

# Cisco

## Exam Questions 300-410

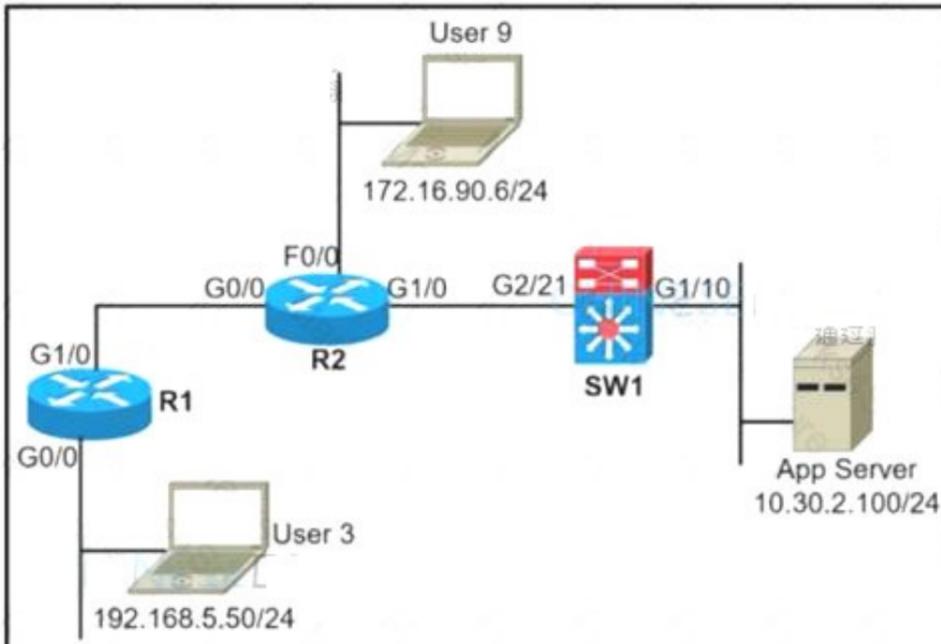
Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)



**NEW QUESTION 1**

- (Exam Topic 3)

Refer to the exhibit.



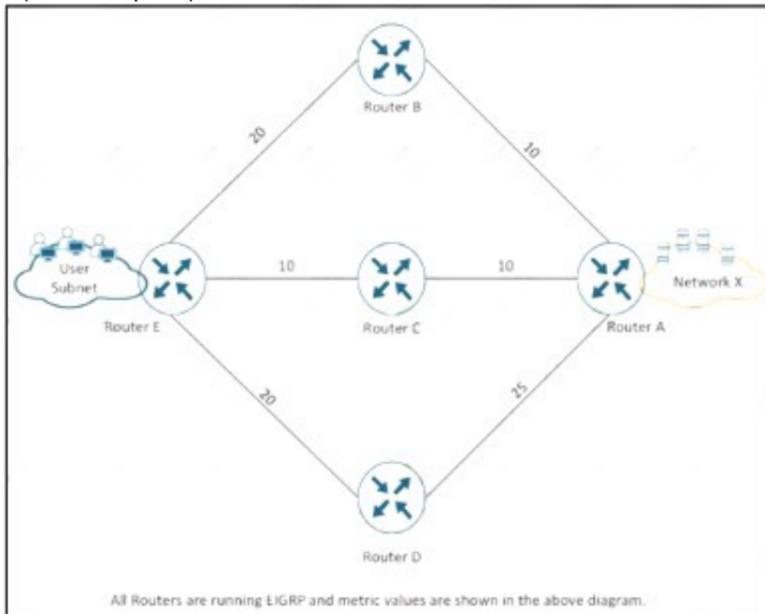
A network administrator must block ping from user 3 to the App Server only. An inbound standard access list is applied to R1 interface G0/0 to block ping. The network administrator was notified that user 3 cannot even ping user 9 anymore. Where must the access list be applied in the outgoing direction to resolve the issue?

- A. R2 interface G1/0
- B. R2 interface G0/0
- C. SW1 interface G1/10
- D. SW1 interface G2/21

**Answer: D**

**NEW QUESTION 2**

- (Exam Topic 3)



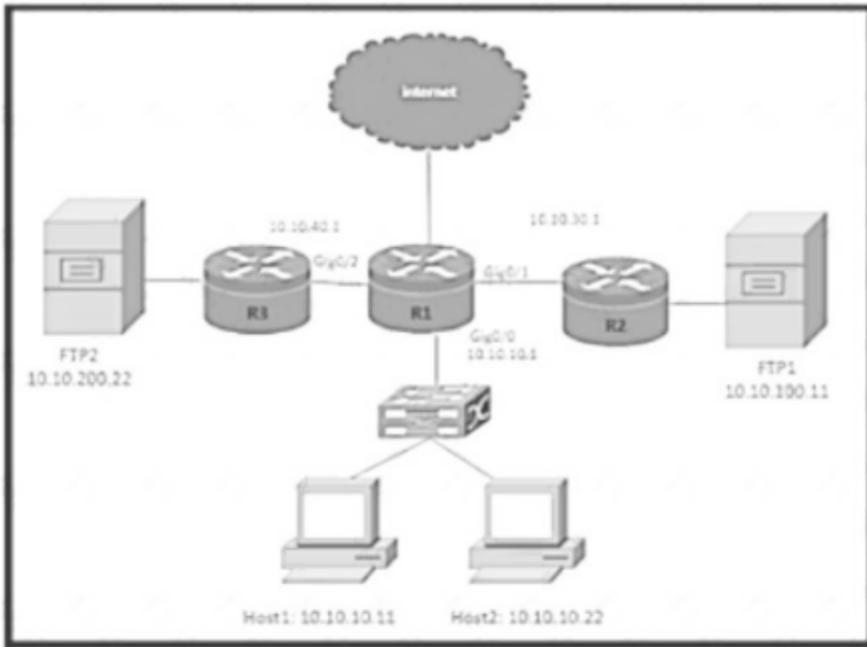
Refer to the exhibit. The IT manager received reports from users about slow application through network x. which action resolves the issue?

- A. Use the variance 2 command to enable load balancing.
- B. Increase the bandwidth from the service provider.
- C. Move the servers into the users subnet.
- D. Upgrade the IOS on router E.

**Answer: A**

**NEW QUESTION 3**

- (Exam Topic 3)



Refer to the exhibit. The R1 routing table has the prefixes for the FTP1 and FTP2 file servers. A network engineer must configure the R1 with these requirements:

- > Host1 must use the FTP1 fileserver.
- > Host2 must use the FTP2 fileserver.

Which configuration meets the requirement on R1?

A)

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.40.1
route-map PBR_FTP permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.30.1
!
ip local policy route-map PBR_FTP
```

B)

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.40.1
!
ip local policy route-map PBR_FTP
```

C)

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.40.1
!
interface GigabitEthernet 0/0
 ip policy route-map PBR_FTP
```

D)

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 any
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 any
route-map PBR_FTP permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.40.1
!
interface GigabitEthernet 0/0
 ip policy route-map PBR_FTP
```

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

**Answer: C**

#### NEW QUESTION 4

- (Exam Topic 3)

- A. Redistribute the static metric in EIGRP.
- B. Add the eigrp stub connected static command.
- C. Redistribute the connected metric in EIGRP.
- D. Remove the eigrp stub connected command.

**Answer: B**

#### NEW QUESTION 5

- (Exam Topic 3)

An engineer configured VRF-Lite on a router for VRF blue and VRF red. OSPF must be enabled on each VRF to peer to a directly connected router in each VRF. Which configuration forms OSPF neighbors over the network 10.10.10.0/28 for VRF blue and 192.168.0.0/30 for VRF red?

- router ospf 1 vrf blue
  - network 10.10.10.0 0.0.0.15 area 0
 router ospf 2 vrf red
  - network 192.168.0.0 0.0.0.3 area 0
- router ospf 1 vrf blue
  - network 10.10.10.0 0.0.0.240 area 0
 router ospf 2 vrf red
  - network 192.168.0.0 0.0.0.252 area 0
- router ospf 1 vrf blue
  - network 10.10.10.0 0.0.0.252 area 0
 router ospf 2 vrf red
  - network 192.168.0.0 0.0.0.240 area 0
- router ospf 1 vrf blue
  - network 10.10.10.0 0.0.0.3 area 0
 router ospf 2 vrf red
  - network 192.168.0.0 0.0.0.15 area 0

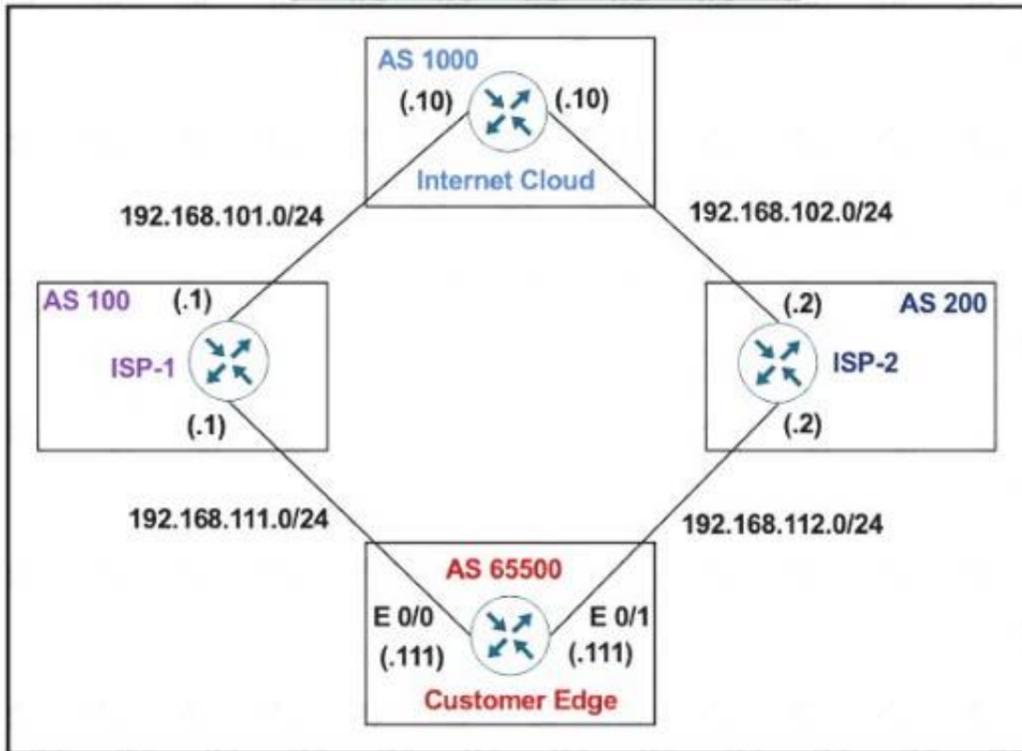
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

#### NEW QUESTION 6

- (Exam Topic 3)

Refer to the exhibit.



The Customer Edge router (AS 65500) wants to use AS 100 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 7**

- (Exam Topic 3)

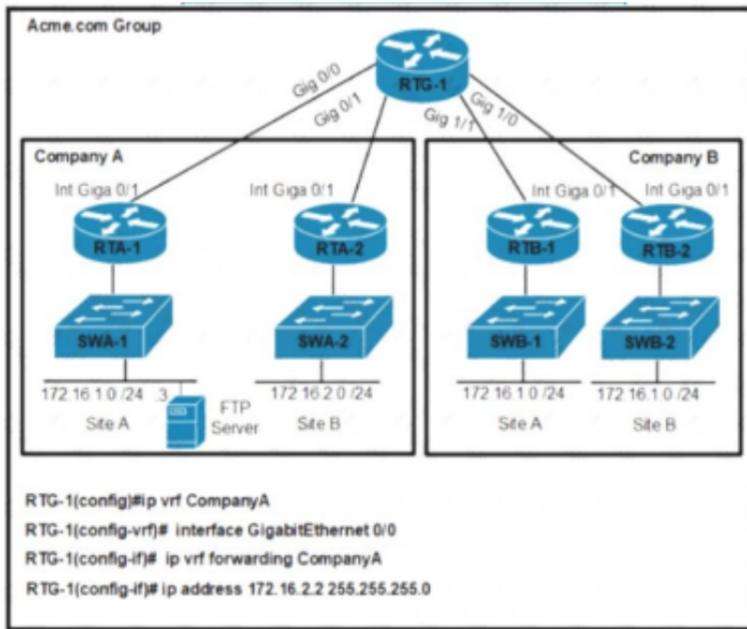
Which technique removes the outermost label of an MPLS-tagged packet before the packet is forwarded to an adjacent LER?

- A. label swap
- B. explicit-null
- C. label imposition
- D. PHP

**Answer: D**

**NEW QUESTION 8**

- (Exam Topic 3)



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 9**

- (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 10**

- (Exam Topic 3)

An engineer must override the normal routing behavior of a router for Telnet traffic that is destined to 10.10.10.10 from 10.10.1.0/24 via a next hop of 10.4.4.4. which is directly connected to the router that is connected to the 10.1.1.0/24 subnet Which configuration reroutes traffic according to this requirement?

```

access-list 100 permit tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23
|
route-map POLICY permit 10
match ip address 100
set ip next-hop recursive 10.4.4.4

access-list 100 permit tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23
|
route-map POLICY permit 10
match ip address 100
set ip next-hop 10.4.4.4
route-map POLICY permit 20

access-list 100 deny tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23
|
route-map POLICY permit 10
match ip address 100
set ip next-hop 10.4.4.4
route-map POLICY permit 20

access-list 100 permit tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23
|
route-map POLICY permit 10
match ip address 100
set ip next-hop recursive 10.4.4.4
route-map POLICY permit 20
    
```

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

**Answer: B**

**NEW QUESTION 10**

- (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 11**

- (Exam Topic 3)

```

R4#show ip route
Gateway of last resort is not set

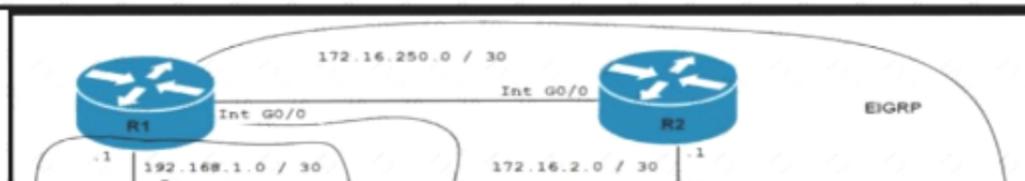
 172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
C   172.16.2.0/30 is directly connected, GigabitEthernet0/1
L   172.16.2.2/32 is directly connected, GigabitEthernet0/1
C   172.16.2.16/28 is directly connected, Loopback1
L   172.16.2.17/32 is directly connected, Loopback1
C   172.16.2.32/28 is 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

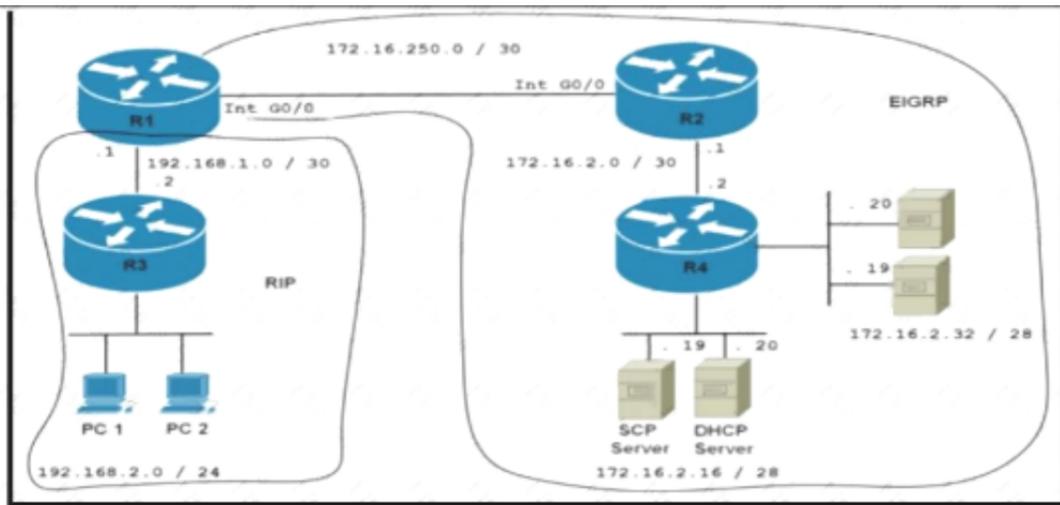
R3#sho ip route
Gateway of last resort is not set

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 13**

- (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 16**

- (Exam Topic 3)

```
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3,
changed state to up
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Ethernet0/0 from
LOADING to FULL, Loading Done
%BGP-3-NOTIFICATION: received from neighbor 192.168.200.1
active 6/7 (Connection Collision Resolution) 0 bytes
%BGP-5-NBR_RESET: Neighbor 192.168.200.1 active reset (BGP
Notification received)
%BGP-5-ADJCHANGE: neighbor 192.168.200.1 active Down BGP
Notification received
%BGP_SESSION-5-ADJCHANGE: neighbor 192.168.200.1 IPv4 Unicast
topology base removed from session BGP Notification received
```

Refer to the exhibit. 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. Configure the debug uptime option
- B. Configure the msec option
- C. Configure the timezone option
- D. Configure the tog uptime option

**Answer: D**

**NEW QUESTION 19**

- (Exam Topic 3)

```

R2#show ip eigrp topology 10.10.10.0 255.255.255.0
IP-EIGRP (AS 1): Topology entry for 10.10.10.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD
  is 256005120
  Routing Descriptor Blocks:
    10.20.20.3 (FastEthernet0/1), from 10.20.20.3, Send flag is
    0x0
    Composite metric is (256005120/256002560), Route is
    External
  Vector metric:
    Minimum bandwidth is 10 Kbit
    Total delay is 200 microseconds
    Reliability is 10/255
    Load is 10/255
    Minimum MTU is 10
    Hop count is 1
  External data:
    Originating router is 10.1.1.1
    AS number of route is 1
    External protocol is OSPF, external metric is 0
    Administrator tag is 0 (0x00000000)

R1#sh run | s eigrp
router eigrp 1
router-id 10.1.1.1
network 10.2.2.0 0.0.0.255
no auto-summary
        
```

Refer to the exhibit. An engineer configured router R3 to redistribute the prefix 10.10.10.0/24 from OSPF into EIGRP. R1 has no connectivity to the prefix. Which action enables receipt of prefixes on R1?

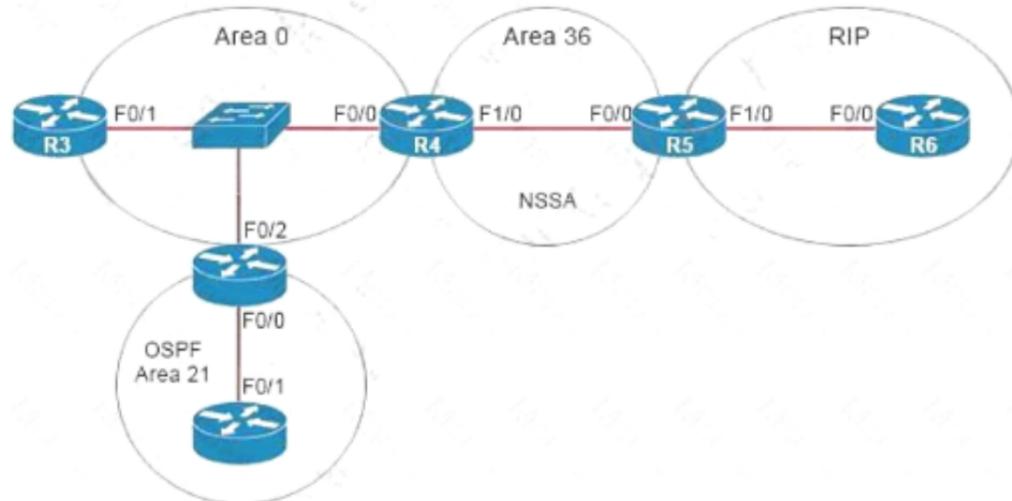
- A. R3 is advertising the 10.20.20.0/24 prefix with a TTL of 1, R3 must set the TTL to 2 for this prefix.
- B. R1 does not have a neighbor relationship with R2. The EIGRP process should be cleared on R1.
- C. Duplicate router IDs on R1 and R3, R1 should modify its router ID.
- D. R1 is not receiving the next-hop IP address of R3. R2 must enable the network 10.20.20.0/24 within EIGRP.

**Answer: B**

**NEW QUESTION 22**

- (Exam Topic 3)

Refer to the exhibit.



```

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

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

- A. R5(config)#router ospf 1 R5(config-router)#no area R5(config-router)#summary-address 172.16.0.0 255.255.252.0
- B. R4(config)#router ospf 99R4(config-router)#network 172.16.0.0 0.255.255.255 area 56R4(config-router)#area 56 range 172.16.0.0 255.255.255.0
- C. R4(config)#router ospf 1 R4(config-router)#no area R4(config-router)#summary-address 172.16.0.0 255.255.252.0
- D. R5(config)#router ospf 99R5(config-router)#network 172.16.0.0 0.255.255.255 area 56R5(config-router)#area 56 range 172.16.0.0 255.255.255.0

**Answer: A**

**Explanation:**

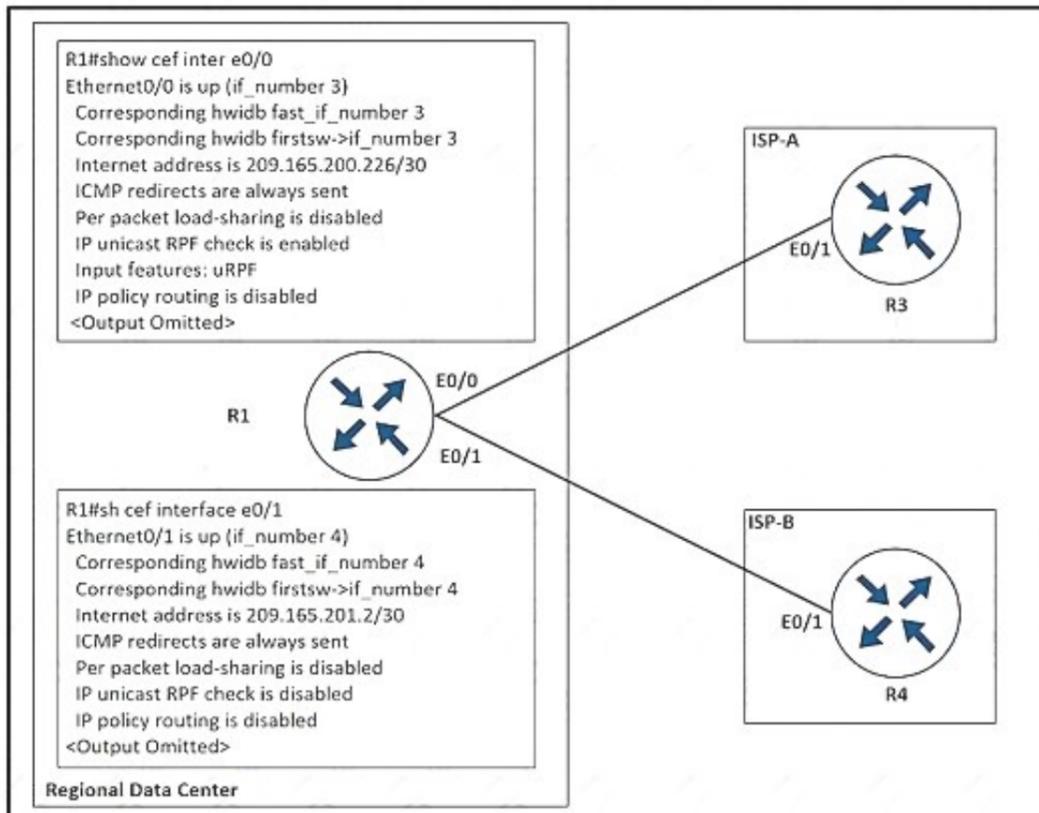
Area 36 is a NSSA so R5 is an ASBR so we can summarize external routes using the “summaryaddress” command. The command “area area-id range” can only be used on ABR so it is not correct.

The summarization must be done on the ASBR which is R5, not R4 so the correct answer must be started with “R5(config)#router ospf 1”.

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

**NEW QUESTION 26**

- (Exam Topic 3)



Refer to the exhibit. The company implemented uRPF to address an antispoofing attack. A network engineer received a call from the IT security department that the regional data center is under an IP attack Which configuration must be implemented on R1 to resolve this issue?

