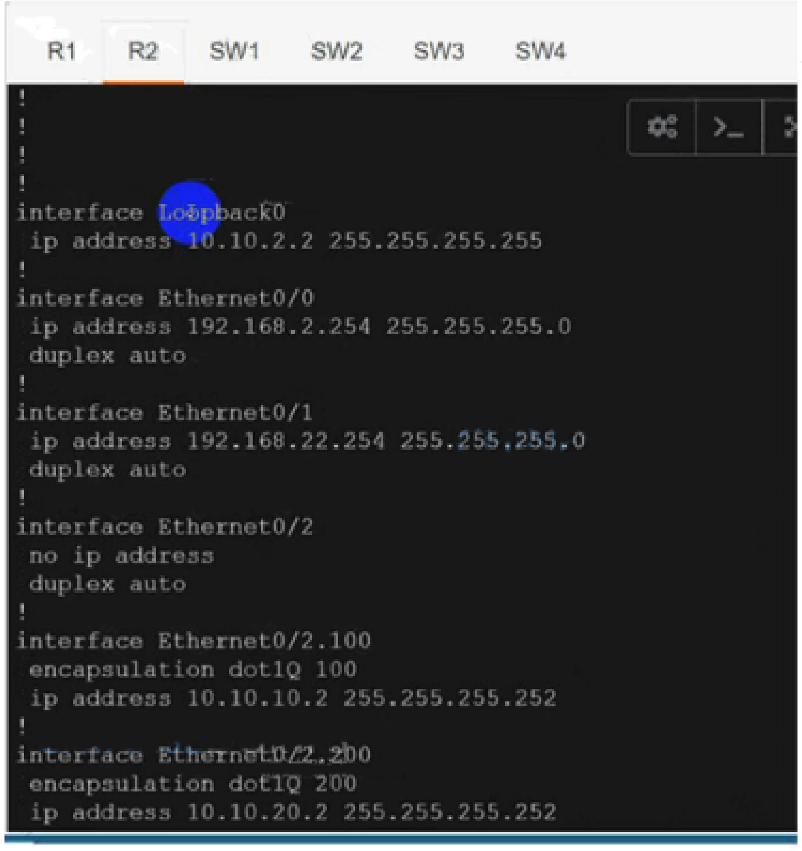
R2



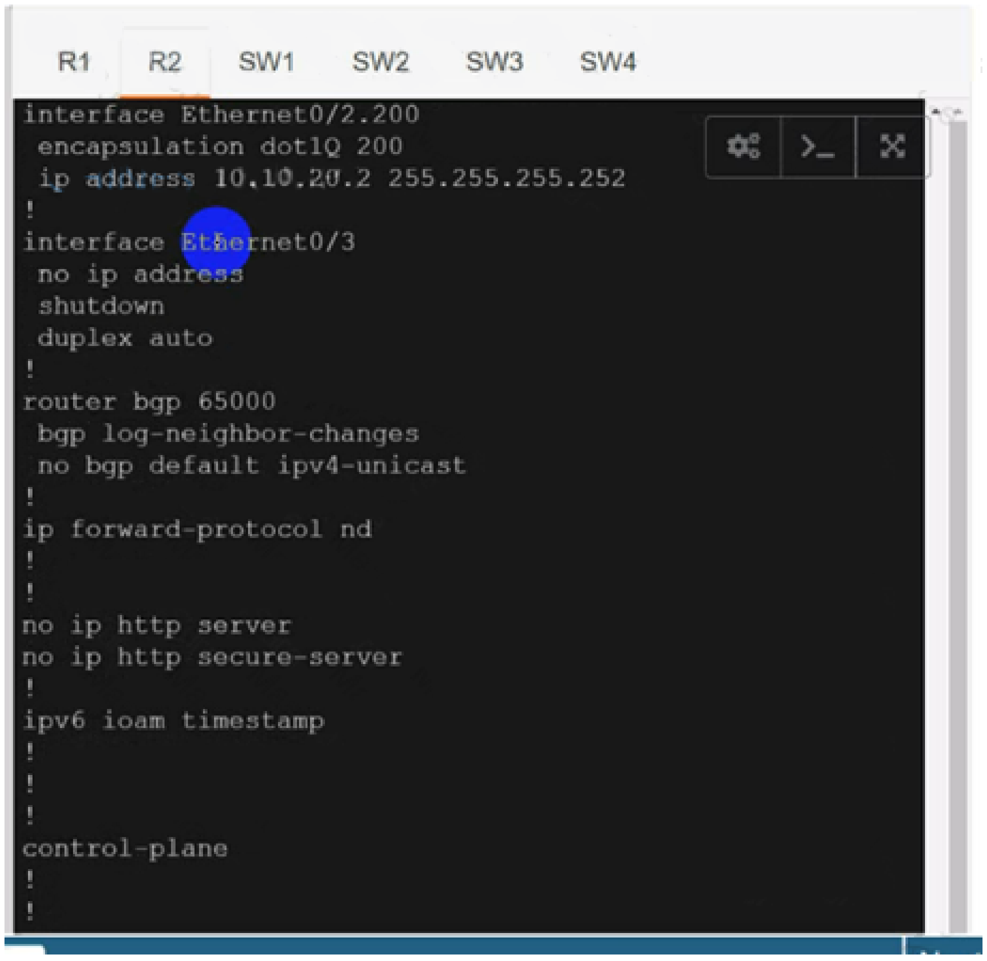
```
R2>en
R2#Show run
Building configuration...

Current configuration : 1353 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
```



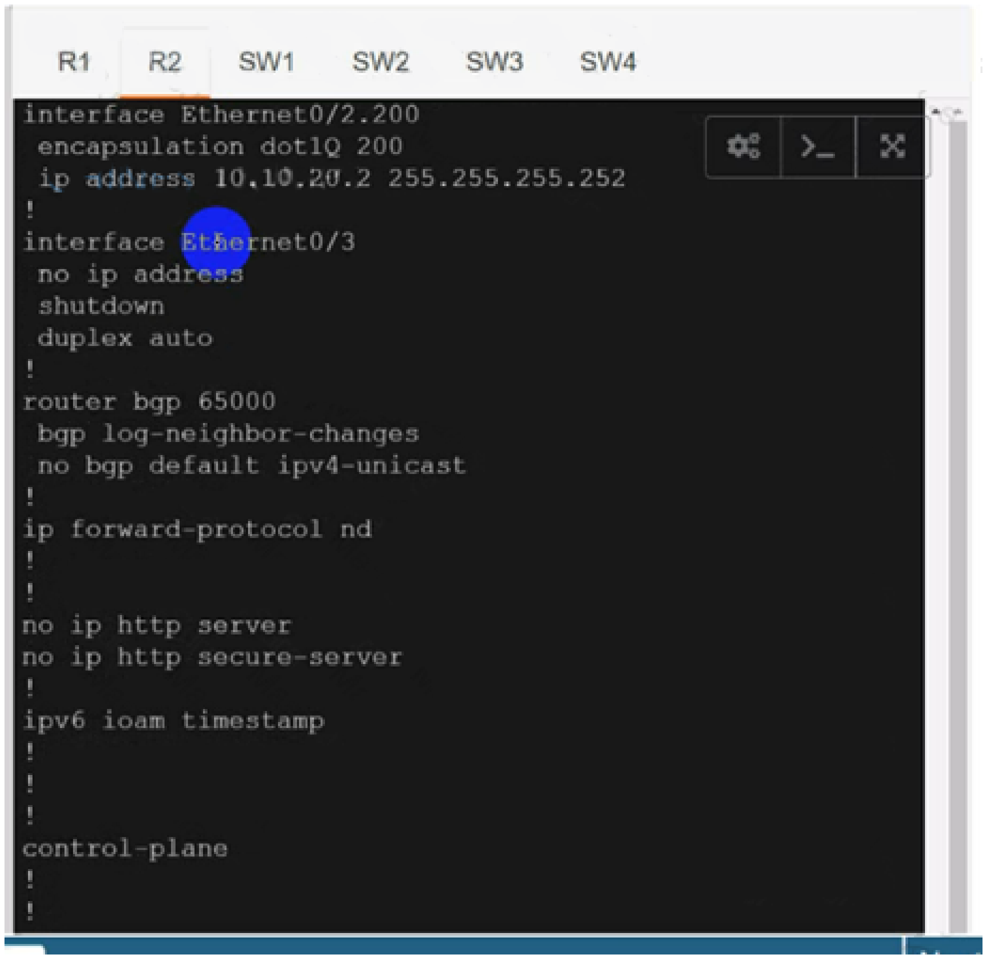
```
!
!
!
!
!
!
!



!
ip vrf cu-green
 rd 65000:200
!
ip vrf cu-red
 rd 65000:100
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
```



```
!
!
!
!
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.2.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.22.254 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 duplex auto
!
interface Ethernet0/2.100
 encapsulation dot1Q 100
 ip address 10.10.10.2 255.255.255.252
!
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.2 255.255.255.252
```

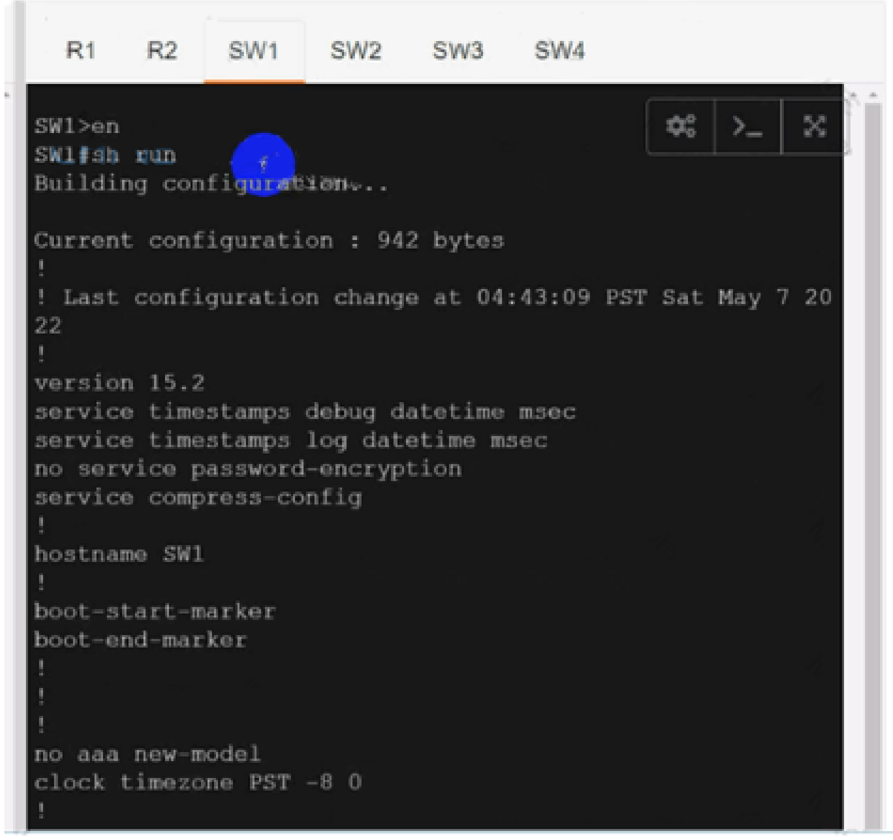


```
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.2 255.255.255.252
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!
```

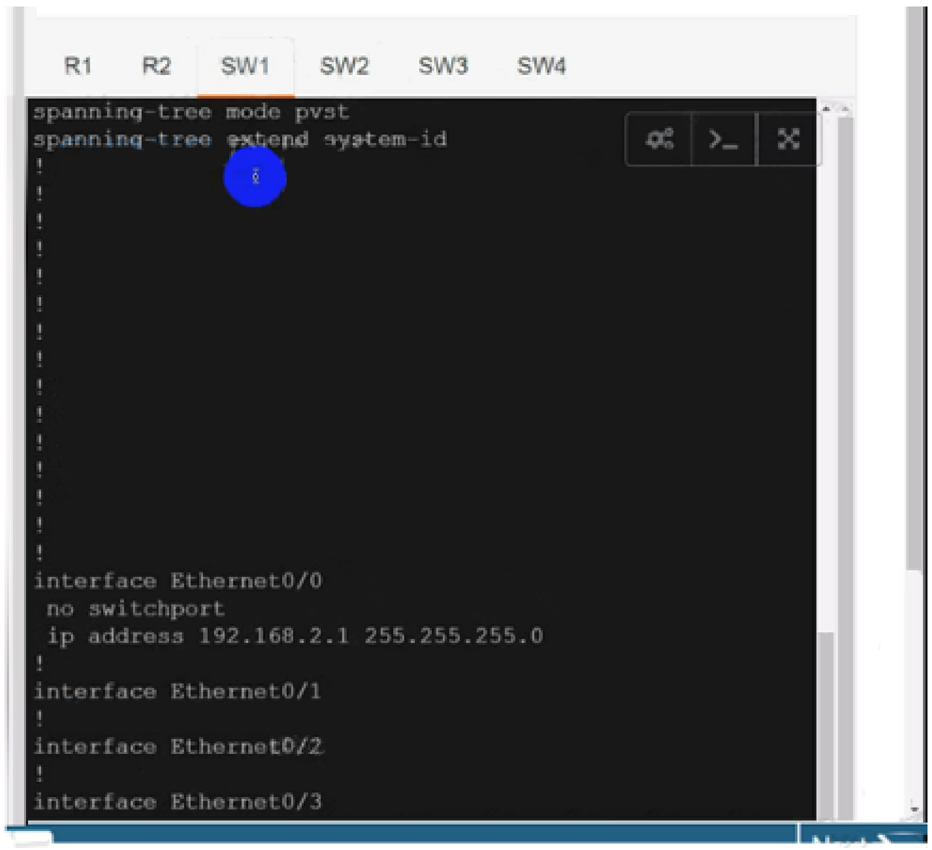

R1 R2 SW1 SW2 SW3 SW4

```
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.2 255.255.255.252
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!
```

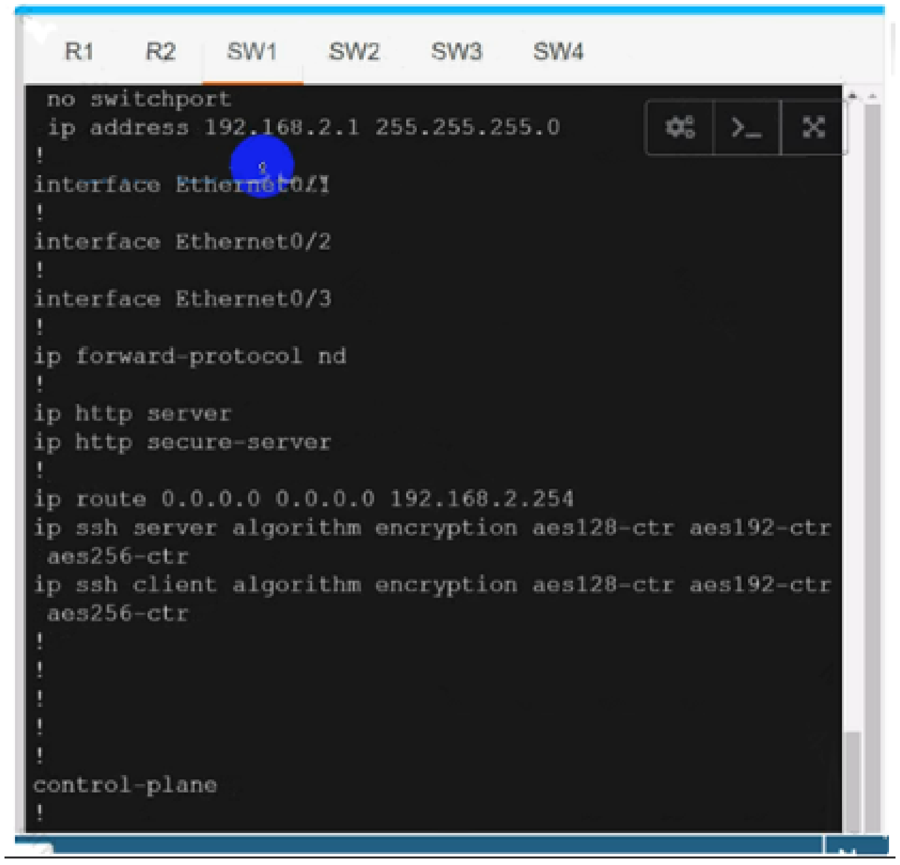
SW1



```
SW1>en
SW1#sh run
Building configuration...

Current configuration : 942 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!
```

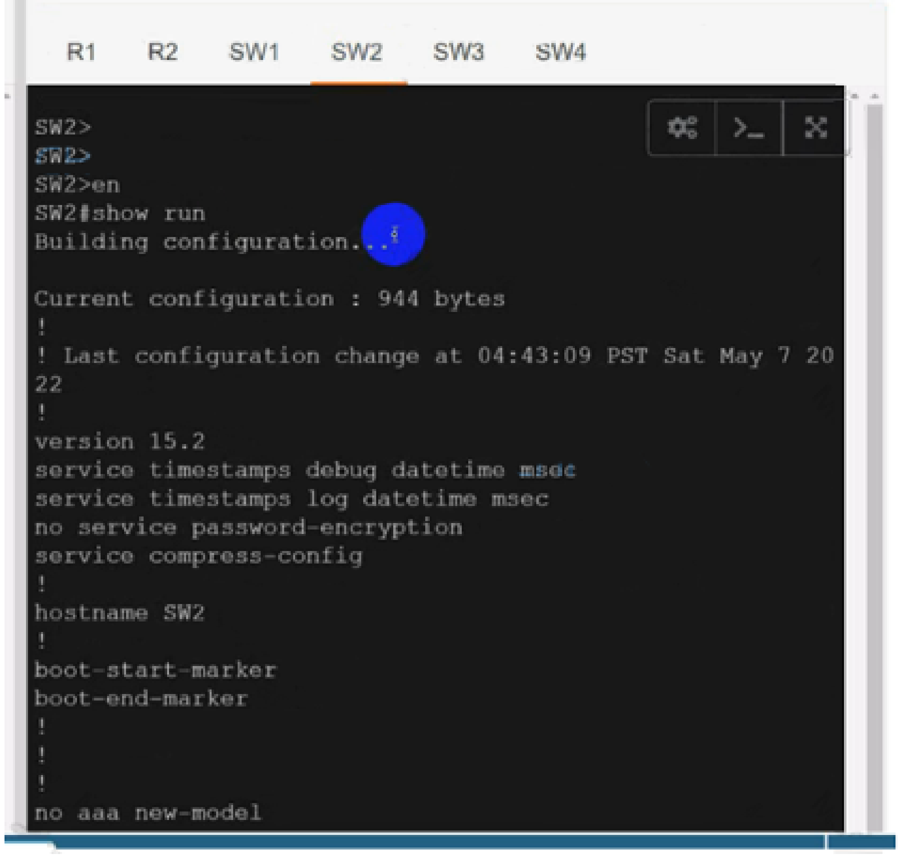


```
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 no switchport
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
```

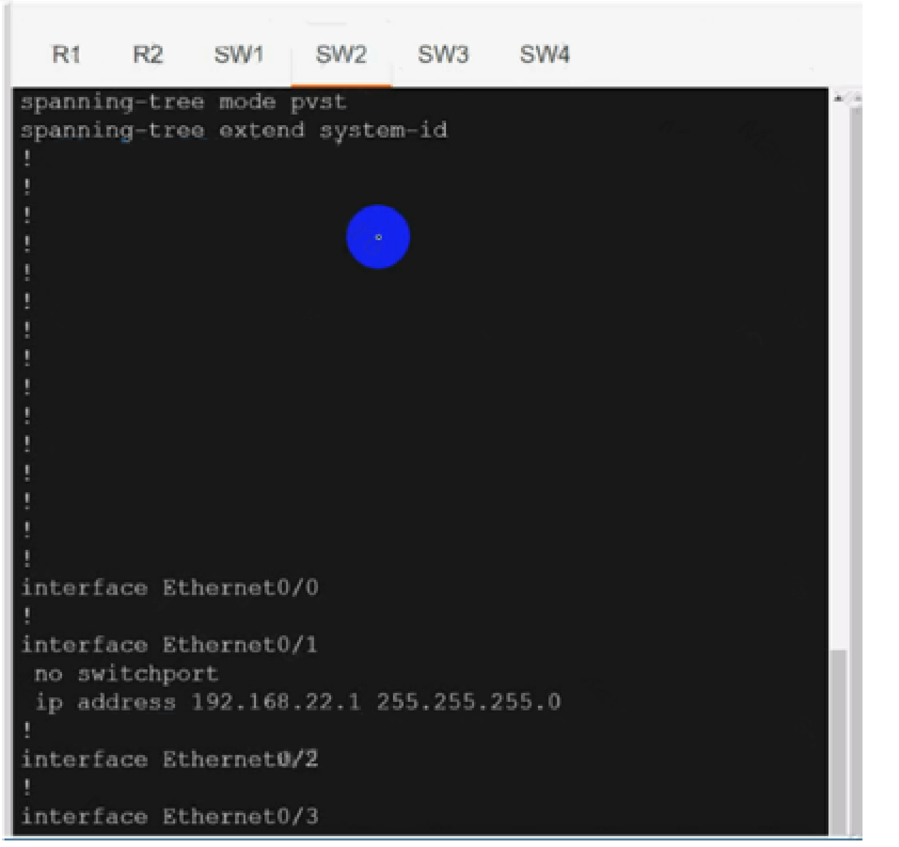


```
 no switchport
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.2.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
 aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
 aes256-ctr
!
!
!
!
!
control-plane
!
```

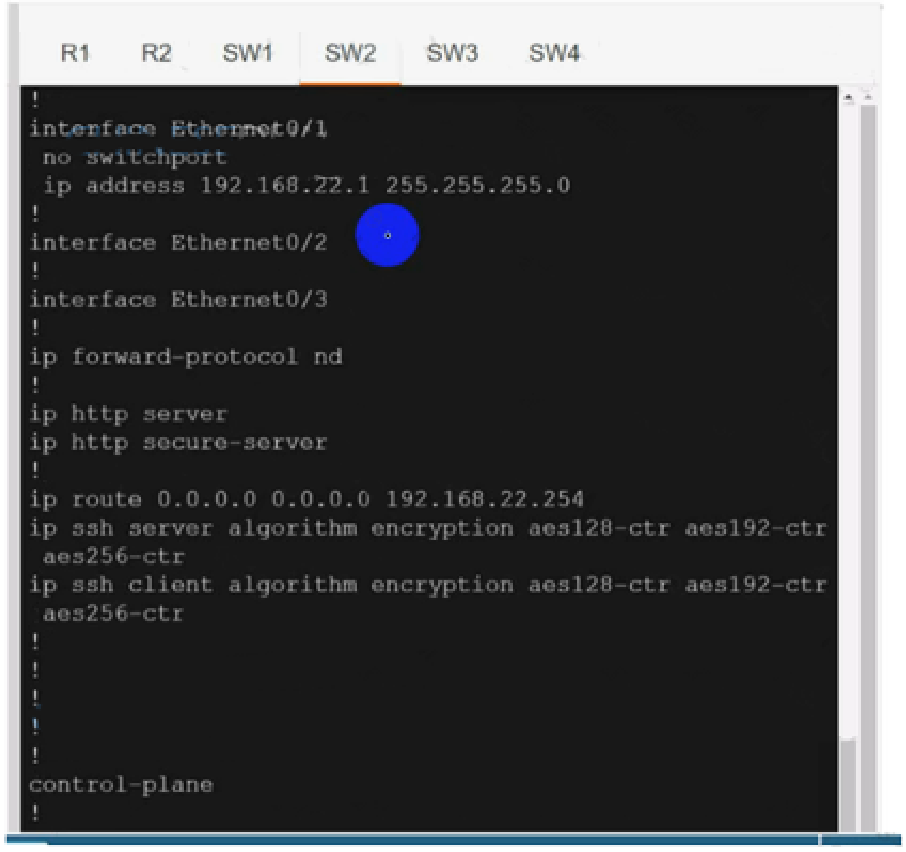
SW2



```
SW2>
SW2>
SW2>en
SW2#show run
Building configuration...

Current configuration : 944 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
```

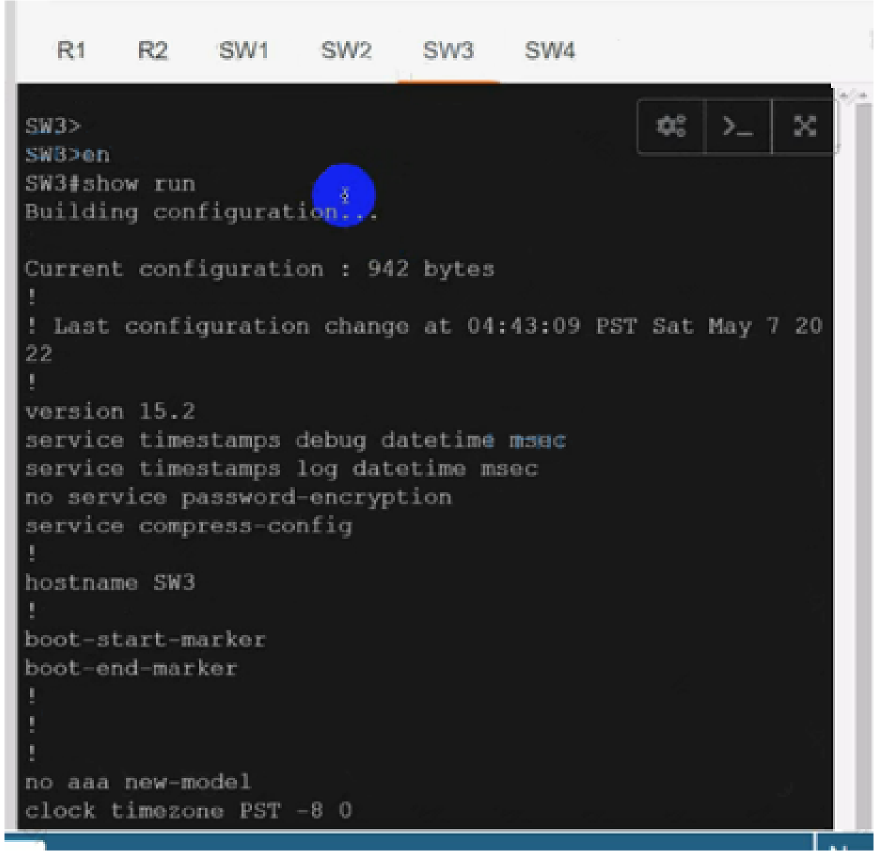


```
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
 no switchport
 ip address 192.168.22.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
```

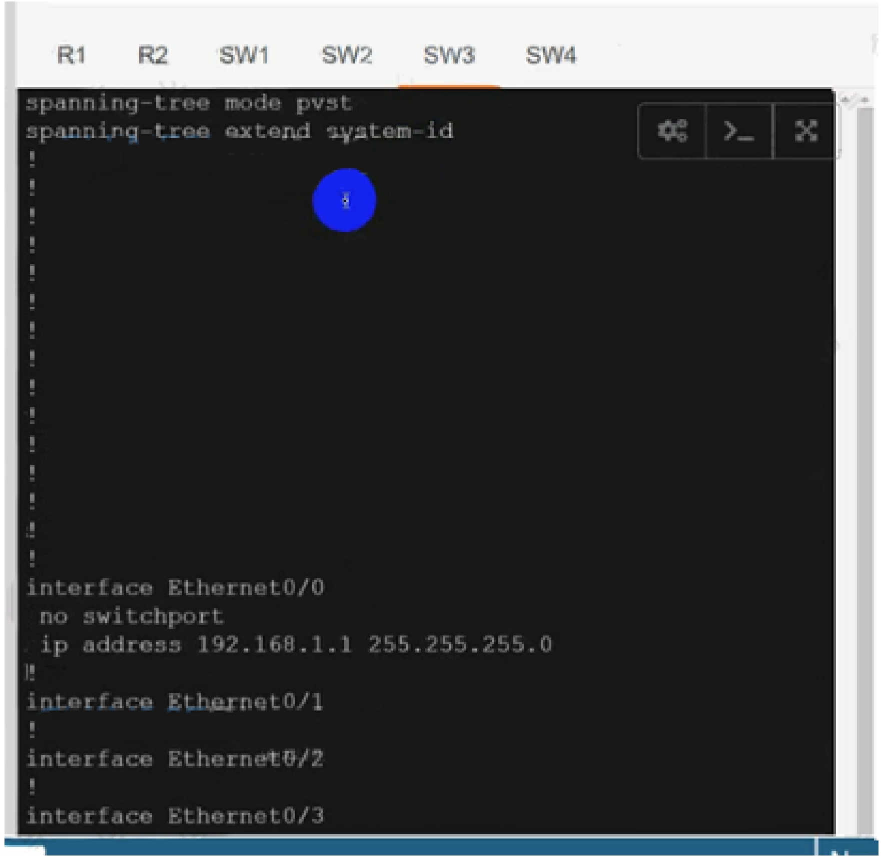


```
!
interface Ethernet0/1
 no switchport
 ip address 192.168.22.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.22.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
 aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
 aes256-ctr
!
!
!
!
!
control-plane
!
```

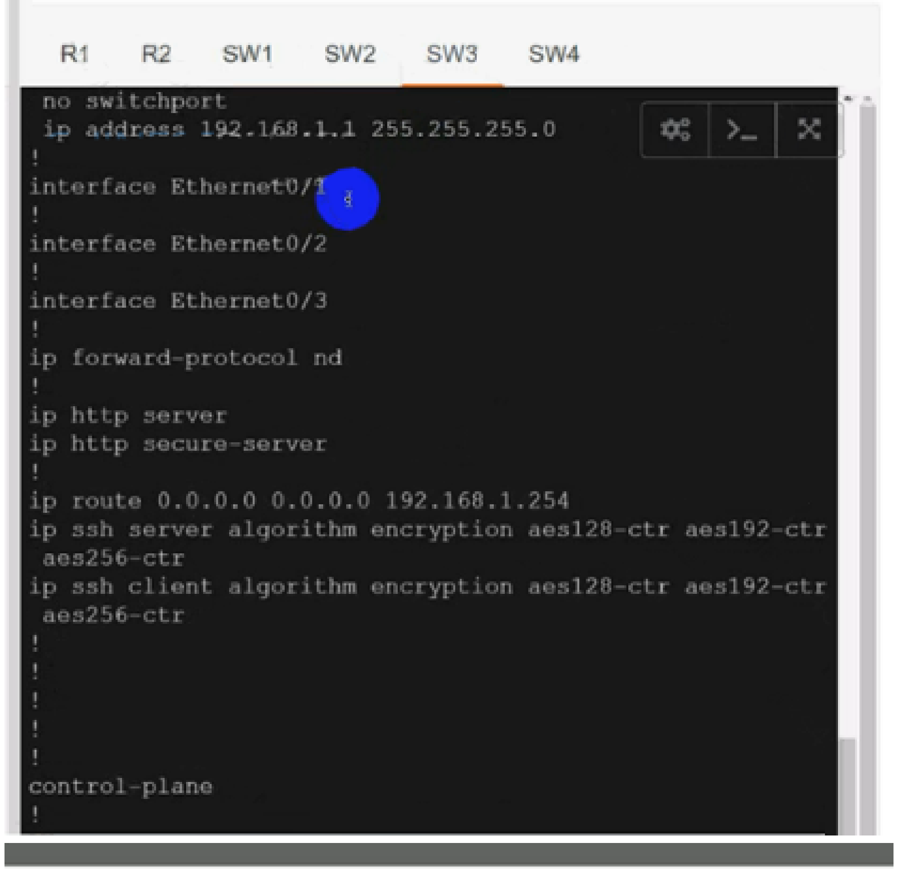
SW3



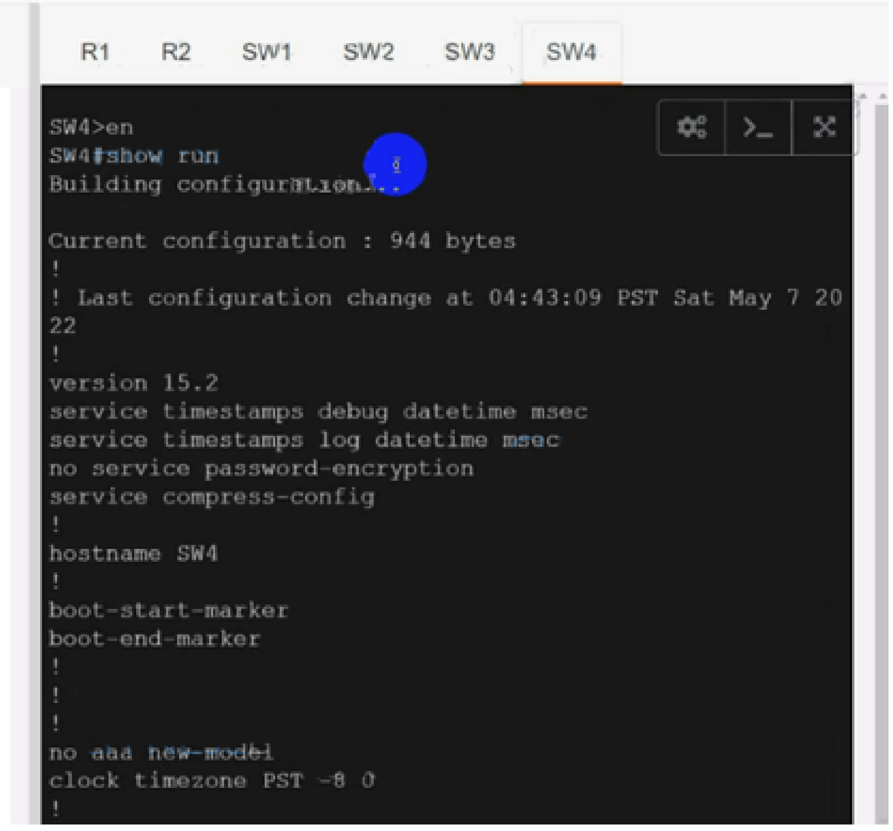
```
SW3>
SW3>en
SW3#show run
Building configuration...

Current configuration : 942 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
```



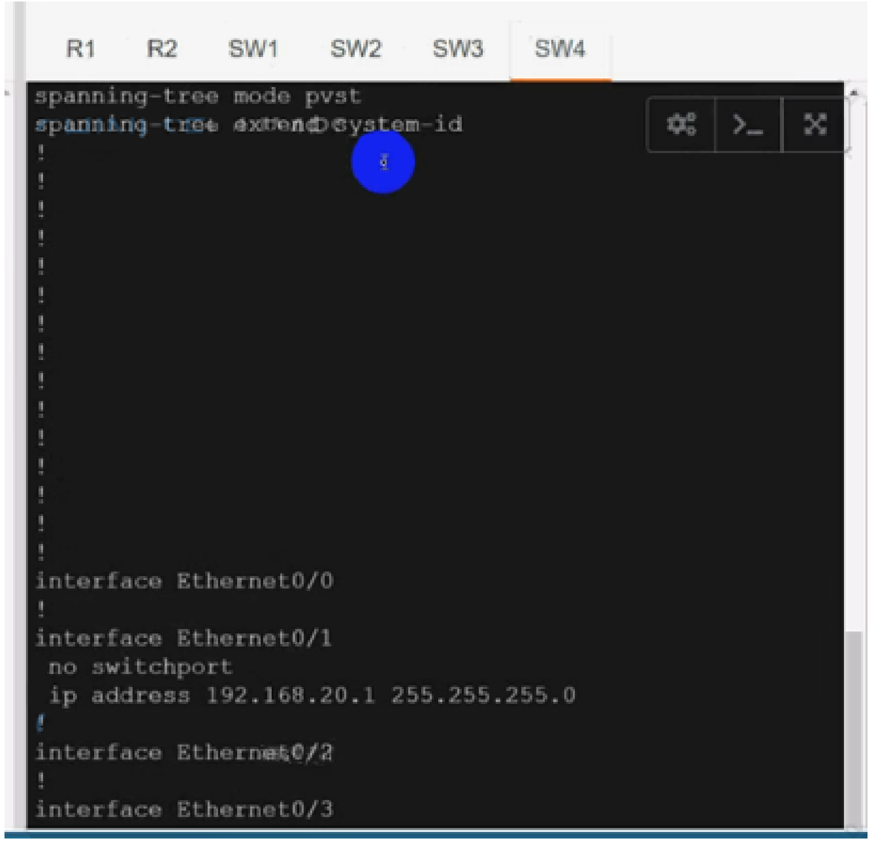
```
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 no switchport
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
```



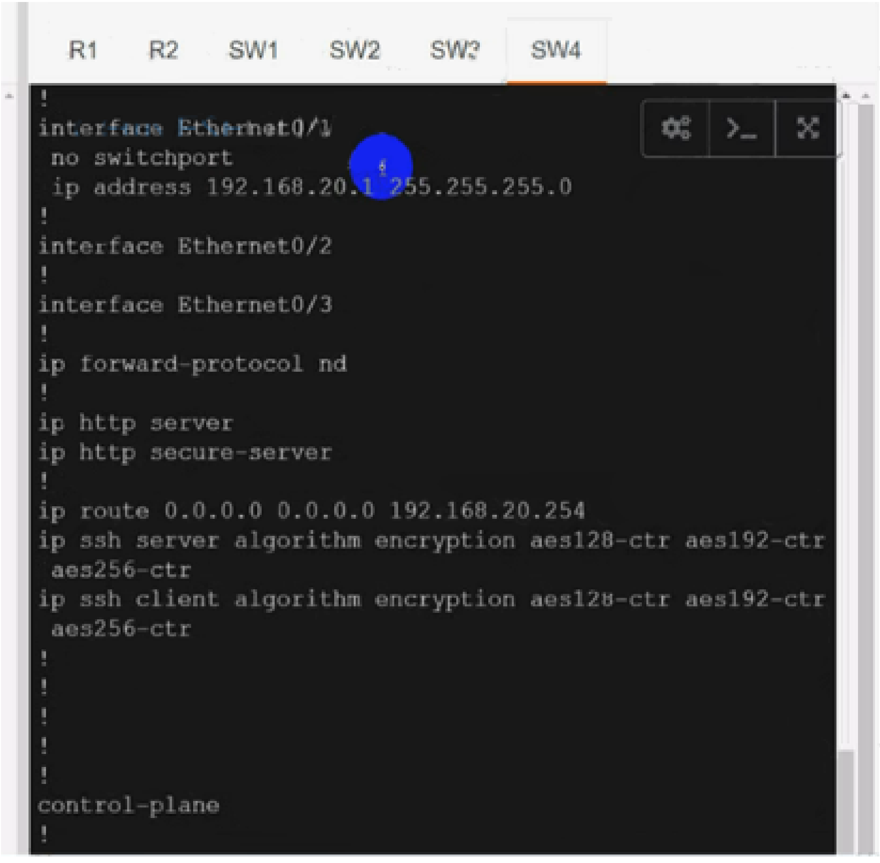
```
 no switchport
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
 aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
 aes256-ctr
!
!
!
!
!
control-plane
!
```



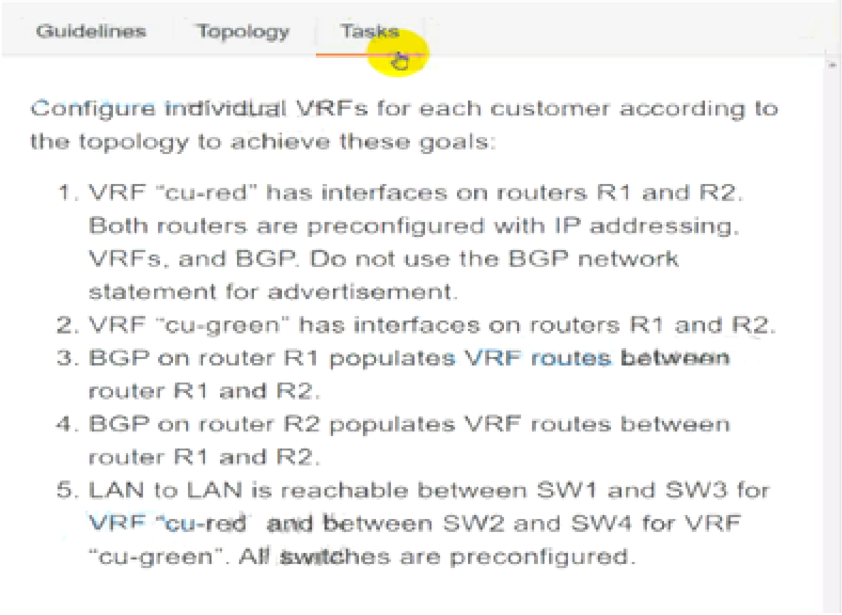
```
SW4>en
SW4#show run
Building configuration...

Current configuration : 944 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW4
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!
```



```
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
 no switchport
 ip address 192.168.20.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
```



```
!
interface Ethernet0/1
 no switchport
 ip address 192.168.20.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.20.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
 aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
 aes256-ctr
!
!
!
!
!
control-plane
!
```



Configure individual VRFs for each customer according to the topology to achieve these goals:

1. VRF "cu-red" has interfaces on routers R1 and R2. Both routers are preconfigured with IP addressing, VRFs, and BGP. Do not use the BGP network statement for advertisement.
2. VRF "cu-green" has interfaces on routers R1 and R2.
3. BGP on router R1 populates VRF routes between router R1 and R2.
4. BGP on router R2 populates VRF routes between router R1 and R2.
5. LAN to LAN is reachable between SW1 and SW3 for VRF "cu-red" and between SW2 and SW4 for VRF "cu-green". All switches are preconfigured.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Solution:
> Use cu-red under interfaces facing SW1 & SW3:
On R1:
interface Ethernet0/0
ip vrf forwarding cu-red
ip address 192.168.1.254 255.255.255.0
Check reachability to SW1: R1#ping vrf cu-red 192.168.1.1 Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
On R2:
interface Ethernet0/0
ip vrf forwarding cu-red
ip address 192.168.2.254 255.255.255.0
Check reachability to SW3: R2#ping vrf cu-red 192.168.2.1 Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
```

- Use vrf cu-green for SW2 & SW4:

```
On R1:
interface Ethernet0/1
ip vrf forwarding cu-green
ip address 192.168.20.254 255.255.255.0
Test reachability to SW2: R1#ping vrf cu-green 192.168.20.1 Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
On R2:
interface Ethernet0/1
ip vrf forwarding cu-green
ip address 192.168.22.254 255.255.255.0
Test reachability to SW4: R2#ping vrf cu-green 192.168.22.1 Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- On R1:

```
interface Ethernet0/2.100 mpls ip
!
interface Ethernet0/2.200 mpls ip
!
Configure BGP:
router bgp 65000
neighbor 10.10.10.2 remote-as 65000
neighbor 10.10.20.2 remote-as 65000
!
address-family vpnv4 neighbor 10.10.10.2 activate
neighbor 10.10.20.2 activate exit-address-family
!
address-family ipv4 vrf cu-green redistribute connected
exit-address-family
!
address-family ipv4 vrf cu-red redistribute connected
exit-address-family
!
R1(config)#ip vrf cu-red
R1(config-vrf)#route-target both 65000:100
!
R1(config)#ip vrf cu-green
R1(config-vrf)#route-target both 65000:200
```

- On R2:

```
interface Ethernet0/2.100
mpls ip
!
interface Ethernet0/2.200 mpls ip
!
router bgp 65000
neighbor 10.10.10.1 remote-as 65000
neighbor 10.10.20.1 remote-as 65000
!
address-family vpnv4 neighbor 10.10.10.1 activate
neighbor 10.10.20.1 activate exit-address-family
!
address-family ipv4 vrf cu-green redistribute connected
exit-address-family
!
address-family ipv4 vrf cu-red redistribute connected
exit-address-family R2(config)#ip vrf cu-red
R2(config-vrf)#route-target both 65000:100
!
R2(config)#ip vrf cu-green
R2(config-vrf)#route-target both 65000:200
```

- Verification:

```
From SW1 to SW3: SW1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
But can’t Reach SW2 or SW4 in VRF cu-green: SW1#ping 192.168.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
```

```
SW1#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
```

Same Test for SW2: From SW2 to SW4: SW2#ping 192.168.20.1

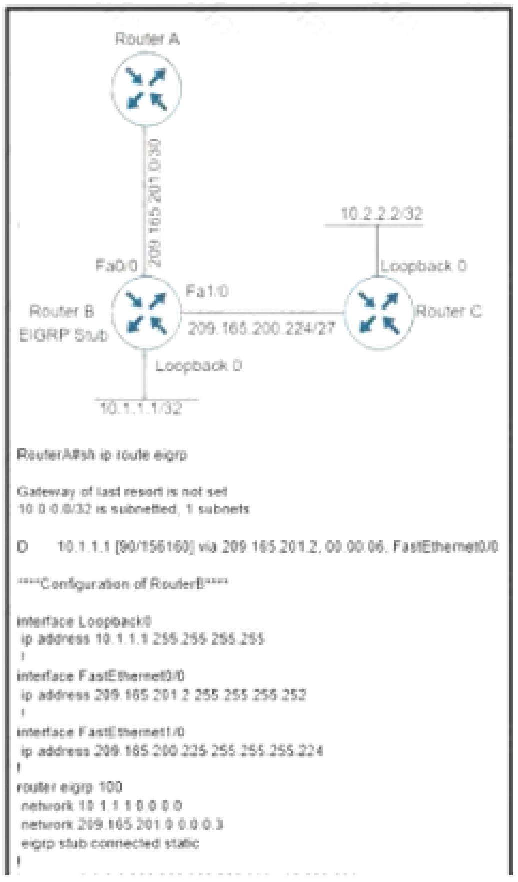
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

But can’t Reach SW3 or SW1 in VRF cu-red: SW2#ping 192.168.1.1

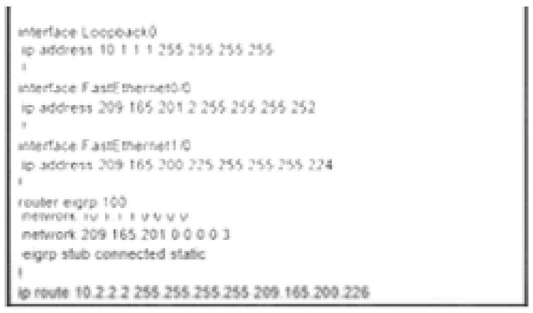
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
SW2#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
```

Both R1 & R2 has separate tables for VRFs cu-red and cu-green.

NEW QUESTION 55
- (Exam Topic 3)



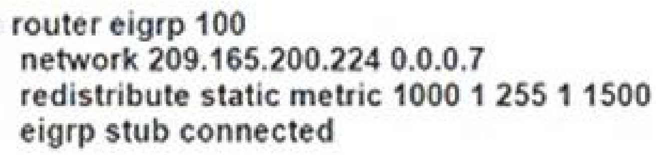
```
RouterA#sh ip route eigrp

Gateway of last resort is not set
10.0.0.0/32 is subnetted, 1 subnets

D      10.1.1.1 [90/156160] via 209.165.201.2, 00:00:06, FastEthernet0/0

****Configuration of RouterB****

interface Loopback0
 ip address 10.1.1.1 255.255.255.255
 !
interface FastEthernet0/0
 ip address 209.165.201.2 255.255.255.252
 !
interface FastEthernet1/0
 ip address 209.165.200.225 255.255.255.224
!
router eigrp 100
 network 10.1.1.1 0.0.0.0
 network 209.165.201.0 0.0.0.3
 eigrp stub connected static
!
```



```
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
 !
interface FastEthernet0/0
 ip address 209.165.201.2 255.255.255.252
 !
interface FastEthernet1/0
 ip address 209.165.200.225 255.255.255.224
!
router eigrp 100
 network 10.1.1.1 0.0.0.0
 network 209.165.201.0 0.0.0.3
 eigrp stub connected static
!
ip route 10.2.2.2 255.255.255.255 209.165.200.226
```

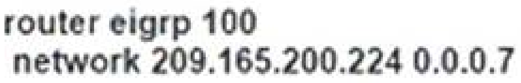
Refer to the exhibit. Not all connected and static routes of router B are received by router A even though EIGRP neighborship is established between the routers. Which configuration resolves the issue?

A)



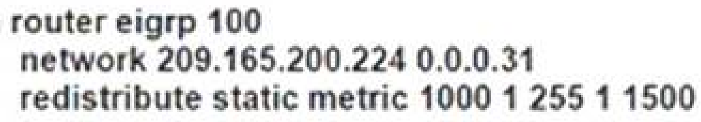
```
router eigrp 100
 network 209.165.200.224 0.0.0.7
 redistribute static metric 1000 1 255 1 1500
 eigrp stub connected
```

B)



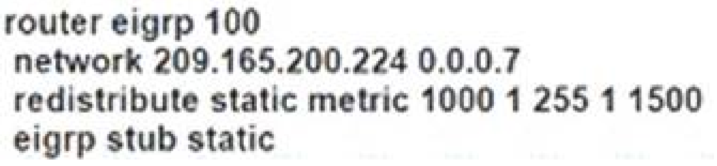
```
router eigrp 100
 network 209.165.200.224 0.0.0.7
```

C)



```
router eigrp 100
 network 209.165.200.224 0.0.0.31
 redistribute static metric 1000 1 255 1 1500
```

D)



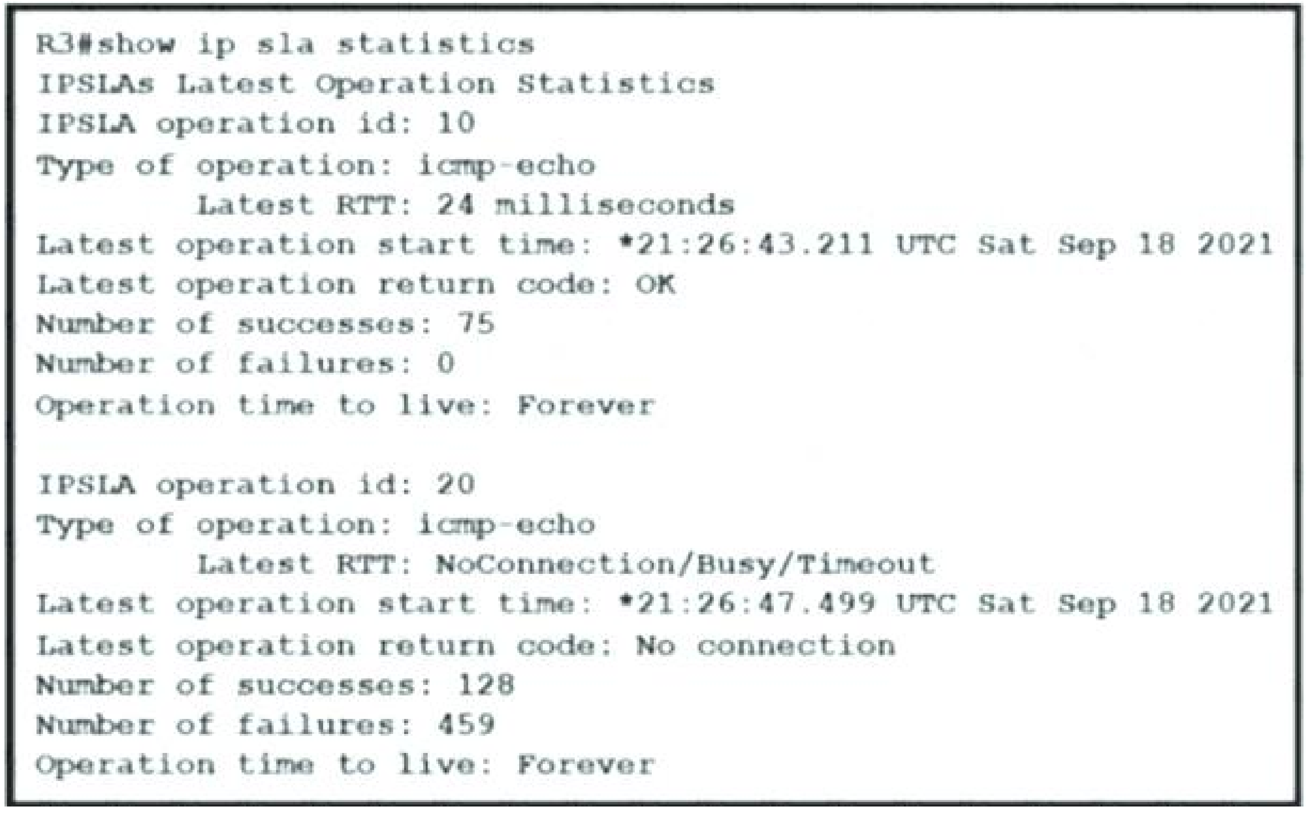
```
router eigrp 100
 network 209.165.200.224 0.0.0.7
 redistribute static metric 1000 1 255 1 1500
 eigrp stub static
```

A. Option A
B. Option B

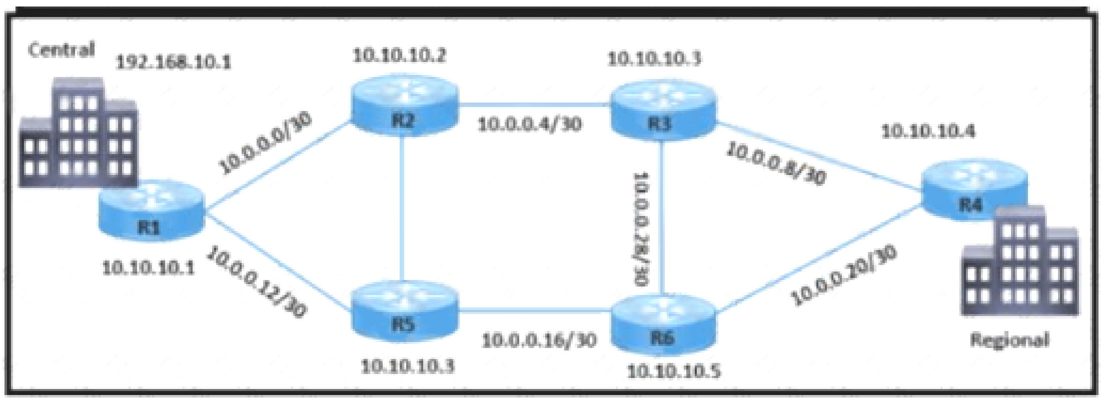
C. Option C
D. Option D

Answer: D

NEW QUESTION 56
- (Exam Topic 3)



```
R3#show ip sla statistics
IPSLAs Latest Operation Statistics
IPSLA operation id: 10
Type of operation: icmp-echo
        Latest RTT: 24 milliseconds
Latest operation start time: *21:26:43.211 UTC Sat Sep 18 2021
Latest operation return code: OK
Number of successes: 75
Number of failures: 0
Operation time to live: Forever

IPSLA operation id: 20
Type of operation: icmp-echo
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: *21:26:47.499 UTC Sat Sep 18 2021
Latest operation return code: No connection
Number of successes: 128
Number of failures: 459
Operation time to live: Forever
```

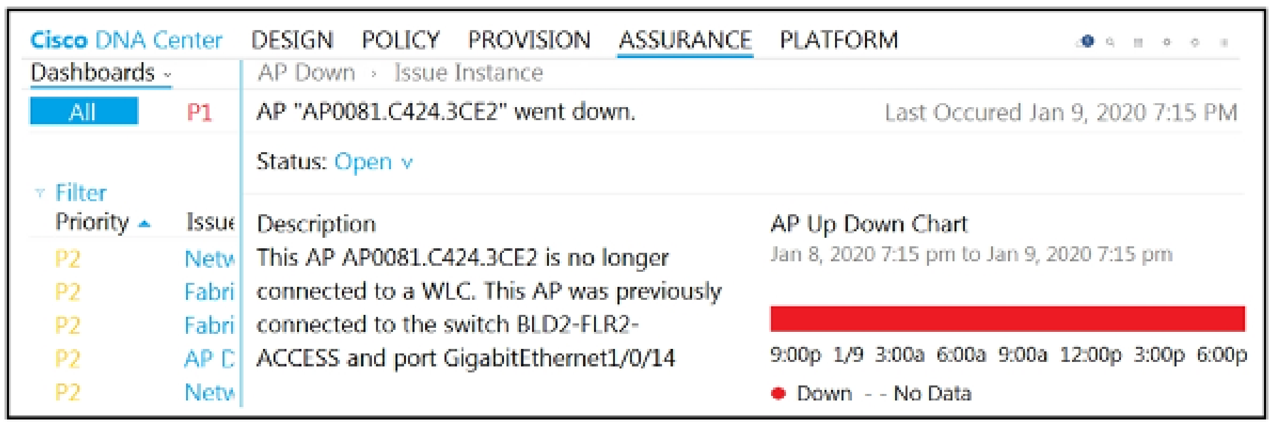


Refer to me exhibit Traffic from R3 to the central site does not use alternate paths when R3 cannot reach 10 10 10 2 Traffic on R3 destined to R4 takes an alternate route via 10 10 10.6 when 10 10 10 4 is not accessible from R3 Which configuration switches traffic destined to 10 10 10 2 from R3 on the alternate path''

A. R3(config)#ip route 192.168.10.1 255.255.265.255 10.10.10.2 track 20
B. R2(config)#ip route 10.10 10 3 255 255.255 255 10.0.0.6
C. R3(config)#track(20 ip sla 20 reachability
D. R6(config)#ip route 10.10.10 3 255.255.255.255 10.0.0.30

Answer: A

NEW QUESTION 58
- (Exam Topic 3)
Refer to the exhibit.



AP "AP0081.C424.3CE2" went down.

Last Occured Jan 9, 2020 7:15 PM

Status: Open

Description

This AP AP0081.C424.3CE2 is no longer connected to a WLC. This AP was previously connected to the switch BLD2-FLR2-ACCESS and port GigabitEthernet1/0/14

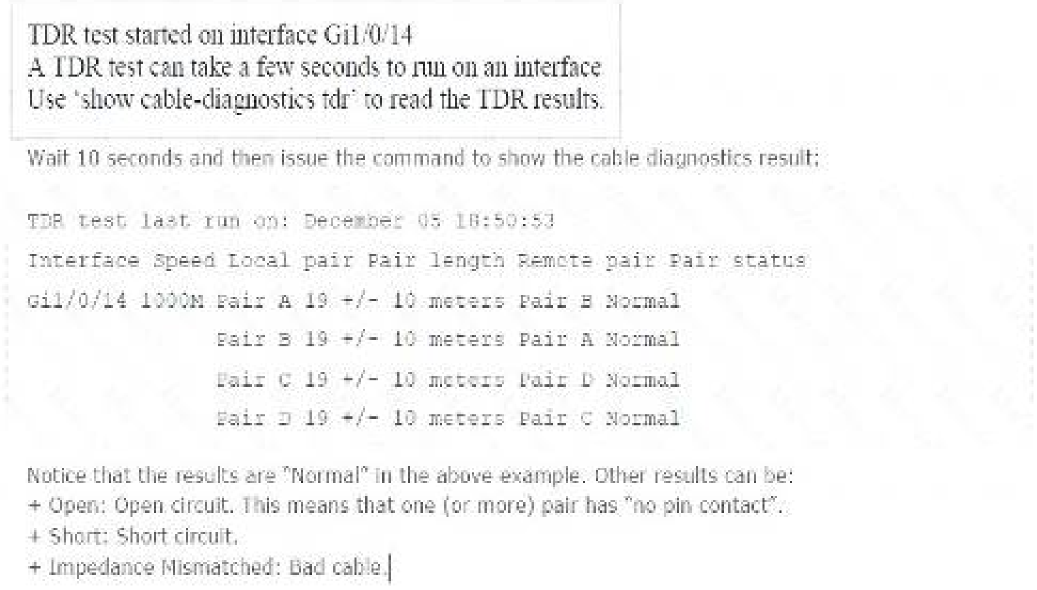
The AP status from Cisco DNA Center Assurance Dashboard shows some physical connectivity issues from access switch interface G1/0/14. Which command generates the diagnostic data to resolve the physical connectivity issues?

A. test cable diagnostics tdr interface GigabitEthernet1/0/14
B. Check cable-diagnostics tdr interface GigabitEthernet1/0/14
C. show cable-diagnostics tdr interface GigabitEthernet1/0/14
D. Verify cable-diagnostics tdr interface GigabitEthernet1/0/14

Answer: A

Explanation:
The Time Domain Reflectometer (TDR) feature allows you to determine if a cable is OPEN or SHORT when it is at fault.
To start the TDR test, perform this task:

Step 1 (Starts the TDR test): test cable-diagnostics tdr {interface {interface-number}}
Step 2 (Displays the TDR test counter information): show cable-diagnostics tdr {interface interface-number}
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/16-11/configuration_guide/int_hw/b_1611_int_and_hw_9600_cg/checking_port_status_and_connectivity pdf
Text, table Description automatically generated



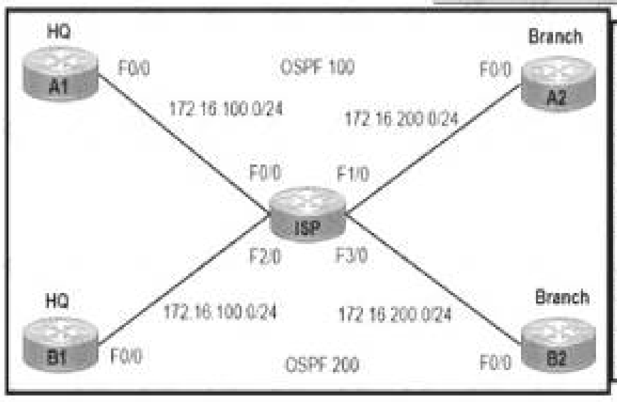
```
TDR test started on interface Gi1/0/14
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

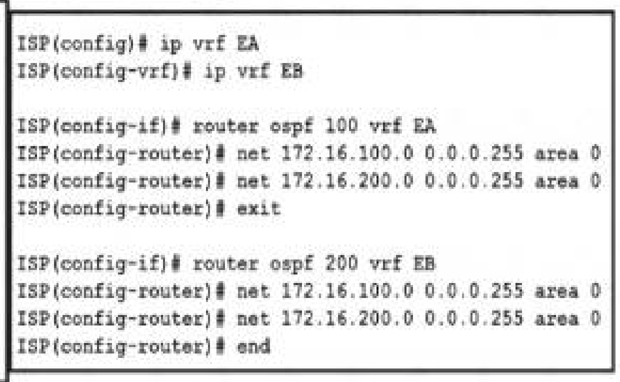
Wait 10 seconds and then issue the command to show the cable diagnostics result:

```
TDR test last run on: December 05 18:50:53
Interface Speed Local pair Pair length Remote pair Pair status
Gi1/0/14 1000M Pair A 19 +/- 10 meters Pair B Normal
               Pair B 19 +/- 10 meters Pair A Normal
               Pair C 19 +/- 10 meters Pair D Normal
               Pair D 19 +/- 10 meters Pair C Normal
```

Notice that the results are "Normal" in the above example. Other results can be:
+ Open: Open circuit. This means that one (or more) pair has "no pin contact".
+ Short: Short circuit.
+ Impedance Mismatched: Bad cable.