- interface ethernet0/0  
ip verify unicast reverse-path
- interface ethernet0/1  
ip verify unicast reverse-path
- interface ethernet0/1  
ip unicast RPF check reachable-via any allow-default allow-self-ping
- interface ethernet0/0  
ip unicast RPF check reachable-via any allow-default allow-self-ping

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

**Answer: B**

**NEW QUESTION 29**

- (Exam Topic 3)

Refer to the exhibit.

```

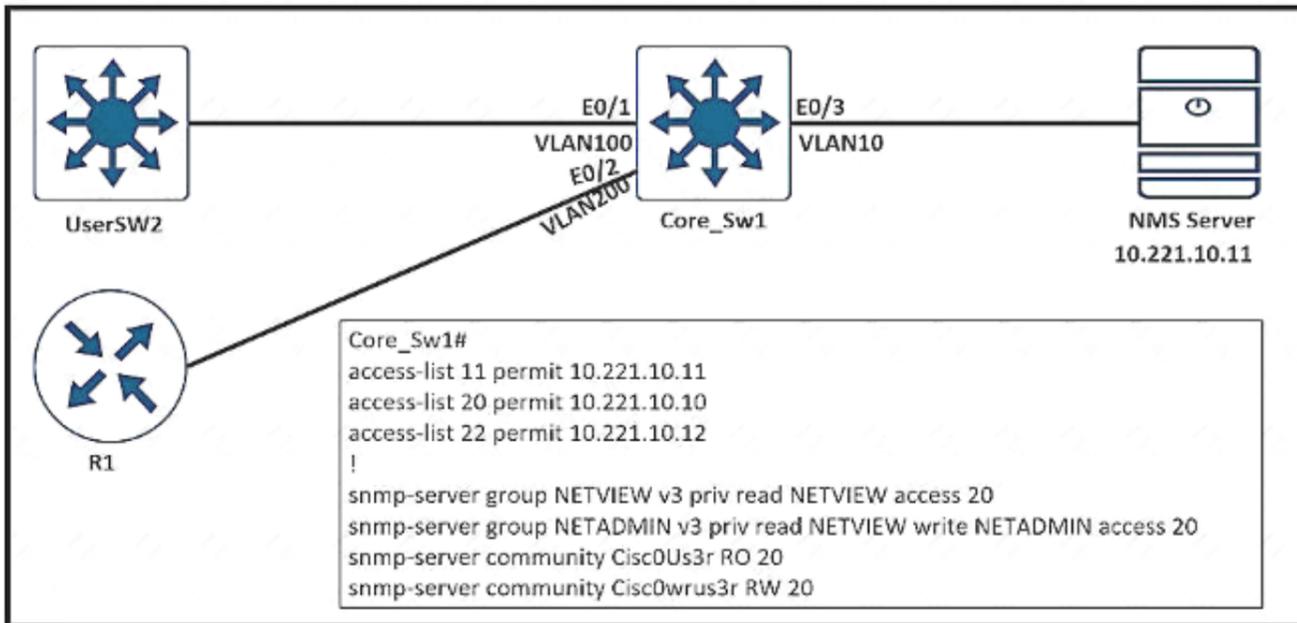
CPE# ping 10.0.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.4, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/1/1 ms
CPE# copy flash:/packages.conf tftp://10.0.2.4/
Address or name of remote host [10.0.2.4]?
Destination filename [packages.conf]?
%Error opening tftp://10.0.2.4/packages.conf (Undefined error)
    
```

The administrator is trying to overwrite an existing file on the TFTP server that was previously uploaded by another router. However, the attempt to update the file fails. Which action resolves this issue?

- A. Make the packages.conf file executable by all on the TFTP server
- B. Make the packages.conf file writable by all on the TFTP server
- C. Make sure to run the TFTP service on the TFTP server
- D. Make the TFTP folder writable by all on the TFTP server

**Answer: B**

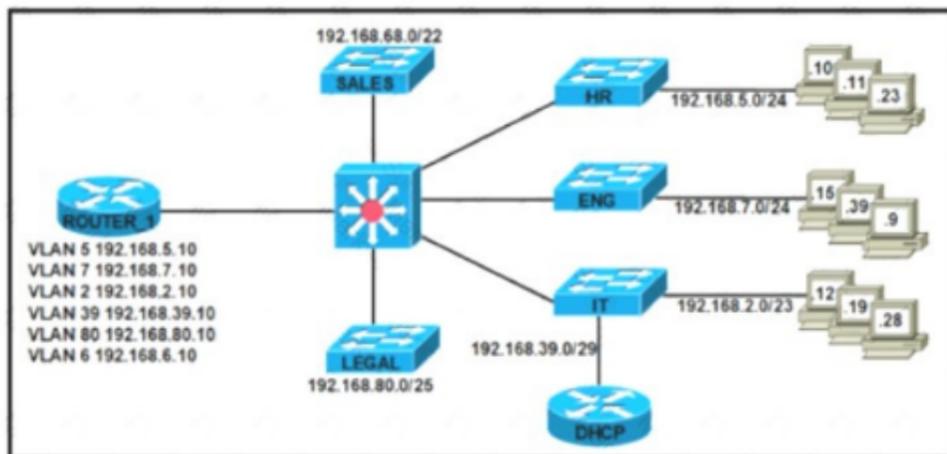
**NEW QUESTION 31**  
 - (Exam Topic 3)



- A. access-list 20 permit 10.221.10.12
- B. snmp-server group NETVIEW v2c priv read NETVIEW access 20
- C. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22
- D. access-list 20 permit 10.221.10.11

**Answer: D**

**NEW QUESTION 33**  
 - (Exam Topic 3)



Refer to the exhibit. After an engineer configured a new Cisco router as a DHCP server, users reported two primary issues:

- > Devices in the HR subnet have intermittent connectivity problems.
- > Workstations in the LEGAL subnet cannot obtain IP addresses.

Which configurations must the engineer apply to ROUTER\_1 to restore connectivity for the affected devices?

- interface GigabitEthernet0/0.5  
 encapsulation dot1Q 5  
 ip address 192.168.5.10 255.255.255.0  
 ip helper-address 192.168.39.100  
 !  
 interface GigabitEthernet0/0.80  
 encapsulation dot1Q 80  
 ip address 192.168.80.10 255.255.255.128  
 ip helper-address 192.168.39.100  
 !  
 ip dhcp excluded-address 192.168.5.1 192.168.5.10  
 ip dhcp excluded-address 192.168.80.1 192.168.80.10  
 !  
 ip dhcp pool LEGAL  
 network 192.168.80.0 255.255.255.128  
 default-router 192.168.80.10  
 !  
 ip dhcp pool HR  
 network 192.168.5.0 255.255.255.0  
 default-router 192.168.5.10
- interface GigabitEthernet0/0.5  
 encapsulation dot1Q 5  
 ip address 192.168.5.10 255.255.255.0  
 ip helper-address 192.168.39.100  
 !  
 interface GigabitEthernet0/0.80  
 encapsulation dot1Q 80  
 ip address 192.168.80.10 255.255.255.128  
 ip helper-address 192.168.39.100  
 !  
 ip dhcp excluded-address 192.168.80.1 192.168.80.10  
 !  
 ip dhcp pool LEGAL  
 network 192.168.80.0 255.255.255.128  
 default-router 192.168.80.10  
 !  
 ip dhcp pool HR  
 network 192.168.5.0 255.255.255.0  
 default-router 192.168.5.10
- interface GigabitEthernet0/0.5  
 encapsulation dot1Q 5  
 ip address 192.168.5.10 255.255.255.0  
 ip helper-address 192.168.93.100  
 !  
 interface GigabitEthernet0/0.80  
 encapsulation dot1Q 80  
 ip address 192.168.80.10 255.255.255.128  
 ip helper-address 192.168.39.100  
 !  
 ip dhcp excluded-address 192.168.5.1 192.168.5.1  
 ip dhcp excluded-address 192.168.80.1 192.168.80.10  
 !  
 ip dhcp pool LEGAL  
 network 192.168.80.0 255.255.255.128  
 default-router 192.168.80.10  
 !  
 ip dhcp pool HR  
 network 192.168.5.0 255.255.255.0  
 default-router 192.168.5.10
- interface GigabitEthernet0/0.5  
 encapsulation dot1Q 5  
 ip address 192.168.5.10 255.255.255.0  
 ip helper-address 192.168.39.100  
 !  
 interface GigabitEthernet0/0.80  
 encapsulation dot1Q 80  
 ip address 192.168.80.10 255.255.255.128  
 ip helper-address 192.168.39.100  
 !  
 ip dhcp excluded-address 192.168.5.1 192.168.5.5  
 ip dhcp excluded-address 192.168.80.1 192.168.80.110  
 !  
 ip dhcp pool LEGAL  
 network 192.168.80.0 255.255.255.128  
 default-router 192.168.80.10  
 !  
 ip dhcp pool HR  
 network 192.168.5.0 255.255.255.0  
 default-router 192.168.5.10

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

Answer: A

**NEW QUESTION 35**  
 - (Exam Topic 3)

configuration on the hub router meets this requirement?

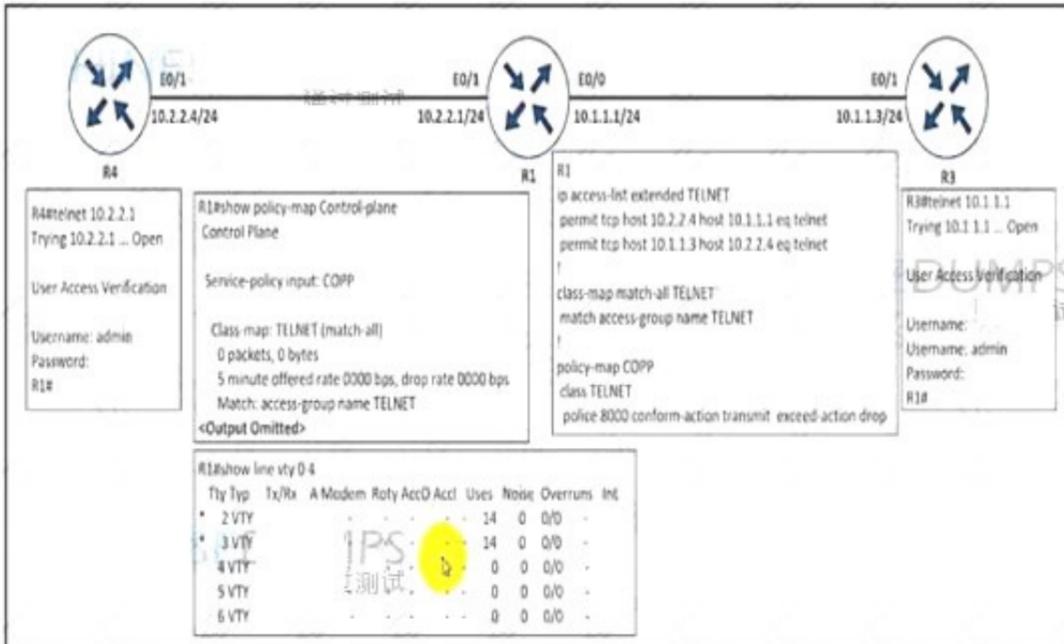
- A. interface Tunnel0 tunnel mode gre multipoint
- B. interface Tunnel0 tunnel mode dvmrp
- C. interface Tunnel0 tunnel mode ipsec ipv4
- D. interface Tunnel0 tunnel mode ip

**Answer: A**

**NEW QUESTION 37**

- (Exam Topic 3)

Refer to the exhibit.



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

- 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 42**

- (Exam Topic 3)

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

Comment

Guidelines Topology Tasks

Topology Diagram

R1 R2 SW1 SW2 SW3 SW4

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

Guidelines Topology Tasks

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 R2 SW1 SW2 SW3 SW4

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

R1

R1 R2 SW1 SW2 SW3 SW4

```
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
!
```





```

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
!
!
!

```

```

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

```

R1  R2  SW1  SW2  SW3  SW4
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
!
!
!

```









```

!!!!
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)

```

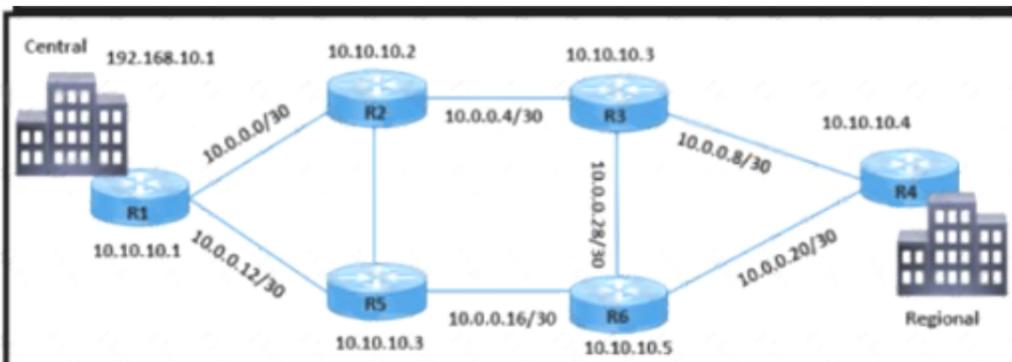
```
SW1#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
Same Test for SW2: From SW2 to SW4: SW2#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, 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 43**

- (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”

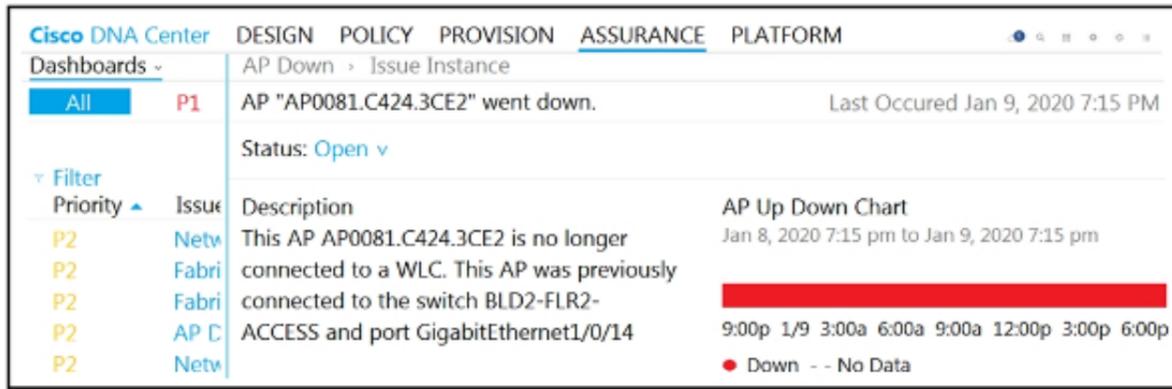
- A. R3(config)#ip route 192.168.10.1 255.255.255.255 10.10.10.2 track 20
- B. R2(config)#ip route 10.10 10 3 255 255.255 255 10.0.0.6
- C. R3(config)#track( 20 ip sla 20 reachability
- D. R6(config)#ip route 10.10.10 3 255.255.255.255 10.0.0.30

**Answer: A**

**NEW QUESTION 44**

- (Exam Topic 3)

Refer to the exhibit.



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](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:

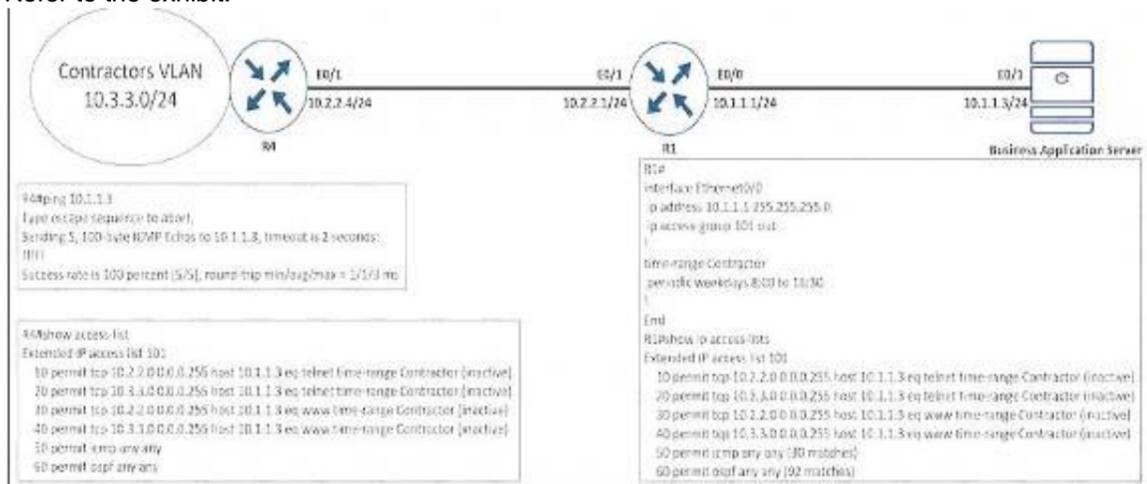
```
TDR test last run on: December 05 18:50:53
Interface Speed Local pair Pair length Remote pair Pair status
Gi1/0/14 1000M Pair A 19 +/- 10 meters Pair B Normal
Pair B 19 +/- 10 meters Pair A Normal
Pair C 19 +/- 10 meters Pair D Normal
Pair D 19 +/- 10 meters Pair C Normal
```

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 45**

- (Exam Topic 3)

Refer to the exhibit.



An engineer is troubleshooting failed access by contractors to the business application server via Telnet or HTTP during the weekend. Which configuration resolves the issue?

- A)
  - R1
  - time-range Contractor
  - no periodic weekdays 8:00 to 16:30
  - periodic daily 8:00 to 16:30
- B)
  - R4
  - time-range Contractor
  - no periodic weekdays 17:00 to 23:59
  - periodic daily 8:00 to 16:30

C)

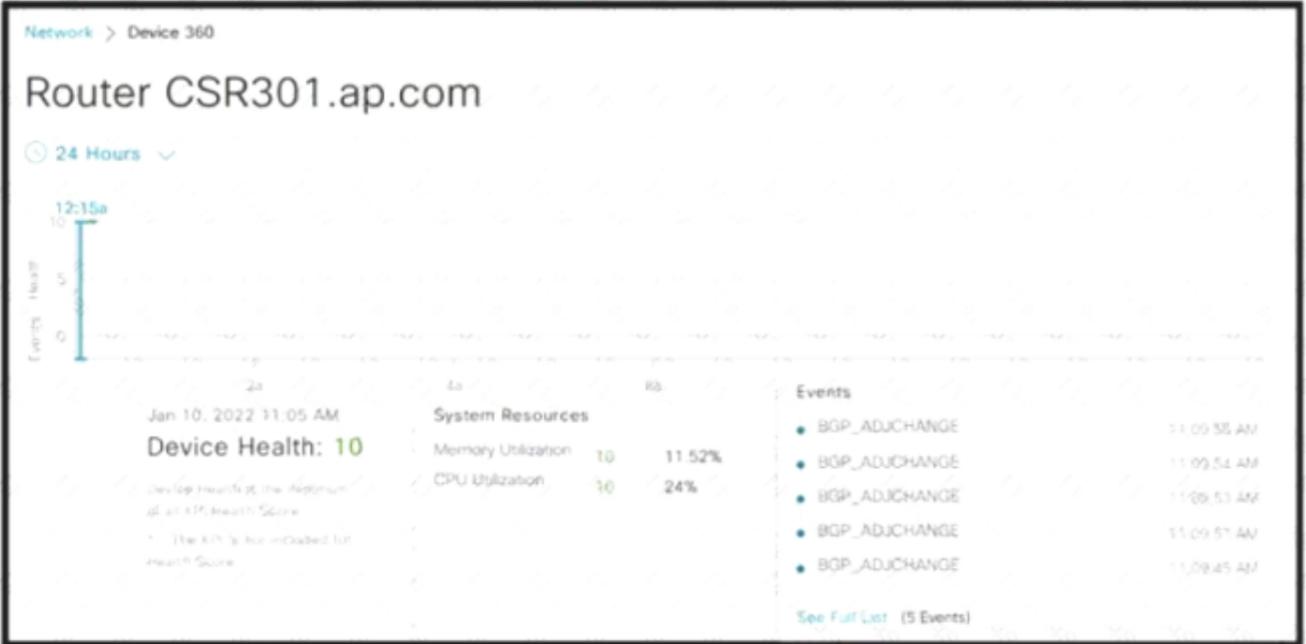
R4  
**no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor**

D)  
R1  
**no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor**

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

**Answer: A**

**NEW QUESTION 47**  
 - (Exam Topic 3)



```
atomic-aggregate, best
  Extended Community: RT:1:4099
  rx pathid: 0, tx pathid: 0x0
  Updated on Jul 28 2022 15:17:49 UTC

router#

router#sh ip bgp 10.140.217.0/24
% Network not in table
router#

router#sh ip bgp 10.140.217.0/24
BGP routing table entry for 10.140.217.0/24, version 685
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
    5      11
  Refresh Epoch 1
  65396, (aggregated by 65396 10.140.210.2), imported path from
1:4099:10.140.217.0/24 (Guest_VN)

    10.140.212.5 from 10.140.212.5 (10.140.210.2)
    Origin IGP, metric 0, localpref 100, valid, external,
atomic-aggregate, best
  Extended Community: RT:1:4099
  rx pathid: 0, tx pathid: 0x0
  Updated on Jul 31 2022 18:32:12 UTC
```

Refer to the exhibit. In Cisco DNA Center, a network engineer identifies that BGP-learned networks are repeatedly withdrawn from peers. Which configuration must the engineer apply to resolve the issue?

- A)
 

```
router bgp 100
  bgp graceful-restart
```
- B)
 

```
router bgp 100
  bgp dampening
```
- C)
 

```
route-map Dampening permit 10
  set dampening 15 750 2000 60
router bgp 100
  neighbor 10.140.212.5 route-map Dampening in
```
- D)
 

```
route-map Dampening permit 10
  set dampening 15 750 2000 60
router bgp 100
  neighbor 10.140.212.5 route-map Dampening out
```

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

**Answer: D**

**NEW QUESTION 48**

- (Exam Topic 3)

Which routing protocol is used by the PE router to advertise routes to a CE router without redistribution or static after removing the RD tag from the P router?

- A. IS-IS
- B. OSPF
- C. BGPIPv4
- D. MP-BGP

**Answer: C**

**NEW QUESTION 51**

- (Exam Topic 3)

How do devices operate in MPLS L3VPN topology?

- A. P and associated PE routers with IGP populate the VRF table in different VPNs.
- B. CE routers connect to the provider network and perform LSP functionality
- C. P routers provide connectivity between PE devices with MPLS switching.
- D. P routers support PE to PE VPN tunnel without LSP functionality

**Answer: C**

**NEW QUESTION 55**

- (Exam Topic 3)

Refer to the exhibit.

```

Router#show ip bgp vpriv4 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 no-label/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 no-label/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 no-label/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 no-label/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 no-label/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 no-label/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-external
  Extended Community RT:1100:1001
  mpls labels in/out no-label/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 no-label/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-external
  Extended Community RT:1100:1001
  mpls labels in/out no-label/278

```

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 current best path
- B. Configure higher MED to select as the best path
- C. Configure AS\_PATH prepend for the desired best path
- D. Configure lower LOCAL\_PREF to select as the best path

**Answer: D**

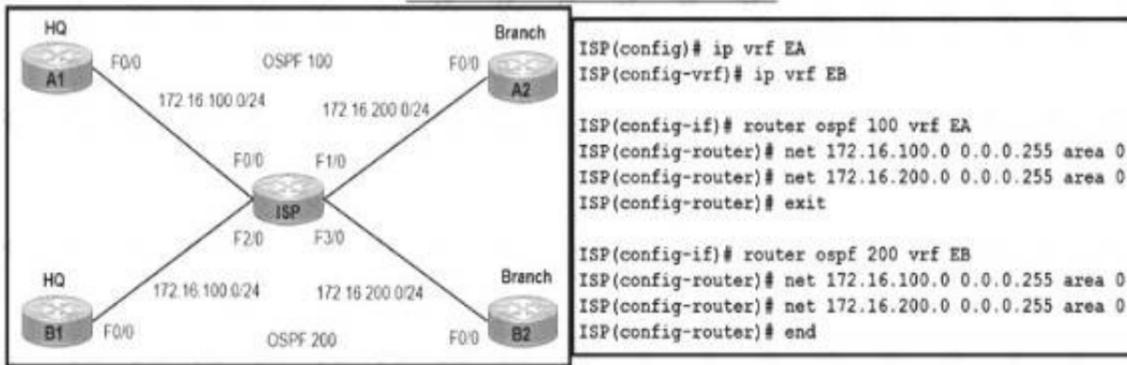
**Explanation:**

From the output, we learn that the current best path is from 10.57.255.11 (which includes "...valid, confed-external, best") and this path is 2 ASes away (64955 65003). Although there are some paths

with only 1 AS away (path from 172.16.254.234 for example) but they were not chosen the best path so AS\_PATH was not used to determine the best path -> Answers A and answer C are not correct. All the paths in the output have metric of 0 and this is the lowest (best) value for this attribute. If we configure higher MED then it is less preferred over other paths -> Answer B is not correct. Only answer D is left but LOCAL\_PREF attribute should be configured with higher value to be preferred so we hope "lower LOCAL\_PREF" here means higher value. But this is the best answer.

**NEW QUESTION 56**

- (Exam Topic 3)



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 61**

- (Exam Topic 3)

How is the LDP router ID used in an MPLS network?

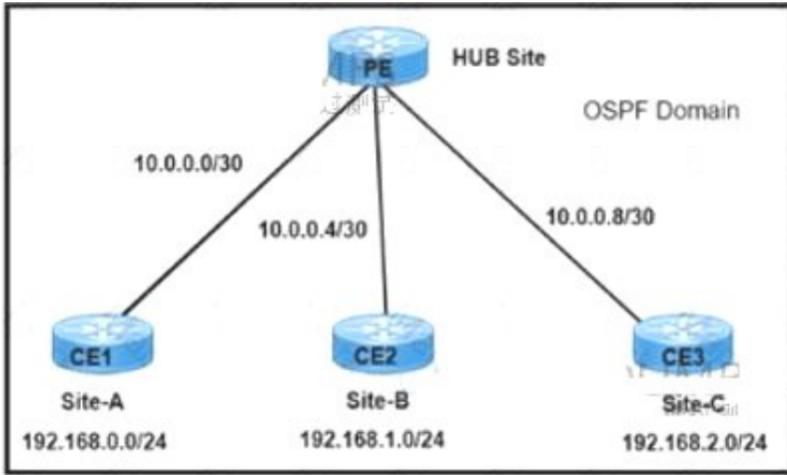
- A. The MPLS LDP router ID must match the IGP router ID.
- B. If not configured, the operational physical interface is chosen as the router ID even d a loopback is configured.
- C. The loopback with the highest IP address is selected as the router ID
- D. The force keyword changes the router ID to the speeded address without causing any impact.

**Answer: D**

**NEW QUESTION 63**

- (Exam Topic 3)

Refer to the exhibit.



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

- > Site-A: must be restricted to access to any users at Site-B or Site-C.
- > Site-B and Site-C must be able to communicate between sites and share routes using OSPF.

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

Which configuration meets the requirements?

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

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

**Answer: C**

**NEW QUESTION 65**

- (Exam Topic 3)

Refer to the exhibit.

```
*Sep 26 19:50:43.504: SNMP: Packet received via UDP from
192.168.1.2 on GigabitEthernet0/1SrParseV3SnmpMessage: No
matching Engine ID.

SrParseV3SnmpMessage: Failed.
SrDoSnmp: authentication failure, Unknown Engine ID

*Sep 26 19:50:43.504: SNMP: Report, reqid 29548, errstat 0,
erridx 0
internet.6.3.15.1.1.4.0 = 3
*Sep 26 19:50:43.508: SNMP: Packet sent via UDP to 192.168.1.2
process_mgmt_req_int: UDP packet being de-queued
```

Which two commands provide the administrator with the information needed to resolve the issue? (Choose two.)

- A. snmp user
- B. debug snmp engine-id
- C. debug snmpv3 engine-id
- D. debug snmp packet
- E. showsnmpv3 user

**Answer: AE**

**NEW QUESTION 68**

- (Exam Topic 3)

Refer to the exhibit.

```
R2(config)# int tun0
*Jun 23 00:42:06.179: %LINEPROTO-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-RECURDOWN: 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:**

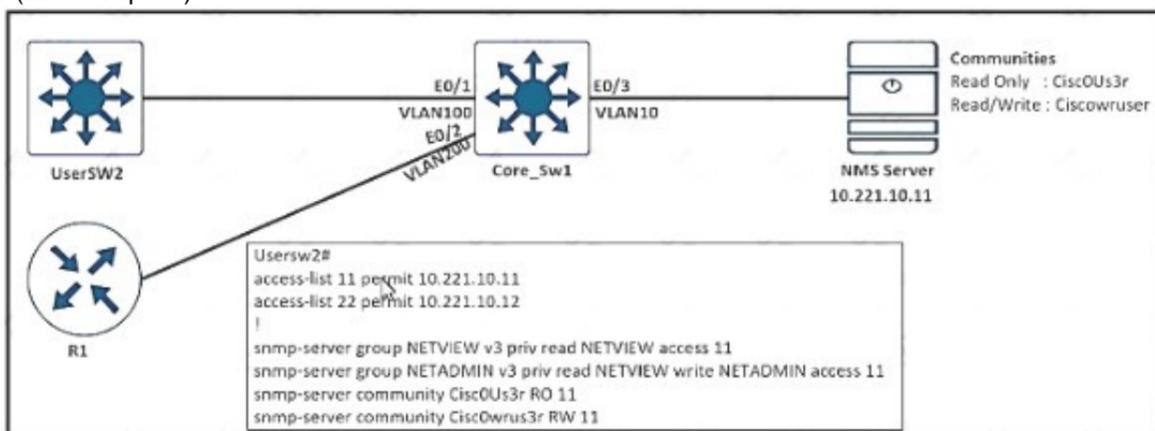
In this question we are advertising the tunnel IP address 192.168.12.2 to the other side. When other end receives the EIGRP advertisement, it realizes it can reach the other side of the tunnel via EIGRP. In other words, it reaches the tunnel destination through the tunnel itself -> This causes "recursive 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 71**

- (Exam Topic 3)



Refer to the exhibit. An engineer configured SNMP Communities on UserSW2 switch, but the SNMP server cannot upload modified configurations to the switch. Which configuration resolves this issue?

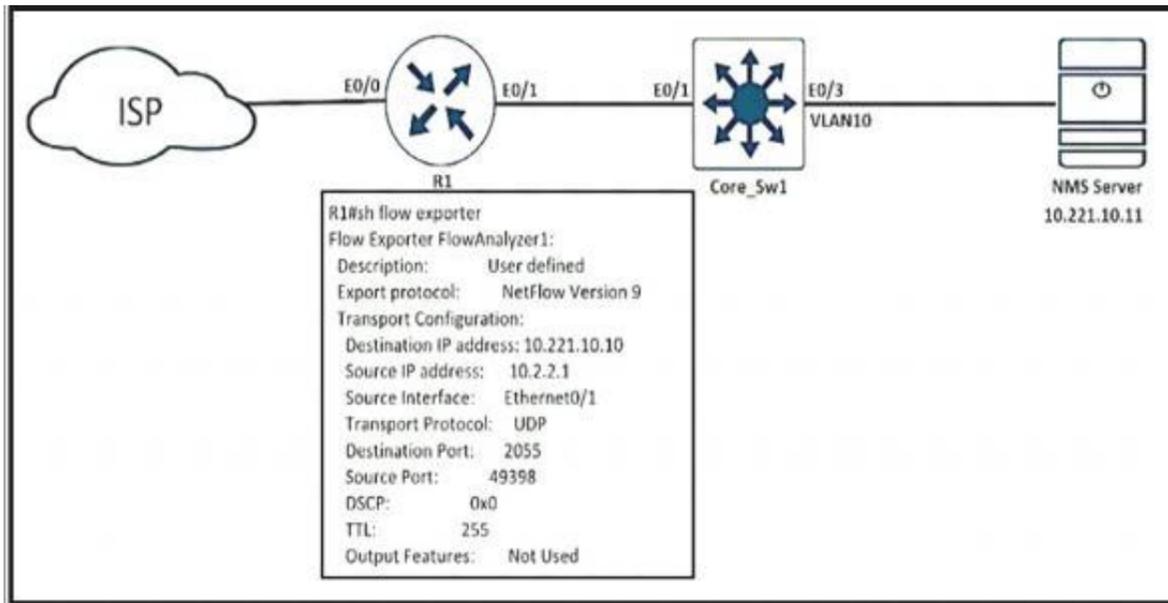
- A. snmp-server community Ciscowruser RW 11
- B. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22
- C. snmp-server community CiscoUs3r RW 11
- D. snmp-server group NETVIEW v2c priv read NETVIEW access 11

**Answer: A**

**NEW QUESTION 75**

- (Exam Topic 3)

Refer to the exhibit.



An engineer configured NetFlow on R1, but the NMS server cannot see the flow from R1. Which configuration resolves the issue?

- A. flow monitor Flowmonitor1 destination 10.221.10.11
- B. flow exporter FlowAnalyzer1 destination 10.221.10.11
- C. interface Ethernet0/1flow-destination 10.221.10.11
- D. interface Ethernet0/0flow-destination 10.221.10.11

**Answer: B**

**Explanation:**

From the output we notice that the destination IP address is not correct. The NMS server IP address should be 10.221.10.11, not 10.221.10.10. Therefore we have to change this information under "flow exporter ..." configuration.

NetFlow configuration reference: <https://www.cisco.com/c/en/us/td/docs/iosxml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/cfg-de-fnflow-exprts.html>

**NEW QUESTION 80**

- (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 83**

- (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 84**

- (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

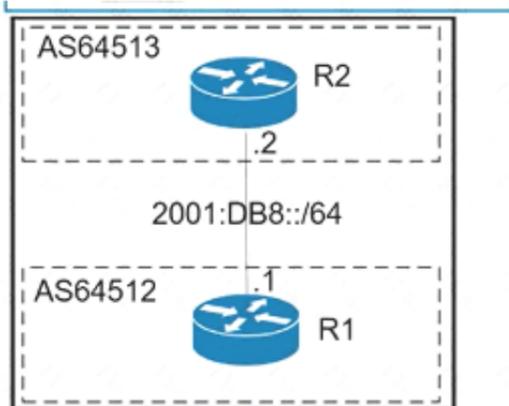
**Answer:** B

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6\\_fhsec/configuration/xr-3s/ip6f-xe-3s-book/ip6-src-guar](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xr-3s/ip6f-xe-3s-book/ip6-src-guar)

**NEW QUESTION 85**

- (Exam Topic 3)



```
R1#show ipv6 access-list
IPv6 access list inbound-acl
  permit tcp host 2001:DB8::2 eq bgp host 2001:DB8::1 (75 matches) sequence 20
  permit tcp host 2001:DB8::2 host 2001:DB8::1 eq bgp (17 matches) sequence 30
  deny ipv6 2001:DB8::/32 any (77 matches) sequence 40
  permit ipv6 any (20 matches) sequence 1000
R1#ping ipv6 2001:DB8::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8::2, timeout is 2 seconds:
```

```
.....
Success rate is 0 percent (0/5)
R1#show ipv6 access-list
IPv6 access list inbound-acl
  permit tcp host 2001:DB8::2 eq bgp host 2001:DB8::1 (77 matches) sequence 20
  permit tcp host 2001:DB8::2 host 2001:DB8::1 eq bgp (19 matches) sequence 30
  deny ipv6 2001:DB8::/32 any (95 matches) sequence 40
  permit ipv6 any (23 matches) sequence 1000
R1#
```

Refer to the exhibit. An engineer applied filter on R1 The interface flapped between R1 and R2 and cleaning the BGP session did not restore the BGP session and failed Which action must the engineer take to restore the BGP session from R2 to R1?

- A. Apply the IPv6 traffic filter in the outbound direction on the interface
- B. ICMPv6 must be permitted by the IPv6 traffic filter
- C. Enable the BGP session, which went down when the session was cleared.
- D. Swap the source and destination IP addresses in the IPv6 traffic filter

**Answer:** B

**NEW QUESTION 88**

- (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 vif
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 90**

- (Exam Topic 3)

**Company XYZ Network**

```

R101#sh run | section sla
ip sla 1
  tcp-connect 2.2.2.2 3000 source-ip 1.1.1.1
  threshold 1000
  timeout 1000

ip sla 2
  icmp-jitter 2.2.2.2 source-ip 1.1.1.1 num-packets 100 interval 10
  threshold 1000
  timeout 1000
  frequency 10
ip sla schedule 2 life forever start-time now
R101#sh ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID   Type           Destination  Stats (ms)  Return Code  Last Run
-----
*1   tcp-connect    2.2.2.2     -           No connection 33 seconds ago
*2   icmp-jitter    2.2.2.2     RTT=4       OK           3 seconds ago
    
```

Refer to the exhibit. While troubleshooting an issue on the network, an engineer notices that a TCP Connect operation failed on port 3000 between R101 and R201. Which command must be configured on R201 to respond to the R101 IP SLA configurations with a control connection on UDP port 1967?

- A. ip sla responder udp-echo ipaddress 1.1.1.1 port 1967
- B. ip sla responder tcp-connect ipaddress 1.1.1.1 port 3000
- C. ip sla responder tcp-connect ipaddress 2.2.2.2 port 3001
- D. ip sla responder

**Answer: A**

**NEW QUESTION 95**

- (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 97**

- (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 98**

- (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?

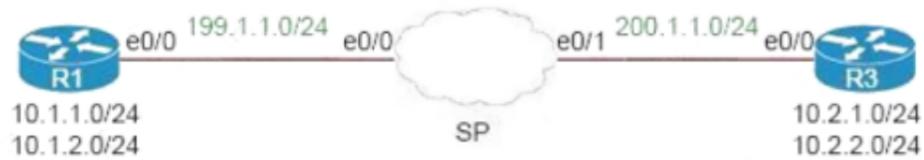
- A. R1 should configure the ip summary-address eigrp <AS number> 10.0.0.0.255.0.0.0 command under the Fast Ethernet 0/0 interface.
- B. The summarization condition is not met Router 10 1 100.10 requires a route for 10 0.0.0/8 that points to null 0
- C. The summarization condition is not met
- D. The 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 102**

- (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 5 authentication pre-share encryption 3des hash sha group 2!crypto isakmp key cisco123 address 200.1.1.3
- B. crypto isakmp policy 5 authentication pre-share encryption 3des hash md5 group 2!crypto isakmp key cisco123 address 200.1.1.3
- C. crypto isakmp policy 5 authentication pre-share encryption 3des hash md5 group 2!crypto isakmp key cisco123 address 199.1.1.1
- D. crypto isakmp policy 5 authentication pre-share encryption 3des hash md5 group 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/xr-16-5/sec-ipsec-management-xr-16-5-book/sec-ipsec-usability-enhance.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_imgmt/configuration/xr-16-5/sec-ipsec-management-xr-16-5-book/sec-ipsec-usability-enhance.html)

**NEW QUESTION 104**

- (Exam Topic 3)

A network administrator successfully established a DMVPN tunnel with one hub and two spokes using EIGRP. One of the requirements was to enable spoke-to-spoke tunnels through the hub router using EIGRP. Which configuration command must the engineer configure to meet the requirement?

- A. no ip eigrp 1 mode multipoint
- B. no ip eigrp 1 split-horizon
- C. no ip eigrp 1 tunnel-redirect
- D. no ip eigrp 1 mode mgre

Answer: B

**NEW QUESTION 109**

- (Exam Topic 3)

```
R1#show bgp ipv6 unicast 2001:db8::1/128
BGP routing table entry for 2001:db8::1/128, version 3
Paths: (1 available, best #1, table Global-IPv6-Table)
Not advertised to any peer
Local
 2001:db8:33:33::33 (metric 128) from 2001:db8:11:11::11 (1.1.1.1)
  Origin IGP, metric 0, localpref 100, valid, internal, best
  Originator: 3.3.3.3, Cluster list: 1.1.1.1
```

Refer to the exhibit. An engineer examines the BGP update for the IPv6 prefix 2001:db8::1/128, which should have been summarized into a /64 prefix. Which

sequence of actions achieves the summarization?

- A. R1 is a route reflector client of a RR with a router ID of 1.1.1.1. and the originator of the prefix has a router ID of 3.3.3.3. Both routers belong to different AS
- B. The prefix is not advertised to any peer and must be advertised using the network statement on R3.
- C. R1 is a route reflector with a router ID of 3.3.3.3. and the originator of the prefix is a route reflector client, which has a router ID of 3.3.3.3. Both routers belong to the same AS Configure an aggregate address on the router with ID 1.1.1.1 for the prefix
- D. R1 is a route reflector with a router ID of 1.111. and the originator of the prefix is a route reflector client, which has a router ID of 3.3.3.3. Both routers belong to the same AS Configure an aggregate address on the router with ID 1.1.1.1 for the prefix
- E. R1 is a route reflector client of a RR with a router ID of 1.1.1.1. and the originator of the prefix has a router ID of 3.3.3.3. Both routers belong to the same A
- F. Configure an aggregate address on the router with ID 3 3.3.3 for the prefix.

**Answer: D**

**NEW QUESTION 113**

- (Exam Topic 3)

Refer to the exhibit.

```

ipv6 inspect udp idle-time 3600
ipv6 inspect name ipv6-firewall tcp
ipv6 inspect name ipv6-firewall udp
!

ipv6 access-list ipv6-internet
deny ipv6 any FEC0::/10
deny ipv6 any FF00::/8
permit ipv6 any FF02::/16
permit ipv6 any FF0E::/16
permit udp any any eq domain log
!

Interface gi0/1
ipv6 traffic-filter ipv6-internet in
ipv6 inspect ipv6-firewall in
ipv6 inspect ipv6-firewall out
    
```

A network administrator configured name resolution for IPv6 traffic to be allowed through an inbound access list. After the access list is applied to resolve the issue, name resolution still did not work. Which action does the network administrator take to resolve the name resolution problem?

- A. Remove ipv6 inspect ipv6-firewall in from interface gi0/1
- B. Add permit udp any eq domain any log in the access list.
- C. inspect ipv6 inspect name ipv6-firewall udp 53 in global config.
- D. Add permit any eq domain 53 any log in the access list.

**Answer: A**

**NEW QUESTION 116**

- (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

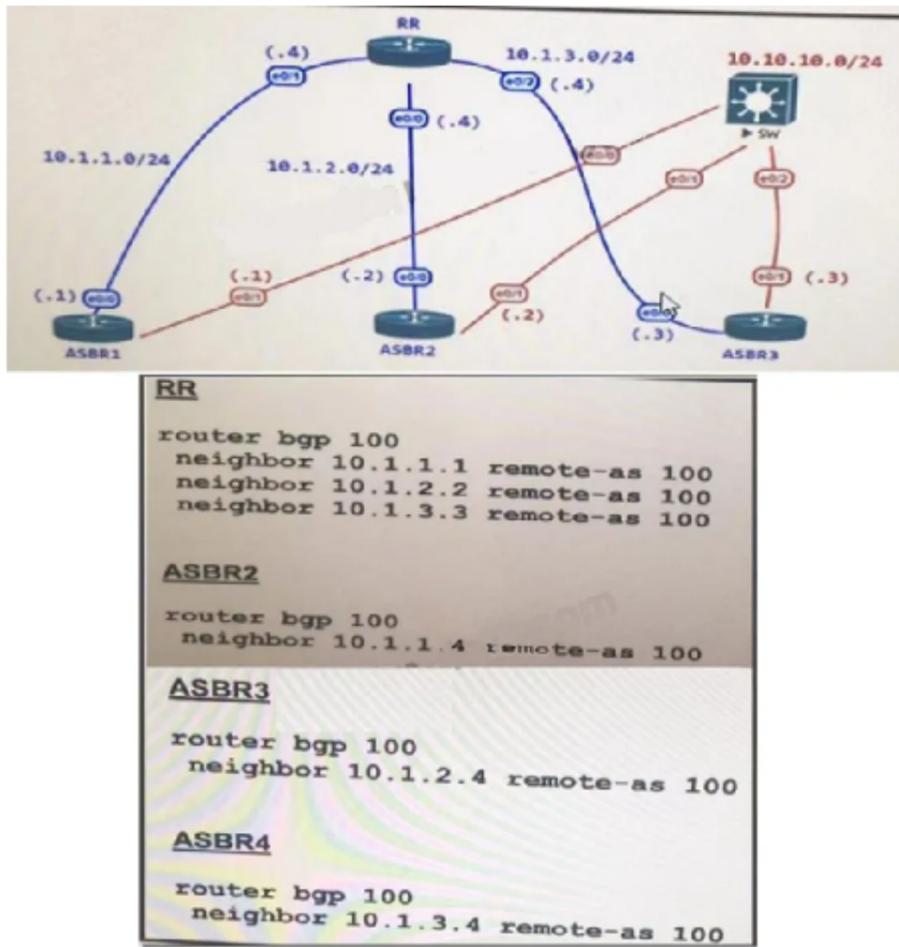
A network administrator notices these console messages from host 10.11.110.12 originating from interface E1/0. The administrator considers this an unauthorized attempt to access SNMP on R1. Which action prevents the attempts to reach R1 E1/0?

- 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 121**

- (Exam Topic 3)  
 Refer to the exhibit.



The administrator configured the network device for end-to-end reachability, but the ASBRs are not propagation routes to each other. Which set of configuration resolves this issue?

- A. router bgp 100 neighbor 10.1.1.1 route-reflector-client neighbor 10.1.2.2 route-reflector-client neighbor 10.1.3.3 route-reflector-client
- B. router bgp 100 neighbor 10.1.1.1 next-hop-self neighbor 10.1.2.2 next-hop-self neighbor 10.1.3.3 next-hop-self
- C. router bgp 100 neighbor 10.1.1.1 update-source Loopback0 neighbor 10.1.2.2 update-source Loopback0 neighbor 10.1.3.3 update-source Loopback0
- D. router bgp 100 neighbor 10.1.1.1 ebgp-multihop neighbor 10.1.2.2 ebgp-multihop neighbor 10.1.3.3 ebgp-multihop

**Answer: A**

**NEW QUESTION 126**

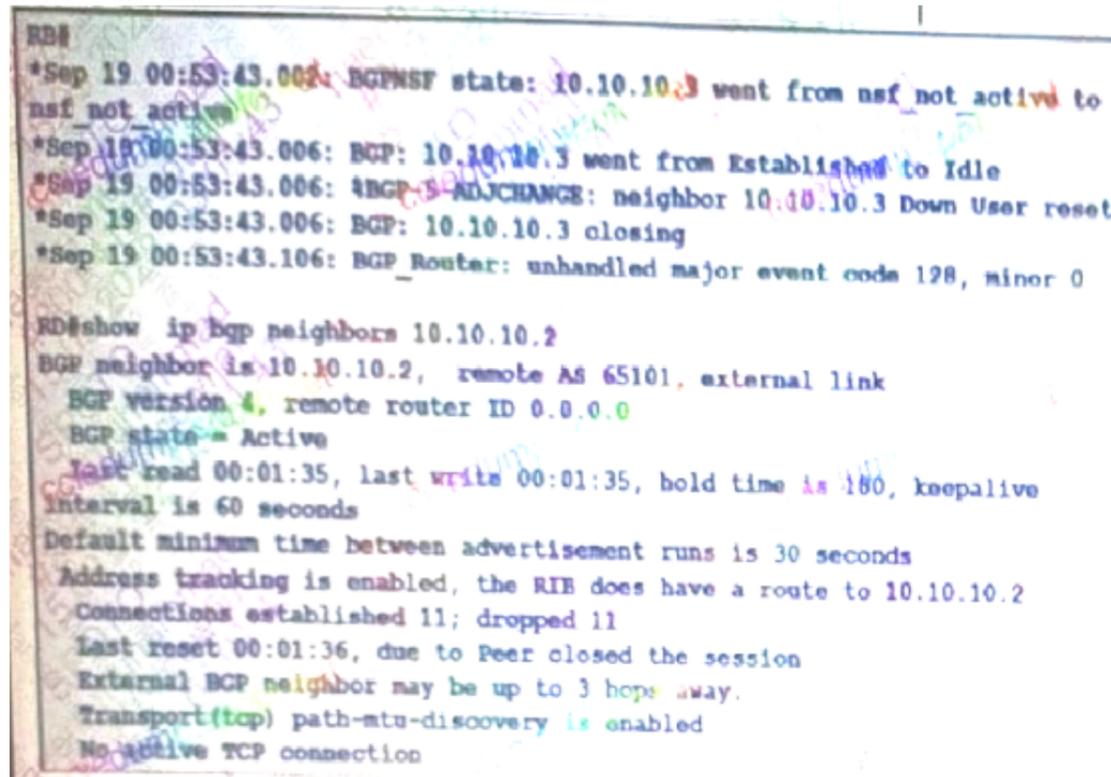
- (Exam Topic 3)  
 What is a function of the IPv6 DHCP Guard feature for DHCP messages?

- 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 131**

- (Exam Topic 3)  
 Refer to the exhibit.



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?

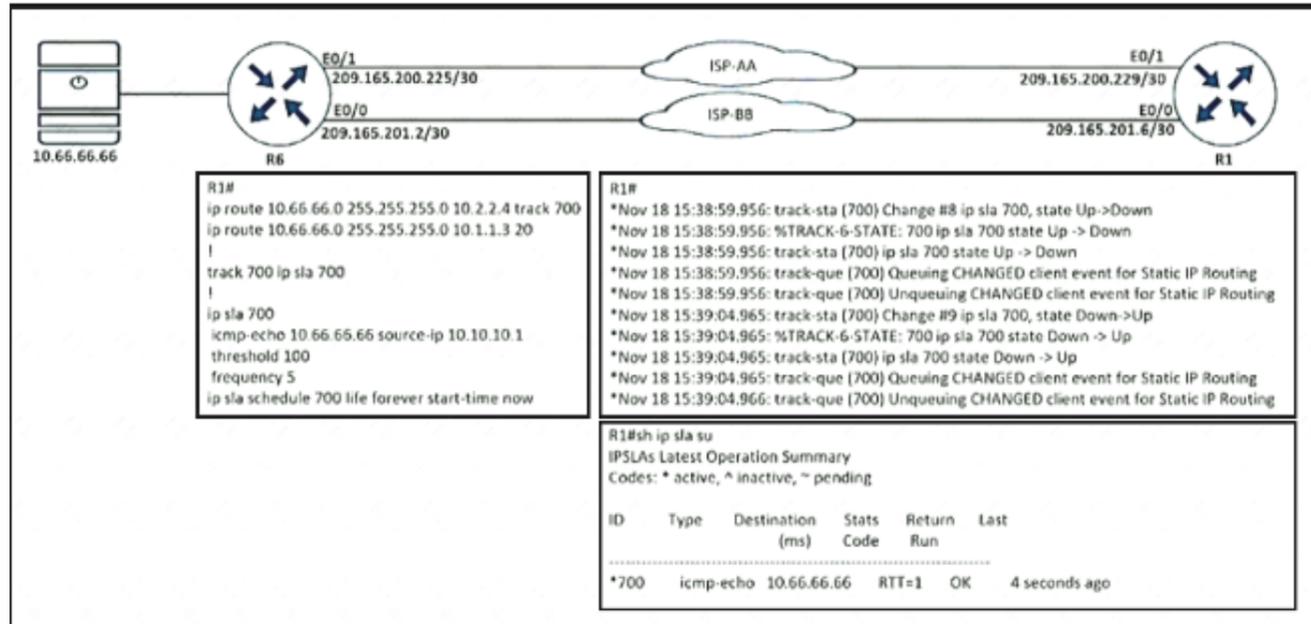
- A. RD(config)#router bgp B5201RD(config-router)# neighbor 10.10.10.2 update-source loopback 0
- B. RD(config-router)# neighbor bgp 65101RB(config-router)# neighbor 10.10.10.3 ebgp-multihop 3
- C. RB(config)# router bgp 65101RB(config)#neighbor 10.10.10.3 update-source loopback 0
- D. RD(config)# router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

**Answer: B**

**NEW QUESTION 134**

- (Exam Topic 3)

Refer to the exhibit.



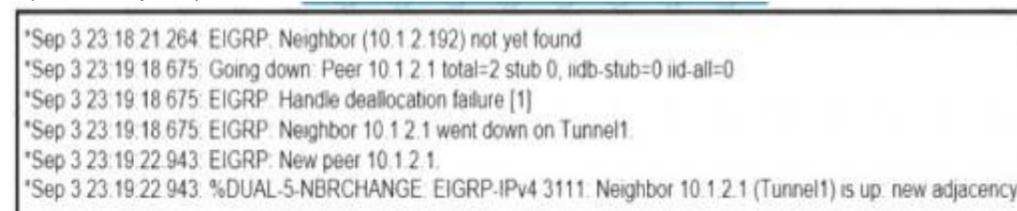
R1 is configured with IP SLA to check the availability of the server behind R6 but it kept failing. Which configuration resolves the issue?

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

**Answer: C**

**NEW QUESTION 137**

- (Exam Topic 3)



Refer to the exhibit. Which configuration command establishes an EIGRP neighbor adjacency between the hub and spoke?

- A. connected 10.1.2.192 command on spoke router
- B. network 10.1.2.192 command on spoke router
- C. eigrp-peer 10.1.2.192 command on the hub router
- D. neighbor 10.1.2.192 command on hub router

**Answer: D**

**NEW QUESTION 141**

- (Exam Topic 3)

The network administrator configured R1 to authenticate Telnet connections based on Cisco ISE using TACACS+. ISE has been configured with an IP address of 192.168.1.5 and with a network device pointing toward R1(192.168.1.1) with a shared secret password of Cisco123.