NEW QUESTION 63
- (Exam Topic 3)

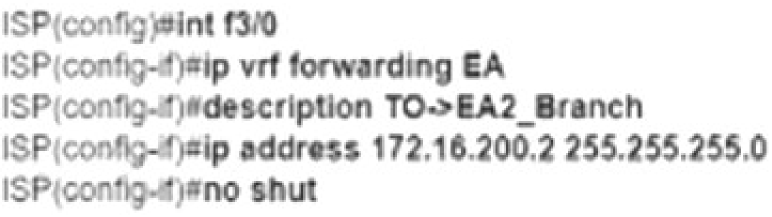




```
ISP(config)# ip vrf EA
ISP(config-vrf)# ip vrf EB

ISP(config-if)# router ospf 100 vrf EA
ISP(config-router)# net 172.16.100.0 0.0.0.255 area 0
ISP(config-router)# net 172.16.200.0 0.0.0.255 area 0
ISP(config-router)# exit

ISP(config-if)# router ospf 200 vrf EB
ISP(config-router)# net 172.16.100.0 0.0.0.255 area 0
ISP(config-router)# net 172.16.200.0 0.0.0.255 area 0
ISP(config-router)# end
```

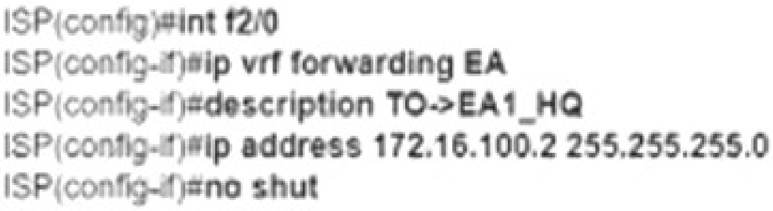
Refer to the exhibit. A network engineer is provisioning end-to-end traffic service for two different enterprise networks with these requirements
- The OSPF process must differ between customers on HQ and Branch office routers, and adjacencies should come up instantly.
- The enterprise networks are connected with overlapping networks between HO and a branch office Which configuration meets the requirements for a customer site?

A)



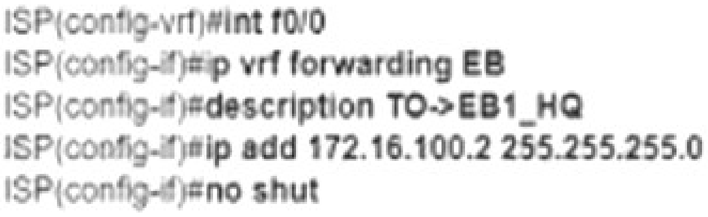
```
ISP(config)#int f3/0
ISP(config-if)#ip vrf forwarding EA
ISP(config-if)#description TO->EA2_Branch
ISP(config-if)#ip address 172.16.200.2 255.255.255.0
ISP(config-if)#no shut
```

B)



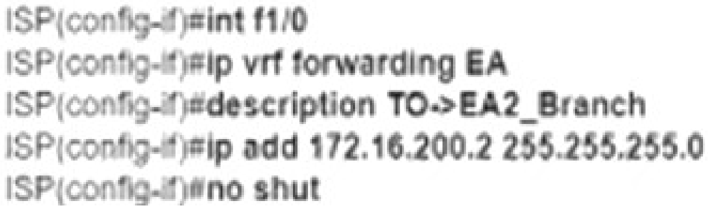
```
ISP(config)#int f2/0
ISP(config-if)#ip vrf forwarding EA
ISP(config-if)#description TO->EA1_HQ
ISP(config-if)#ip address 172.16.100.2 255.255.255.0
ISP(config-if)#no shut
```

C)



```
ISP(config-vrf)#int f0/0
ISP(config-if)#ip vrf forwarding EB
ISP(config-if)#description TO->EB1_HQ
ISP(config-if)#ip add 172.16.100.2 255.255.255.0
ISP(config-if)#no shut
```

D)



```
ISP(config-if)#int f1/0
ISP(config-if)#ip vrf forwarding EA
ISP(config-if)#description TO->EA2_Branch
ISP(config-if)#ip add 172.16.200.2 255.255.255.0
ISP(config-if)#no shut
```

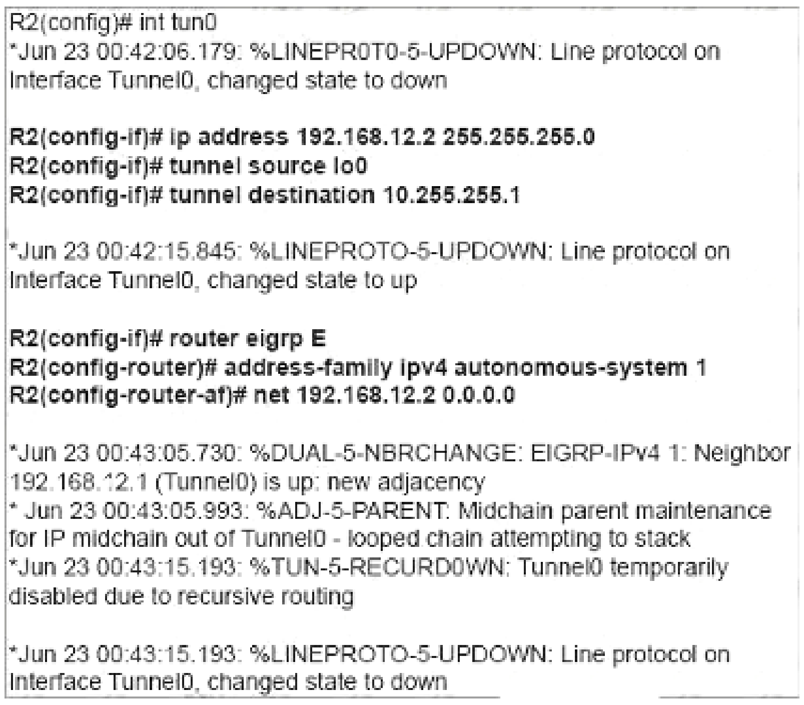
A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 66

- (Exam Topic 3)

Refer to the exhibit.



```
R2(config)# int tun0
*Jun 23 00:42:06.179: %LINEPR0T0-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to down

R2(config-if)# ip address 192.168.12.2 255.255.255.0
R2(config-if)# tunnel source lo0
R2(config-if)# tunnel destination 10.255.255.1

*Jun 23 00:42:15.845: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to up

R2(config-if)# router eigrp E
R2(config-router)# address-family ipv4 autonomous-system 1
R2(config-router-af)# net 192.168.12.2 0.0.0.0

*Jun 23 00:43:05.730: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.12.1 (Tunnel0) is up: new adjacency
* Jun 23 00:43:05.993: %ADJ-5-PARENT: Midchain parent maintenance
for IP midchain out of Tunnel0 - looped chain attempting to stack
*Jun 23 00:43:15.193: %TUN-5-RECURD0WN: Tunnel0 temporarily
disabled due to recursive routing

*Jun 23 00:43:15.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to down
```

An administrator is configuring a GRE tunnel to establish an EIGRP neighbor to a remote router. The other tunnel endpoint is already configured. After applying the configuration as shown, the tunnel started flapping. Which action resolves the issue?

A. Modify the network command to use the Tunnel0 interface netmask
B. Advertise the Loopback0 interface from R2 across the tunnel
C. Stop sending a route matching the tunnel destination across the tunnel
D. Readdress the IP network on the Tunnel0 on both routers using the /31 netmask

Answer: C

Explanation:

In this question we are advertising the tunnel IP address 192.168.12.2 to the other side. When other end receives the EIGRP advertisement, it realizes it can reach the other side of the tunnel via EIGRP. In other words, it reaches the tunnel destination through the tunnel itself -> This causes “recursive routing” error.

Note: In order to avoid this error, do not advertise the tunnel destination IP address on the tunnel interface to other side.

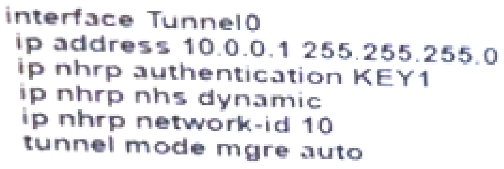
Good recursive routing reference: https://networklessons.com/cisco/ccie-routing-switching/gretunnel- recursive-routing-error

NEW QUESTION 67

- (Exam Topic 3)

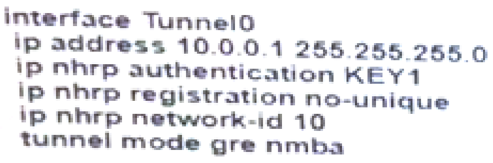
A company is expanding business by opening 35 branches over the Internet. A network engineer must configure DMVPN at the branch routers to connect with the hub router and allow NHRP to add spoke routers securely to the multicast NHRP mappings automatically Which configuration meets this requirement at the hub router?

A)



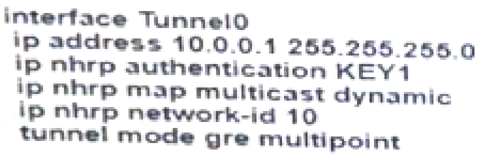
```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication KEY1
 ip nhrp nhs dynamic
 ip nhrp network-id 10
 tunnel mode mgre auto
```

B)



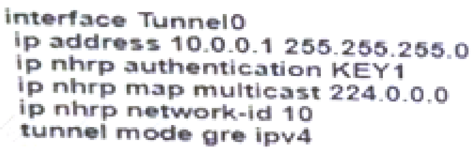
```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication KEY1
 ip nhrp registration no-unique
 ip nhrp network-id 10
 tunnel mode gre nmba
```

C)



```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication KEY1
 ip nhrp map multicast dynamic
 ip nhrp network-id 10
 tunnel mode gre multipoint
```

D)



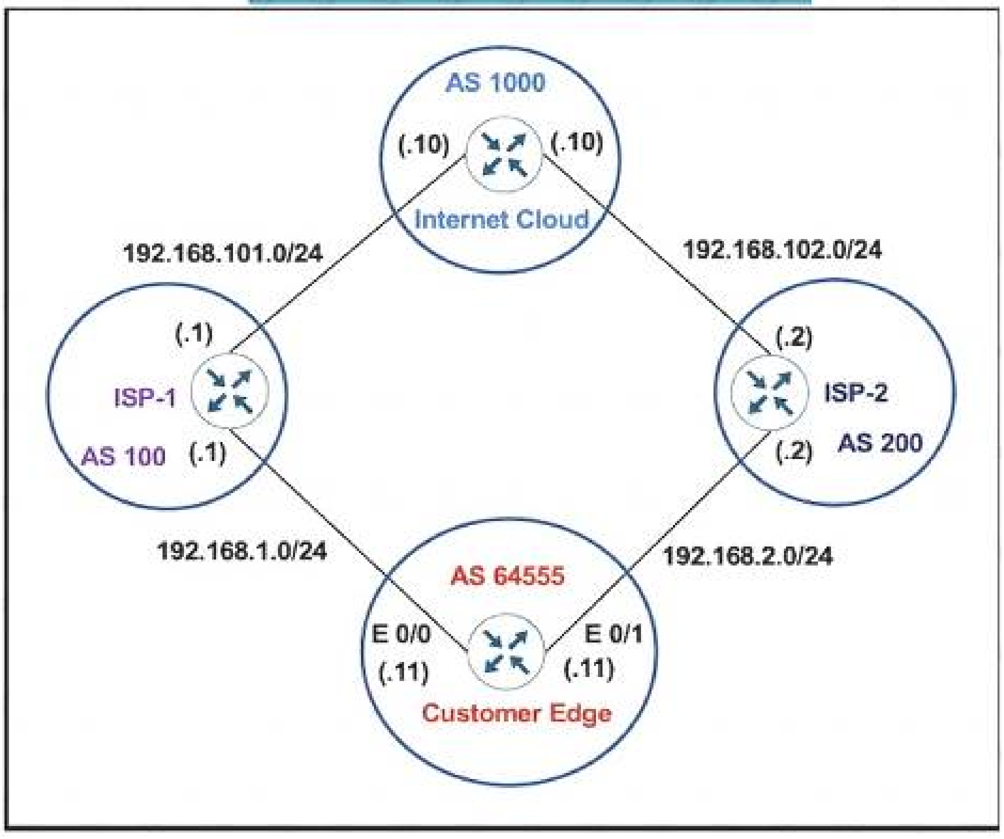
```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication KEY1
 ip nhrp map multicast 224.0.0.0
 ip nhrp network-id 10
 tunnel mode gre ipv4
```

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

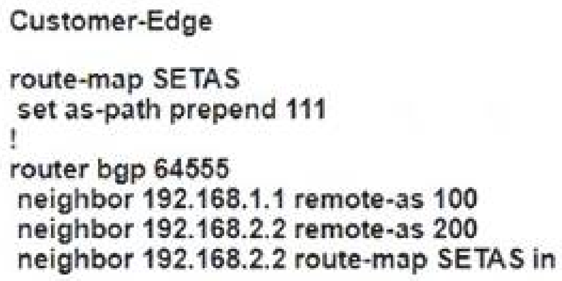
Answer: C

Explanation:
The command “ip nhrp map multicast dynamic” allows NHRP to automatically add spoke routers to the multicast NHRP mappings.

NEW QUESTION 68
- (Exam Topic 3)



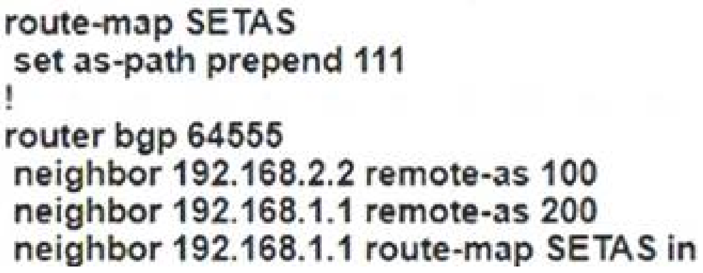
Refer lo lhe exhibit. The Customer Edge rouler wants to use AS 100 as the preferred ISP for all external routes and ISP-2 as a backup.



```
Customer-Edge

route-map SETAS
 set as-path prepend 111
!
router bgp 64555
 neighbor 192.168.1.1 remote-as 100
 neighbor 192.168.2.2 remote-as 200
 neighbor 192.168.2.2 route-map SETAS in
```

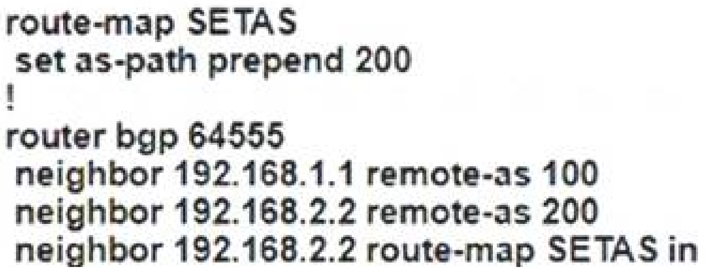
After this configuration, all the backup routes have disappeared from the BGP table on the Customer Edge router. Which set of configurations resolves the issue on the Customer Edge router?

A)



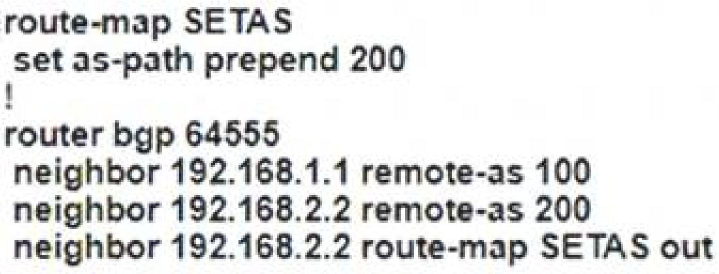
```
route-map SETAS
 set as-path prepend 111
!
router bgp 64555
 neighbor 192.168.2.2 remote-as 100
 neighbor 192.168.1.1 remote-as 200
 neighbor 192.168.1.1 route-map SETAS in
```

B)



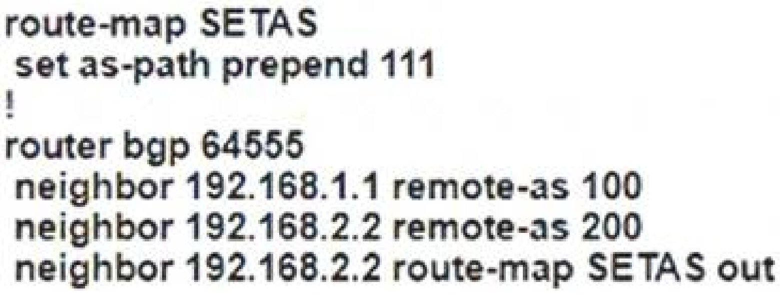
```
route-map SETAS
 set as-path prepend 200
!
router bgp 64555
 neighbor 192.168.1.1 remote-as 100
 neighbor 192.168.2.2 remote-as 200
 neighbor 192.168.2.2 route-map SETAS in
```

C)



```
route-map SETAS
 set as-path prepend 200
!
router bgp 64555
 neighbor 192.168.1.1 remote-as 100
 neighbor 192.168.2.2 remote-as 200
 neighbor 192.168.2.2 route-map SETAS out
```

D)

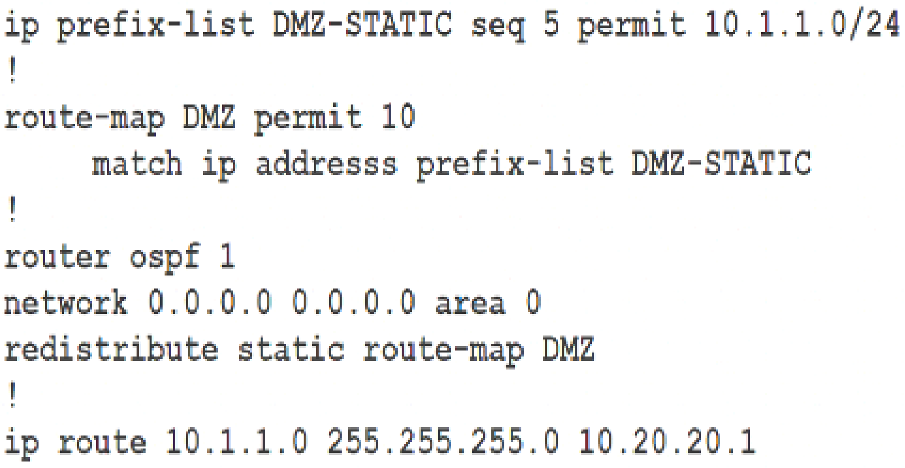


```
route-map SETAS
 set as-path prepend 111
!
router bgp 64555
 neighbor 192.168.1.1 remote-as 100
 neighbor 192.168.2.2 remote-as 200
 neighbor 192.168.2.2 route-map SETAS out
```

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

Answer: C

NEW QUESTION 69
- (Exam Topic 3)
Refer to the exhibit.



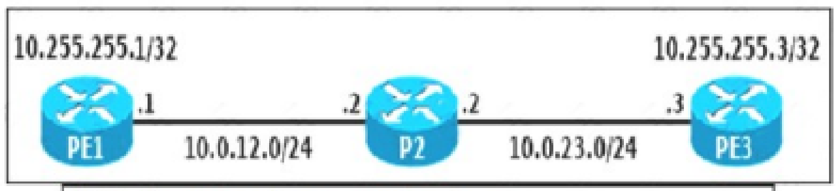
```
ip prefix-list DMZ-STATIC seq 5 permit 10.1.1.0/24
!
route-map DMZ permit 10
     match ip addresss prefix-list DMZ-STATIC
!
router ospf 1
network 0.0.0.0 0.0.0.0 area 0
redistribute static route-map DMZ
!
ip route 10.1.1.0 255.255.255.0 10.20.20.1
```

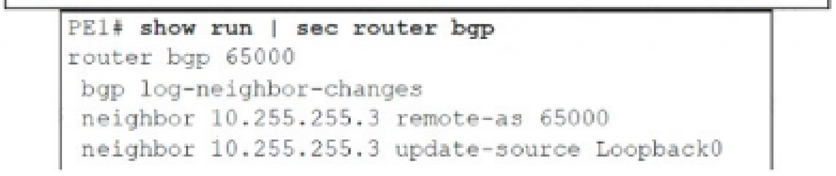
The static route is not present in the routing table of an adjacent OSPF neighbor router. Which action resolves the issue?

A. Configure the next hop of 10.20.20.1 in the prefix list DMZ-STATIC
B. Configure the next-hop interface at the end of the static router for it to get redistributed
C. Configure a permit 20 statement to the route map to redistribute the static route
D. Configure the subnets keyword in the redistribution command

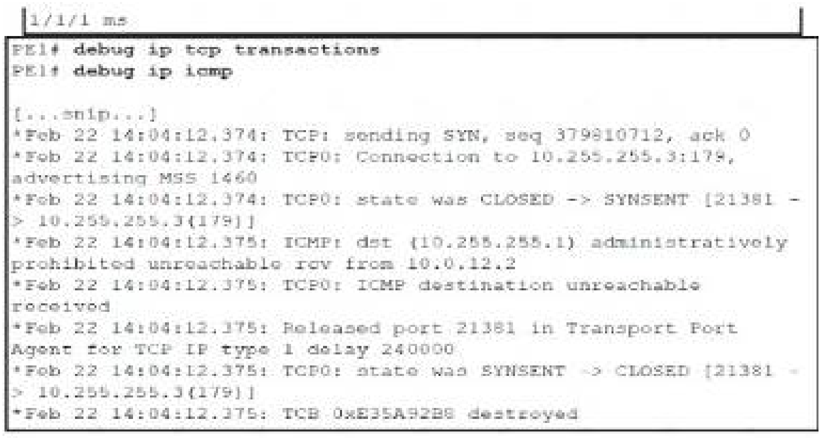
Answer: D

NEW QUESTION 71
- (Exam Topic 3)





```
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. P2 must have a route to PE3 to establish a BGP session to PE1
B. Disable sending ICMP unreachables on P2 to allow PE1 to establish a session with PE3
C. Ensure that the PE3 loopback address is used as a source for BGP peering to PE1
D. Remove the traffic filtering rules on P2 blocking the BGP communication between PE1 and PE3

Answer: C

NEW QUESTION 75
- (Exam Topic 3)
A customer requested a GRE tunnel through the provider network between two customer sites using loopback to hide internal networks. Which configuration on R2 establishes the tunnel with R1?

A. R2(config)# interface Tunnel 1R2(config-if)# ip address 172.20.1.2 255.255.255.0 R2(config-if)# ip mtu 1400R2(config-if)# ip tcp adjust-mss 1360 R2(config-if)# tunnel source 192.168.20.1 R2(config-if)# tunnel destination 192.168.10.1
B. R2(config)# interface Tunnel 1R2(config-if)# ip address 172.20.1.2 255.255.255.0 R2(config-if)# ip mtu 1400R2(config-if)# ip tcp adjust-mss 1360 R2(config-if)# tunnel source 10.10.2.2R2(config-if)# tunnel destination 10.10.1.1
C. R2(config)# interface Tunnel 1R2(config-if)# ip address 172.20.1.2 255.255.255.0 R2(config-if)# ip mtu 1500R2(config-if)# ip tcp adjust-mss 1360 R2(config-if)# tunnel source 192.168.20.1 R2(config-if)# tunnel destination 10.10.1.1
D. R2(config)# interface Tunnel 1R2(config-if)# ip address 172.20.1.2 255.255.255.0 R2(config-if)# ip mtu 1500R2(config-if)# ip tcp adjust-mss 1360 R2(config-if)# tunnel source 10.10.2.2 R2(config-if)# tunnel destination 10.10.1.1

Answer: D

NEW QUESTION 78

- (Exam Topic 3)
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.

Answer: AC

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: https://www.ccexpert.us/mpls-network/mpls-ldp-session-protection.html 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:
I. When a link flaps (for a short time),
… Solution:
+ When LDP session supported by link hello is setup, create a targeted hello to protect the session.

NEW QUESTION 80
- (Exam Topic 3)
What are the two reasons for RD and VPNv4 addresses in an MPLS Layer 3 VPN? (Choose two.)

A. RD is prepended to each prefix to make routes unique.
B. VPN RT communities are used to identify customer unique routes.
C. When the PE redistributes customer routes into MP-BGP, they must be unique.
D. They are on a CE device to use for static configuration.
E. They are used for a BGP session with the CE device.

Answer: AC

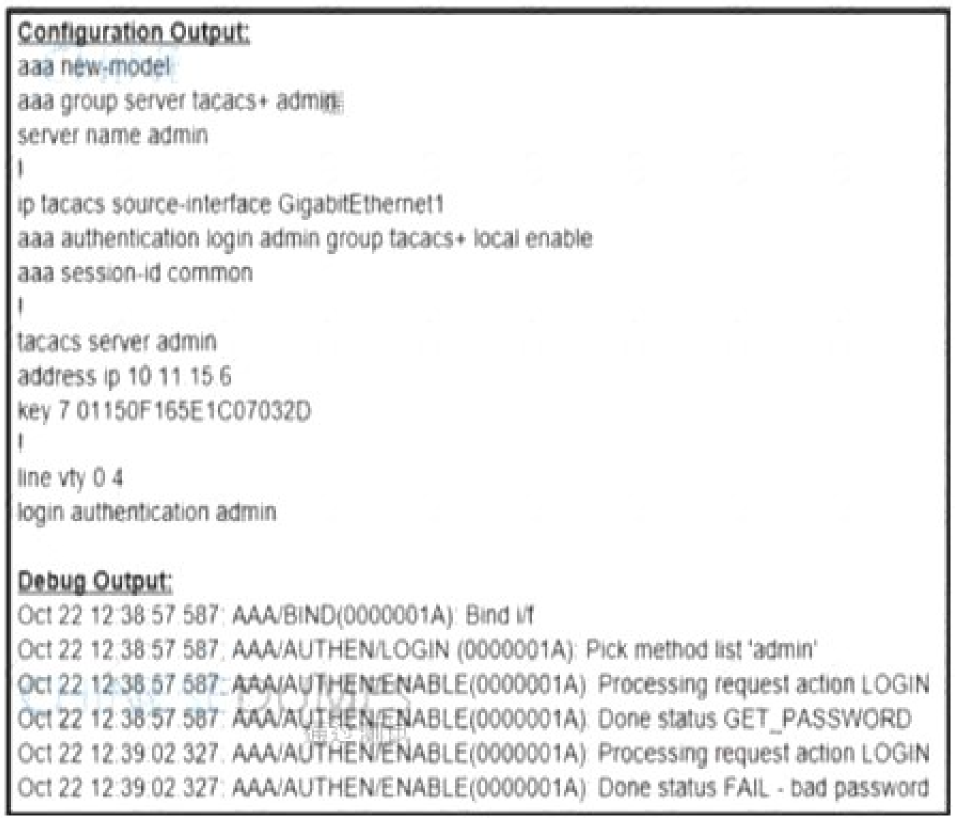
NEW QUESTION 82
- (Exam Topic 3)
Which IPv6 feature enables a device to reject traffic when it is originated from an address that is not stored in the device binding table?

A. IPv6 Snooping
B. IPv6 Source Guard
C. IPv6 DAD Proxy
D. IPv6 RA Guard

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3s/ip6f-xe-3s-book/ip6-src-guar

NEW QUESTION 85
- (Exam Topic 3)
Refer to the exhibit.



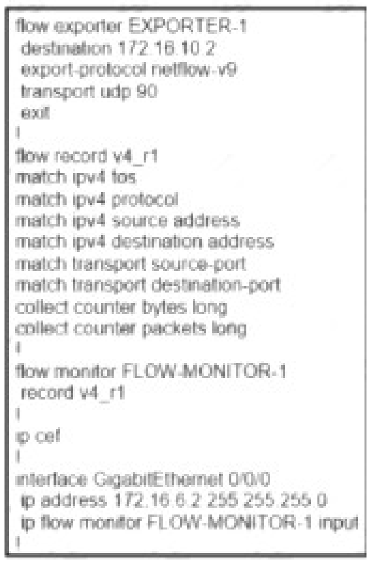
```
Configuration Output:
aaa new-model
aaa group server tacacs+ admin
server name admin
!
ip tacacs source-interface GigabitEthernet1
aaa authentication login admin group tacacs+ local enable
aaa session-id common
!
tacacs server admin
address ip 10 11 15 6
key 7 01150F165E1C07032D
!
line vty 0 4
login authentication admin

Debug Output:
Oct 22 12:38:57.587: AAA/BIND(0000001A): Bind i/f
Oct 22 12:38:57.587: AAA/AUTHEN/LOGIN (0000001A): Pick method list 'admin'
Oct 22 12:38:57.587: AAA/AUTHEN/ENABLE(0000001A): Processing request action LOGIN
Oct 22 12:38:57.587: AAA/AUTHEN/ENABLE(0000001A): Done status GET_PASSWORD
Oct 22 12:39:02.327: AAA/AUTHEN/ENABLE(0000001A): Processing request action LOGIN
Oct 22 12:39:02.327: AAA/AUTHEN/ENABLE(0000001A): Done status FAIL - bad password
```

An administrator configured a Cisco router for TACACS authentication, but the router is using the local enable password instead Which action resolves the issue?

A. Configure the aaa authentication login admin group admin local enable command instead.
B. Configure the aaa authentication login admin group tacacs* local enable none command instead.
C. Configure the aaa authentication login admin group tacacs* local if-authenticated command instead.
D. Configure the aaa authentication login default group admin local if-authenticated command instead.

Answer: C

NEW QUESTION 88
- (Exam Topic 3)
Refer to the exhibit.



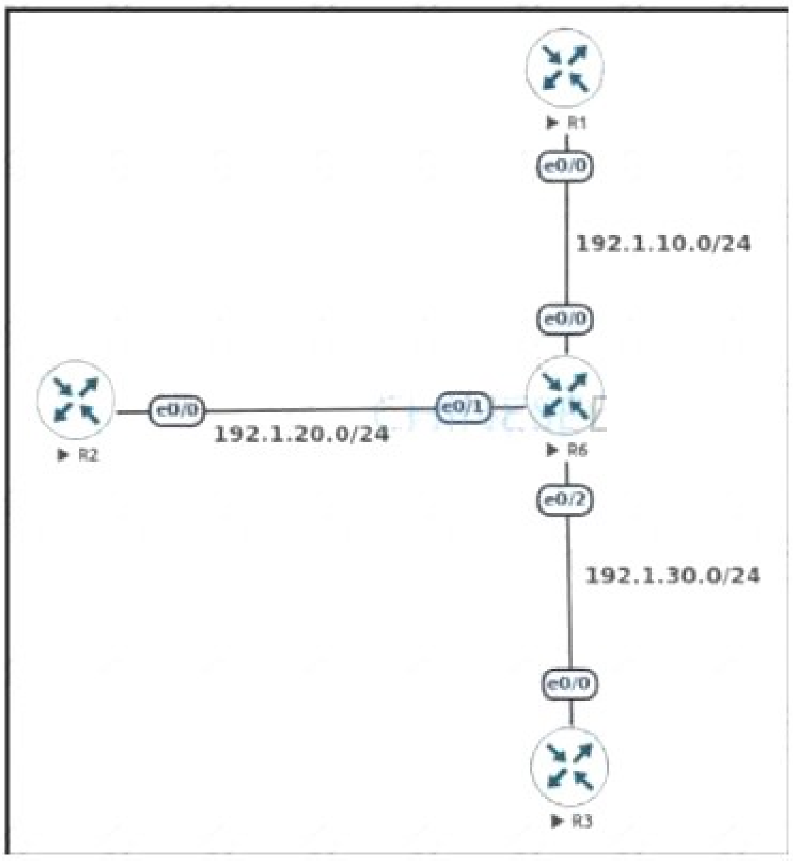
```
flow exporter EXPORTER-1
 destination 172.16.10.2
 export-protocol netflow-v9
 transport udp 90
 exit
!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
 record v4_r1
!
ip cef
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

An engineer configured NetFlow to capture traffic information through the router, but it iOS not working as expected. Which action captures the flow information from this router to the collector?

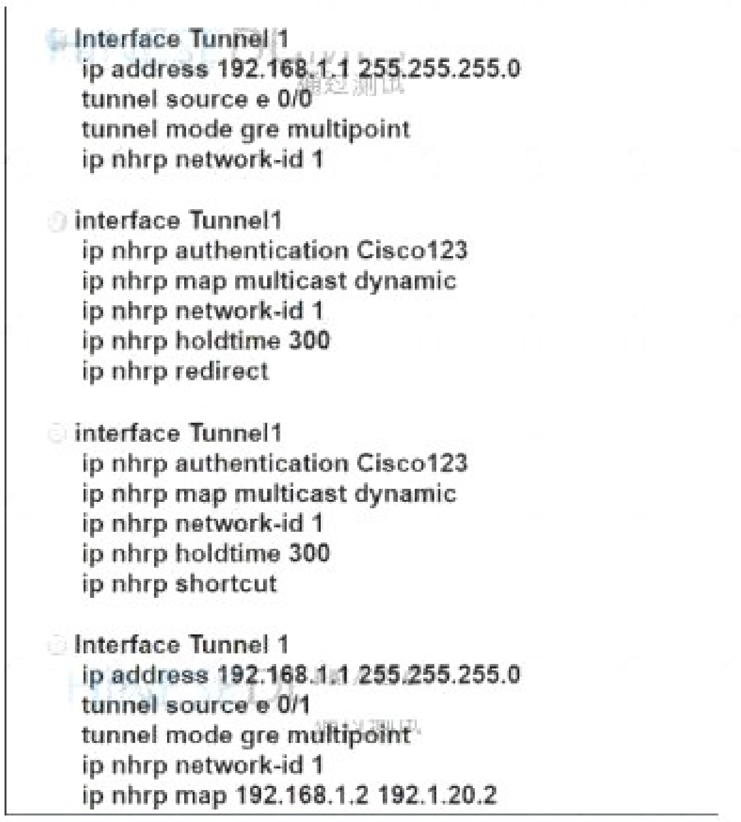
A. Change the interface configuration FLOW-MONITOR-1 from input to output.
B. Configure a flow exporter under flow FLOW-MONITOR-1.
C. Configure more than one flow exporter destination addresses.
D. Change the flow exporter transport protocol from UDP to TCP

Answer: B

NEW QUESTION 89
- (Exam Topic 3)
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?

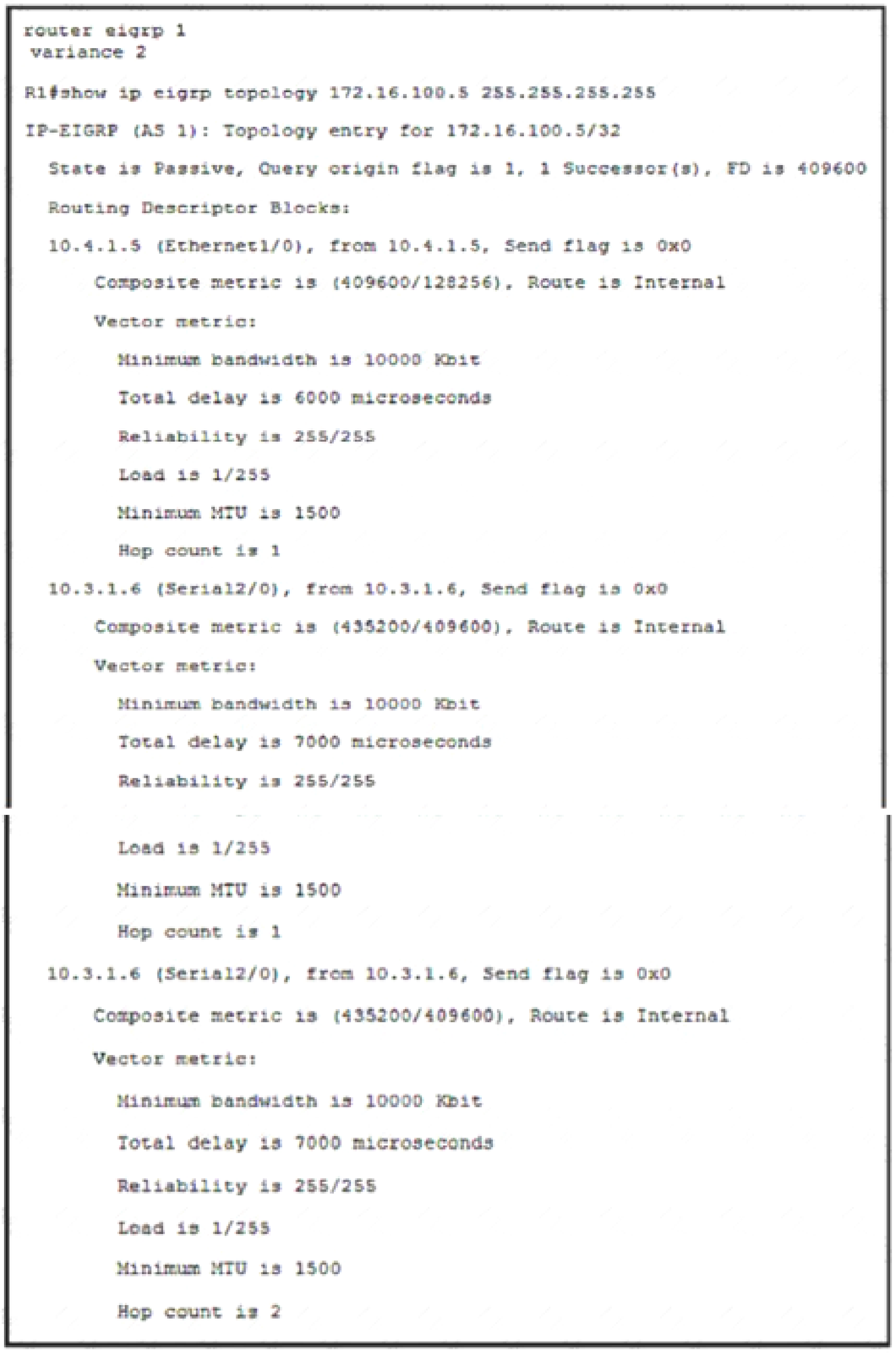


```
○ Interface Tunnel 1
   ip address 192.168.1.1 255.255.255.0
   tunnel source e 0/0
   tunnel mode gre multipoint
   ip nhrp network-id 1

○ interface Tunnel1
   ip nhrp authentication Cisco123
   ip nhrp map multicast dynamic
   ip nhrp network-id 1
   ip nhrp holdtime 300
   ip nhrp redirect

○ interface Tunnel1
   ip nhrp authentication Cisco123
   ip nhrp map multicast dynamic
   ip nhrp network-id 1
   ip nhrp holdtime 300
   ip nhrp shortcut

○ Interface Tunnel 1
   ip address 192.168.1.1 255.255.255.0
   tunnel source e 0/1
   tunnel mode gre multipoint
   ip nhrp network-id 1
   ip nhrp map 192.168.1.2 192.1.20.2
```

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

Answer: B

NEW QUESTION 94
- (Exam Topic 3)



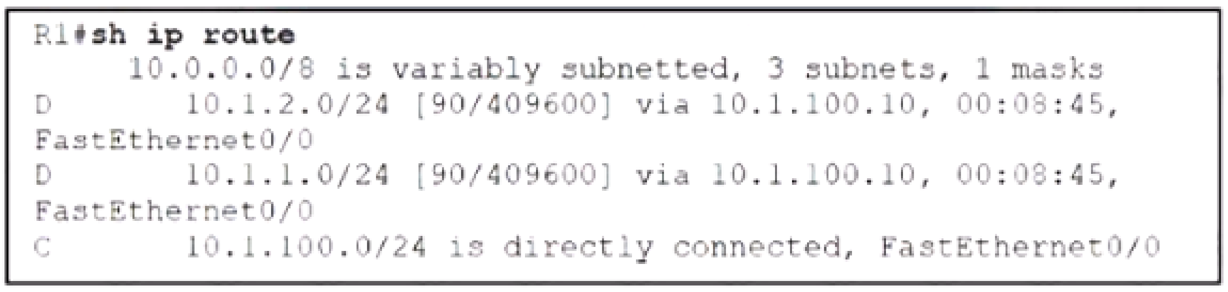
```
router eigrp 1
 variance 2
R1#show ip eigrp topology 172.16.100.5 255.255.255.255
IP-EIGRP (AS 1): Topology entry for 172.16.100.5/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
  Routing Descriptor Blocks:
  10.4.1.5 (Ethernet1/0), from 10.4.1.5, Send flag is 0x0
      Composite metric is (409600/128256), Route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 6000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  10.3.1.6 (Serial2/0), from 10.3.1.6, Send flag is 0x0
      Composite metric is (435200/409600), Route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 7000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  10.3.1.6 (Serial2/0), from 10.3.1.6, Send flag is 0x0
      Composite metric is (435200/409600), Route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 7000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
```

Refer to the exhibit. A network engineer troubleshooting a packet drop problem for the host 172.16.100.5 notices that only one link is used and installed on the routing table, which saturates the bandwidth. Which action must the engineer take to resolve the high bandwidth utilization problem and share the traffic toward this host between the two available links?

A. Set the eigrp variance equal to 4 to install a second route with a metric not larger than 4 times of the best metric.
B. Change the EIGRP delay metric to meet the feasibility condition.
C. Set the eigrp variance equal to 3 to install a second route with a metric not larger than 3 times of the best metric.
D. Disable the eigrp split horizon loop protection mechanism.

Answer: B

NEW QUESTION 95
- (Exam Topic 3)
Refer to the exhibit.



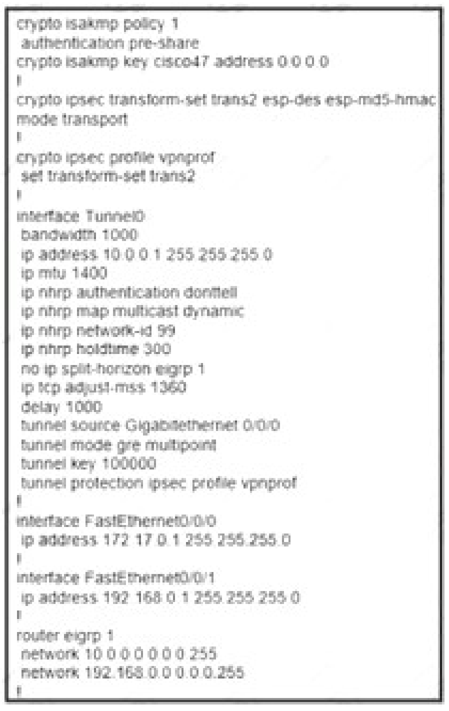
```
R1#sh ip route
     10.0.0.0/8 is variably subnetted, 3 subnets, 1 masks
D       10.1.2.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
D       10.1.1.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
C       10.1.100.0/24 is directly connected, FastEthernet0/0
```

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. 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.
B. 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
C. The summarization condition is not me
D. The network 10.1.100.0/24 should be changed to 172.16.0.0/24.
E. 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

NEW QUESTION 98
- (Exam Topic 3)
Refer to the exhibit.



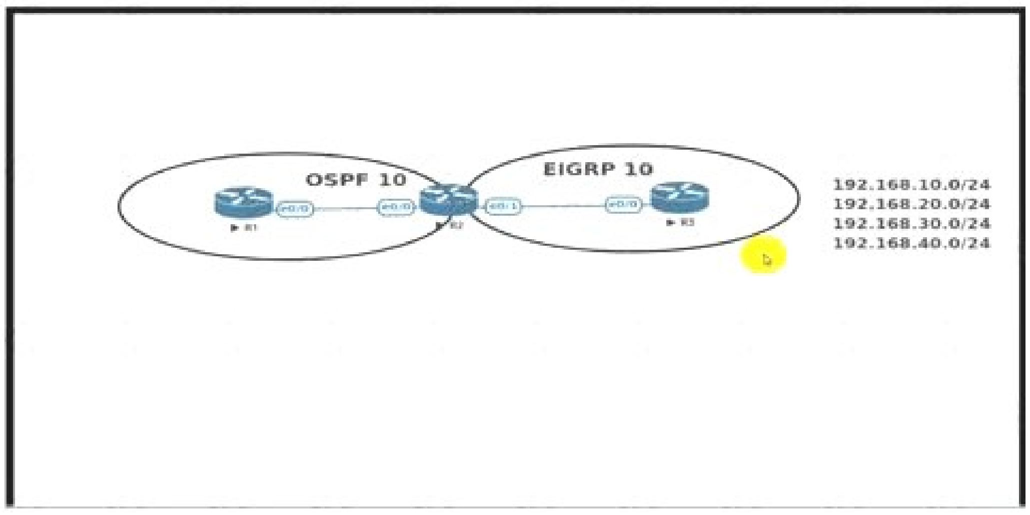
```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0 0 0 0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10 0 0 1 255 255 255 0
 ip mtu 1400
 ip nhrp authentication donttell
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Gigabitethernet 0/0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface FastEthernet0/0/0
 ip address 172 17 0 1 255 255 255 0
!
interface FastEthernet0/0/1
 ip address 192 168 0 1 255 255 255 0
!
router eigrp 1
 network 10 0 0 0 0 0 0 255
 network 192.168.0.0 0.0.0.255
!
```

A network administrator must configure DMVPN tunnels between the hub and spoke with dynamic spoke-to-spoke tunnel capabilities using EIGRP. Which tunnel interface command must the network administrator configure to establish an EIGRP peer?

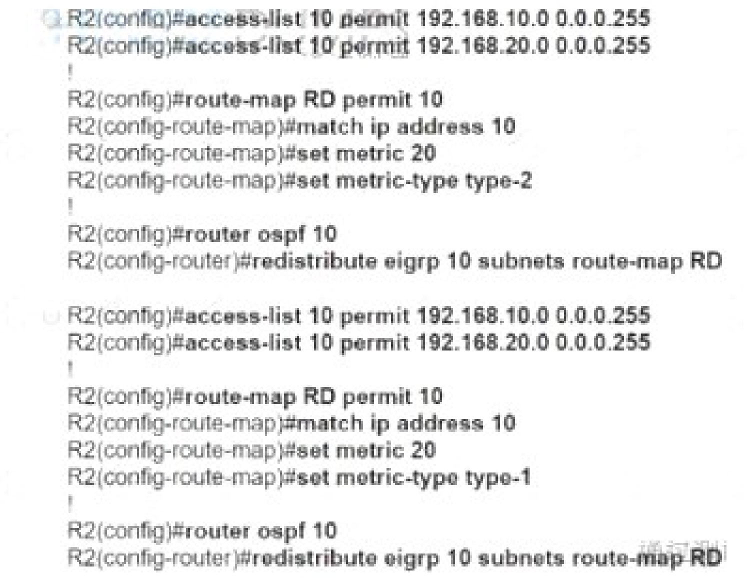
A. no ip next-hop-self eigrp 1
B. ip next-hop-self eigrp 1
C. no Ip nhrp ntxt-hop-self
D. ip nhrp next-hop-self

Answer: C

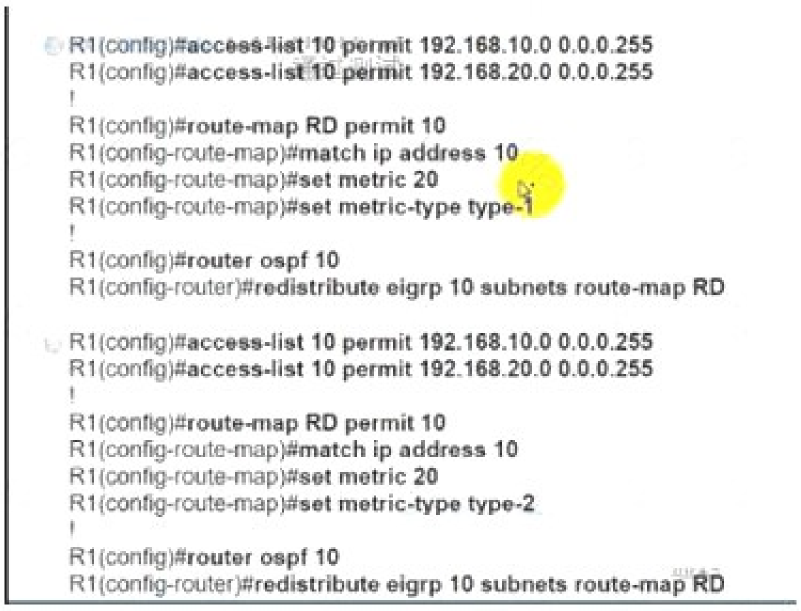
NEW QUESTION 99
- (Exam Topic 3)
Refer to the exhibit.



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
```

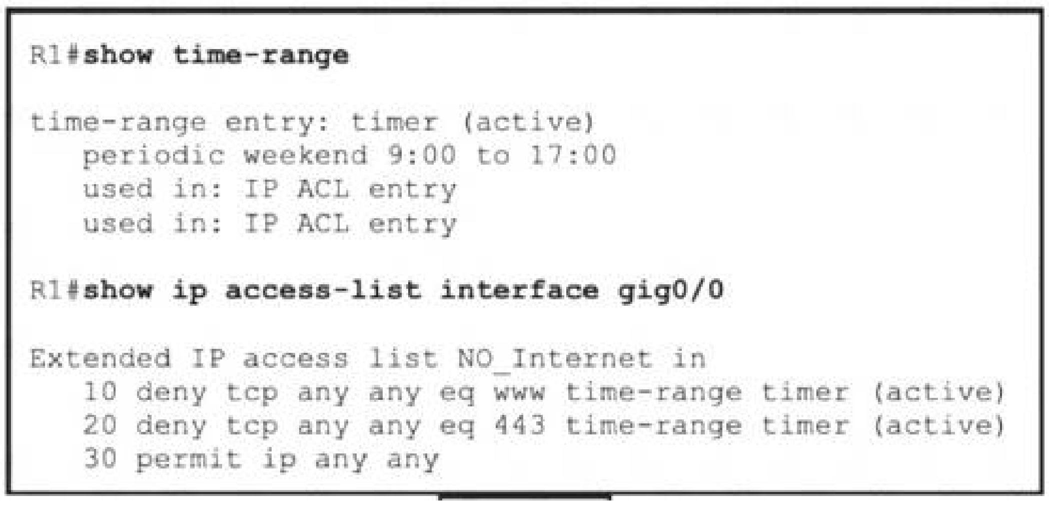


```
R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit 192.168.20.0 0.0.0.255
!
R1(config)#route-map RD permit 10
R1(config-route-map)#match ip address 10
R1(config-route-map)#set metric 20
R1(config-route-map)#set metric-type type-1
!
R1(config)#router ospf 10
R1(config-router)#redistribute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

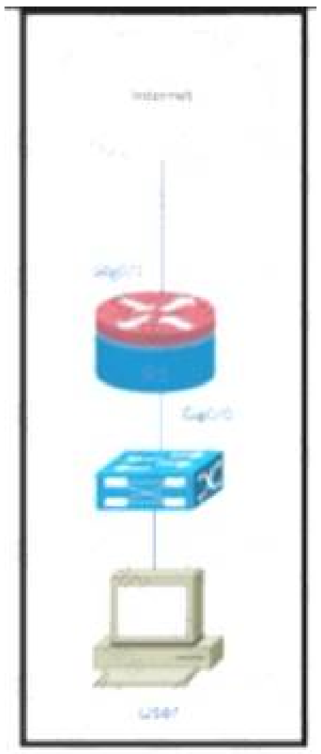
A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 104
- (Exam Topic 3)

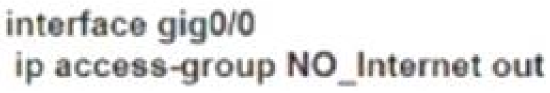


```
R1#show time-range

time-range entry: timer (active)
   periodic weekend 9:00 to 17:00
   used in: IP ACL entry
   used in: IP ACL entry

R1#show ip access-list interface gig0/0

Extended IP access list NO_Internet in
   10 deny tcp any any eq www time-range timer (active)
   20 deny tcp any any eq 443 time-range timer (active)
   30 permit ip any any
```



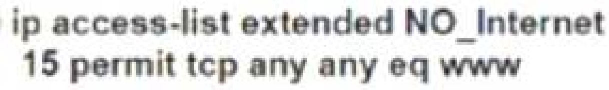
Refer to the exhibit. Users on a call center report that they cannot browse the internet on Saturdays during the afternoon. Which configuration resolves the issue?

A)



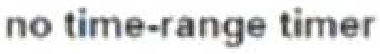
```
interface gig0/0
 ip access-group NO_Internet out
```

B)



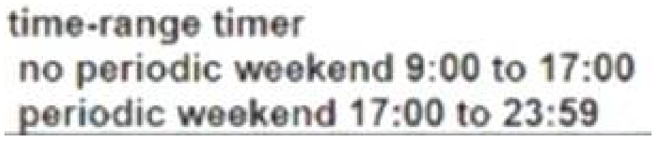
```
ip access-list extended NO_Internet
 15 permit tcp any any eq www
```

C)



```
no time-range timer
```

D)

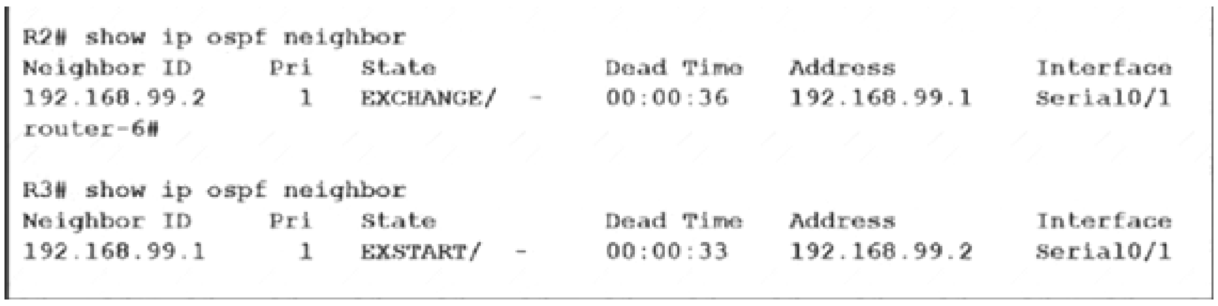


```
time-range timer
 no periodic weekend 9:00 to 17:00
 periodic weekend 17:00 to 23:59
```

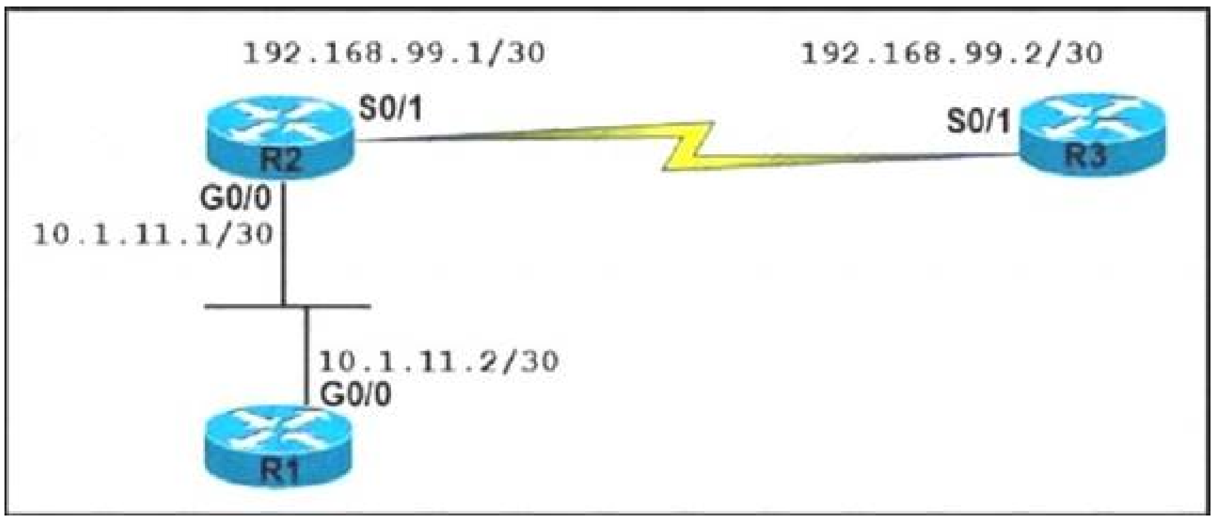
A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

NEW QUESTION 107
- (Exam Topic 3)
Refer to the exhibit.



```
R2# show ip ospf neighbor
Neighbor ID     Pri   State          Dead Time   Address         Interface
192.168.99.2      1   EXCHANGE/  -   00:00:36    192.168.99.1    Serial0/1
router-6#

R3# show ip ospf neighbor
Neighbor ID     Pri   State          Dead Time   Address         Interface
192.168.99.1      1   EXSTART/  -    00:00:33    192.168.99.2    Serial0/1
```



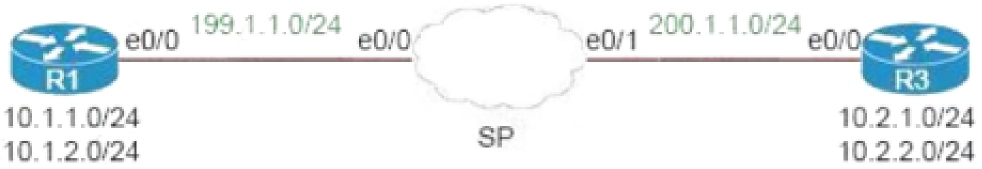
An OSPF neighbor relationship between R2 and R3 is showing stuck in EXCHANGE/EXSTART state. The neighbor is established between R1 and R2. The network engineer can ping from R2 to R3 and vice versa, but the neighbor is still down. Which action resolves the issue?

A. Restore the Layer 2/Layer 3 conectivity issue in the ISP network.
B. Match MTU on both router interfaces or ignore MTU.
C. Administrative "shut then no shut" both router interfaces.
D. Enable OSPF on the interface, which is required.

Answer: B

Explanation:
After two OSPF neighboring routers establish bi-directional communication and complete DR/BDR election (on multi-access networks), the routers transition to the exstart state. In this state, the
neighboring routers establish a master/slave relationship and determine the initial database descriptor (DBD) sequence number to use while exchanging DBD packets.
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.

NEW QUESTION 112
- (Exam Topic 3)
Refer to the exhibit.



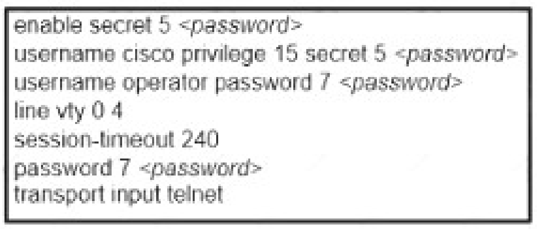
An engineer must configure a LAN-to-LAN IPsec VPN between R1 and the remote router. Which IPsec Phase 1 configuration must the engineer use for the local router?

A. crypto isakmp policy 5authentication pre-share encryption 3deshash sha group 2!crypto isakmp key cisco123 address 200.1.1.3
B. crypto isakmp policy 5 authentication pre-share encryption 3deshash md5 group 2!crypto isakmp key cisco123 address 200.1.1.3
C. crypto isakmp policy 5 authentication pre-share encryption 3deshash md5 group 2!crypto isakmp key cisco123 address 199.1.1.1
D. crypto isakmp policy 5 authentication pre-share encryption 3deshash md5group 2!crypto isakmp key cisco123! address 199.1.1.1

Answer: A

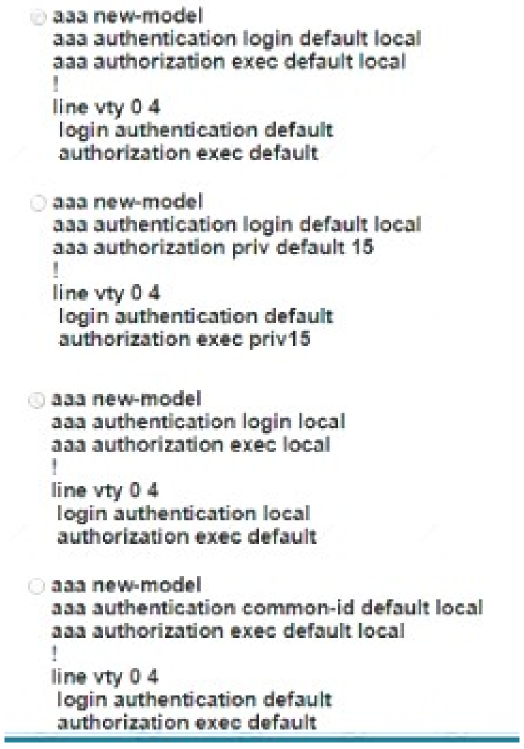
Explanation:
In the "crypto isakmp key … address " command, the address must be of the IP address of the other end (which is 200.1.1.3 in this case) so Option A and Option B are correct. The difference between these two options are in the hash SHA or MD5 method but both of them can be used although SHA is better than MD5 so we choose Option A the best answer.
Note: Cisco no longer recommends using 3DES, MD5 and DH groups 1, 2 and 5.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_imgmt/configuration/xe-16- 5/sec-ipsec-management-xe-16-5-book/sec-ipsec-usability-enhance.html

NEW QUESTION 114
- (Exam Topic 3)



```
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?



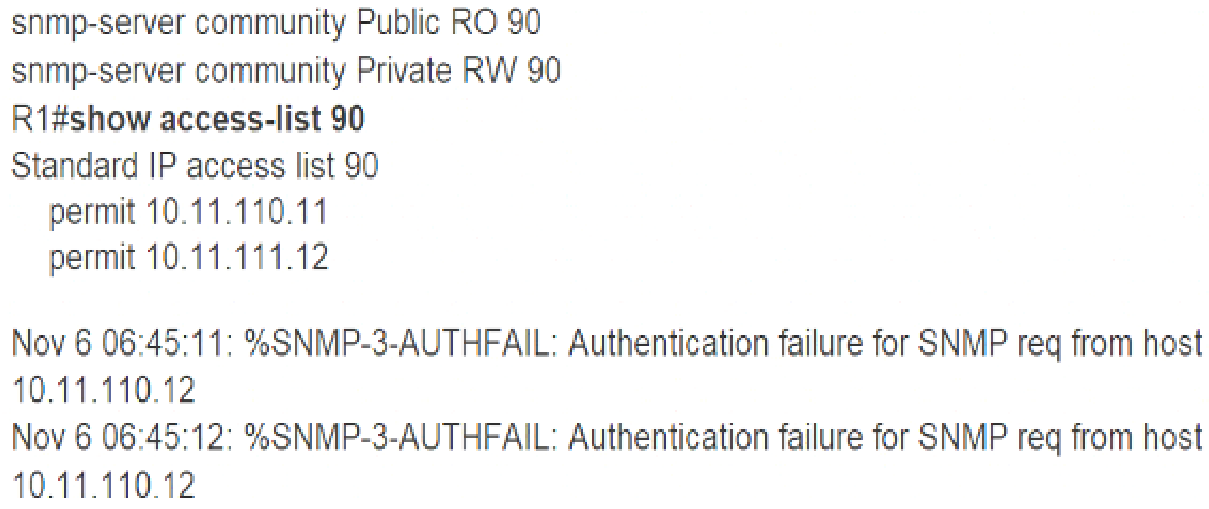
```
○ aaa new-model
  aaa authentication login default local
  aaa authorization exec default local
  !
  line vty 0 4
   login authentication default
   authorization exec default

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

Answer: C

NEW QUESTION 117

- (Exam Topic 3)
Refer to the exhibit.



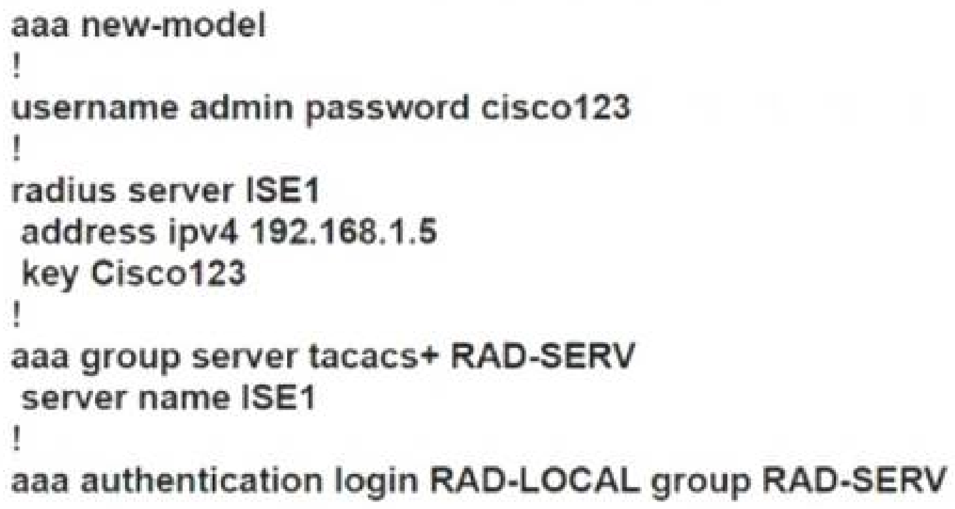
```
snmp-server community Public RO 90
snmp-server community Private RW 90
R1#show access-list 90
Standard IP access list 90
    permit 10.11.110.11
    permit 10.11.111.12

Nov 6 06:45:11: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host
10.11.110.12
Nov 6 06:45:12: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host
10.11.110.12
```

A network administrator notices these console messages from host 10.11.110.12 originating from interface E1/0. The administrator considers this an unauthorized attempt to access SNMP on R1. Which action prevents the attempts to reach R1 E1/0?

A. Configure IOS control plane protection using ACL 90 on interface E1/0
B. Configure IOS management plane protection using ACL 90 on interface E1/0
C. Create an inbound ACL on interface E1/0 to deny SNMP from host 10.11.110.12
D. Add a permit statement including the host 10.11.110.12 into ACL 90

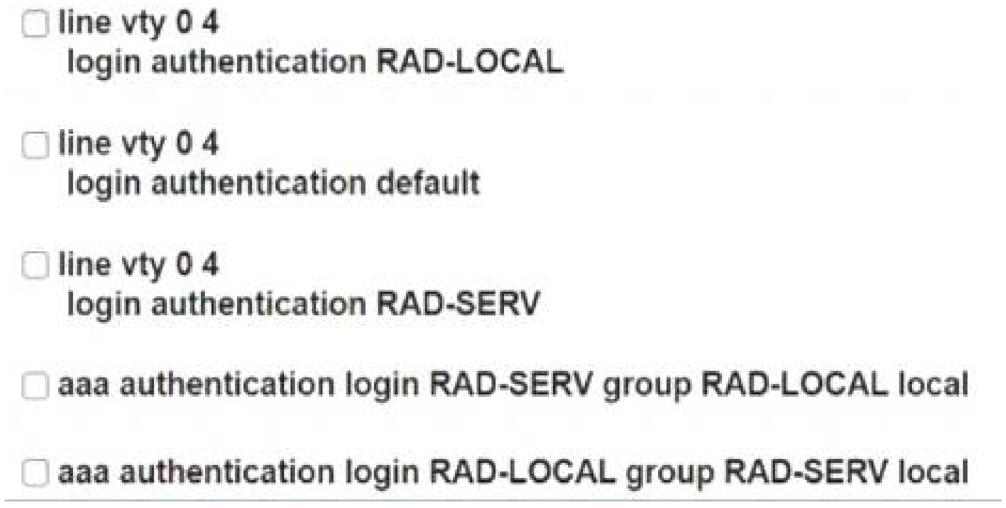
Answer: C

NEW QUESTION 119
- (Exam Topic 3)
The network administrator is tasked to configure R1 to authenticate telnet connections based on Cisco ISE using RADIUS. ISE has been configured with an IP address of 192.168.1.5 and with a network device pointing towards R1 (192.168.1.1) with a shared secret password of Cisco123. If ISE is down, the administrator should be able to connect using the local database with a username and password combination of admin/cisco123.
The administrator has configured the following on R1:



```
aaa new-model
!
username admin password cisco123
!
radius server ISE1
 address ipv4 192.168.1.5
 key Cisco123
!
aaa group server tacacs+ RAD-SERV
 server name ISE1
!
aaa authentication login RAD-LOCAL group RAD-SERV
```

ISE has gone down. The Network Administrator is not able to Telnet to R1 when ISE went down. Which two configuration changes will fix the issue? (Choose two.)



☐ line vty 0 4
  login authentication RAD-LOCAL

☐ line vty 0 4
  login authentication default

☐ line vty 0 4
  login authentication RAD-SERV

☐ aaa authentication login RAD-SERV group RAD-LOCAL local

☐ aaa authentication login RAD-LOCAL group RAD-SERV local

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

Answer: CE

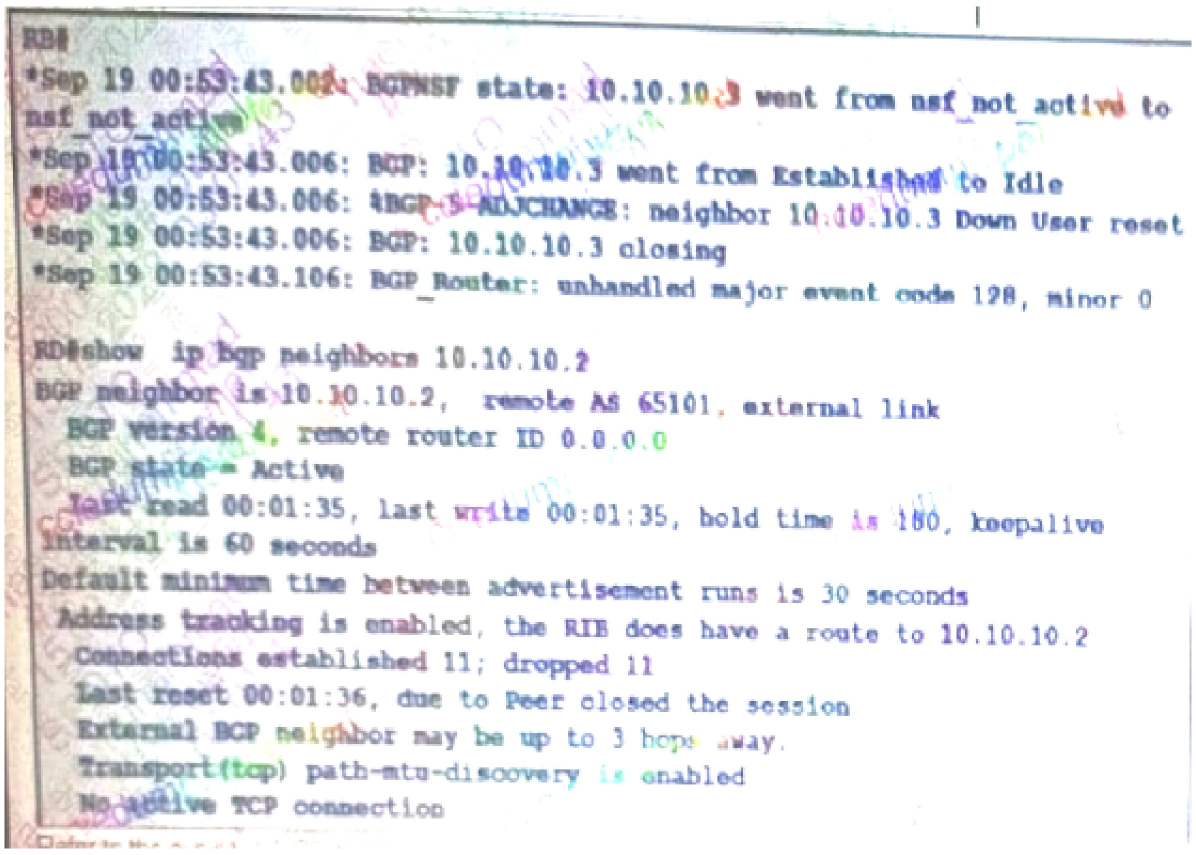
NEW QUESTION 121
- (Exam Topic 3)
What is a function of the IPv6 DHCP Guard feature for DHCP messages?

A. Only access lists are supported for matching traffic.
B. All client messages are always switched regardless of the device role.
C. It blocks only DHCP request messages.

D. If the device is configured as a DHCP server, no message is switched.

Answer: B

NEW QUESTION 124
- (Exam Topic 3)
Refer to the exhibit.



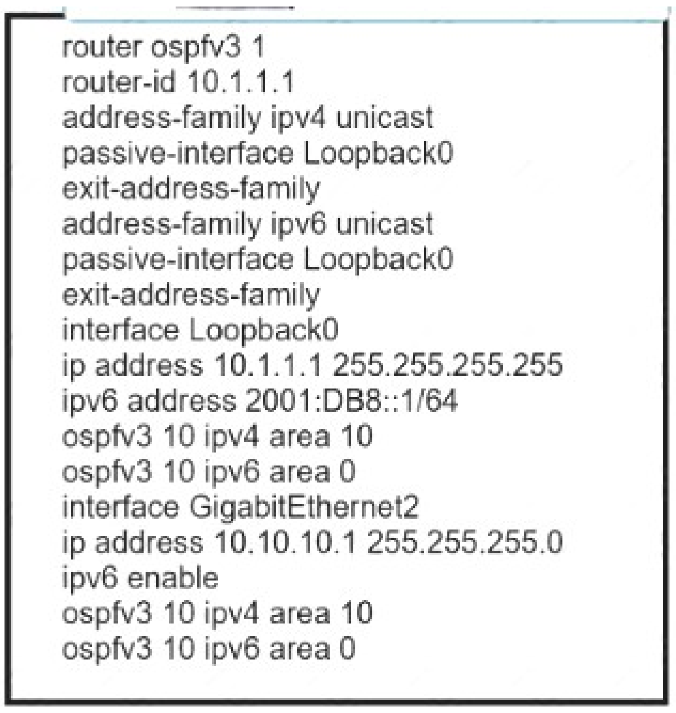
```
RD#
*Sep 19 00:53:43.002: BGPNSF state: 10.10.10.3 went from nsf_not_active to
nsf_not_active
*Sep 19 00:53:43.006: BGP: 10.10.10.3 went from Established to Idle
*Sep 19 00:53:43.006: %BGP-5-ADJCHANGE: neighbor 10.10.10.3 Down User reset
*Sep 19 00:53:43.006: BGP: 10.10.10.3 closing
*Sep 19 00:53:43.106: BGP_Router: unhandled major event code 128, minor 0

RD#show  ip bgp neighbors 10.10.10.2
BGP neighbor is 10.10.10.2,  remote AS 65101, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
  last read 00:01:35, last write 00:01:35, hold time is 180, keepalive
interval is 60 seconds
Default minimum time between advertisement runs is 30 seconds
 Address tracking is enabled, the RIB does have a route to 10.10.10.2
  Connections established 11; dropped 11
  Last reset 00:01:36, due to Peer closed the session
  External BGP neighbor may be up to 3 hops away.
  Transport(tcp) path-mtu-discovery is enabled
  No active TCP connection
```

A NOC team receives a ticket that data traffic from RA to RF is not forwarded when the link between the RC-RE path goes down. All routers learn loopback IP through the IGP protocol. Which configuration resolves?

A. RD(config)#router bgp B5201RD(config-router)# neighbor 10.10.10.2 update-source loopback 0
B. RD(config-router)# neighbor bgp 65101RB(config-router)# neighbor 10.10.10.3 ebgp-multihop 3
C. RB(config)# router bgp 65101RB(config)#neighbor 10.10.10.3 update-source loopback 0
D. RD(config)# router bgp 65201RDI(config-router)# neighbor 10.10.10.2 ebgp-multihop 3

Answer: B

NEW QUESTION 126
- (Exam Topic 3)
Refer to the exhibit.



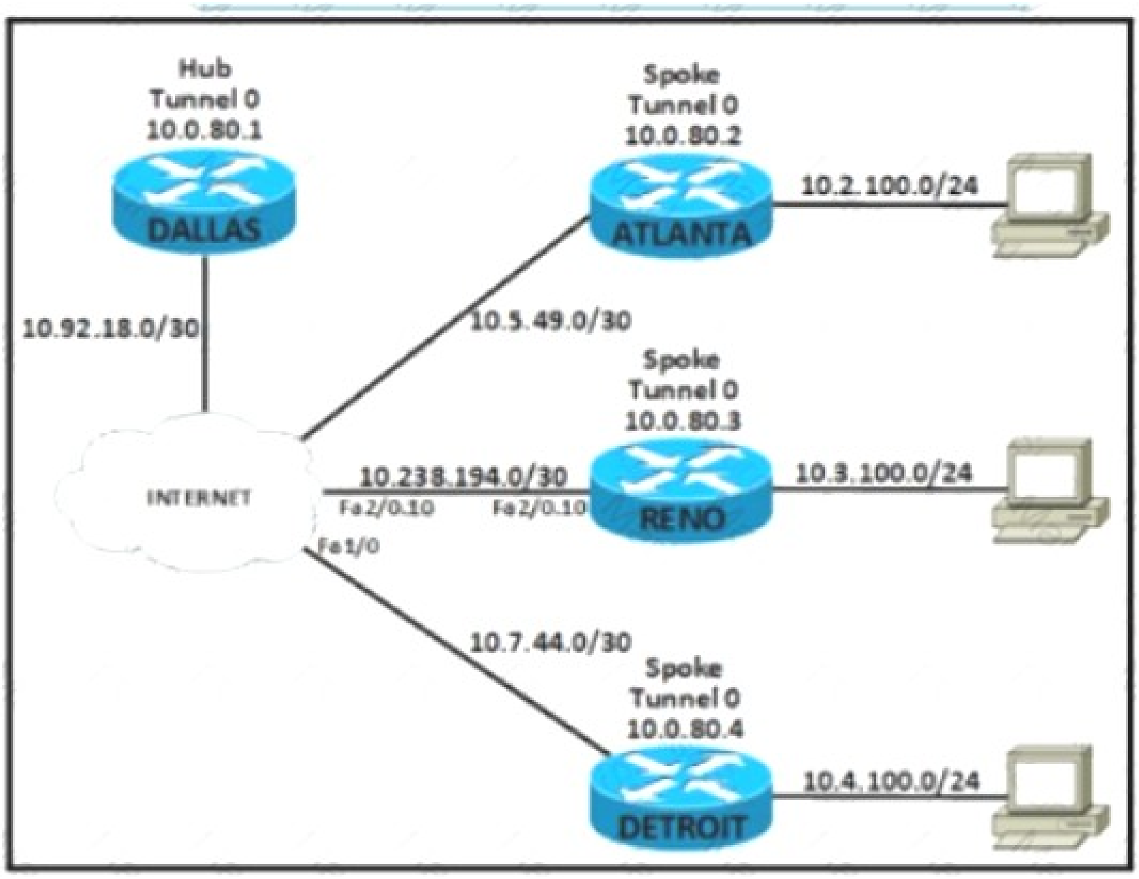
```
router ospfv3 1
router-id 10.1.1.1
address-family ipv4 unicast
passive-interface Loopback0
exit-address-family
address-family ipv6 unicast
passive-interface Loopback0
exit-address-family
interface Loopback0
ip address 10.1.1.1 255.255.255.255
ipv6 address 2001:DB8::1/64
ospfv3 10 ipv4 area 10
ospfv3 10 ipv6 area 0
interface GigabitEthernet2
ip address 10.10.10.1 255.255.255.0
ipv6 enable
ospfv3 10 ipv4 area 10
ospfv3 10 ipv6 area 0
```

An engineer noticed that the router log messages do not have any information about when the event occurred. Which action should the engineer take when enabling service time stamps to improve the logging functionality at a granular level?

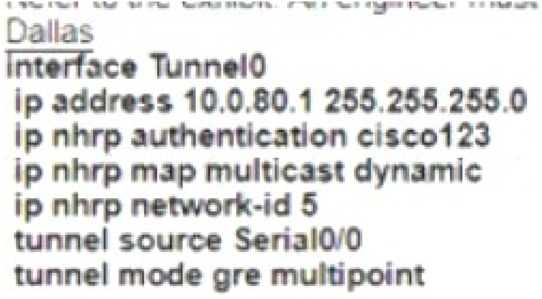
A. Replace OSPF process 10 on the interfaces with OSPF process 1 and configure an additional router IO with IPv6 address
B. Replace OSPF process 10 on the interfaces with OSPF process 1. and remove process 10 from the global configuration
C. Replace OSPF process 10 on the interfaces with OSPF process 1 for the IPv6 address and remove process 10 from the global configuration
D. Replace OSPF process 10 on the interfaces with OSPF process 1 for the IPv4 address and remove process 10 from the global configuration

Answer: D

NEW QUESTION 129
- (Exam Topic 3)



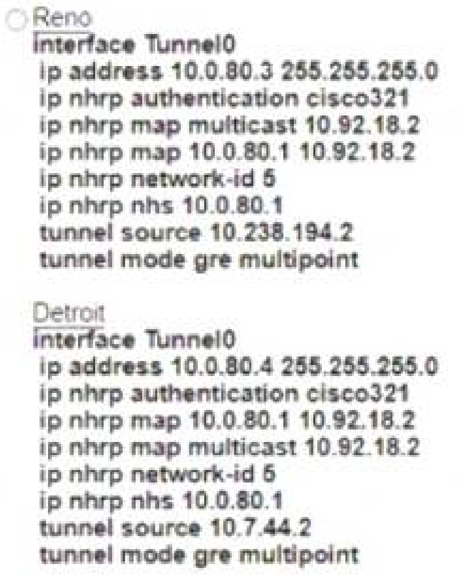
Refer to the exhibit An engineer must connect the Reno and Detroit spokes using DMVPN phase 2 Hub tunnel configuration is



```
Dallas
interface Tunnel0
 ip address 10.0.80.1 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 5
 tunnel source Serial0/0
 tunnel mode gre multipoint
```

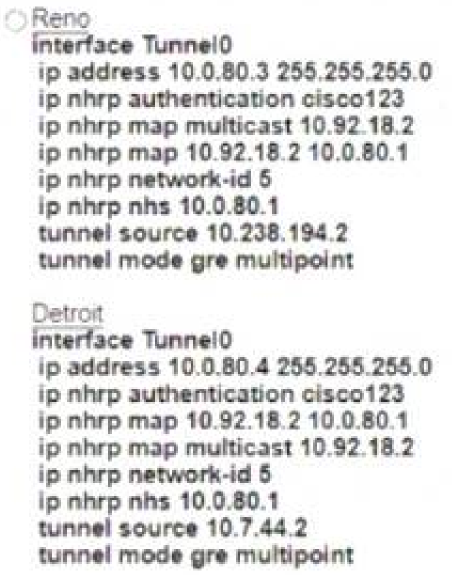
Which configuration accomplishes the task?

○

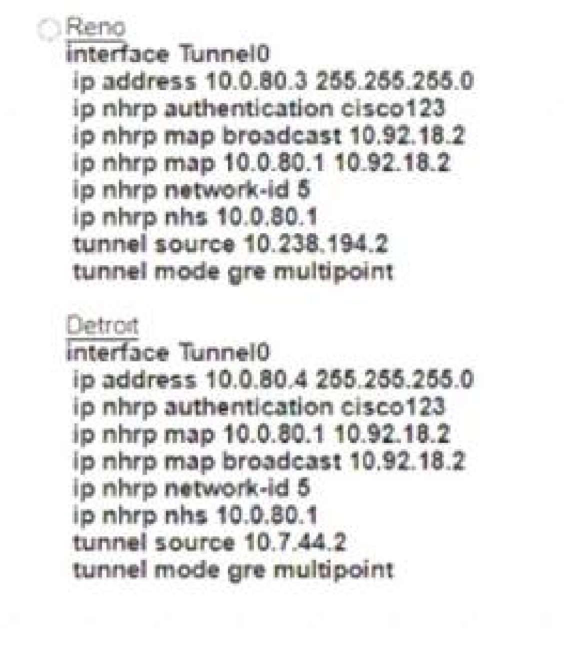


```
Reno
interface Tunnel0
 ip address 10.0.80.3 255.255.255.0
 ip nhrp authentication cisco321
 ip nhrp map multicast 10.92.18.2
 ip nhrp map 10.0.80.1 10.92.18.2
 ip nhrp network-id 5
 ip nhrp nhs 10.0.80.1
 tunnel source 10.238.194.2
 tunnel mode gre multipoint

Detroit
interface Tunnel0
 ip address 10.0.80.4 255.255.255.0
 ip nhrp authentication cisco321
 ip nhrp map 10.0.80.1 10.92.18.2
 ip nhrp map multicast 10.92.18.2
 ip nhrp network-id 5
 ip nhrp nhs 10.0.80.1
 tunnel source 10.7.44.2
 tunnel mode gre multipoint
```

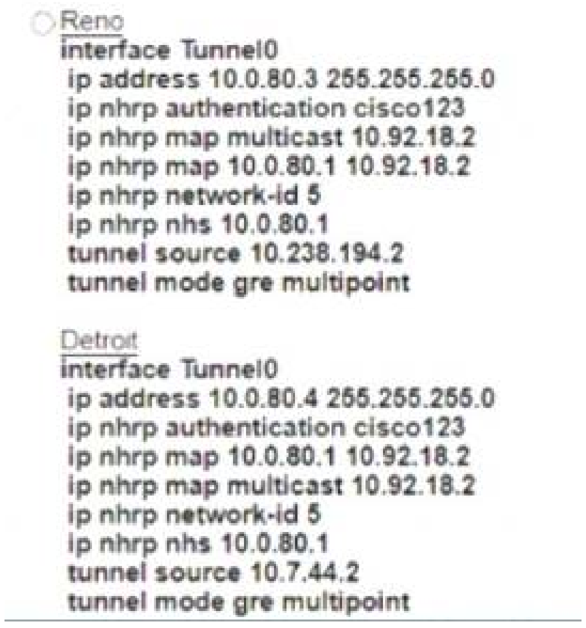
○



```
Reno
interface Tunnel0
 ip address 10.0.80.3 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map multicast 10.92.18.2
 ip nhrp map 10.92.18.2 10.0.80.1
 ip nhrp network-id 5
 ip nhrp nhs 10.0.80.1
 tunnel source 10.238.194.2
 tunnel mode gre multipoint

Detroit
interface Tunnel0
 ip address 10.0.80.4 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map 10.92.18.2 10.0.80.1
 ip nhrp map multicast 10.92.18.2
 ip nhrp network-id 5
 ip nhrp nhs 10.0.80.1
 tunnel source 10.7.44.2
 tunnel mode gre multipoint
```



```
○ Reno
interface Tunnel0
 ip address 10.0.80.3 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map broadcast 10.92.18.2
 ip nhrp map 10.0.80.1 10.92.18.2
 ip nhrp network-id 5
 ip nhrp nhs 10.0.80.1
 tunnel source 10.238.194.2
 tunnel mode gre multipoint

Detroit
interface Tunnel0
 ip address 10.0.80.4 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map 10.0.80.1 10.92.18.2
 ip nhrp map broadcast 10.92.18.2
 ip nhrp network-id 5
 ip nhrp nhs 10.0.80.1
 tunnel source 10.7.44.2
 tunnel mode gre multipoint
```

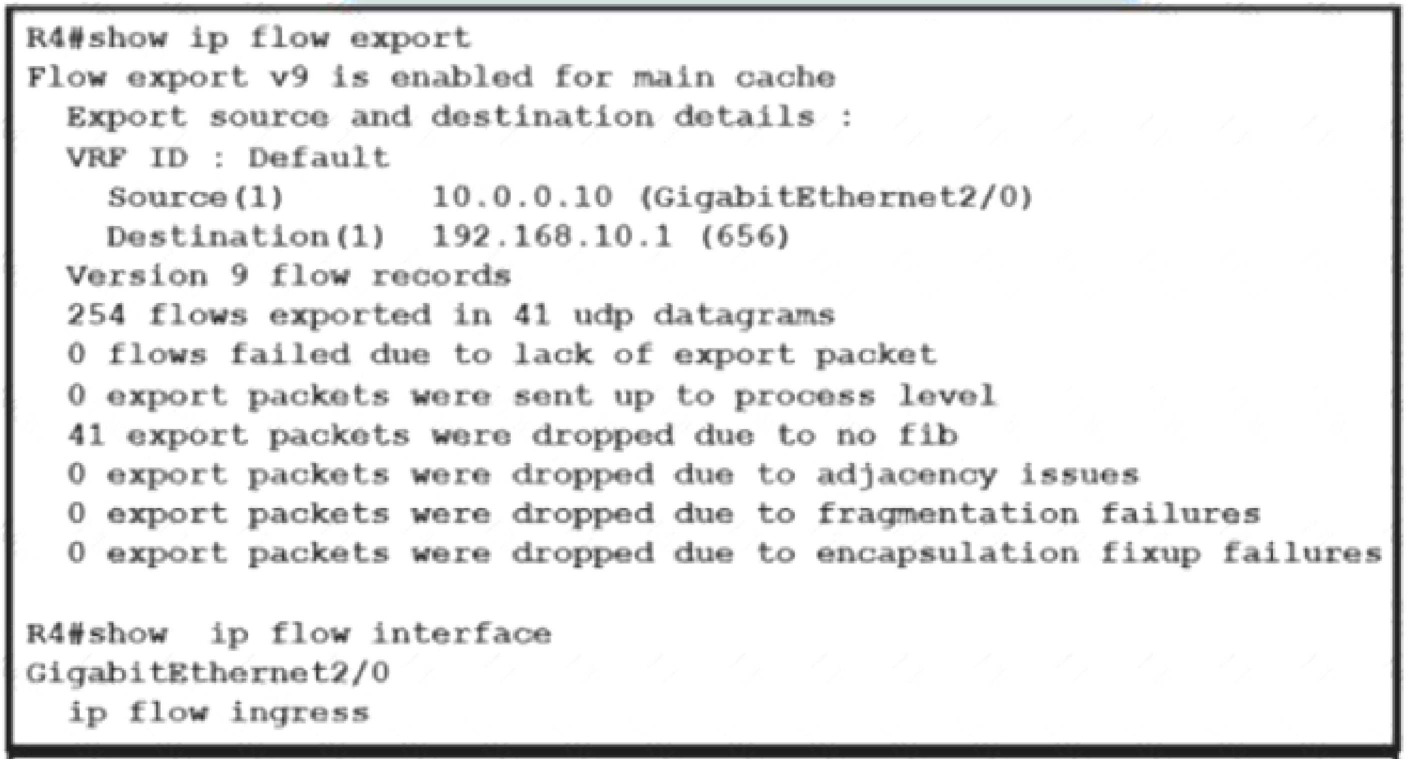


```
○ Reno
interface Tunnel0
 ip address 10.0.80.3 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map multicast 10.92.18.2
 ip nhrp map 10.0.80.1 10.92.18.2
 ip nhrp network-id 5
 ip nhrp nhs 10.0.80.1
 tunnel source 10.238.194.2
 tunnel mode gre multipoint

Detroit
interface Tunnel0
 ip address 10.0.80.4 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map 10.0.80.1 10.92.18.2
 ip nhrp map multicast 10.92.18.2
 ip nhrp network-id 5
 ip nhrp nhs 10.0.80.1
 tunnel source 10.7.44.2
 tunnel mode gre multipoint
```

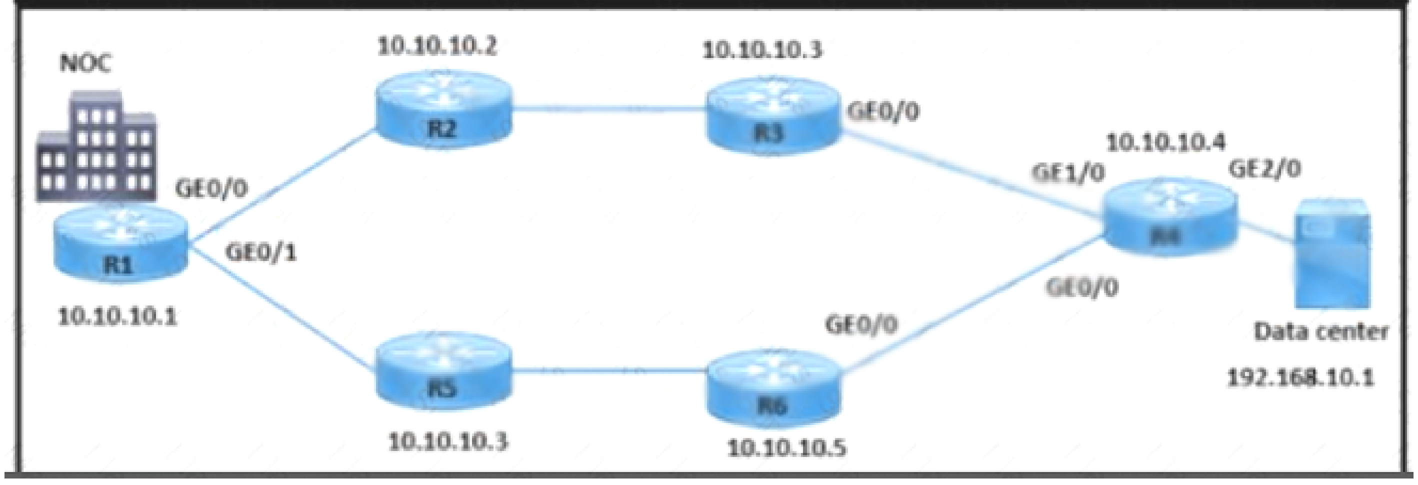
A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

NEW QUESTION 132
- (Exam Topic 3)

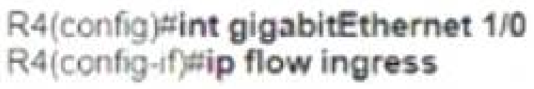


```
R4#show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Source(1)        10.0.0.10 (GigabitEthernet2/0)
    Destination(1)   192.168.10.1 (656)
  Version 9 flow records
  254 flows exported in 41 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  41 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures

R4#show  ip flow interface
GigabitEthernet2/0
  ip flow ingress
```



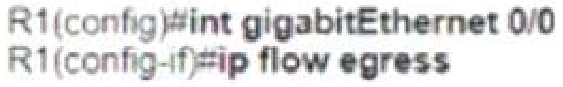
Refer to the exhibit An enterprise operations team must monitor all application server traffic in the data center The team finds that traffic coming from the hub site from R3 and R6 rs monitored successfully but traffic destined to the application server is not monitored Which action resolves the issue?

A)



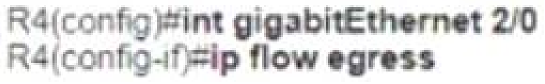
```
R4(config)#int gigabitEthernet 1/0
R4(config-if)#ip flow ingress
```

B)



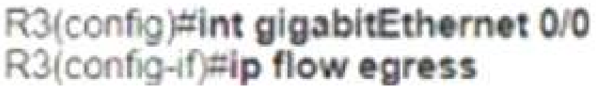
```
R1(config)#int gigabitEthernet 0/0
R1(config-if)#ip flow egress
```

C)



```
R4(config)#int gigabitEthernet 2/0
R4(config-if)#ip flow egress
```

D)



```
R3(config)#int gigabitEthernet 0/0
R3(config-if)#ip flow egress
```

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

Answer: C

NEW QUESTION 133
- (Exam Topic 3)
What are two characteristics of a VRF instance? (Choose two)

A. It is defined by the VPN membership of a customer site attached to a P device.
B. Each VRF has a different set of routing and CEF tables.
C. All VRFS share customers routing and CEF tables.
D. An interface must be associated to one VRF
E. A customer site can be associated to different VRFs.

Answer: BD

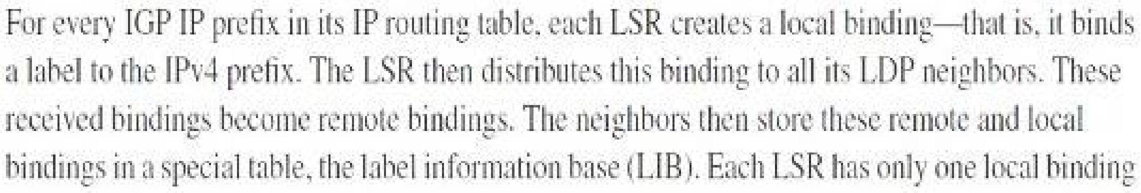
NEW QUESTION 134
- (Exam Topic 3)
What is LDP label binding?

A. neighboring router with label

B. source prefix with label
C. destination prefix with label
D. two routers with label distribution session

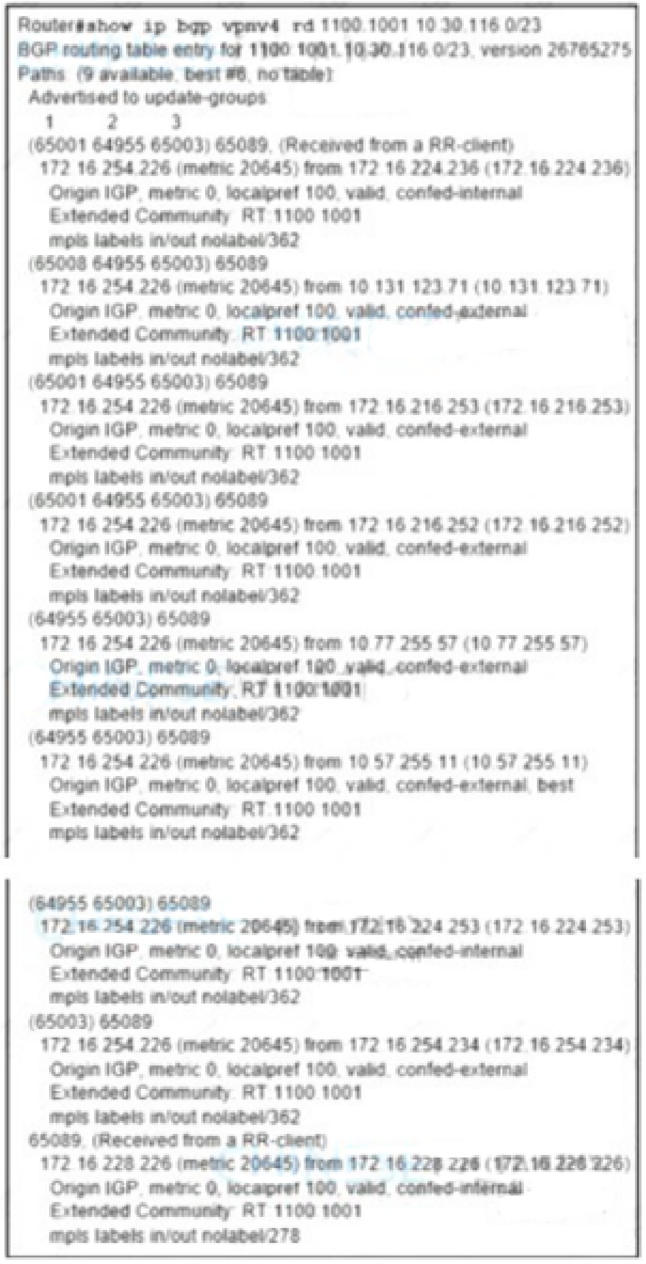
Answer: C

Explanation:
Text Description automatically generated with medium confidence



For every IGP IP prefix in its IP routing table, each LSR creates a local binding—that is, it binds a label to the IPv4 prefix. The LSR then distributes this binding to all its LDP neighbors. These received bindings become remote bindings. The neighbors then store these remote and local bindings in a special table, the label information base (LIB). Each LSR has only one local binding

NEW QUESTION 135
- (Exam Topic 3)



```
Router#show ip bgp vpnv4 rd 1100:1001 10.30.116.0/23
BGP routing table entry for 1100:1001:10.30.116.0/23, version 26765275
Paths: (9 available, best #6, no table)
  Advertised to update-groups:
     1        2        3
  (65001 64955 65003) 65089, (Received from a RR-client)
    172.16.254.226 (metric 20645) from 172.16.224.236 (172.16.224.236)
      Origin IGP, metric 0, localpref 100, valid, confed-internal
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (65008 64955 65003) 65089
    172.16.254.226 (metric 20645) from 10.131.123.71 (10.131.123.71)
      Origin IGP, metric 0, localpref 100, valid, confed-external
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (65001 64955 65003) 65089
    172.16.254.226 (metric 20645) from 172.16.216.253 (172.16.216.253)
      Origin IGP, metric 0, localpref 100, valid, confed-external
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (65001 64955 65003) 65089
    172.16.254.226 (metric 20645) from 172.16.216.252 (172.16.216.252)
      Origin IGP, metric 0, localpref 100, valid, confed-external
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (64955 65003) 65089
    172.16.254.226 (metric 20645) from 10.77.255.57 (10.77.255.57)
      Origin IGP, metric 0, localpref 100, valid, confed-external
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (64955 65003) 65089
    172.16.254.226 (metric 20645) from 10.57.255.11 (10.57.255.11)
      Origin IGP, metric 0, localpref 100, valid, confed-external, best
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362

  (64955 65003) 65089
    172.16.254.226 (metric 20645) from 172.16.224.253 (172.16.224.253)
      Origin IGP, metric 0, localpref 100, valid, confed-internal
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (65003) 65089
    172.16.254.226 (metric 20645) from 172.16.254.234 (172.16.254.234)
      Origin IGP, metric 0, localpref 100, valid, confed-external
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  65089, (Received from a RR-client)
    172.16.228.226 (metric 20645) from 172.16.228.226 (172.16.228.226)
      Origin IGP, metric 0, localpref 100, valid, confed-internal
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/278
```

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

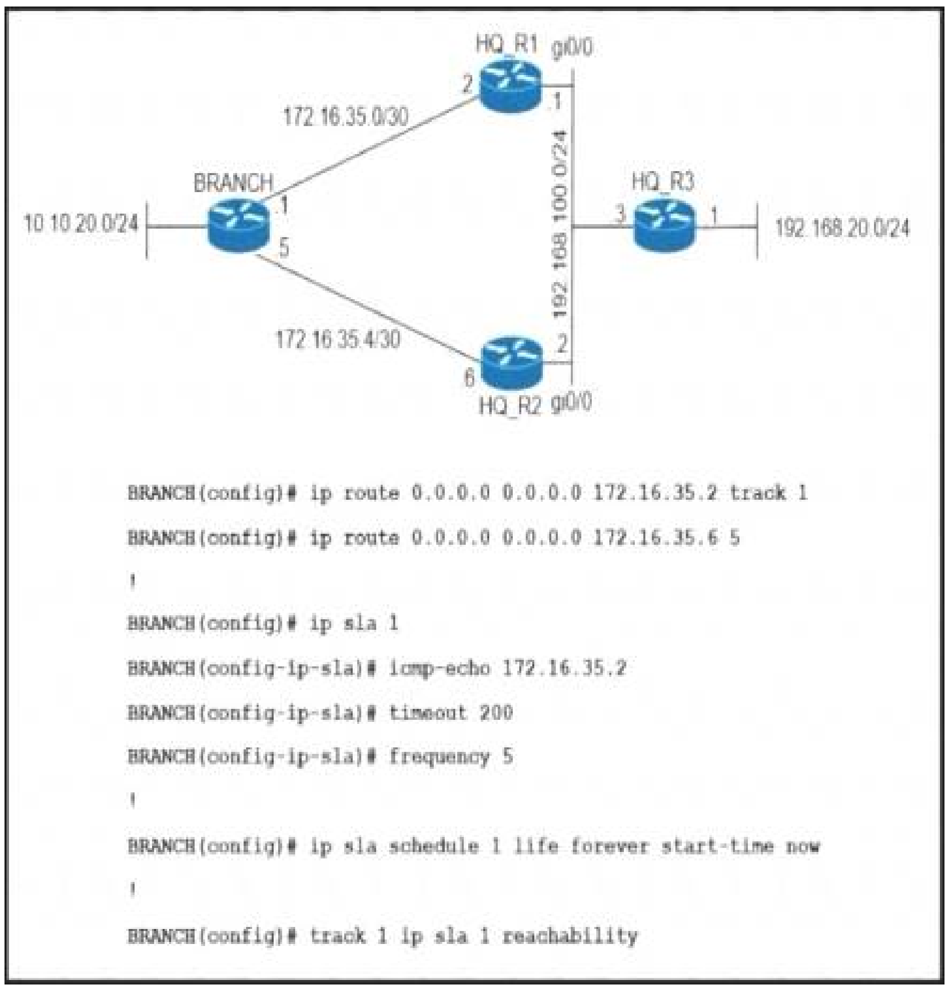
Answer: D

NEW QUESTION 140
- (Exam Topic 3)
An engineer configured routing between multiple OSPF domains and introduced a routing loop that caused network instability. Which action resolves the problem?