```

aaa new-model
!
tacacs server ISE1
address ipv4 192.168.1.5
key Cisco123
!
aaa group server tacacs+ TAC-SERV
server name ISE1
!
aaa authentication login telnet group TAC-SERV
    
```

The administrator cannot authenticate to R1 based on ISE. Which configuration fixes the issue?

- A. ip tacacs-server host 192.168.1.5 key Cisco123
- B. line vty 0 4login authentication TAC-SERV
- C. line vty 0 4login authentication telnet
- D. tacacs-server host 192.168.1.5 key Cisco123

**Answer:** C

**Explanation:**

The last command "aaa authentication login telnet group TAC-SERV" created the method list name telnet so we need to assign it to line vty.

Reference: <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208-Configure-ISE-2-0-IOS-TACACS-Authentic.html>

**NEW QUESTION 142**

- (Exam Topic 3)

```
R1#show ip bgp 10.0.0.0/8
BGP routing table entry for 10.0.0.0/8, version 0
Paths: (1 available, no best path)
Not advertised to any peer
Refresh Epoch 1
100
192.168.10.20 (inaccessible) from 192.168.20.20 (192.168.20.20)
Origin incomplete, metric 0, localpref 100, valid, internal rx
pathid: 0, tx pathid: 0
```

Refer to the exhibit. An engineer is troubleshooting a prefix advertisement issue from R3, which is not directly connected to R1. Which configuration resolves the issue?

A)

```
R1(config)#router bgp 64512
R1(config-router)#neighbor 192.168.10.20 next-hop-self
```

B)

```
R1(config)#router bgp 64512
R1(config-router)#neighbor 192.168.20.20 next-hop-self
```

C)

```
R2(config)#router bgp 64512
R2(config-router)#neighbor 192.168.20.10 next-hop-self
```

D)

```
R2(config)#router bgp 64512
R2(config-router)#neighbor 192.168.10.20 next-hop-self
```

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

**Answer:** A

**NEW QUESTION 146**

- (Exam Topic 3)

A customer is running an mGRE DMVPN tunnel over WAN infrastructure between hub and spoke sites. The existing configuration allows NHRP to add spoke routers automatically to the multicast NHRP mappings. The customer is migrating the network from IPv4 to the IPv6 addressing scheme for those spokes' routers that support IPv6 and can run DMVPN tunnel over the IPv6 network. Which configuration must be applied to support IPv4 and IPv6 DMVPN tunnel on spoke routers?

- A. Tunnel mode ipv6ip 6to4
- B. Tunnel mode ipv6ip isatap
- C. Tunnel mode ipv6ip auto-tunnel
- D. Tunnel mode ipv6ip 6rd

**Answer:** C

**NEW QUESTION 150**

- (Exam Topic 3)

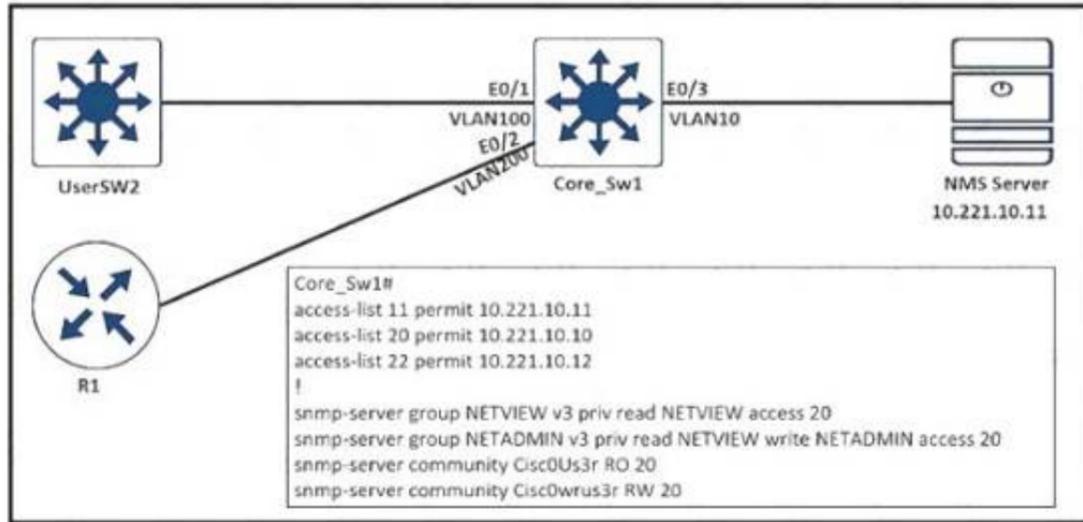
- A. The administrator distance should be raised to 120 from the ASBR 104 15.5.
- B. The redistributed prefixes should be advertised as Type 1.
- C. The ASBR 10 4 17 6 should assign a tag to match and assign a lower metric on R1
- D. The administrative distance should be raised to 120 from the ASBR 104 17 6

**Answer:** B

**NEW QUESTION 153**

- (Exam Topic 3)

Refer to the exhibit.



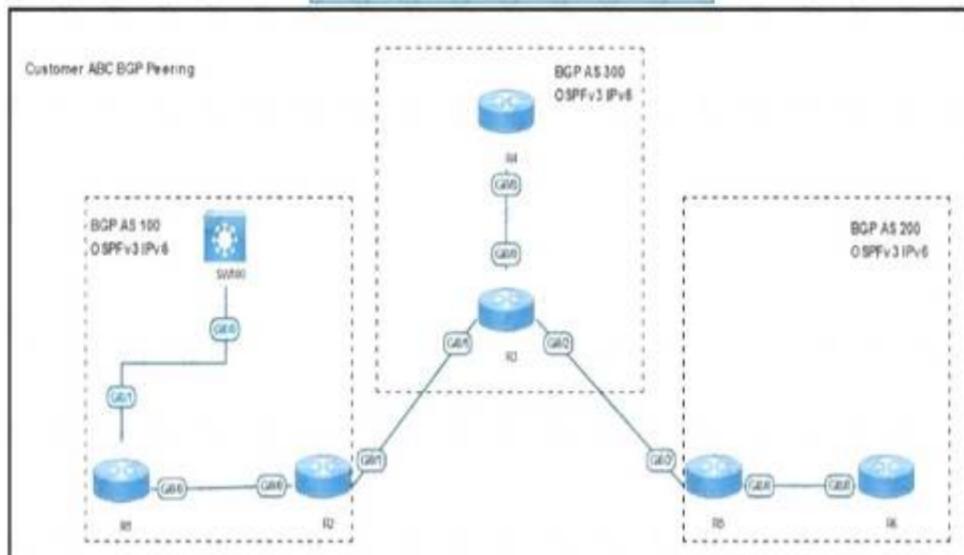
An engineer configured SNMP communities on the Core\_SW1, but the SNMP server cannot obtain information from Core\_SW1. Which configuration resolves this issue?

- A. snmp-server group NETVIEW v2c priv read NETVIEW access 20
- B. access-list 20 permit 10.221.10.11
- C. access-list 20 permit 10.221.10.12
- D. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22

**Answer: B**

**NEW QUESTION 154**

- (Exam Topic 3)



```
R2#sh ip bgp ipv6 uni
BGP table version is 45, local router ID is 2.2.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
               t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
```

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

Network      Next Hop      Metric LocPrf Weight Path
*> 2001::5/128 2001::5        0         0 300 200 i
*> 2001::4/128 2001::4        0         0 300 i
*> 2002::2/128 ::              0       32768 i

R2#sh run | section bgp
router bgp 100
  address-family ipv6
  neighbor 2001::4 route-map Filter in

ip as-path access-list 1 permit _300_[0-9]

route-map Filter permit 10
match as-path 1
```

Refer to the exhibit R2 has been receiving routes from R4 that originated outside AS300 A network engineer configured an AS-Path ACL to avoid adding these routes to the R2 BGP table but the routes are still present in the R2 routing table Which action resolves the issue?

- A. Replace as-path access-list 1 with the ip as-path access-list 1 permit A300\$ command
- B. Replace as-path access-list 1 with the ip as-path access-list 1 permit ..300." command
- C. Replace as-path access-list 1 with the ip as-path access-list 1 permit A300\_ command.
- D. Replace as-path access-list 1 with the ip as-path access-list 1 permit A300." command

**Answer: B**

**NEW QUESTION 156**

- (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**

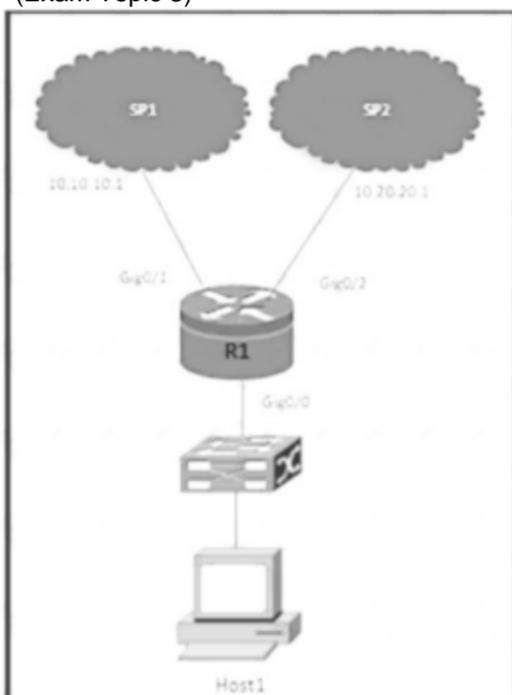
**Explanation:**

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 161**

- (Exam Topic 3)



Refer to the exhibit. R1 uses SP1 as the primary path. A network engineer must force all SSH traffic generated from R1 toward SP2. Which configuration accomplishes the task?

A)

```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.20.20.1
!
interface Gig0/0
 ip policy route-map PBR_SSH
```

B)

```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.10.10.1
!
ip local policy route-map PBR_SSH
```

C)

```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.20.20.1
!
ip local policy route-map PBR_SSH
```

D)

```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.20.20.1
!
interface Gig0/1
 ip policy route-map PBR_SSH
```

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

**Answer: C**

**NEW QUESTION 163**

- (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
```

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

Which action resolves this issue?

- A. Router R1 should configure ip summary address eigrp (AS number) 10.0.0.0 255.0.0.0 for the R1 Fast Ethernet 0/0 connected interface.
- B. Router R1 should configure ip route 10.0.0.0 255.0.0.0 null 0 for the routes that are received on R1.
- C. Router 10.1.100.10 should configure ip route 10.0.0.0 255.0.0.0 null 0 for the routes that are summarized toward R1.
- D. Router 10.1.100.10 should configure ip summary address eigrp (AS number) 10.0.0.0 255.0.0.0 for the R1 Fast Ethernet 0/0 connected interface.

**Answer: D**

**NEW QUESTION 166**

- (Exam Topic 3)

```
ip access-list extended CoPP-ICMP
 permit icmp any any echo
!
ip access-list extended CoPP-BGP
 permit tcp any eq bgp any established
!
ip access-list extended CoPP-EIGRP
 permit eigrp any host 224.0.0.10
!
Class-map match-all CoPP-CLASS
 match access-group name CoPP-ICMP
 match access-group name CoPP-BGP
 match access-group name CoPP-EIGRP
!
```

Refer to the exhibit A CoPP policy is implemented to allow specific control traffic, but the traffic is not matching as expected and is getting unexpected behavior of control traffic. Which action resolves the issue?

- A. Use match-any instruction in class-map
- B. Create a separate class map against each ACL.
- C. Create a separate class map for ICMP traffic.
- D. Use default-class to match ICMP traffic

**Answer: A**

**NEW QUESTION 167**

- (Exam Topic 2)

Which configuration feature should be used to block rogue router advertisements instead of using the IPv6 Router Advertisement Guard feature?

- A. VACL blocking broadcast frames from nonauthorized hosts
- B. PVLANS with promiscuous ports associated to route advertisements and isolated ports for nodes
- C. PVLANS with community ports associated to route advertisements and isolated ports for nodes
- D. IPv4 ACL blocking route advertisements from nonauthorized hosts

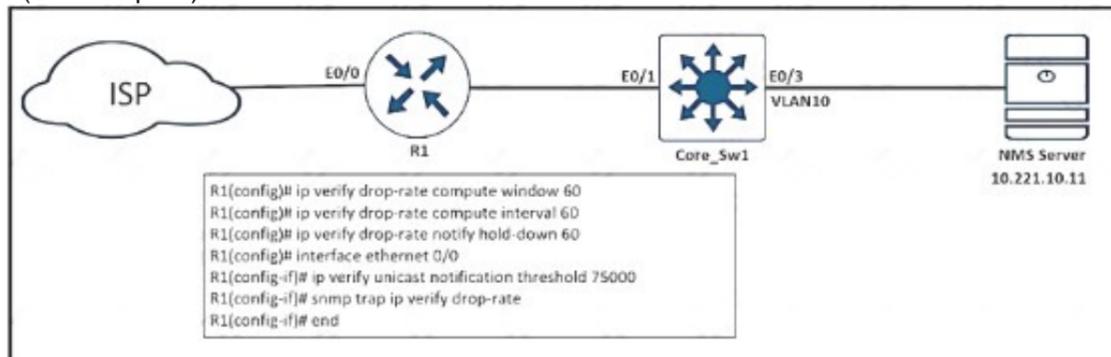
**Answer: B**

**Explanation:**

The IPv6 Router Advertisement Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement guard messages that arrive at the network device platform. Router Advertisements are used by devices to announce themselves on the link. The IPv6 Router Advertisement Guard feature analyzes these router advertisements and filters out router advertisements that are sent by unauthorized devices. Certain switch platforms can already implement some level of rogue RA filtering by the administrator configuring Access Control Lists (ACLs) that block RA ICMP messages that might be inbound on "user" ports.  
 Reference: <https://datatracker.ietf.org/doc/html/rfc6104>

**NEW QUESTION 168**

- (Exam Topic 3)



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?

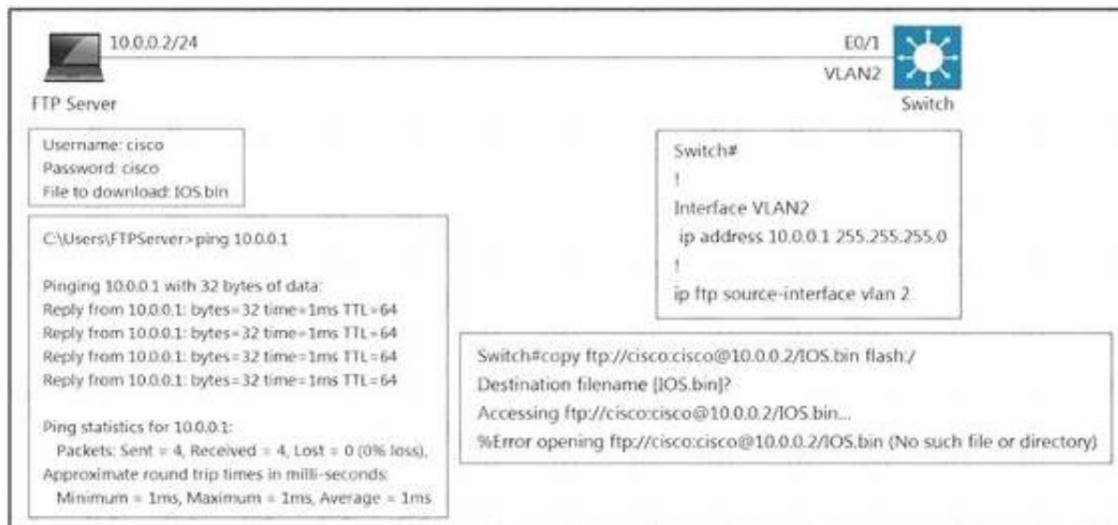
- A. ip verify unicast notification threshold 48000
- B. ip verify unicast notification threshold 8000
- C. ip verify unicast notification threshold 800
- D. ip verify unicast notification threshold 80

**Answer: C**

**NEW QUESTION 173**

- (Exam Topic 3)

Refer to the exhibit.



An engineer cannot copy the IOS.bin file from the FTP server to the switch. Which action resolves the issue?

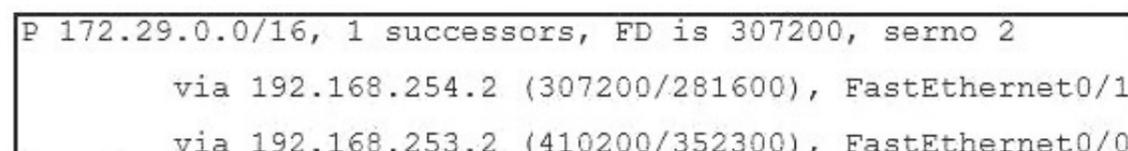
- A. Allow file permissions to download the file from the FTP server.
- B. Add the IOS.bin file, which does not exist on FTP server.
- C. Make memory space on the switch flash or USB drive to download the file.
- D. Use the copy flash:/ ftp://cisco@10.0.0.2/IOS.bin command.

**Answer: B**

**NEW QUESTION 177**

- (Exam Topic 3)

Refer to the exhibit.



When the FastEthernet0/1 goes down, the route to 172.29.0 0/16 via 192.168.253 2 is not installed in the RIB. Which action resolves the issue?

- A. Configure reported distance greater than the feasible distance
- B. Configure feasible distance greater than the successor's feasible distance.
- C. Configure reported distance greater than the successor's feasible distance.
- D. Configure feasible distance greater than the reported distance

**Answer: D**

**Explanation:**

From the exhibit, we notice network 172.29.0.0/16 was learned via two routes:

- + From 192.168.254.2 with FD = 307200 and AD = 281600
- + From 192.168.253.2 with FD = 410200 and AD = 352300

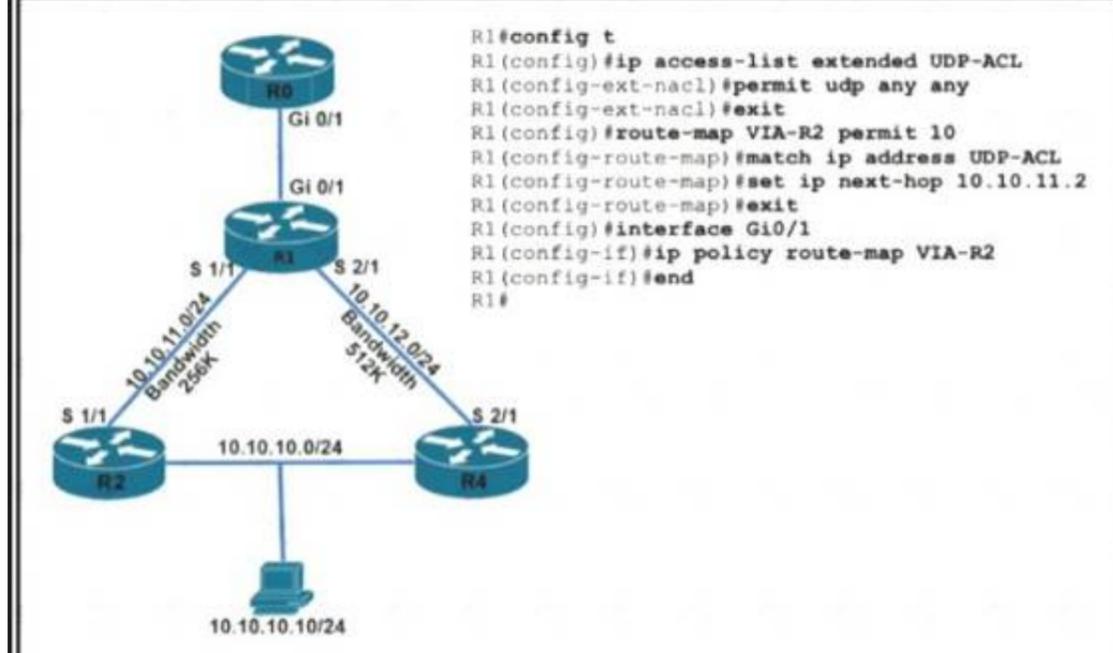
The first route is installed into the RIB as the successor route because of lower FD.

When the first route fails, router will not use the second route as it does not satisfy the feasibility condition. The feasibility condition states that, the Advertised Distance (AD, also called the reported distance) of a route must be lower than the feasible distance of the current successor route.

**NEW QUESTION 182**

- (Exam Topic 3)

Refer to the exhibit.



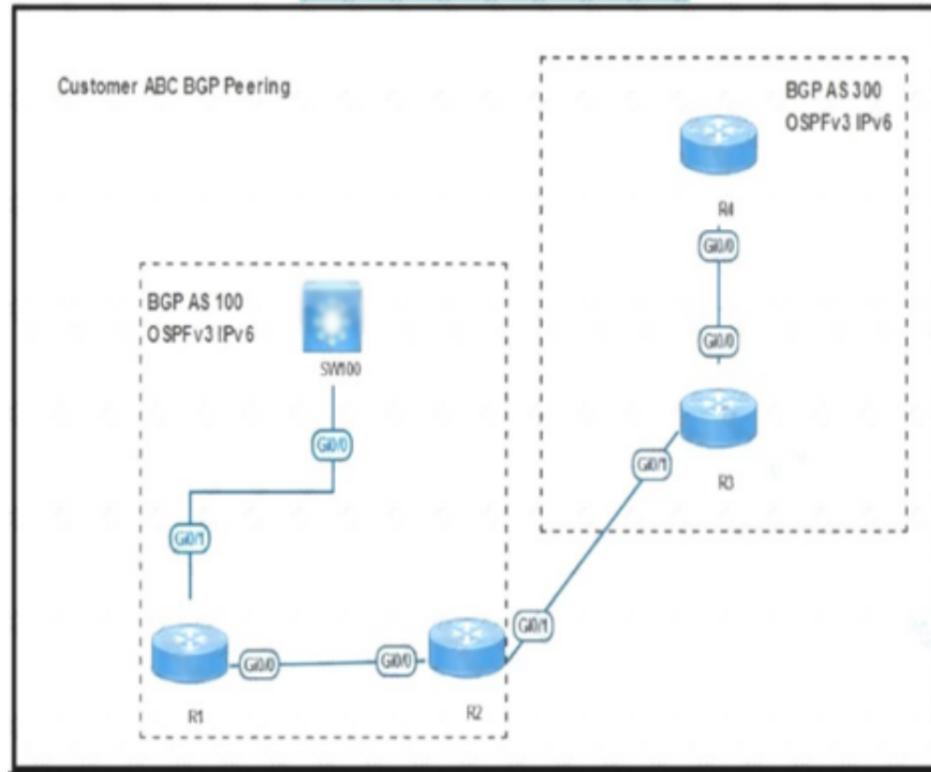
TCP traffic should be reaching host 10.10.10.10/24 via R2. Which action resolves the issue?

- 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 186**

- (Exam Topic 3)