A. Set a tag using the redistribute command toward a domain and deny inbound m the other domain by a matching tag
B. Set a tag using the redistribute command toward a different domain and deny the matching tag when exiting from that domain
C. Set a tag using the network command in a domain and use the route-map command to deny the matching lag when exiting toward a different domain
D. Set a tag using the network command in a domain and use the route-map command to deny the matching tag when entering into a different domain

Answer: A

NEW QUESTION 145
- (Exam Topic 2)



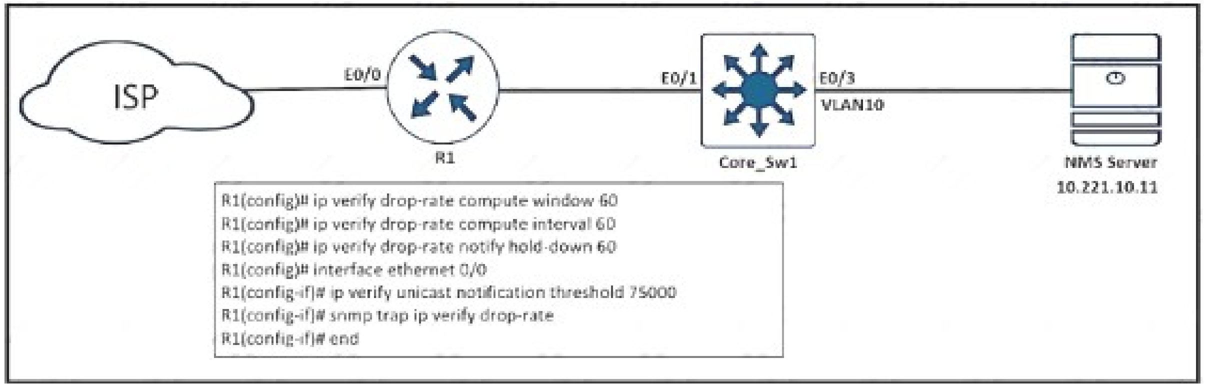
```
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.2 track 1
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.6 5
!
BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 172.16.35.2
BRANCH(config-ip-sla)# timeout 200
BRANCH(config-ip-sla)# frequency 5
!
BRANCH(config)# ip sla schedule 1 life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

Refer to the exhibit. 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. HQ_R3(config)# ip sla responderHQ_R3(config)# ip sla responder icmp-echo 172.16.35.1
B. BRANCH(config)# ip sla 1BRANCH(config-ip-sla)# icmp-echo 192.168.100.2
C. HQ R3(config)# Ip sla responderHQ R3(config)# Ip sla responder Icmp-echo 172.16.35.5
D. BRANCH(config)# Ip sla 1BRANCH(config-ip-sta)# Icmp-echo 192.168.100.1

Answer: D

NEW QUESTION 150
- (Exam Topic 3)



```
R1(config)# ip verify drop-rate compute window 60
R1(config)# ip verify drop-rate compute interval 60
R1(config)# ip verify drop-rate notify hold-down 60
R1(config)# interface ethernet 0/0
R1(config-if)# ip verify unicast notification threshold 75000
R1(config-if)# snmp trap ip verify drop-rate
R1(config-if)# end
```

Refer to the exhibit. An engineer configured SNMP traps to record spoofed packets drop of more than 48000 a minute on the ethernet0/0 interlace. During an IP spoofing attack, the engineer noticed that no notifications have been received by the SNMP server. Which configuration resolves the issue on R1?

A. ip verity unicast notification threshold 48000
B. ip verify unicast notification threshold 8000
C. ip verify unicast notification threshold 800
D. ip verify unicast notification threshold 80

Answer: C

NEW QUESTION 153
- (Exam Topic 3)
What is a function of an end device configured with DHCPv6 guard?

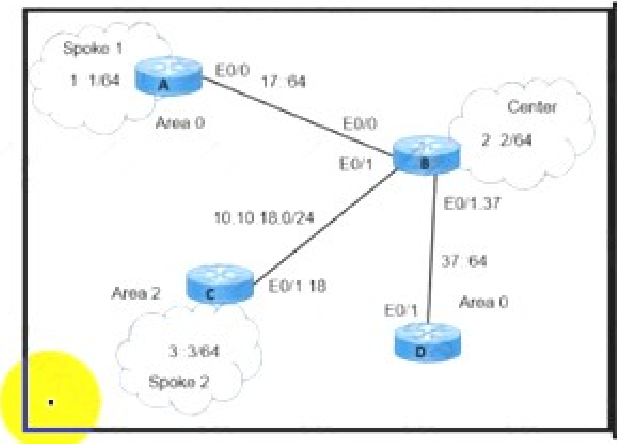
A. If it is configured as a server, only prefix assignments are permitted.
B. If it is configured as a relay agent, only prefix assignments are permitted.
C. If it is configured as a client, messages are switched regardless of the assigned role.
D. If it is configured as a client, only DHCP requests are permitted.

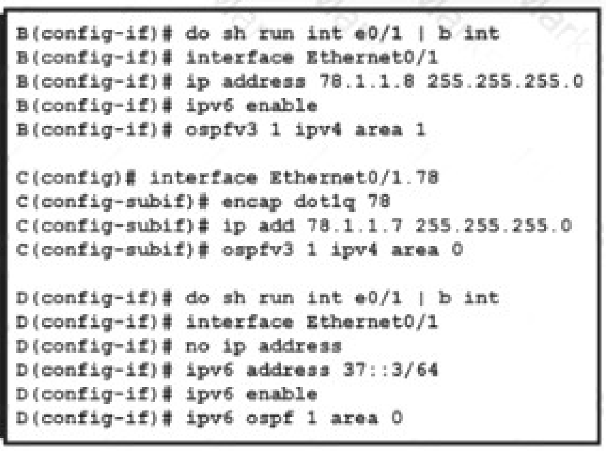
Answer: C

Explanation:

The DHCPv6 Guard feature blocks reply and advertisement messages that come from unauthorized DHCP servers and relay agents.
Packets are classified into one of the three DHCP type messages. All client messages are always switched regardless of device role. DHCP server messages are only processed further if the device role is set to server. Further processing of server messages includes DHCP server advertisements (for source validation and server preference) and DHCP server replies (for permitted prefixes).
If the device is configured as a DHCP server, all the messages need to be switched, regardless of the device role configuration.

NEW QUESTION 156
- (Exam Topic 3)





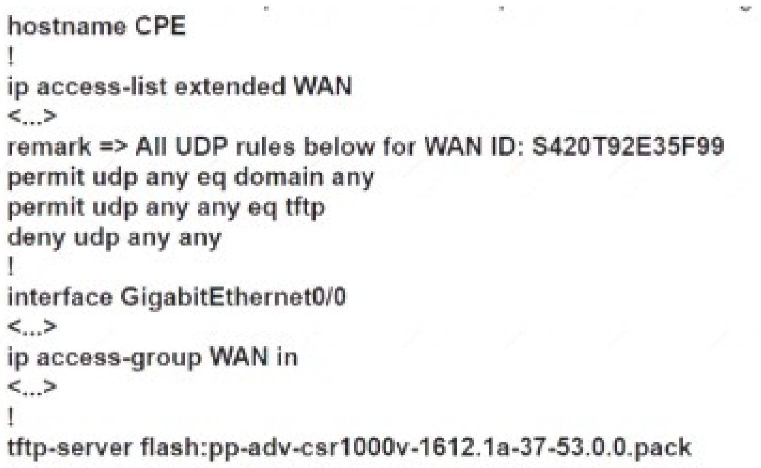
```
B(config-if)# do sh run int e0/1 | b int
B(config-if)# interface Ethernet0/1
B(config-if)# ip address 78.1.1.8 255.255.255.0
B(config-if)# ipv6 enable
B(config-if)# ospfv3 1 ipv4 area 1

C(config)# interface Ethernet0/1.78
C(config-subif)# encap dot1q 78
C(config-subif)# ip add 78.1.1.7 255.255.255.0
C(config-subif)# ospfv3 1 ipv4 area 0

D(config-if)# do sh run int e0/1 | b int
D(config-if)# interface Ethernet0/1
D(config-if)# no ip address
D(config-if)# ipv6 address 37::3/64
D(config-if)# ipv6 enable
D(config-if)# ipv6 ospf 1 area 0
```

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 the Spoke 2 users IP on the router B OSPF domain
B. Configure encapsulation dot1q 78 on the router C interface.
C. Configure IPv6 on the routers B and C interfaces
D. Configure OSPFv2 on the routers B and C interfaces

Answer: C

NEW QUESTION 158
- (Exam Topic 3)
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:



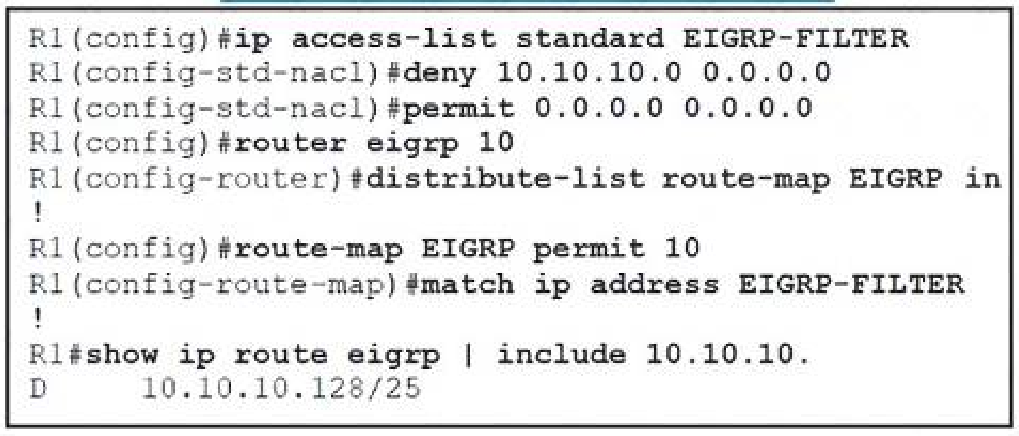
```
hostname CPE
!
ip access-list extended WAN
<...>
remark => All UDP rules below for WAN ID: S420T92E35F99
permit udp any eq domain any
permit udp any any eq tftp
deny udp any any
!
interface GigabitEthernet0/0
<...>
ip access-group WAN in
<...>
!
tftp-server flash:pp-adv-csr1000v-1612.1a-37-53.0.0.pack
```

The transfer fails. Which action resolves the issue?

A. Change the WAN ACL to permit the UDP port 69 to allow TFTP
B. Make the permit udp any eq tftp any entry the last entry in the WAN ACL.
C. Change the WAN ACL to permit the entire UDP destination port range
D. Shorten the file name to the 8+3 naming convention.

Answer: B

NEW QUESTION 163
- (Exam Topic 3)



```
R1(config)#ip access-list standard EIGRP-FILTER
R1(config-std-nacl)#deny 10.10.10.0 0.0.0.0
R1(config-std-nacl)#permit 0.0.0.0 0.0.0.0
R1(config)#router eigrp 10
R1(config-router)#distribute-list route-map EIGRP in
!
R1(config)#route-map EIGRP permit 10
R1(config-route-map)#match ip address EIGRP-FILTER
!
R1#show ip route eigrp | include 10.10.10.
D      10.10.10.128/25
```

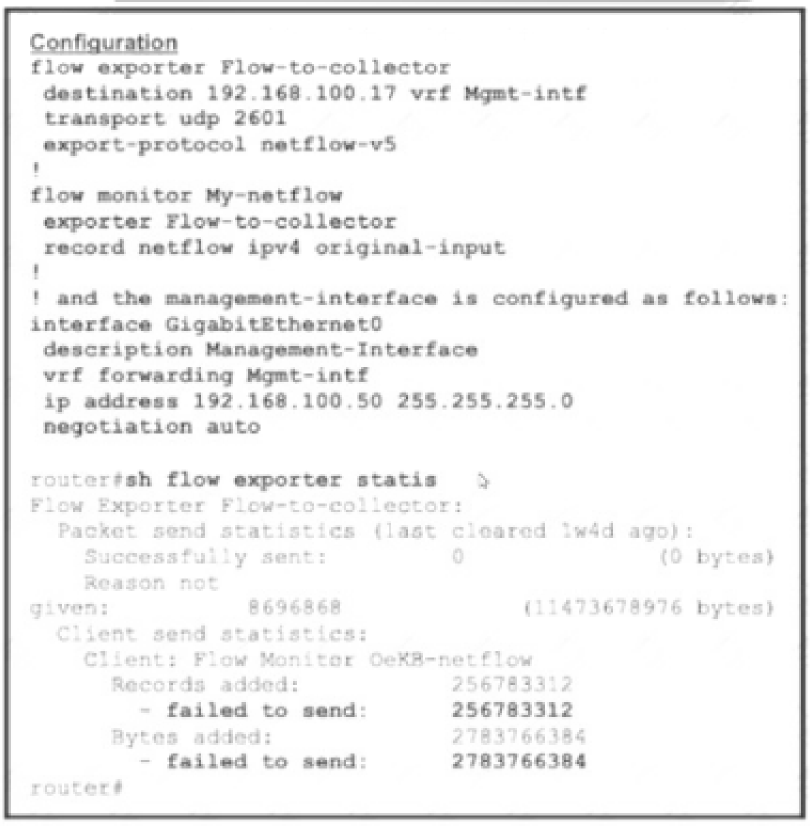
Refer to lhe exhibit An engineer must filter EIGRP updates that are received to block all 10 10 10.0/24 prefixes The engineer tests the distribute list and finds one associated prefix. Which action resolves the issue?

A. There is a permit in the route map that allows this prefix A deny 20 statement is required with a match condition to match a new ACL that denies all prefixes
B. There is a permit in the ACL that allows this prefix into EI6R
C. The ACL should be modified to deny 10.10.10.0 0.0.0.255.
D. There is a permit in the route map that allows this prefix A deny 20 statement is required with no match condition to block the prefix.
E. There is a permit in the ACL that allows this prefix into EIGR
F. The ACL should be modified to deny 10.10.10.0 255.255.255.0.

Answer: B

NEW QUESTION 167

- (Exam Topic 3)



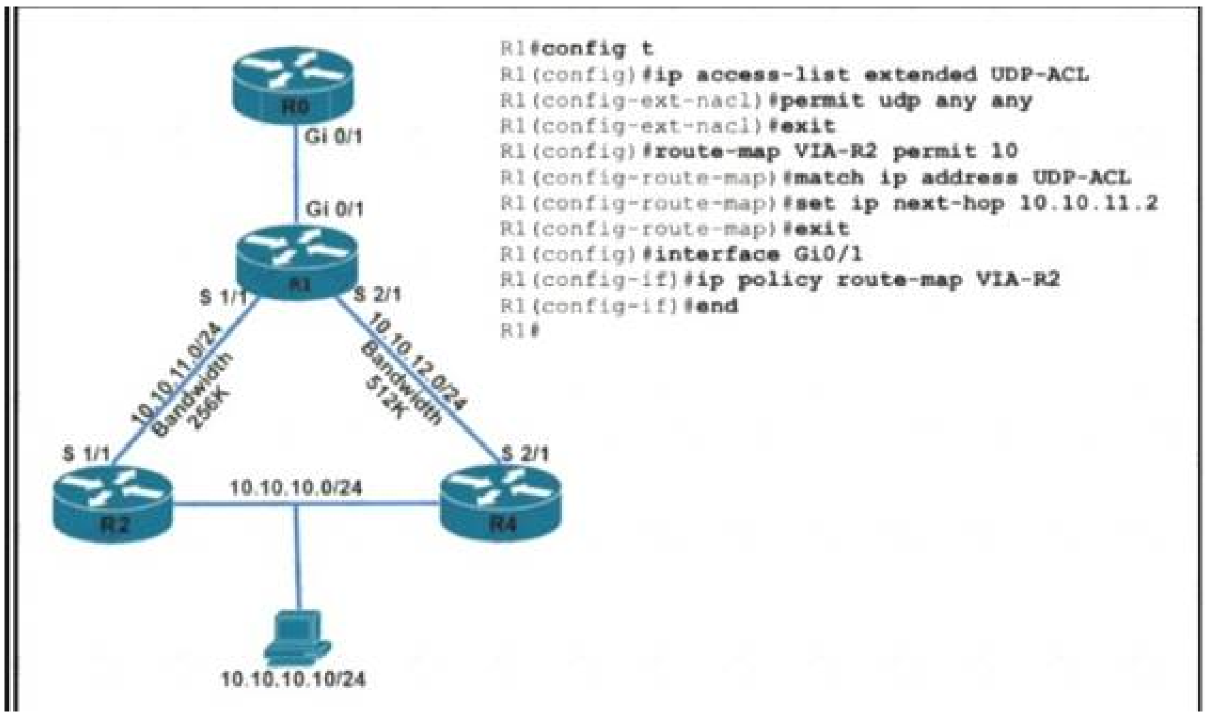
```
Configuration
flow exporter Flow-to-collector
 destination 192.168.100.17 vrf Mgmt-intf
 transport udp 2601
 export-protocol netflow-v5
!
flow monitor My-netflow
 exporter Flow-to-collector
 record netflow ipv4 original-input
!
! and the management-interface is configured as follows:
interface GigabitEthernet0
 description Management-Interface
 vrf forwarding Mgmt-intf
 ip address 192.168.100.50 255.255.255.0
 negotiation auto

router#sh flow exporter statis
Flow Exporter Flow-to-collector:
  Packet send statistics (last cleared 1w4d ago):
    Successfully sent:          0                 (0 bytes)
    Reason not
given:              8696868              (11473678976 bytes)
  Client send statistics:
    Client: Flow Monitor OeKB-netflow
      Records added:            256783312
        - failed to send:       256783312
      Bytes added:              2783766384
        - failed to send:       2783766384
router#
```

Refer to the exhibit. A network administrator configured NetFlow data, but the data is not visible at the NetFlow collector. Which configuration allows the router to send the records?

A. Configure the management interface in the global routing table to send the records.
B. Configure a different interface to send the records.
C. Configure the NetFlow collector to listen at export-protocol netflow-v5.
D. Rectify NetFlow collector reachability from the management interface.

Answer: B

NEW QUESTION 168
- (Exam Topic 3)
Refer to the exhibit.



```
R1#config t
R1(config)#ip access-list extended UDP-ACL
R1(config-ext-nacl)#permit udp any any
R1(config-ext-nacl)#exit
R1(config)#route-map VIA-R2 permit 10
R1(config-route-map)#match ip address UDP-ACL
R1(config-route-map)#set ip next-hop 10.10.11.2
R1(config-route-map)#exit
R1(config)#interface Gi0/1
R1(config-if)#ip policy route-map VIA-R2
R1(config-if)#end
R1#
```

TCP traffic should be reaching host 10.10.10.10/24 via R2. Which action resolves the issue?

A. TCP traffic will reach the destination via R2 without any changes
B. Add a permit 20 statement in the route map to allow TCP traffic
C. Allow TCP in the access list with no changes to the route map
D. Set IP next-hop to 10.10.12.2 under the route-map permit 10 to allow TCP traffic.

Answer: C

NEW QUESTION 170
- (Exam Topic 3)
What is a characteristic of IPv6 RA Guard?

A. RA messages are allowed from the host port to the switch
B. It is unable to protect tunneled traffic
C. It filters rogue RA broadcasts from connected hosts
D. It is supported on the egress direction of the switch

Answer: C

NEW QUESTION 175

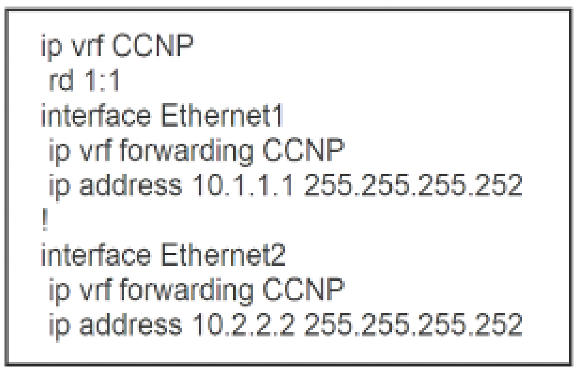
- (Exam Topic 3)
A CoPP policy is applied for receiving SSH traffic from the WAN interface on a Cisco ISR4321 router. However, the SSH response from the router is abnormal and stuck during the high link utilization. The problem is identified as SSH traffic does not match in the ACL. Which action resolves 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

Explanation:
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 180
- (Exam Topic 3)
Refer to the exhibit.



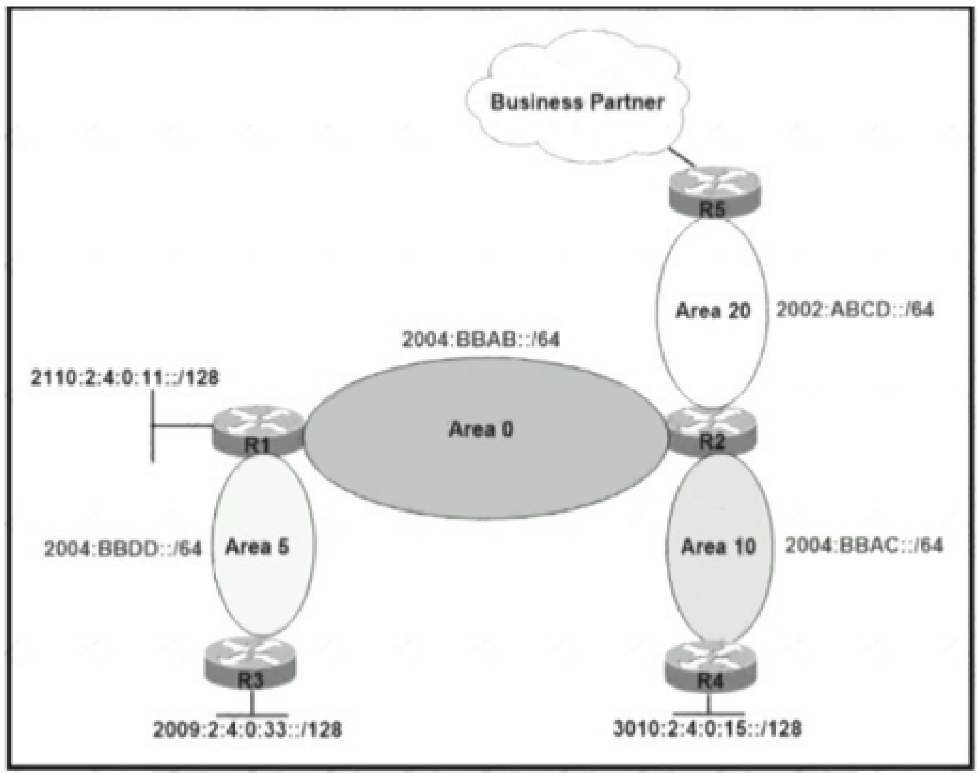
```
ip vrf CCNP
 rd 1:1
interface Ethernet1
 ip vrf forwarding CCNP
 ip address 10.1.1.1 255.255.255.252
!
interface Ethernet2
 ip vrf forwarding CCNP
 ip address 10.2.2.2 255.255.255.252
```

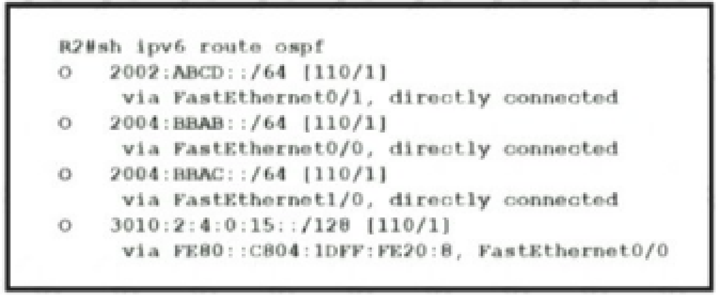
Which configuration enables OSPF for area 0 interfaces to adjacency with a neighboring router with the same VRF?

A. router ospf 1 vrf CCNP interface Ethernet1ip ospf 1 area 0.0.0.0 interface Ethernet2 ip ospf 1 area 0.0.0.0
B. router ospf 1 interface Ethernet1ip ospf 1 area 0.0.0.0 interface Ethernet2 ip ospf 1 area 0.0.0.0
C. router ospf 1 vrf CCNP network 10.1.1.1 0.0.0.0 area 0network 10.2.2.2 0.0.0.0 area 0
D. router ospf 1 vrf CCNPnetwork 10.0.0.0 0.0.255.255 area 0

Answer: C

NEW QUESTION 181
- (Exam Topic 3)
Refer to the exhibit.





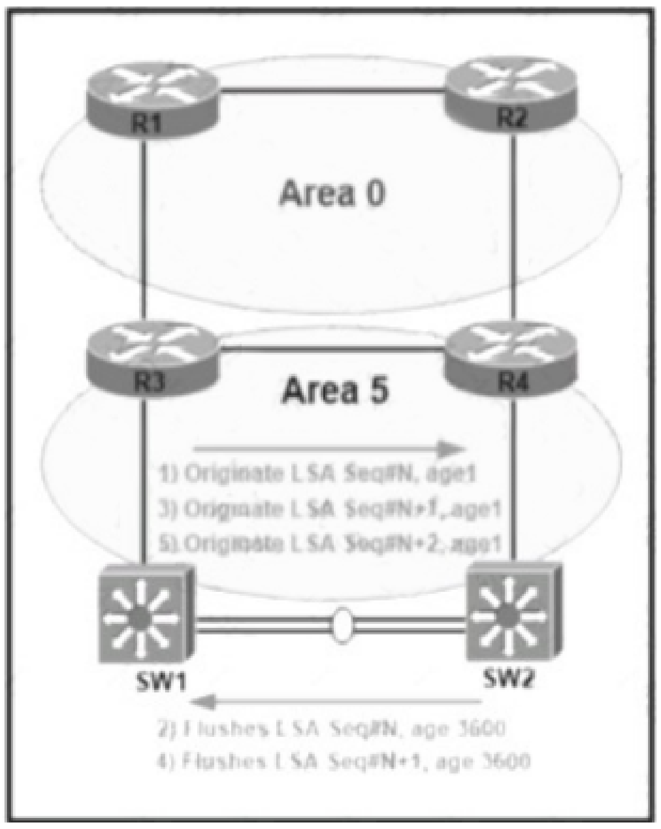
```
R2#sh ipv6 route ospf
O    2002:ABCD::/64 [110/1]
      via FastEthernet0/1, directly connected
O    2004:BBAB::/64 [110/1]
      via FastEthernet0/0, directly connected
O    2004:BBAC::/64 [110/1]
      via FastEthernet1/0, directly connected
O    3010:2:4:0:15::/128 [110/1]
      via FE80::C804:1DFF:FE20:8, FastEthernet0/0
```

A network engineer applied a filter for LSA traffic on OSPFv3 interarea routes on the area 5 ABR to protect advertising the internal routes of area 5 to the business partner network. All other areas should receive the area 5 internal routes. After the respective route filtering configuration is applied on the ABR, area 5 routes are not visible on any of the areas. How must the filter list be applied on the ABR to resolve this issue?

A. in the “in” direction for area 5 on router R1
B. in the “out” direction for area 5 on router R1
C. in the “in” direction for area 20 on router R2
D. in the “out” direction for area 20 on router R2

Answer: D

NEW QUESTION 182
- (Exam Topic 3)
Refer to the exhibit.

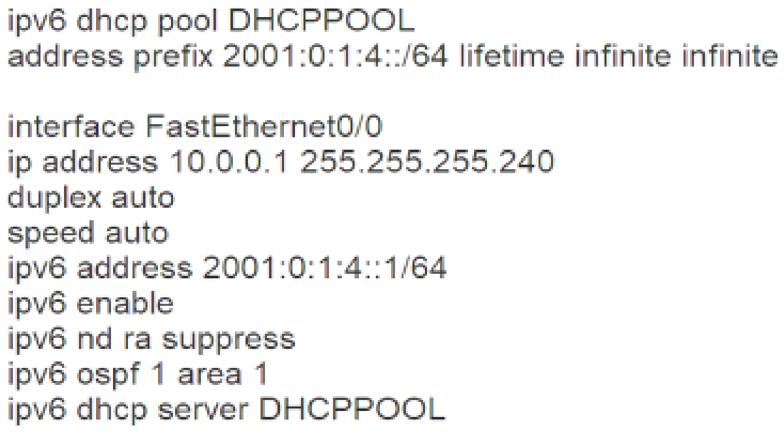

R1
R2
Area 0
R3
R4
Area 5
1) Originate LSA Seq#N, age1
3) Originate LSA Seq#N+1, age1
5) Originate LSA Seq#N+2, age1
SW1
SW2
2) Flushes LSA Seq#N, age 3600
4) Flushes LSA Seq#N+1, age 3600

An error message "an OSPF-4-FLOOD_WAR” is received on SW2 from SW1. SW2 is repeatedly receiving its own link-state advertisement and flushes it from the network. Which action resolves the issue?

A. Change area 5 to a normal area from a nonstub area
B. Resolve different subnet mask issue on the link
C. Configure Layer 3 port channel on interfaces between switches
D. Resolve duplicate IP address issue in the network

Answer: D

NEW QUESTION 183
- (Exam Topic 3)
Refer to the exhibit.



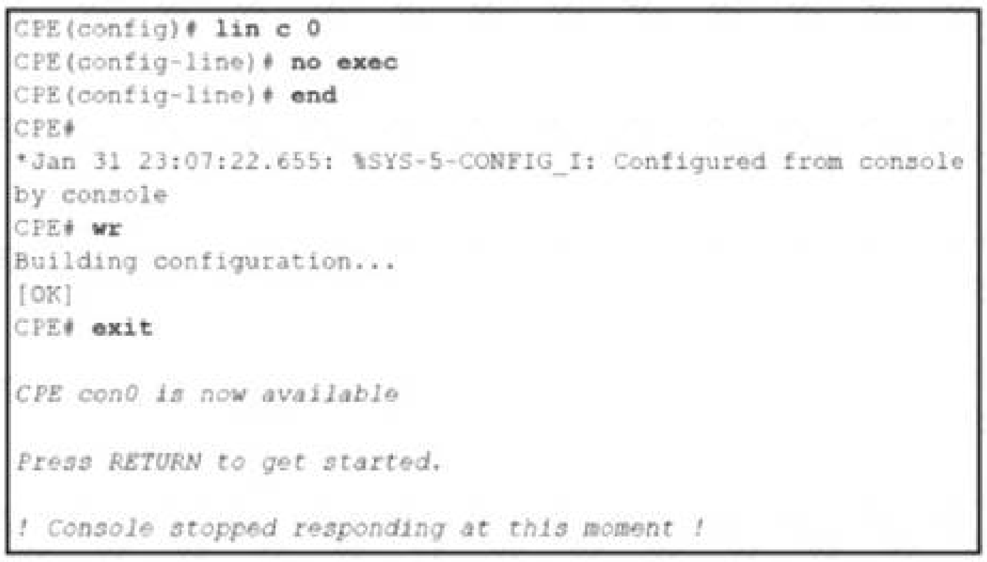
```
ipv6 dhcp pool DHCPPOOL
address prefix 2001:0:1:4::/64 lifetime infinite infinite

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. ipv6 dhcp server DHCPPOOL
B. ipv6 address 2001:0:1:4::/64
C. ipv6 nd ra suppress
D. address prefix 2001:0:1:4::/64 lifetime infinite infinite

Answer: C

NEW QUESTION 187
- (Exam Topic 3)
Refer to the exhibit.



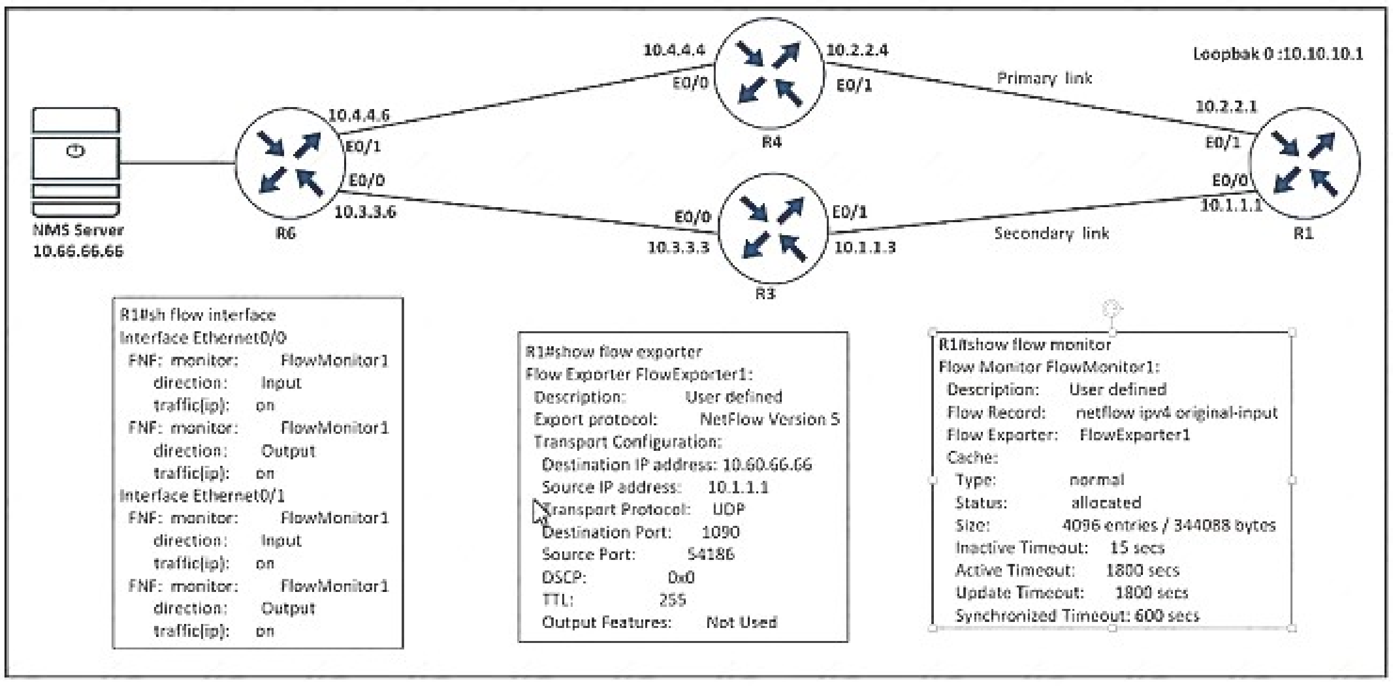
```
CPE(config)# lin c 0
CPE(config-line)# no exec
CPE(config-line)# end
CPE#
*Jan 31 23:07:22.655: %SYS-5-CONFIG_I: Configured from console
by console
CPE# wr
Building configuration...
[OK]
CPE# exit

CPE con0 is now available

Press RETURN to get started.

! Console stopped responding at this moment !
```

An administrator is attempting to disable the automatic logout after a period of inactivity. After logging out the console stopped responding to all keyword inputs. Remote access through SSH still work resolves the issue?

A. Configure the exec command on line con 0.
B. Configure the absolute-timeout command on line con 0.
C. Configure the default exec-timeout command on line con 0.
D. Configure the no exec-timeout command on line con 0.

Answer: D

NEW QUESTION 188
- (Exam Topic 3)

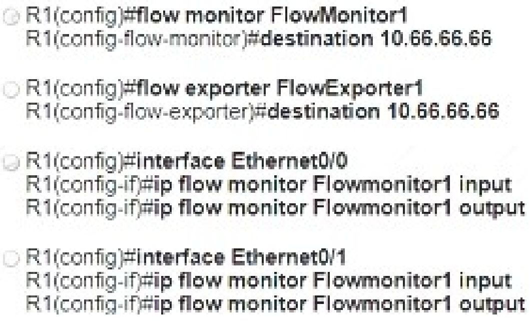


```
R1#sh flow interface
Interface Ethernet0/0
  FNF:  monitor:        FlowMonitor1
        direction:      Input
        traffic(ip):    on
  FNF:  monitor:        FlowMonitor1
        direction:      Output
        traffic(ip):    on
Interface Ethernet0/1
  FNF:  monitor:        FlowMonitor1
        direction:      Input
        traffic(ip):    on
  FNF:  monitor:        FlowMonitor1
        direction:      Output
        traffic(ip):    on
```

```
R1#show flow exporter
Flow Exporter FlowExporter1:
  Description:            User defined
  Export protocol:        NetFlow Version 5
  Transport Configuration:
    Destination IP address: 10.60.66.66
    Source IP address:     10.1.1.1
    Transport Protocol:    UDP
    Destination Port:      1090
    Source Port:           54186
    DSCP:                  0x0
    TTL:                   255
    Output Features:       Not Used
```

```
R1#show flow monitor
Flow Monitor FlowMonitor1:
  Description:      User defined
  Flow Record:      netflow ipv4 original-input
  Flow Exporter:    FlowExporter1
  Cache:
    Type:                 normal
    Status:               allocated
    Size:                 4096 entries / 344088 bytes
    Inactive Timeout:     15 secs
    Active Timeout:       1800 secs
    Update Timeout:       1800 secs
    Synchronized Timeout: 600 secs
```

Refer to the exhibit. An engineer configured NetFlow on R1, but the flows do not reach the NMS server from R1. Which configuration resolves this Issue?



○ R1(config)#**flow monitor FlowMonitor1**
R1(config-flow-monitor)#**destination 10.66.66.66**

○ R1(config)#**flow exporter FlowExporter1**
R1(config-flow-exporter)#**destination 10.66.66.66**

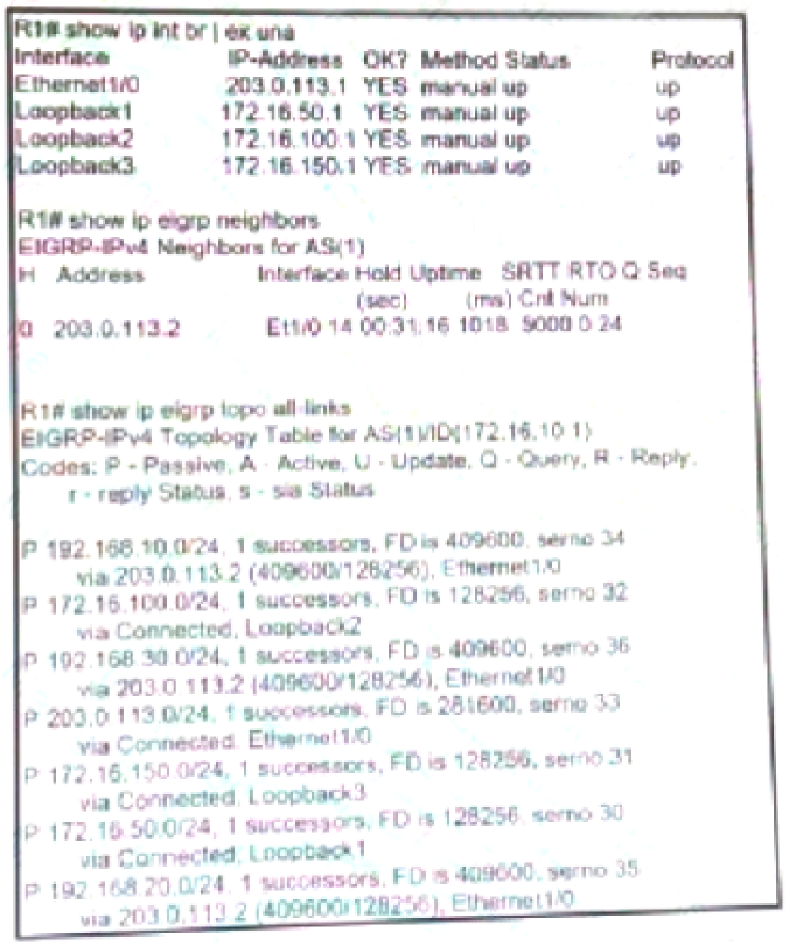
○ R1(config)#**interface Ethernet0/0**
R1(config-if)#**ip flow monitor Flowmonitor1 input**
R1(config-if)#**ip flow monitor Flowmonitor1 output**

○ R1(config)#**interface Ethernet0/1**
R1(config-if)#**ip flow monitor Flowmonitor1 input**
R1(config-if)#**ip flow monitor Flowmonitor1 output**

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

Answer: B

NEW QUESTION 191
- (Exam Topic 3)
Refer to the exhibit.



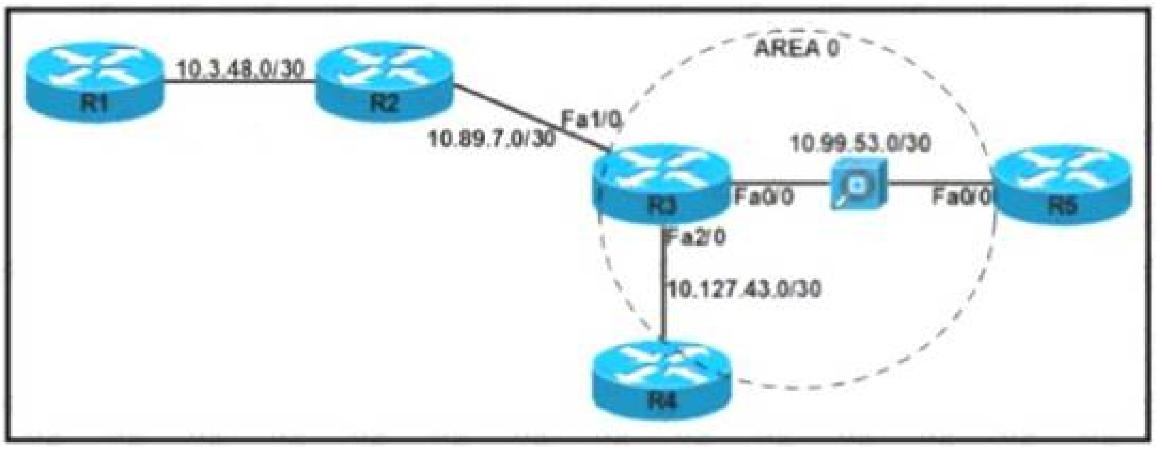
```
R1# show ip int br | ex una
Interface           IP-Address  OK? Method Status      Protocol
Ethernet1/0         203.0.113.1 YES manual up          up
Loopback1           172.16.50.1 YES manual up          up
Loopback2           172.16.100.1 YES manual up         up
Loopback3           172.16.150.1 YES manual up         up

R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address            Interface Hold Uptime   SRTT RTO Q Seq
                                 (sec)         (ms) Cnt Num
0   203.0.113.2        Et1/0 14 00:31:16 1018 5000 0 24


R1# show ip eigrp topo all-links
EIGRP-IPv4 Topology Table for AS(1)/ID(172.16.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.0/24, 1 successors, FD is 409600, serno 34
        via 203.0.113.2 (409600/128256), Ethernet1/0
P 172.16.100.0/24, 1 successors, FD is 128256, serno 32
        via Connected, Loopback2
P 192.168.30.0/24, 1 successors, FD is 409600, serno 36
        via 203.0.113.2 (409600/128256), Ethernet1/0
P 203.0.113.0/24, 1 successors, FD is 281600, serno 33
        via Connected, Ethernet1/0
P 172.16.150.0/24, 1 successors, FD is 128256, serno 31
        via Connected, Loopback3
P 172.16.50.0/24, 1 successors, FD is 128256, serno 30
        via Connected, Loopback1
P 192.168.20.0/24, 1 successors, FD is 409600, serno 35
        via 203.0.113.2 (409600/128256), Ethernet1/0
```

Routers R1 and R2 have established a network adjacency using EIGRP, and both routers are advertising subnets to its neighbor. After issuing the show ip EIGRP topology all-links command in R1, some prefixes are no showing R2 as a successor. Which action resolves the issue?

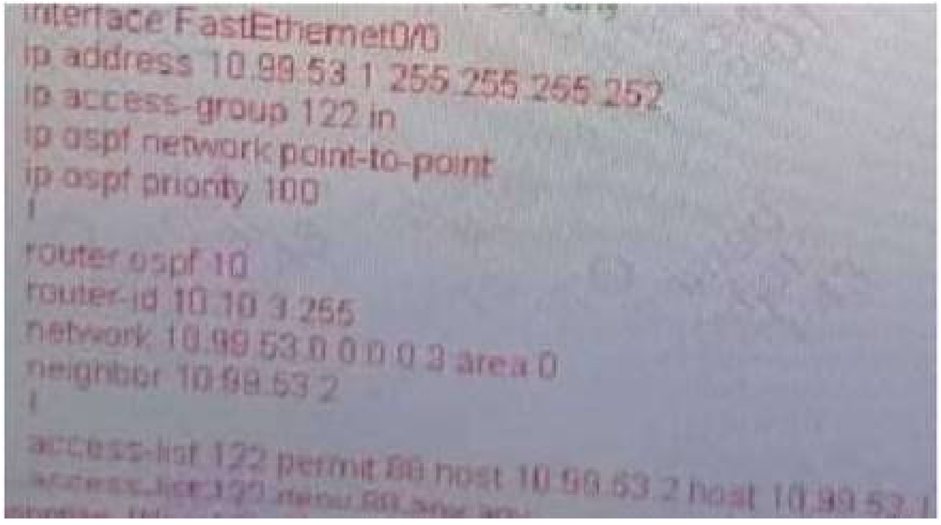
A. Rectify the incorrect router ID in R2.
B. Enable split-horizon.
C. Configure the network statement on the neighbor.
D. Resolve the incorrect metric on the link.

Answer: D

NEW QUESTION 196
- (Exam Topic 3)
Refer to the exhibit.

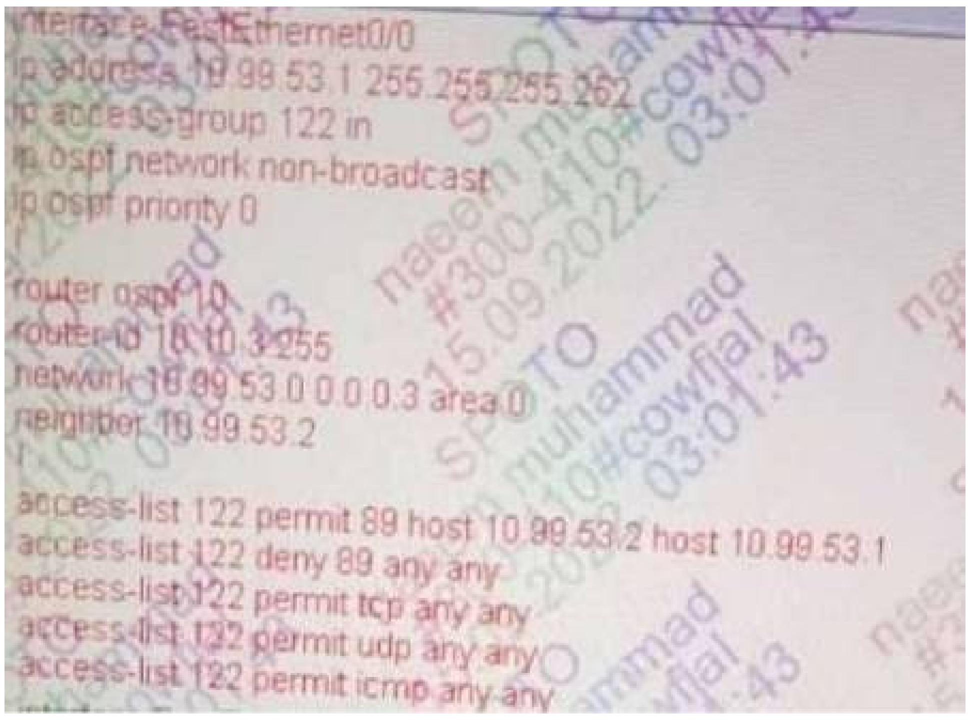


The security department recently installed a monitoring device between routers R3 and R5, which a loss of network connectivity for users connected to R5. Troubleshooting revealed that the monitoring device cannot forward multicast packets. The team already updated R5 with the correct configuration. Which configuration must be implemented on R3 to resolve the problem by ensuring R3 as the DR for the R3-R5 segment?
A)



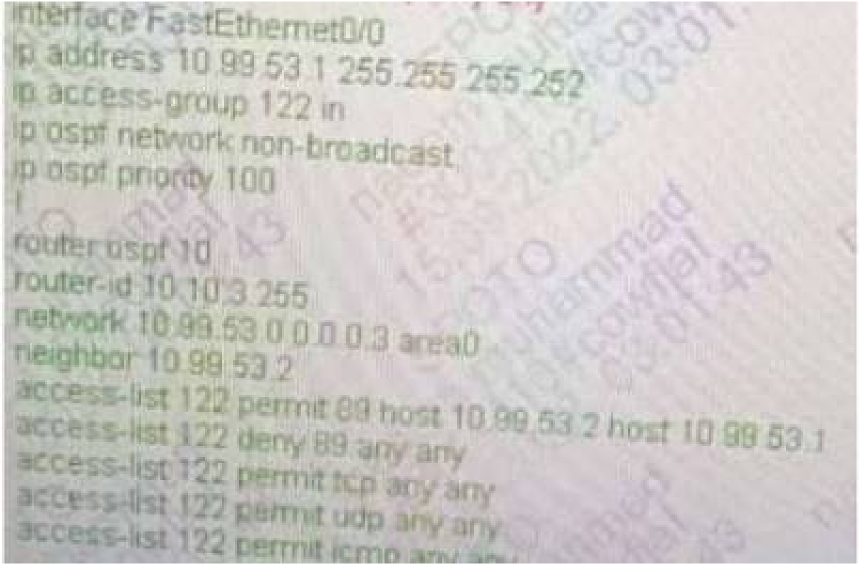
```
interface FastEthernet0/0
ip address 10.99.53.1 255.255.255.252
ip access-group 122 in
ip ospf network point-to-point
ip ospf priority 100
!
router ospf 10
router-id 10.10.3.255
network 10.99.53.0 0.0.0.3 area 0
neighbor 10.99.53.2
!
access-list 122 permit 89 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 89 any any
```

B)



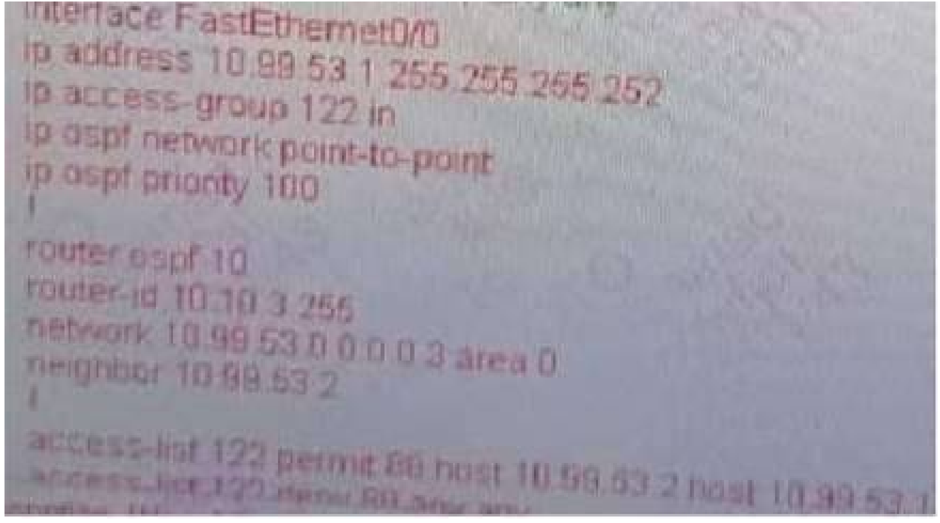
```
interface FastEthernet0/0
ip address 10.99.53.1 255.255.255.252
ip access-group 122 in
ip ospf network non-broadcast
ip ospf priority 0
!
router ospf 10
router-id 10.10.3.255
network 10.99.53.0 0.0.0.3 area 0
neighbor 10.99.53.2
!
access-list 122 permit 89 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 89 any any
access-list 122 permit tcp any any
access-list 132 permit udp any any
access-list 122 permit icmp any any
```

C)



```
interface FastEthernet0/0
ip address 10.99.53.1 255.255.255.252
ip access-group 122 in
ip ospf network non-broadcast
ip ospf priority 100
!
router ospf 10
router-id 10.10.3.255
network 10.99.53.0 0.0.0.3 area0
neighbor 10.99.53.2
access-list 122 permit 89 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 89 any any
access-list 122 permit tcp any any
access-list 122 permit udp any any
access-list 122 permit icmp any any
```

D)

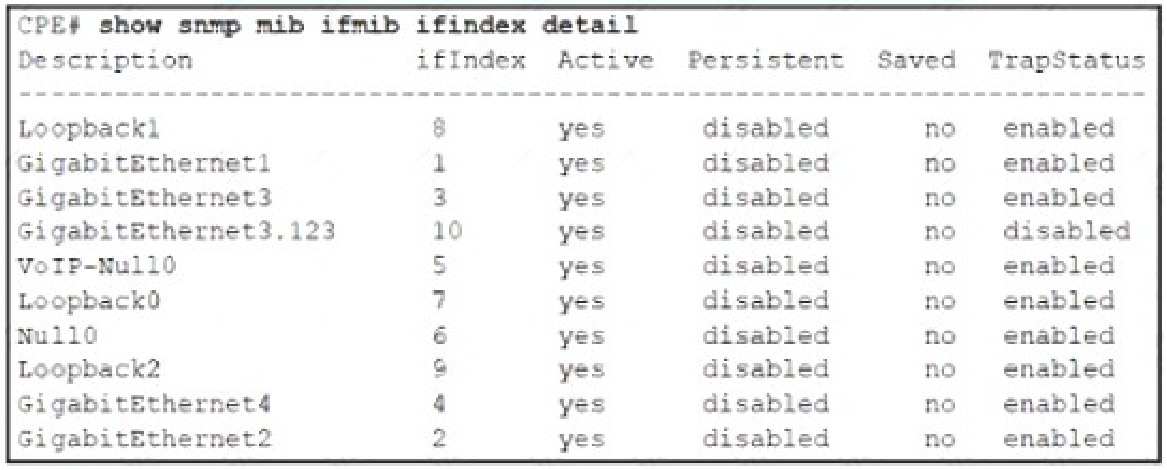


```
interface FastEthernet0/0
ip address 10.99.53.1 255.255.255.252
ip access-group 122 in
ip ospf network point-to-point
ip ospf priority 100
!
router ospf 10
router-id 10.10.3.255
network 10.99.53.0 0.0.0.3 area 0
neighbor 10.99.53.2
!
access-list 122 permit 89 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 89 any any
```

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

Answer: C

NEW QUESTION 198
- (Exam Topic 3)



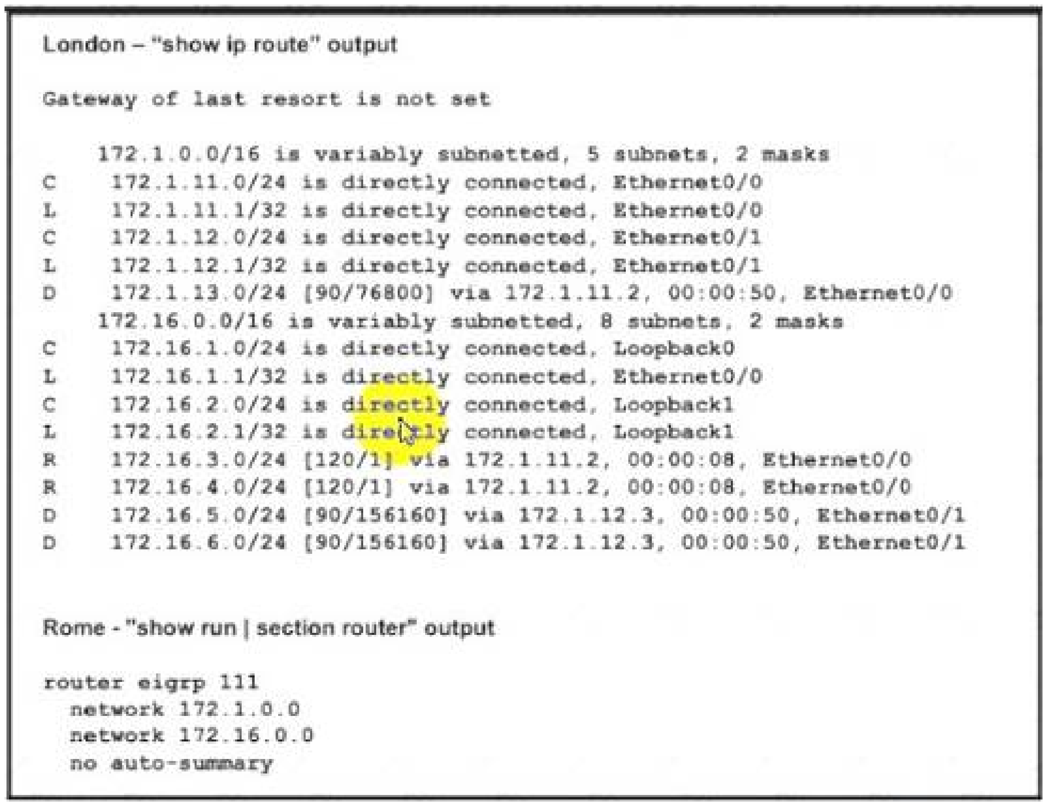
```
CPE# show snmp mib ifmib ifindex detail
Description              ifIndex  Active   Persistent   Saved   TrapStatus
-------------------------------------------------------------------------
Loopback1                  8       yes      disabled      no     enabled
GigabitEthernet1           1       yes      disabled      no     enabled
GigabitEthernet3           3       yes      disabled      no     enabled
GigabitEthernet3.123       10      yes      disabled      no     disabled
VoIP-Null0                 5       yes      disabled      no     enabled
Loopback0                  7       yes      disabled      no     enabled
Null0                      6       yes      disabled      no     enabled
Loopback2                  9       yes      disabled      no     enabled
GigabitEthernet4           4       yes      disabled      no     enabled
GigabitEthernet2           2       yes      disabled      no     enabled
```

Refer to the exhibit. After reloading the router an administrator discovered that the interface utilization graphs displayed inconsistencies with their previous history in the NMS. Which action prevents this issue from occurring after another router reload in the future?