```

SW100#sh ip bgp ipv6 uni summ
BGP router identifier 100.0.0.1, local AS number 100
BGP table version is 1, main routing table version 1

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:ABC:AABB:1100:1122:1111:2222:AAA1
              4    100    6     5      1     0   0 00:00:58      0

SW100#sh ip bgp ipv6 unicast
SW100#

R1#sh ip bgp ipv6 uni
BGP table version is 4, local router ID is 1.1.1.1
  Network        Next Hop        Metric LocPrf Weight Path
 * i  2001::4/128   2001::4          0   100    0 300 i
 *>i  2002::2/128   2001::2          0   100    0 i
R1#
R1#sh ipv6 route
O  2001::2/128 [110/1]
   via FE80::5200:C3FF:FE01:E600, GigabitEthernet0/0
B  2002::2/128 [200/0]
   via 2001::2
  
```

Refer to the exhibit SW100 cannot receive routes from R1 Which configuration resolves the issue?

- R1
 

```

router bgp 100
address-family ipv6
neighbor 2001::2 route-reflector-client
neighbor 2001:ABC:AABB:1100:1122:1111:2222:AAA2 route-reflector-client
      
```
- R2
 

```

router bgp 100
address-family ipv6
neighbor 2001::2
neighbor 2001::1 next-hop-self
      
```
- R1
 

```

router bgp 100
address-family ipv6
neighbor 2001::2 route-reflector-client
neighbor 2001:ABC:AABB:1100:1122:1111:2222:AAA2 route-reflector-client
      
```
- R2
 

```

router bgp 100
address-family ipv6
neighbor 2001::2
neighbor 2001::1 as-override
      
```
- R1
 

```

router bgp 100
address-family ipv6
no synchronization
      
```
- R2
 

```

router bgp 100
address-family ipv6
no synchronization
SW100
router bgp 100
address-family ipv6
no synchronization
      
```
- R1
 

```

router bgp 100
address-family ipv6
redistribute connected
      
```
- R2
 

```

router bgp 100
address-family ipv6
redistribute connected
      
```

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

Answer: A

**NEW QUESTION 191**

- (Exam Topic 3)

An engineer creates a default static route on a router with a hop of 10.1.1.1. On inspection, the engineer finds the router has two VRFs, Red and Blue. The next hop is valid for both VRFs and exists in each assigned VRF. Which configuration achieves connectivity?

A)

```
ip route vrf BLUE 0.0.0.0 255.255.255.255 10.1.1.1
ip route vrf RED 0.0.0.0 255.255.255.255 10.1.1.1
```

B)

```
ip route vrf Red 0.0.0.0 0.0.0.0 10.1.1.1
ip route vrf Blue 0.0.0.0 0.0.0.0 10.1.1.1
```

C)

```
ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

D)

```
ip route vrf Red 0.0.0.0 255.255.255.255 10.1.1.1
ip route vrf Blue 0.0.0.0 255.255.255.255 10.1.1.1
```

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

**Answer: A**

**NEW QUESTION 193**

- (Exam Topic 3)

A network administrator added a new spoke site with dynamic IP on the DMVPN network. Which configuration command passes traffic on the DMVPN tunnel from the spoke router?

- A. ip nhrp registration ignore
- B. ip nhrp registration no-registration
- C. ip nhrp registration dynamic
- D. ip nhrp registration no-unique

**Answer: D**

**NEW QUESTION 194**

- (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 198**

- (Exam Topic 3)

The network administrator configured the router for Control Plane Policing so that inbound SSH traffic is policed to 500 kbps This policy must apply to traffic coming in from 101010 0<24 and 192 168 10.0/24 networks

```
access-list 100 permit ip 10.10.10.0 0.0.0.255 any
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 23
!
class-map CLASS-SSH
match access-group 100
!
policy-map PM-COPP
class CLASS-SSH
police 500000 conform-action transmit
!
Interface E0/0
service-policy input PM-COPP
!
Interface E0/1
service-policy input PM-COPP
```

The Control Plane Policing is not applied to SSH traffic and SSH is open to use any bandwidth available. Which configuration resolves this issue?

- no access-list 100  
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22  
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22  
!  
policy-map PM-COPP  
class CLASS-SSH  
no police 500000 conform-action transmit  
police 500000 conform-action transmit exceed-action drop
- interface E0/0  
no service-policy input PM-COPP  
!  
interface E0/1  
no service-policy input PM-COPP  
!  
control-plane  
service-policy input PM-COPP
- no access-list 100  
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22  
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22  
!  
Interface E0/0  
no service-policy input PM-COPP  
!  
Interface E0/1  
no service-policy input PM-COPP  
!  
control-plane  
service-policy input PM-COPP
- no access-list 100  
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22  
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22

A)

```
no access-list 100
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22
!
policy-map PM-COPP
class CLASS-SSH
no police 500000 conform-action transmit
police 500000 conform-action transmit exceed-action drop
```

B)

```
interface E0/0
no service-policy input PM-COPP
!
interface E0/1
no service-policy input PM-COPP
!
control-plane
service-policy input PM-COPP
```

C)

```
no access-list 100
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22
!
Interface E0/0
no service-policy input PM-COPP
!
Interface E0/1
no service-policy input PM-COPP
!
control-plane
service-policy input PM-COPP
```

D)

```
no access-list 100
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22
```

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

**Answer: C**

**NEW QUESTION 201**

- (Exam Topic 3)

Refer to the exhibit.

```

R1# show ip int br | ex up
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 not showing R2 as a successor. Which action resolves the issue?

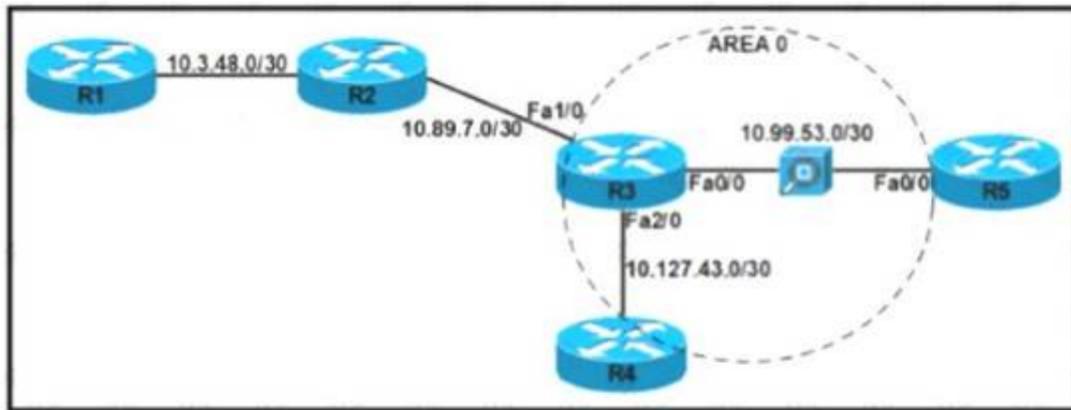
- A. Rectify the incorrect router ID in R2.
- B. Enable split-horizon.
- C. Configure the network statement on the neighbor.
- D. Resolve the incorrect metric on the link.

**Answer: D**

**NEW QUESTION 206**

- (Exam Topic 3)

Refer to the exhibit.



The security department recently installed a monitoring device between routers R3 and R5, which caused 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 88 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 88 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 122 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 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 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 211  
- (Exam Topic 3)

```

R1#show running-config | begin router eigrp
router eigrp 100
network 172.16.250.0 0.0.0.3
redistribute ospf 10 metric 1 1 1 1
!
router ospf 10
redistribute eigrp 100 metric 100 subnets route-map CCNP
network 172.16.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
route-map CCNP deny 10
match route-type local
!
access-list 10 permit 172.16.2.32
!

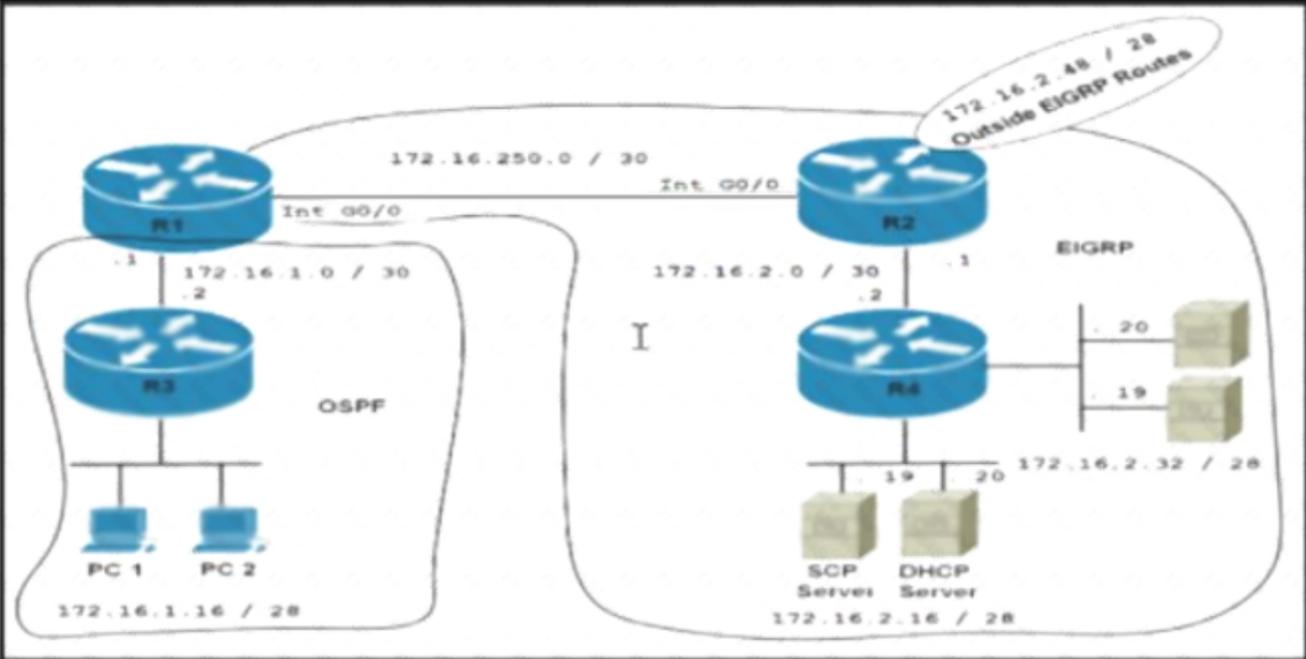
R3#sh ip route

Gateway of last resort is not set

  172.16.0.0/16 is variably subnetted, 7 subnets, 3 masks
  C   172.16.1.0/30 is directly connected, GigabitEthernet0/1
  L   172.16.1.2/32 is directly connected, GigabitEthernet0/1
  C   172.16.1.16/28 is directly connected, Loopback1
  L   172.16.1.17/32 is directly connected, Loopback1
  C   172.16.1.32/28 is directly connected, Loopback2
  L   172.16.1.33/32 is directly connected, Loopback2
  S   172.16.1.48/28 [1/0] via 172.16.2.18
R3#

R4#show running-config | begin router eigrp
router eigrp 100
network 172.16.2.0 0.0.0.3
network 172.16.2.16 0.0.0.15
network 172.16.2.32 0.0.0.15
redistribute static metric 100 1 1 1 route-map CCNP
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 172.16.2.48 255.255.255.240 172.16.2.1
!
!
route-map CCNP permit 10
match ip address 10
set tag 200
!
!
access-list 10 permit 172.16.2.48 0.0.0.15
!

```



Refer to the exhibit. Which configuration resolves the route filtering issue on R1 to redistribute all the routes except 172.16.2.48/28?

- A)
 

```

R1(config)#route-map CCNP deny 10
R1(config-route-map)#no match route-type local
R1(config-route-map)#match route-type external type-1
R1(config)#route-map CCNP permit 20
      
```
- B)
 

```

R1(config)#route-map CCNP deny 10
R1(config-route-map)#no match route-type local
R1(config-route-map)# match route-type level-2
R1(config)#route-map CCNP permit 20
      
```
- C)
 

```

R1(config)#route-map CCNP deny 10
R1(config-route-map)#no match route-type local
R1(config-route-map)#match route-type external
R1(config)#route-map CCNP permit 20
      
```
- D)
 

```

R1(config)#route-map CCNP deny 10
R1(config-route-map)#no match route-type local
R1(config-route-map)#match route-type external type-2
R1(config)#route-map CCNP permit 20
      
```

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

Answer: D

**NEW QUESTION 215**

- (Exam Topic 3)

What is a function of BFD?

- A. peer recovery after a Layer 3 protocol adjacency failure
- B. peer recovery after a Layer 2 adjacency failure
- C. failure detection independent of routing protocols and media types
- D. failure detection dependent on routing protocols and media types

Answer: D

**NEW QUESTION 217**

- (Exam Topic 3)

A network administrator is troubleshooting a failed AAA login issue on a Cisco Catalyst c3560 switch. When the network administrator tries to log in with SSH using TACACS+ username and password credentials, the switch is no longer authenticating and is failing back to the local account. Which action resolves this issue?

- A. Configure ip tacacs source-interface GigabitEthernet 1/1
- B. Configure ip tacacs source-ip 192.168.100.55
- C. Configure ip tacacs-server source-ip 192.168.100.55
- D. Configure ip tacacs-server source-interface GigabitEthernet 1/1

Answer: A

**NEW QUESTION 221**

- (Exam Topic 3)

Which two label distribution methods are used by routers in MPLS? (Choose two )

- A. targeted hello message
- B. LDP discovery hello message
- C. LDP session protection message
- D. downstream unsolicited
- E. downstream on demand

Answer: DE

**NEW QUESTION 224**

- (Exam Topic 3)

Refer to the exhibits.

```

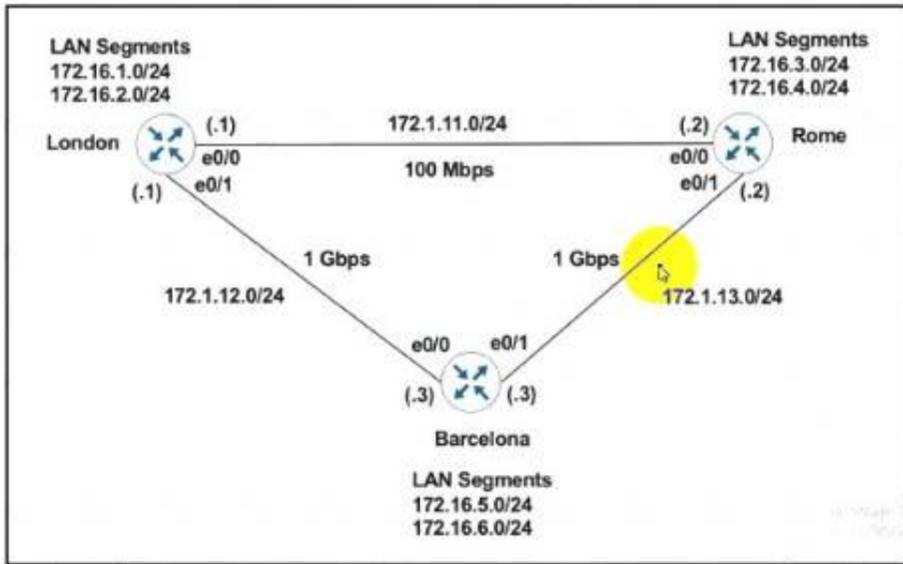
London - "show ip route" output

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
    
```



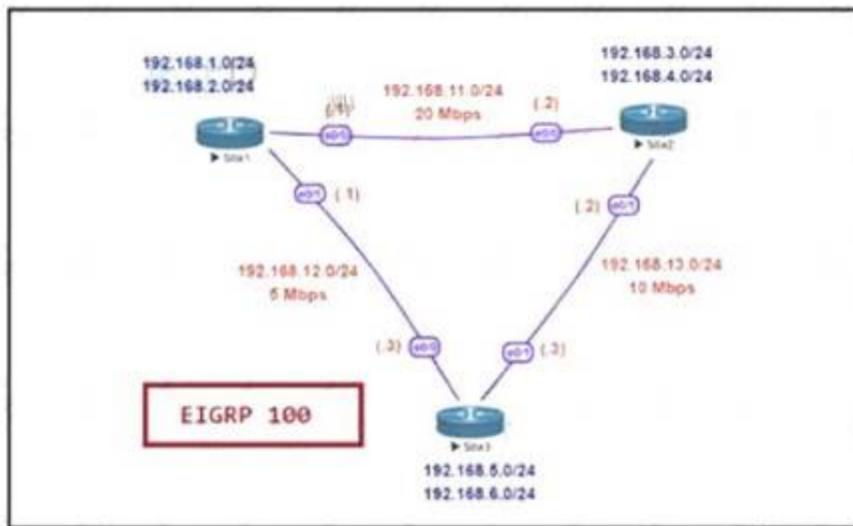
London must reach Rome using a faster path via EIGRP if all the links are up but it failed to take this path Which action resolves the issue?

- 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 228**

- (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 subnetted, 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
```

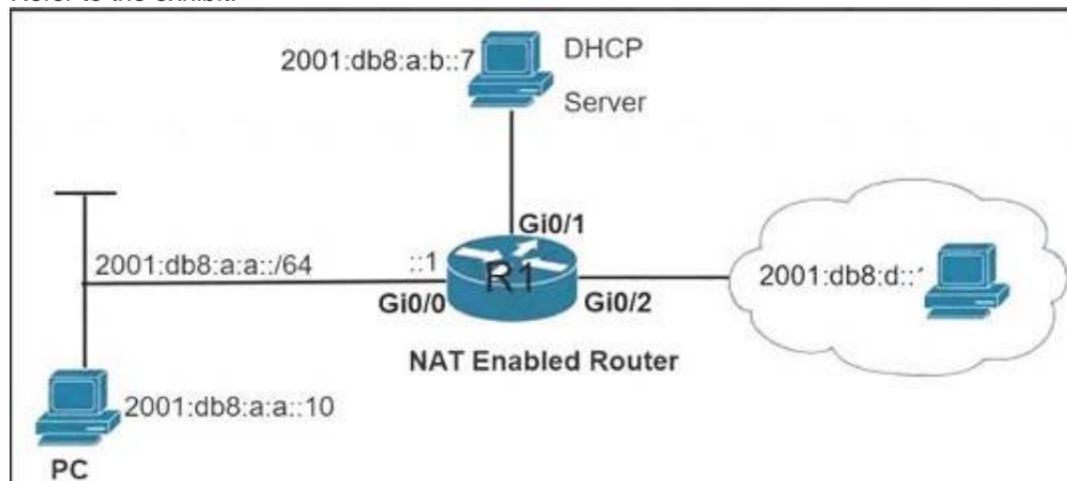
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

**NEW QUESTION 233**

- (Exam Topic 3)

Refer to the exhibit.



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

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

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

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

- A. Remove sequence 30 and add it back to the IPv6 traffic filter as sequence 5.
- B. Remove sequence 20 and add it back to the IPv6 traffic filter as sequence 5.
- C. Remove sequence 10 to add the PC source IP address and add it back as sequence 10.
- D. Remove sequence 20 for sequence 40 in the access list to allow Telnet.

**Answer: B**

**NEW QUESTION 238**

- (Exam Topic 3)  
 Refer to the exhibit.

```
interface Tunnel0
 ip address 172.23.5.10 255.255.255.0
 no ip redirects
 ip mtu 1420
 ip nhrp authentication C@trts81
 ip nhrp map multicast 192.168.200.1
 ip nhrp map 172.23.5.1 192.168.200.1
 ip nhrp network-id 10
 ip nhrp holdtime 300
 ip nhrp shortcut
 ip ospf network broadcast
 ip ospf priority 0
 tunnel source 192.168.100.146
 tunnel mode gre multipoint
 tunnel key 100
```

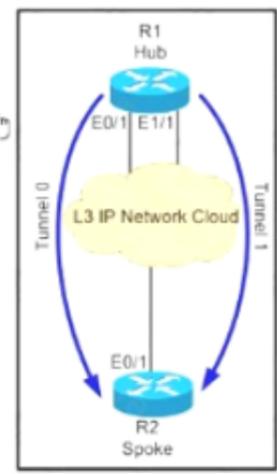
A network engineer is adding a new spoke router into an existing DMVPN Phase 3 tunnel with a hub router to provide secure communication between sites Which additional configuration must the engineer apply to enable the tunnel to come up?

- A. ip nhrp registration no-unique
- B. ip nhrp server-only non-caching
- C. ip nhrp responder tunnel
- D. ip nhrpns 172.23.5.1

Answer: D

**NEW QUESTION 240**

- (Exam Topic 3)



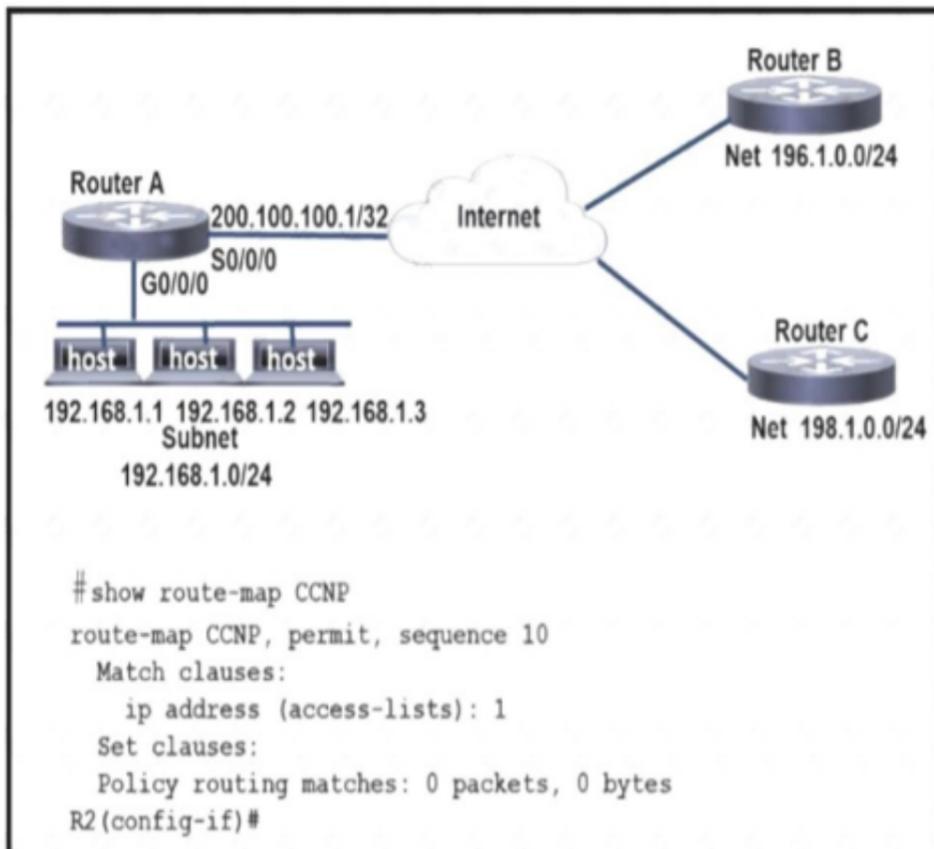
Refer to me exhibit. The hub and spoke are connected via two DMVPN tunnel interfaces The NHRP is configured and the tunnels are detected on the hub and the spoke Which configuration command adds an IPsec profile on both tunnel interfaces to encrypt traffic?