A. Rediscover all the router interfaces through SNMP after the router is reloaded
B. Save the router configuration to startup-config before reloading the router
C. Configure SNMP to use static OIDs referring to individual router interfaces
D. Configure SNMP interface index persistence on the router

Answer: D

NEW QUESTION 201
- (Exam Topic 3)
Refer to the exhibits.

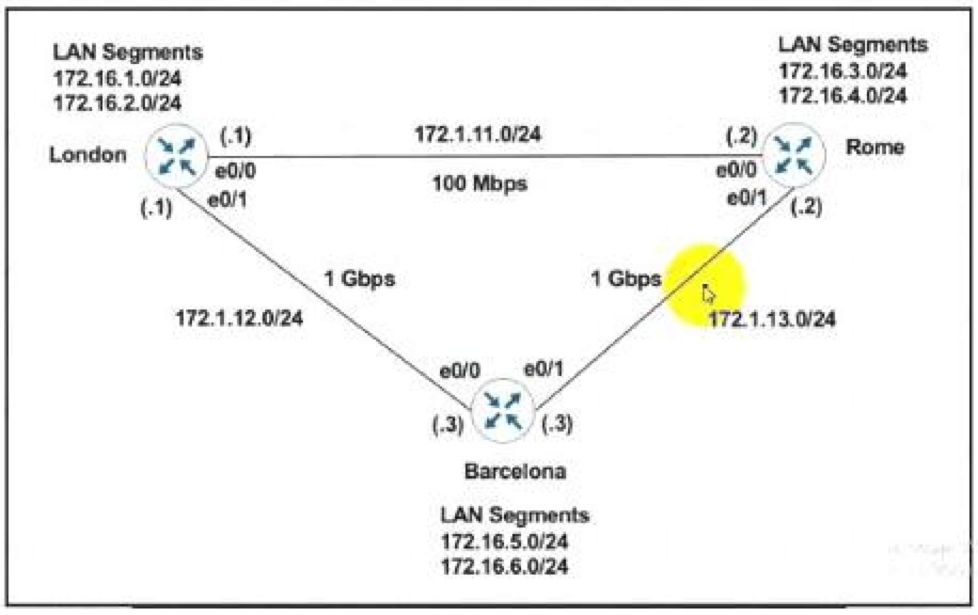


London – "show ip route" output

```
Gateway of last resort is not set

    172.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
C     172.1.11.0/24 is directly connected, Ethernet0/0
L     172.1.11.1/32 is directly connected, Ethernet0/0
C     172.1.12.0/24 is directly connected, Ethernet0/1
L     172.1.12.1/32 is directly connected, Ethernet0/1
D     172.1.13.0/24 [90/76800] via 172.1.11.2, 00:00:50, Ethernet0/0
    172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C     172.16.1.0/24 is directly connected, Loopback0
L     172.16.1.1/32 is directly connected, Ethernet0/0
C     172.16.2.0/24 is directly connected, Loopback1
L     172.16.2.1/32 is directly connected, Loopback1
R     172.16.3.0/24 [120/1] via 172.1.11.2, 00:00:08, Ethernet0/0
R     172.16.4.0/24 [120/1] via 172.1.11.2, 00:00:08, Ethernet0/0
D     172.16.5.0/24 [90/156160] via 172.1.12.3, 00:00:50, Ethernet0/1
D     172.16.6.0/24 [90/156160] via 172.1.12.3, 00:00:50, Ethernet0/1
```

Rome - "show run | section router" output

```
router eigrp 111
  network 172.1.0.0
  network 172.16.0.0
  no auto-summary
```



London must reach Rome using a faster path via EIGRP if all the links are up but it failed to take this path Which action resolves the issue?

A. Increase the bandwidth of the link between London and Barcelona
B. Use the network statement on London to inject the 172 16 X 0/24 networks into EIGRP.
C. Change the administrative distance of RIP to 150
D. Use the network statement on Rome to inject the 172 16 X 0/24 networks into EIGRP

Answer: D

NEW QUESTION 204
- (Exam Topic 3)
Which table is used to map the packets in an MPLS LSP that exit from the same interface, via the same next hop, and have the same queuing policies?

A. RIB
B. FEC
C. LDP
D. CEF

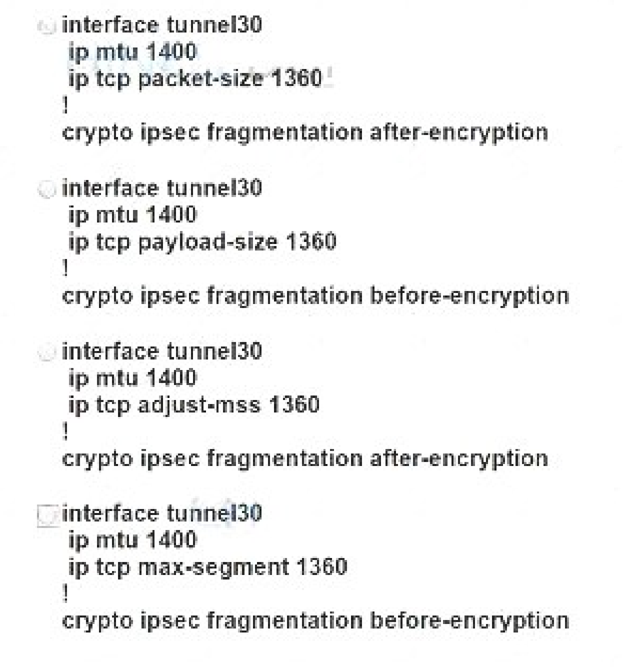
Answer: B

NEW QUESTION 207
- (Exam Topic 3)
How does an MPLS Layer 3 VPN differentiate the IP address space used between each VPN?

A. by RD
B. by address family
C. by MP-BGP
D. byRT

Answer: A

NEW QUESTION 208
- (Exam Topic 3)
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?

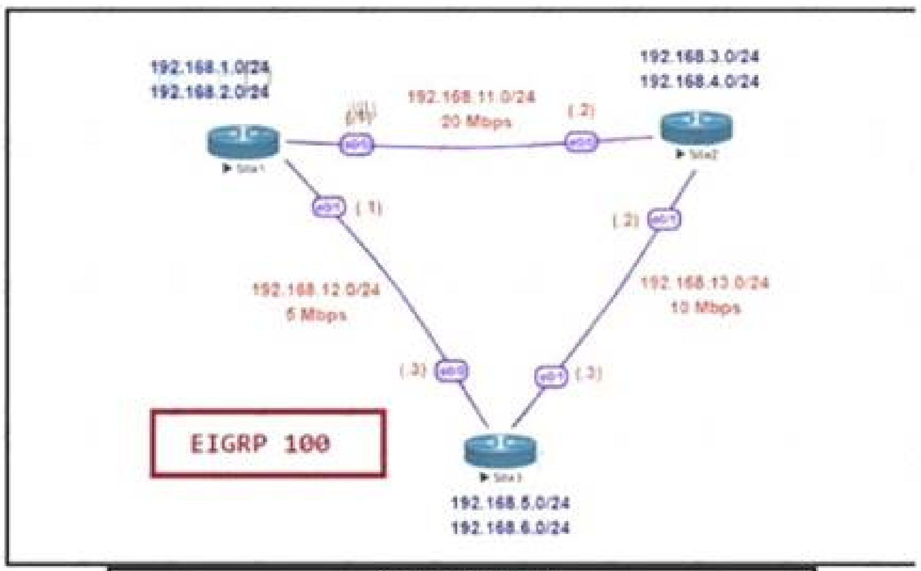


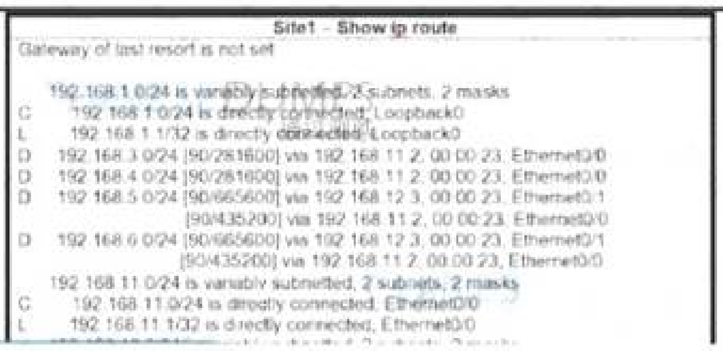
```
○ interface tunnel30
   ip mtu 1400
   ip tcp packet-size 1360
  !
  crypto ipsec fragmentation after-encryption

○ interface tunnel30
   ip mtu 1400
   ip tcp payload-size 1360
  !
  crypto ipsec fragmentation before-encryption

○ interface tunnel30
   ip mtu 1400
   ip tcp adjust-mss 1360
  !
  crypto ipsec fragmentation after-encryption

□ interface tunnel30
   ip mtu 1400
   ip tcp max-segment 1360
  !
  crypto ipsec fragmentation before-encryption
```

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

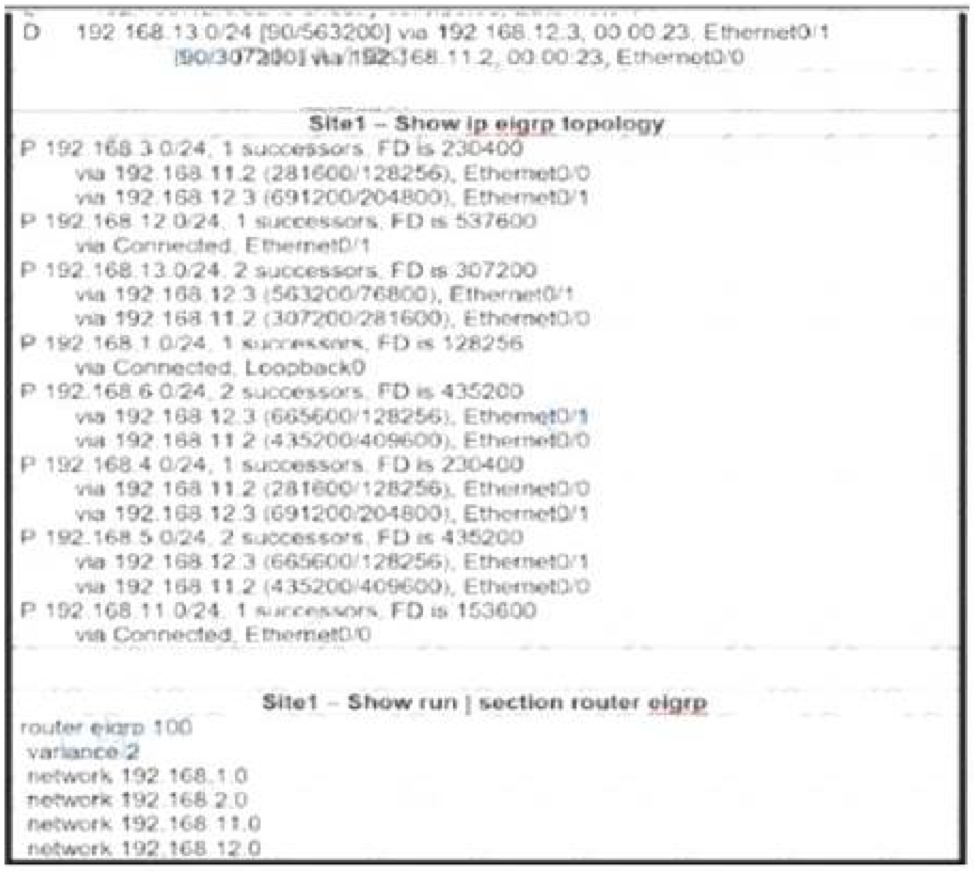
Answer: C

NEW QUESTION 213
- (Exam Topic 3)



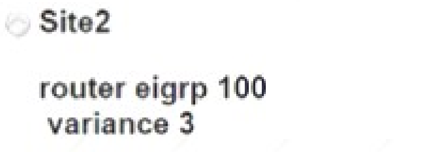


```
                        Site1 - Show ip route
Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback0
L       192.168.1.1/32 is directly connected, Loopback0
D     192.168.3.0/24 [90/281600] via 192.168.11.2, 00:00:23, Ethernet0/0
D     192.168.4.0/24 [90/281600] via 192.168.11.2, 00:00:23, Ethernet0/0
D     192.168.5.0/24 [90/665600] via 192.168.12.3, 00:00:23, Ethernet0/1
                     [90/435200] via 192.168.11.2, 00:00:23, Ethernet0/0
D     192.168.6.0/24 [90/665600] via 192.168.12.3, 00:00:23, Ethernet0/1
                     [90/435200] via 192.168.11.2, 00:00:23, Ethernet0/0
     192.168.11.0/24 is variably submitted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, Ethernet0/0
L       192.168.11.1/32 is directly connected, Ethernet0/0
```



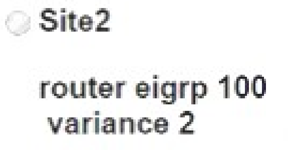
```
D     192.168.13.0/24 [90/563200] via 192.168.12.3, 00:00:23, Ethernet0/1
               [90/307200] via 192.168.11.2, 00:00:23, Ethernet0/0

                    Site1 – Show ip eigrp topology
P 192.168.3.0/24, 1 successors, FD is 230400
      via 192.168.11.2 (281600/128256), Ethernet0/0
      via 192.168.12.3 (691200/204800), Ethernet0/1
P 192.168.12.0/24, 1 successors, FD is 537600
      via Connected, Ethernet0/1
P 192.168.13.0/24, 2 successors, FD is 307200
      via 192.168.12.3 (563200/76800), Ethernet0/1
      via 192.168.11.2 (307200/281600), Ethernet0/0
P 192.168.1.0/24, 1 successors, FD is 128256
      via Connected, Loopback0
P 192.168.6.0/24, 2 successors, FD is 435200
      via 192.168.12.3 (665600/128256), Ethernet0/1
      via 192.168.11.2 (435200/409600), Ethernet0/0
P 192.168.4.0/24, 1 successors, FD is 230400
      via 192.168.11.2 (281600/128256), Ethernet0/0
      via 192.168.12.3 (691200/204800), Ethernet0/1
P 192.168.5.0/24, 2 successors, FD is 435200
      via 192.168.12.3 (665600/128256), Ethernet0/1
      via 192.168.11.2 (435200/409600), Ethernet0/0
P 192.168.11.0/24, 1 successors, FD is 153600
      via Connected, Ethernet0/0

               Site1 – Show run | section router eigrp
router eigrp 100
 variance 2
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.11.0
 network 192.168.12.0
```

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?



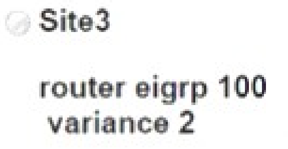
○ Site2

```
router eigrp 100
 variance 3
```



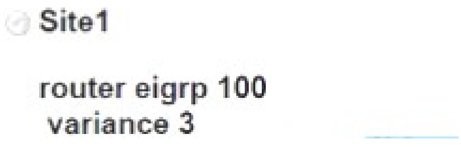
○ Site2

```
router eigrp 100
 variance 2
```



○ Site3

```
router eigrp 100
 variance 2
```



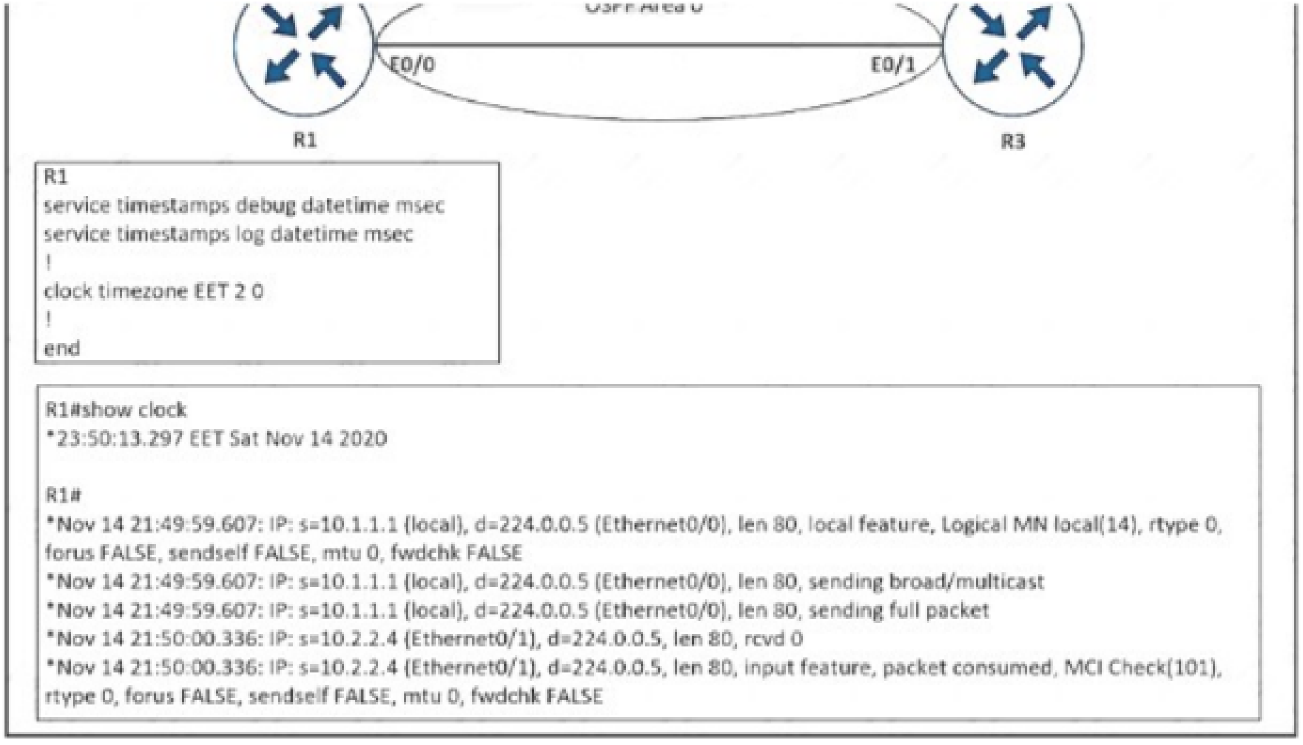
○ Site1

```
router eigrp 100
 variance 3
```

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

Answer: D

NEW QUESTION 215
- (Exam Topic 3)



```
R1
service timestamps debug datetime msec
service timestamps log datetime msec
!
clock timezone EET 2 0
!
end
```

```
R1#show clock
*23:50:13.297 EET Sat Nov 14 2020

R1#
*Nov 14 21:49:59.607: IP: s=10.1.1.1 (local), d=224.0.0.5 (Ethernet0/0), len 80, local feature, Logical MN local(14), rtype 0,
forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Nov 14 21:49:59.607: IP: s=10.1.1.1 (local), d=224.0.0.5 (Ethernet0/0), len 80, sending broad/multicast
*Nov 14 21:49:59.607: IP: s=10.1.1.1 (local), d=224.0.0.5 (Ethernet0/0), len 80, sending full packet
*Nov 14 21:50:00.336: IP: s=10.2.2.4 (Ethernet0/1), d=224.0.0.5, len 80, rcvd 0
*Nov 14 21:50:00.336: IP: s=10.2.2.4 (Ethernet0/1), d=224.0.0.5, len 80, input feature, packet consumed, MCI Check(101),
rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
```

Refer to the exhibit. An engineer cannot determine the time of the problem on R1 due to a mismatch between the router local clock and legs. Which command synchronizes the time between new log entries and the local clock on R1?

A. service timestamps debug datetime msec show.timezone
B. service timestamps log datetime locatetime msec
C. service timestamps datebug datetime localtime msec
D. service timestamps log datetime msec show-timezone

Answer: B

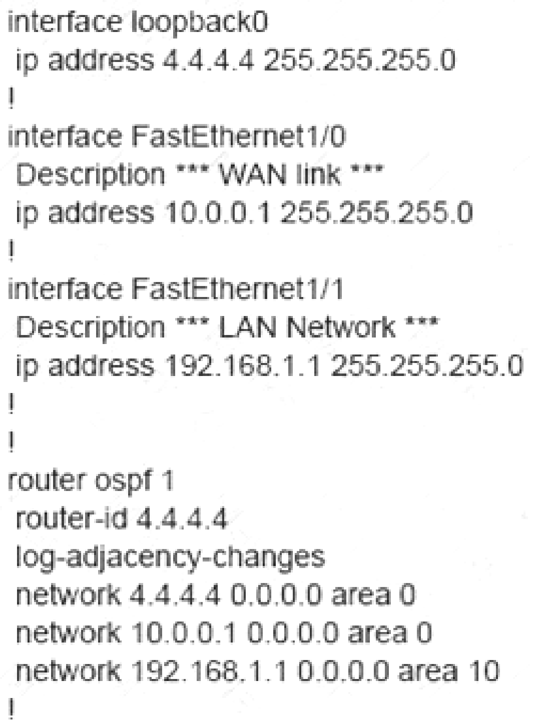
NEW QUESTION 216
- (Exam Topic 3)
Which feature minimizes DoS attacks on an IPv6 network?

A. IPv6 Binding Security Table
B. IPv6 Router Advertisement Guard
C. IPv6 Prefix Guard
D. IPv6 Destination Guard

Answer: D

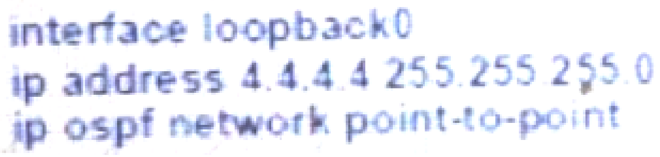
Explanation:
The Destination Guard feature helps in minimizing denial-of-service (DoS) attacks. It performs
address resolutions only for those addresses that are active on the link, and requires the FHS binding table to be populated with the help of the IPv6 snooping feature.The feature enables the filtering of IPv6 traffic based on the destination address, 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 unknown destination.
Reference: https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_1 5_0s_book/IPv6_Security.pdf

NEW QUESTION 219
- (Exam Topic 3)
Refer to the exhibit.



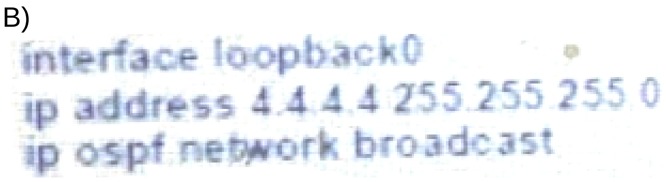
```
interface loopback0
 ip address 4.4.4.4 255.255.255.0
!
interface FastEthernet1/0
 Description *** WAN link ***
 ip address 10.0.0.1 255.255.255.0
!
interface FastEthernet1/1
 Description *** LAN Network ***
 ip address 192.168.1.1 255.255.255.0
!
!
router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes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



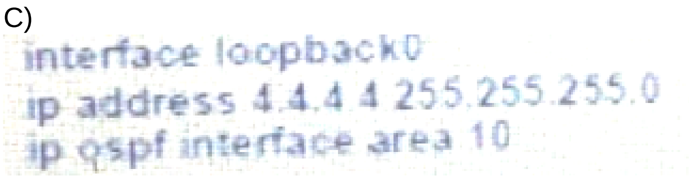
```
interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf network point-to-point
```

B)



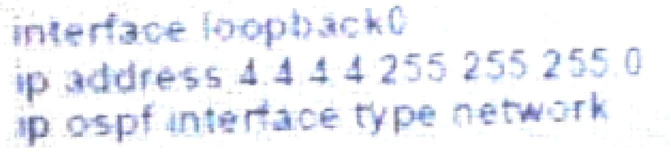
```
interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf network broadcast
```

C)



```
interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf interface area 10
```

D)

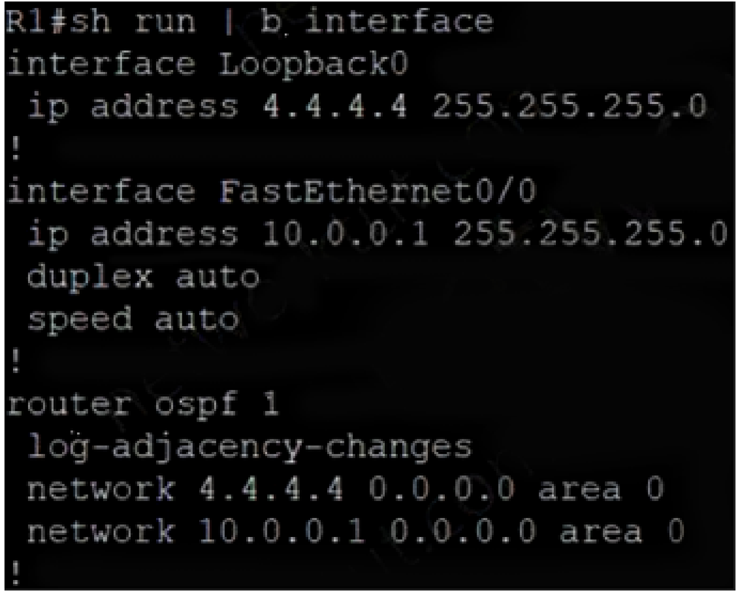


```
interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf interface type network
```

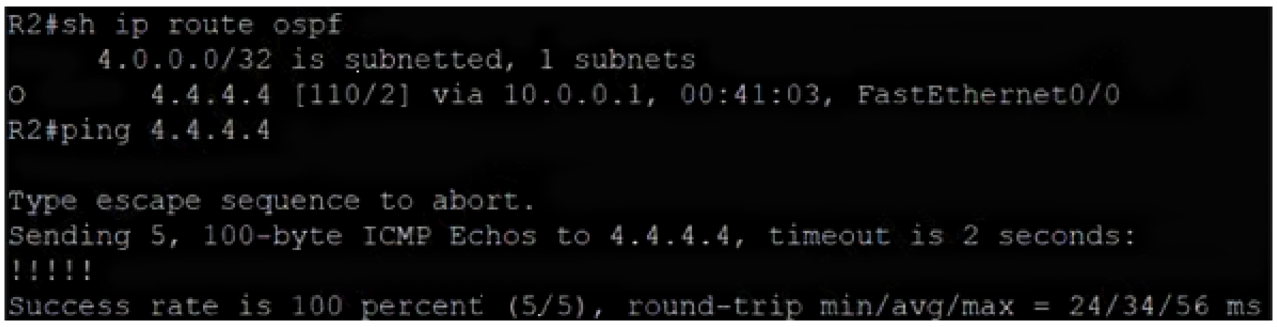
A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:
We tested this config in GNS3 (except the LAN interface) but R1 loopback0 was advertised normally on R2 and R2 could reach this loopback0.



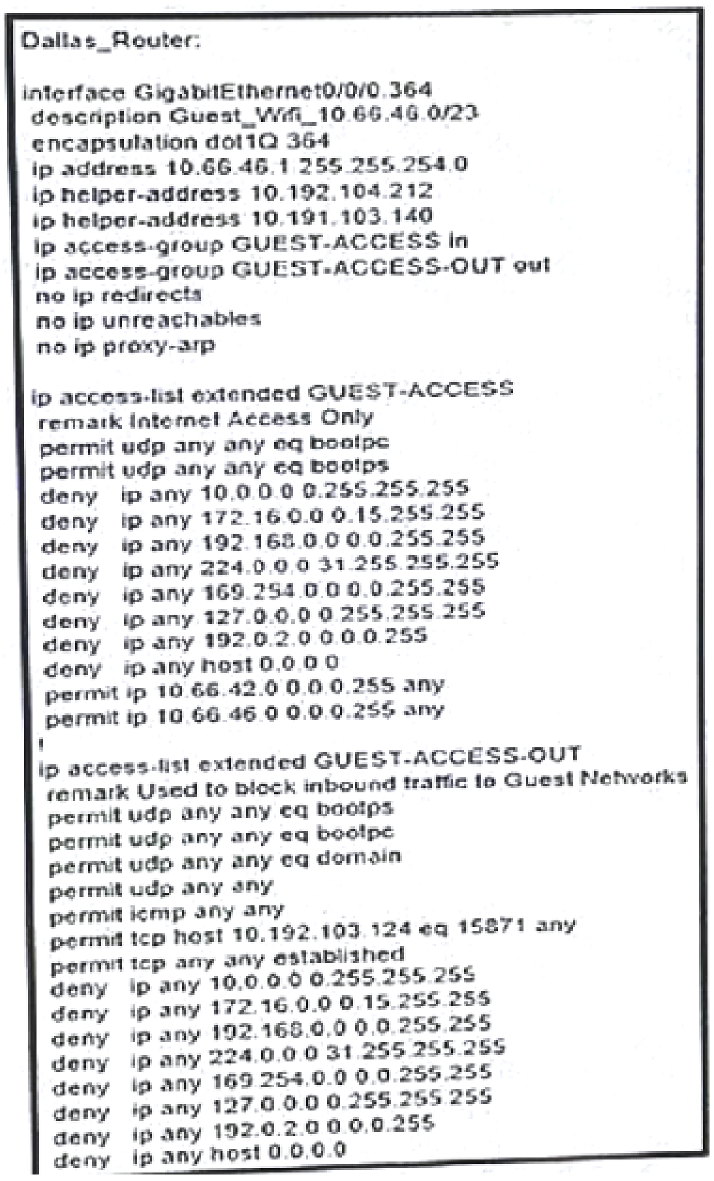
```
R1#sh run | b interface
interface Loopback0
 ip address 4.4.4.4 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 4.4.4.4 0.0.0.0 area 0
 network 10.0.0.1 0.0.0.0 area 0
!
```



```
R2#sh ip route ospf
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/2] via 10.0.0.1, 00:41:03, FastEthernet0/0
R2#ping 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/34/56 ms
```

Note: Although the configured loopback address is 4.4.4.4/24 but by default OSPF will advertise this route to loopback0 as 4.4.4.4/32 (most specific route to that loopback). In order to override this, we have to change the network type to point-to-point. After this OSPF will advertise the address to loopback as 4.4.4.0/24.

NEW QUESTION 223
- (Exam Topic 3)
Refer to the exhibit.



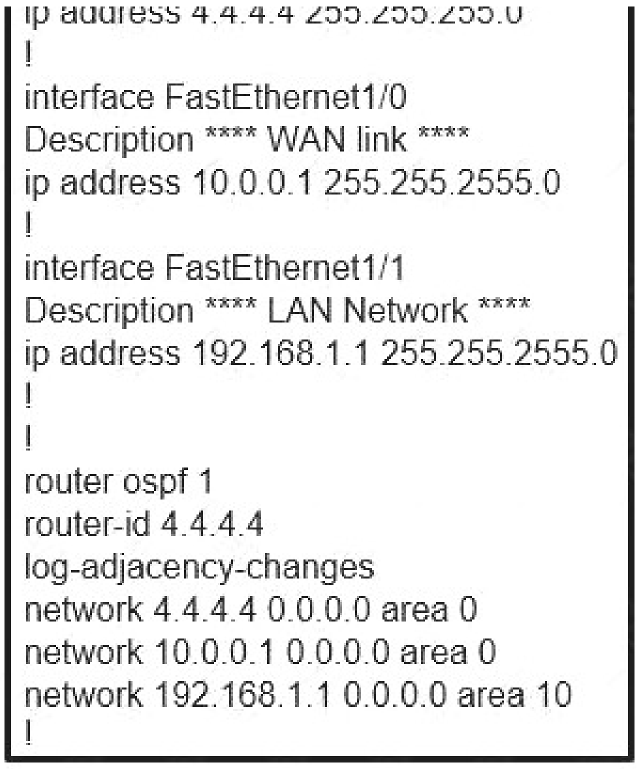
```
Dallas_Router:

interface GigabitEthernet0/0/0.364
 description Guest_Wifi_10.66.46.0/23
 encapsulation dot1Q 364
 ip address 10.66.46.1 255.255.254.0
 ip helper-address 10.192.104.212
 ip helper-address 10.191.103.140
 ip access-group GUEST-ACCESS in
 ip access-group GUEST-ACCESS-OUT out
 no ip redirects
 no ip unreachables
 no ip proxy-arp

ip access-list extended GUEST-ACCESS
 remark Internet Access Only
 permit udp any any eq bootpc
 permit udp any any eq bootps
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 224.0.0.0 31.255.255.255
 deny   ip any 169.254.0.0 0.0.255.255
 deny   ip any 127.0.0.0 0.255.255.255
 deny   ip any 192.0.2.0 0.0.0.255
 deny   ip any host 0.0.0.0
 permit ip 10.66.42.0 0.0.0.255 any
 permit ip 10.66.46.0 0.0.0.255 any
!
ip access-list extended GUEST-ACCESS-OUT
 remark Used to block inbound traffic to Guest Networks
 permit udp any any eq bootps
 permit udp any any eq bootpc
 permit udp any any eq domain
 permit udp any any
 permit icmp any any
 permit tcp host 10.192.103.124 eq 15871 any
 permit tcp any any established
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 224.0.0.0 31.255.255.255
 deny   ip any 169.254.0.0 0.0.255.255
 deny   ip any 127.0.0.0 0.255.255.255
 deny   ip any 192.0.2.0 0.0.0.255
 deny   ip any host 0.0.0.0
```

After a new regional office is set up,not all guests can access the internet via guest WiFi. Clients are getting the correct IP address from guest Wi-Fi VLAN 364. which action resolves the issue ?

A. Allow 10.66.46.0/23 in the outbound ACL
B. Allow DNS traffic through the outbound ACL
C. Allow DNS traffic through the inbound ACL
D. Allow 10.66.46.0/23 in the inbound ACL

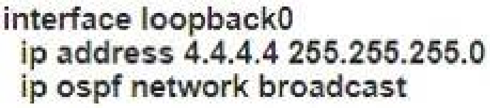
Answer: C

NEW QUESTION 225
- (Exam Topic 3)
Refer to the exhibit.



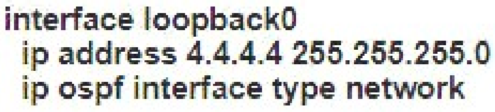
```
ip address 4.4.4.4 255.255.255.0
!
interface FastEthernet1/0
Description **** WAN link ****
ip address 10.0.0.1 255.255.2555.0
!
interface FastEthernet1/1
Description **** LAN Network ****
ip address 192.168.1.1 255.255.2555.0
!
!
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
network 4.4.4.4 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
!
```

A)



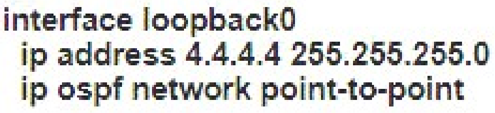
```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf network broadcast
```

B)



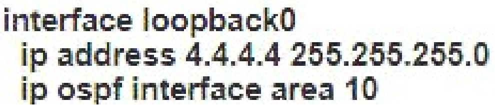
```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf interface type network
```

C)



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

D)

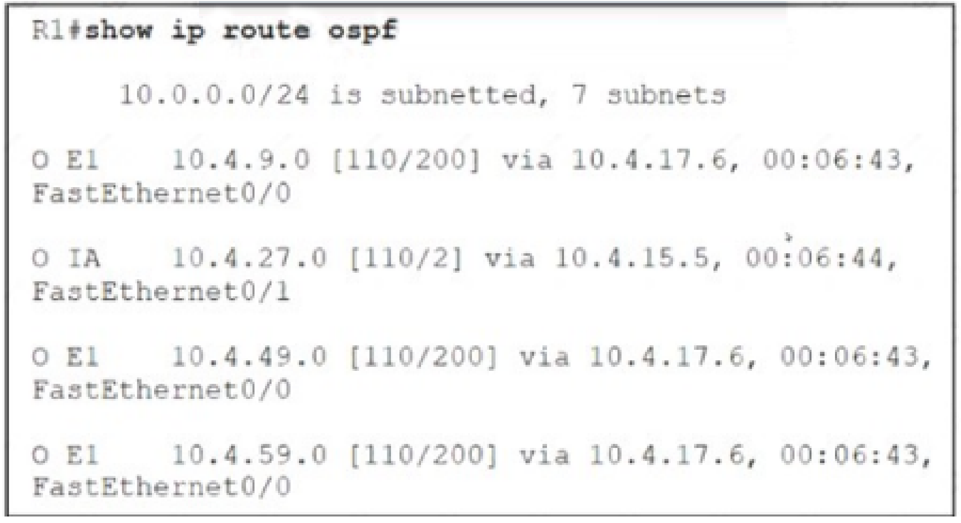


```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf interface area 10
```

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

Answer: A

NEW QUESTION 228
- (Exam Topic 3)



```
R1#show ip route ospf

     10.0.0.0/24 is subnetted, 7 subnets

O E1     10.4.9.0 [110/200] via 10.4.17.6, 00:06:43,
FastEthernet0/0

O IA     10.4.27.0 [110/2] via 10.4.15.5, 00:06:44,
FastEthernet0/1

O E1     10.4.49.0 [110/200] via 10.4.17.6, 00:06:43,
FastEthernet0/0

O E1     10.4.59.0 [110/200] via 10.4.17.6, 00:06:43,
FastEthernet0/0
```

Refer to the exhibit. An engineer configured two ASBRs, 10.4.17.6 and 10.4.15.5, in an OSPF network to redistribute identical routes from BGR However, only prefixes from 10.4.17.6 are installed into the routing table on R1. Which action must the engineer take to achieve load sharing for the BGP-originated prefixes?

A. The ASBRs are advertising the redistributed prefixes with the iBGP metric and must be modified to Type 1 on ASBR 10.4.17.6.
B. The ASBRs are advertising the redistributed prefixes with a different admin distance and must be changed to 110 on ASBR 10.4.15.5.
C. The admin distance of the prefixes must be adjusted to 20 on ASBR 10.4.15.5 to advertise prefixes to R1 identically from both ASBRs.
D. The ASBRs are advertising the redistributed prefixes as Type 1 and must be modified to Type 2

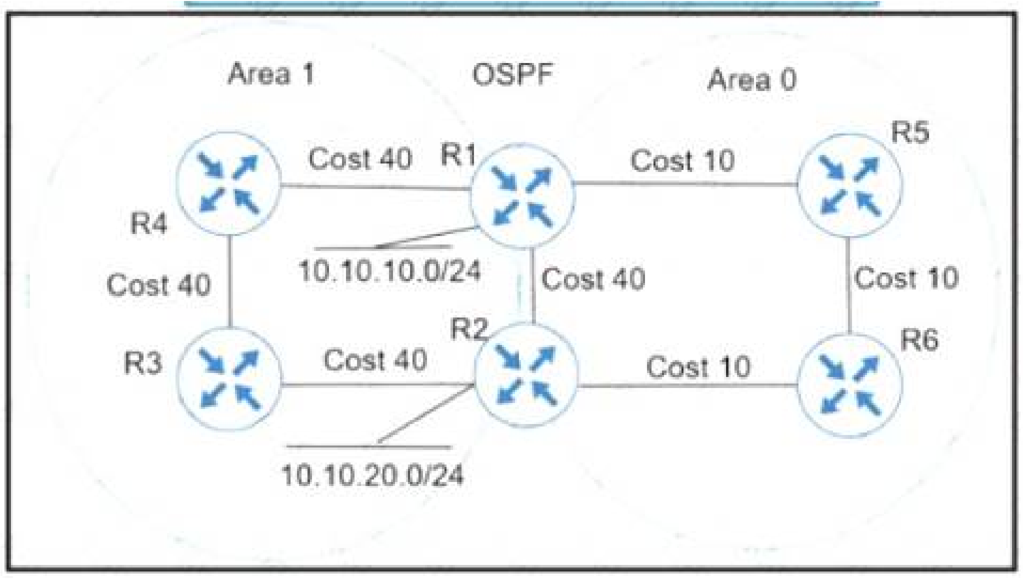
Answer: D

NEW QUESTION 231
- (Exam Topic 3)
What must a network architect consider for RTs when planning for a single customer full-mesh VPN m an MPLS Layer 3 network?

A. RT must be globally unique within the same VPN
B. RT must be globally identical within the same VPN
C. RT values must be Afferent from the RD values in the same VPN
D. Each RT value must be identical to an RD value within the same VPN.

Answer: D

NEW QUESTION 233
- (Exam Topic 3)

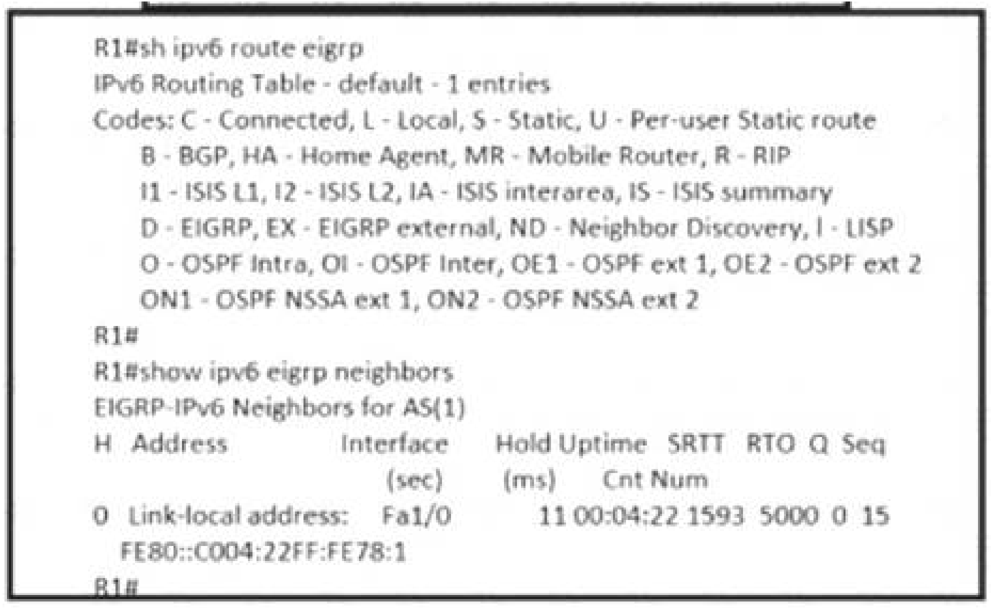


Refer to the exhibit Which action ensures that 10 10 10 0/24 reaches 10 10 20 0/24 through the direct link between R1 and R2?

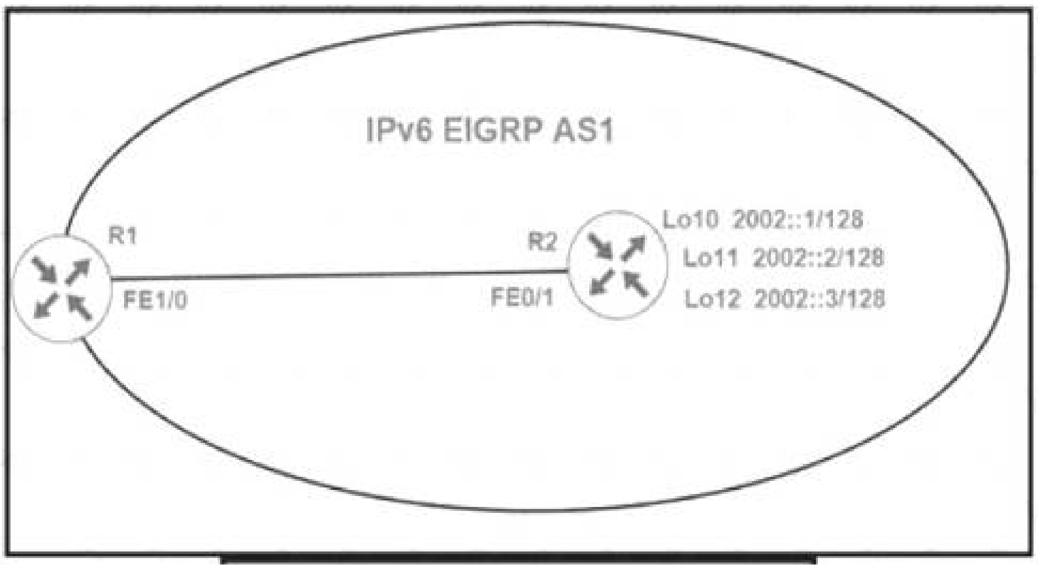
A. Configure R1 and R2 LAN links as nonpassive.
B. Configure R1 and R2 links under area 1
C. Configure OSPF link cost to 1 between R1 and R2
D. Configure OSPF path cost to 3 between R1 and R2

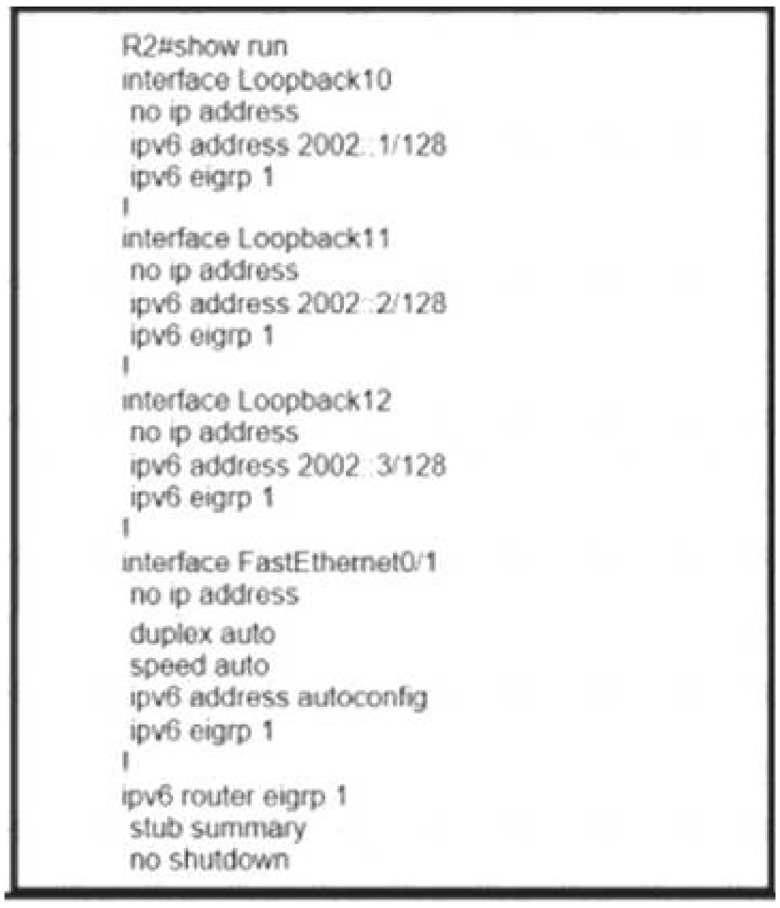
Answer: B

NEW QUESTION 237
- (Exam Topic 3)



```
R1#sh ipv6 route eigrp
IPv6 Routing Table - default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
    B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
    I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
    D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery, l - LISP
    O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
    ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R1#
R1#show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(1)
H  Address              Interface       Hold Uptime   SRTT   RTO  Q  Seq
                              (sec)           (ms)        Cnt Num
0  Link-local address:    Fa1/0            11 00:04:22 1593  5000  0  15
   FE80::C004:22FF:FE78:1
R1#
```





```
R2#show run
interface Loopback10
 no ip address
 ipv6 address 2002::1/128
 ipv6 eigrp 1
!
interface Loopback11
 no ip address
 ipv6 address 2002::2/128
 ipv6 eigrp 1
!
interface Loopback12
 no ip address
 ipv6 address 2002::3/128
 ipv6 eigrp 1
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address autoconfig
 ipv6 eigrp 1
!
ipv6 router eigrp 1
 stub summary
 no shutdown
```

R1 cannot receive the R2 Interfaces with individual prefixes. What must be reconfigured to advertise R2 Interfaces to R1?

A. EIGRP process on R2 by removing the stub command Keyword summary
B. interface FastEthernet0/1 on R2 with an EIGRP summary for all three loopback prefixes
C. EIGRP process on R2 with the command stub summary receive-only
D. ElGRP process on R2 with the command stub summary connected

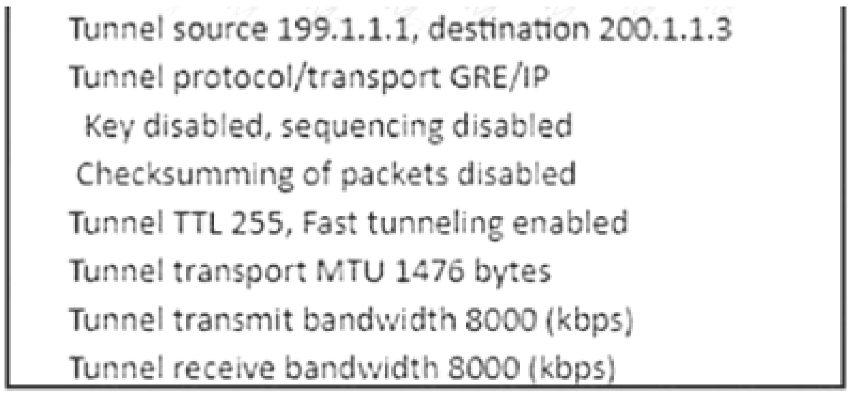
Answer: D

NEW QUESTION 242
- (Exam Topic 3)
Which control plane process allows the MPLS forwarding state to recover when a secondary RP takes over from a failed primary RP?

A. MP-BGP uses control plane services for label prefix bindings in the MPLS forwarding table
B. LSP uses NSF to recover from disruption *i control plane service
C. FEC uses a control plane service to distribute information between primary and secondary processors
D. LDP uses SSO to recover from disruption in control plane service

Answer: C

NEW QUESTION 243
- (Exam Topic 3)
Refer to the exhibit.