- A. tunnel protection ipsec profile DMVPN multipoint
- B. tunnel protection ipsec profile DMVPN tunnel1
- C. tunnel protection ipsec profile DMVPN shared
- D. tunnel protection ipsec profile DMVPN unique

Answer: C

**NEW QUESTION 241**

- (Exam Topic 3)



Refer to the exhibit. An engineer configures router A to mark all inside to outside traffic from network 192.168.1.0, except from host 192.168.1.1, with critical IP precedence. The policy did not work as expected. Which configuration resolves the issue?

A)

```

RouterA(config)#access-list 1 deny host 192.168.1.1
RouterA(config)#route-map CCNP permit 10
RouterA(config)#match ip address 1
RouterA(config)#set ip precedence critical
RouterA(config)#route-map CCNP permit 20
RouterA(config)# interface g0/0/0
RouterA(config-if)#ip address 192.168.1.4 255.255.255.0
RouterA(config-if)#ip policy route-map CCNP
  
```

B)

```

RouterA(config)#access-list 1 deny host 192.168.1.1
RouterA(config)#access-list 1 permit any any
RouterA(config)#route-map CCNP deny 10
RouterA(config)#match ip address 1
RouterA(config)#set ip precedence critical
RouterA(config)#route-map CCNP permit 20
RouterA(config)# interface g0/0/0
RouterA(config-if)#ip address 192.168.1.4 255.255.255.0
RouterA(config-if)#ip policy route-map CCNP
  
```

C)

```

RouterA(config)#access-list 1 deny host 192.168.1.1
RouterA(config)#access-list 1 permit any any
RouterA(config)#route-map CCNP permit 10
RouterA(config)#match ip address 1
RouterA(config)#set ip precedence critical
RouterA(config)#route-map CCNP permit 20
RouterA(config)#set ip precedence critical
RouterA(config)# interface g0/0/0
RouterA(config-if)#ip address 192.168.1.4 255.255.255.0
RouterA(config-if)#ip policy route-map CCNP
  
```

D)

```

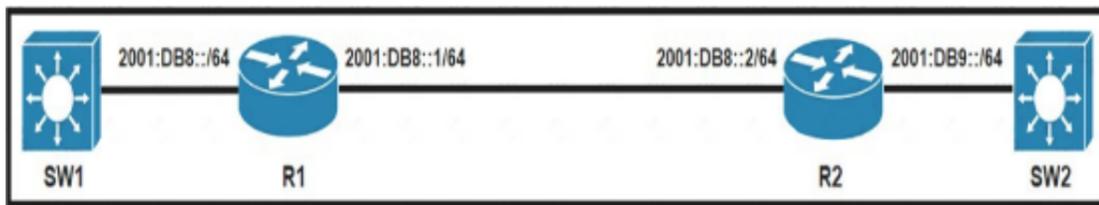
RouterA(config)#access-list 1 deny host 192.168.1.1
RouterA(config)#access-list 1 permit any any
RouterA(config)#route-map CCNP permit 10
RouterA(config)#match ip address 1
RouterA(config)#set ip precedence critical
RouterA(config)# interface g0/0/0
RouterA(config-if)#ip address 192.168.1.4 255.255.255.0
RouterA(config-if)#ip policy route-map CCNP
  
```

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

**Answer: A**

**NEW QUESTION 244**

- (Exam Topic 3)  
 Refer to the exhibit.



An engineer must advertise routes into IPv6 MP-BGP and failed. Which configuration resolves the issue on R1?

- A. router bgp 65000no bgp default ipv4-unicast address-family ipv6 multicast network 2001:DB8::/64
- B. router bgp 65000no bgp default ipv4-unicast address-family ipv6 unicast network 2001:DB8::/64
- C. router bgp 64900no bgp default ipv4-unicast address-family ipv6 unicast network 2001:DB8::/64
- D. router bgp 64900no bgp default ipv4-unicast address-family ipv6 multicastneighbor 2001:DB8:7000::2 translate-update ipv6 multicast

**Answer: B**

**NEW QUESTION 249**

- (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 250**

- (Exam Topic 3)

A network administrator performed a Compact Flash Memory upgrade on a Cisco Catalyst 6509 Switch. Everything is functioning normally except SNMP, which was configured to monitor the bandwidth of key interfaces but the interface indexes are changed. Which global configuration resolves the issue?

- A. snmp-server ifindex permanent
- B. snmp ifindex permanent
- C. snmp-server ifindex persist
- D. snmp ifindex persist

**Answer: C**

**Explanation:**

The SNMP ifIndex persistence feature provides an interface index (ifIndex) value that is retained and used when the router reboots. The ifIndex value is a unique identifying number associated with a physical or logical interface. In the following example, SNMP ifIndex persistence is enabled for all interfaces:  
 router(config)# snmp-server ifindex persist

**NEW QUESTION 254**

- (Exam Topic 3)

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

host	Receives router advertisements from valid routers, and no router solicitation are received.
router	Receives router solicitation and sends router advertisements.
monitor	Receives valid and rogue router advertisements and all router solicitation.
switch	Received router advertisements are trusted and are flooded to synchronize states.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, text, application, email Description automatically generated

Reference:

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/security/configuration/guide/b\\_Ci](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/security/configuration/guide/b_Ci)

**NEW QUESTION 256**

- (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 unreachable
no ip proxy-arp

ip access-list extended GUEST-ACCESS
remark Internet Access Only
permit udp any any eq bootps
permit udp any any eq bootpc
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 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 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 0.0.255
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 ?

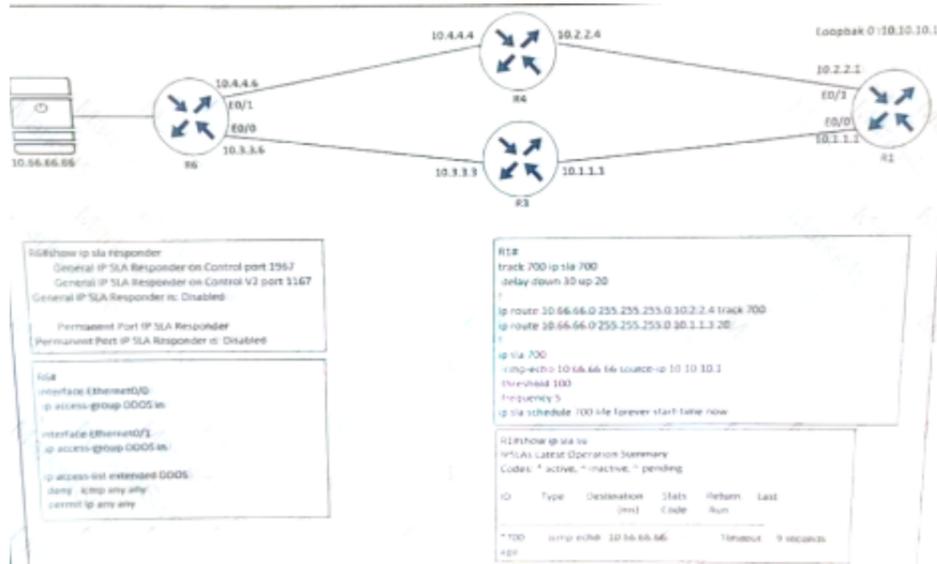
- A. Allow 10.66.46.0/23 in the outbound ACL
- B. Allow DNS traffic through the outbound ACL
- C. Allow DNS traffic through the inbound ACL
- D. Allow 10.66.46.0/23 in the inbound ACL

**Answer: C**

**NEW QUESTION 258**

- (Exam Topic 3)

Refer to the exhibit.



R1 is configured with IP SLA to check the availability of the server behind R6 but it kept failing. Which configuration resolves the issue?

- A. R6(config)# ip sla responder
- B. R6(config)# ip sla responder udp-echo ip address 10.10.10.1 port 5000
- C. R6(config)# ip access-list extended DDOSR6(R6(config ext-nac)# 5 permit icmp host 10.66.66.66 host 10.10.10.1
- D. R6(config)# ip access-list extended DDOSR6(R6(config ext-nac)# 5 permit icmp host 10.10.10.1 host 10.66.66.66

**Answer: D**

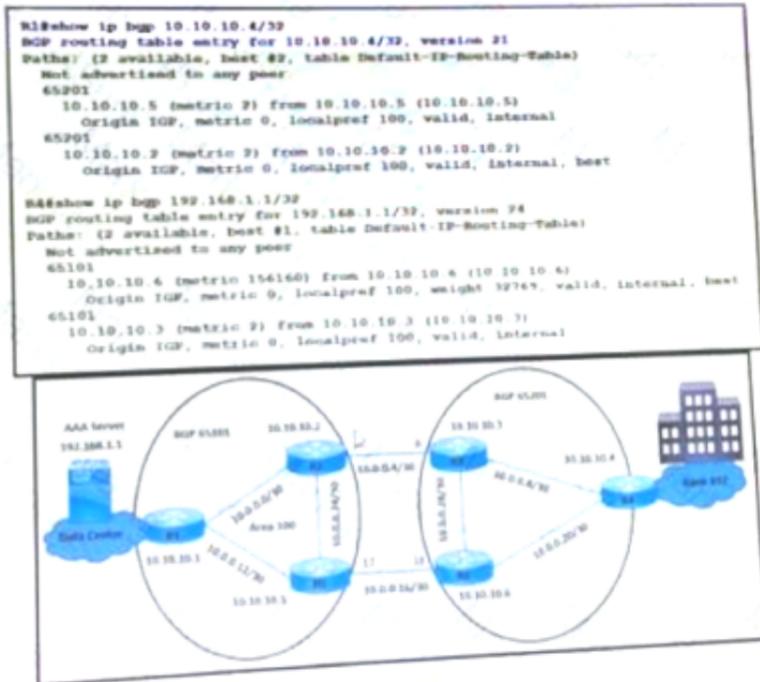
**Explanation:**

In this IP SLA tracking, we don't need a IP SLA Responder so the command "ip sla responder" on R6 is not necessary. We also notice that the ACL is blocking ICMP packets on both interfaces E0/0 & E0/1 of R6 so we need to allow ICMP from source 10.10.10.1 to destination 10.66.66.66.

**NEW QUESTION 260**

- (Exam Topic 3)

Refer to the exhibit.



A customer reports that user traffic of bank XYZ to the AAA server is not using the primary path via the R3-R2 link. The network team observes: No fiber is cut on links R2 and R3.

As101 and AS 201 routers established BGP peering. Which configuration resolves the issue?

A)

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

B)

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

C)

```
R4(config)#router bgp 65201
R4(config-router)#no neighbor 10.10.10.6 weight 32769
```

D)

```
R1(config)#route-map BGP-Path permit 3
R1(config-route-map)# set local-preference 200
R1(config)#router bgp 65101
R1(config-router)# neighbor 10.10.10.2 route-map BGP-Path out
```

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

**Answer: A**

**NEW QUESTION 261**

- (Exam Topic 3)

A network administrator opens a telnet connection to the router and gets the message:

R1#telnet 10.1.1.2

Trying 10.1.1.2 Open

(Connection to 10.1.1.2 closed by foreign host)

Router R2 is configured with enable secret and password commands. Which action resolves the issue?

- A. Configure the logging synchronous command on line vty.
- B. Configure the exec command on line vty.
- C. Configure the login local command on line vty
- D. Configure the enable password command on line vty.

**Answer: C**

**NEW QUESTION 263**

- (Exam Topic 3)

Refer to the exhibit.

```
*Sep 26 19:50:43.504: SNMP: Packet received via UDP from
192.168.1.2 on GigabitEthernet0/1SrParseV3Snmplib: No
matching Engine ID.

SrParseV3Snmplib: Failed.
SrDoSnmplib: authentication failure, Unknown Engine ID

*Sep 26 19:50:43.504: SNMP: Report, reqid 29548, errstat 0,
erridx 0
internet.6.3.15.1.1.4.0 = 3
*Sep 26 19:50:43.508: SNMP: Packet sent via UDP to 192.168.1.2
process_mgmt_req_int: UDP packet being de-queued
```

Which two commands provide the administrator with the information needed to resolve the issue? (Choose two.)

- A. Show snmp user
- B. debug snmp engine-id
- C. debug snmpv3 engine-id
- D. debug snmp packet
- E. showsnmpv3 user

**Answer:** AD

**Explanation:**

There are 3 values in the SNMPv3 header that must match for the communication to take place: snmpEngineID, snmpEngineTime, snmpEngineBoots. The error received indicates a problem with the EngineID value: "authentication failure, Unknown Engine ID"

To specify the Engine ID, we can use the command "show snmp user". The following example specifies the username as abcd with Engine ID: 00000009020000000C025808:

```
Router#show snmp user abcd
User name: abcd
Engine ID: 00000009020000000C025808
storage-type: nonvolatile active access-list: 10
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: 3DES
Group name: VacmGroupName
Group name: VacmGroupName
```

The "debug snmp packet" command displays all SNMP packets that are arriving and being replied to.

**NEW QUESTION 266**

- (Exam Topic 3)

The network administrator configured CoPP so that all routing protocol traffic toward the router CPU is limited to 1 mbps. All traffic that exceeds this limit must be dropped. The router is running BGP and OSPF Management traffic for Telnet and SSH must be limited to 500kbps.

```
access-list 100 permit tcp any any eq 179 access-list 100 permit tcp any any range 22 23 access-list 100 permit ospf any any
!
```

```
class-map CM-ROUTING match access-group 100 class-map CM-MGMT match access-group 100
!
```

```
policy-map PM-COPP class CM-ROUTING
police 1000000 conform-action transmit class CM-MGMT
police 500000 conform-action transmit
!
```

control-plane

service-policy output PM-COPP

No traffic is filtering through CoPP, which is resulting in high CPU utilization, which configuration resolves the issue ?

- A. no access-list 100access-list 100 permit tcp any any eq 179 access-list 100 permit ospf any anyaccess-list 101 Permit tcp any any range 22 23!class-map CM-MGMTno match access-group 100 match access-group 101
- B. control-planeno service-policy output PM-COPP service-policy input PM-COPP
- C. No access-list 100access-list 100 permit tcp any any eq 179 access-list 100 permit tcp any any range eq 22 access-list 100 permit tcp any any range eq 23 access-list 100 permit ospf any any
- D. no access-list 100access-list 100 permit tcp any any eq 179 access-list 100 permit ospf any anyaccess-list 101 Permit tcp any any range 22 23!class-map CM-MGMTno match access-group 100 match access-group 101!control-planeno service-policy output PM-COPP service-policy input PM-COPP

**Answer:** D

**NEW QUESTION 267**

- (Exam Topic 3)

```
CPE# copy flash:packages.conf ftp://192.0.2.40/
Address or name of remote host [192.0.2.40]?
Destination filename [packages.conf]?
Writing packages.conf
%Error opening ftp://192.0.2.40/packages.conf (Incorrect
Login/Password)
CPE#
```

Refer to the exhibit. An administrator must upload the packages conf file to an FTP server. However, the FTP server rejected anonymous service and required users to authenticate. What are the two ways to resolve the issue? (Choose two.)

- A. Use is ftp username and ip ftp password configuration commands to specify valid FTP server credentials.
- B. Use the copy flash:packages.conf scp: command instead and enter the FTP server credentials when prompted.
- C. Enter the FTP server credentials directly In the FTP URL using the ftp://username:password@192.0.2.40/ syntax .
- D. Create a user on the router matching the username and password on the FTP server and log in before attempting the copy
- E. Use the copy flash-packages conf ftp: command instead and enter the FTP server credent-ais when prompted.

**Answer:** AC

**NEW QUESTION 272**

- (Exam Topic 3)

Refer to the exhibit.

```

R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

D    10.0.0.0/8 [90/409600] via 172.16.1.200, 00:00:28, Ethernet0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.1.0/24 is directly connected, Ethernet0/0
L    172.16.1.100/32 is directly connected, Ethernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, Loopback0
L    192.168.1.100/32 is directly connected, Loopback0
R1#
    
```

The R2 loopback interface is advertised with RIP and EIGRP using default values. Which configuration changes make R1 reach the R2 loopback using RIP?

- A. R1(config)# router rip R1(config-router)# distance 90
- B. R1(config)# router rip R1(config-router)# distance 100
- C. R1(config)# router eigrp 1R1(config-router)# distance eigrp 130 120
- D. R1(config)# router eigrp 1R1(config-router)# distance eigrp 120 120

**Answer:** C

**Explanation:**

distance (AD Number u want to change to) (neighbor IP) (Wildcard Mask) (access-list number)

**NEW QUESTION 276**

- (Exam Topic 3)



Refer to the exhibit. An engineer is investigating an OSPF issue reported by the Cisco DNA Assurance Center. Which action resolves the issue?

- A. One of the neighbor links is down Bring the interface up by running shut and no shut
- B. One of the interfaces is using the wrong MTU Match interface MTU on both links
- C. An ACL entry blocking multicast on the interfaces Allow multicast through the interface ACL
- D. One of the interfaces is using the wrong authentication Match interface authentication on both links

**Answer:** B

**NEW QUESTION 277**

- (Exam Topic 3)

Refer to the exhibit.

```
CPE# show ntp associations
address      ref clock    st  when  poll reach delay
offset  disp
-10.1.255.40 .INIT.      16      64    0 0.000
0.000 15937.
* syn.peer, † selected, † candidate, - outlier, x false ticker,
- configured

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

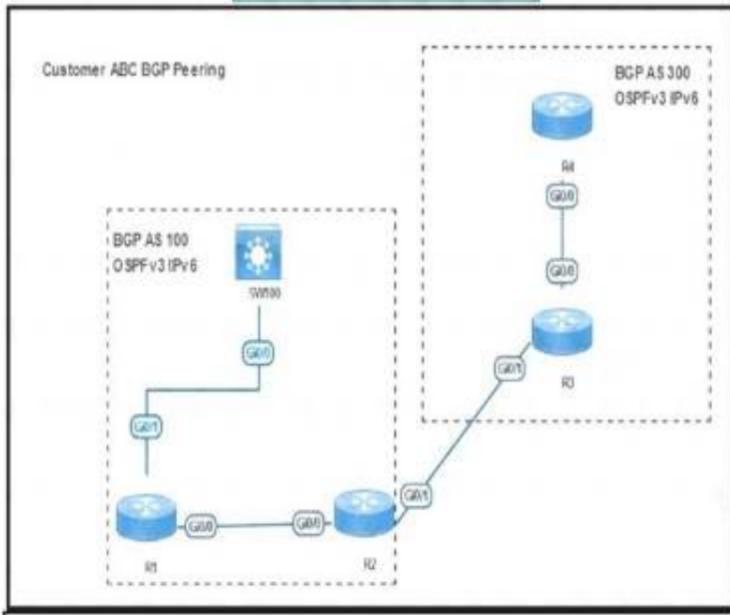
An administrator is troubleshooting a time synchronization problem for the router time to another Cisco IOS XE-based device that has recently undergone hardening. Which action resolves the issue?

- A. Allow NTP in the ingress ACL on 10.1.225.40 by permitting UDP destined to port 123.
- B. Ensure that the CPE router has a valid route to 10.1.255.40 for NTP and rectify if not reachable.
- C. NTP service is disabled and must be enabled on 10.1.225.40.
- D. Allow NTP in the ingress ACL on 10.1.255.40 by permitting TCP destined to port 123.

**Answer: C**

**NEW QUESTION 278**

- (Exam Topic 3)



```
SW100#sh ip bgp ipv6 uni summ
BGP router identifier 100.0.0.1, local AS number 100
BGP table version is 1, main routing table version 1

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
2001:ABC:AABB:1100:1122:1111:2222:AAA1
              4      100      6      5        1    0    0 00:00:58      0

SW100#sh ip bgp ipv6 unicast
SW100#

R1#sh ip bgp ipv6 uni
BGP table version is 4, local router ID is 1.1.1.1
  Network      Next Hop      Metric LocPrf Weight Path
  * i  2001::4/128  2001::4        0   100   0 300 i
  *>i  2002::2/128  2001::2        0   100   0 i
R1#
R1#sh ipv6 route
O  2001::2/128 [110/1]
   via FE80::5200:C3FF:FE01:E600, GigabitEthernet0/0
B  2002::2/128 [200/0]
   via 2001::2
```

Refer to the exhibit SW100 cannot receive routes from R1 Which configuration resolves the issue?

- R1
 

```
router bgp 100
address-family ipv6
neighbor 2001::2 route-reflector-client
neighbor 2001:ABC:AABB:1100:1122:1111:2222:AAA2 route-reflector-client
```
- R2
 

```
router bgp 100
address-family ipv6
neighbor 2001::2
neighbor 2001::1 next-hop-self
```
- R1
 

```
router bgp 100
address-family ipv6
neighbor 2001::2 route-reflector-client
neighbor 2001:ABC:AABB:1100:1122:1111:2222:AAA2 route-reflector-client
```
- R2
 

```
router bgp 100
address-family ipv6
neighbor 2001::2
neighbor 2001::1 as-override
```
- R1
 

```
router bgp 100
address-family ipv6
no synchronization
```
- R2
 

```
router bgp 100
address-family ipv6
no synchronization
SW100
router bgp 100
address-family ipv6
no synchronization
```
- R1
 

```
router bgp 100
address-family ipv6
redistribute connected
```
- R2
 

```
router bgp 100
address-family ipv6
redistribute connected
```

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

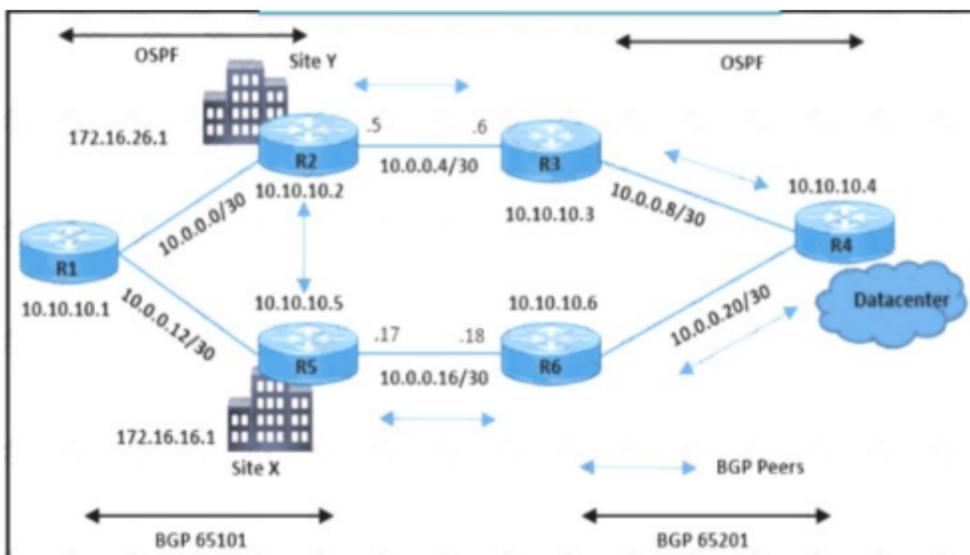
Answer: A

**NEW QUESTION 279**

- (Exam Topic 3)

```
R5#
*Sep 19 08:29:51.088: BGP: 10.10.10.2 open active, local address 10.0.0.14
*Sep 19 08:29:51.120: BGP: 10.10.10.2 read request no-op
*Sep 19 08:29:51.124: BGP: 10.10.10.2 open failed: Connection refused by
remote host, open active delayed 12988ms (20000ms max, 60% jitter)

R2#show ip bgp neighbors 10.10.10.5
BGP neighbor is 10.10.10.5, remote AS 65101, internal link
BGP version 4, remote router ID 0.0.0.0
BGP state = Active
Last read 00:01:18, last write 00:01:18, hold time is 15, keepalive
interval is 3 seconds
Configured hold time is 15, keepalive interval is 3 seconds
Minimum holdtime from neighbor is 0 seconds
Address tracking is enabled, the RIB does have a route to 10.10.10.5
Connections established 13; dropped 13
Last reset 00:01:18, due to User reset
Transport(tcp) path-mtu-discovery is enabled
No active TCP connection
```



Refer to the exhibit A customer reported a failure and intermittent disconnection between two office buildings site X and site Y The network team finds that site X

and site Y are exchanging email application traffic with the data center network Which configuration resolves the issue between site X and site Y?

- A)  
 RC(config)# ip prefix-list Customer seq 5 permit 192.168.30.1/32
- B)  
 RC(config)#router bgp 65101  
 RC(config-router)# neighbor 10.0.0.18 prefix-list Customer in
- C)  
 RF(config)#no ip prefix-list Customer seq 5 deny 192.168.1.1/32
- D)  
 RF(config)#router bgp 65201  
 RF(config-router)# neighbor 10.0.0.17 prefix-list Customer out

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

Answer: C

**NEW QUESTION 282**

- (Exam Topic 3)

Refer to the exhibit.

```

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

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

Which command resolves this issue?

- A. access-class INTERNET in
- B. ip access-group INTERNET in
- C. ipv6 traffic-filter INTERNET in
- D. ipv6 access-class INTERNET in

Answer: D

**NEW QUESTION 286**

- (Exam Topic 3)

Refer to the exhibit.

```

R1# show ip ospf database self-originate
      OSPF Router with ID (10.255.255.1) (Process ID 1)
      Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum
Link count
10.255.255.1 10.255.255.1 4           0x800003BD  0x001AD9
3

      Summary Net Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum
10.0.34.0    10.255.255.1 3604        0x80000380  0x00276C
10.255.255.4 10.255.255.1 3604        0x80000380  0x00762B

      Type-5 AS External Link States

Link ID      ADV Router   Age         Seq#         Checksum
Tag
0.0.0.0      10.255.255.1 3604        0x800001D0  0x001C8C
0

*Feb 22 22:50:39.523: %OSPF-4-FLOOD_WARN: Process 1 flushes LSA
ID 0.0.0.0 type-5 adv-rtr 10.255.255.1 in area 0
  
```

After configuring OSPF in R1, some external destinations in the network became unreachable. Which action resolves the issue?

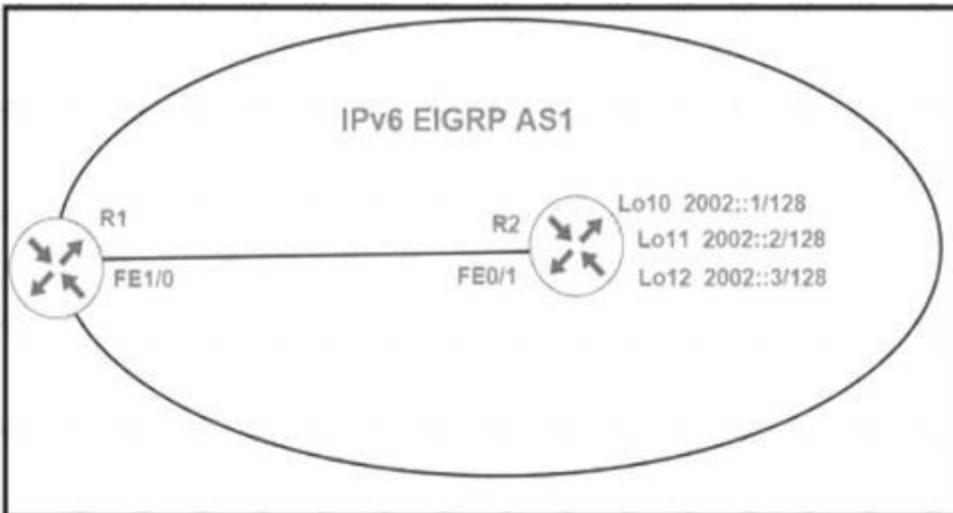
- A. Clear the OSPF process on R1 to flush stale LSAs sent by other routers.
- B. Change the R1 router ID from 10.255.255.1 to a unique value and clear the process.
- C. Increase the SPF delay interval on R1 to synchronize routes.
- D. Disconnect the router with the OSPF router ID 0.0.0.0 from the network.

Answer: B

**NEW QUESTION 290**

- (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, I - 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. EIGRP process on R2 with the command stub summary connected

Answer: D

**NEW QUESTION 293**

- (Exam Topic 3)

```

GigabitEthernet2 is up, line protocol is up
Internet Address 172.16.1.42/30, Interface ID 8, Area 1
Attached via Network Statement
Process ID 1, Router ID 172.16.100.7, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
0 1 no no Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 172.16.100.7, Interface address 172.16.1.42
Backup Designated router (ID) 172.16.100.5, Interface address 172.16.1.41
Timer Intervals configured, Hello 10, Dead 40, wait 40, Retransmit 5
 oob-resync timeout 40
 hello due in 00:00:01

Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 172.16.100.5 (Backup Designated Router)
 Suppress hello for 0 neighbor(s)
 Cryptographic authentication enabled
 Sending SA: key 1, Algorithm HMAC-SHA-256 - key chain ospf
 Rollover in progress, 1 neighbor(s) using the old key(s):
 key id 1 algorithm MD5
CSR103#
CSR103#
CSR103#sh ip ospf nei

Neighbor ID Pri State Dead Time Address Interface
172.16.100.3 1 FULL/DR 00:00:30 172.16.1.25 GigabitEthernet3
172.16.100.5 1 FULL/BDR 00:00:16 172.16.1.41 GigabitEthernet2
CSR103#
CSR103#
*Jan 11 16:49:35.311: %SYS-6-LOGOUT: user admin has exited tty session 1(10.228.200.250)
*Jan 11 16:49:45.396: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.100.5 on GigabitEthernet2 from
FULL to DOWN, Neighbor Down: Dead timer expired

```

Refer to the exhibit. Which configuration resolves the issue?

A)

```

router ospf 1
 area 1 authentication message-digest
 int GigabitEthernet 2
 ip ospf message-digest-key 1 md5 cisco

```

B)

```

int GigabitEthernet 2
 ip ospf message-digest-key 1 md5 cisco
 ip ospf authentication message-digest

```

C)

```

int GigabitEthernet 2
 ip ospf key 1 cisco
 ip ospf authentication

```

D)

```

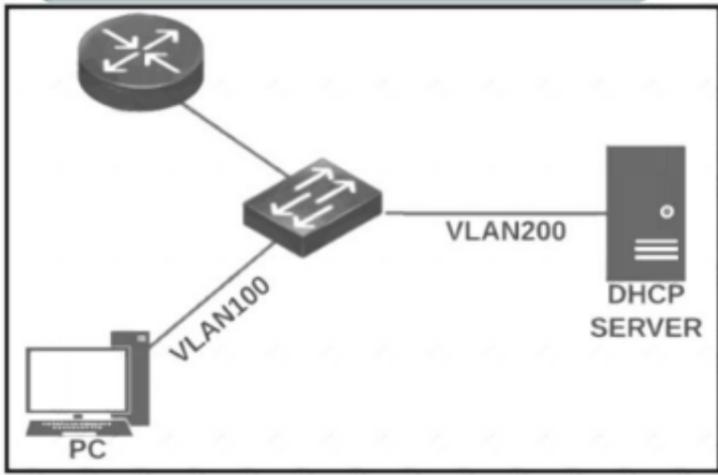
key chain ospf
 key 1
 key-string 7 02050D480809
 cryptographic-algorithm hmac-sha-1
 interface GigabitEthernet2
 ip ospf authentication key-chain ospf

```

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

**Answer: D**

**NEW QUESTION 295**  
 - (Exam Topic 3)



Refer to the exhibit. APC is configured to obtain an IP address automatically, but it receives an IP address only from the 169.254.0.0 subnet. The DHCP server logs contained no DHCPDISCOVER message from the MAC address of the PC. Which action resolves the issue?

- A. Configure an ip helper-address on the router to forward DHCP messages to the server.
- B. Configure DHCP Snooping on the switch to forward DHCP messages to the server.
- C. Configure a DHCP reservation on the server for the PC.
- D. Configure a static IP address on the PC and exclude it from the DHCP pool.

**Answer: A**

**NEW QUESTION 296**

- (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?

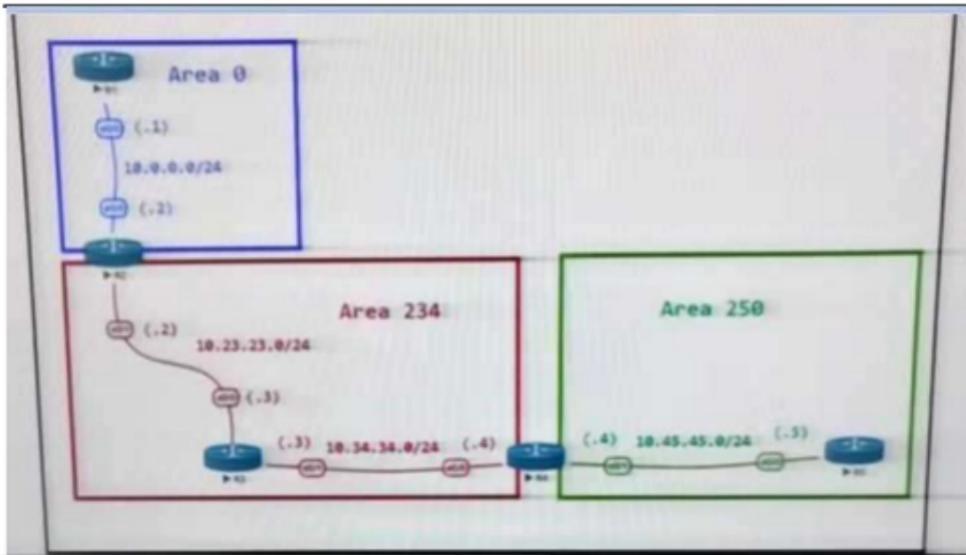
- A. MP-BGP uses control plane services for label prefix bindings in the MPLS forwarding table
- B. LSP uses NSF to recover from disruption \*i control plane service
- C. FEC uses a control plane service to distribute information between primary and secondary processors
- D. LDP uses SSO to recover from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

**Answer: C**

**NEW QUESTION 298**

- (Exam Topic 3)

Refer to the exhibit.



ABR Configurations	
<b>R2</b> router ospf 1 router-id 0.0.0.22 area 234 virtual-link 10.34.34.4 network 10.0.0.0 0.0.0.255 area 0 network 10.2.2.0 0.0.0.255 area 0 network 10.22.22.0 0.0.0.255 area 234 network 10.23.23.0 0.0.0.255 area 234	<b>R4</b> router ospf 1 router-id 0.0.0.44 area 234 virtual-link 10.23.23.2 network 10.34.34.0 0.0.0.255 area 234 network 10.44.44.0 0.0.0.255 area 234 network 10.45.45.0 0.0.0.255 area 250

Virtual Link Status	
<b>R2 -&gt; sh ip ospf virtual-links</b> Virtual Link OSPF_VL0 to router 10.34.34.4 is down Run as demand circuit DoNotAge LSA allowed. Transit area 234 Topology-MTID Cost Disabled Shutdown Topology Name 0 65535 no no Base Transmit Delay is 1 sec, State DOWN.	

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

- A. R2router ospf 1router-id 10.23.23.2
- B. R2router ospf 1no area area 234 virtual-link 10.34.34.4area 0 virtual-link 0.0.0.44
- C. R4router ospf 1no area 234 virtual-link 10.23.23.2area 234 virtual-link 0.0.0.22

- D. R2router ospf 1no area 234 virtual-link 10.34.34.4area 234 virtual-link 0.0.0.44
- E. R4router ospf 1no area area 234 virtual-link 10.23.23.2area 0 virtual-link 0.0.0.22

**Answer:** CD

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html> An important thing to remember when configuring virtual-link is we need to configure the OSPF router ID and NOT the IP address of the ABR. Therefore in this question we have to use the command "area 234 virtual-link 0.0.0.44" on R2 and "area 234 virtual-link 0.0.0.22" on R4.

**NEW QUESTION 299**

- (Exam Topic 3)

Refer to the exhibit.

```
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.
```

Which command must be configured to make VRF CCNP work?

- A. interface Loopback0 vrf forwarding CCNP
- B. interface Loopback0ip address 10.1.1.1 255.255.255.0
- C. interface Loopback0ip address 10.1.1.1 255.255.255.0 vrf forwarding CCNP
- D. interface Loopback0ip address 10.1.1.1 255.255.255.0ip vrf forwarding CCNP

**Answer:** B

**Explanation:**

From the exhibit, we learn that the command "ip address 10.1.1.1 255.255.255.0" has been issued before the command "ip vrf forwarding CCNP". But the second command removed the IP address configured in the first command so we have to retype the IP address command.

**NEW QUESTION 301**

- (Exam Topic 3)

Drag and drop the descriptions from the left onto the corresponding MPLS components on the right.

FEC	routers in the core of the provider network known as P routers
LSP	all traffic to be forwarded using the same path and same label
LER	routers that connect to the customer routers known as PE routers
LSR	used for exchanging label mapping information between MPLS enabled routers
LDP	path along which the traffic flows across an MPLS network

- A. Mastered
- B. Not Mastered

**Answer:** A

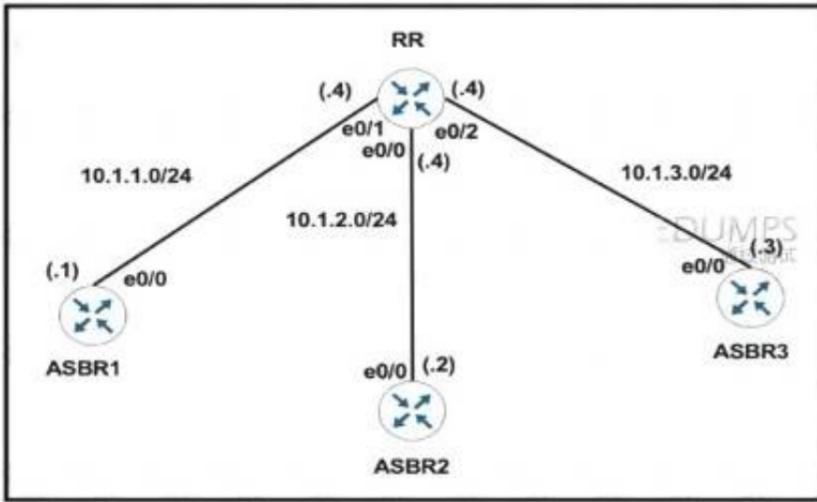
**Explanation:**

Table Description automatically generated

**NEW QUESTION 306**

- (Exam Topic 3)

Refer to the exhibit.



RR Configuration:

```
router bgp 100
neighbor IBGP peer-group
neighbor IBGP route-reflector-client
neighbor 10.1.1.1 remote-as 100
neighbor 10.1.2.2 remote-as 100
neighbor 10.1.3.3 remote-as 100
```

The network administrator configured the network to establish connectivity between all devices and notices that the ASBRs do not have routes for each other. Which set of configurations resolves this issue?

- router bgp 100
  - neighbor 10.1.1.1 next-hop-self
  - neighbor 10.1.2.2 next-hop-self
  - neighbor 10.1.3.3 next-hop-self
- router bgp 100
  - neighbor IBGP update-source Loopback0
- router bgp 100
  - neighbor IBGP next-hop-self
- router bgp 100
  - neighbor 10.1.1.1 peer-group IBGP
  - neighbor 10.1.2.2 peer-group IBGP
  - neighbor 10.1.3.3 peer-group IBGP

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

Answer: D

**NEW QUESTION 309**

- (Exam Topic 3)

Refer to the exhibit.

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

R1#show ip route eigrp | include 10.
D EX 10.0.0.0/8 [170/2665332] via 192.168.10.1, 00:00:10,
Ethernet0/0
```

An engineer applies a prefix-list filter that filters most of the network 10 prefixes instead of allowing them. Which action resolves the issue?

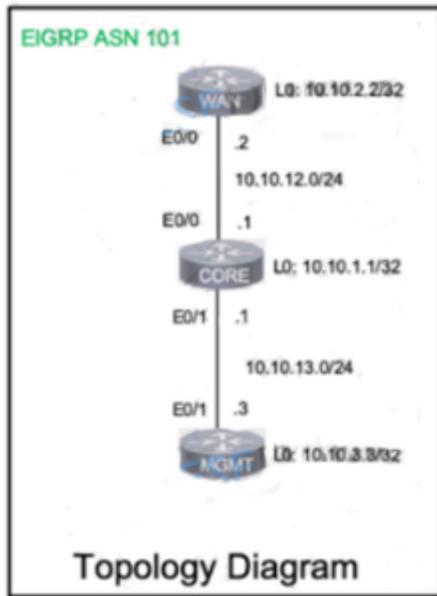
- A. Modify the ip prefix-list EIGRP seq 10 permit 10.0.0.0/8 le 9 command.
- B. Modify the command Modify the Ip prefix-list EIGRP seq 10 permit 10.0.0.0/8 le 32 command.
- C. Modify the Ip prefix-list EIGRP seq 20 permit 0.0.0.0/0 le 32 command.
- D. Modify the ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9 command

Answer: C

**NEW QUESTION 311**

- (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:



Guidelines | Topology | **Tasks**

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 any 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
!
```

```
WAN  CORE  MGMT
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
 ip address 172.16.2.2 255.255.255.0
!
interface Ethernet0/0
 ip address 10.10.12.2 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 network 172.16.2.0 0.0.0.255
 eigrp router-id 10.10.2.2
```

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

CORE

```

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

```

```

!
interface 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

```

WAN  CORE  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

```

```

WAN  CORE  MGMT
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 telnet
!
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 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 Uptime
me  SRTT    RTO   Q   Seq
   (ms)          Cnt Num
0   10.10.13.3      Et0/1         11 00:00
3:15   5    100  0   35
1   10.10.12.2      Et0/0         11 00:00
3:24   7    100  0   33
CORE#copy run star
    
```

MGMT  
 Graphical user interface, text Description automatically generated

```

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 313**

- (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?

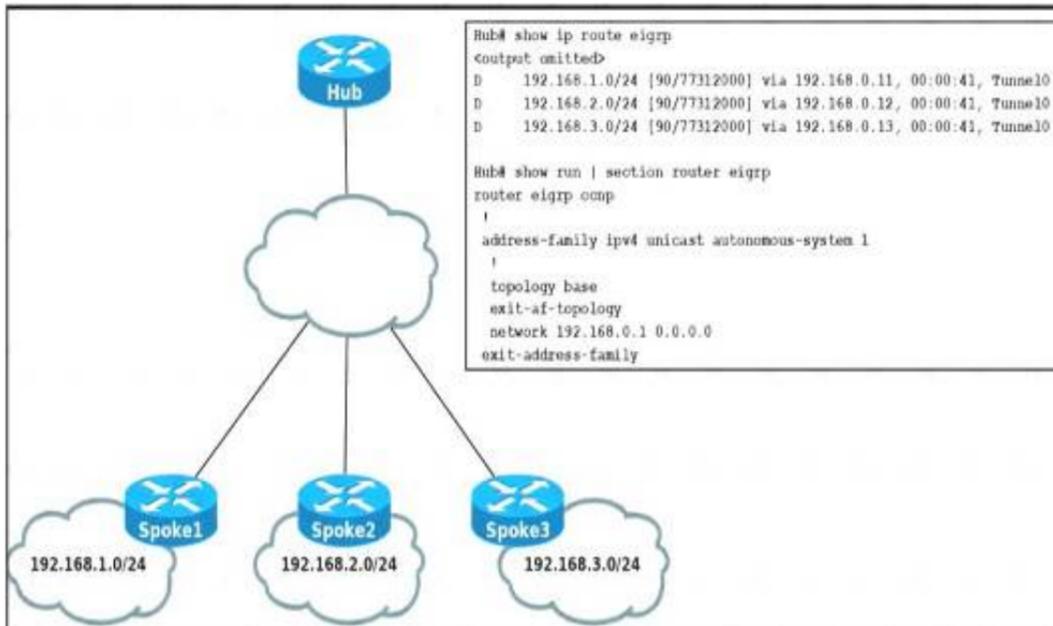
- A. RC(config)#router bgp 65201RC(config-router)#neighbor 10.10.10.4 route-reflector-client
- B. RF(config)#router bgp 65201RF(config-router)#neighbor 10.10.10.6 route-reflector-client
- C. RC(config)#router bgp 65201RC(config-router)#neighbor 10.10.10.2 route-reflector-client
- D. RB(config)#router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

**Answer: A**

**NEW QUESTION 314**

- (Exam Topic 3)

Refer to the exhibit.



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 Tunnel0 interface of the hub router.

**Answer: D**

**NEW QUESTION 316**

- (Exam Topic 3)

Refer to the exhibit.

```

R2# show ip ospf neighbor
R2#
R2# debug ip ospf hello

*Feb 22 23:46:58.699: OSPF-1 HELLO Et1/1: Rcv hello from
10.255.255.1 area 0 10.0.23.1
*Feb 22 23:46:58.703: OSPF-1 HELLO Et1/1: Mismatched hello
parameters from 10.0.23.1
*Feb 22 23:46:58.703: OSPF-1 HELLO Et1/1: Dead R 30 C 20, Hello
R 10 C 10 Mask R 255.255.255.0 C 255.255.255.0
    
```

The connected routers do not show up as OSPF neighbors. Which action resolves the issue?

- A. Change the R1 dead timer to 20.
- B. Change the R2 dead timer to 20.
- C. Change the R2 hello timer to 20.
- D. Change the R1 hello timer to 20.

**Answer: A**

**NEW QUESTION 320**

- (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 connect 32 seconds ago
                                     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 322**

- (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 on R3 E0/0
- B. 120 on R4 E0/1

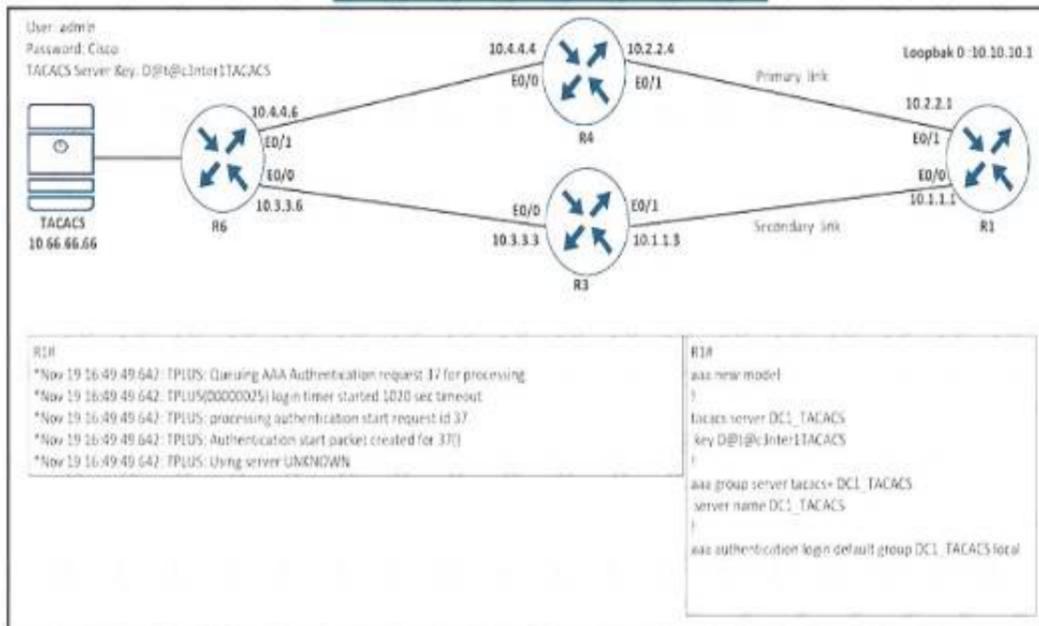
C. 120/ on R3 E0/1  
 D. 2200 on R4 E0/1

**Answer: C**

**NEW QUESTION 324**

- (Exam Topic 3)

Refer to the exhibit.



Refer to the exhibit

R1 cannot authenticate via TACACS

Which configuration resolves the issue?

- aaa group server tacacs+ DC\_TACACS**  
**server name DC\_TACACS**
- tacacs server DC1\_TACACS**  
**address ipv4 10.66.66.66**  
**key D@t@c3nter1TACACS**
- aaa group server tacacs+ DC1\_TACACS**  
**server name DC\_TACACS**
- tacacs server DC1\_TACACS**  
**address ipv4 10.60.66.66**  
**key D@t@c3nter1TACACS**

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

**Answer: B**

**NEW QUESTION 329**

- (Exam Topic 3)

Which function does LDP provide in an MPLS topology?

- A. It enables a MPLS topology to connect multiple VPNs to P routers.
- B. It provides hop-by-hop forwarding in an MPLS topology for LSRs.
- C. It exchanges routes for MPLS VPNs across different VRFs.
- D. It provides a means for LSRs to exchange IP routes.

**Answer: B**

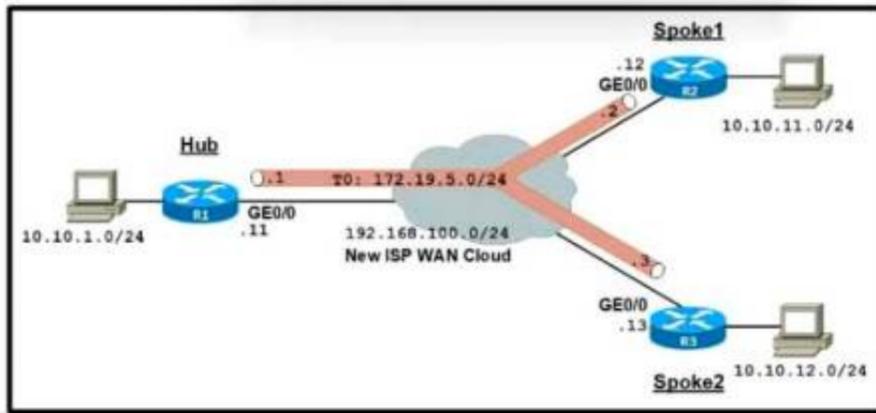
**Explanation:**

LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward label traffic across an MPLS backbone to particular destinations.