```
Tunnel source 199.1.1.1, destination 200.1.1.3
Tunnel protocol/transport GRE/IP
 Key disabled, sequencing disabled
 Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
```

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 Tunnel1 tunnel source 199.1.1.1tunnel destination 200.1.1.3ip address 192.168.1.3 255.255.255.0
B. Interface Tunnel1 tunnel source 200.1.1.3tunnel destination 199.1.1.1ip address 192.168.1.1.255.255.255.0
C. Interface Tunnel1 tunnel source 200.1.1.3tunnel destination 199.1.1.1ip address 192.168.1.3.255.255.255.0
D. Interface Tunnel lunnel source 199.1.1.1tunnel destination 200.1.1.3ip address 192.168.1.1.255.255.255.0

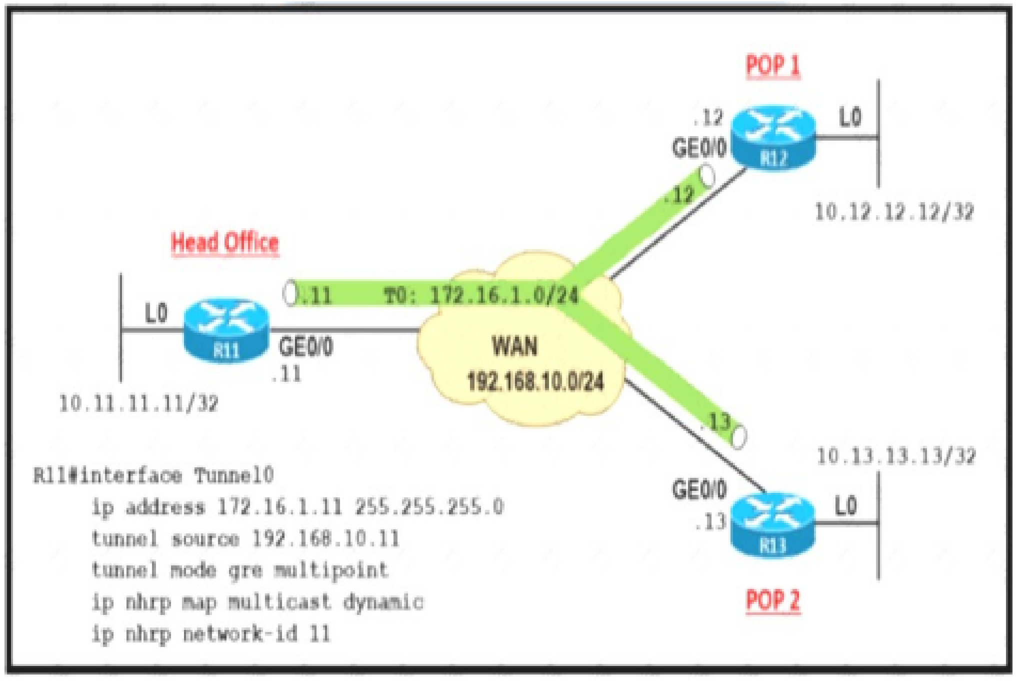
Answer: C

NEW QUESTION 246
- (Exam Topic 3)
Which method provides failure detection in BFD?

A. short duration, high overhead
B. short duration, low overhead
C. long duration, high overhead
D. long duration, low overhead

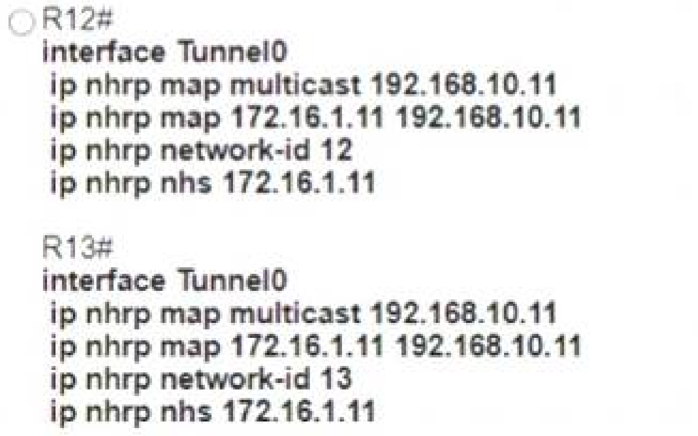
Answer: B

NEW QUESTION 247
- (Exam Topic 3)



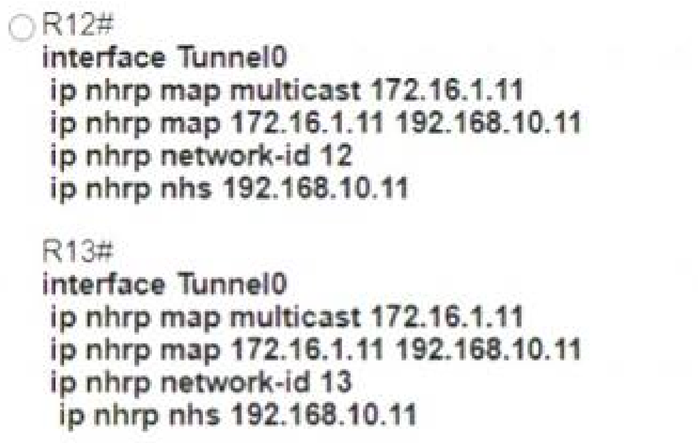
```
R11#interface Tunnel0
    ip address 172.16.1.11 255.255.255.0
    tunnel source 192.168.10.11
    tunnel mode gre multipoint
    ip nhrp map multicast dynamic
    ip nhrp network-id 11
```

Refer to the exhibit A company builds WAN infrastructure between the head office and POPs using DMVPN hub-and-spoke topology to provide end-to-end communication All POPs must maintain point-to-point connectivity with the head office Which configuration meets the requirement at routers R12 and R13?



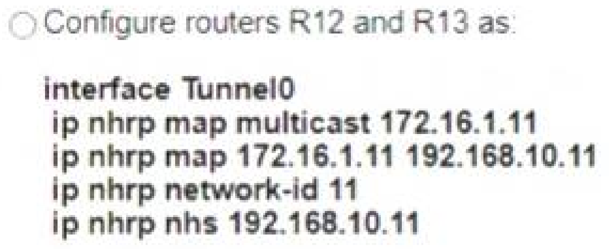
○ R12#
```
interface Tunnel0
 ip nhrp map multicast 192.168.10.11
 ip nhrp map 172.16.1.11 192.168.10.11
 ip nhrp network-id 12
 ip nhrp nhs 172.16.1.11
```

R13#
```
interface Tunnel0
 ip nhrp map multicast 192.168.10.11
 ip nhrp map 172.16.1.11 192.168.10.11
 ip nhrp network-id 13
 ip nhrp nhs 172.16.1.11
```



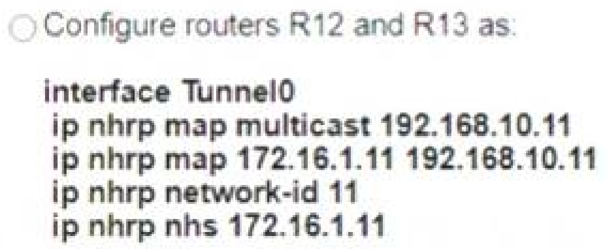
○ R12#
```
interface Tunnel0
 ip nhrp map multicast 172.16.1.11
 ip nhrp map 172.16.1.11 192.168.10.11
 ip nhrp network-id 12
 ip nhrp nhs 192.168.10.11
```

R13#
```
interface Tunnel0
 ip nhrp map multicast 172.16.1.11
 ip nhrp map 172.16.1.11 192.168.10.11
 ip nhrp network-id 13
  ip nhrp nhs 192.168.10.11
```



○ Configure routers R12 and R13 as:

```
interface Tunnel0
 ip nhrp map multicast 172.16.1.11
 ip nhrp map 172.16.1.11 192.168.10.11
 ip nhrp network-id 11
 ip nhrp nhs 192.168.10.11
```



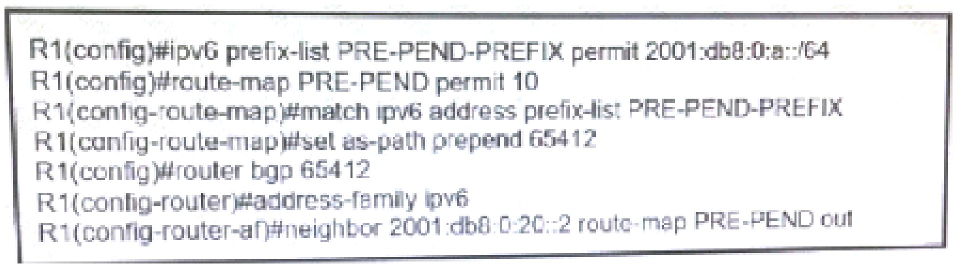
○ Configure routers R12 and R13 as:

```
interface Tunnel0
 ip nhrp map multicast 192.168.10.11
 ip nhrp map 172.16.1.11 192.168.10.11
 ip nhrp network-id 11
 ip nhrp nhs 172.16.1.11
```

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

Answer: D

NEW QUESTION 249
- (Exam Topic 3)
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 neighbor requires a soft reconfiguration, and this will clear the policy without resetting the BGP TCP connection.
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 route map requires a deny 20 statement without set conditions, and this will allow additional prefixes to be advertised.
D. The route map requires a permit 20 statement without set conditions, and this will allow additional prefixes to be advertised.

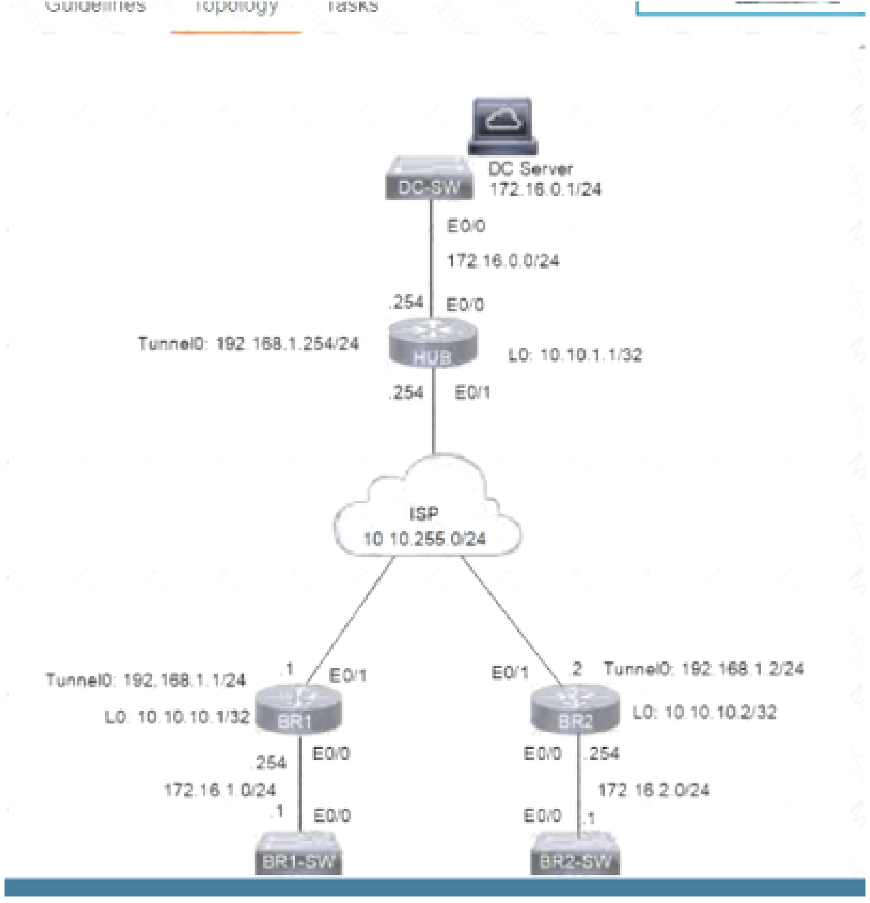
Answer: D

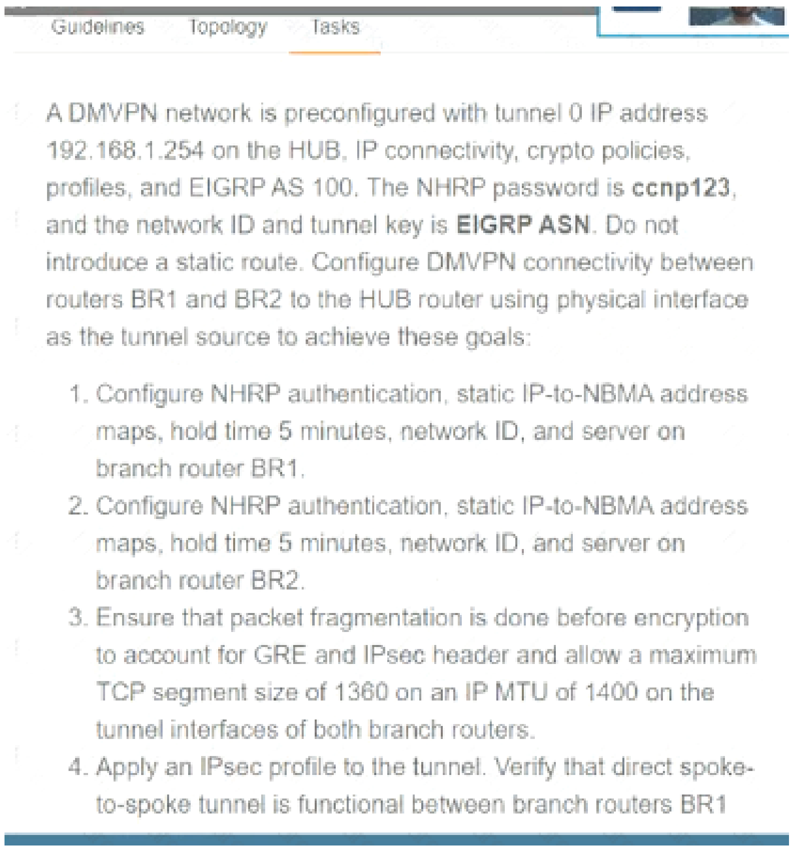
NEW QUESTION 254
- (Exam Topic 3)
What is an advantage of implementing BFD?

A. BFD provides faster updates for any flapping route.
B. BFD provides millisecond failure detection
C. BFD is deployed without the need to run any routing protocol
D. BFD provides better capabilities to maintain the routing table

Answer: B

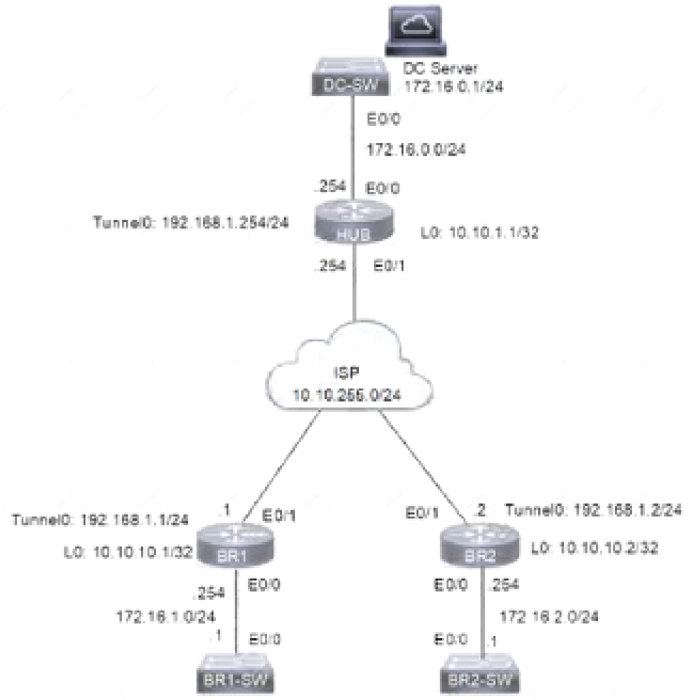
NEW QUESTION 259
- (Exam Topic 3)
A DMVPN network is preconfigured with tunnel 0 IP address 192.168.1.254 on the HUB, IP connectivity, crypto policies, profiles, and EIGRP AS 100. The NHRP password is ccnp123, and the network ID and tunnel key is EIGRP ASN Do not introduce a static route. Configure DMVPN connectivity between routers BR1 and BR2 to the HUB router using physical interface as the tunnel source to achieve these goals:



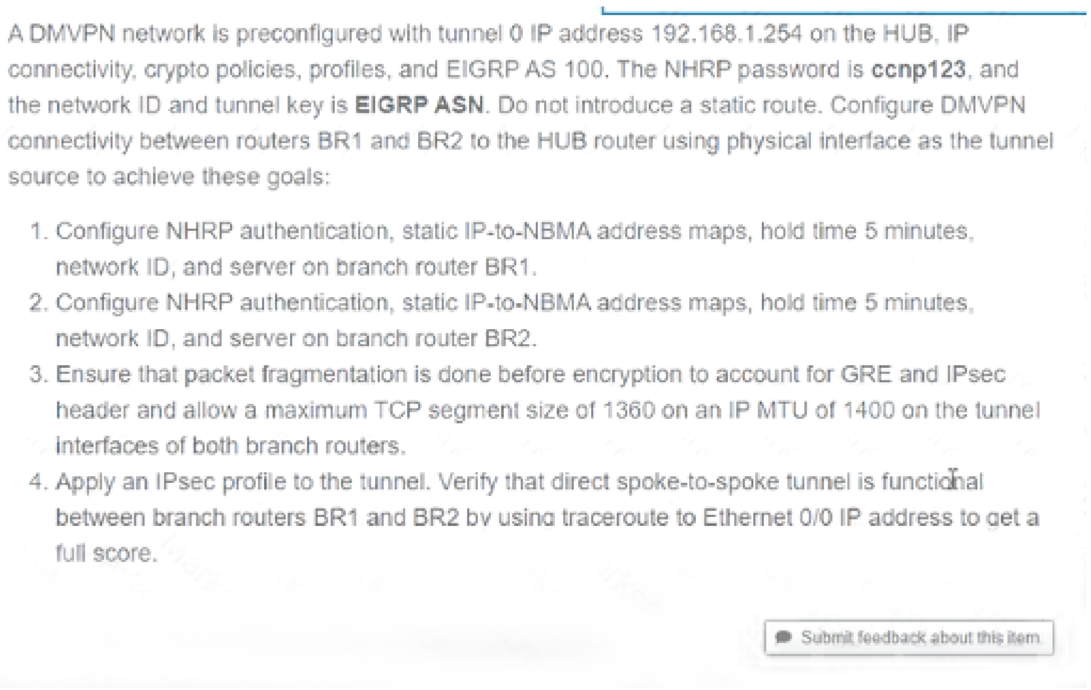


A DMVPN network is preconfigured with tunnel 0 IP address 192.168.1.254 on the HUB, IP connectivity, crypto policies, profiles, and EIGRP AS 100. The NHRP password is **ccnp123**, and the network ID and tunnel key is **EIGRP ASN**. Do not introduce a static route. Configure DMVPN connectivity between routers BR1 and BR2 to the HUB router using physical interface as the tunnel source to achieve these goals:

1. Configure NHRP authentication, static IP-to-NBMA address maps, hold time 5 minutes, network ID, and server on branch router BR1.
2. Configure NHRP authentication, static IP-to-NBMA address maps, hold time 5 minutes, network ID, and server on branch router BR2.
3. Ensure that packet fragmentation is done before encryption to account for GRE and IPsec header and allow a maximum TCP segment size of 1360 on an IP MTU of 1400 on the tunnel interfaces of both branch routers.
4. Apply an IPsec profile to the tunnel. Verify that direct spoke-to-spoke tunnel is functional between branch routers BR1



Topology Diagram



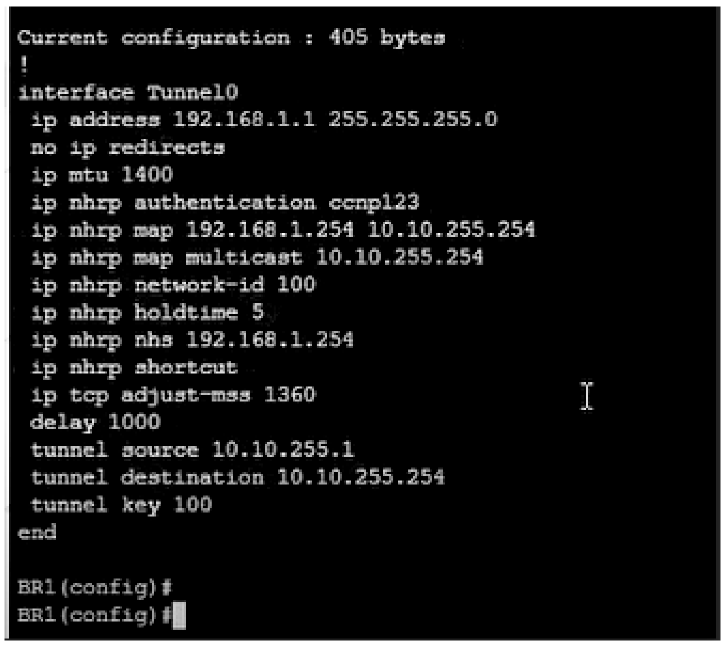
A DMVPN network is preconfigured with tunnel 0 IP address 192.168.1.254 on the HUB, IP connectivity, crypto policies, profiles, and EIGRP AS 100. The NHRP password is **ccnp123**, and the network ID and tunnel key is **EIGRP ASN**. Do not introduce a static route. Configure DMVPN connectivity between routers BR1 and BR2 to the HUB router using physical interface as the tunnel source to achieve these goals:

1. Configure NHRP authentication, static IP-to-NBMA address maps, hold time 5 minutes, network ID, and server on branch router BR1.
2. Configure NHRP authentication, static IP-to-NBMA address maps, hold time 5 minutes, network ID, and server on branch router BR2.
3. Ensure that packet fragmentation is done before encryption to account for GRE and IPsec header and allow a maximum TCP segment size of 1360 on an IP MTU of 1400 on the tunnel interfaces of both branch routers.
4. Apply an IPsec profile to the tunnel. Verify that direct spoke-to-spoke tunnel is functional between branch routers BR1 and BR2 bv usina traceroute to Ethernet 0/0 IP address to aet a full score.

A. Mastered
B. Not Mastered

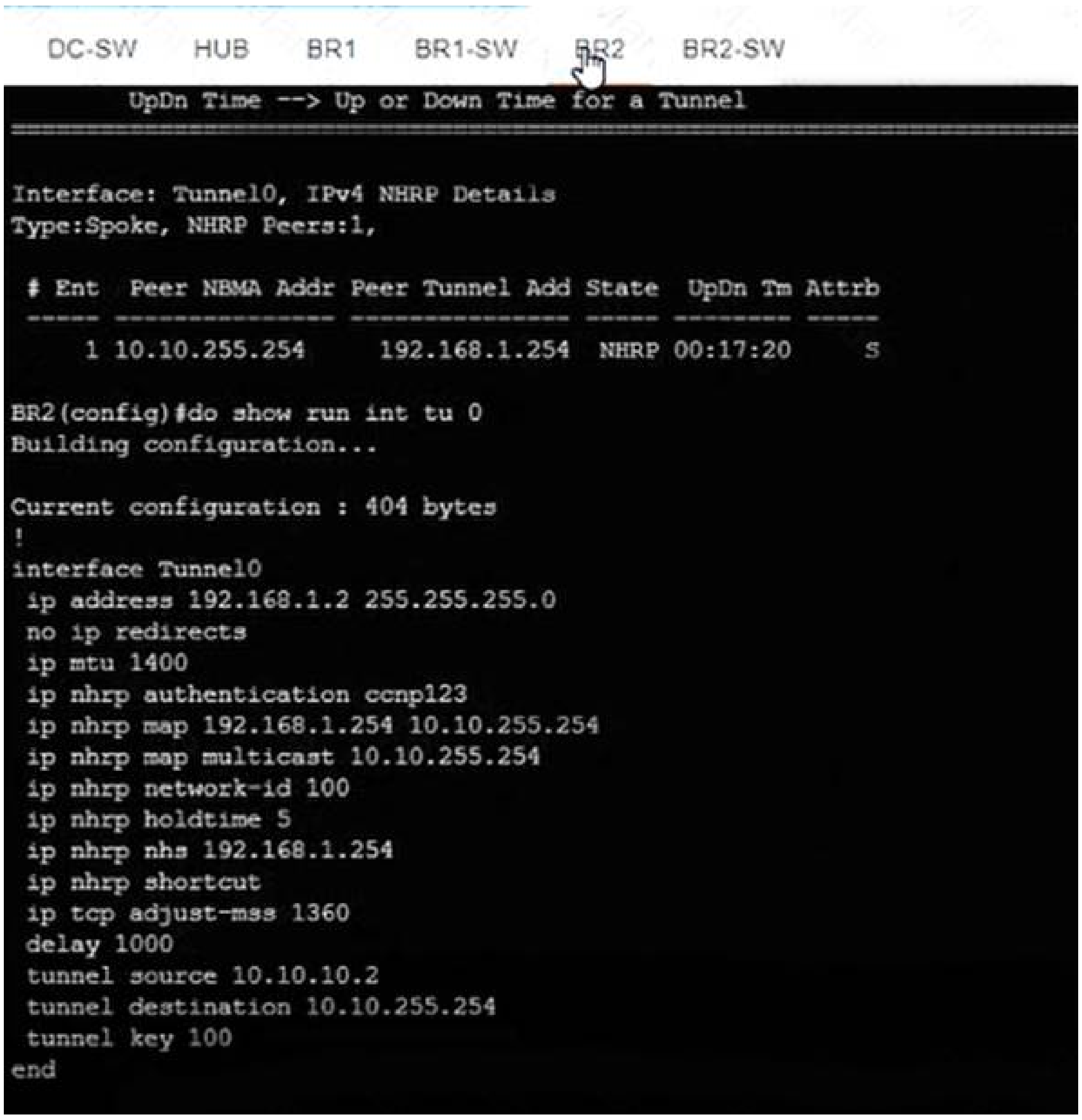
Answer: A

Explanation:
ON BR1



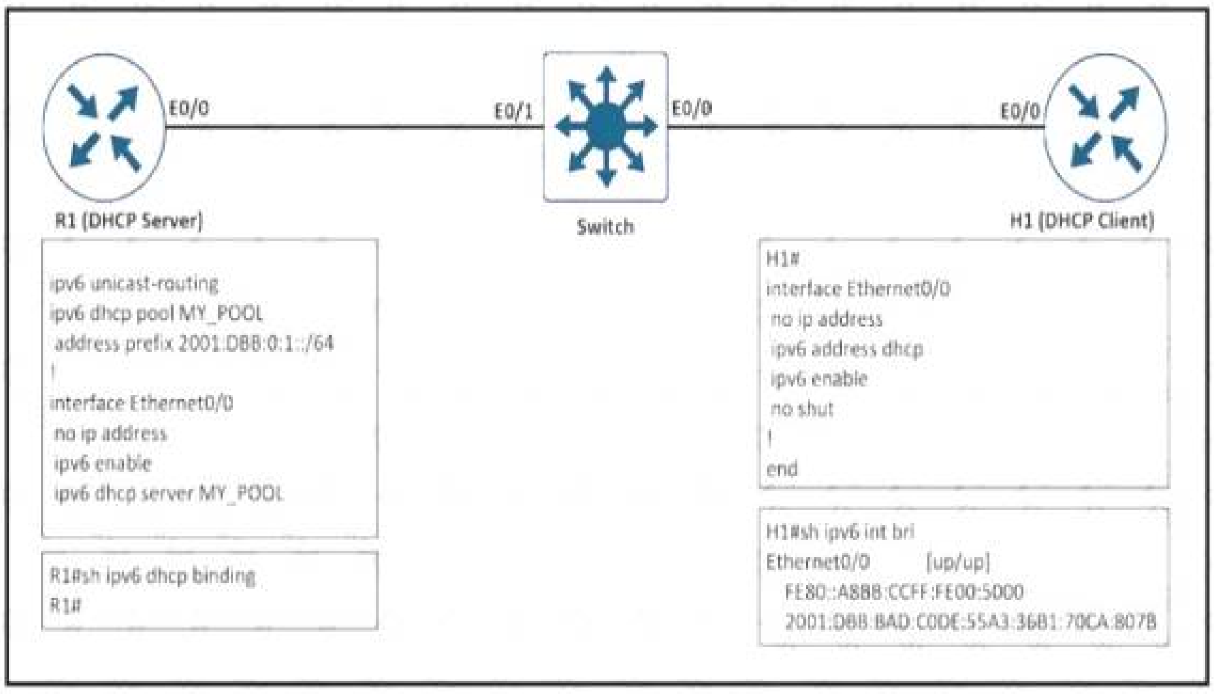
```
Current configuration : 405 bytes
!
interface Tunnel0
 ip address 192.168.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication ccnp123
 ip nhrp map 192.168.1.254 10.10.255.254
 ip nhrp map multicast 10.10.255.254
 ip nhrp network-id 100
 ip nhrp holdtime 5
 ip nhrp nhs 192.168.1.254
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source 10.10.255.1
 tunnel destination 10.10.255.254
 tunnel key 100
end

BR1(config)#
BR1(config)#
```

ON BR2



```
      UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 10.10.255.254     192.168.1.254  NHRP 00:17:20     S

BR2(config)#do show run int tu 0
Building configuration...

Current configuration : 404 bytes
!
interface Tunnel0
 ip address 192.168.1.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication ccnp123
 ip nhrp map 192.168.1.254 10.10.255.254
 ip nhrp map multicast 10.10.255.254
 ip nhrp network-id 100
 ip nhrp holdtime 5
 ip nhrp nhs 192.168.1.254
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source 10.10.10.2
 tunnel destination 10.10.255.254
 tunnel key 100
end
```

NEW QUESTION 262
- (Exam Topic 3)



```
ipv6 unicast-routing
ipv6 dhcp pool MY_POOL
 address prefix 2001:DB8:0:1::/64
!
interface Ethernet0/0
 no ip address
 ipv6 enable
 ipv6 dhcp server MY_POOL
```

```
R1#sh ipv6 dhcp binding
R1#
```

```
H1#
interface Ethernet0/0
 no ip address
 ipv6 address dhcp
 ipv6 enable
 no shut
!
end
```

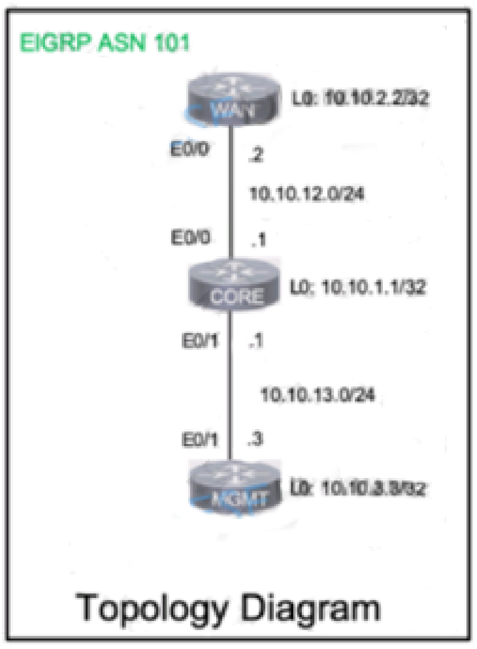
```
H1#sh ipv6 int bri
Ethernet0/0          [up/up]
   FE80::A8BB:CCFF:FE00:5000
   2001:DBB:BAD:C0DE:55A3:36B1:70CA:807B
```

Refer to the exhibit. The client server but the show command does not show the IPv6 DHCP bindings on the server. Which action resolves the issue?

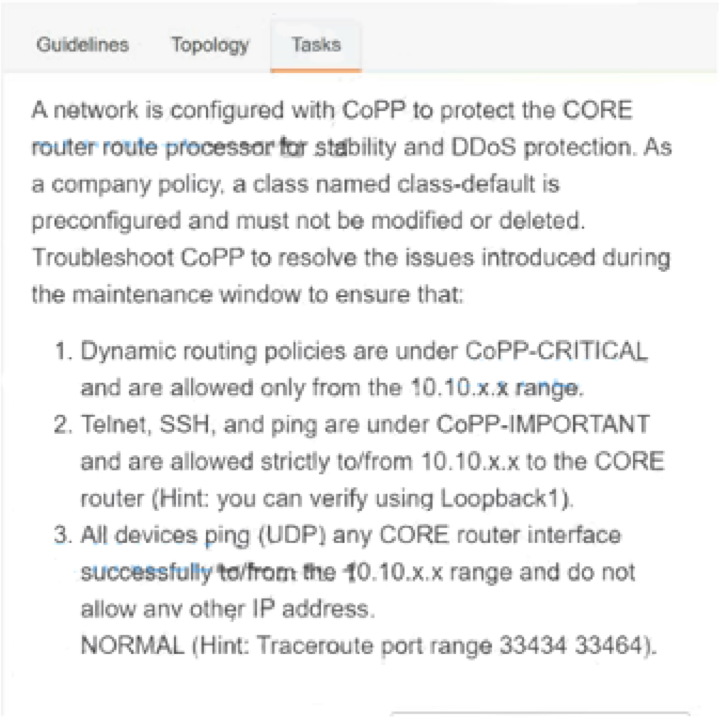
A. Extend the DHCP lease time because R1 removed the IPv6 address earlier after the lease expired.
B. Configure H1 as the DHCP client that manually assigns the IPv6 address on interlace e0/0..
C. Use the 2001:DBB:BAD:C0DE::/64 prefix for the DHCP pool on R1.
D. Configure authorized DHCP servers to avoid IPv6 addresses from a rogue DHCP server.

Answer: C

NEW QUESTION 265
- (Exam Topic 3)
A network is configured with CoPP to protect the CORE router route processor for stability and DDoS protection. As a company policy, a class named class-default is preconfigured and must not be modified or deleted. Troubleshoot CoPP to resolve the issues introduced during the maintenance window to ensure that:



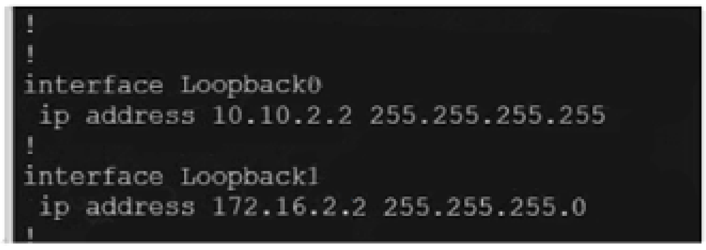
Topology Diagram



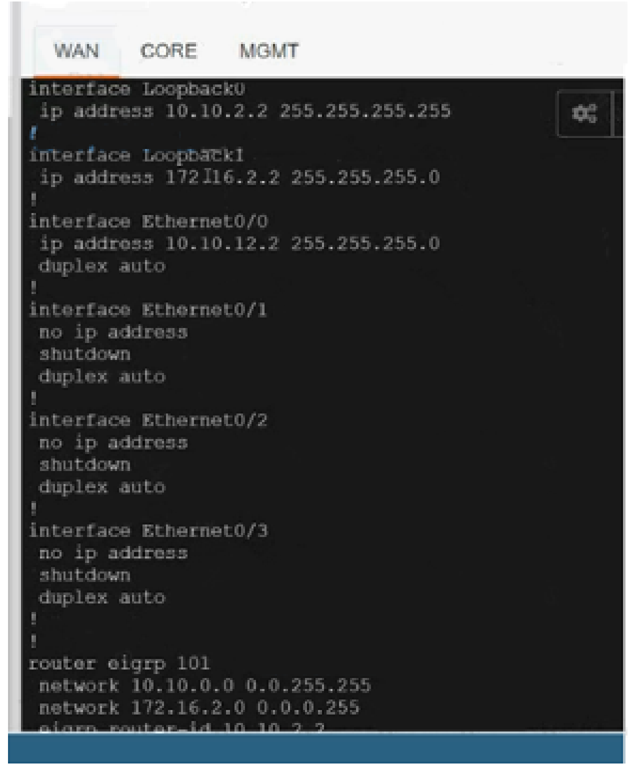
A network is configured with CoPP to protect the CORE router route processor for stability and DDoS protection. As a company policy, a class named class-default is preconfigured and must not be modified or deleted. Troubleshoot CoPP to resolve the issues introduced during the maintenance window to ensure that:

1. Dynamic routing policies are under CoPP-CRITICAL and are allowed only from the 10.10.x.x range.
2. Telnet, SSH, and ping are under CoPP-IMPORTANT and are allowed strictly to/from 10.10.x.x to the CORE router (Hint: you can verify using Loopback1).
3. All devices ping (UDP) any CORE router interface successfully to/from the 10.10.x.x range and do not allow anv other IP address.
NORMAL (Hint: Traceroute port range 33434 33464).

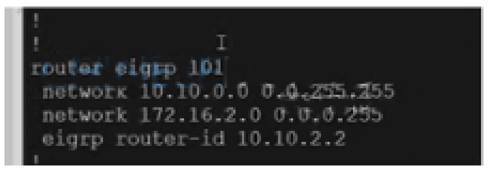
WAN



```
!
!
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
 ip address 172.16.2.2 255.255.255.0
```

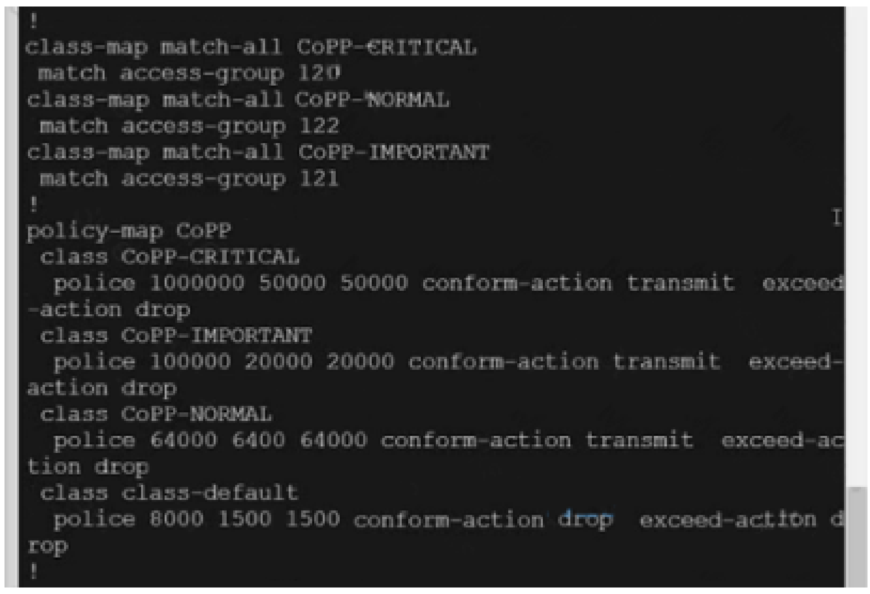


```
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
 ip address 172.16.2.2 255.255.255.0
!
interface Ethernet0/0
 ip address 10.10.12.2 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 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
```

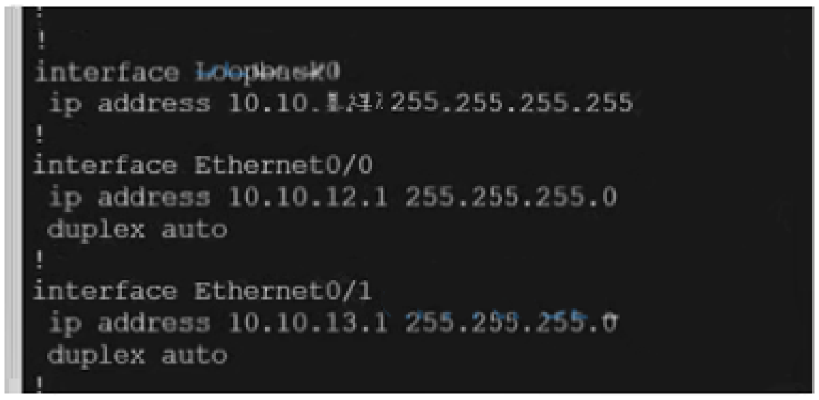


```
!
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 network 172.16.2.0 0.0.0.255
 eigrp router-id 10.10.2.2
!
```

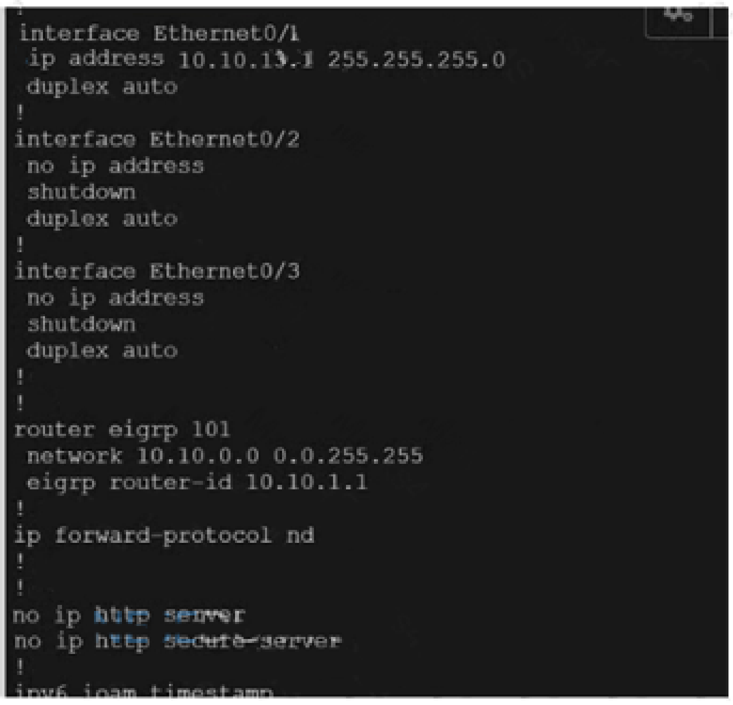
CORE



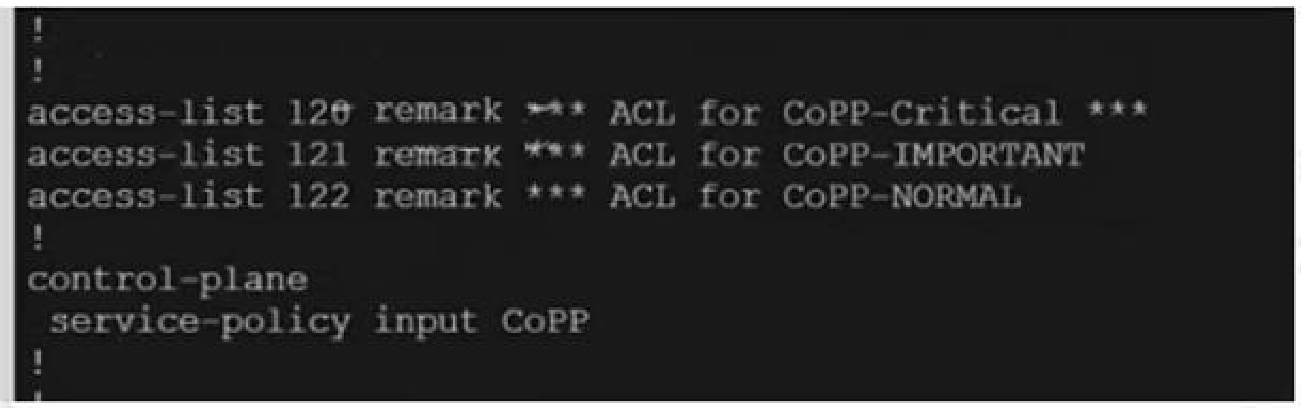
```
!
class-map match-all CoPP-CRITICAL
 match access-group 120
class-map match-all CoPP-NORMAL
 match access-group 122
class-map match-all CoPP-IMPORTANT
 match access-group 121
!
policy-map CoPP
 class CoPP-CRITICAL
  police 1000000 50000 50000 conform-action transmit  exceed
-action drop
 class CoPP-IMPORTANT
  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 Loopback0
 ip address 10.10.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.10.12.1 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 10.10.13.1 255.255.255.0
 duplex auto
!
```

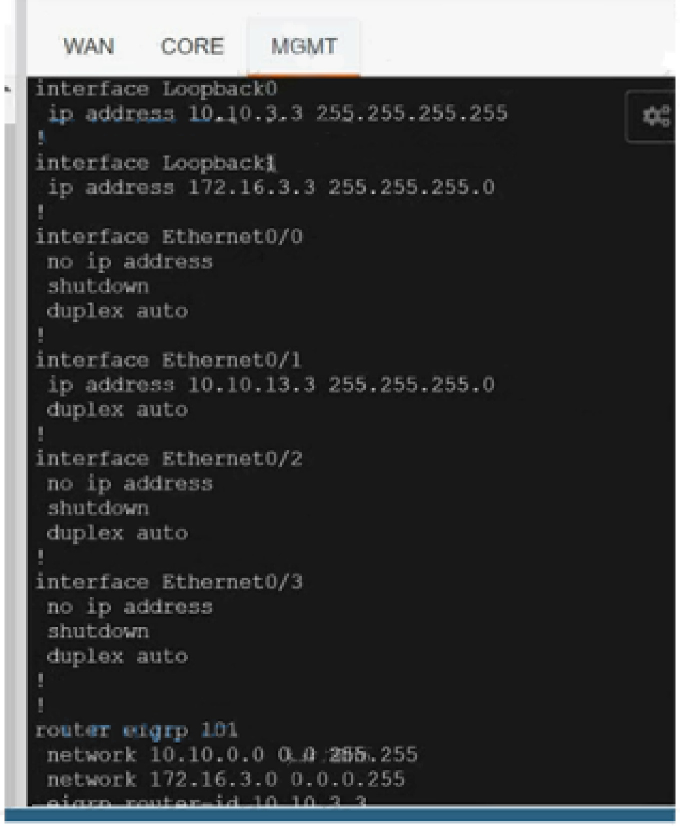


```
interface Ethernet0/1
 ip address 10.10.13.1 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 eigrp router-id 10.10.1.1
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
```

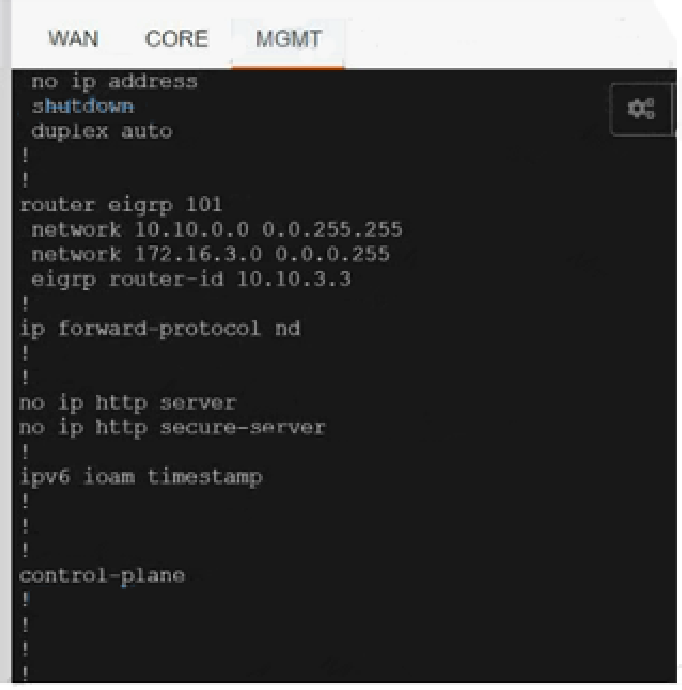


```
!
!
access-list 120 remark *** ACL for CoPP-Critical ***
access-list 121 remark *** ACL for CoPP-IMPORTANT
access-list 122 remark *** ACL for CoPP-NORMAL
!
control-plane
 service-policy input CoPP
!
!
```

MGMT



```
interface Loopback0
 ip address 10.10.3.3 255.255.255.255
!
interface Loopback1
 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
```

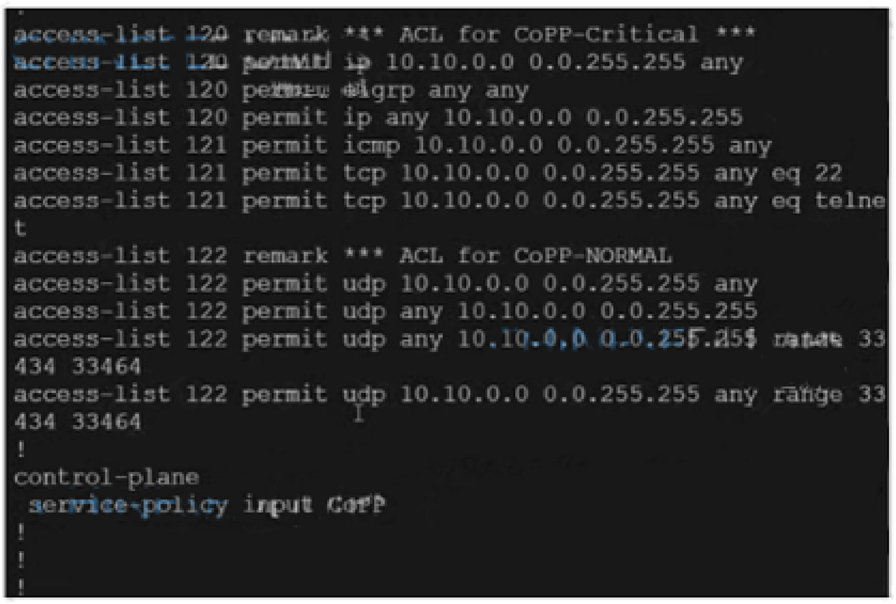


```
 no ip address
 shutdown
 duplex auto
!
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 network 172.16.3.0 0.0.0.255
 eigrp router-id 10.10.3.3
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!
!
!
```

A. Mastered
B. Not Mastered

Answer: A

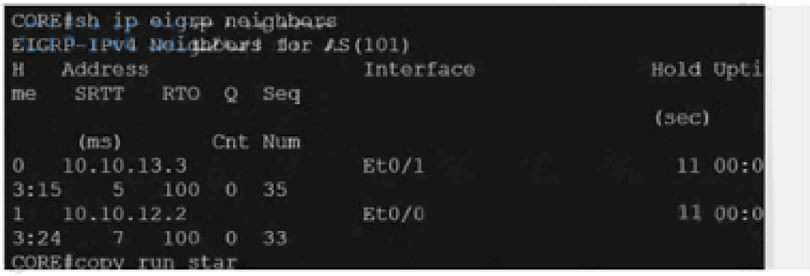
Explanation:
CORE
policy-mao CoPP
class CoPP-CRITICAL
police 1000000 50000 50000 conform-action transmit exceed-action transmit
Text Description automatically generated with medium confidence



```
access-list 120 remark *** ACL for CoPP-Critical ***
access-list 120 permit ip 10.10.0.0 0.0.255.255 any
access-list 120 permit eigrp any any
access-list 120 permit ip any 10.10.0.0 0.0.255.255
access-list 121 permit icmp 10.10.0.0 0.0.255.255 any
access-list 121 permit tcp 10.10.0.0 0.0.255.255 any eq 22
access-list 121 permit tcp 10.10.0.0 0.0.255.255 any eq telne
t
access-list 122 remark *** ACL for CoPP-NORMAL
access-list 122 permit udp 10.10.0.0 0.0.255.255 any
access-list 122 permit udp any 10.10.0.0 0.0.255.255
access-list 122 permit udp any 10.10.0.0 0.0.255.255 range 33
434 33464
access-list 122 permit udp 10.10.0.0 0.0.255.255 any range 33
434 33464
!
control-plane
 service-policy input CoPP
!
!
!
```

CORE# Copy run start TESTING: CORE

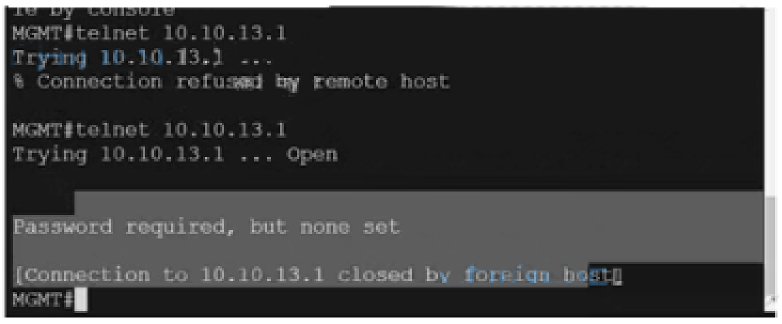
Graphical user interface Description automatically generated with medium confidence



```
CORE#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(101)
H   Address                 Interface              Hold Upti
me    SRTT   RTO  Q  Seq
                                                   (sec)
      (ms)       Cnt Num
0   10.10.13.3              Et0/1                    11 00:0
3:15     5   100  0  35
1   10.10.12.2              Et0/0                    11 00:0
3:24     7   100  0  33
CORE#copy run star
```

MGMT

Graphical user interface, text Description automatically generated



```
le by console
MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ...
% Connection refused by remote host

MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ... Open


Password required, but none set

[Connection to 10.10.13.1 closed by foreign host]
MGMT#
```

NEW QUESTION 270

- (Exam Topic 3)

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?

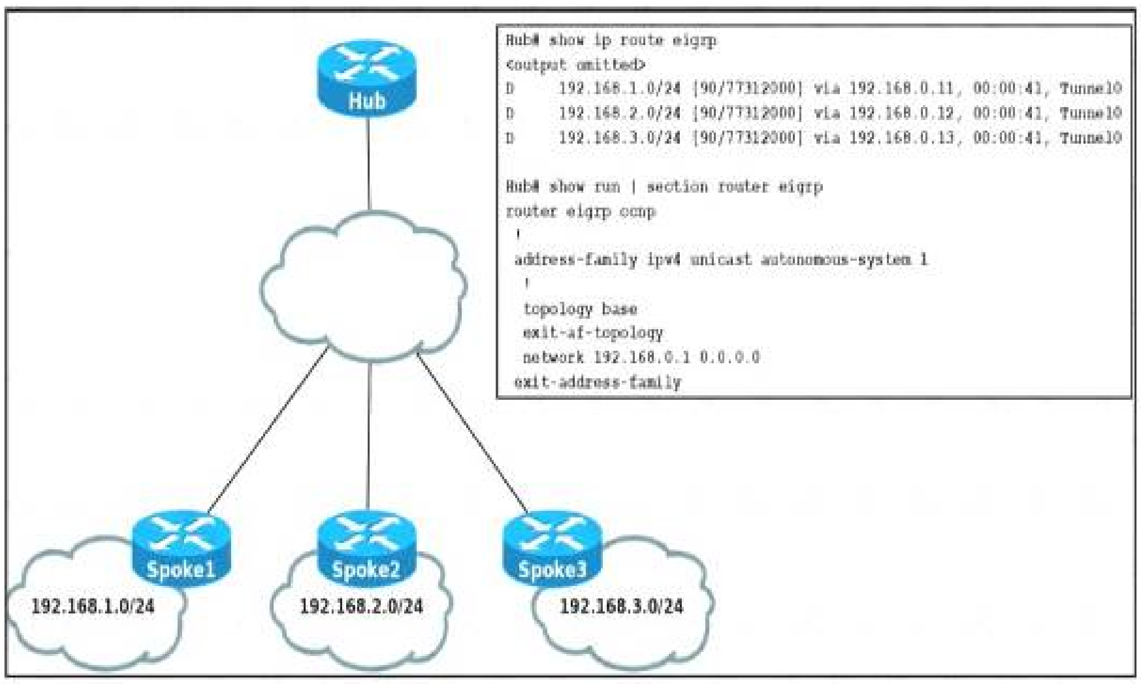
A. RC(config)#router bgp 65201RC(config-router)#neighbor 10.10.10.4 route-reflector-client
B. RF(config)#router bgp 65201RF(config-router)#neighbor 10.10.10.6 route-reflector-client
C. RC(config)#router bgp 65201RC(config-router)#neighbor 10.10.10.2 route-reflector-client
D. RB(config)router bgp 65201RB(config-router)#neighbor 10.10.10.3 route-reflector-client

Answer: A

NEW QUESTION 272

- (Exam Topic 3)

Refer to the exhibit.