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp\\_ldp/configuration/12-4t/mp-ldp-12-4t-book.pdf](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4t/mp-ldp-12-4t-book.pdf)

**NEW QUESTION 334**

- (Exam Topic 3)



<pre>R1 interface Tunnel0 ip address 172.19.5.1 255.255.255.0 ip nhrp authentication t81i\$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</pre>	<pre>R2 interface Tunnel0 ip address 172.19.5.2 255.255.255.0 ip nhrp authentication t81i\$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</pre>	<pre>R3 interface Tunnel0 ip address 172.19.5.3 255.255.255.0 ip nhrp authentication t81i\$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</pre>
---	---	---

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 336**

- (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](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 341**

- (Exam Topic 3)

In a DMVPN network, the Spoke1 user observed that the voice traffic is coming to Spoke2 users via the hub router. Which command is required on both spoke routers to communicate directly to one another?

- A. ip nhrp map dynamic
- B. ip nhrp shortcut
- C. ip nhrp nhs multicast
- D. ip nhrp redirect

**Answer: B**

**NEW QUESTION 343**

- (Exam Topic 3)

How is VPN routing information distributed in an MPLS network?

- A. The top level of the customer data packet directs it to the correct CE device
- B. It is established using VPN IPsec peers.
- C. It is controlled using of VPN target communities.
- D. It is controlled through the use of RD.

**Answer: C**

**Explanation:**

The distribution of virtual private network (VPN) routing information is controlled through the use of VPN route target communities, implemented by Border Gateway Protocol (BGP) extended communities.

Reference:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp\\_l3\\_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/m](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/m)

**NEW QUESTION 348**

- (Exam Topic 2)

What are two functions of LDP? (Choose two.)

- A. It is defined in RFC 3038 and 3039.
- B. It requires MPLS Traffic Engineering.
- C. It advertises labels per Forwarding Equivalence Class.
- D. It must use Resource Reservation Protocol.
- E. It uses Forwarding Equivalence Class

**Answer: CE**

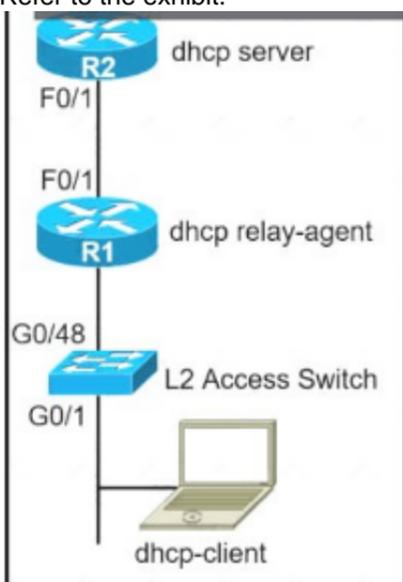
**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5\\_x/nx-os/mpls/configuration/guide/mpls\\_cg/mp](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/mpls/configuration/guide/mpls_cg/mp)

**NEW QUESTION 352**

- (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: DHCPDP: inconsistent relay information. *Feb 22 23:54:57.759: DHCPDP: 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 356**

- (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 in 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 in the output direction

**Answer: B**

**NEW QUESTION 357**

- (Exam Topic 2)

Refer to the exhibit.

```
ipv6 access-list inbound
permit tcp any any
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound out
```

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

- ```
ipv6 access-list inbound
permit tcp any any established
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound out
```
- ```
ipv6 access-list inbound
permit tcp any any syn
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound out
```
- ```
ipv6 access-list inbound
permit tcp any any established
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound in
```
- ```
ipv6 access-list inbound
permit tcp any any syn
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound in
```

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

**Answer: C**

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/122\\_55\\_se/configuration/guid](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/122_55_se/configuration/guid)

**NEW QUESTION 358**

- (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:**

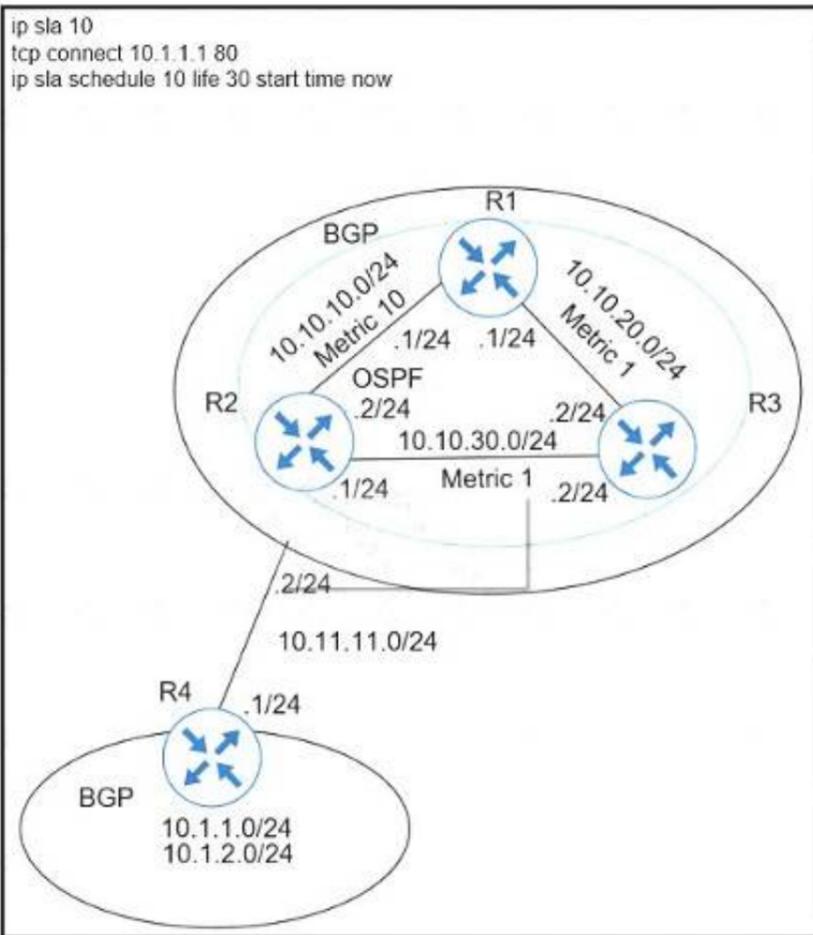
**Neighbors Stuck in Exstart/Exchange State**

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 than the MTU set on the neighboring router, the neighboring router ignores the packet. When

**NEW QUESTION 361**

- (Exam Topic 2)

Refer to the exhibit.



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

- A. Re-issue the ip sla schedule command.
- B. Add icmp-echo command for the host.
- C. Add the control disable option to the tcp connect.
- D. Modify the ip sla schedule frequency to forever.

**Answer: C**

**NEW QUESTION 365**

- (Exam Topic 2)

Refer to the exhibit.

```
login block-for 15 attempts 10 within 120
login on-failure log
login on-success log
archive
log config
logging enable
logging size 300
notify syslog
```

```
snmp-server enable traps syslog
snmp-server host 172.16.17.1 public syslog
```

The administrator can see the traps for the failed login attempts, but cannot see the traps of successful login attempts. What command is needed to resolve the issue?

- A. Configure logging history 2
- B. Configure logging history 3
- C. Configure logging history 4
- D. Configure logging history 5

**Answer:** D

**Explanation:**

By default, the maximum severity sent as a syslog trap is warning. That is why you see syslog traps for login failures. Since a login success is severity 5 (notifications), those syslog messages will not be converted to traps. To fix this, configure:

**logging history 5**

Syslog levels are listed below

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

Note:

The syntax of login block is:

login block-for seconds attempts tries within seconds

**NEW QUESTION 366**

- (Exam Topic 2)

Refer to the exhibit.

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

Which two actions should be taken to access the server? (Choose two.)

- A. Modify the access list to add a second line of permit ip any
- B. Modify the access list to deny the route to 192.168.2.2.
- C. Modify distribute list seq 10 to permit the route to 192.168.2.2.
- D. Add a sequence 20 in the route map to permit access list 1.
- E. Add a floating static route to reach to 192.168.2.2 with administrative distance higher than OSPF

**Answer:** BE

**NEW QUESTION 368**

- (Exam Topic 2)

Refer to the exhibit.

```
Debug output:
username: USER55
password:
Aug 26 12:39:23.813: TPLUS: Queuing AAA Authentication request 4950 for processing
Aug 26 12:39:23.813: TPLUS(00001356) login timer started 1020 sec timeout
Aug 26 12:39:23.813: TPLUS: processing authentication continue request id 4950
Aug 26 12:39:23.813: TPLUS: Authentication continue packet generated for 4950
Aug 26 12:39:23.813: TPLUS(00001356)/0/WRITE/3A72C8D0: Started 5 sec timeout
!
!---- output omitted ----!
!
Aug 26 12:40:01.241: TAC+: using previously set server 192.168.1.3 from group tacacs+
Aug 26 12:40:01.241: TAC+: Opening TCP/IP to 192.168.1.3/49 timeout=5
Aug 26 12:40:01.249: TAC+: Opened TCP/IP handle 0x3BE31D1C to 192.168.1.3/49
Aug 26 12:40:01.249: TAC+: Opened 192.168.1.3 index=1
Aug 26 12:40:01.250: TAC+: 192.168.1.3 (3653537180) AUTHOR/START queued
Aug 26 12:40:01.449: TAC+: (3653537180) AUTHOR/START processed
Aug 26 12:40:01.449: TAC+: (-641430116): received author response status = FAIL
Aug 26 12:40:01.450: TAC+: Closing TCP/IP 0x3BE31D1C connection to 192.168.1.3/49
```

A network administrator logs into the router using TACACS+ username and password credentials, but the administrator cannot run any privileged commands. Which action resolves the issue?

- A. Configure TACACS+ synchronization with the Active Directory admin group
- B. Configure the username from a local database
- C. Configure full access for the username from TACACS+ server
- D. Configure an authorized IP address for this user to access this router

**Answer:** C

**NEW QUESTION 373**

- (Exam Topic 2)

```

R1
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0
router eigrp 100
 no auto-summary
 network 192.168.12.0
 network 172.16.0.0
 neighbor 192.168.12.2 FastEthernet0/0

R2
interface Loopback0
 ip address 172.16.2.2 255.255.255.255
interface FastEthernet0/0
 ip address 192.168.12.2 255.255.255.0
router eigrp 100
 network 192.168.12.0
 network 172.16.0.0
 neighbor 192.168.12.1 FastEthernet0/0
 passive-interface FastEthernet0/0
    
```

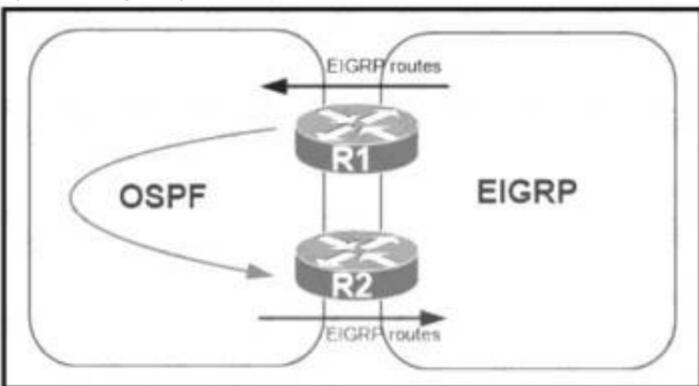
Refer to the exhibit. R1 and R2 cannot establish an EIGRP adjacency. Which action establishes EIGRP adjacency?

- A. Remove the current autonomous system number on one of the routers and change to a different value.
- B. Remove the passive-interface command from the R2 configuration so that it matches the R1 configuration.
- C. Add the no auto-summary command to the R2 configuration so that it matches the R1 configuration.
- D. Add the passive-interface command to the R1 configuration so that it matches the R2 configuration.

**Answer: B**

**NEW QUESTION 378**

- (Exam Topic 2)



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

- A. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag on R2 to deny when redistributing OSPF into EIGRP.
- B. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag on R2 to allow when redistributing OSPF into EIGRP.
- C. Advertise summary routes of EIGRP to OSPF and deny specific EIGRP routes when redistributing into OSPF.
- D. Apply a prefix list of EIGRP network routes in OSPF domain on R1 to propagate back into the EIGRP routing domain.

**Answer: A**

**Explanation:**

When doing mutual redistribution at multiple points (between OSPF and EIGRP on R1 & R2), we may create routing loops so we should use route-map to prevent redistributed routes from redistributing again into the original domain.

In the below example, the route-map "SET-TAG" is used to prevent any routes that have been redistributed into EIGRP from redistributed again into OSPF domain by tagging these routes with tag 1:

```

R3
route-map SET-TAG permit 10
 set tag 1
    
```

These routes are prevented from redistributed again by route-map FILTER\_TAG by denying any routes with tag 1 set:

```

R4
route-map FILTER-TAG deny 10
 match tag 1
    
```

**NEW QUESTION 379**

- (Exam Topic 2)

An engineer configured SNMP notifications sent to the management server using authentication and encrypting data with DES. An error in the response PDU is received as "UNKNOWNUSERNAME. WRONGDIGEST". Which action resolves the issue?

- A. Configure the correct authentication password using SNMPv3 authPriv .
- B. Configure the correct authentication password using SNMPv3 authNoPriv.
- C. Configure correct authentication and privacy passwords using SNMPv3 authNoPriv.
- D. Configure correct authentication and privacy passwords using SNMPv3 authPriv.

**Answer: D**

**Explanation:**

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm>

**NEW QUESTION 384**

- (Exam Topic 2)

What statement about route distinguishes in an MPLS network is true?

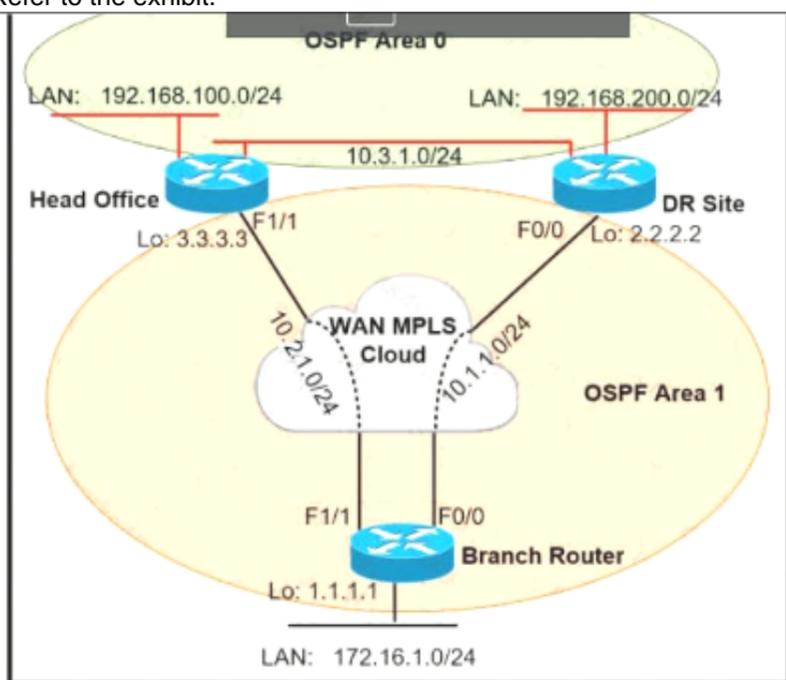
- A. Route distinguishes make a unique VPNv4 address across the MPLS network.
- B. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.
- C. Route distinguishers are used for label bindings
- D. Route distinguishers define which prefixes are imported and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

**Answer: A**

**NEW QUESTION 387**

- (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 390**

- (Exam Topic 2)

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

- A. LSP
- B. RSVP
- C. ECMP
- D. LDP
- E. MPLS OAM

**Answer: BD**

**NEW QUESTION 394**

- (Exam Topic 2)

Refer to the exhibit.

```
R1
ip prefix-list ccnp1 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 ccnp1
 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 399**

- (Exam Topic 2)

Drag and drop the LDP features from the left onto the descriptions on the right

implicit null label	provides ways of improving load balancing by eliminating the need for DPI at transit LSRs
explicit null label	LSR receives an MPLS header with the label set to 3
inbound label binding filtering	packet is encapsulated in MPLS with the option of copying the IP precedence to EXP bits
entropy label	controls the amount of memory used to store LDP label bindings advertised by other devices

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Diagram Description automatically generated

The MPLS LDP Inbound Label Binding Filtering feature can be used to control the amount of memory used to store Label Distribution Protocol (LDP) label bindings advertised by other devices. For example, in a simple Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment, the VPN provider edge (PE) devices might require label switched paths (LSPs) only to their peer PE devices (that is, they do not need LSPs to core devices). Inbound label binding filtering enables a PE device to accept labels only from other PE devices.

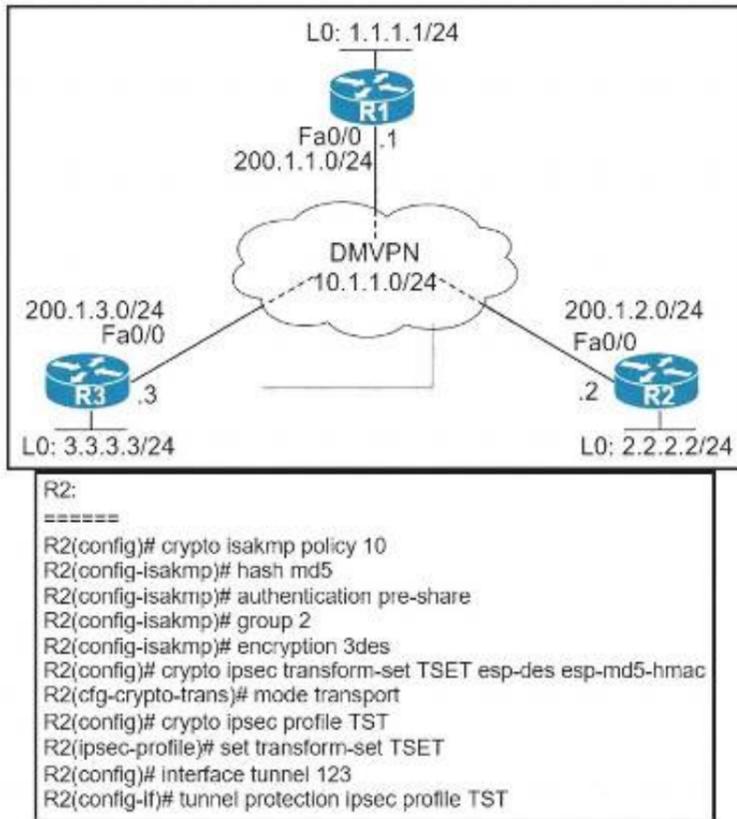
Reference:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp\\_ldp/configuration/15-sy/mp-ldp-15-sy-book/mp-ldp-inbound-filtr.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/15-sy/mp-ldp-15-sy-book/mp-ldp-inbound-filtr.html)

**NEW QUESTION 404**

- (Exam Topic 2)

Refer to the exhibits.



When DMVPN is configured, which configuration allows spoke-to-spoke communication using loopback as a tunnel source?

- A. Configure crypto isakmp key cisco address 0.0.0.0 on the hub.
- B. Configure crypto isakmp key Cisco address 200.1.0.0 255.255.0.0 on the hub.
- C. Configure crypto isakmp key cisco address 200.1.0.0 255.255.0.0 on the spokes.
- D. Configure crypto isakmp key cisco address 0.0.0.0 on the spokes.

**Answer: D**

**Explanation:**

[https://www.cisco.com/en/US/technologies/tk583/tk372/technologies\\_white\\_paper0900aecd802b8f3c.html](https://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd802b8f3c.html)

**NEW QUESTION 405**

- (Exam Topic 2)

What are two MPLS label characteristics? (Choose two.)

- A. The label edge router swaps labels on the received packets.
- B. Labels are imposed in packets after the Layer 3 header.
- C. LDP uses TCP for reliable delivery of information.
- D. An MPLS label is a short identifier that identifies a forwarding equivalence class.
- E. A maximum of two labels can be imposed on an MPLS packet.

**Answer: CD**

**Explanation:**

Reference:

<https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html>

**NEW QUESTION 410**

- (Exam Topic 2)

Refer to the exhibit.

```

Router#show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(1)
Interface      Xmit Queue PeerQ      Mean Pacing Time Multicast F
Peers Un/Reliable Un/Reliable SRTT Un/Reliable Flow T
Lo0            0      0/0      0/0      0      0/0      0      0
Fa0/0         1      0/0      0/0      7      0/2      50     0

Router#show running-config | section eigrp
router eigrp 1
 network 172 16 0 0 0 0 255
 network 192 168 2 2 0 0 0
 network 192 168 12 2 0 0 0

Router#show running-config interface Fa0/3
Building configuration

Current configuration 93 bytes
!
interface FastEthernet0/3
 ip vrf forwarding CLIENT1
 ip address 172 16 0 1 255 255 255 0
    
```

While troubleshooting an EIGRP neighbor adjacency problem, the network engineer notices that the interface connected to the neighboring router is not participating in the EIGRP process. Which action resolves the issues?

- A. Configure the network command to network 172.16.0.1 0.0.0.0
- B. Configure the network command under EIGRP address family vrf CLIENT1
- C. Configure EIGRP metrics on interface FastEthernet0/3
- D. Configure the network command under EIGRP address family ipv4

**Answer:** B

**Explanation:**

```
router eigrp 1
!
address-family ipv4 vrf CLIENT1 network 172.16.0.0 0.0.0.255
no auto-summary autonomous-system 1 exit-address-family
```

**NEW QUESTION 413**

- (Exam Topic 2)

Drag and drop the MPLS VPN device types from the left onto the definitions on the right.

Customer (C) device	device in the core of the provider network that switches MPLS packets
CE device	device that attaches and detaches the VPN labels to the packets in the provider network
PE device	device in the enterprise network that connects to other customer devices
Provider (P) device	device at the edge of the enterprise network that connects to the SP network

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, application Description automatically generated

**NEW QUESTION 417**

- (Exam Topic 2)

Drag and drop the actions from the left into the correct order on the right to configure a policy to avoid following packet forwarding based on the normal routing path.

Configure route map instances.	step 1
Configure set commands.	step 2
Configure fast switching for PBR.	step 3
Configure ACLs.	step 4
Configure match commands.	step 5
Configure PBR on the interface.	step 6

- A. Mastered
- B. Not Mastered

**Answer:** A

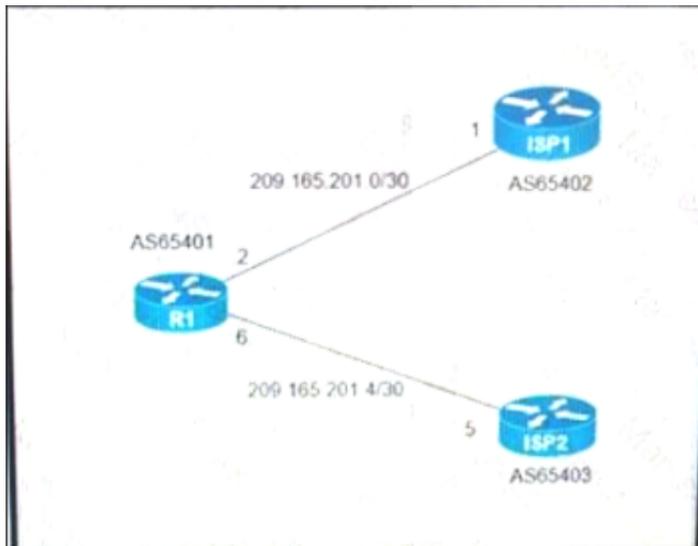
**Explanation:**

<https://community.cisco.com/t5/networking-documents/how-to-configure-pbr/ta-p/3122774>

**NEW QUESTION 420**

- (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 Null0
ip route 209.165.202.128 255.255.255.224 Null0
!

```

A company with autonomous system number AS65401 has obtained IP address block 209.165.200.224/27 from ARIN. The company needed more IP addresses and was assigned block 209.165.202.128/27 from ISP2. An engineer at ISP1 reports they are receiving ISP2 routes from AS65401. Which configuration on R1 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 423**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

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

2nd - Questions and Answers in PDF Format

### **300-410 Practice Exam Features:**

- \* 300-410 Questions and Answers Updated Frequently
- \* 300-410 Practice Questions Verified by Expert Senior Certified Staff
- \* 300-410 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 300-410 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 300-410 Practice Test Here](#)**