```
Hub# show ip route eigrp
<output omitted>
D     192.168.1.0/24 [90/77312000] via 192.168.0.11, 00:00:41, Tunnel0
D     192.168.2.0/24 [90/77312000] via 192.168.0.12, 00:00:41, Tunnel0
D     192.168.3.0/24 [90/77312000] via 192.168.0.13, 00:00:41, Tunnel0

Hub# show run | section router eigrp
router eigrp ccnp
 !
 address-family ipv4 unicast autonomous-system 1
  !
  topology base
  exit-af-topology
  network 192.168.0.1 0.0.0.0
 exit-address-family
```

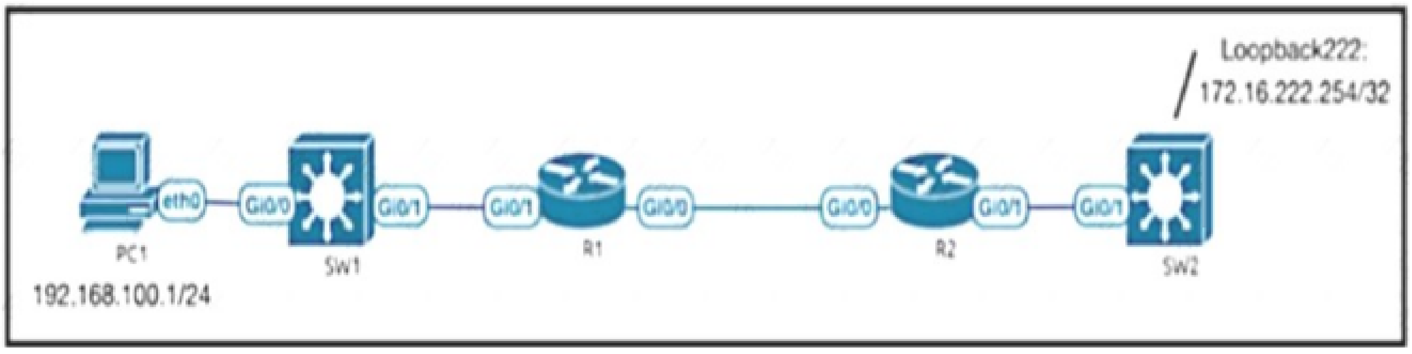
Spoke routers do not learn about each other's routes in the DMVPN Phase2 network. Which action resolves the issue?

A. Remove default route from spoke routers to establish a spoke-to-spoke tunnel.
B. Configure a static route in each spoke to establish a spoke-to-spoke tunnel.

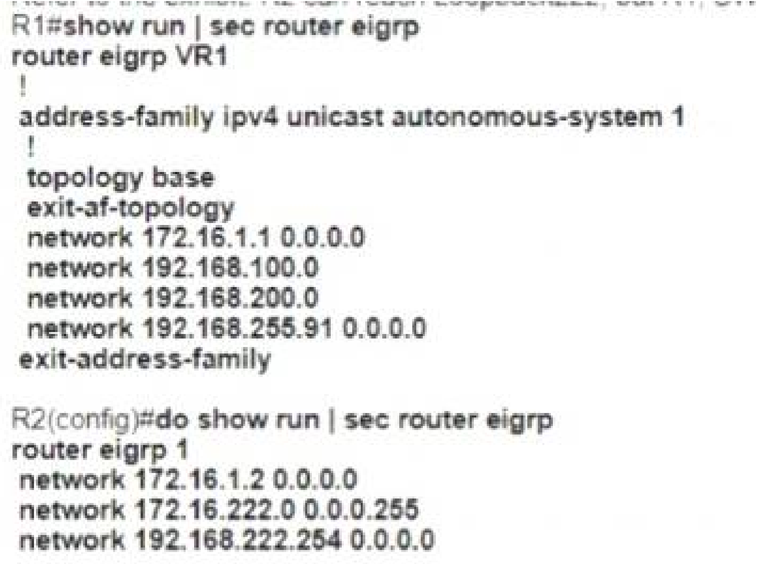
C. Rectify incorrect wildcard mask configured on the hub router network command.
D. Disable EIGRP split horizon on the TunnelO interface of the hub router.

Answer: D

NEW QUESTION 273
- (Exam Topic 3)



Refer to the exhibit R2 can reach Loopback222, but R1 SW1 and PC1 cannot communicate with 172.16.222 254 R1 and R2 configurations are shown here



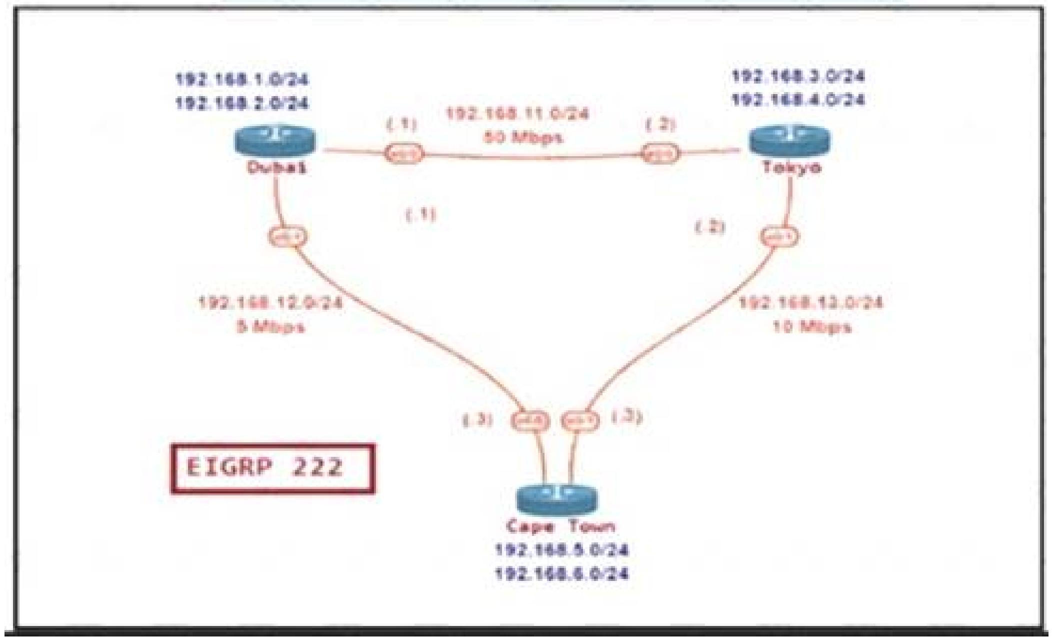
```
R1#show run | sec router eigrp
router eigrp VR1
 !
 address-family ipv4 unicast autonomous-system 1
  !
  topology base
  exit-af-topology
  network 172.16.1.1 0.0.0.0
  network 192.168.100.0
  network 192.168.200.0
  network 192.168.255.91 0.0.0.0
 exit-address-family

R2(config)#do show run | sec router eigrp
router eigrp 1
 network 172.16.1.2 0.0.0.0
 network 172.16.222.0 0.0.0.255
 network 192.168.222.254 0.0.0.0
```

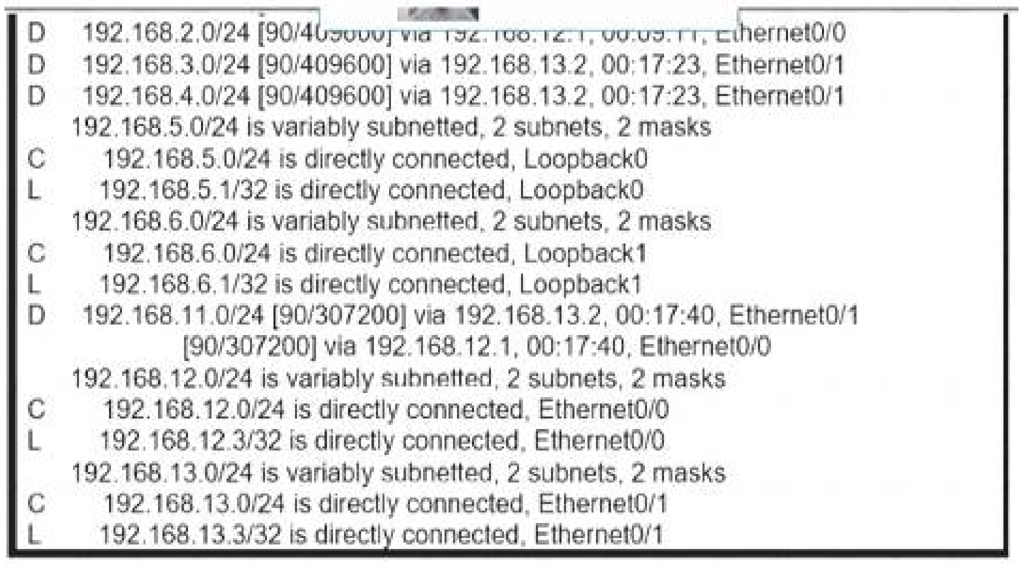
Which EIGRP configuration command resolves the issue?

A. R2(config-router) # redistribute static
B. R1(conftg-router)# network 172.16.222.254 0.0.0.0
C. R1 (config-router)# network 172.16.222.264 255.255.255.255
D. R1(config-router)# redistribute static

Answer: A

NEW QUESTION 277
- (Exam Topic 3)
Refer to the exhibit.

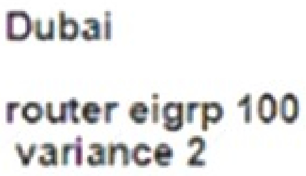




```
D    192.168.2.0/24 [90/409600] via 192.168.12.1, 00:09:11, Ethernet0/0
D    192.168.3.0/24 [90/409600] via 192.168.13.2, 00:17:23, Ethernet0/1
D    192.168.4.0/24 [90/409600] via 192.168.13.2, 00:17:23, Ethernet0/1
     192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.5.0/24 is directly connected, Loopback0
L       192.168.5.1/32 is directly connected, Loopback0
     192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.6.0/24 is directly connected, Loopback1
L       192.168.6.1/32 is directly connected, Loopback1
D    192.168.11.0/24 [90/307200] via 192.168.13.2, 00:17:40, Ethernet0/1
                     [90/307200] via 192.168.12.1, 00:17:40, Ethernet0/0
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/24 is directly connected, Ethernet0/0
L       192.168.12.3/32 is directly connected, Ethernet0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/24 is directly connected, Ethernet0/1
L       192.168.13.3/32 is directly connected, Ethernet0/1
```

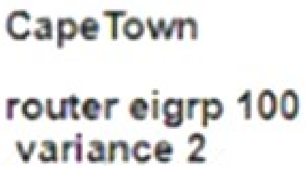
The network administrator must configure Cape Town to reach Dubai via Tokyo based on the speeds provided by the service provider. It was noticed that Cape Town is reaching Dubai directly and failed to meet the requirement. Which configuration fixes the issue?

A)



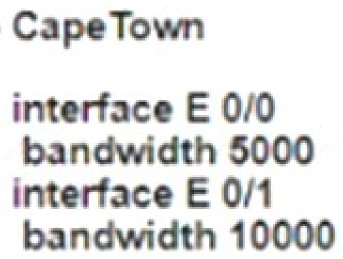
```
Dubai

router eigrp 100
 variance 2
```

B)



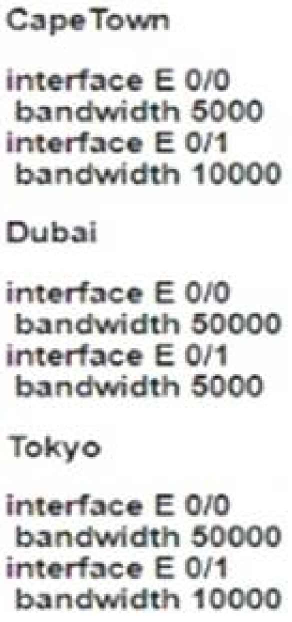
```
CapeTown

router eigrp 100
 variance 2
```

C)



```
CapeTown

interface E 0/0
 bandwidth 5000
interface E 0/1
 bandwidth 10000
```

D)

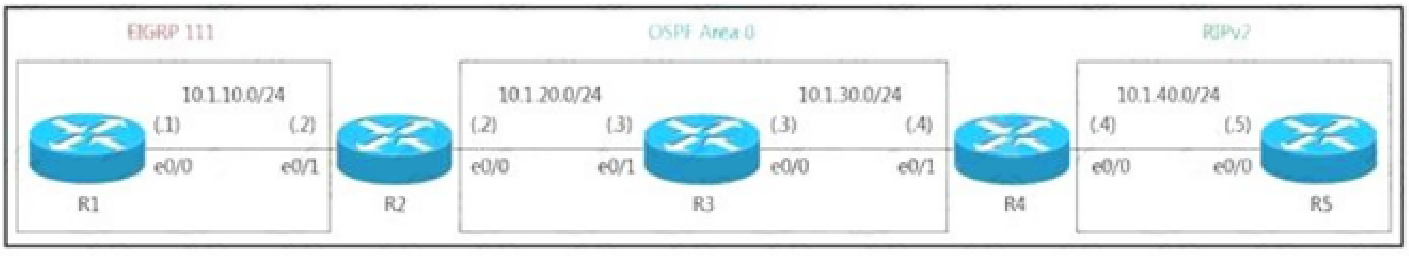


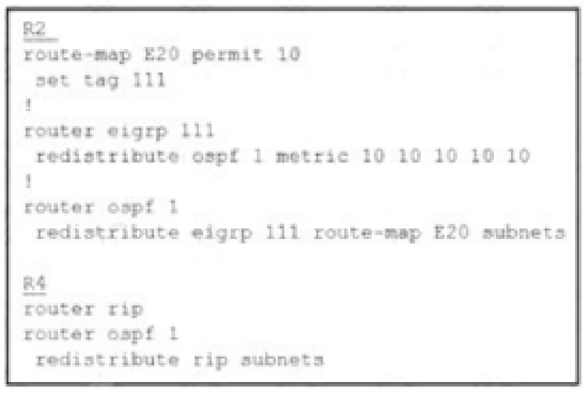
```
CapeTown

interface E 0/0
 bandwidth 5000
interface E 0/1
 bandwidth 10000

Dubai

interface E 0/0
 bandwidth 50000
interface E 0/1
 bandwidth 5000

Tokyo

interface E 0/0
 bandwidth 50000
interface E 0/1
 bandwidth 10000
```

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

Answer: D

NEW QUESTION 278
- (Exam Topic 3)
Refer to the exhibit.





```
R2
route-map E20 permit 10
 set tag 111
!
router eigrp 111
 redistribute ospf 1 metric 10 10 10 10 10
!
router ospf 1
 redistribute eigrp 111 route-map E20 subnets

R4
router rip
router ospf 1
 redistribute rip subnets
```

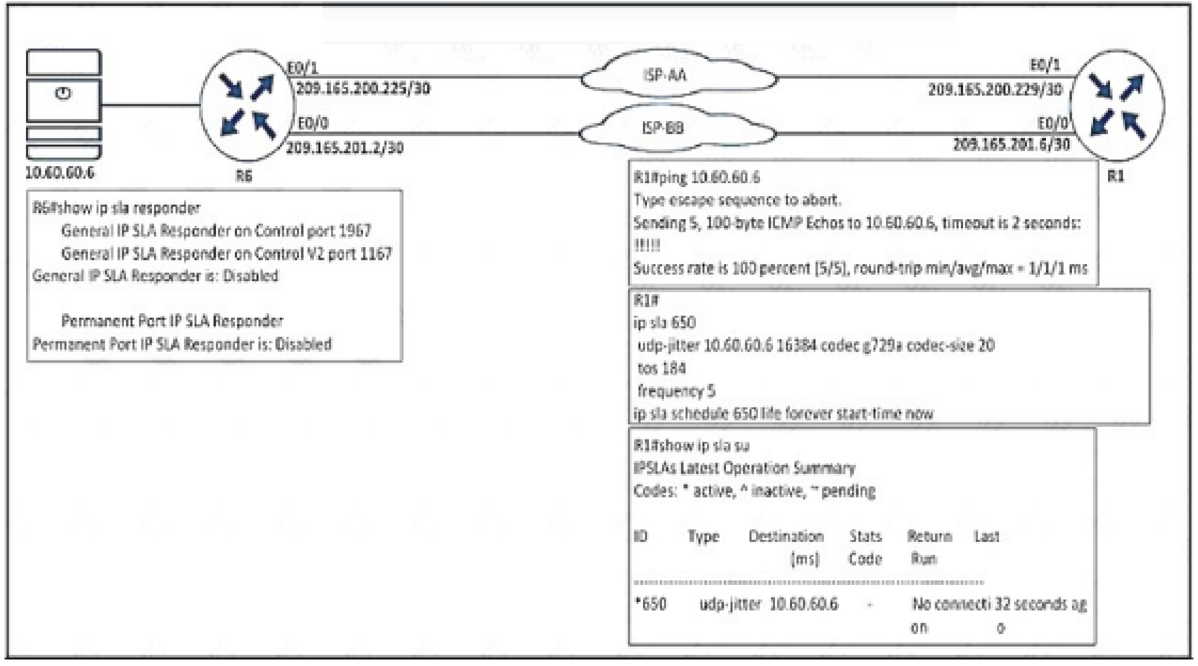
R5 should not receive any routes originated in the EIGRP domain. Which set of configuration changes removes the EIGRP routes from the R5 routing table to fix the issue?

A. R4route-map O2R deny 10 match tag 111route-map O2R permit 20!router ripredistribute ospf 1 route-map O2R metric 1
B. R2route-map E20 deny 20 R4route-map O2R deny 10 match tag 111!router ripredistribute ospf 1 route-map O2R metric 1
C. R4route-map O2R permit 10 match tag 111route-map O2R deny 20!router ripredistribute ospf 1 route-map O2R metric 1
D. R4route-map O2R deny 10 match tag 111!router ripredistribute ospf 1 route-map O2R metric 1

Answer: A

Explanation:
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 279
- (Exam Topic 3)



```
R6#show ip sla responder
    General IP SLA Responder on Control port 1967
    General IP SLA Responder on Control V2 port 1167
General IP SLA Responder is: Disabled

    Permanent Port IP SLA Responder
Permanent Port IP SLA Responder is: Disabled
```

```
R1#ping 10.60.60.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.60.60.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
R1#
ip sla 650
 udp-jitter 10.60.60.6 16384 codec g729a codec-size 20
 tos 184
 frequency 5
ip sla schedule 650 life forever start-time now
```

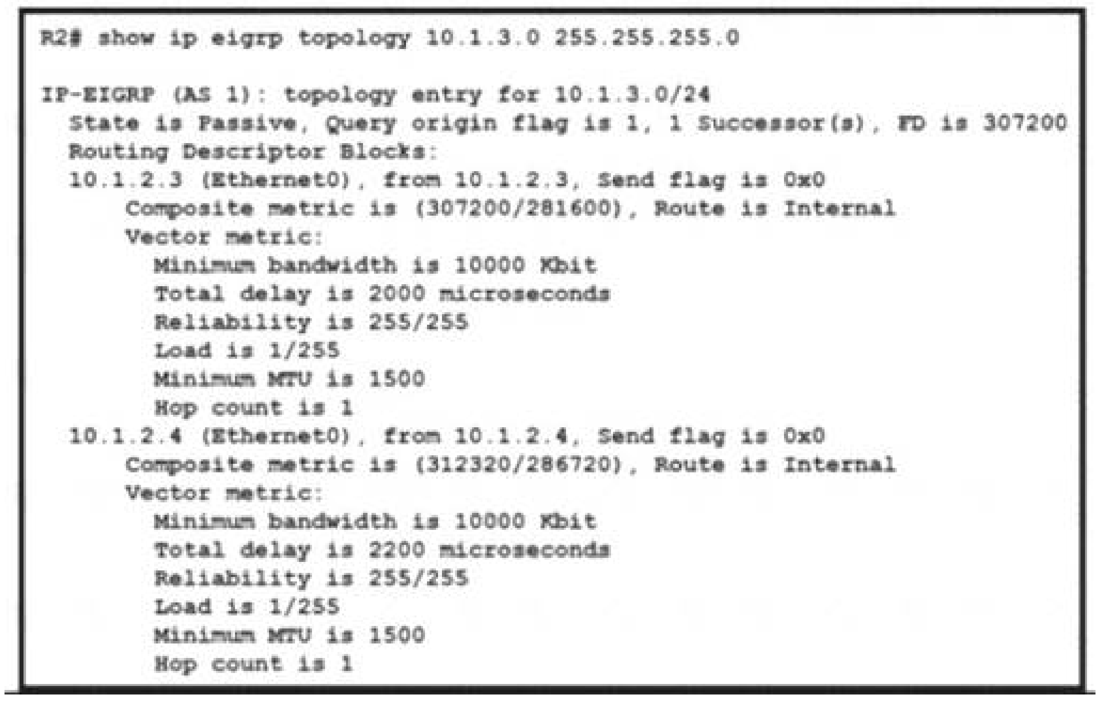
```
R1#show ip sla su
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID      Type       Destination   Stats   Return    Last
                   (ms)          Code    Run
------------------------------------------------------------
*650    udp-jitter  10.60.60.6    -      No connecti 32 seconds ag
                                         on          o
```

Refer to the exhibit. Which configuration resolves the IP SLA issue from R1 to the server?

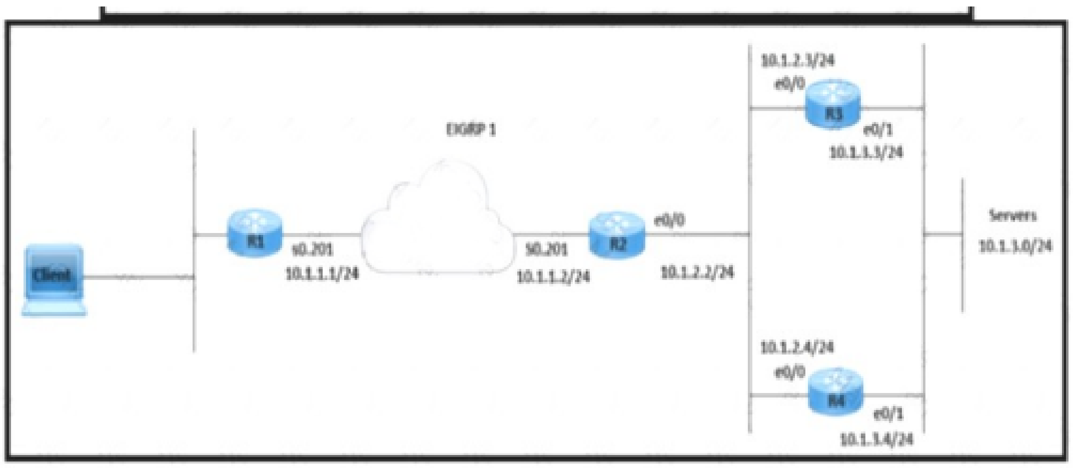
A. R6(config)#ip sla responder
B. R6(config)#ip sla responder udp-echo ipaddress 10.60.60.6 po 5000
C. R6(config)#ip sla 650 R6(config-ip-sla)ff udp-jitter 10.60.60.6
D. R6(config)#ip sla schedule 10 life forever start-time now

Answer: A

NEW QUESTION 284
- (Exam Topic 3)
Exhibit.



```
R2# show ip eigrp topology 10.1.3.0 255.255.255.0

IP-EIGRP (AS 1): topology entry for 10.1.3.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 307200
  Routing Descriptor Blocks:
  10.1.2.3 (Ethernet0), from 10.1.2.3, Send flag is 0x0
      Composite metric is (307200/281600), Route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 2000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  10.1.2.4 (Ethernet0), from 10.1.2.4, Send flag is 0x0
      Composite metric is (312320/286720), Route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 2200 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```



Refer to the exhibit. A network is configured for EIGRP equal-cost load balancing, but the traffic destined to the servers is not load balanced. Link metrics from router R2 to R3 and R4 are the same. Which delay value must be configured to resolve the issue?

A. 208 oon R3 E0/0
B. 120 on R4 E0/1
C. 120/on R3 E0/1
D. 2200 on R4 E0/1

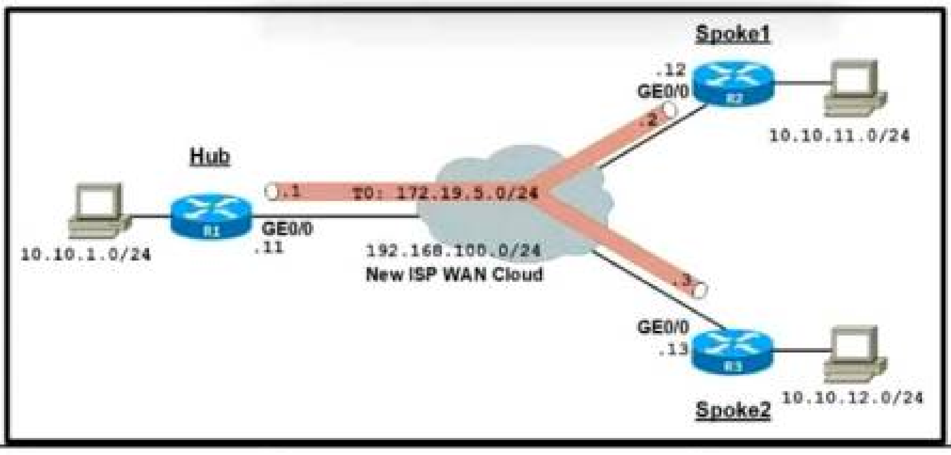
Answer: C

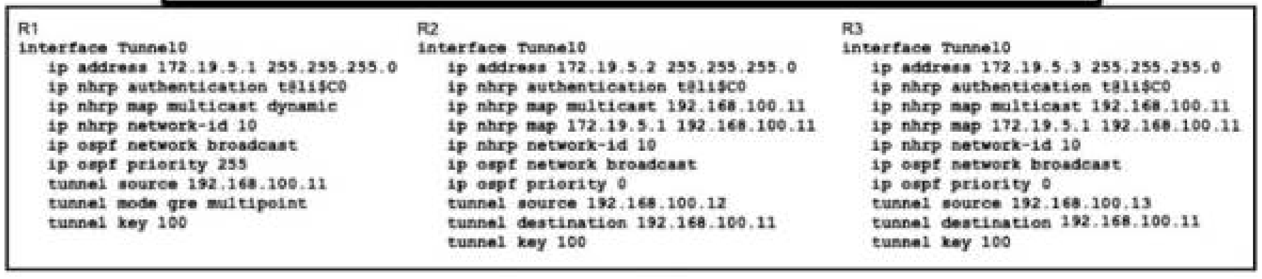
NEW QUESTION 288
- (Exam Topic 3)
How does LDP operate in an MPLS network?

A. When topology changes occur such as a router failure, LDP generates peer discovery messages that terminate the LDP season to propagate an LSP change.
B. When an adjacent LSR receives LDP discovery message
C. TCP two-way handshake ensures that the LDP session has unidirectional connectivity.
D. Peer routers establish the LDP session, and the LDP neighbors maintain and terminate the session by exchanging messages
E. LDP notification messages allow LERs to exchange label information to determine the next hops within a particular LSP.

Answer: D

NEW QUESTION 290
- (Exam Topic 3)





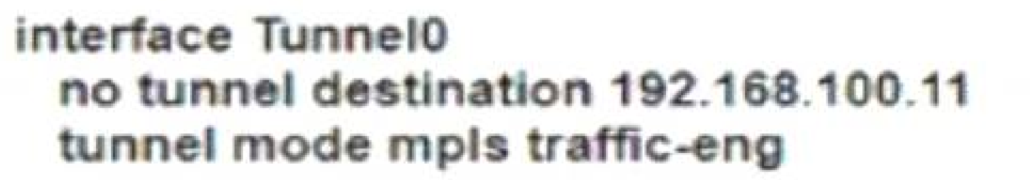
```
R1
interface Tunnel0
  ip address 172.19.5.1 255.255.255.0
  ip nhrp authentication t@li$C0
  ip nhrp map multicast dynamic
  ip nhrp network-id 10
  ip ospf network broadcast
  ip ospf priority 255
  tunnel source 192.168.100.11
  tunnel mode gre multipoint
  tunnel key 100
```

```
R2
interface Tunnel0
  ip address 172.19.5.2 255.255.255.0
  ip nhrp authentication t@li$C0
  ip nhrp map multicast 192.168.100.11
  ip nhrp map 172.19.5.1 192.168.100.11
  ip nhrp network-id 10
  ip ospf network broadcast
  ip ospf priority 0
  tunnel source 192.168.100.12
  tunnel destination 192.168.100.11
  tunnel key 100
```

```
R3
interface Tunnel0
  ip address 172.19.5.3 255.255.255.0
  ip nhrp authentication t@li$C0
  ip nhrp map multicast 192.168.100.11
  ip nhrp map 172.19.5.1 192.168.100.11
  ip nhrp network-id 10
  ip ospf network broadcast
  ip ospf priority 0
  tunnel source 192.168.100.13
  tunnel destination 192.168.100.11
  tunnel key 100
```

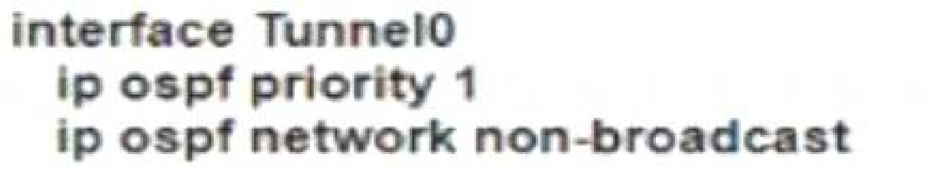
Refer to the exhibit. An organization is installing a new L3 MPLS link to establish DM VPN Phase 2 tunnels between the hub and two spoke routers Which additional configuration should the engineer implement on each device to achieve optimal routing between the spokes?

A)



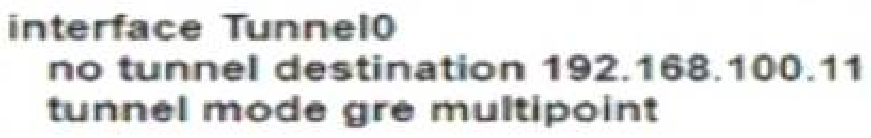
```
interface Tunnel0
  no tunnel destination 192.168.100.11
  tunnel mode mpls traffic-eng
```

B)



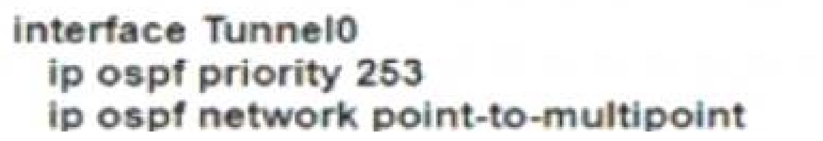
```
interface Tunnel0
  ip ospf priority 1
  ip ospf network non-broadcast
```

C)



```
interface Tunnel0
  no tunnel destination 192.168.100.11
  tunnel mode gre multipoint
```

D)

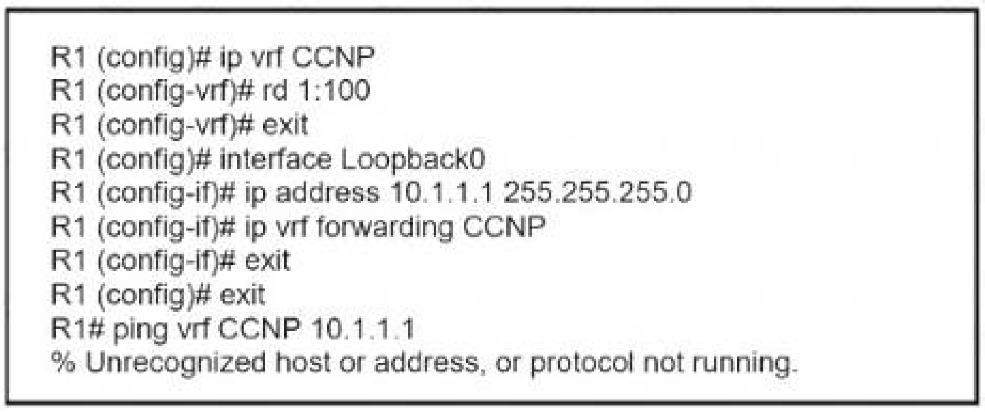


```
interface Tunnel0
  ip ospf priority 253
  ip ospf network point-to-multipoint
```

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

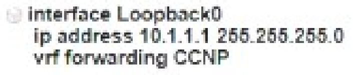
Answer: C

NEW QUESTION 292
- (Exam Topic 3)

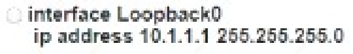


```
R1 (config)# ip vrf CCNP
R1 (config-vrf)# rd 1:100
R1 (config-vrf)# exit
R1 (config)# interface Loopback0
R1 (config-if)# ip address 10.1.1.1 255.255.255.0
R1 (config-if)# ip vrf forwarding CCNP
R1 (config-if)# exit
R1 (config)# exit
R1# ping vrf CCNP 10.1.1.1
% Unrecognized host or address, or protocol not running.
```

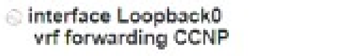
Refer to the exhibit Which command must be configured to make VRF CCNP work?



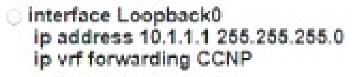
```
○ interface Loopback0
   ip address 10.1.1.1 255.255.255.0
   vrf forwarding CCNP
```



```
○ interface Loopback0
   ip address 10.1.1.1 255.255.255.0
```



```
○ interface Loopback0
   vrf forwarding CCNP
```



```
○ interface Loopback0
   ip address 10.1.1.1 255.255.255.0
   ip vrf forwarding CCNP
```

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

Answer: B

NEW QUESTION 293
- (Exam Topic 3)
An engineer creates a Cisco DNA Center cluster with three nodes, but all the services are running on one host node. Which action resolves this issue?

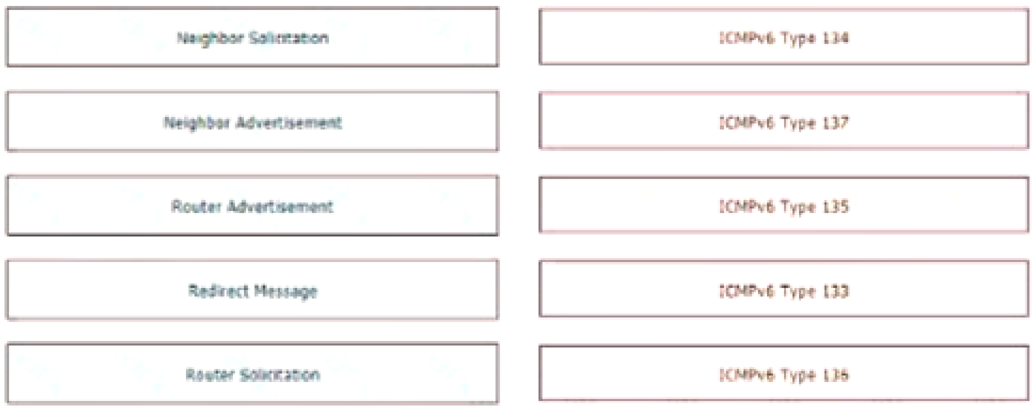
A. Restore the link on the switch interface that is connected to a cluster link on the Cisco DNA Center
B. Click the master host node with all the services and select services to be moved to other hosts
C. Enable service distribution from the Systems 360 page.
D. Click system updates, and upgrade to the latest version of Cisco DNA Center.

Answer: C

Explanation:
To deploy Cisco DNA Center on a three-node cluster with High Availability (HA) enabled, complete the following procedure:
Step 1: Configure Cisco DNA Center on the first node in your cluster… Step 2: Configure Cisco DNA Center on the second node in your cluster… Step 3: Configure

Cisco DNA Center on the third node in your cluster… Step 4: Enable high availability on your cluster:
* a. In the Cisco DNA Center GUI, click and choose System Settings. The System 360 tab is displayed by default.
* b. In the Hosts area, click Enable Service Distribution.
After you click Enable Service Distribution, Cisco DNA Center enters into maintenance mode. In this mode, Cisco DNA Center is unavailable until the redistribution of services is completed. You should take this into account when scheduling an HA deployment.
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automationand- management/dna-center/1-3-3-0/ha_guide/b_cisco_dna_center_ha_guide_1_3_3_0.html
Therefore we can choose “Enable Service Distribution” to distribute services to other host nodes.

NEW QUESTION 294
- (Exam Topic 3)
Drag and drop the ICMPv6 neighbor discovery messages from the left onto the correct packet types on the right.



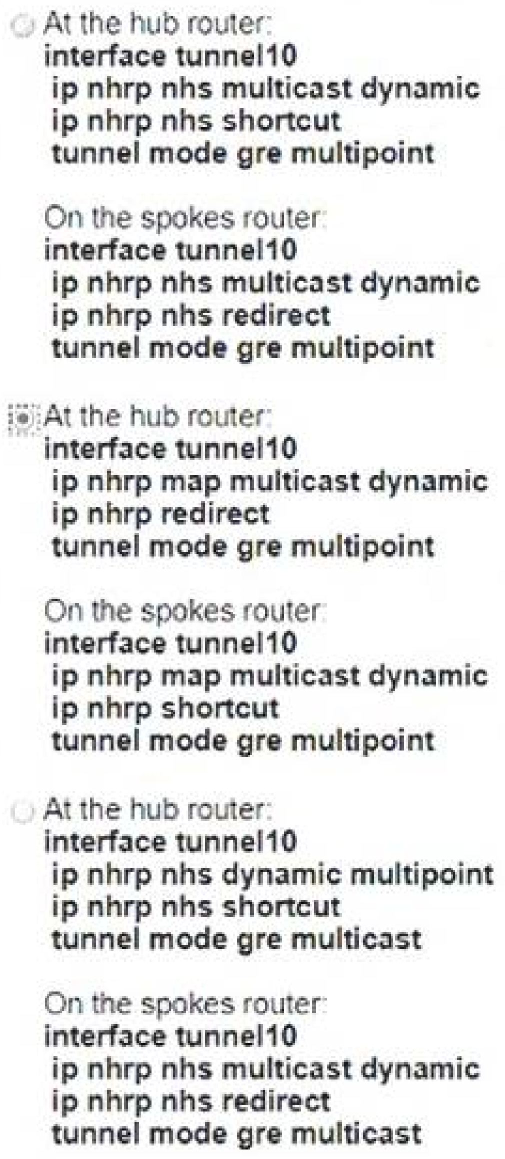
Neighbor Solicitation	ICMPv6 Type 134
Neighbor Advertisement	ICMPv6 Type 137
Router Advertisement	ICMPv6 Type 135
Redirect Message	ICMPv6 Type 133
Router Solicitation	ICMPv6 Type 136

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated with medium confidence

NEW QUESTION 295
- (Exam Topic 3)
A network engineer must configure a DMVPN network so that a spoke establishes a direct path to another spoke if the two must send traffic to each other. A spoke must send traffic directly to the hub if required Which configuration meets this requirement?



○ At the hub router:

```
interface tunnel10
 ip nhrp nhs multicast dynamic
 ip nhrp nhs shortcut
 tunnel mode gre multipoint
```

On the spokes router:

```
interface tunnel10
 ip nhrp nhs multicast dynamic
 ip nhrp nhs redirect
 tunnel mode gre multipoint
```

● At the hub router:

```
interface tunnel10
 ip nhrp map multicast dynamic
 ip nhrp redirect
 tunnel mode gre multipoint
```

On the spokes router:

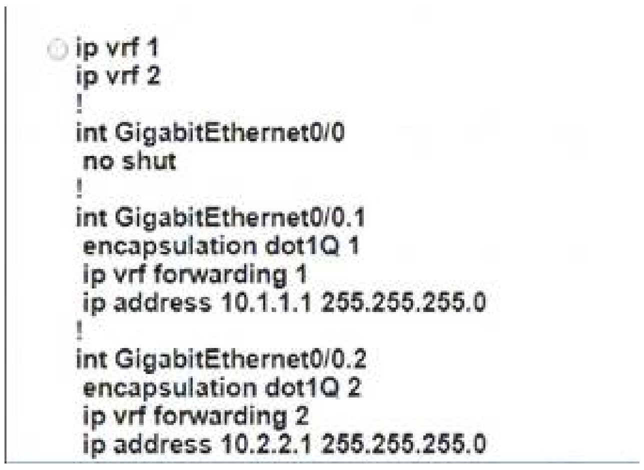
```
interface tunnel10
 ip nhrp map multicast dynamic
 ip nhrp shortcut
 tunnel mode gre multipoint
```

○ At the hub router:

```
interface tunnel10
 ip nhrp nhs dynamic multipoint
 ip nhrp nhs shortcut
 tunnel mode gre multicast
```

On the spokes router:

```
interface tunnel10
 ip nhrp nhs multicast dynamic
 ip nhrp nhs redirect
 tunnel mode gre multicast
```

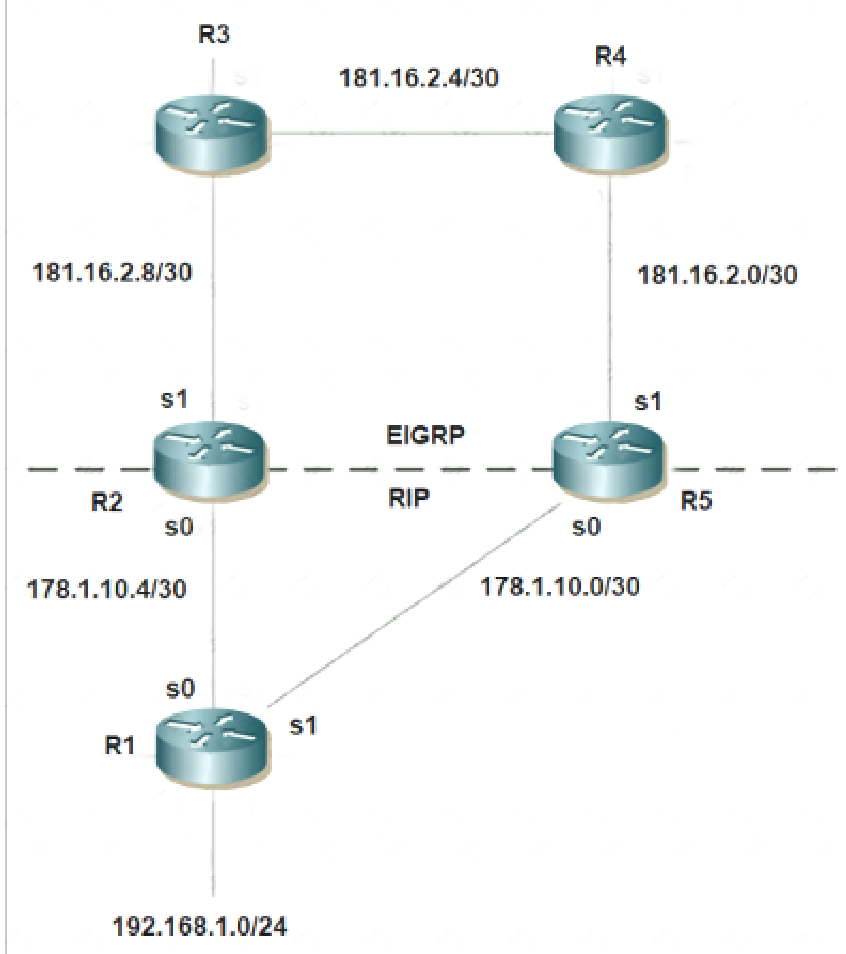


```
○ ip vrf 1
  ip vrf 2
  !
  int GigabitEthernet0/0
   no shut
  !
  int GigabitEthernet0/0.1
   encapsulation dot1Q 1
   ip vrf forwarding 1
   ip address 10.1.1.1 255.255.255.0
  !
  int GigabitEthernet0/0.2
   encapsulation dot1Q 2
   ip vrf forwarding 2
   ip address 10.2.2.1 255.255.255.0
```

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

Answer: B

NEW QUESTION 296
- (Exam Topic 3)
Refer to the exhibit.



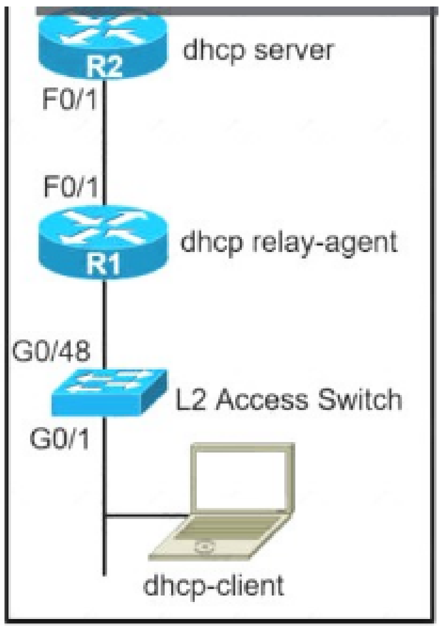
Mutual redistribution is enabled between RIP and EIGRP on R2 and R5. Which configuration resolves the routing loop for the 192.168.1.0/24 network?

A. R2:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit anyR5:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit any
B. R2:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit anyR5:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit any
C. R2:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit anyR5:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit any
D. R2:router eigrp 7network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 7 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit anyR5:router eigrp 7network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 7 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit any

Answer: D

Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.ht

NEW QUESTION 298
- (Exam Topic 2)
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-relay command on R1
B. ip dhcp option 82 command on R2
C. service dhcp command on R1
D. ip dhcp relay information enable command on R1
E. ip dhcp relay information trust-all command on R2

Answer: CE

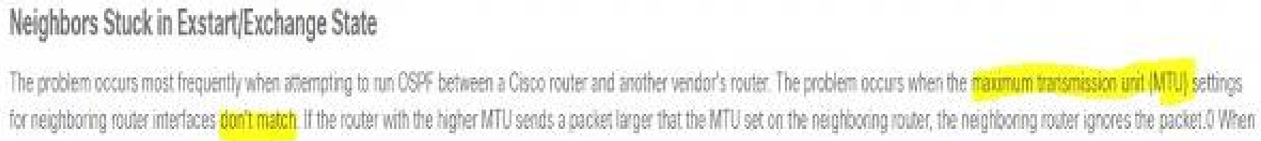
Explanation:
* 1. R1 received DHCP packet and its interface was configured with the DHCP helper address. But we are not sure if R1 forward DHCP packet to R2 or not. 2. If we connect PC directly to R2 then this problem will not appear -> DHCP Server function was configured on R2.
From these facts, the most likely problem is related to Option 82. Maybe R2 ignored DHCP request packets because it was receiving these packets with the giant field set to 0.0.0.0.
By default Cisco IOS devices reject packets with zero “giaddr” and by default Cisco Catalyst switches use “giaddr” of zero when configured for DHCP snooping!
Reference: https://blog.ine.com/2009/07/22/understanding-dhcp-option-82
If we can run the “debug ip dhcp server packet” on R2, we may see these messages:
*Feb 22 23:54:57.759: IP: s=0.0.0.0 (FastEthernet0/1), d=255.255.255.255, len 34 4, input feature, MCI Check(64), rtype 0, forus FALSE, sendself FALSE, mtu 0, fw dchk FALSE *Feb 22 23:54:57.759: IP: s=0.0.0.0 (FastEthernet0/1), d=255.255.255.255, len 34 4, rcvd 2 *Feb 22 23:54:57.759: IP: s=0.0.0.0 (FastEthernet0/1), d=255.255.255.255, len 34 4, stop process pak for forus packet
*Feb 22 23:54:57.759: DHCPD: inconsistent relay information. *Feb 22 23:54:57.759: DHCPD: relay information option exists, but giaddr is zero
We are receiving the DHCP packet from R1, source 0.0.0.0, and destination 255.255.255.255 broadcast, but if you notice from the debug output, R2, our DHCP Server, is complaining that the relay information is inconsistent. Option 82, Information Option, is contained in the packet but the GIADDR is zero. The GIADDR stands for Gateway IP Address, which is the IP Address of the relaying agent. The Option 82, Information Option, would then contain the receiving port and hostname of the Relaying Agent by default.
R2 sees the Option 82 information, signalling that the DHCP packet might have been relayed, BUT there is no relaying IP Address. This is the behavior of DHCP Snooping when enabling it on a switch, and since the switchport does not contain an IP Address, since it’s Layer 2, no GIADDR will be added.
Instead, just the Option 82 Information is added and this is the problem we have, but there are options:
* 1. You could trust all on R2 the DHCP Server, which will cause the server to not be so suspicious: – ip dhcp relay information trust-all – ip dhcp relay information trusted 2. Disable the addition of Option 82 information on SW: – no ip dhcp snooping information option 3. Trust the port that is receiving the DHCP Discover: – ip dhcp snooping trust
Any of these options will fix our predicament. Reference: https://evilttl.com/wiki/DHCP-Snooping
But in the answer choices, we only have 1 correct answer which is the command “ip dhcp relay information trust-all”. We checked if we need any “service dhcp…” command on both IOS version 12.4 and 15.1:
Therefore we only have the “service dhcp” command, we don’t have any “service dhcp-relay” command available. But the description of the “service dhcp” command says that it enables both DHCP server and relay agent so this is the best answer left.

NEW QUESTION 303
- (Exam Topic 2)
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: C

Explanation:



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

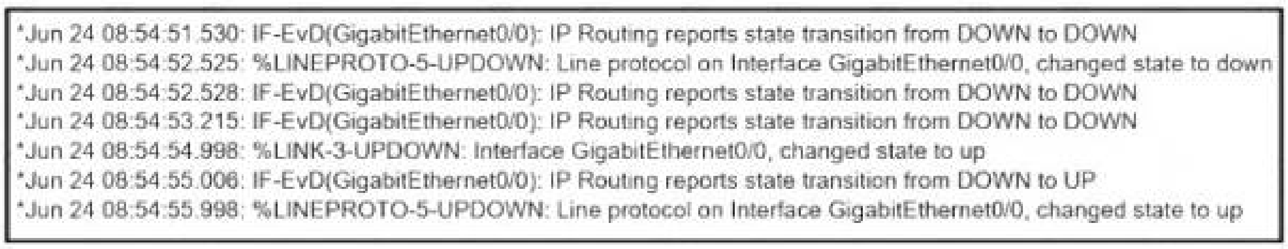
NEW QUESTION 306
- (Exam Topic 2)
What are two functions of MPLS Layer 3 VPNs? (Choose two.)

A. LDP and BGP can be used for Pseudowire signaling.
B. It is used for transparent point-to-multipoint connectivity between Ethernet links/sites.
C. BGP is used for signaling customer VPNv4 routes between PE nodes.
D. A packet with node segment ID is forwarded along with shortest path to destination.
E. Customer traffic is encapsulated in a VPN label when it is forwarded in MPLS network.

Answer: CE

Explanation:
MPLS Layer-3 VPNs provide IP connectivity among CE sites* MPLS VPNs enable full-mesh, hub-andspoke, and hybrid IP connectivity* CE sites connect to the MPLS network via IP peering across PE-CE links* MPLS Layer-3 VPNs are implemented via VRFs on PE edge nodes* VRFs providing customer routing and forwarding segmentation* BGP used for signaling customer VPN (VPNv4) routes between PE nodes* To ensure traffic separation, customer traffic is encapsulated in an additional VPN label when forwarded in MPLS network* Key applications are layer-3 business VPN services, enterprise network segmentation, and segmented layer-3 Data Center access
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKMPL-1100.pdf

NEW QUESTION 311
- (Exam Topic 2)
Refer to the exhibit.



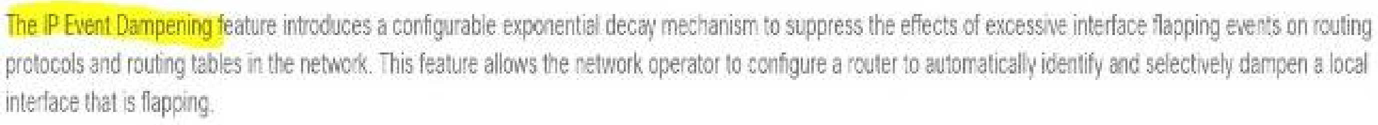
```
*Jun 24 08:54:51.530: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:52.525: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
*Jun 24 08:54:52.528: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:53.215: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:54.998: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun 24 08:54:55.006: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to UP
*Jun 24 08:54:55.998: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

R1 is connected with R2 via GigabitEthernet0/0, and R2 cannot ping R1. What action will fix the issue?

A. Fix route dampening configured on the router.
B. Replace the SFP module because it is not supported.
C. Fix IP Event Dampening configured on the interface.
D. Correct the IP SLA probe that failed.

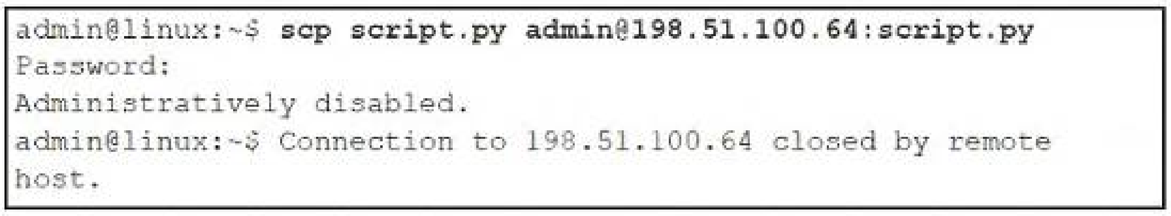
Answer: C

Explanation:



The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping.

NEW QUESTION 316
- (Exam Topic 2)
Refer to the exhibit.



```
admin@linux:~$ scp script.py admin@198.51.100.64:script.py
Password:
Administratively disabled.
admin@linux:~$ Connection to 198.51.100.64 closed by remote
host.
```

A network administrator has developed a Python script on the local Linux machine and is trying to transfer it to the router. However, the transfer fails. Which action resolves this issue?

A. The SSH service must be enabled with the crypto key generate rsa command.
B. The SCP service must be enabled with the ip scp server enable command.
C. The Python interpreter must first be enabled with the guestshell enable command.
D. The SSH access must be allowed on the VTY lines using the transport input ssh command.

Answer: B

Explanation:
The error “Administratively disabled” means we need to enable SCP on the router with the command: Router(config)#ip scp server enable

NEW QUESTION 317
- (Exam Topic 2)
What are two characteristics of VRF instance? (Choose two.)

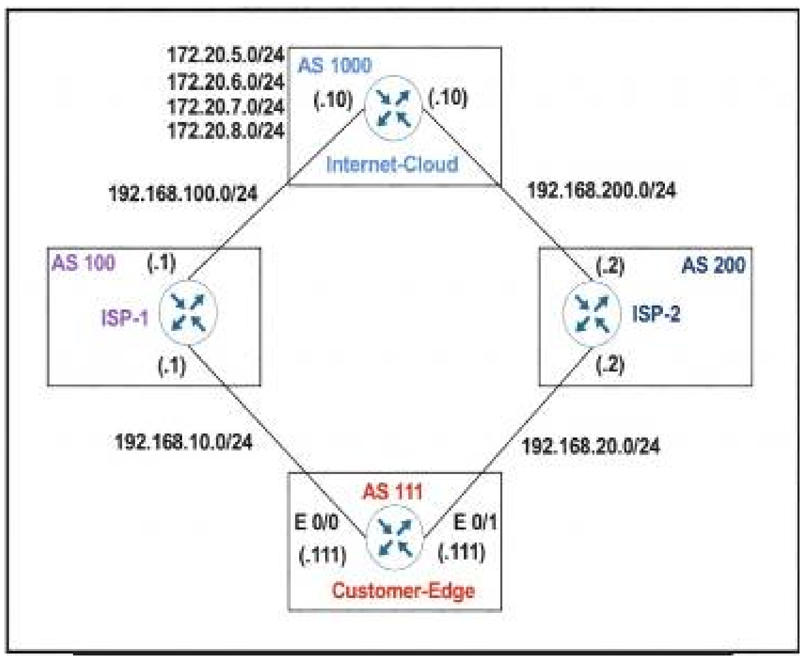
A. All VRFs share customers routing and CEF tables .
B. An interface must be associated to one VRF.
C. Each VRF has a different set of routing and CEF tables
D. It is defined by the VPN membership of a customer site attached to a P device.
E. A customer site can be associated to different VRFs

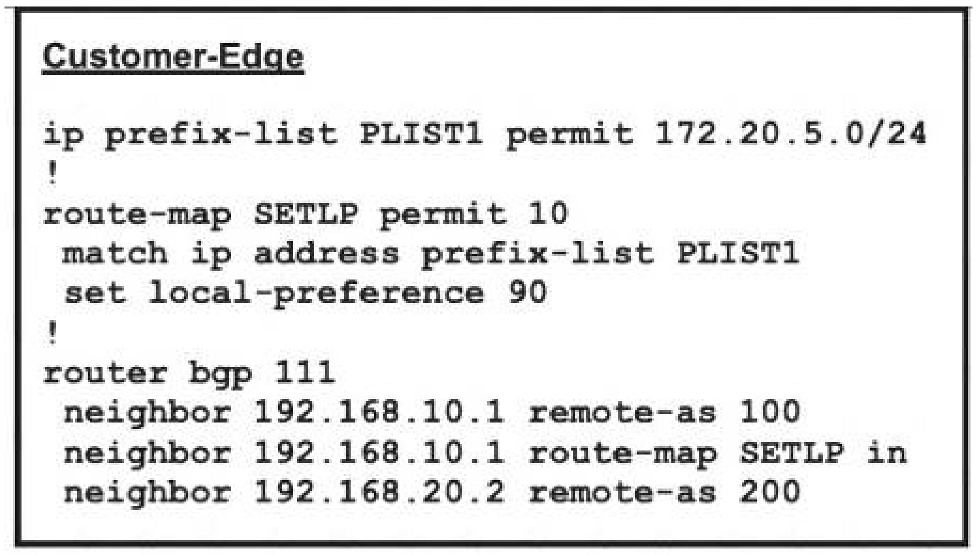
Answer: BC

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/xe-3s/isw-cef-xe-3s-book/isw-cef

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-s/mp-l3-vpns-15-s-book/mp-b

NEW QUESTION 320
- (Exam Topic 2)
Refer to Exhibit:





Customer-Edge

```
ip prefix-list PLIST1 permit 172.20.5.0/24
!
route-map SETLP permit 10
 match ip address prefix-list PLIST1
 set local-preference 90
!
router bgp 111
 neighbor 192.168.10.1 remote-as 100
 neighbor 192.168.10.1 route-map SETLP in
 neighbor 192.168.20.2 remote-as 200
```

AS 111 wanted to use AS 200 as the preferred path for 172.20.5.0/24 and AS 100 as the backup. After the configuration, AS 100 is not used for any other routes. Which configuration resolves the issue?

A. route-mmap SETLP permit 10 match ip address prefix-list PLIST1 set local-preference 99route-map SETLP permit 20
B. route-map SETLP permit 10match ip address prefix-list PLIST1 set local-preference 110route-map SETLP permit 20
C. router bgp 111no neighbor 192.168.10.1 route-map SETLP in neighbor 192.168.10.1 route-map SETLP out
D. router bap 111no neighbor 192.168.10.1 route-map SETLP in neighbor 192.168.20.2 route-map SE TLP in

Answer: A

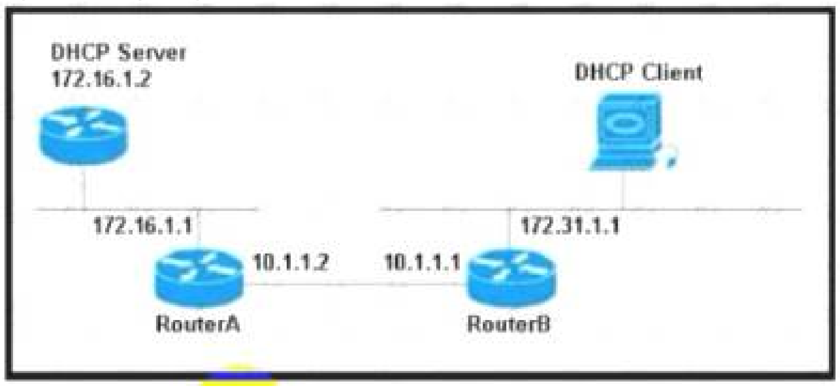
Explanation:
There is an implicit deny all at the end of any route-map so all other traffic that does not match 172.20.5.0/24 would be dropped. Therefore we have to add a permitsequence at the end of the route-map to allow other traffic.
The default value of Local Preference is 100 and higher value is preferred so we have to set the local preference of AS100 lower than that of AS200.

NEW QUESTION 325
- (Exam Topic 2)
What statement about route distinguishes in an MPLS network is true?

A. Route distinguishes make a unique VPNv4 address across the MPLS network.
B. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.
C. Route distinguishes are used for label bindings
D. Route distinguishes define which prefixes are imported and exported on the edge router

Answer: A

NEW QUESTION 329
- (Exam Topic 2)



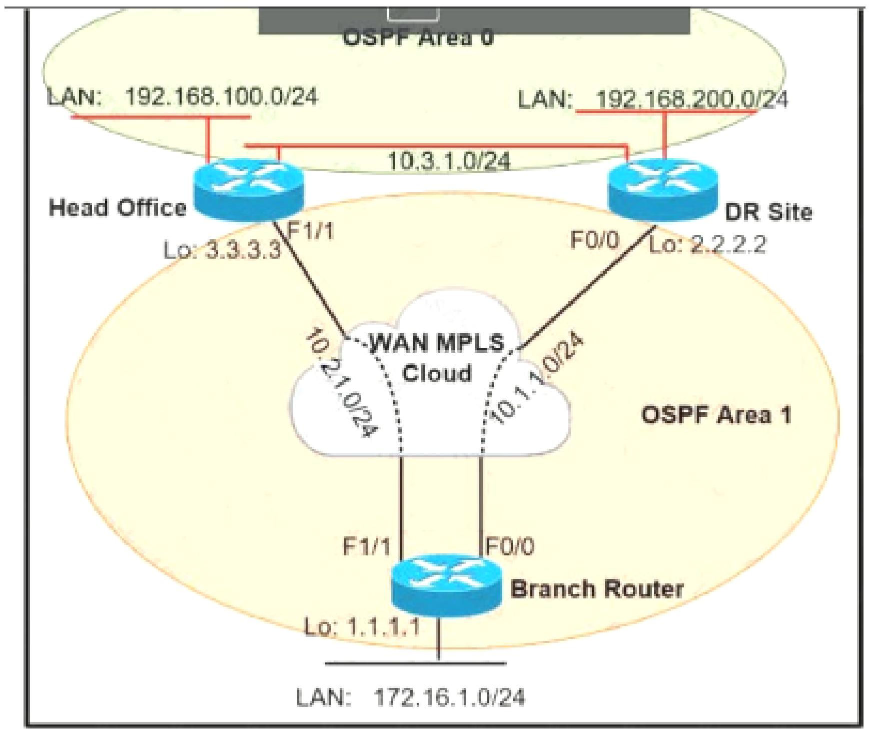
Refer to the exhibit. The DHCP client is unable to receive an IP address from the DHCP server RouterB is configured as follows:

Interface fastethernet 0/0
description Client DHCP ID 394482431 Ip address 172 31 11 255 255.255 0
!
ip route 172.16.1.0 255 255 255.0 10.1.1.2
Which command is required on the fastethernet 0/0 interface of RouterB to resolve this issue?

A. RouterB(config-if)#lp helper-address 172.31.1.1
B. RouterBiconfig-ififclp helper-address 255.255 255 255
C. RouterB(config-if)#lp helper-address 172.16.1.1
D. RouterB(config-if)#lp helper-address 172.16.1.2

Answer: D

NEW QUESTION 333
- (Exam Topic 2)
Refer to the exhibit.

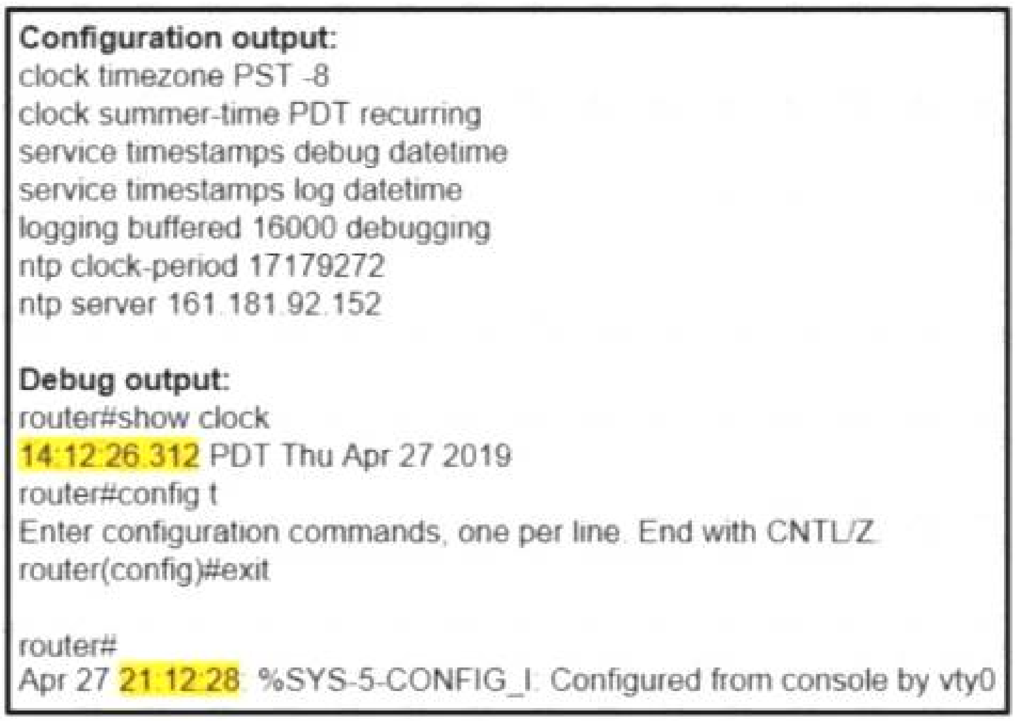


A network administrator reviews the branch router console log to troubleshoot the OSPF adjacency issue with the DR router. Which action resolves this issue?

A. Advertise the branch WAN interface matching subnet for the DR site.
B. Configure matching hello and dead intervals between sites.
C. Configure the WAN interface for DR site in the related OSPF area.
D. Stabilize the DR site flapping link to establish OSPF adjacency.

Answer: A

NEW QUESTION 334
- (Exam Topic 2)



```
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
```

Refer to the exhibit. 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

Explanation:
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

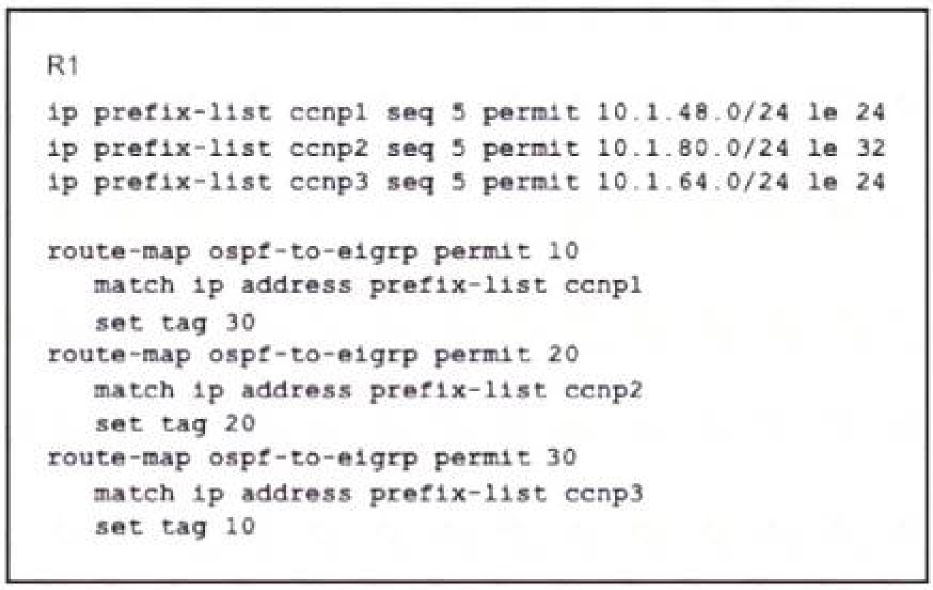
systemclock if the [localtime] option is not in the service timestamps log command. To solve this issue, add the [localtime] option to the service timestamps log command. Thetimes should now be synchronized between the system clock and the log message timestamps.
Reference:
https://community.cisco.com/t5/networking-documents/router-log-timestamp-entries-are-different-from-the-syst

NEW QUESTION 338
- (Exam Topic 2)
When configuring Control Plane Policing on a router to protect it from malicious traffic, an engineer observes that the configured routing protocols start flapping on that device. Which action in the Control Plane Policy prevents this problem in a production environment while achieving the security objective?

A. Set the conform-action and exceed-action to transmit initially to test the ACLs and transmit rates and apply the Control Plane Policy in the output direction
B. Set the conform-action and exceed-action to transmit initially to test the ACLs and transmit rates and apply the Control Plane Policy in the input direction
C. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and apply the Control Plane Policy m the input direction
D. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and apply the Control Plane Policy m the output direction

Answer: B

NEW QUESTION 339
- (Exam Topic 2)
Refer to the exhibit.



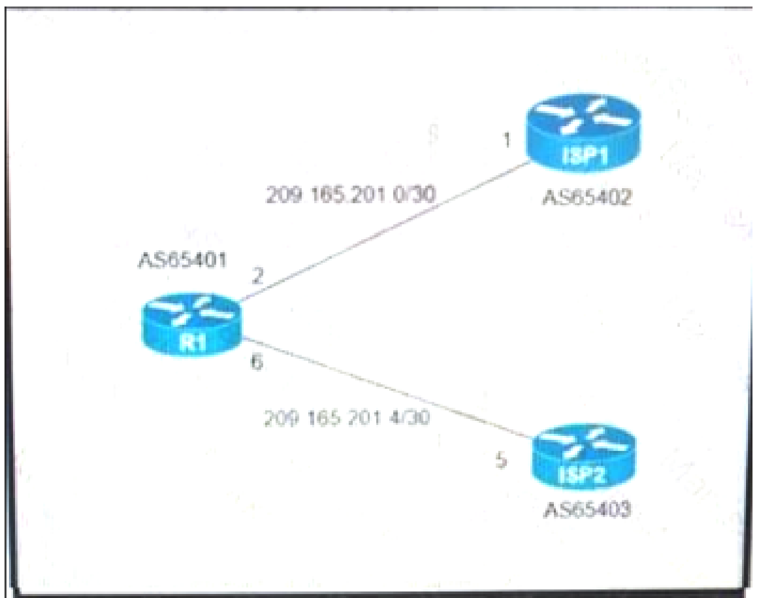
```
R1
ip prefix-list ccnpl seq 5 permit 10.1.48.0/24 le 24
ip prefix-list ccnp2 seq 5 permit 10.1.80.0/24 le 32
ip prefix-list ccnp3 seq 5 permit 10.1.64.0/24 le 24

route-map ospf-to-eigrp permit 10
   match ip address prefix-list ccnpl
   set tag 30
route-map ospf-to-eigrp permit 20
   match ip address prefix-list ccnp2
   set tag 20
route-map ospf-to-eigrp permit 30
   match ip address prefix-list ccnp3
   set tag 10
```

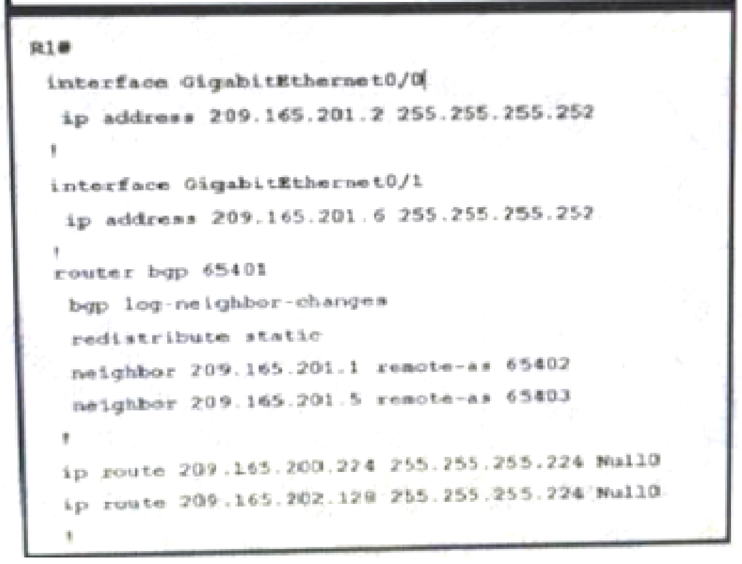
An engineer wanted to set a tag of 30 to route 10 1.80.65/32 but it failed How is the issue fixed?

A. Modify route-map ospf-to-eigrp permit 30 and match prefix-list ccnp2.
B. Modify route-map ospf-to-eigrp permit 10 and match prefix-list ccnp2.
C. Modify prefix-list ccnp3 to add 10.1.64.0/20 le 24
D. Modify prefix-list ccnp3 to add 10.1.64.0/20 ge 32

Answer: B

NEW QUESTION 340
- (Exam Topic 2)
Refer to the exhibit.

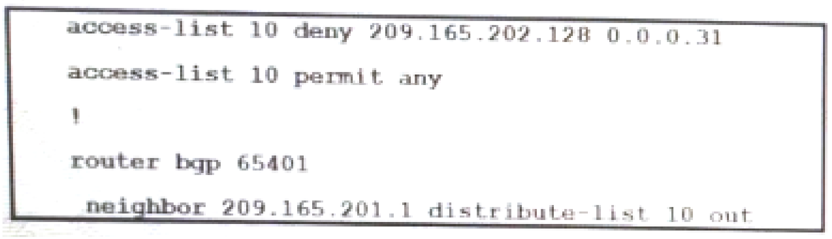




```
R1#
 interface GigabitEthernet0/0
  ip address 209.165.201.2 255.255.255.252
 !
 interface GigabitEthernet0/1
  ip address 209.165.201.6 255.255.255.252
 !
 router bgp 65401
  bgp log-neighbor-changes
  redistribute static
  neighbor 209.165.201.1 remote-as 65402
  neighbor 209.165.201.5 remote-as 65403
 !
 ip route 209.165.200.224 255.255.255.224 Null10
 ip route 209.165.202.128 255.255.255.224 Null10
 !
```

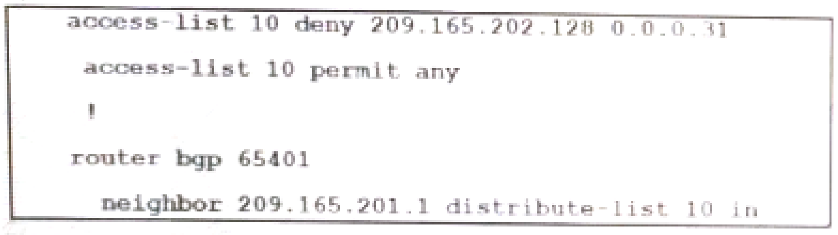
A company with autonomous system number AS65401 has obtained IP address block 209.165.200.224/27 fro, ARIN. The company needed more IP addresses and was assigned block 209.165.202.128/27 from ISP2. An engineer is ISP1 reports they are receiving ISP2 routes from AS65401. Which configuration onR1 resolves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

A)



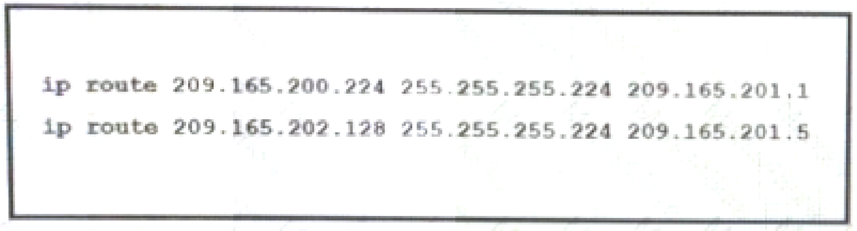
```
access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
 neighbor 209.165.201.1 distribute-list 10 out
```

B)



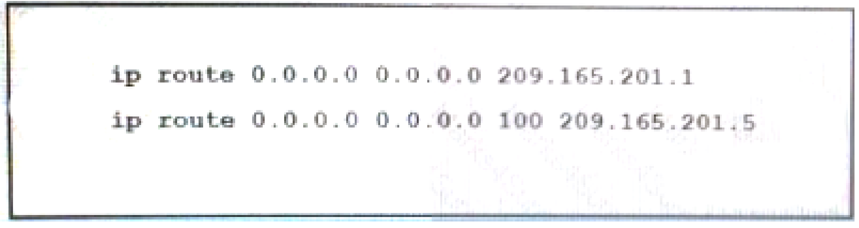
```
access-list 10 deny 209.165.202.128 0.0.0.31
 access-list 10 permit any
 !
router bgp 65401
  neighbor 209.165.201.1 distribute-list 10 in
```

C)



```
ip route 209.165.200.224 255.255.255.224 209.165.201.1
ip route 209.165.202.128 255.255.255.224 209.165.201.5
```

D)



```
ip route 0.0.0.0 0.0.0.0 209.165.201.1
ip route 0.0.0.0 0.0.0.0 100 209.165.201.5
```

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

Answer: A

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

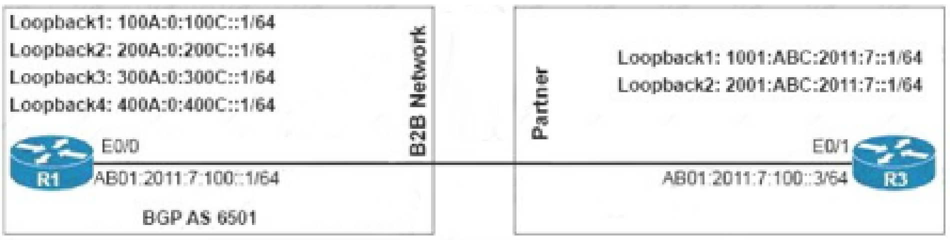
NEW QUESTION 342
- (Exam Topic 2)
What is the minimum time gap required by the local system before putting a BFD control packet on the wire?

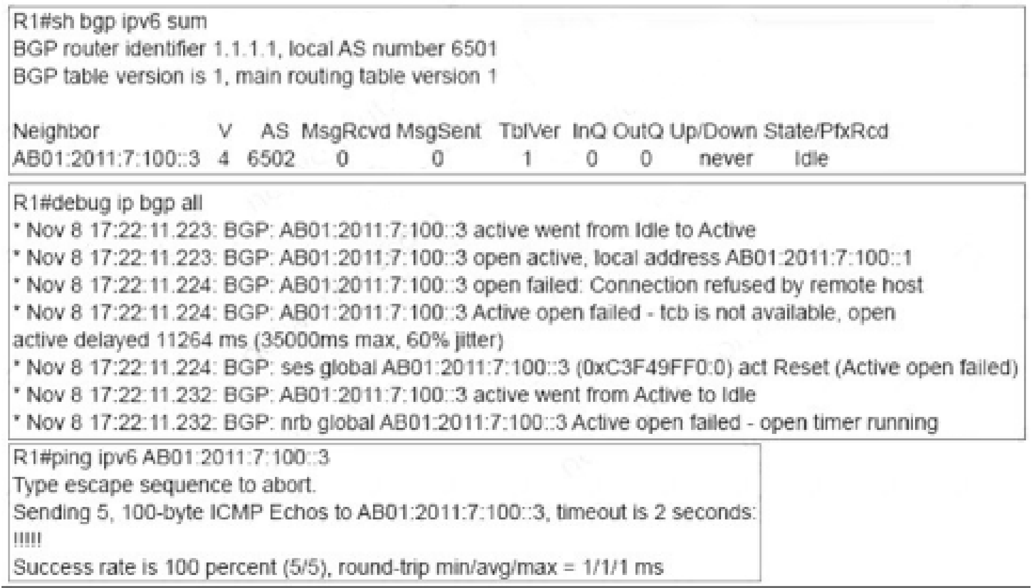
A. Detect Mult
B. Required Min Echo RX Interval
C. Desired Min TX Interval
D. Required Min RX Interval

Answer: C

Explanation:
Desired Min TX Interval: This is the minimum interval, in microseconds, that the local system would like to use when transmitting BFD Control packets, less any jitterapplied. The value zero is reserved.
Required Min Echo RX Interval: This is the minimum interval, in microseconds, between received BFD Echo packets that this system is capable of supporting, less anyjitter applied by the sender. If this value is zero, the transmitting system does not support the receipt of BFD Echo packets.
Reference: https://tools.ietf.org/html/rfc5880

NEW QUESTION 345
- (Exam Topic 2)
Refer to the exhibit.


Loopback1: 100A:0:100C::1/64
Loopback2: 200A:0:200C::1/64
Loopback3: 300A:0:300C::1/64
Loopback4: 400A:0:400C::1/64
B2B Network
R1
E0/0
AB01:2011:7:100::1/64
BGP AS 6501
Partner
Loopback1: 1001:ABC:2011:7::1/64
Loopback2: 2001:ABC:2011:7::1/64
E0/1
AB01:2011:7:100::3/64
R3



```
R1#sh bgp ipv6 sum
BGP router identifier 1.1.1.1, local AS number 6501
BGP table version is 1, main routing table version 1

Neighbor            V    AS  MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
AB01:2011:7:100::3  4  6502     0        0        1      0    0    never     Idle
```

```
R1#debug ip bgp all
* Nov 8 17:22:11.223: BGP: AB01:2011:7:100::3 active went from Idle to Active
* Nov 8 17:22:11.223: BGP: AB01:2011:7:100::3 open active, local address AB01:2011:7:100::1
* Nov 8 17:22:11.224: BGP: AB01:2011:7:100::3 open failed: Connection refused by remote host
* Nov 8 17:22:11.224: BGP: AB01:2011:7:100::3 Active open failed - tcb is not available, open
active delayed 11264 ms (35000ms max, 60% jitter)
* Nov 8 17:22:11.224: BGP: ses global AB01:2011:7:100::3 (0xC3F49FF0:0) act Reset (Active open failed)
* Nov 8 17:22:11.232: BGP: AB01:2011:7:100::3 active went from Active to Idle
* Nov 8 17:22:11.232: BGP: nrb global AB01:2011:7:100::3 Active open failed - open timer running
```

```
R1#ping ipv6 AB01:2011:7:100::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to AB01:2011:7:100::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

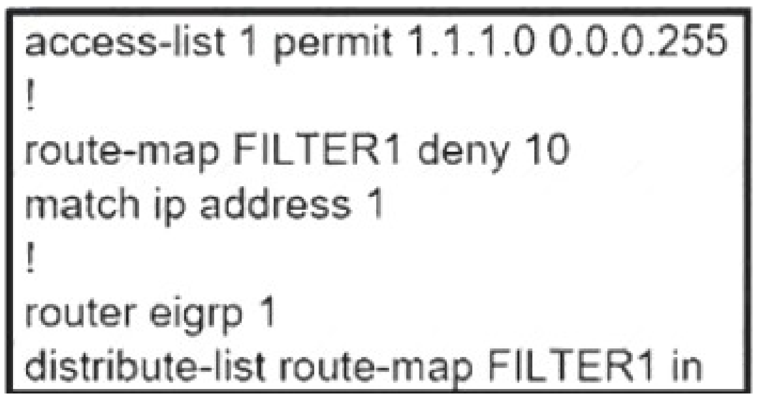
An engineer configured BGP between routers R1 and R3 The BOP peers cannot establish neighbor adjacency to be able to exchange routes. Which configuration resolves this issue?

A. R3router bgp 6502 address-family ipv6neighbor AB01:2011:7:100::1 activate
B. R1router bgp 6501 address-family ipv6neighbor AB01:2011:7:100;:3 activate
C. R3router bgp 6502neighbor AB01:2011:7:100::1 ebgp-muttlhop 255
D. R1router bgp 6501 neighborAB01:2011:7:100::3ebgp-multihop255

Answer: A

Explanation:
From the output, we learned that R1 was trying to establish BGP neighbor relationship with R3 but failed. Both of them were using physical interface to establish neighbor relationship so we don’t need the “… ebgp-multihop” command here. The only reasonable answer is R3 has not been configured to activate BGP neighbor relationship with R1.

NEW QUESTION 347
- (Exam Topic 2)
Refer to the exhibit.



```
access-list 1 permit 1.1.1.0 0.0.0.255
!
route-map FILTER1 deny 10
match ip address 1
!
router eigrp 1
distribute-list route-map FILTER1 in
```

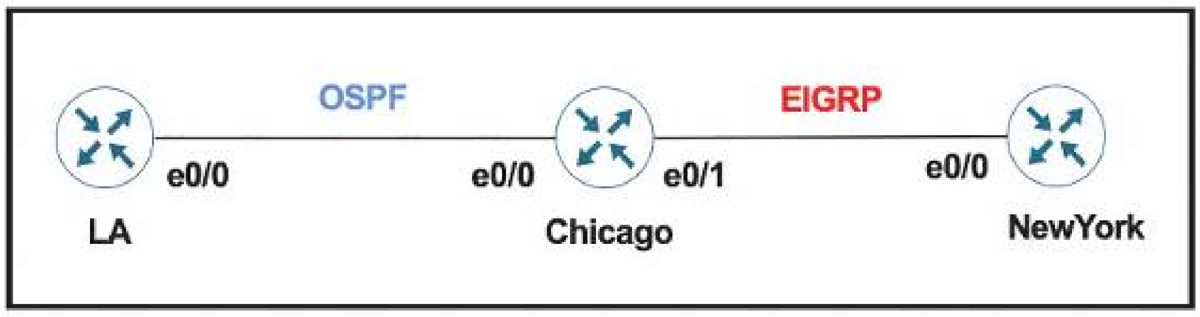
Which action restores the routes from neighbors while still filtering 1.1.1.0/24?

A. Add a second line in the access list to permit any.
B. Modify the route map to permit the access list instead of deny it
C. Modify the access list to deny instead of permit it.
D. Add a second sequence in the route map permit 20

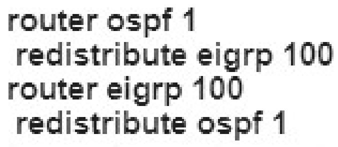
Answer: D

NEW QUESTION 350

- (Exam Topic 2)
Refer to the exhibit.



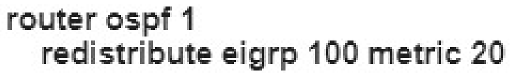
The network administrator must mutually redistribute routes at the Chicago router to the LA and NewYork routers. The configuration of the Chicago router is this:



```
router ospf 1
 redistribute eigrp 100
router eigrp 100
 redistribute ospf 1
```

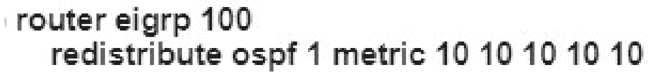
After the configuration, the LA router receives all the NewYork routes, but NewYork router does not receive any LA routes. Which set of configurations fixes the problem on the Chicago router?

A)



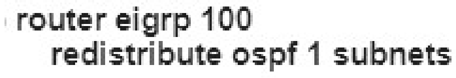
```
router ospf 1
    redistribute eigrp 100 metric 20
```

B)



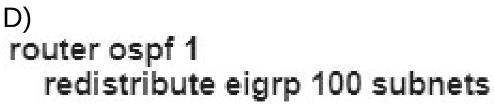
```
router eigrp 100
    redistribute ospf 1 metric 10 10 10 10 10
```

C)



```
router eigrp 100
    redistribute ospf 1 subnets
```

D)



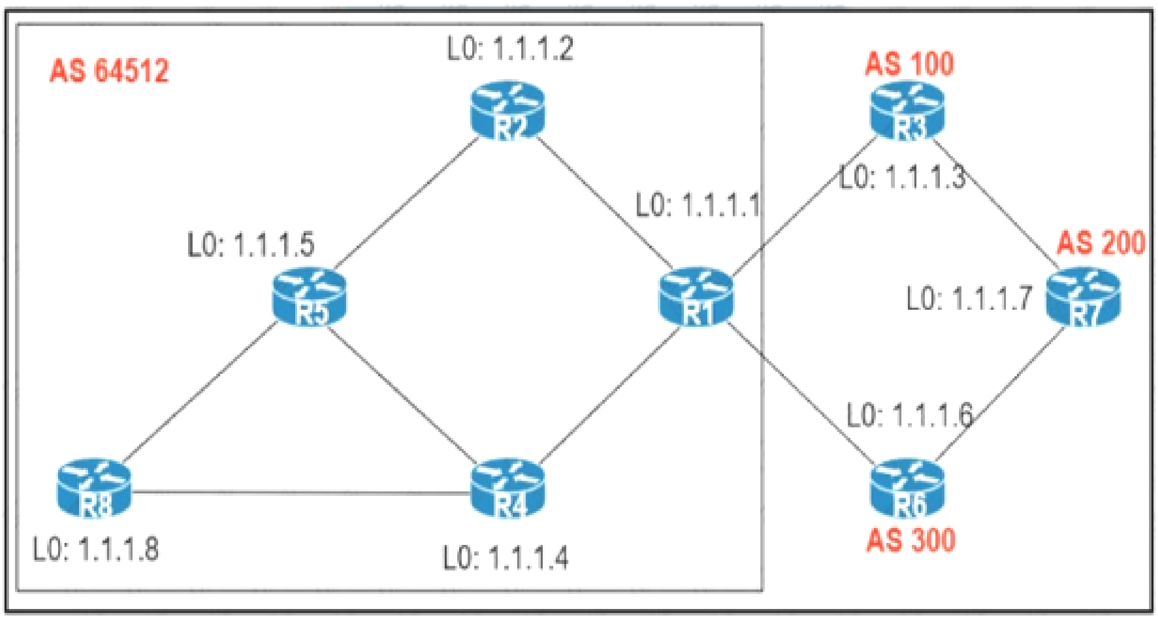
```
router ospf 1
    redistribute eigrp 100 subnets
```

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

Answer: B

Explanation:
"LA router receives all the NewYork routes but it does not receive any LA routes" because when redistrubuting into EIGRP, we must configure the default metric.

NEW QUESTION 355
- (Exam Topic 2)
Exhibit:



An engineer configured R2 and R5 as route reflectors and noticed that not all routes are sent to R1 to advertise to the eBGP peers. Which iBGP routers must be configured as route reflectors to advertise all routes to restore reachability across all networks?

A. R1 and R4
B. R1 and R5
C. R4 and R5
D. R2 and R5

Answer: C

Explanation:
When R2 & R5 are route reflectors (RRs), routes from R4 & R8 are advertised to R5 and R5 advertises to R2. But R2 would drop them as R2 is also a RR. Therefore some routes are missing on R1 to advertise to eBGP peers.
Good reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2015/pdf/TECRST-2310.pdf
Route reflectors (RR) must be fully iBGP meshed so we cannot configure RR on both R1 and R5.

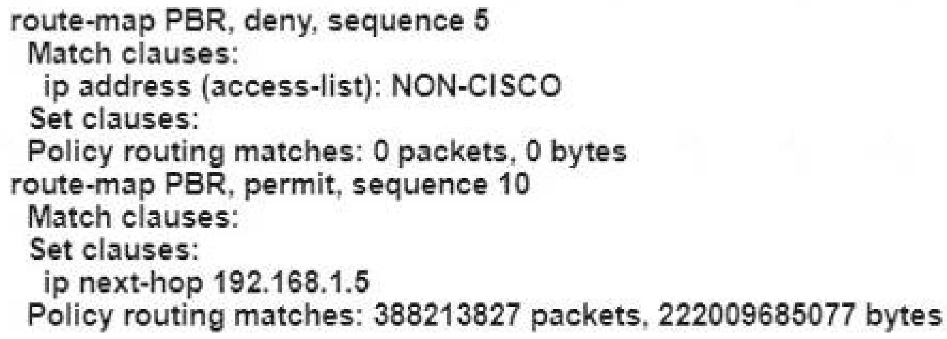
We should choose routers at the center of the topology RRs, in this case R4 & R5.

NEW QUESTION 358
- (Exam Topic 2)
An engineer configured two routers connected to two different service providers using BGP with default attributes. One of the links is presenting high delay, which causes slowness in the network. Which BGP attribute must the engineer configure to avoid using the high-delay ISP link if the second ISP link is up?

A. LOCAL_PREF
B. MED
C. WEIGHT
D. AS-PATH

Answer: A

NEW QUESTION 362
- (Exam Topic 2)
An engineer configured access list NON-CISCO in a policy to influence routes



```
route-map PBR, deny, sequence 5
  Match clauses:
    ip address (access-list): NON-CISCO
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map PBR, permit, sequence 10
  Match clauses:
  Set clauses:
    ip next-hop 192.168.1.5
  Policy routing matches: 388213827 packets, 222009685077 bytes
```

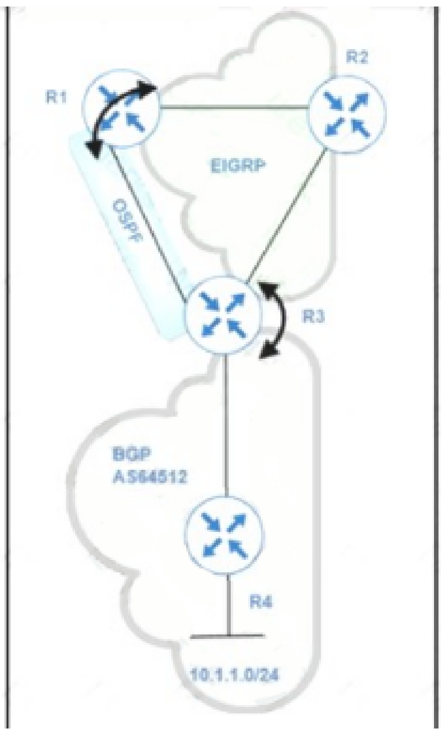
What are the two effects of this route map configuration? (Choose two.)

A. Packets are not evaluated by sequence 10.
B. Packets are evaluated by sequence 10.
C. Packets are forwarded to the default gateway.
D. Packets are forwarded using normal route lookup.
E. Packets are dropped by the access list.

Answer: BC

Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/47121-pbr-cmds-ce.html

NEW QUESTION 366
- (Exam Topic 2)
Refer to exhibit.



Routing protocols are mutually redistributed on R3 and R1. Users report intermittent connectivity to services hosted on the 10.1.1.0/24 prefix. Significant routing update changes are noticed on R3 when the show ip route profile command is run. How must the services be stabilized?

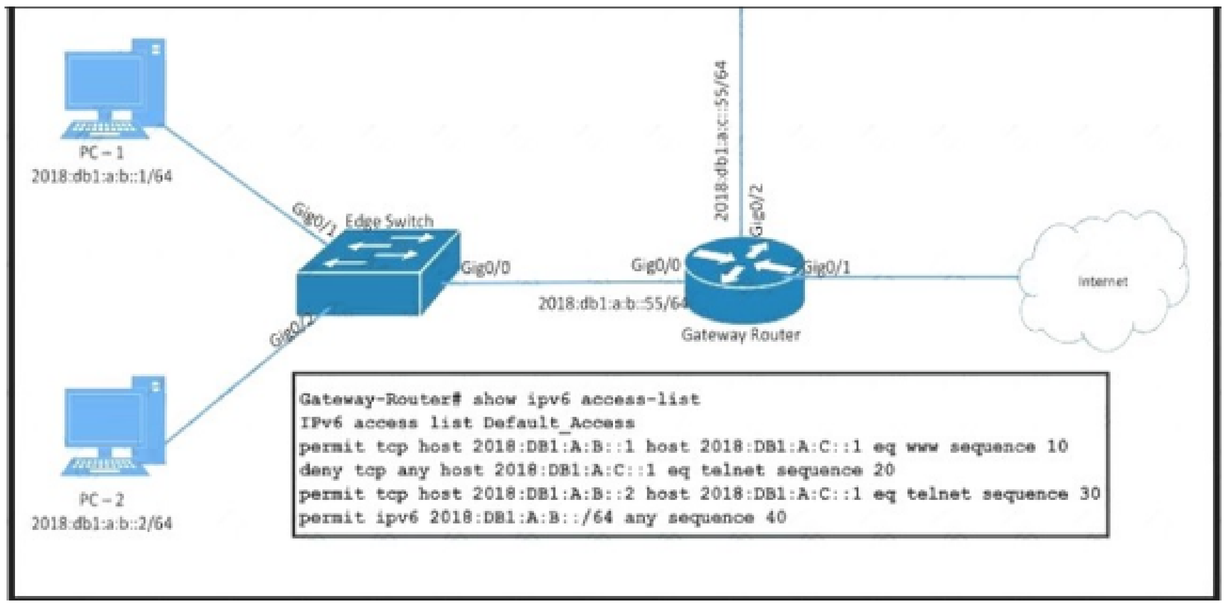
A. The issue with using BGP must be resolved by using another protocol and redistributing it into EIGRP on R3
B. The routing loop must be fixed by reducing the admin distance of iBGP from 200 to 100 on R3
C. The routing loop must be fixed by reducing the admin distance of OSPF from 110 to 80 on R3
D. The issue with using iBGP must be fixed by running eBGP between R3 and R4

Answer: B

Explanation:
After redistribution, R3 learns about network 10.1.1.0/24 via two paths:+ Internal BGP (IBGP): advertised from R4 with AD of 200 (and metric of 0)+ OSPF: advertised from R1 with AD of 110 (O E2) (and metric of 20)Therefore R3 will choose the path with the lower AD via OSPF
But this is a looped path which is received from R3 -> R2 -> R1 -> R3. So when the advertised route from R4 is expired, the looped path is also expired soon and R3 willreinstall the main path from R4. This is the cause of intermittent connectivity.In order to solve this issue, we can lower the AD of iBGP to a value which is

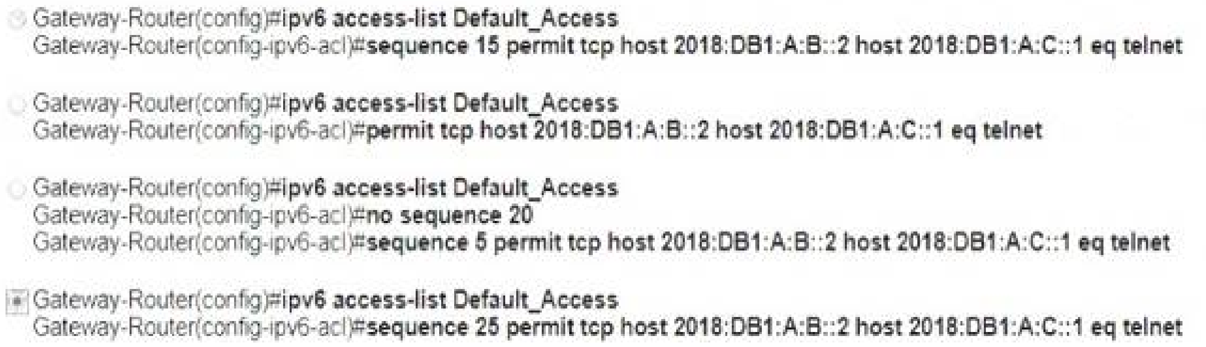
lower than 110 so that it is preferred over OSPF-advertised route.

NEW QUESTION 370
- (Exam Topic 2)
Refer to the exhibit.



```
Gateway-Router# show ipv6 access-list
IPv6 access list Default_Access
permit tcp host 2018:DB1:A:B::1 host 2018:DB1:A:C::1 eq www sequence 10
deny tcp any host 2018:DB1:A:C::1 eq telnet sequence 20
permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet sequence 30
permit ipv6 2018:DB1:A:B::/64 any sequence 40
```

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



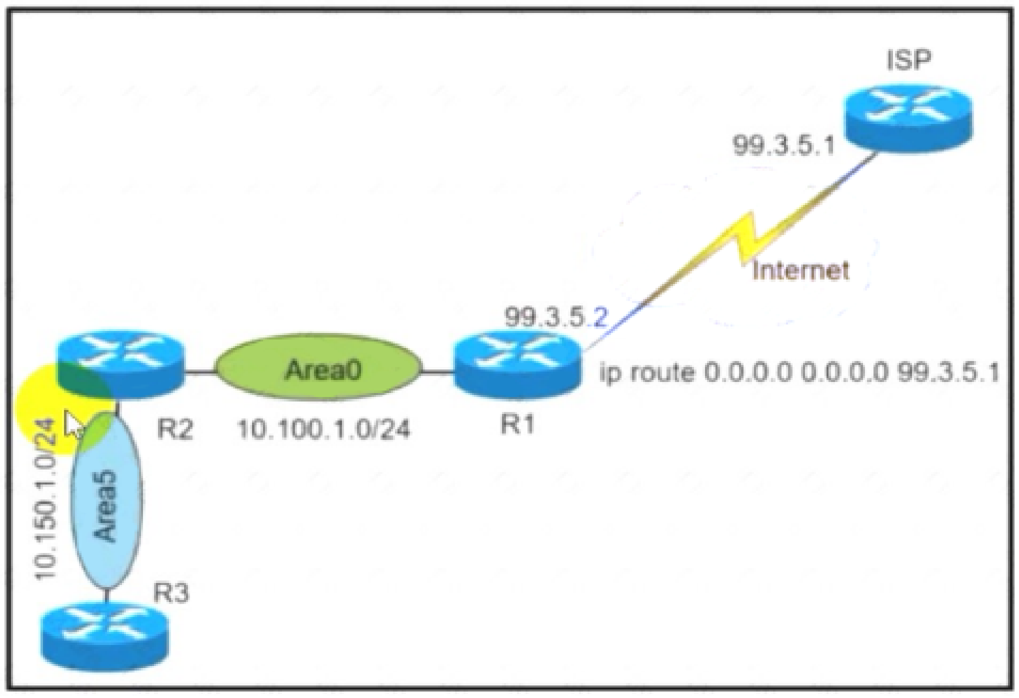
```
○ Gateway-Router(config)#ipv6 access-list Default_Access
  Gateway-Router(config-ipv6-acl)#sequence 15 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet

○ Gateway-Router(config)#ipv6 access-list Default_Access
  Gateway-Router(config-ipv6-acl)#permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet

○ Gateway-Router(config)#ipv6 access-list Default_Access
  Gateway-Router(config-ipv6-acl)#no sequence 20
  Gateway-Router(config-ipv6-acl)#sequence 5 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet

● Gateway-Router(config)#ipv6 access-list Default_Access
  Gateway-Router(config-ipv6-acl)#sequence 25 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet
```

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

Answer: A

Explanation:
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 375
- (Exam Topic 2)



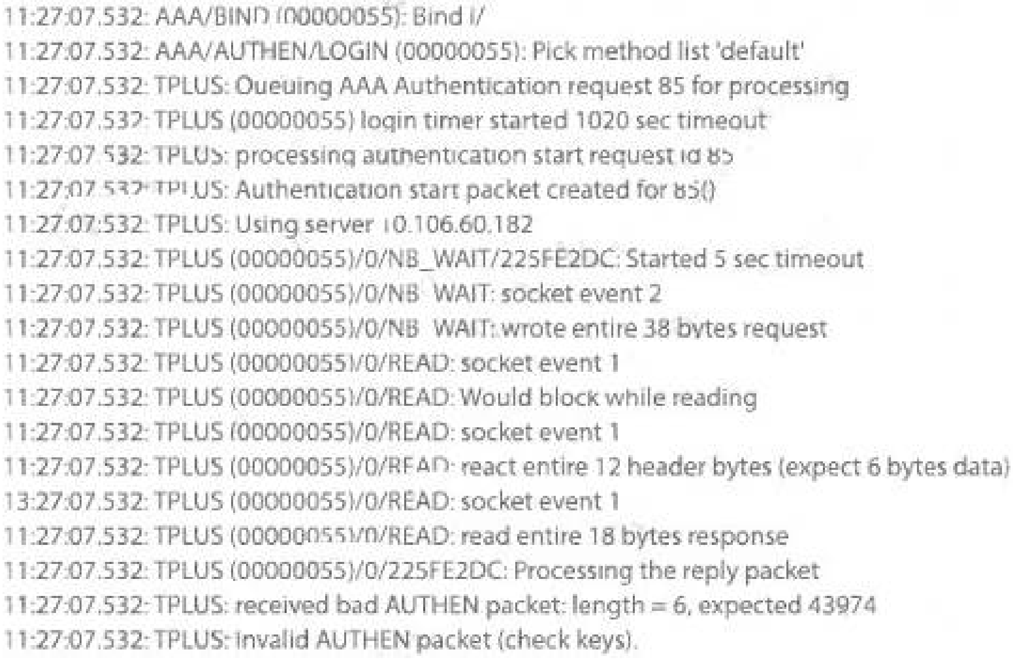
Refer to the exhibit. A network administrator redistributed the default static route into OSPF toward all internal routers to reach to Internet. Which set of commands restores reachability to the Internet by internal routers?

A. router ospf 1default-information originate
B. router ospf 1network 0.0.0.0 0.0.0.0 area 0
C. router ospf 1redistribute connected 0.0.0.0
D. router ospf 1redistribute static subnets

Answer: A

NEW QUESTION 378

- (Exam Topic 2)
Exhibit:



```
11:27:07.532: AAA/BIND (00000055): Bind i/
11:27:07.532: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
11:27:07.532: TPLUS: Queuing AAA Authentication request 85 for processing
11:27:07.532: TPLUS (00000055) login timer started 1020 sec timeout
11:27:07.532: TPLUS: processing authentication start request id 85
11:27:07.532: TPLUS: Authentication start packet created for 85()
11:27:07:532: TPLUS: Using server 10.106.60.182
11:27:07.532: TPLUS (00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
11:27:07.532: TPLUS (00000055)/0/NB WAIT: socket event 2
11:27:07.532: TPLUS (00000055)/0/NB WAIT: wrote entire 38 bytes request
11:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: Would block while reading
11:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: react entire 12 header bytes (expect 6 bytes data)
13:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: read entire 18 bytes response
11:27:07.532: TPLUS (00000055)/0/225FE2DC: Processing the reply packet
11:27:07.532: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
11:27:07.532: TPLUS: invalid AUTHEN packet (check keys).
```

Which action resolves the authentication problem?

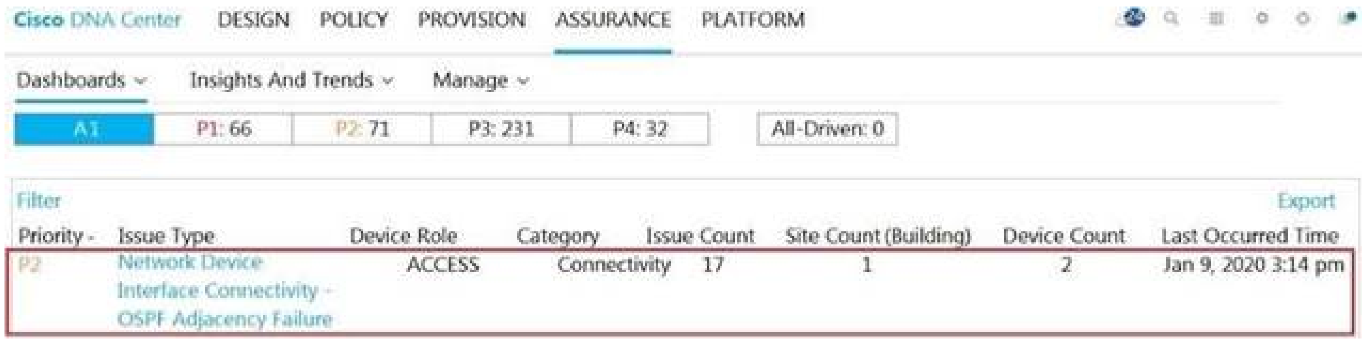
A. Configure the user name on the TACACS+ server
B. Configure the UDP port 1812 to be allowed on the TACACS+ server
C. Configure the TCP port 49 to be reachable by the router
D. Configure the same password between the TACACS+ server and router.

Answer: D

Explanation:

From the last line of the output, we notice that the result was “Invalid AUTHEN packet”. Therefore something went wrong with the username or password.
Reference:
https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-taca

NEW QUESTION 379
- (Exam Topic 2)
Refer to the exhibit.



Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Building)	Device Count	Last Occurred Time
P2	Network Device Interface Connectivity - OSPF Adjacency Failure	ACCESS	Connectivity	17	1	2	Jan 9, 2020 3:14 pm

A network administrator is using the DNA Assurance Dashboard panel to troubleshoot an OSPF adjacency that failed between Edge_NYC interface GigabitEthernet1/3 with Neighbor Edge_SNJ. The administrator observes that the neighborship is stuck in exstart state. How does the administrator fix this issue?

A. Configure to match the OSPF interface speed and duplex settings on both routers.
B. Configure to match the OSPF interface MTU settings on both routers.
C. Configure to match the OSPF interface unique IP address and subnet mask on both routers.
D. Configure to match the OSPF interface network types on both routers.

Answer: B

Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13684-12.html

NEW QUESTION 381
- (Exam Topic 2)
In which two ways does the IPv6 First-Hop Security Binding Table operate? (Choose two.)

A. by IPv6 routing protocols to securely build neighborships without the need of authentication
B. by the recovery mechanism to recover the binding table in the event of a device reboot
C. by IPv6 HSRP to make sure neighbors are authenticated before being used as gateways
D. by various IPv6 guard features to validate the data link layer address
E. by storing hashed keys for IPsec tunnels for the built-in IPsec features

Answer: BD

Explanation:
Overview of the IPv6 First-Hop Security Binding Table
A database table of IPv6 neighbors connected to the device is created from information sources such as NDP snooping. This database, or binding table, is used by variousIPv6 guard features to validate the link-layer address (LLA), the IPv4 or IPv6 address, and the prefix binding of the neighbors to prevent spoofing and redirect attacks.
IPv6 First-Hop Security Binding Table Recovery MechanismThe IPv6 first-hop security binding table recovery mechanism enables the binding table to recover in the event of a device reboot.

Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-s/ip6-fhs-bind-table.html

NEW QUESTION 386
- (Exam Topic 1)
Which Cisco VPN technology can use multipoint tunnel, resulting in a single GRE tunnel interface on the hub, to support multiple connections from multiple spoke devices?

A. DMVPN
B. GETVPN
C. Cisco Easy VPN
D. FlexVPN

Answer: A

NEW QUESTION 390
- (Exam Topic 1)
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 manages the import and export of routes between two or more VRF instances
C. It enables multicast distribution for VRF-Lite setups to enhance EGP routing protocol capabilities
D. It enables multicast distribution for VRF-Lite setups to enhance IGP routing protocol capabilities

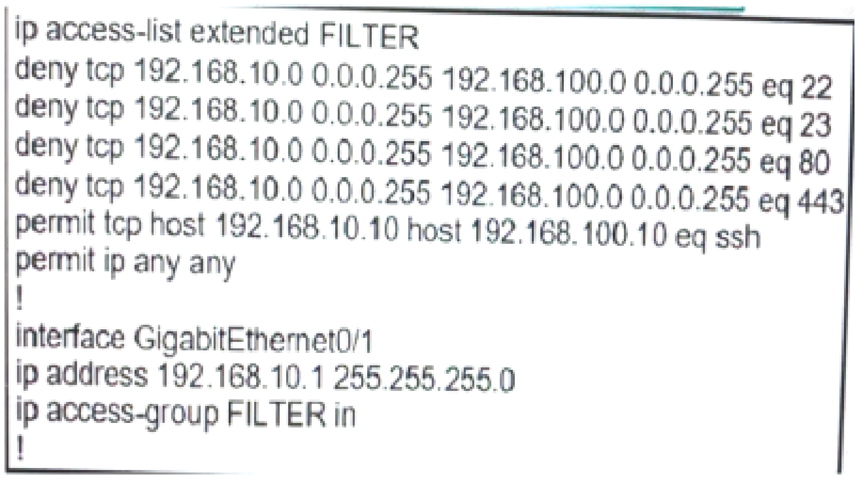
Answer: A

NEW QUESTION 393
- (Exam Topic 1)
An engineer is trying to copy an IOS file from one router to another router by using TFTP. Which two actions are needed to allow the file to copy? (Choose two.)

A. Copy the file to the destination router with the copy tftp: flash: command
B. Enable the TFTP server on the source router with the tftp-server flash: <filename> command
C. TFTP is not supported in recent IOS versions, so an alternative method must be used
D. Configure a user on the source router with the username tftp password tftp command
E. Configure the TFTP authentication on the source router with the tftp-server authentication local command

Answer: AB

NEW QUESTION 395
- (Exam Topic 1)
Refer to the exhibit.



```
ip access-list extended FILTER
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 22
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 23
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 80
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 443
permit tcp host 192.168.10.10 host 192.168.100.10 eq ssh
permit ip any any
!
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip access-group FILTER in
!
```

The ACL is placed on the inbound Gigabit 0/1 interface of the router. Host 192.168.10.10 cannot SSH to host 192.168.100.10 even though the flow is permitted. Which action resolves the issue without opening full access to this router?

A. Move the SSH entry to the beginning of the ACL
B. Temporarily move the permit ip any any line to the beginning of the ACL to see if the flow works
C. Temporarily remove the ACL from the interface to see if the flow works
D. Run the show access-list FILTER command to view if the SSH entry has any hit statistic associated with it

Answer: A

NEW QUESTION 399
- (Exam Topic 1)
Which configuration adds an IPv4 interface to an OSPFv3 process in OSPFv3 address family configuration?

A. Router ospf3 1 address-family ipv4
B. Router(config-router)#ospfv3 1 ipv4 area 0
C. Router(config-if)#ospfv3 1 ipv4 area 0
D. Router ospfv3 1 address-family ipv4 unicast

Answer: C

Explanation:
Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-xe-3s-book/ip6-route-os

NEW QUESTION 401

......